Configurar a ID REST do ISE 3.0 com o Azure Ative Diretory

Contents

Introduction

Este documento descreve a integração do Cisco ISE 3.0 com o Azure AD implementada através do serviço REST Identity com Credenciais de Senha de Proprietário de Recurso.

Informações de Apoio

Este documento descreve como configurar e solucionar problemas da integração do Identity Services Engine (ISE) 3.0 com o Microsoft Azure Ative Diretory (AD) implementado através do serviço de Identidade (ID) de Transferência de Estado Representacional (REST) com a ajuda do ROPC (Credenciais de Senha de Proprietário de Recurso).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- ISE
- AD do MS Azure
- Compreensão da implementação e limitações do protocolo ROPC; link

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 3.0

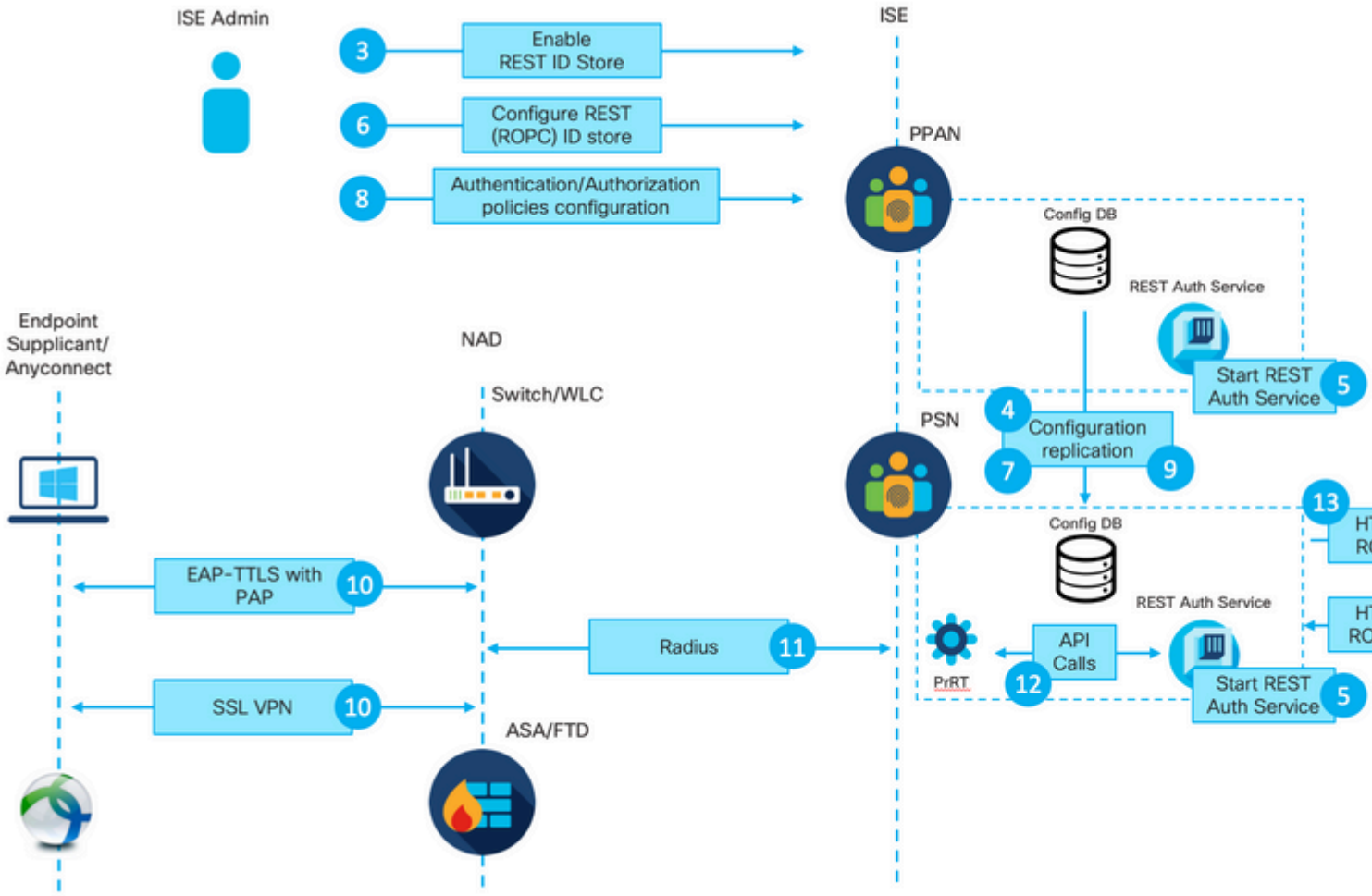
- AD do MS Azure
- WS-C3850-24P com s/w 16.9.2
- ASAv com 9.10 (1)
- Windows 10.0.18363

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

A funcionalidade de ID REST do ISE baseia-se no novo serviço introduzido no ISE 3.0 - Serviço de Autenticação REST. Este serviço é responsável pela comunicação com o Azure AD sobre trocas de ROPC de Autorização Aberta (OAuth) para executar a autenticação de usuário e a recuperação de grupo. O Serviço de Autenticação REST é desabilitado por padrão e, depois que o administrador o habilita, ele é executado em todos os nós do ISE na implantação. Como a comunicação do Serviço de Autenticação REST com a nuvem ocorre quando no momento da autenticação do usuário, qualquer atraso no caminho traz latência adicional ao fluxo de Autenticação/Autorização. Essa latência está fora do controle do ISE e qualquer implementação de autenticação REST deve ser cuidadosamente planejada e testada para evitar impacto em outros serviços do ISE.

Visão geral do fluxo de alto nível



1. O administrador de nuvem do Azure cria um novo Registro de Aplicativo. Os detalhes deste Aplicativo são usados posteriormente no ISE para estabelecer uma conexão com o Azure AD.

2. O administrador de nuvem do Azure deve configurar o Aplicativo com:

- Criar um segredo do cliente
- Ativar ROPC
- Adicionar declarações de grupo
- Definir permissões da Interface de Programação de Aplicativo (API)

3. O administrador do ISE ativa o serviço de autenticação REST. Isso precisa ser feito antes que qualquer outra ação possa ser executada.

4. As alterações são gravadas no banco de dados de configuração e replicadas em toda a implantação do ISE.

5. O Serviço de Autenticação REST é iniciado em todos os nós.

6. O administrador do ISE configura o armazenamento de ID REST com detalhes da Etapa 2.

7. As alterações são gravadas no banco de dados de configuração e replicadas em toda a implantação do ISE.

8. O administrador do ISE cria uma nova sequência de armazenamento de identidade ou modifica a que já existe e configura as políticas de autenticação/autorização.

9. As alterações são gravadas no banco de dados de configuração e replicadas em toda a implantação do ISE.

10. O ponto de extremidade inicia a autenticação. De acordo com a especificação do protocolo ROPC, a senha do usuário deve ser fornecida para a plataforma de identidade da Microsoft em texto claro sobre uma conexão HTTP criptografada; devido a esse fato, as únicas opções de autenticação disponíveis suportadas pelo ISE até agora são:

- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) com Password Authentication Protocol (PAP) como o método interno
- Autenticação AnyConnect SSL VPN com PAP

11. Troca com o Nó de Serviço de Política (PSN - Policy Service Node) do ISE sobre Radius.

12. O Process Runtime (PrRT) envia uma solicitação ao serviço REST ID com detalhes do usuário (Nome

de Usuário/Senha) sobre a API interna.

13. O serviço de ID REST envia a solicitação ROPC OAuth ao Azure AD sobre o HyperText Transfer Protocol Secure (HTTPS).

14. O Azure AD executa a autenticação de usuário e busca grupos de usuários.

15. O resultado da autenticação/autorização retornou ao ISE.

Após o ponto 15, o resultado da autenticação e os grupos buscados retornaram ao PrRT, que envolve o fluxo de avaliação da política e atribui o resultado final da Autenticação/Autorização. Access-Accept com atributos do perfil de autorização ou Access-Reject retornou ao Network Access Device (NAD).

