Configuración de ISE 3.0 REST ID con Azure Active Directory

Contenido

Introducción

Este documento describe la integración de Cisco ISE 3.0 con Azure AD implementada a través del servicio de identidad REST con credenciales de contraseña de propietario de recurso.

Antecedentes

Este documento describe cómo configurar y solucionar problemas de integración de Identity Services Engine (ISE) 3.0 con Microsoft (MS) Azure Active Directory (AD) implementado a través del servicio de identidad (ID) de transferencia de estado representacional (REST) con la ayuda de Credenciales de contraseña de propietario de recurso (ROPC).

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- ISE
- MS Azure AD
- Comprensión de la implementación y limitaciones del protocolo ROPC; link

Componentes Utilizados

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

- Cisco ISE versión 3.0

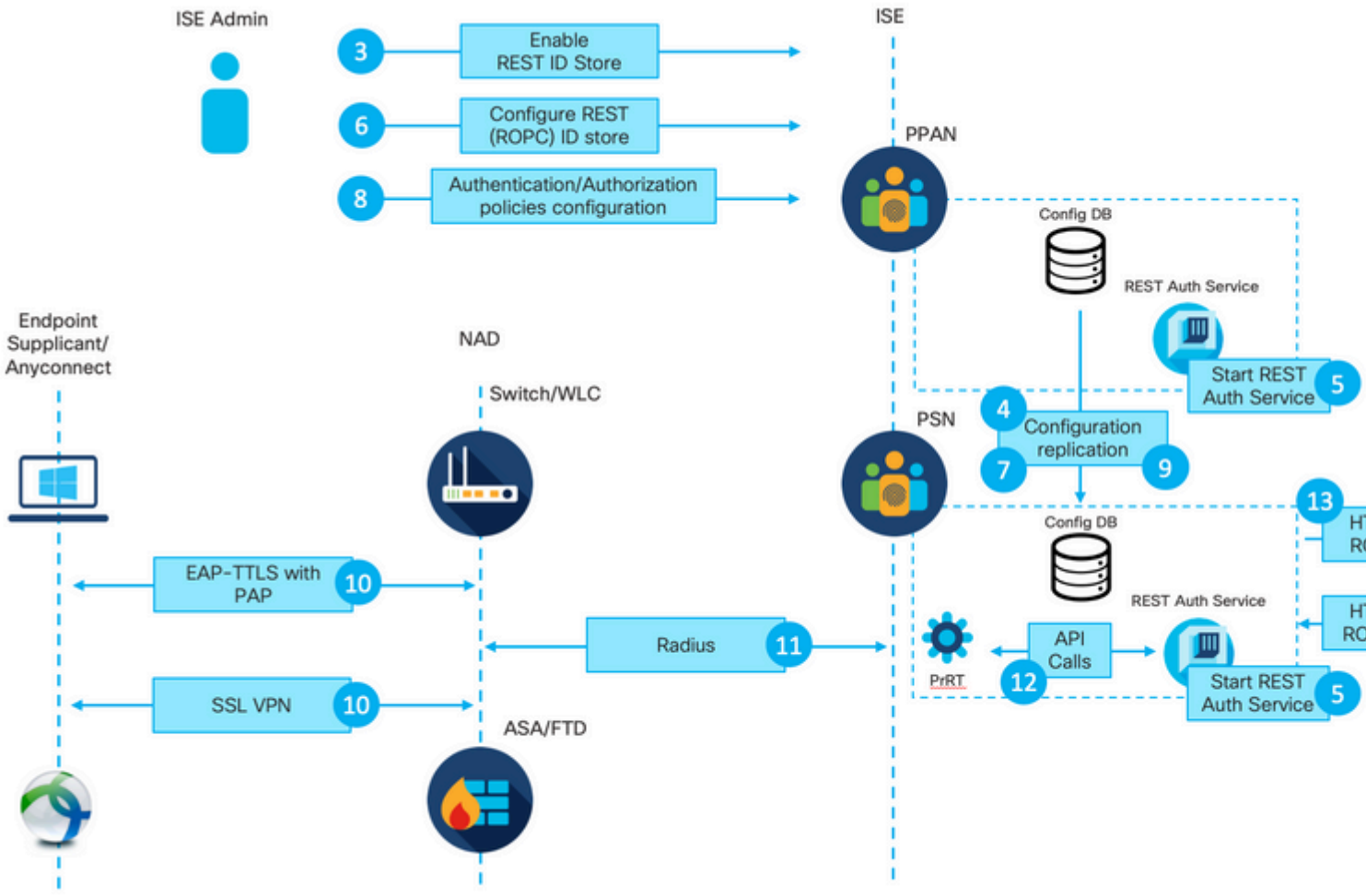
- MS Azure AD
- WS-C3850-24P con software 16.9.2
- ASAv con 9.10 (1)
- Windows 10.0.18363

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.

Configurar

La funcionalidad ISE REST ID se basa en el nuevo servicio introducido en ISE 3.0: REST Auth Service. Este servicio es responsable de la comunicación con Azure AD a través de intercambios ROPC de autorización abierta (OAuth) para realizar la autenticación de usuarios y la recuperación de grupos. El servicio de autenticación REST está deshabilitado de forma predeterminada y, una vez que el administrador lo habilita, se ejecuta en todos los nodos ISE de la implementación. Dado que la comunicación del servicio de autenticación REST con la nube se produce cuando, en el momento de la autenticación del usuario, cualquier retraso en la ruta conlleva latencia adicional en el flujo de autenticación/autorización. Esta latencia está fuera del control de ISE y cualquier implementación de REST Auth debe planificarse y probarse cuidadosamente para evitar el impacto en otros servicios de ISE.

Descripción general del flujo de alto nivel



1. El administrador de la nube de Azure crea un nuevo registro de aplicación (App). Los detalles de esta aplicación se utilizan posteriormente en ISE para establecer una conexión con Azure AD.

2. El administrador de la nube de Azure debe configurar la aplicación con:

- Crear un secreto de cliente
- Activar ROPC
- Agregar notificaciones de grupo
- Definir los permisos de la interfaz de programación de aplicaciones (API)

3. El administrador de ISE activa el servicio de autenticación REST. Debe hacerse antes de que se pueda ejecutar cualquier otra acción.

4. Los cambios se escriben en la base de datos de configuración y se replican en toda la implementación de ISE.

5. El servicio de autenticación REST se inicia en todos los nodos.

6. ISE Admin configura el almacén de ID de REST con los detalles del paso 2.

7. Los cambios se escriben en la base de datos de configuración y se replican en toda la implementación de ISE.

8. El administrador de ISE crea una nueva secuencia de almacén de identidad o modifica la que ya existe y configura las políticas de autenticación/autorización.

9. Los cambios se escriben en la base de datos de configuración y se replican en toda la implementación de ISE.

10. El terminal inicia la autenticación. Según la especificación del protocolo ROPC, la contraseña de usuario debe proporcionarse a la plataforma de identidad de Microsoft en texto no cifrado a través de una conexión HTTP cifrada; debido a este hecho, las únicas opciones de autenticación disponibles admitidas por ISE hasta el momento son:

- Protocolo de autenticación extensible-Seguridad de la capa de transporte en túnel (EAP-TTLS) con protocolo de autenticación de contraseña (PAP) como método interno
- Autenticación VPN SSL de AnyConnect con PAP

11. Exchange con ISE Policy Service Node (PSN) a través de Radius.

12. Process Runtime (PrRT) envía una solicitud al servicio REST ID con los detalles del usuario (nombre de usuario/contraseña) a través de la API interna.

13. El servicio de ID de REST envía la solicitud ROPC de OAuth a Azure AD a través de Protocolo de transferencia de hipertexto seguro (HTTPS).

14. Azure AD realiza la autenticación de usuarios y recupera los grupos de usuarios.

15. Resultado de autenticación/autorización devuelto a ISE.

Después del punto 15, el resultado de la autenticación y los grupos obtenidos volvieron a PrRT, lo que implica un flujo de evaluación de políticas y asigna el resultado final de autenticación/autorización. Access-Accept con atributos del perfil de autorización o Access-Reject devuelto al dispositivo de acceso a la red (NAD).

