Konfigurieren der REST-ID von ISE 3.0 mit Azure Active Directory

Inhalt

Einleitung

In diesem Dokument wird die Integration von Cisco ISE 3.0 in Azure AD beschrieben, die über den REST-Identitätsdienst mit Anmeldeinformationen für das Ressourcenbesitzerkennwort implementiert wurde.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie Sie die Identity Services Engine (ISE) 3.0-Integration mit Microsoft (MS) Azure Active Directory (AD) konfigurieren und mithilfe des REST-Identitätsdiensts (REST Identity ID) mithilfe von ROPC (Resource Owner Password Credentials) Fehler beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- ISE

- Microsoft Azure AD
- Verständnis der Implementierung und der Einschränkungen des ROPC-Protokolls; Link

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.0
- Microsoft Azure AD

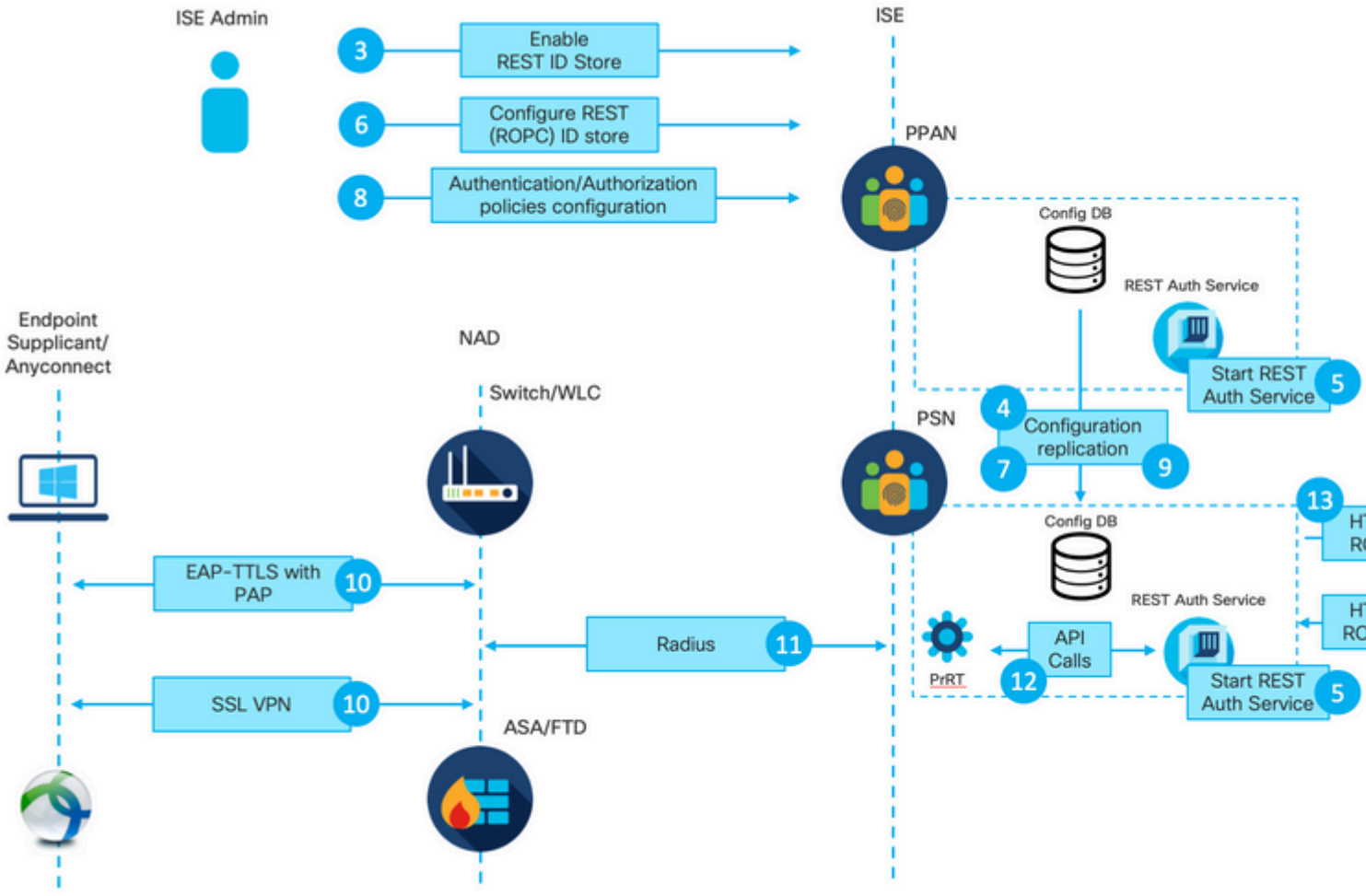
- WS-C3850-24P mit s/w 16.9.2
- ASAv mit 9.10 (1)
- Windows 10.0.18363

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Die REST-ID-Funktion der ISE basiert auf dem neuen Service, der mit dem REST-Auth-Service ISE 3.0 eingeführt wurde. Dieser Dienst ist für die Kommunikation mit Azure AD über Open Authorization (OAuth)-ROPC-Austausche zuständig, um die Benutzerauthentifizierung und den Gruppenabruf durchzuführen. Der REST-Auth-Service ist standardmäßig deaktiviert. Nach der Aktivierung durch den Administrator wird er auf allen ISE-Knoten in der Bereitstellung ausgeführt. Da die Kommunikation des REST-Auth-Service mit der Cloud zum Zeitpunkt der Benutzerauthentifizierung stattfindet, führen Verzögerungen auf dem Pfad zu zusätzlicher Latenz im Authentifizierungs-/Autorisierungsablauf. Diese Latenz liegt außerhalb der Kontrolle der ISE, und jede Implementierung der REST-Authentifizierung muss sorgfältig geplant und getestet werden, um Beeinträchtigungen anderer ISE-Services zu vermeiden.