Configurar o Azure AD para Integração

1. Localize o AppRegistration Service como mostrado na imagem.

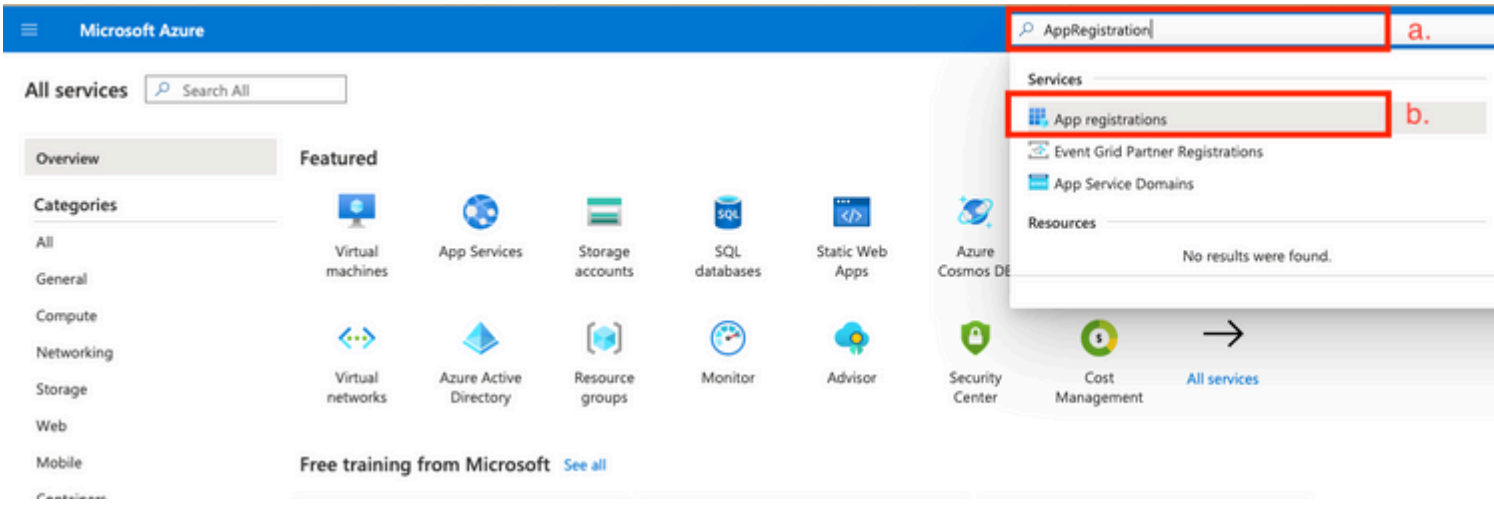


Figura 2.

a. Digite AppRegistration na barra de pesquisa Global.

b. Clique no serviço de registro do aplicativo.

2. Crie um novo Registro de Aplicativo.

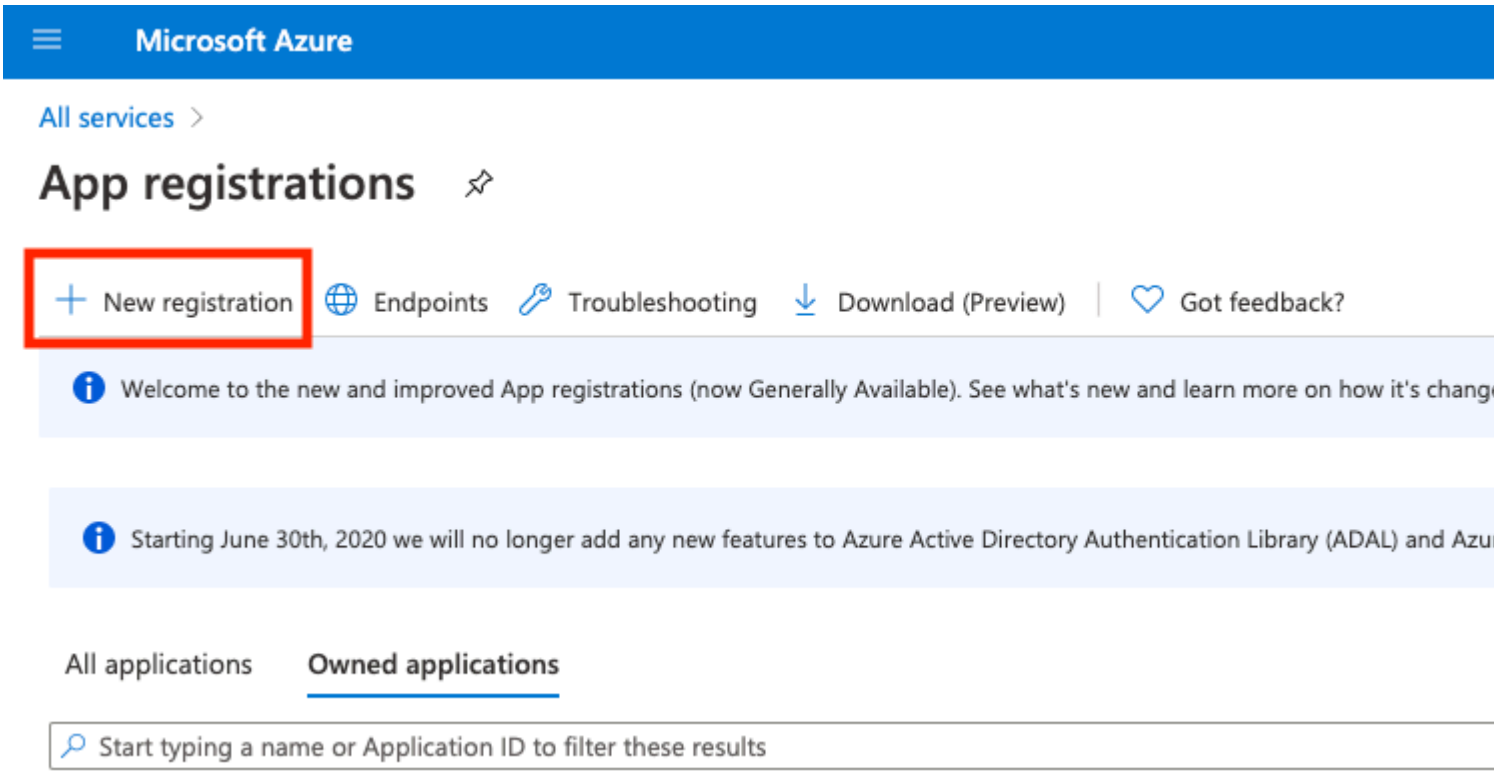


Figura 3.

3. Registre um novo Aplicativo.

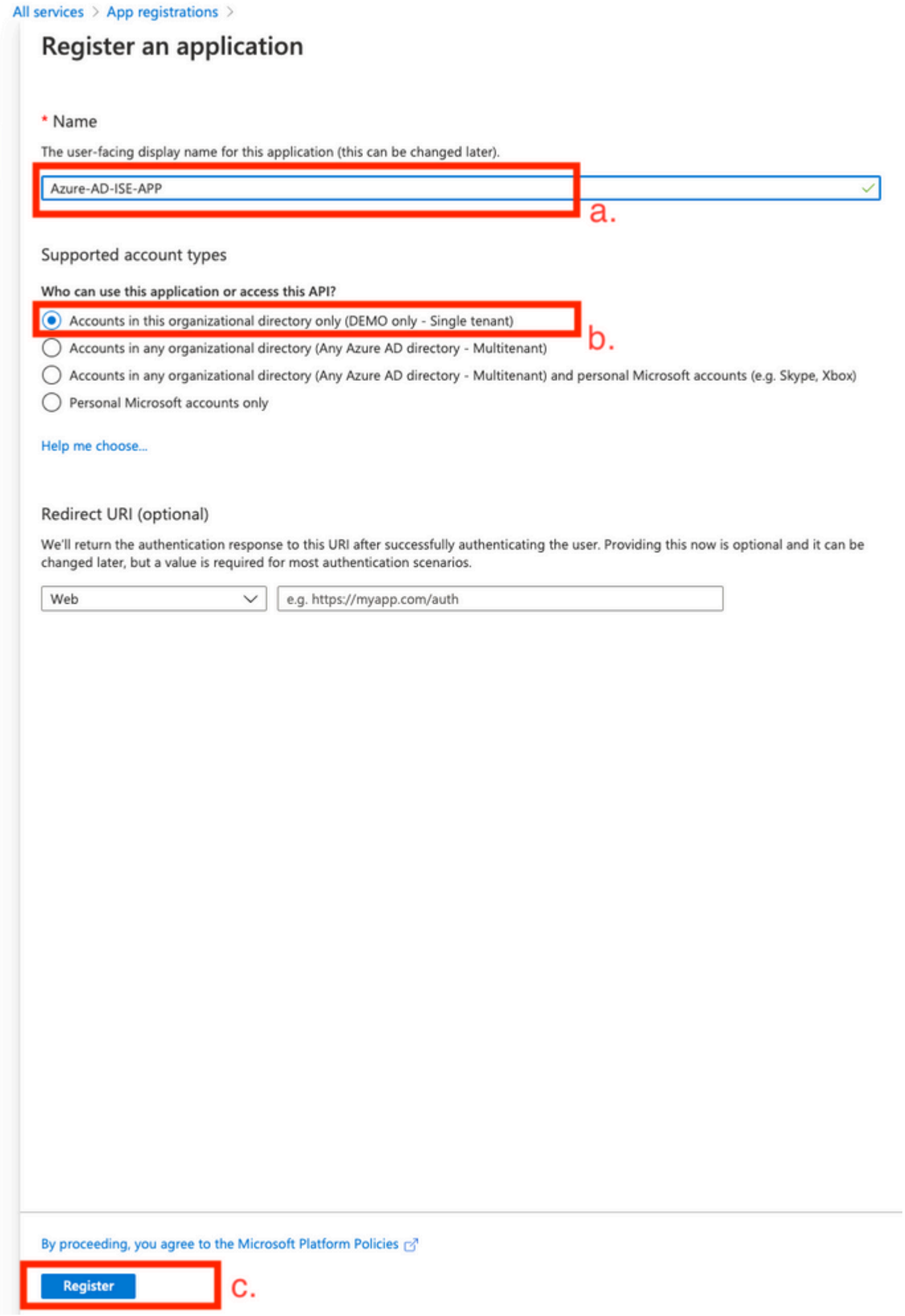


Figura 4.