Configurar Azure AD para la integración

1. Localice AppRegistration Service como se muestra en la imagen.

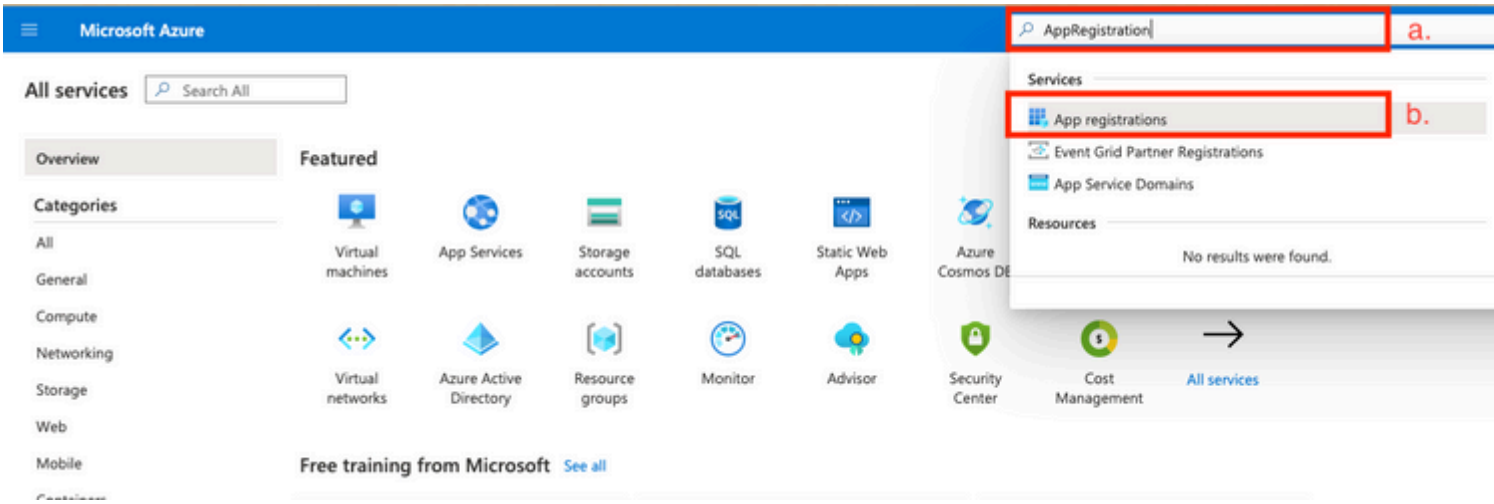


Figura 2

a. Escriba AppRegistration en la barra de búsqueda global.

b. Haga clic en el servicio de registro de aplicaciones.

2. Cree un nuevo registro de aplicación.

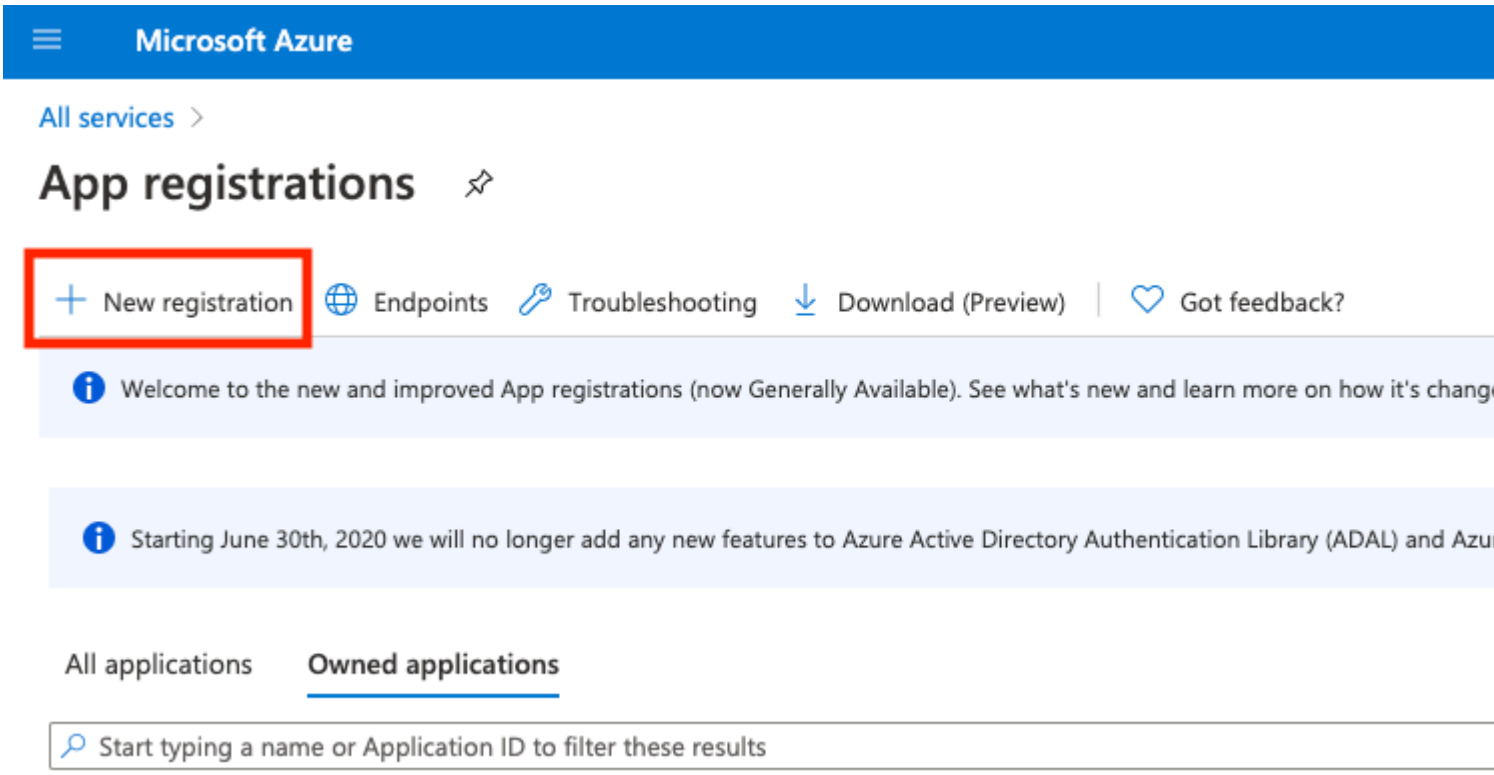


Figura 3.