High-Level-Flow - Übersicht



1. Azure Cloud-Administrator erstellt eine neue Anwendungsregistrierung (App). Details dieser App werden später auf der ISE verwendet, um eine Verbindung mit dem Azure AD herzustellen.

2. Azure Cloud-Administrator muss die App mit folgenden Einstellungen konfigurieren:

- Erstellen eines Client-Schlüssels
- ROPC aktivieren
- Gruppenansprüche hinzufügen
- Definieren von API-Berechtigungen (Application Programming Interface)

3. Der ISE-Administrator aktiviert den REST-Auth-Service. Sie muss ausgeführt werden, bevor eine andere Aktion ausgeführt werden kann.

4. Die Änderungen werden in die Konfigurationsdatenbank geschrieben und über die gesamte ISE-Bereitstellung repliziert.

5. Der REST-Auth-Dienst wird auf allen Knoten gestartet.

6. ISE-Administrator konfiguriert den REST-ID-Speicher mit Details aus Schritt 2.

7. Die Änderungen werden in die Konfigurationsdatenbank geschrieben und in der gesamten ISE-Bereitstellung repliziert.

8. ISE-Administrator erstellt eine neue Identitätsspeichersequenz oder ändert die bereits vorhandene Sequenz und konfiguriert die Authentifizierungs-/Autorisierungsrichtlinien.

9. Die Änderungen werden in die Konfigurationsdatenbank geschrieben und in der gesamten ISE-Bereitstellung repliziert.

10. Der Endpunkt initiiert die Authentifizierung. Gemäß ROPC-Protokollspezifikation muss das Benutzerkennwort in Klartext über eine verschlüsselte HTTP-Verbindung an die Microsoft-Identitätsplattform übermittelt werden; aus diesem Grund sind die einzigen von der ISE derzeit unterstützten Authentifizierungsoptionen:

- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) mit Password Authentication Protocol (PAP) als internem Verfahren
- AnyConnect SSL VPN-Authentifizierung mit PAP

11. Austausch mit ISE Policy Service Node (PSN) über Radius.

12. Process Runtime (PrRT) sendet über interne API eine Anfrage an den REST-ID-Dienst mit

Benutzerdetails (Benutzername/Passwort).

13. Der REST-ID-Dienst sendet eine OAuth-ROPC-Anforderung über HTTPS (HyperText Transfer Protocol Secure) an Azure AD.

14. Azure AD führt eine Benutzerauthentifizierung durch und ruft Benutzergruppen ab.

15. Das Authentifizierungs-/Autorisierungsergebnis wird an die ISE zurückgegeben.

Nach Punkt 15 kehrten das Authentifizierungsergebnis und die abgerufenen Gruppen zu PrRT zurück, das einen Richtlinienauswertungsfluss beinhaltet und das endgültige Authentifizierungs-/Autorisierungsergebnis zuweist. Entweder Access-Accept mit Attributen aus dem Autorisierungsprofil oder Access-Reject wird an Network Access Device (NAD) zurückgegeben.

Azure AD für die Integration konfigurieren

1. Suchen Sie den AppRegistration-Dienst, wie im Bild dargestellt.

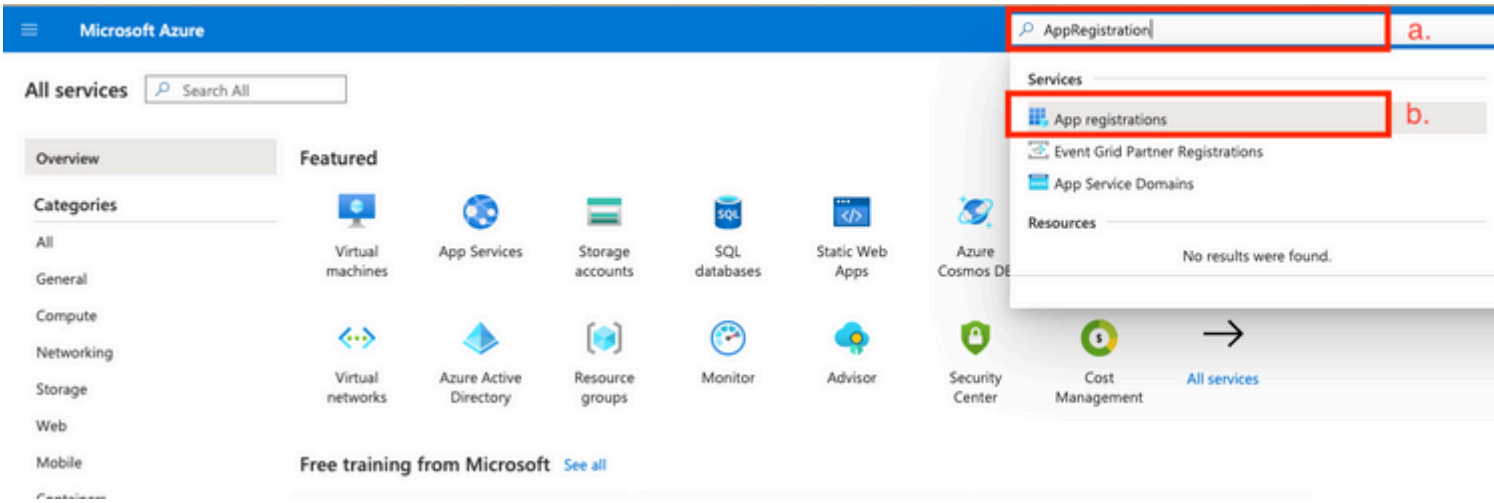


Abbildung 2.

antwort: Geben Sie AppRegistration in die globale Suchleiste ein.

b. Klicken Sie auf den App-Registrierungsdienst.