- Definir nombre de Aplicación

: os dados do grupo de usuários podem ser buscados do Azure AD de várias maneiras com a ajuda de permissões de API diferentes. O método descrito neste exemplo é comprovadamente bem-sucedido no laboratório do Cisco TAC. Use outras permissões de API caso seu administrador do Azure AD a recomende.

16. Grant admin consent para permissões de API.

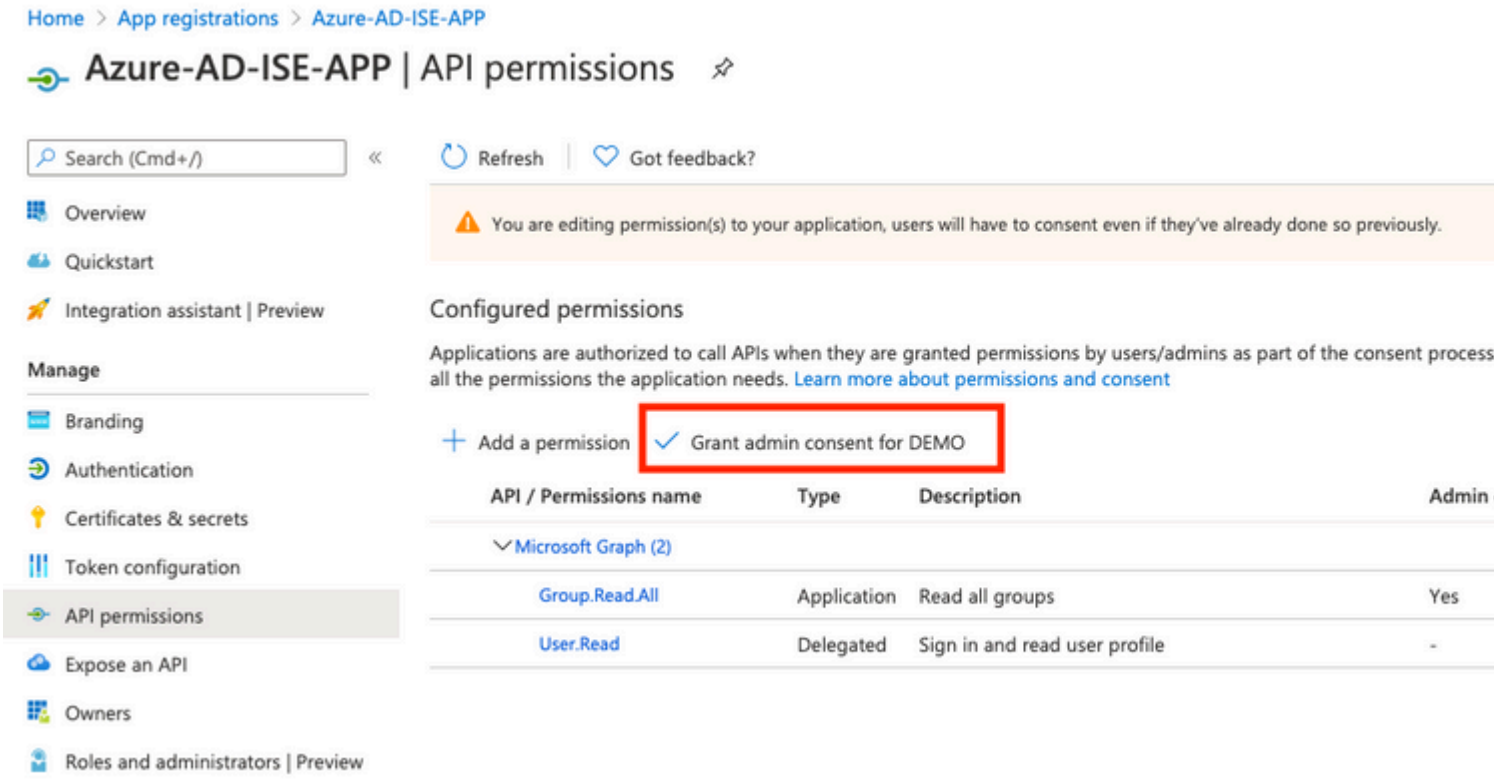


Figura 17.

17. Confirme a Concessão de consentimento para Admin.

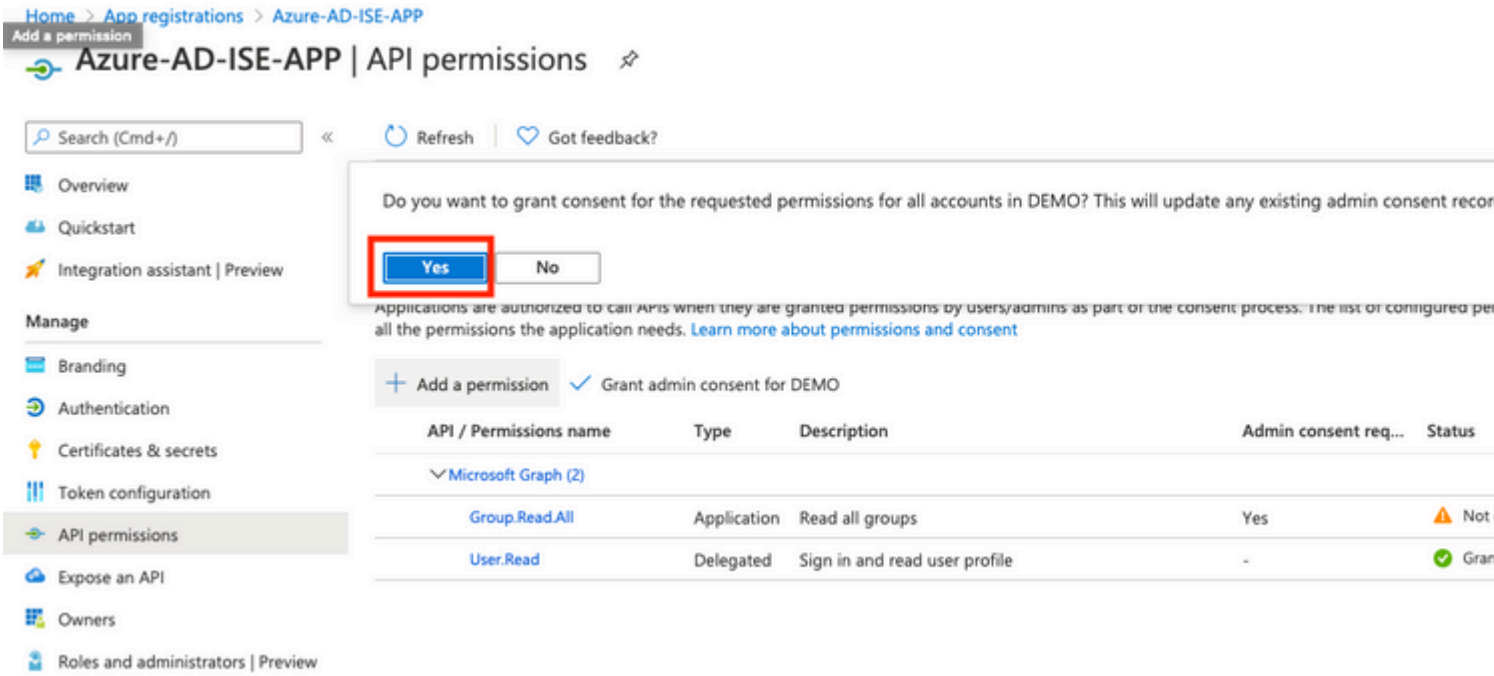


Figura 18.