3. Registrar una nueva Aplicación.

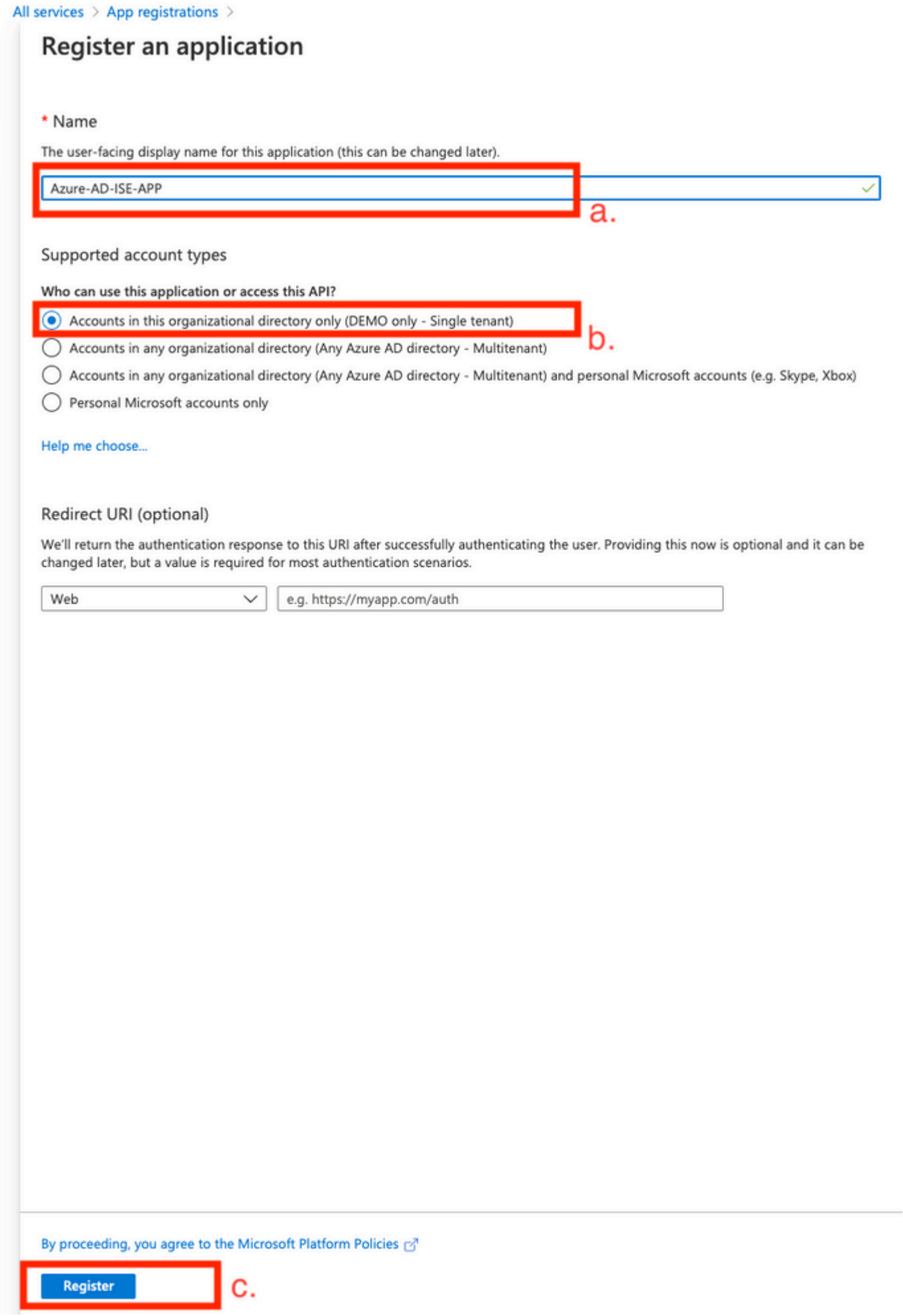


Figura 4

- Definir el nombre de la aplicación

: los datos del grupo de usuarios se pueden obtener de Azure AD de varias maneras con la ayuda de diferentes permisos de API. El método descrito en este ejemplo ha demostrado ser exitoso en el laboratorio del TAC de Cisco. Utilice otros permisos de API en caso de que el administrador de Azure AD lo recomiende.

16. Grant admin consent para permisos de API.

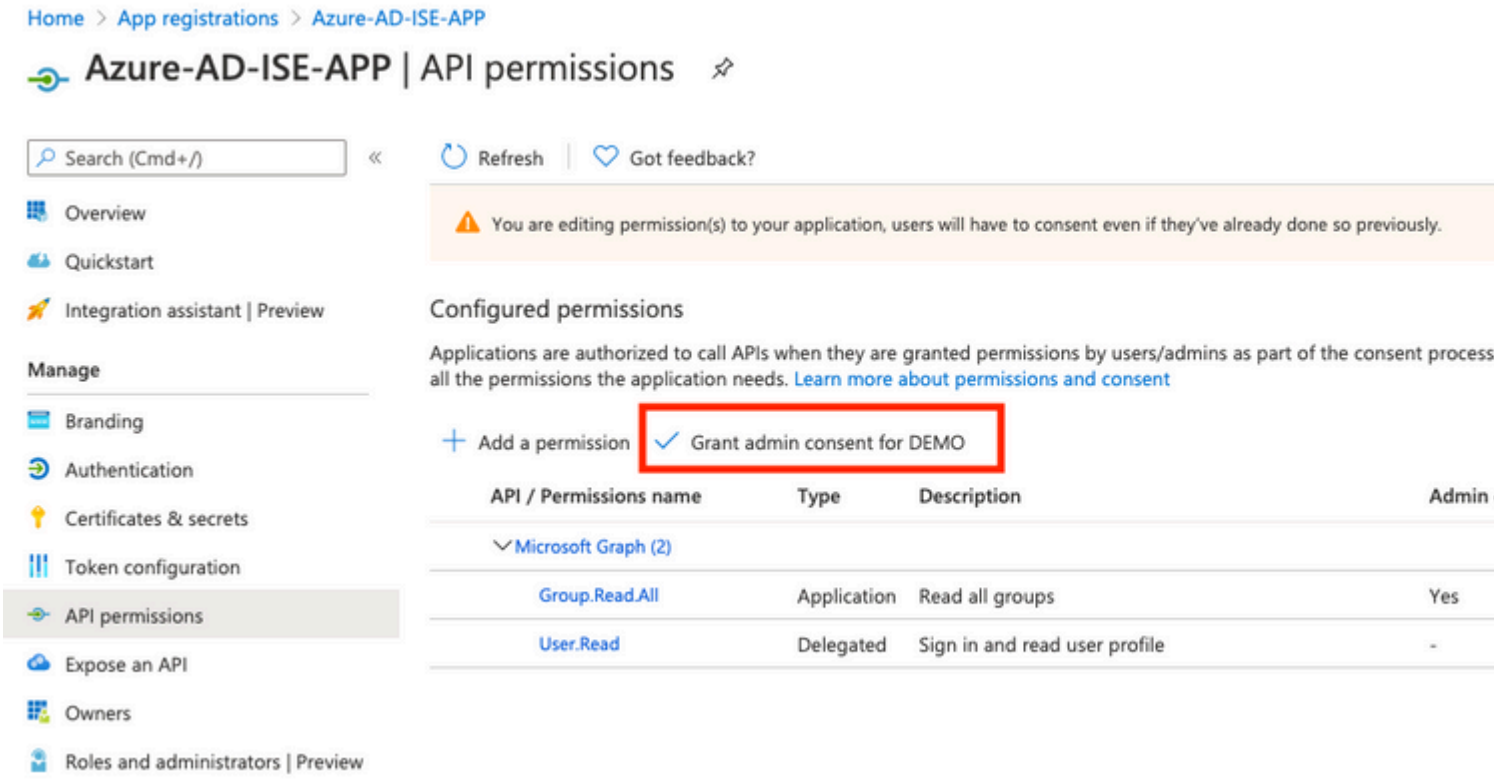


Figura 17

17. Confirme el consentimiento de concesión para el administrador.

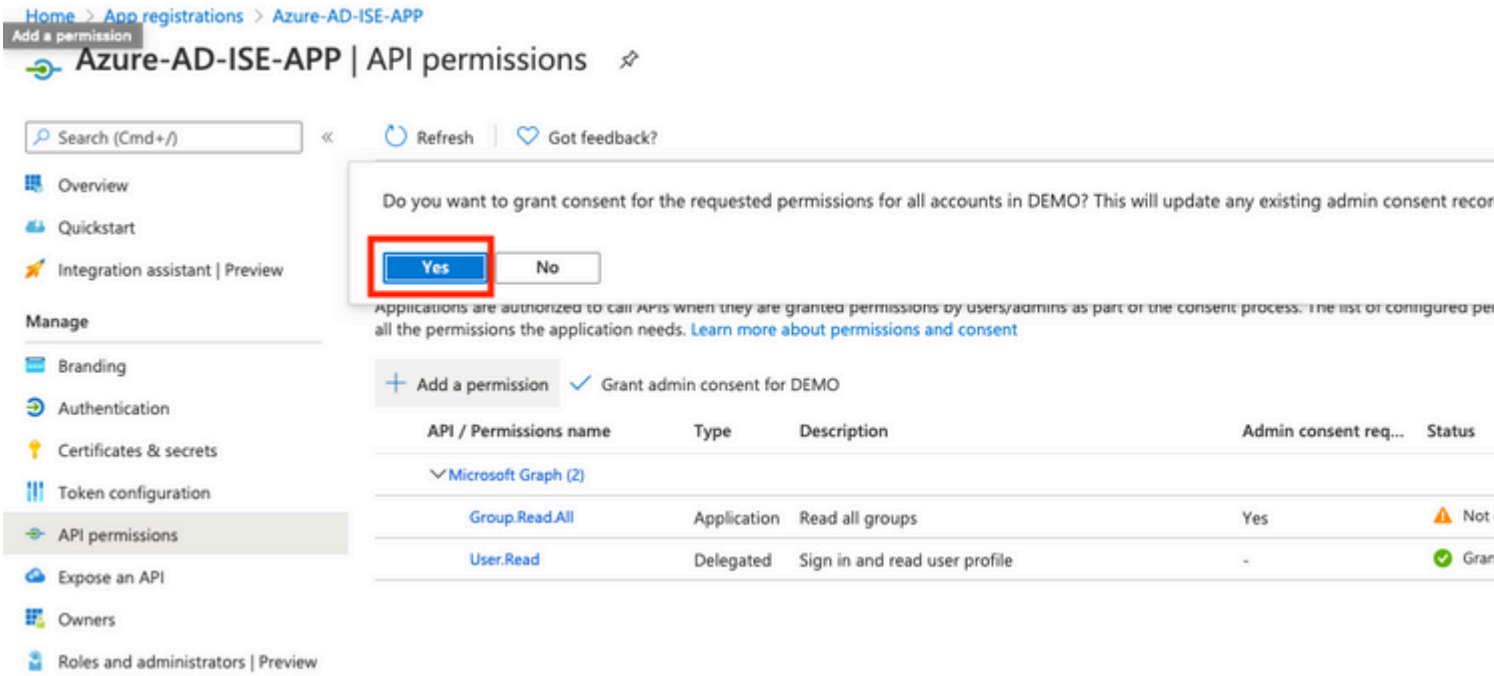


Figura 18

En este momento, puede considerar la integración completamente configurada en el lado de Azure AD.

