

# Configuración de Cisco ISE 3.2 EAP-TLS con Microsoft Azure Active Directory

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe cómo configurar y resolver problemas de políticas de autorización en ISE basadas en la pertenencia al grupo de Azure AD y otros atributos de usuario con EAP-TLS o TEAP como protocolos de autenticación.

Colaboró Emmanuel Cano, Ingeniero de consultoría de seguridad, y Romeo Migisha, Ingeniero de consultoría técnica

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- Microsoft Azure AD, suscripción y aplicaciones
- EAP-TLS autenticación

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE 3.2
- Microsoft Azure AD

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

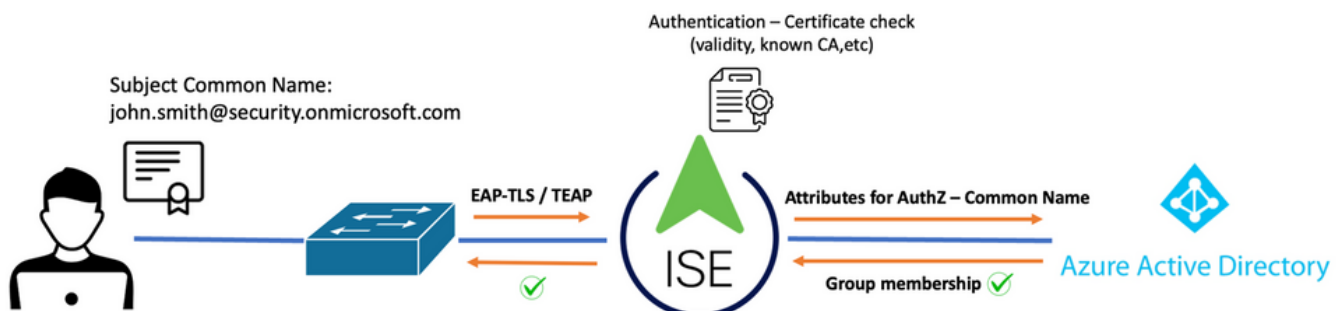
En ISE 3.0 es posible aprovechar la integración entre ISE y Azure Active Directory (AAD) para autenticar a los usuarios basándose en los grupos y atributos de Azure AD a través de la comunicación de credenciales de contraseña de propietario de recurso (ROPC). Con ISE 3.2, puede configurar la autenticación basada en certificados y se puede autorizar a los usuarios en función de las pertenencias a grupos de Azure AD y otros atributos. ISE consulta a Azure a través de la API gráfica para obtener grupos y atributos para el usuario autenticado. Utiliza el nombre común de sujeto (CN) del certificado con el nombre principal de usuario (UPN) en el lado de Azure.

**Nota:** las autenticaciones basadas en certificados pueden ser EAP-TLS o TEAP con EAP-TLS como método interno. A continuación, puede seleccionar atributos de Azure Active Directory y agregarlos al diccionario de Cisco ISE. Estos atributos se pueden utilizar para la autorización. Sólo se admite la autenticación de usuario.

## Configurar

### Diagrama de la red

La siguiente imagen proporciona un ejemplo de un diagrama de red y flujo de tráfico



### Procedimiento:

1. El certificado se envía a ISE a través de EAP-TLS o TEAP con EAP-TLS como método interno.
2. ISE evalúa el certificado del usuario (período de validez, CA de confianza, CRL, etc.).
3. ISE toma el nombre del sujeto del certificado (CN) y realiza una búsqueda en la API de Microsoft Graph para obtener los grupos del usuario y otros atributos de dicho usuario. Esto se conoce como Nombre principal de usuario (UPN) en el lado de Azure.
4. Las políticas de autorización de ISE se evalúan en función de los atributos del usuario devueltos desde Azure.

**Nota:** debe configurar y conceder permisos de la API de Graph a la aplicación ISE en Microsoft Azure, como se muestra a continuación:

API / Permissions name	Type	Description
<a href="#">Microsoft Graph (3)</a>		
<a href="#">Group.Read.All</a>	Application	Read all groups
<a href="#">User.Read</a>	Delegated	Sign in and read user profile
<a href="#">User.Read.All</a>	Application	Read all users' full profiles

## Configuraciones

### Configuración de ISE

**Nota:** la funcionalidad de ROPC y la integración entre ISE y Azure AD están fuera del alcance de este documento. Es importante que los grupos y los atributos de usuario se agreguen desde Azure. Consulte la guía de configuración [aquí](#).