Neste ponto, você pode considerar a integração totalmente configurada no Azure AD.

Configurar o ISE para integração

1. Navegue até as configurações do Gerenciamento de Identidades.

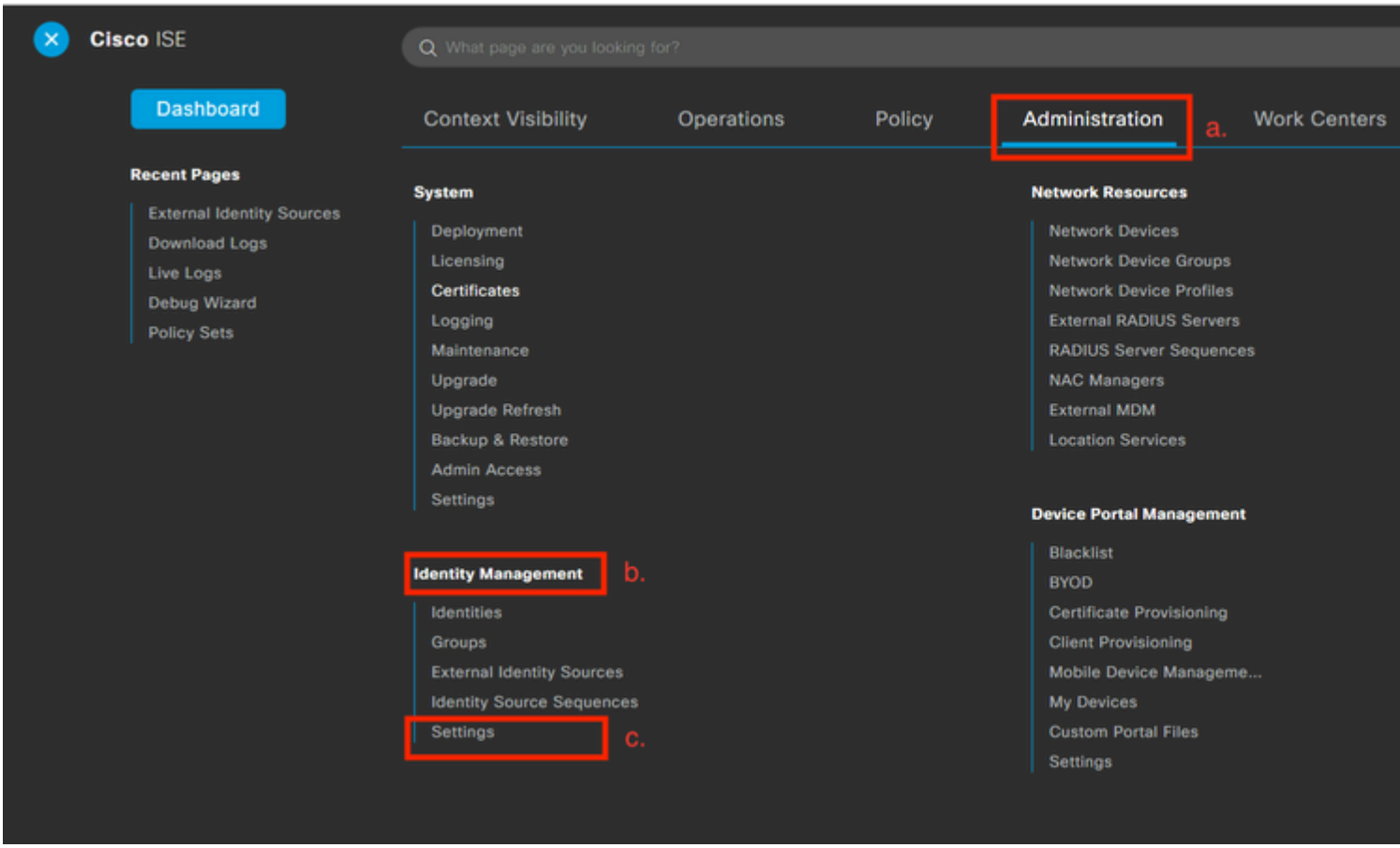


Figura 19.

Navegue até Administration > Identity Management> Settings .

2. Habilitar serviço de ID REST (desabilitado por padrão).

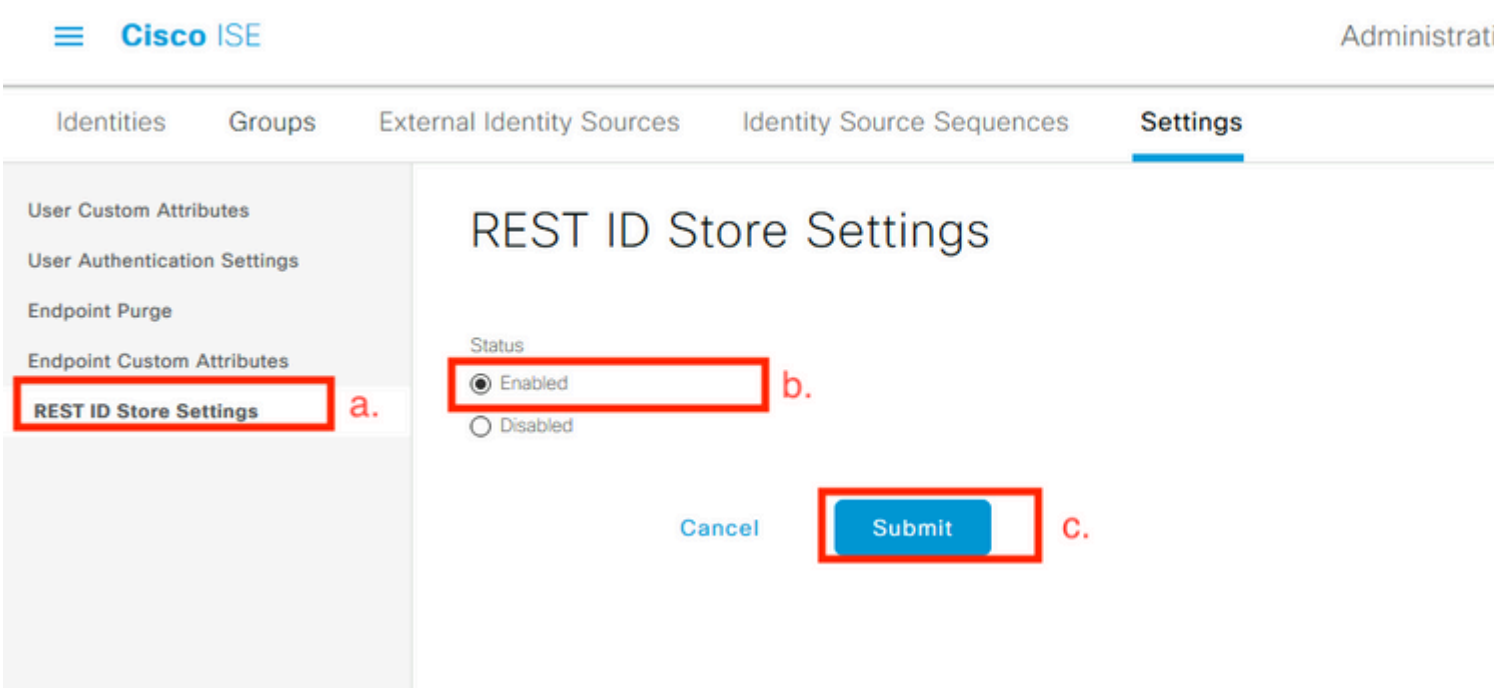


Figura 20.

Navegue até REST ID Store Settings e altere o status das configurações de armazenamento de ID REST para Enable,em seguida Submit suas alterações.