Configuración de ISE para la integración

1. Acceda a Configuración de gestión de identidades.

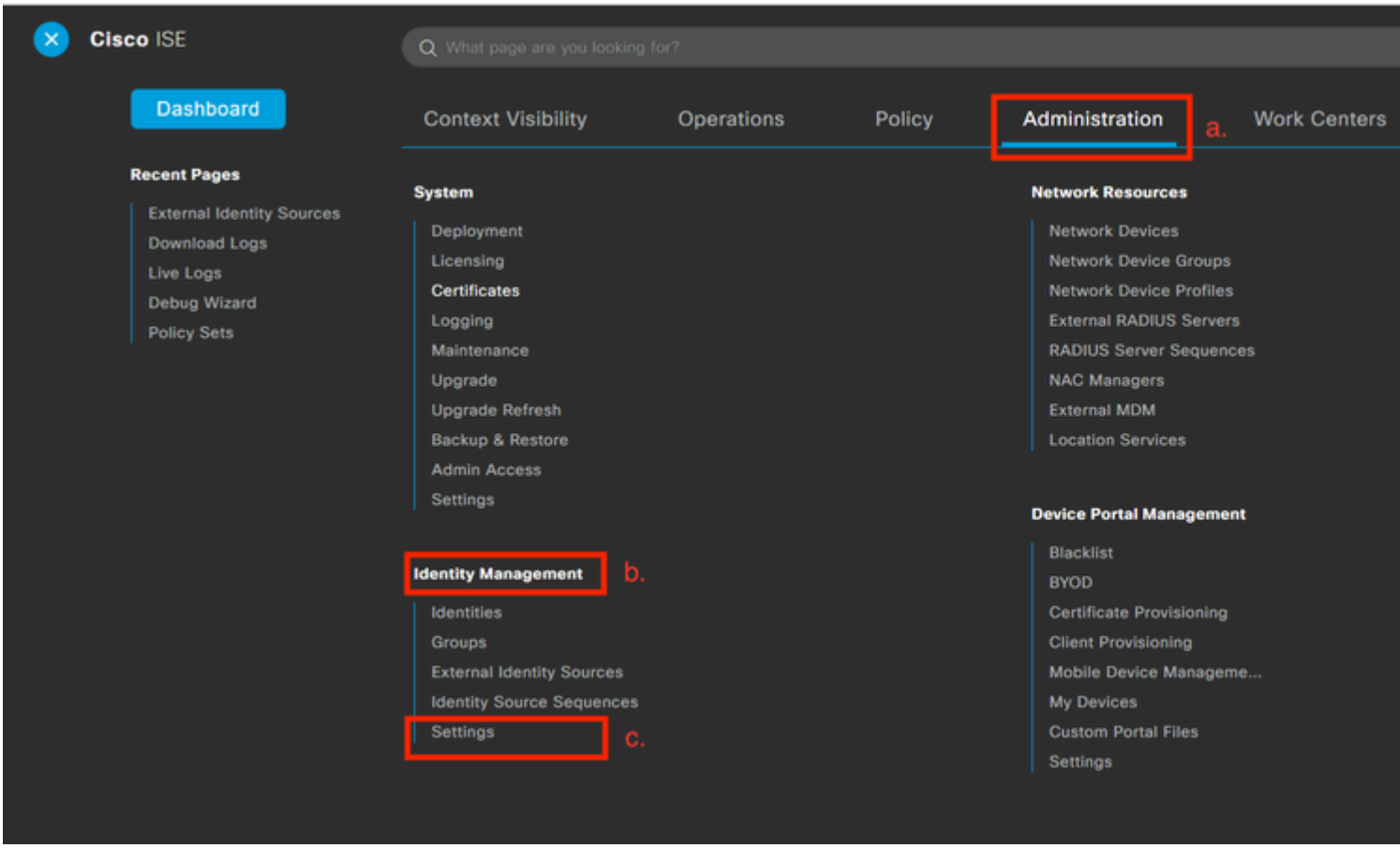


Figura 19

Desplácese hasta Administration > Identity Management> Settings .

2. Active el servicio REST ID (desactivado de forma predeterminada).

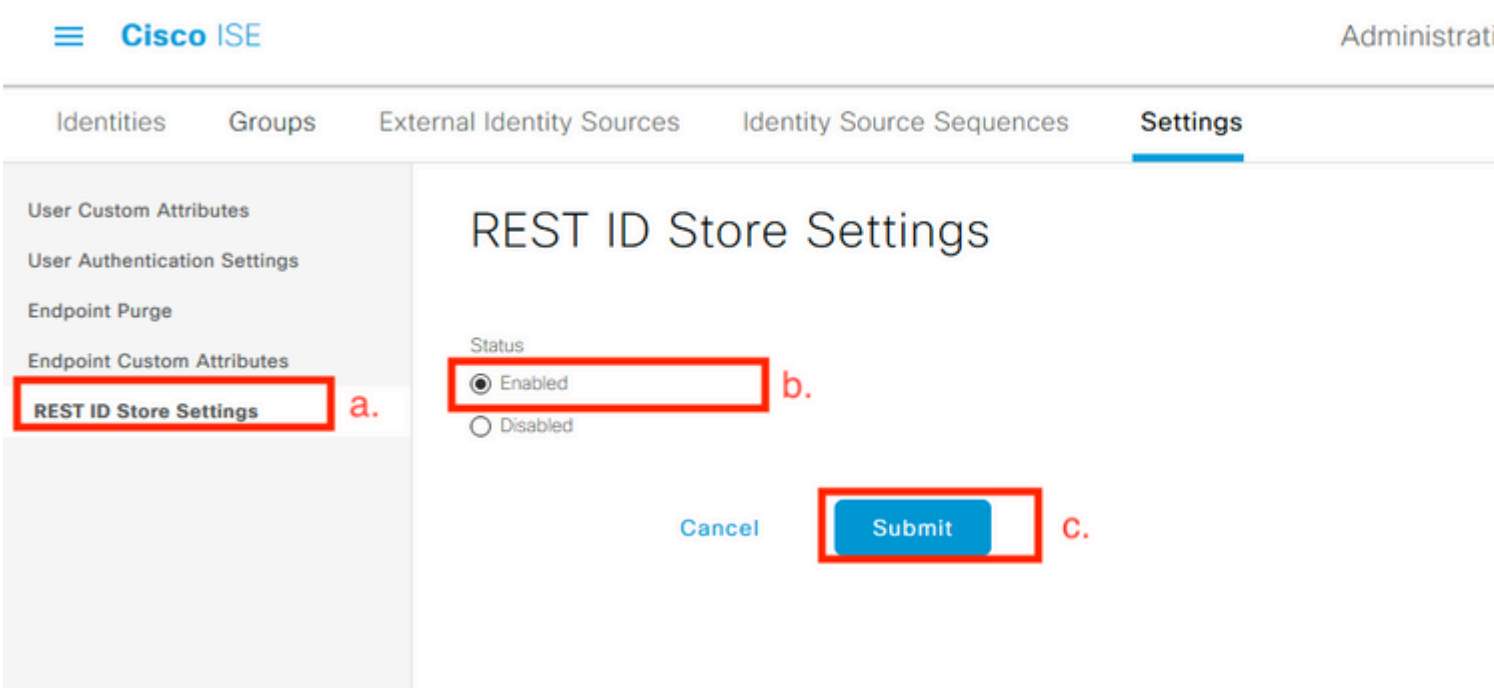


Figura 20

Desplácese hasta REST ID Store Settings y cambiar el estado de REST ID Store Settings para Enable,luego Submit sus cambios.