### Configuración del perfil de autenticación de certificados

**Paso 1.** Desplácese hasta el icono Menú  situado en la esquina superior izquierda y seleccione **Administration > Identity Management > External Identity Sources**.

**Paso 2.** Seleccionar **Autenticación de certificados** Haga clic en Perfil y, a continuación, en **Agregar**.

**Paso 3.** Defina el nombre, Defina el **Almacén de identidades** como [No aplicable] y seleccione Asunto - Nombre común en **Usar identidad de** campo. Seleccione Nunca al coincidir **Certificado de cliente contra certificado en almacén de identidades** 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

**Paso 4.** Haga clic en **Guardar**

Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings


### Certificate Authentication Profile


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

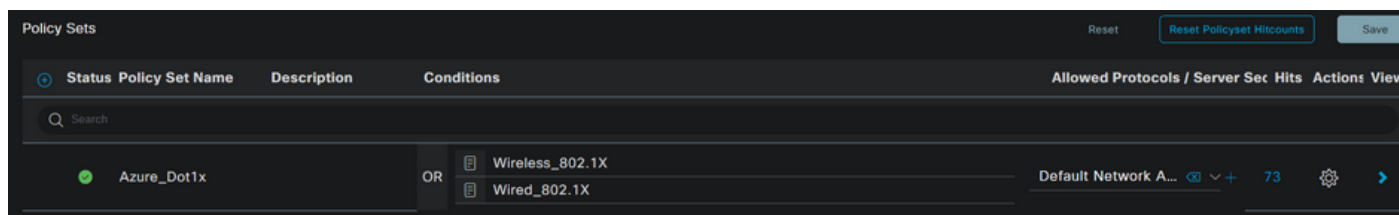
Edit + Add Duplicate Delete


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

**Paso 5.** Desplácese hasta el icono Menú  situado en la esquina superior izquierda y seleccione **Directiva > Conjuntos de directivas**.

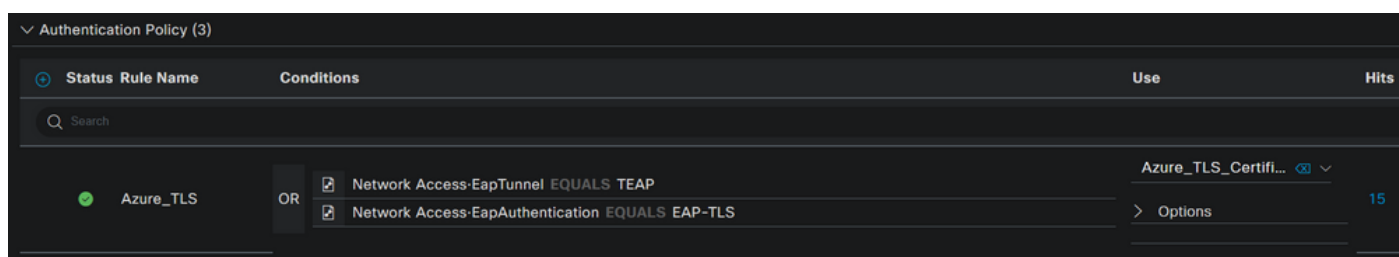
**Paso 6.** Seleccione el signo más  para crear un nuevo conjunto de directivas. Defina un

nombre y seleccione Wireless 802.1x (Inalámbrico 802.1x) o Wired 802.1x (con cables 802.1x) como condiciones. En este ejemplo se utiliza la opción Default Network Access (Acceso a red predeterminado)