2. Erstellen einer neuen App-Registrierung

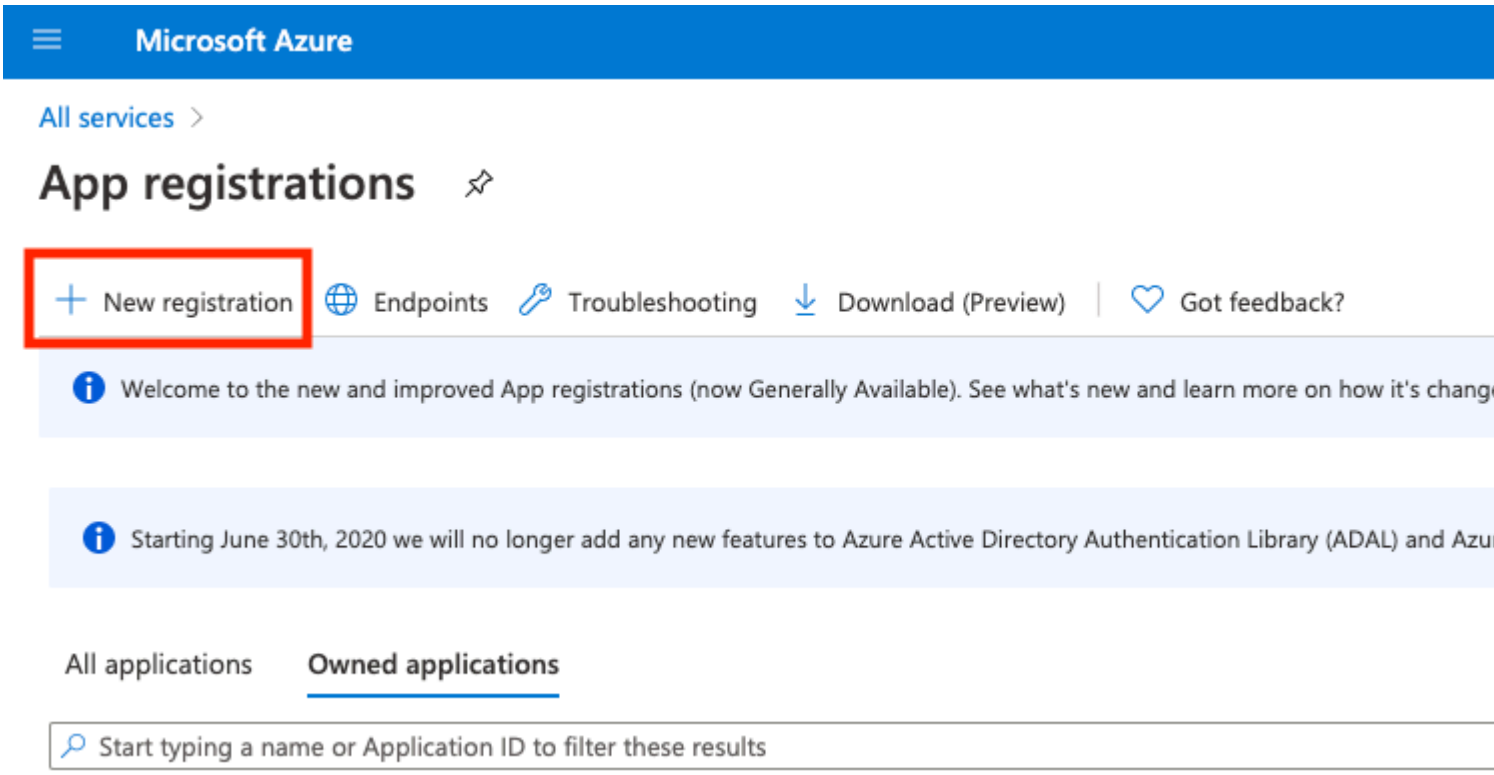


Abbildung 3:

3. Registrieren Sie eine neue App.

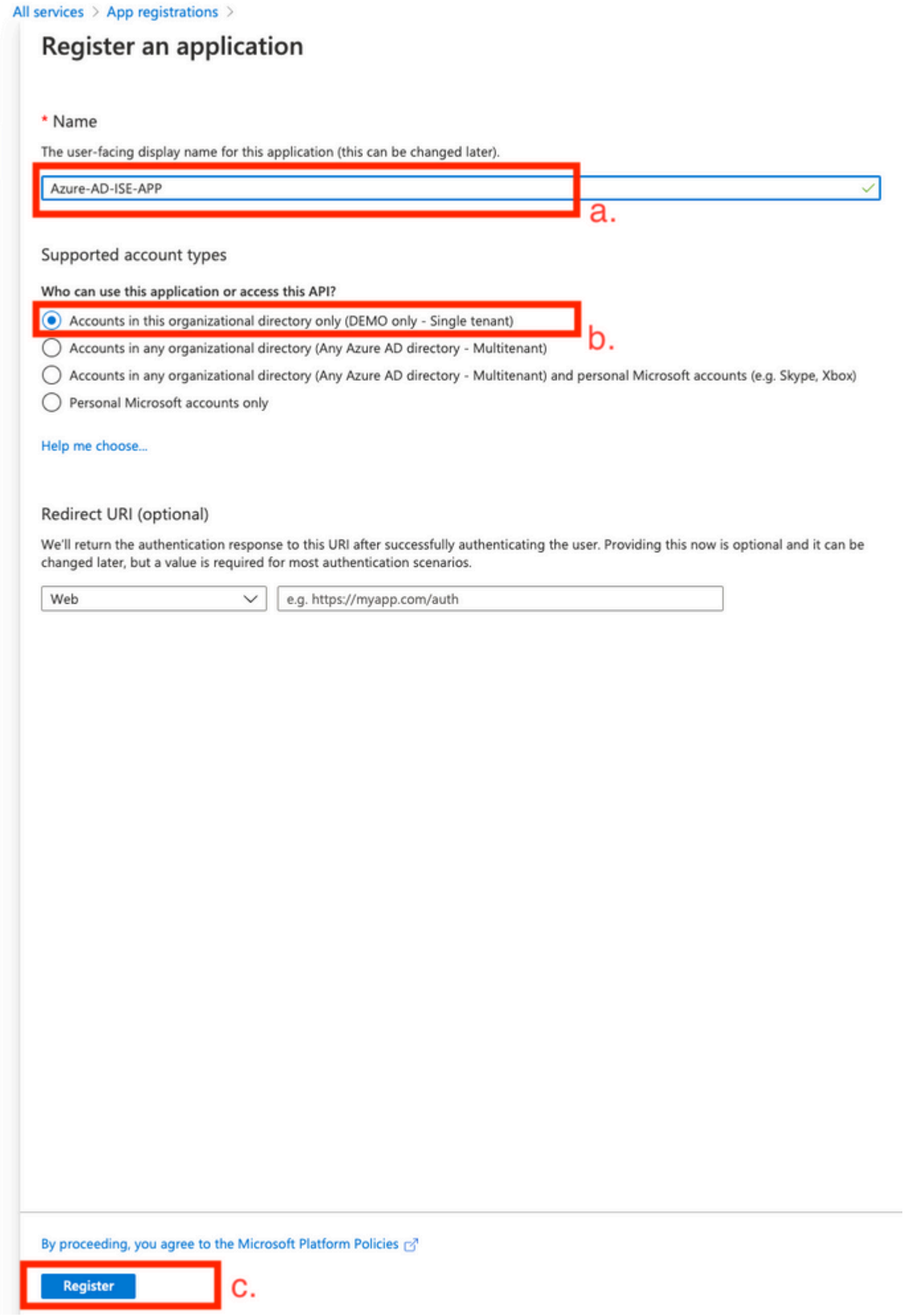

All services > App registrations >
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Azure-AD-ISE-APP
a.
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (DEMO only - Single tenant)
b.
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft accounts only
Help me choose...
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web
e.g. https://myapp.com/auth
By proceeding, you agree to the Microsoft Platform Policies
Register
c.

Abbildung 4:

: Benutzergruppendaten können auf verschiedene Weise mithilfe unterschiedlicher API-Berechtigungen aus Azure AD abgerufen werden. Die in diesem Beispiel beschriebene Methode hat sich im Cisco TAC Lab als erfolgreich erwiesen. Verwenden Sie andere API-Berechtigungen, falls Ihr Azure AD-Administrator dies empfiehlt.