3. Crie um armazenamento de ID REST.

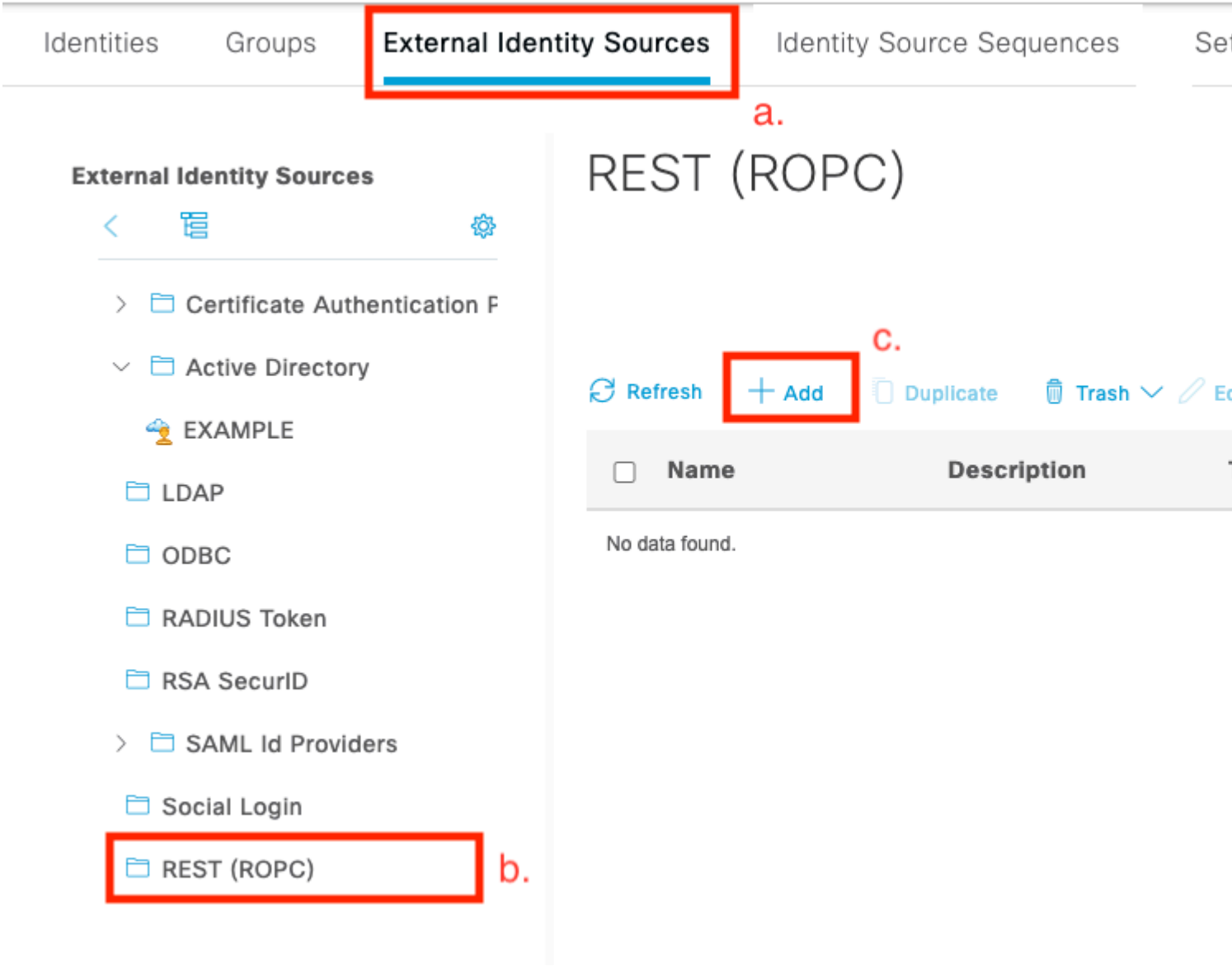


Figura 21.

Mude para a External Identity Sources clique em REST (ROPC) e clique em **Adicionar**.

4. Configure o armazenamento de ID REST.

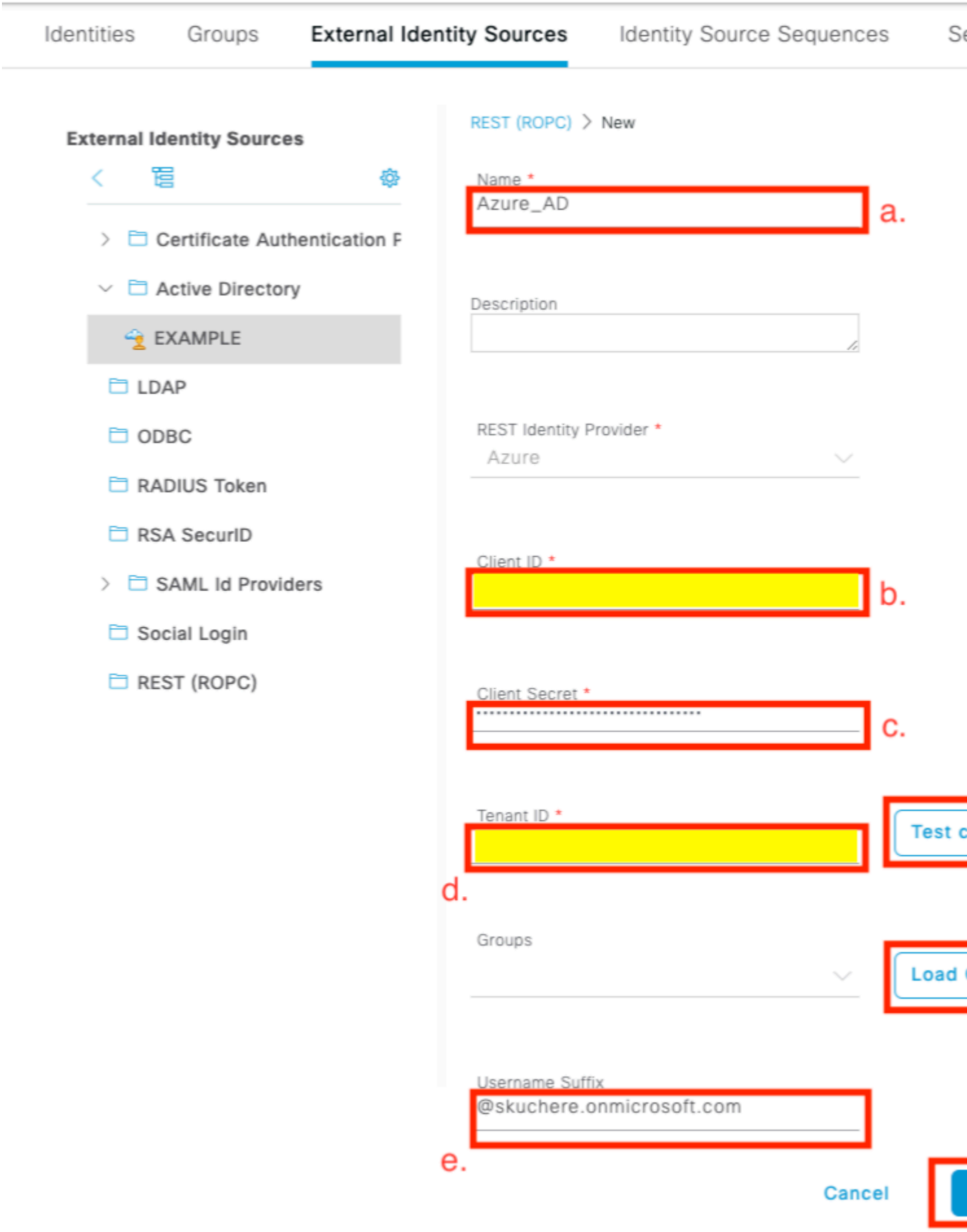

Identities
Groups
External Identity Sources
Identity Source Sequences
External Identity Sources
Certificate Authentication F
Active Directory
EXAMPLE
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
REST (ROPC)
REST (ROPC) > New
Name *
Azure_AD
a.
Description
REST Identity Provider *
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 o nome do armazenamento de ID. Posteriormente, esse nome poderá ser encontrado na lista de dicionários do ISE quando você configurar políticas de autorização. Além disso, esse nome é exibido na lista de repositórios de IDs disponíveis nas configurações de Política de autenticação e na lista de repositórios de IDs disponíveis na configuração de sequência do Repositório de identidades.

b. Forneça a ID do cliente (obtida do Azure AD na Etapa 8 da seção de configuração de integração do Azure AD).

c. Forneça o segredo do cliente (obtido do Azure AD na Etapa 7 da seção de configuração de integração do Azure AD).

d. Forneça a ID do Locatário (obtida do Azure AD na Etapa 8 da seção de configuração de integração do Azure AD).

e. Configurar sufixo do nome de usuário - por padrão, o ISE PSN usa um nome de usuário fornecido pelo usuário final, que é fornecido no formato sAMAccountName (nome de usuário curto, por exemplo, bob); nesse caso, o Azure AD não pode localizar o usuário. Username Sufix é o valor adicionado ao nome de usuário fornecido pelo usuário para trazer o nome de usuário para o formato UPN.

> **Observação**: o ROPC é limitado à autenticação do usuário, pois ele depende do atributo Username durante a autenticação. Os objetos de dispositivo no Azure AD não têm atributos de Nome de Usuário.

---

f. Pressione na conexão de Teste para confirmar se o ISE pode usar os detalhes do Aplicativo fornecidos para estabelecer uma conexão com o Azure AD.

g. Pressione Carregar Grupos para adicionar grupos disponíveis no Azure AD ao repositório de ID REST. O exemplo aqui mostra como é a experiência do administrador.