3. Cree un almacén de ID de REST.

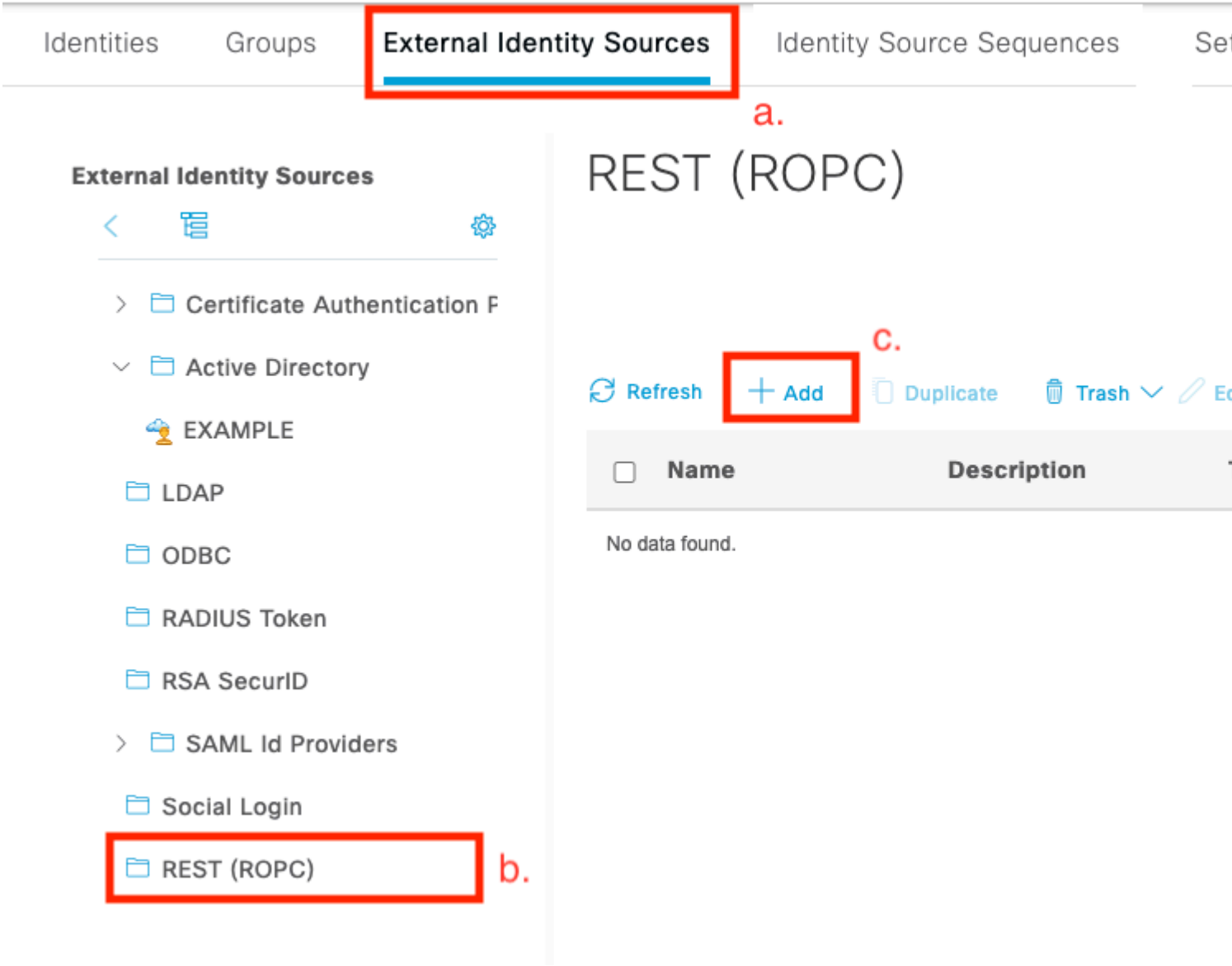


Figura 21

Cambie a la External Identity Sources , haga clic en REST (ROPC) y haga clic en **Agregar**.

4. Configure el almacén de ID de REST.

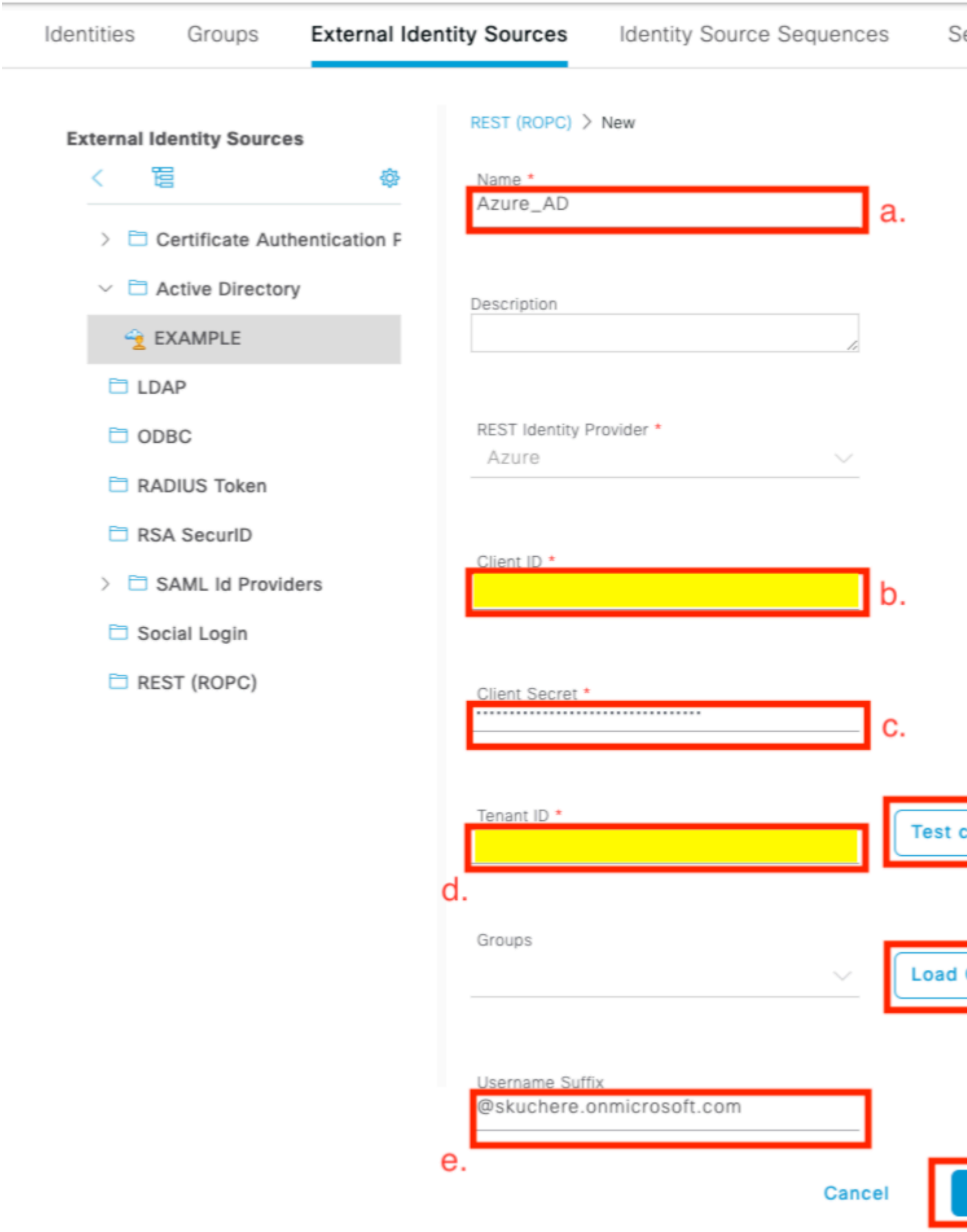

Identities
Groups
External Identity Sources
Identity Source Sequences
External Identity Sources
Certificate Authentication F
Active Directory
EXAMPLE
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
REST (ROPC)
REST (ROPC) > New
Name *
Azure_AD
a.
Description
REST Identity Provider *
Azure
Client ID *
b.
Client Secret *
c.
Tenant ID *
Test c
d.
Groups
Load
Username Suffix
@skuchere.onmicrosoft.com
e.
Cancel

Figura 22

a. Defina el nombre del almacén de ID. Más adelante, este nombre se puede encontrar en la lista de diccionarios ISE al configurar las políticas de autorización. Además, este nombre se muestra en la lista de almacenes de ID disponibles en la configuración de la directiva de autenticación y en la lista de almacenes de ID disponibles en la configuración de secuencia del almacén de identidad.

b. Proporcione el ID de cliente (tomado de Azure AD en el paso 8 de la sección de configuración de la integración de Azure AD).

c. Proporcione el secreto de cliente (tomado de Azure AD en el paso 7 de la sección de configuración de la integración de Azure AD).

d. Proporcione la ID de arrendatario (tomada de Azure AD en el paso 8 de la sección de configuración de la integración de Azure AD).

e. Configurar nombre de usuario Sufijo: de forma predeterminada, ISE PSN utiliza un nombre de usuario proporcionado por el usuario final, que se proporciona en el formato sAMAccountName (nombre de usuario corto, por ejemplo, bob); en este caso, Azure AD no puede localizar al usuario. El sufijo de nombre de usuario es el valor agregado al nombre de usuario proporcionado por el usuario para llevar el nombre de usuario al formato UPN.

> **Nota**: ROPC está limitado a la autenticación de usuario, ya que se basa en el atributo Username durante la autenticación. Los objetos de dispositivo de Azure AD no tienen atributos de nombre de usuario.

---

f. Presione en Probar conexión para confirmar que ISE puede usar los detalles de la aplicación proporcionados para establecer una conexión con Azure AD.

g Presione en Cargar grupos para agregar grupos disponibles en el almacén de ID de Azure AD a REST. En el ejemplo siguiente se muestra el aspecto de la experiencia del administrador.