16. Grant admin consent für API-Berechtigungen.

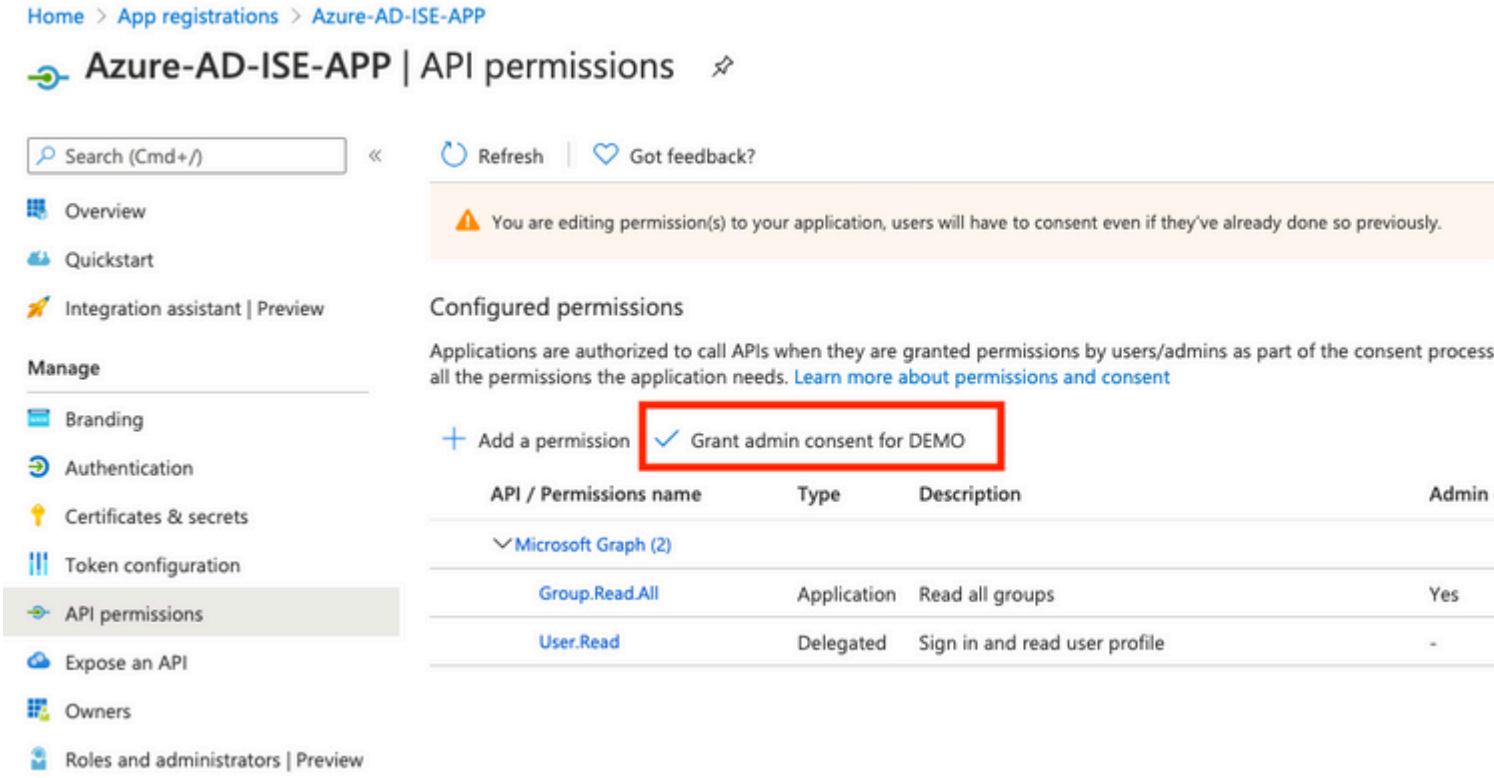


Abbildung 17:

17. Bestätigen Sie die Einwilligung des Administrators.

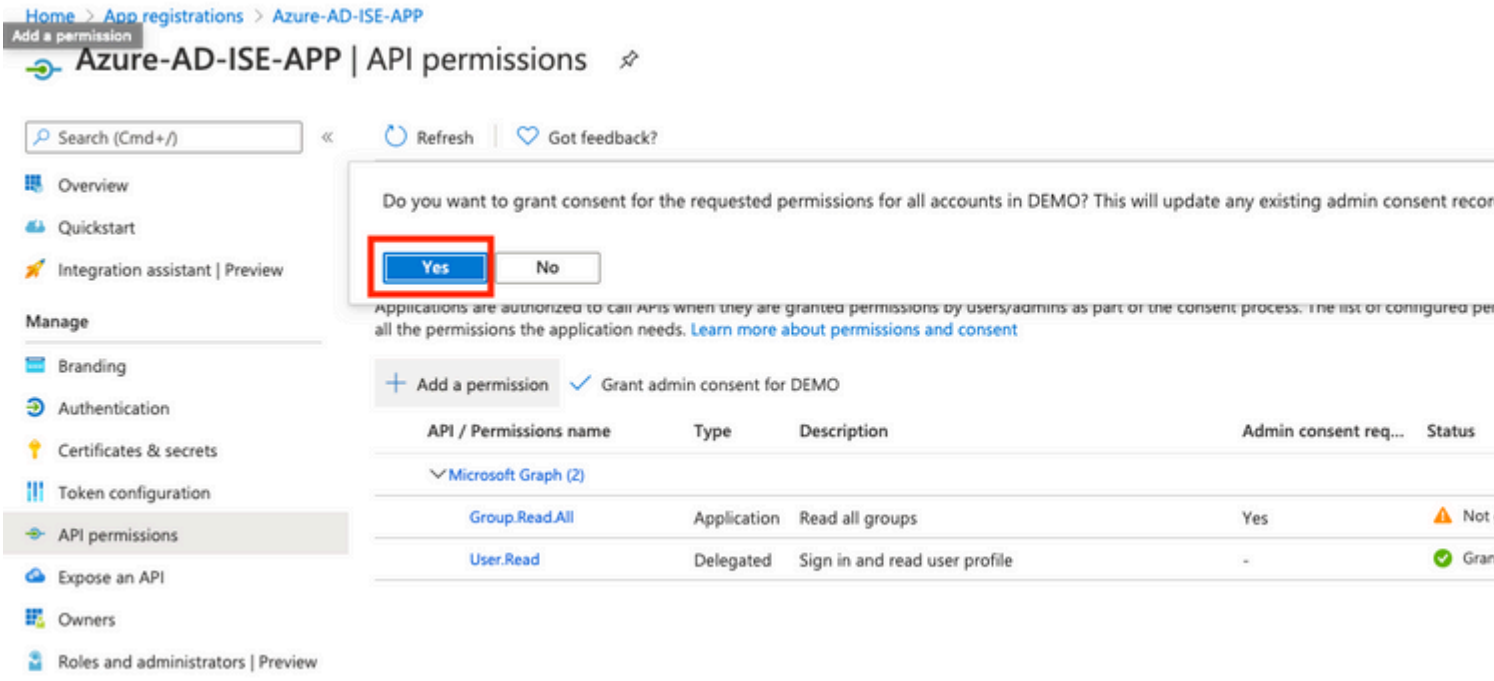


Abbildung 18:

An diesem Punkt können Sie die Integration betrachten, die auf der Azure AD-Seite vollständig konfiguriert ist.