> **Observação**: esteja ciente do defeito na ID de bug da Cisco CSCvx00345, pois isso faz com que os grupos não carreguem. O defeito foi corrigido no patch 2 do ISE 3.0.

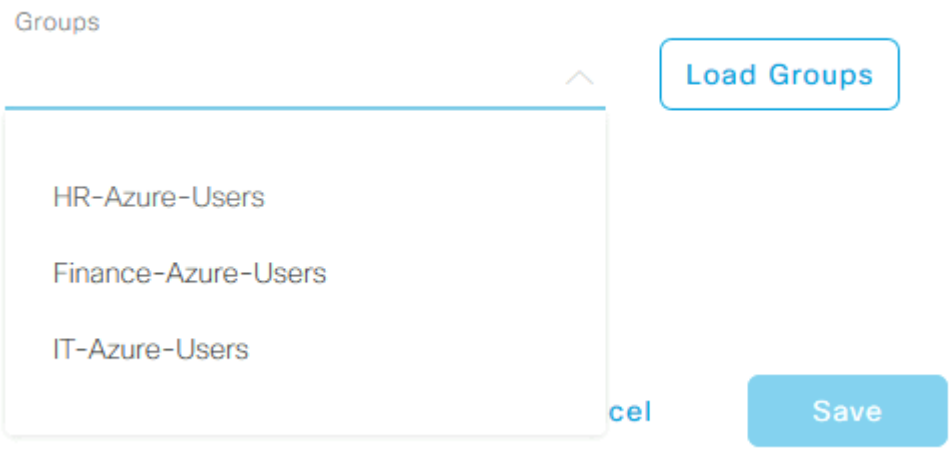


Figura 23.

h. Envie suas alterações.

5. Nesta etapa, considere a criação de uma nova Sequência de Armazenamento de Identidade, que inclui um armazenamento de ID REST recém-criado.

6. No momento em que o armazenamento de ID REST ou a sequência do armazenamento de identidade que a contém são atribuídos à política de autenticação, altere uma ação padrão para Falha de processo de DROP para REJECT, conforme mostrado na imagem.

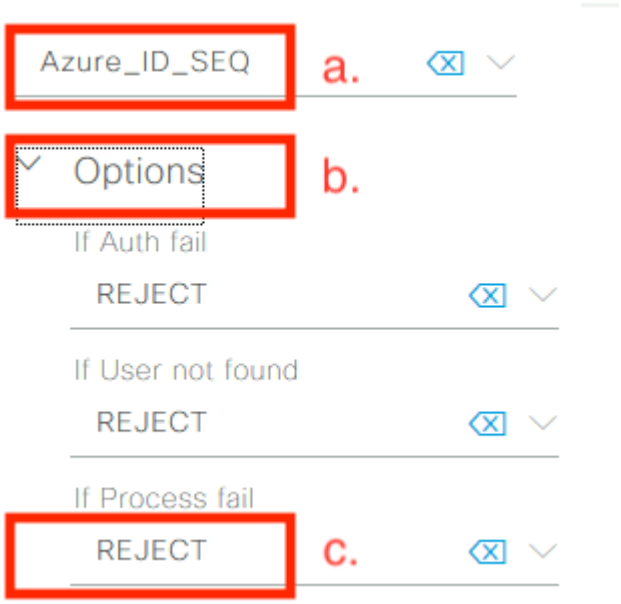


Figura 24.

a. Localize a política de Autenticação que usa o repositório de ID REST.

b. Abra a lista suspensa Opções.

c. A ação padrão de alteração para Processo Falhou de DROP para REJECT.

Isso é necessário para evitar que a PSN seja marcada como inoperante no lado dos NADs em um momento em que ocorram falhas específicas no armazenamento de ID REST, como:

- O usuário não é membro de nenhum grupo no Azure AD.
- A senha do usuário precisa ser alterada.

7. Adicione o dicionário de armazenamento de ID REST na política de Autorização.

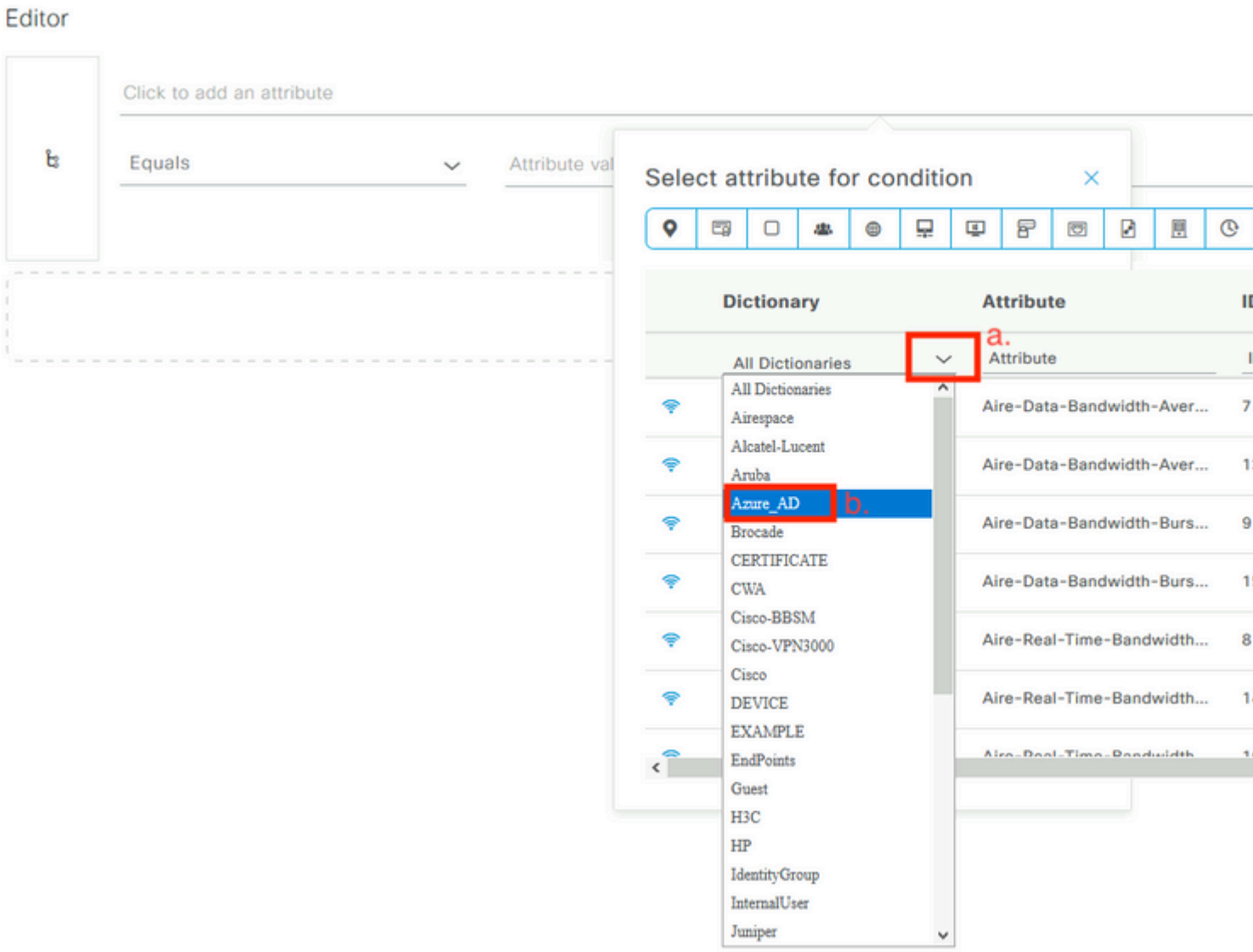


Figura 25.

a. Abra a lista suspensa Todos os dicionários.

b. Localize o dicionário com o mesmo nome do armazenamento de ID REST.

8. Adicione grupos de identidade externos (a partir do ISE 3.0, o único atributo disponível no dicionário de armazenamento de ID REST é um grupo externo).