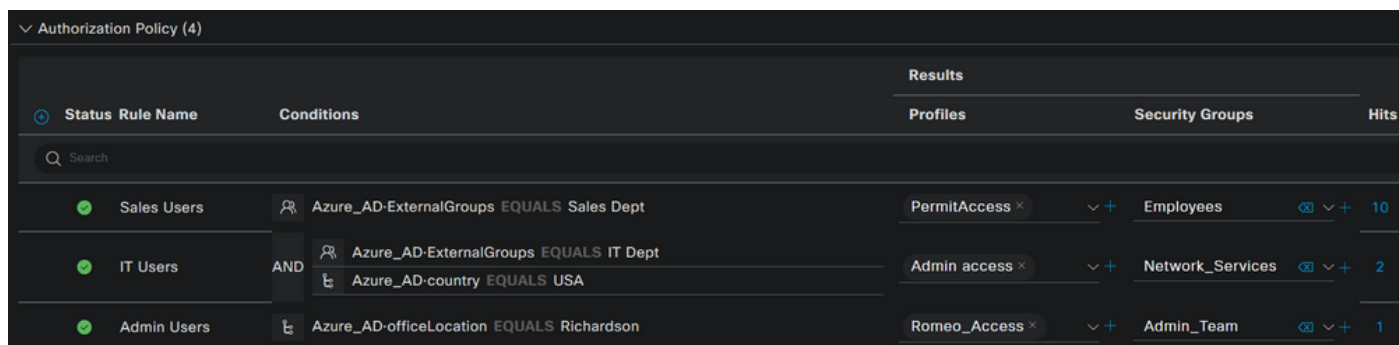


**Paso 7.** Seleccione la flecha  junto a Acceso a red predeterminado para configurar las directivas de autenticación y autorización.

**Paso 8.** Seleccione la opción Authentication Policy , defina un nombre y agregue EAP-TLS como Network Access EAPuthentication , es posible agregar TEAP como Network Access EAPunnel si TEAP se utiliza como protocolo de autenticación. Seleccione el perfil de autenticación de certificado creado en el paso 3 y haga clic en **Guardar**.



**Paso 9.** Seleccione la opción de directiva de autorización, defina un nombre y agregue atributos de usuario o grupo de Azure AD como condición. Elija el perfil o el grupo de seguridad en Resultados, en función del caso práctico y, a continuación, haga clic en **Guardar**.



## Configuración de usuario.

El nombre común de sujeto (CN) del certificado de usuario debe coincidir con el nombre principal de usuario (UPN) en el lado de Azure para recuperar la pertenencia al grupo de AD y los atributos de usuario que se utilizarán en las reglas de autorización. Para que la autenticación sea correcta, la CA raíz y cualquier certificado de CA intermedia deben estar en el almacén de confianza de ISE.



**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
<b>User principal name</b>	<b>john.smith@romlab.onmicrosoft.com</b>
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

## Verificación

### Verificación de ISE

En la GUI de Cisco ISE, haga clic en el icono Menu (Menú)  y elija **Operations > RADIUS > Live Logs** para autenticaciones de red (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

Haga clic en el icono de lupa de la columna Detalles para ver un informe de autenticación detallado y confirmar si el flujo funciona según lo esperado.

1. Verificar las políticas de autenticación/autorización
2. Método/protocolo de autenticación

3. Nombre de asunto del usuario tomado del certificado

4. Grupos de usuarios y otros atributos obtenidos del directorio de Azure

## 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		

## Troubleshoot

### Habilitar depuraciones en ISE

Desplácese hasta **Administration > System > Logging > Debug Log Configuration** para establecer los componentes siguientes en el nivel especificado.

Nodo	Nombre del componente	Nivel de registro	Nombre de archivo de registro
PSN	rest-id-store	Depurar	rest-id-store.log
PSN	Runtime-AAA	Depurar	prrt-server.log

**Nota:** Cuando haya terminado con la resolución de problemas, recuerde reiniciar las depuraciones. Para ello, seleccione el nodo relacionado y haga clic en "Restablecer a valor

predeterminado".

## Fragmentos de registro

Los siguientes extractos muestran las dos últimas fases del flujo, como se mencionó anteriormente en la sección del diagrama de red.

1. ISE toma el nombre del sujeto del certificado (CN) y realiza una búsqueda en la API de Azure Graph para obtener los grupos de usuarios y otros atributos para ese usuario. Esto se conoce como Nombre principal de usuario (UPN) en el lado de Azure.
2. Las políticas de autorización de ISE se evalúan en función de los atributos del usuario devueltos desde Azure.

### Registros de Rest-id:

```
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
```

### Registros de puerto:

```
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
```

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).