Konfigurieren der ISE für die Integration

1. Navigieren Sie zu den Einstellungen für die Identitätsverwaltung.

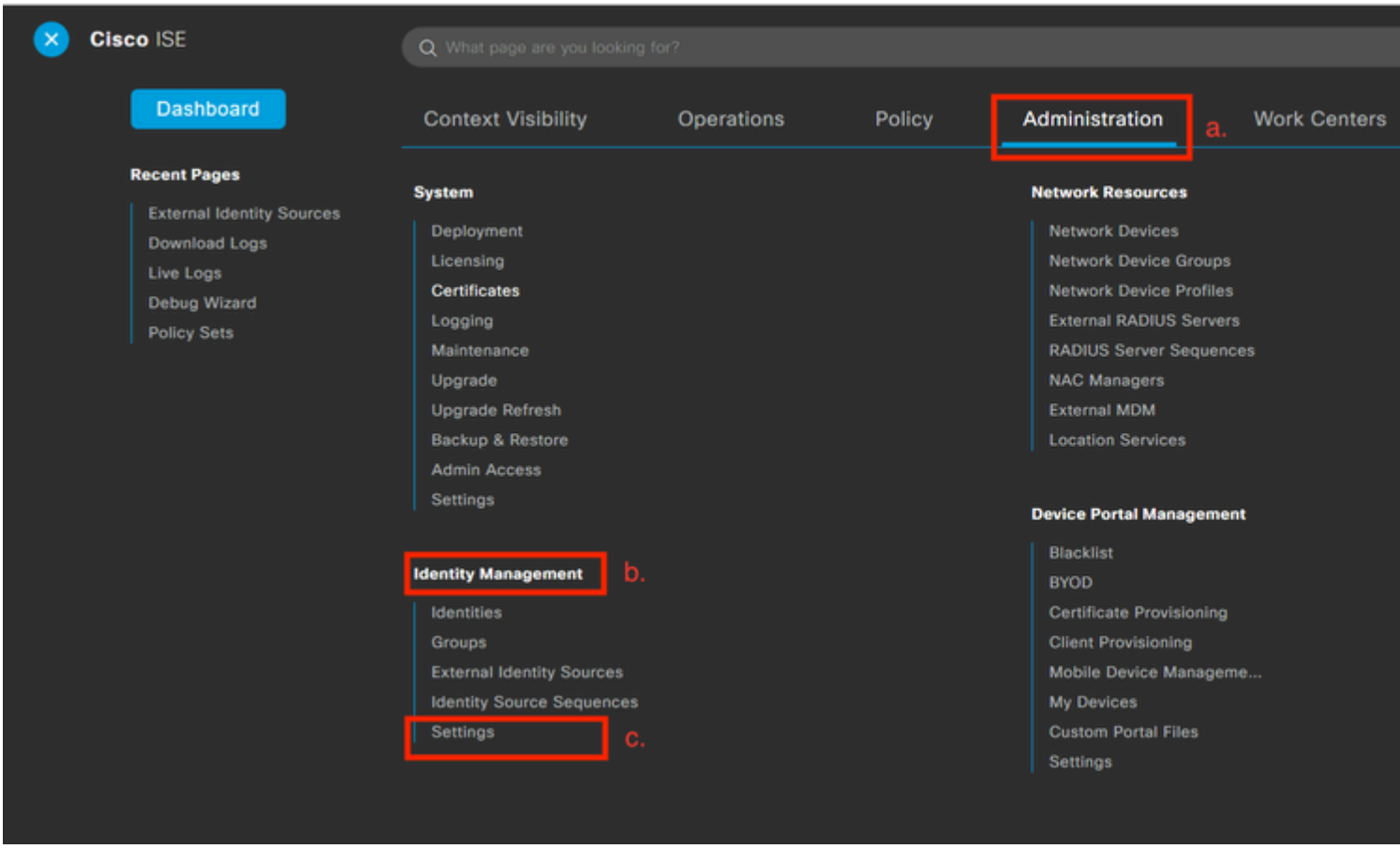


Abbildung 19:

Navigieren Sie zu Administration > Identity Management> Settings .

2. Aktivieren Sie den REST-ID-Dienst (standardmäßig deaktiviert).

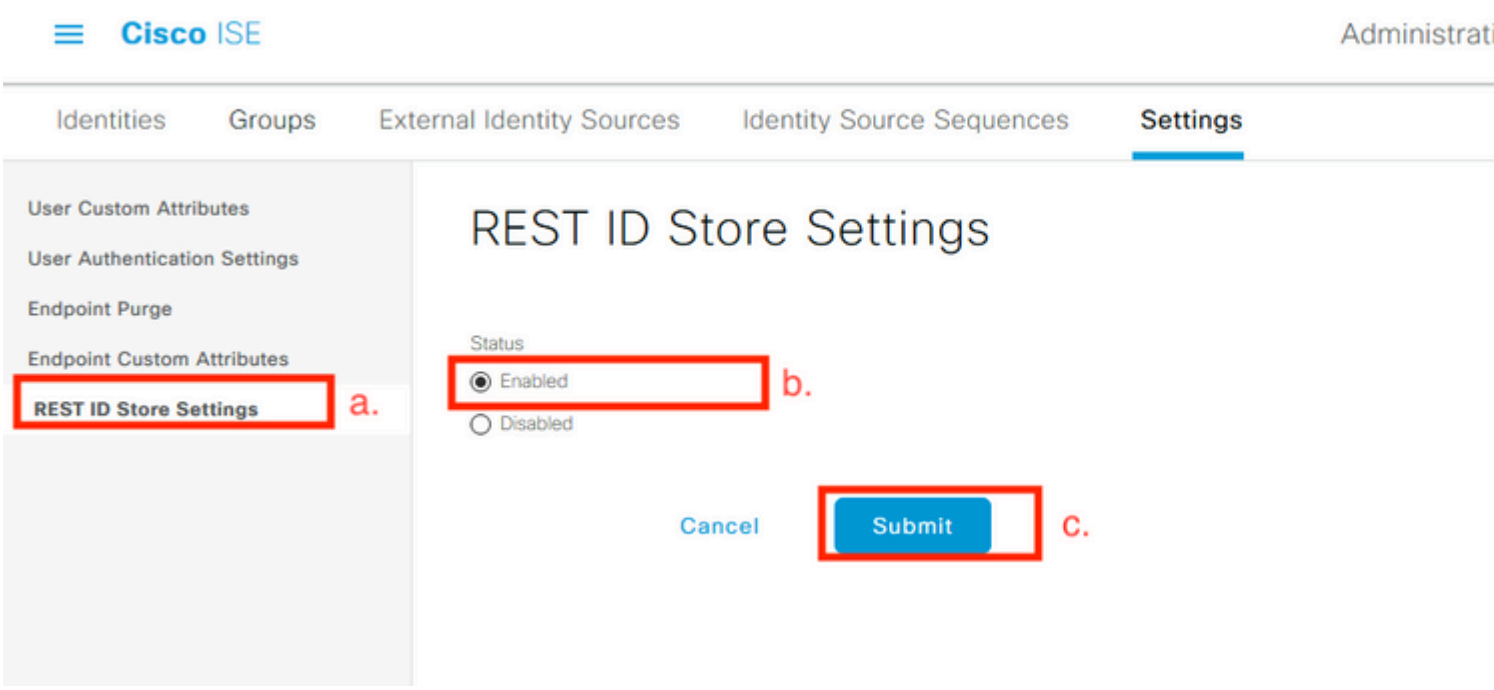


Abbildung 20:

Navigieren Sie zu REST ID Store Settings und den Status der REST-ID-Speichereinstellungen ändern, um Enable, dann Submit Ihre Änderungen.