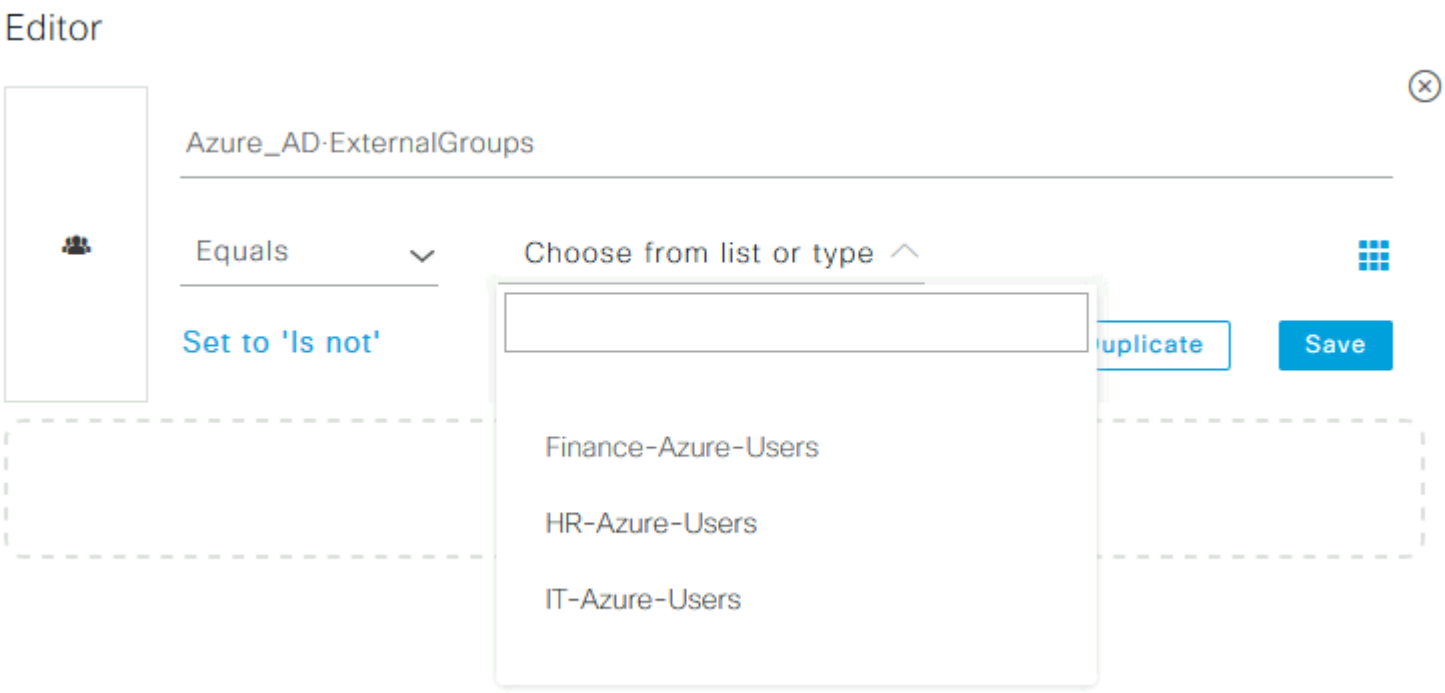


Figura 26.

Exemplos de políticas do ISE para diferentes casos de uso

No caso da autenticação Dot1x, a condição de túnel EAP do dicionário de acesso à rede pode ser usada para corresponder tentativas EAP-TTLS, como mostrado na imagem.

Figura 27.

a. Defina EAP Tunnel EQUAL para EAP-TTLS para corresponder as tentativas que precisam ser encaminhadas ao armazenamento de ID REST.

b. Selecione diretamente no armazenamento de ID REST ou Sequência de armazenamento de identidade, que o contém na coluna Usar.

Dentro das políticas de autorização individuais, os grupos externos do Azure AD podem ser usados com o tipo de túnel EAP:

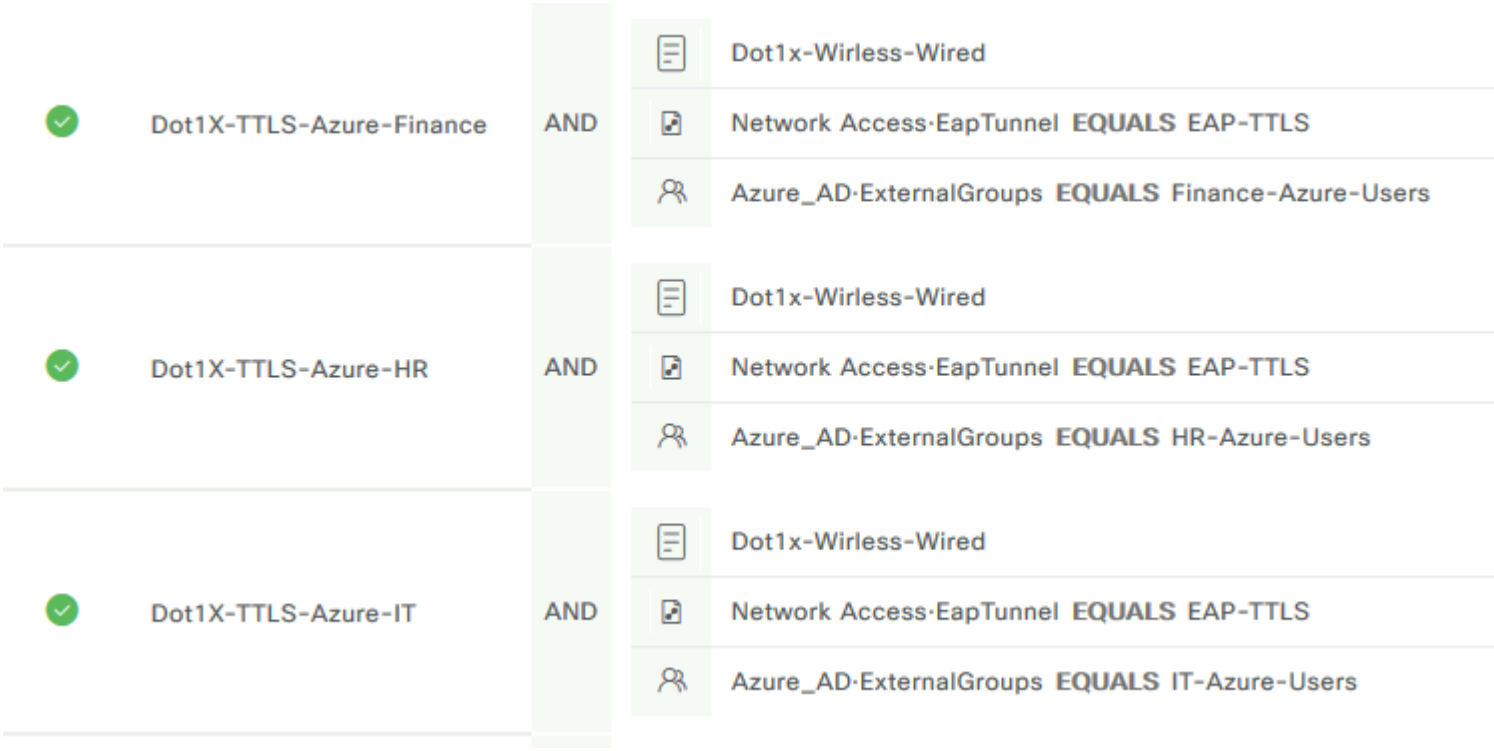


Figura 28.

Para o fluxo baseado em VPN, você pode usar um nome de grupo de túneis como um diferenciador:

Política de autenticação:

Políticas de autorização:

Figura 29.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Confirme se o serviço de autenticação REST é executado no nó ISE.

Para verificar isso, você precisa executar o comando **show application status ise** no shell Secure Shell (SSH) de um nó ISE de destino:

<#root>

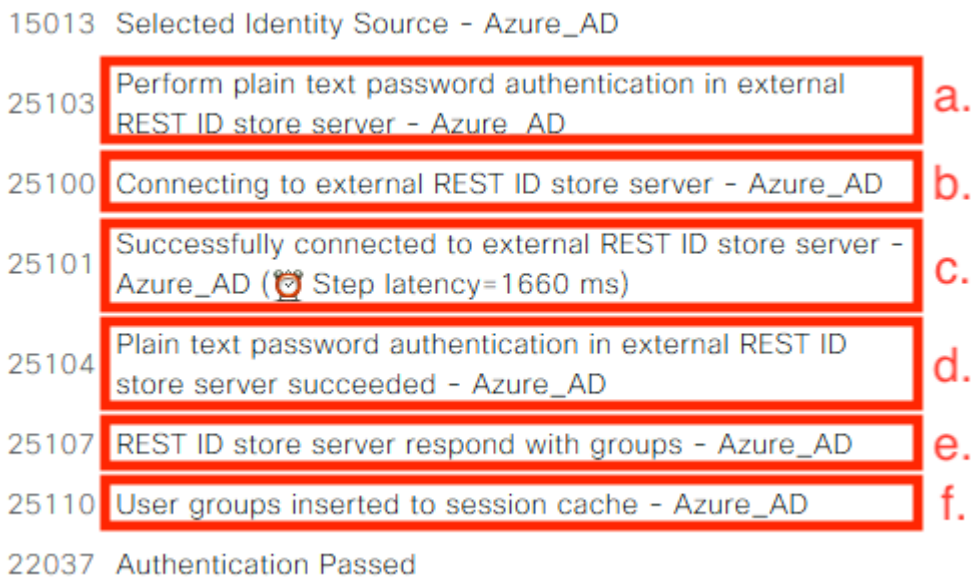
```
skuchere-ise30-1/admin# show application status ise

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. Verifique se o armazenamento de ID REST é usado no momento da autenticação (consulte a seção Etapas. do relatório de autenticação detalhado).



a. A PSN inicia a autenticação de texto sem formatação com o armazenamento de ID REST selecionado.

b. Conexão estabelecida com o Azure Cloud.

c. Etapa de autenticação real - preste atenção no valor de latência apresentado aqui. Caso todas as suas autenticações com o Aure Cloud tenham dificuldades devido à latência significativa, isso afeta o outro fluxo do ISE e, como resultado, toda a implantação do ISE se torna instável.

d. Confirmação de autenticação bem-sucedida.

e. Confirmação dos dados do grupo apresentados em resposta.

f. Contexto de sessão preenchido com dados do grupo de usuários. Para obter mais detalhes sobre o processo de gerenciamento de sessão do ISE, considere uma revisão deste artigo - link.

3. Confirme se as políticas de Autenticação/Autorização esperadas estão selecionadas (para esta seção Visão Geral de investigação do relatório de autenticação detalhado).

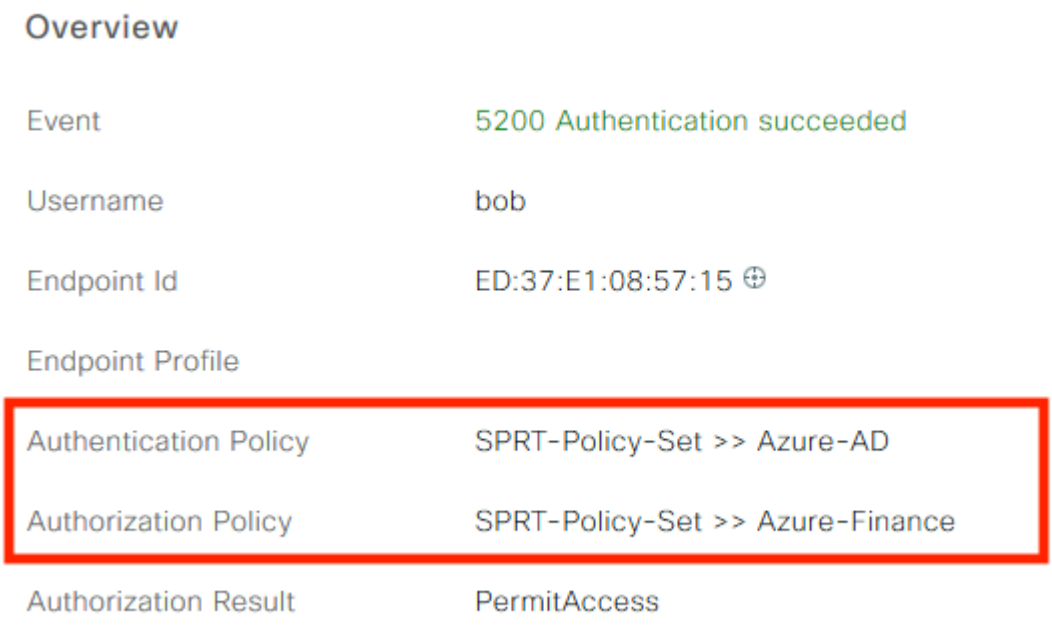


Figura 30.

Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

Problemas com o serviço de autenticação REST

Para solucionar quaisquer problemas com o Serviço de Autenticação REST, você precisa começar com a revisão do arquivo **ADE.log**. Localização do pacote de suporte - **/support/adeos/ade**

Uma palavra-chave de pesquisa para o Serviço de Autenticação REST é - **ROPC-control**.

Este exemplo mostra como o Serviço de Autenticação REST é iniciado:

```
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
```

Nos casos em que o serviço falha ao iniciar ou cai inesperadamente, sempre faz sentido começar revisando o **ADE.log** em torno de um período de tempo problemático.

Problemas com autenticação de ID REST

No caso de falhas de autenticação quando o armazenamento de ID REST é usado, você sempre precisa começar de um relatório de autenticação detalhado. Na área Outros Atributos, você pode ver uma seção - **RestAuthErrorMsg** que contém um erro retornado pela nuvem do Azure:

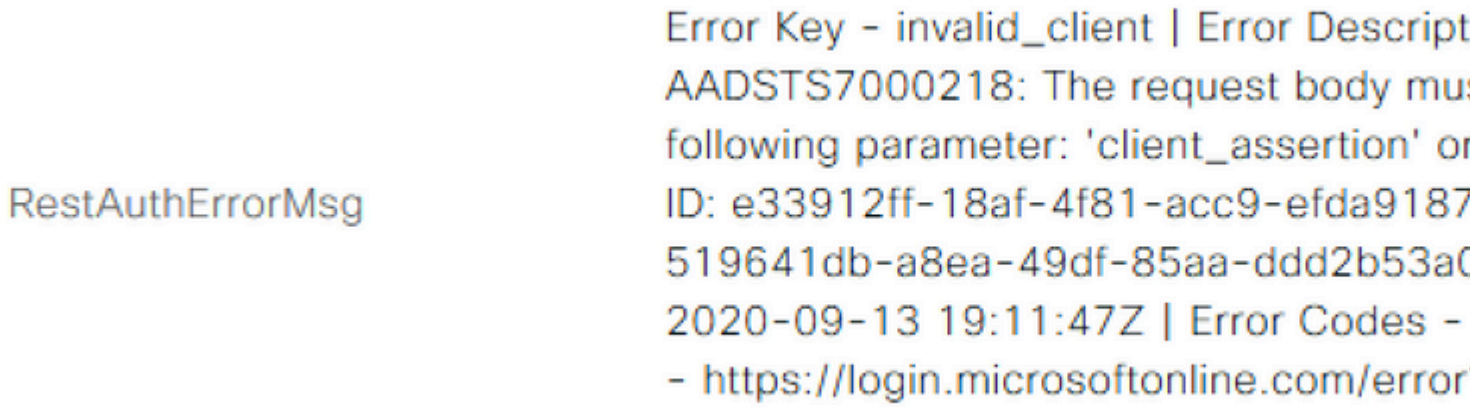


Figura 31.

Trabalhar com os arquivos de log

No ISE 3.0 devido à Introdução controlada do recurso REST ID, as depurações para ele são habilitadas por padrão. Todos os registros relacionados a ID REST são armazenados em arquivos ROPC que podem ser visualizados via 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
```

No ISE 3.0 com o patch instalado, observe que o nome do arquivo é rest-id-store.log e não ropc.log. O exemplo de pesquisa anterior fornecido funciona porque o nome da pasta não foi alterado.

Ou esses arquivos podem ser extraídos do pacote de suporte do ISE.

Aqui estão alguns exemplos de log que mostram cenários de trabalho e de não funcionamento diferentes:

1. Erro de certificado quando o Azure Graph não é confiável pelo nó ISE. Esse erro pode ser visto quando os grupos não são carregados na configuração de armazenamento de ID 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)
```

Esse problema indica que o certificado da API do Microsoft Graph não é confiável para o ISE. O ISE 3.0.0.458 não tem uma CA raiz global do DigiCert G2 instalada no armazenamento confiável. Isso está documentado no defeito

- ID de bug da Cisco CSCv80297 Para resolver esse problema, você precisa instalar a CA raiz global G2 da DigiCert no armazenamento confiável do ISE e marcá-lo como confiável para serviços Cisco.

O certificado pode ser baixado aqui - https://www.digicert.com/kb/digicert-root-certificates.htm

2. Segredo de aplicativo errado.

```
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(AzureIdentityF
```

3. ID do APLICATIVO incorreta.

```
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. Usuário não 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. Senha do usuário expirada - normalmente pode acontecer para o usuário recém-criado, pois a senha definida pelo administrador do Azure precisa ser alterada no momento do logon no 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. Os grupos não podem ser carregados devido a permissões de API incorretas.

```
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. A autenticação falha quando o ROPC não é permitido no 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. A autenticação falha, pois o usuário não pertence a nenhum grupo no 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: "m
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. Autenticação de usuário e recuperação de grupo bem-sucedidas.

```
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" : [ ]
}
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.