> **Nota**: Tenga en cuenta el ID de bug de Cisco CSCvx00345 defectuoso, ya que hace que los grupos no se carguen. El defecto se corrige en el parche 2 de ISE 3.0.

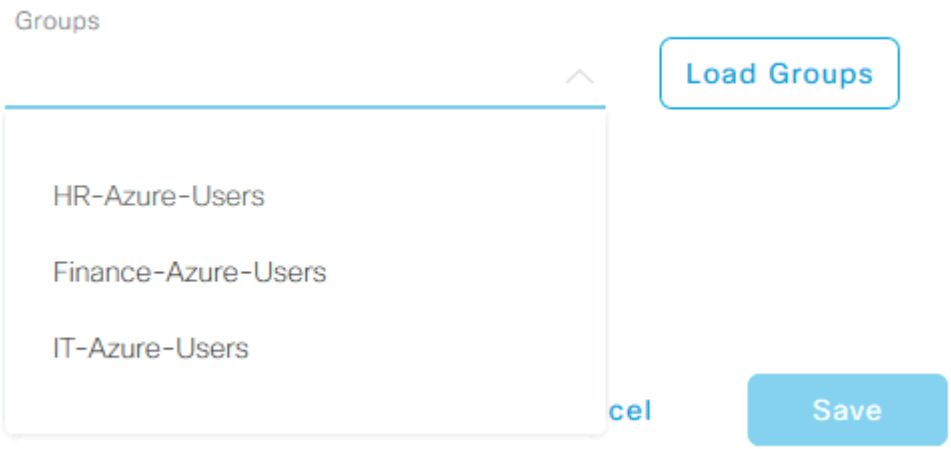


Figura 23

h. Envíe los cambios.

5. En este paso, considere la creación de una nueva secuencia de almacén de identidades, que incluya un almacén de ID de REST recién creado.

6. En el momento en que el almacén de ID de REST o la secuencia de almacén de identidades que lo contiene están asignados a la política de autenticación, cambie una acción predeterminada para Falla de Proceso de DROP a REJECT como se muestra en la imagen.

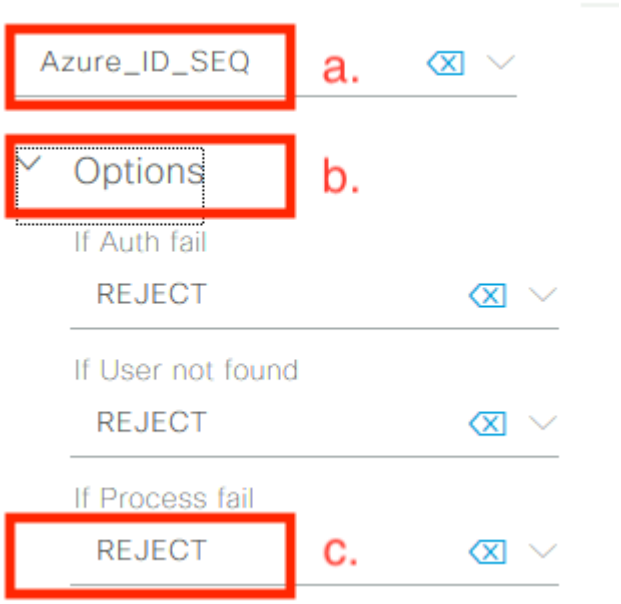


Figura 24

a. Busque la directiva de autenticación que utiliza el almacén de ID de REST.

b. Abra la lista desplegable Opciones.

c. La acción predeterminada de cambio para el proceso falló de DROP a REJECT.

Esto es necesario para evitar que PSN se marque como "muerto" en el lado de los NAD en un momento en que ocurren fallas específicas dentro del almacén de ID de REST como:

- El usuario no es miembro de ningún grupo de Azure AD.
- Debe cambiar la contraseña de usuario.

7. Agregue el diccionario del almacén de ID de REST a la directiva de autorización.

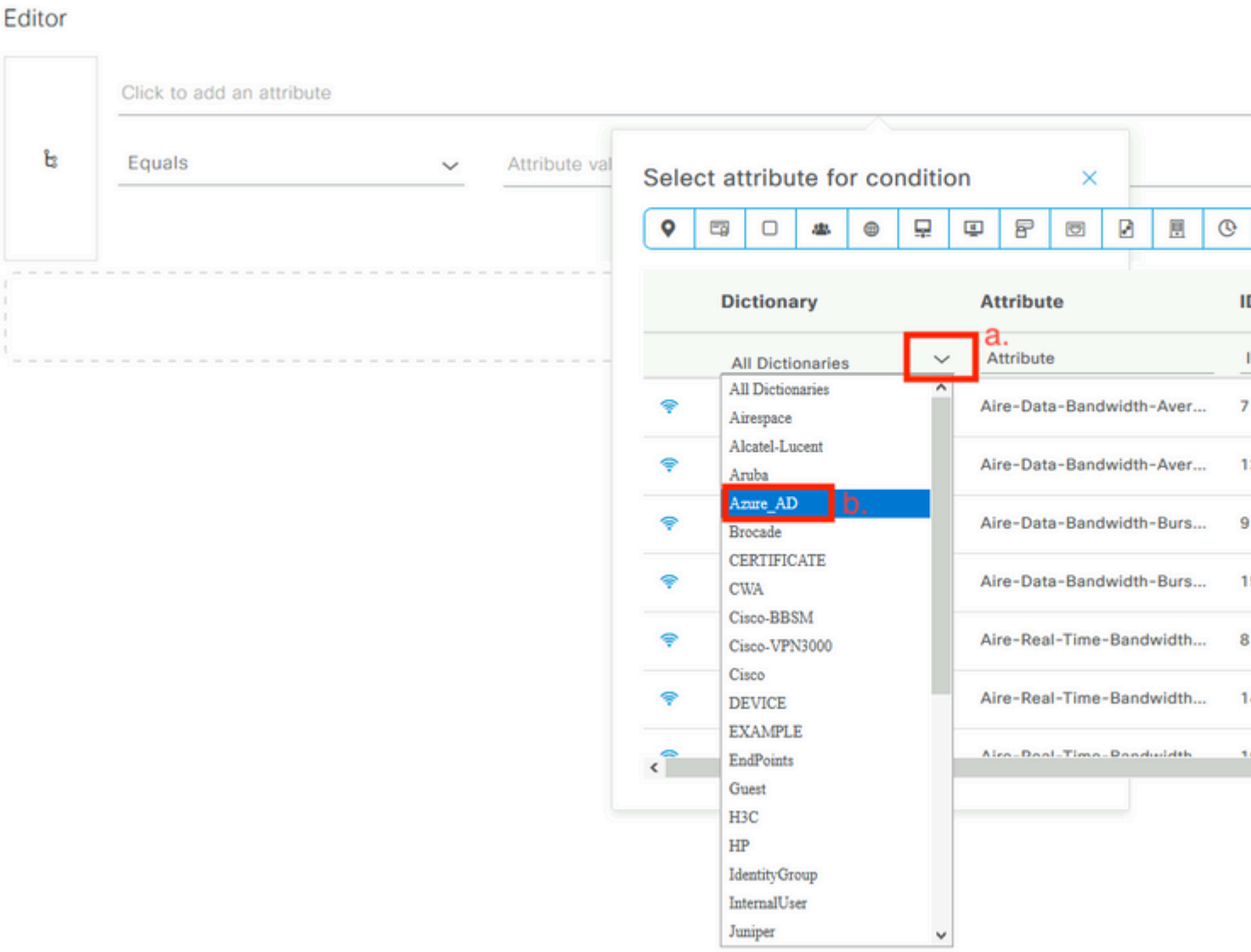


Figura 25

a. Abra la lista desplegable Todos los diccionarios.

b. Localice el diccionario con el mismo nombre que el almacén de ID de REST.

8. Agregue grupos de identidades externas (a partir de ISE 3.0, el único atributo disponible en el diccionario de almacén de ID de REST es un grupo externo).