3. Erstellen Sie einen REST-ID-Speicher.

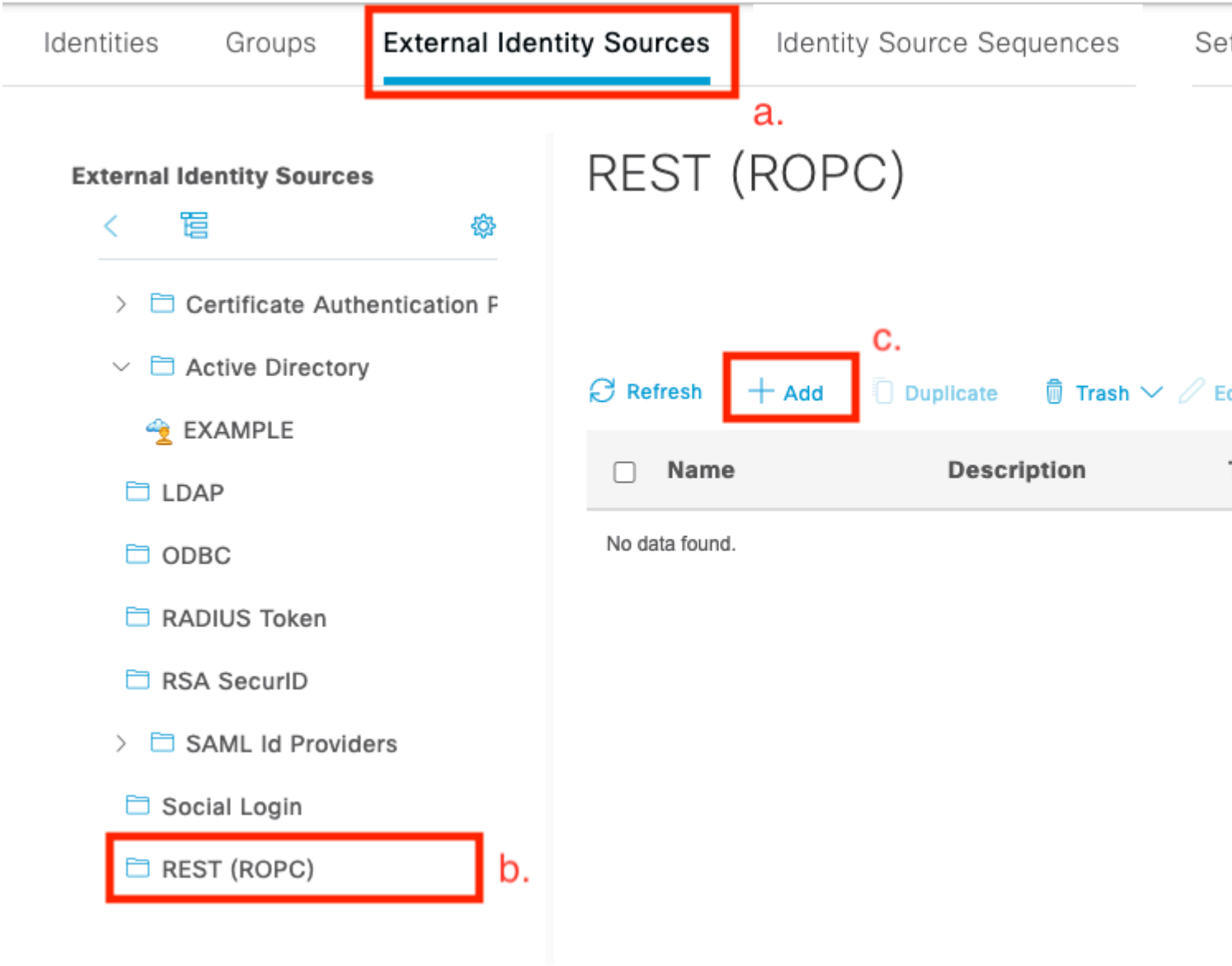


Abbildung 21:

Wechseln Sie zum External Identity Sources Registerkarte klicken Sie auf REST (ROPC) und klicken Sie auf **Hinzufügen**.