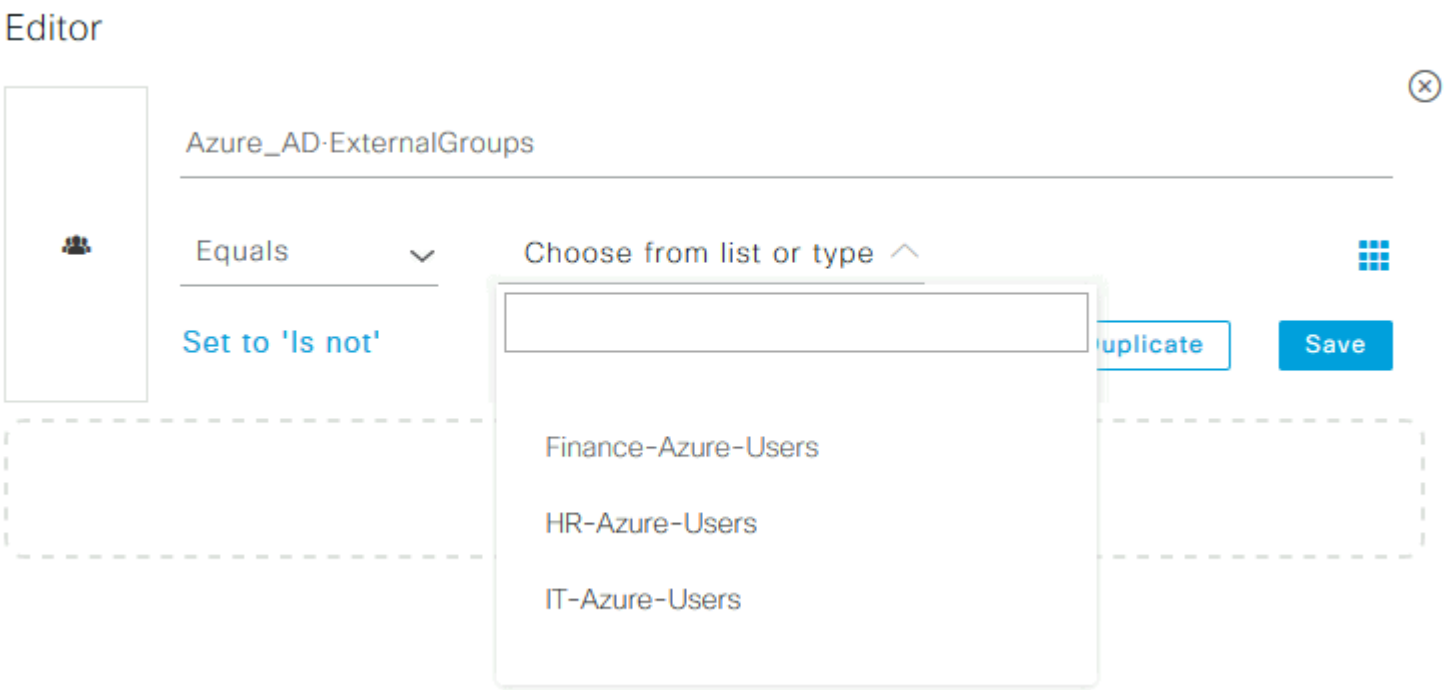


Figura 26

Ejemplos de políticas de ISE para diferentes casos prácticos

En el caso de la autenticación Dot1x, la condición de túnel EAP del diccionario Network Access se puede utilizar para hacer coincidir los intentos de EAP-TTLS como se muestra en la imagen.

Figura 27

a. Defina EAP Tunnel EQUAL to EAP-TTLS para que coincida con los intentos que deben reenviarse al almacén de ID de REST.

b. Seleccione en el almacén de ID de REST directamente o Secuencia de almacén de identidad, que la contiene en la columna Usar.

Dentro de las directivas de autorización individuales, se pueden utilizar grupos externos de Azure AD junto con el tipo de túnel EAP:

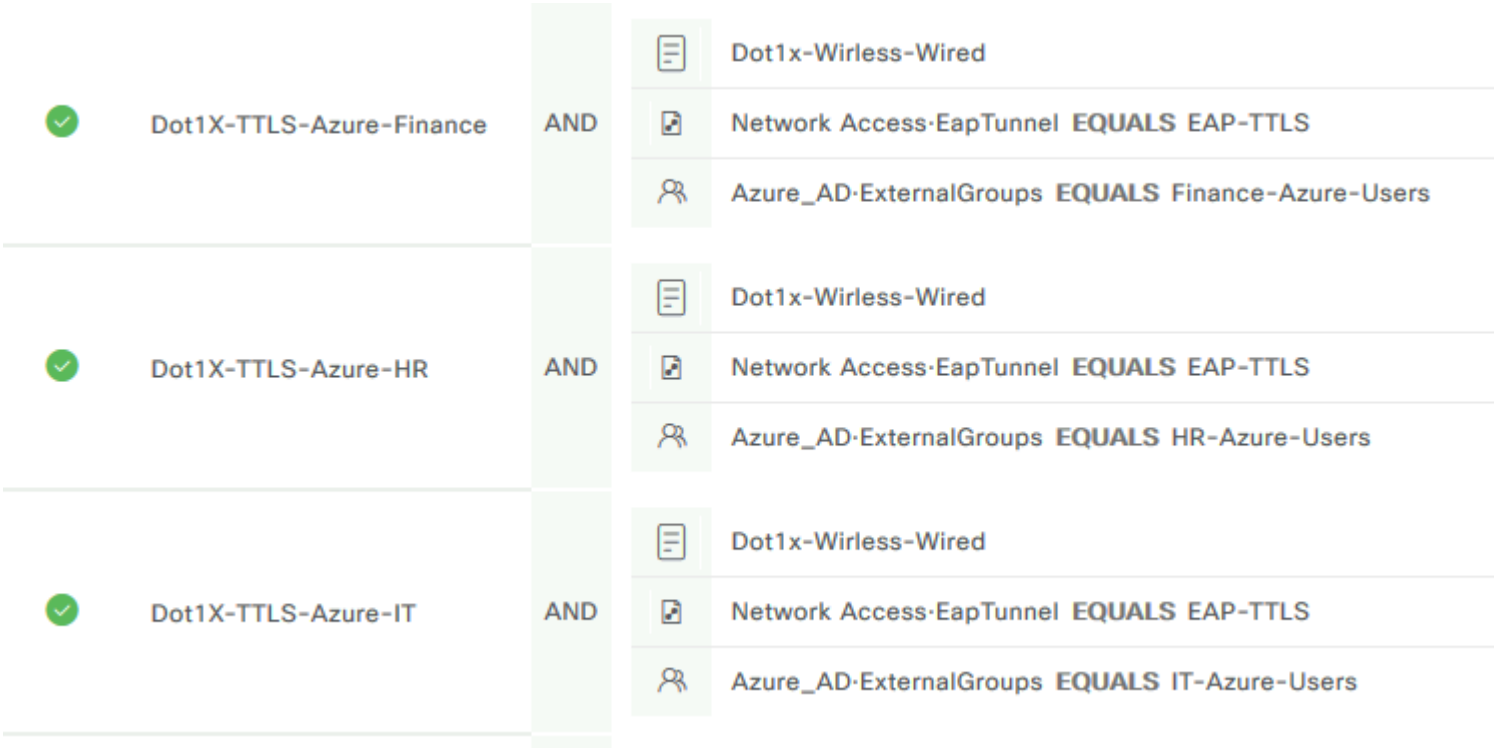


Figura 28

Para el flujo basado en VPN, puede utilizar un nombre de grupo de túnel como diferenciador:

Política de autenticación:

Políticas de autorización:

Figura 29

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. Confirme que el servicio de autenticación REST se ejecute en el nodo ISE.

Para comprobarlo, debe ejecutar el comando **show application status ise** en el shell de Secure Shell (SSH) de un nodo de ISE de destino:

<#root>

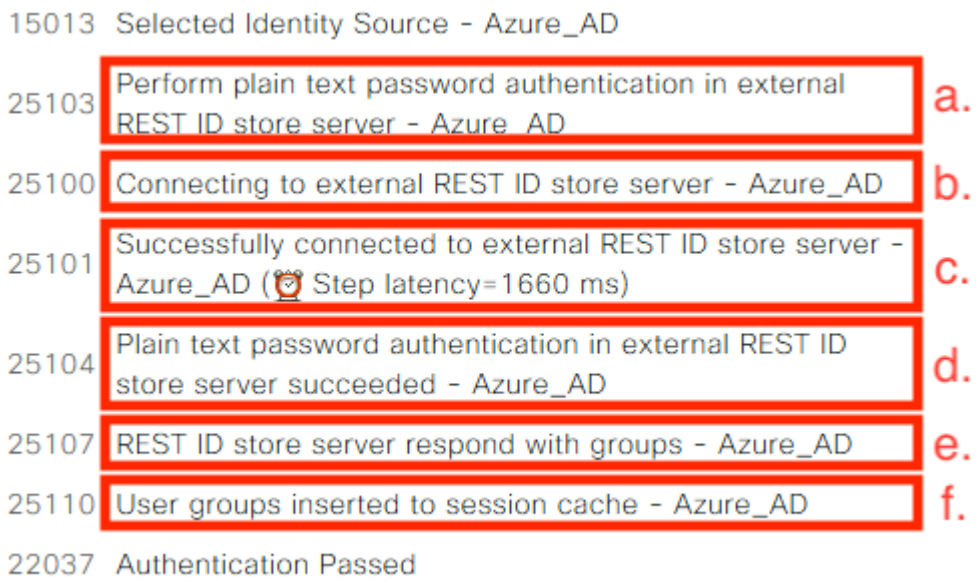
```
skuchere-ise30-1/admin# show application status ise

ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled
```

REST Auth Service running 63052

```
SSE Connector disabled
```

2. Compruebe que el almacén de ID de REST se utiliza en el momento de la autenticación (consulte la sección Pasos del informe de autenticación detallado).



a. PSN inicia la autenticación de texto sin formato con el almacén de ID de REST seleccionado.

b. Conexión establecida con Azure Cloud.

c. Paso de autenticación real: preste atención al valor de latencia que se presenta aquí. En caso de que todas sus autenticaciones con la nube de Aure se enfrenten a una latencia significativa, esto afectará al otro flujo de ISE y, como resultado, toda la implementación de ISE se volverá inestable.

d. Confirmación de la autenticación correcta.

e. Confirmación de los datos del grupo presentados como respuesta.

f. Contexto de sesión rellenado con datos de grupos de usuarios. Para obtener más información sobre el proceso de gestión de sesiones de ISE, considere la posibilidad de revisar este enlace del artículo.

3. Confirme que las políticas de Autenticación/Autorización esperadas están seleccionadas (para esta sección de descripción general de investigación del informe de autenticación detallado).

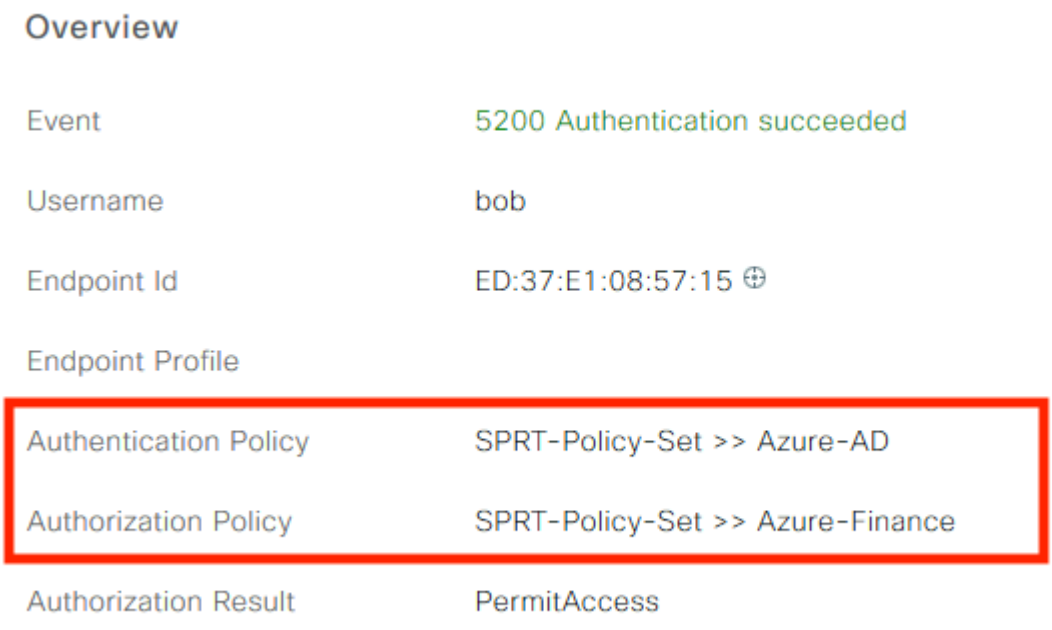


Figura 30

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Problemas con el servicio de autenticación REST

Para resolver cualquier problema con el servicio de autenticación REST, debe comenzar con la revisión del archivo **ADE.log**. Ubicación del paquete de asistencia: **/support/adeos/ade**

Una palabra clave de búsqueda para el servicio de autenticación REST es - **ROPC-control**.

Este ejemplo muestra cómo se inicia el servicio de autenticación REST:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] St
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] in
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Im
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Do
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Ex
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Do
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Se
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] in
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Cr
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] Co
```

En los casos en que el servicio no se inicia o se cae inesperadamente, siempre tiene sentido comenzar revisando el **ADE.log** en torno a un marco de tiempo problemático.

Problemas con la Autenticación de ID de REST

En el caso de fallas de autenticación cuando se utiliza el almacén de ID de REST, siempre debe comenzar desde un informe de autenticación detallado. En el área Otros atributos, puede ver una sección - **RestAuthErrorMsg** que contiene un error devuelto por la nube de Azure:

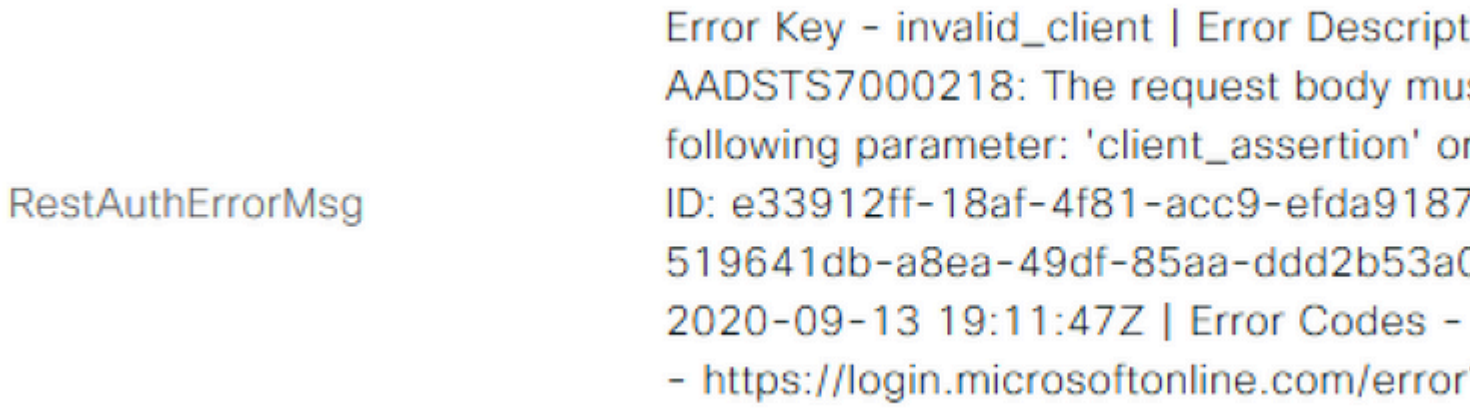


Figura 31

Trabajar con los archivos de registro

En ISE 3.0, debido a la función de introducción controlada de ID de REST, se habilitan las depuraciones para ella de forma predeterminada. Todos los registros relacionados con REST ID se almacenan en archivos ROPC que se pueden ver a través de CLI:

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log

skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

En ISE 3.0 con la revisión instalada, observe que el nombre de archivo es rest-id-store.log y no ropc.log. El ejemplo de búsqueda anterior proporcionado funciona porque el nombre de la carpeta no ha cambiado.

O bien, estos archivos se pueden extraer del paquete de asistencia de ISE.

A continuación, se incluyen un par de ejemplos de registro que muestran diferentes escenarios de trabajo y no trabajo:

1. Error de certificado cuando el nodo ISE no confía en Azure Graph. Este error se puede ver cuando los grupos no se cargan en la configuración del almacén de ID de REST.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https:

20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appli
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate f
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

Este problema indica que ISE no confía en el certificado API gráfico de Microsoft. ISE 3.0.0.458 no tiene una CA DigiCert Global Root G2 instalada en el almacén de confianza. Esto está documentado en el defecto

- Id. de error de Cisco CSCvv80297 Para solucionar este problema, debe instalar la CA DigiCert Global Root G2 en el almacén de confianza de ISE y marcarla como de confianza para los servicios de Cisco.

El certificado se puede descargar desde aquí: https://www.digicert.com/kb/digicert-root-certificates.htm

2. Secreto de aplicación incorrecto.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client se
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentityP
```

3. ID de aplicación incorrecta.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with i
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4. Usuario no encontrado.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_descr
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvider
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. La contraseña de usuario ha caducado: normalmente puede ocurrir para el usuario recién creado, ya que la contraseña definida por el administrador de Azure debe cambiarse en el momento del inicio de sesión en Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_descr
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvider
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. Los grupos no se pueden cargar debido a permisos de API incorrectos.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Statu
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. La autenticación falla cuando ROPC no está permitido en el lado de Azure.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvider
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. La autenticación falla porque el usuario no pertenece a ningún grupo del lado de Azure.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "r
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id toke
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. Autenticación de usuario y recuperación de grupo exitosas.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https:
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168.
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials t
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.2
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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).