4. Konfigurieren Sie den REST-ID-Speicher.

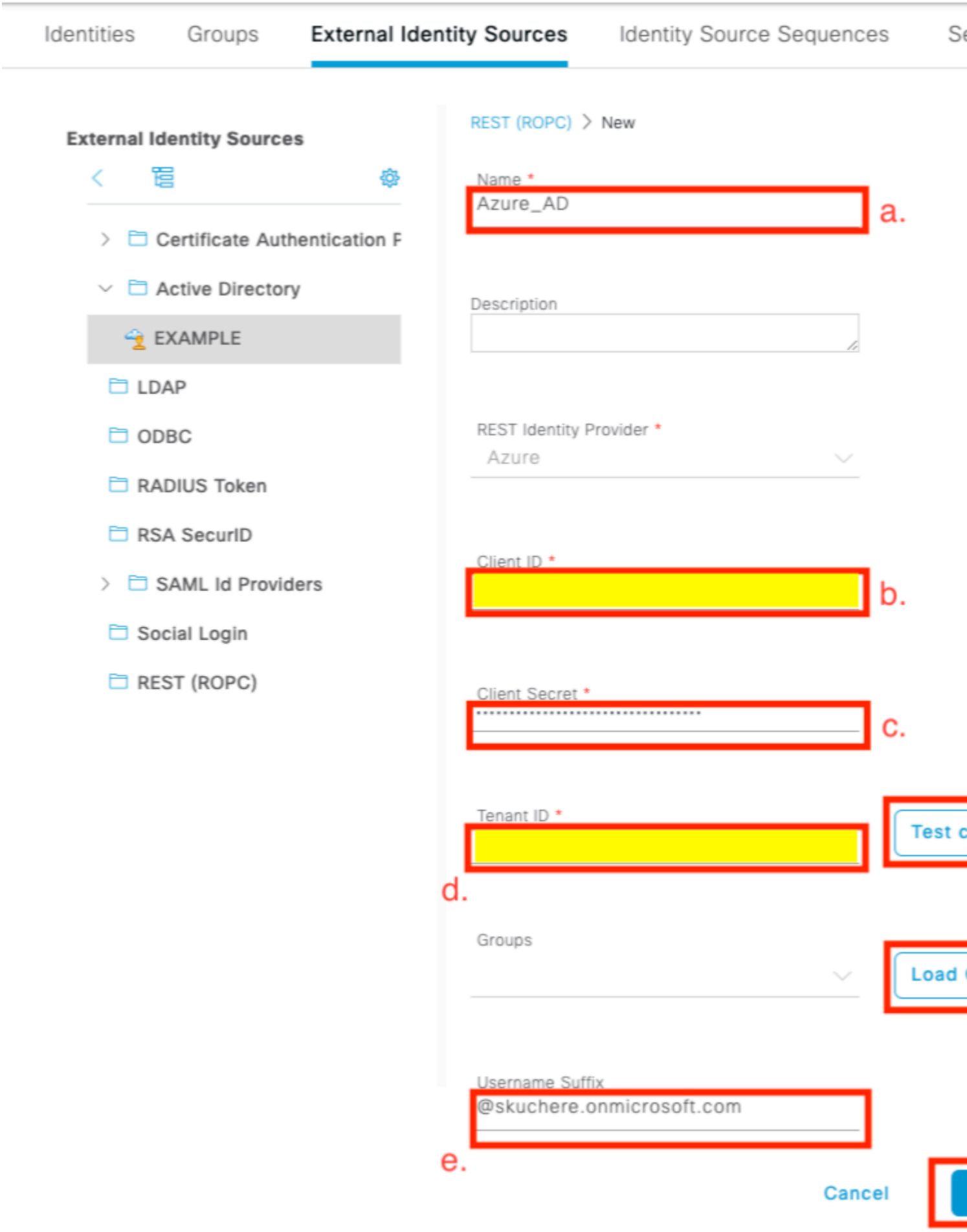

Identities
Groups
External Identity Sources
Identity Source Sequences
External Identity Sources
Certificate Authentication F
Active Directory
EXAMPLE
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
REST (ROPC)
REST (ROPC) > New
Name *
Azure_AD
a.
Description
REST Identity Provider *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

Abbildung 22:

antwort: Definieren Sie den ID-Speichernamen. Später kann dieser Name in der Liste der ISE-Wörterbücher gefunden werden, wenn Sie Autorisierungsrichtlinien konfigurieren. Außerdem wird dieser Name in der Liste der ID-Speicher angezeigt, die in den Authentifizierungsrichtlinieneinstellungen verfügbar sind, sowie in der Liste der ID-Speicher, die in der Identity Store-Sequenzkonfiguration verfügbar sind.

b. Geben Sie die Client-ID an (aus Azure AD in Schritt 8 des Azure AD-Integrationskonfigurationsabschnitts).

c. Geben Sie einen Clientschlüssel an (aus Azure AD in Schritt 7 des Azure AD-Integrationskonfigurationsabschnitts).

d. Geben Sie die Tenant-ID an (aus Azure AD in Schritt 8 des Abschnitts zur Konfiguration der Azure AD-Integration).

e. Benutzernamen-Sufix konfigurieren - ISE PSN verwendet standardmäßig einen vom Endbenutzer bereitgestellten Benutzernamen, der im sAMAccountName-Format bereitgestellt wird (kurzer Benutzername, z. B. bob). In diesem Fall kann Azure AD den Benutzer nicht finden. Benutzername Sufix ist der Wert, der dem Benutzernamen hinzugefügt wird, der vom Benutzer bereitgestellt wird, um den Benutzernamen in das UPN-Format zu bringen.

> **Hinweis**: ROPC ist auf die Benutzerauthentifizierung beschränkt, da es bei der Authentifizierung auf dem Benutzernamenattribut beruht. Geräteobjekte in Azure AD verfügen nicht über Benutzernamenattribute.

---

f. Drücken Sie auf Verbindung testen, um zu bestätigen, dass ISE die bereitgestellten App-Details verwenden kann, um eine Verbindung mit Azure AD herzustellen.

g. Drücken Sie auf "Gruppen laden", um im Azure AD verfügbare Gruppen zum REST-ID-Speicher hinzuzufügen. Das Beispiel hier zeigt, wie eine Administrationsumgebung aussieht.

> **Hinweis**: Bitte beachten Sie den Defekt Cisco Bug-ID CSCvx00345, da dies dazu führt, dass Gruppen nicht geladen werden. Der Fehler wurde in ISE 3.0 Patch 2 behoben.

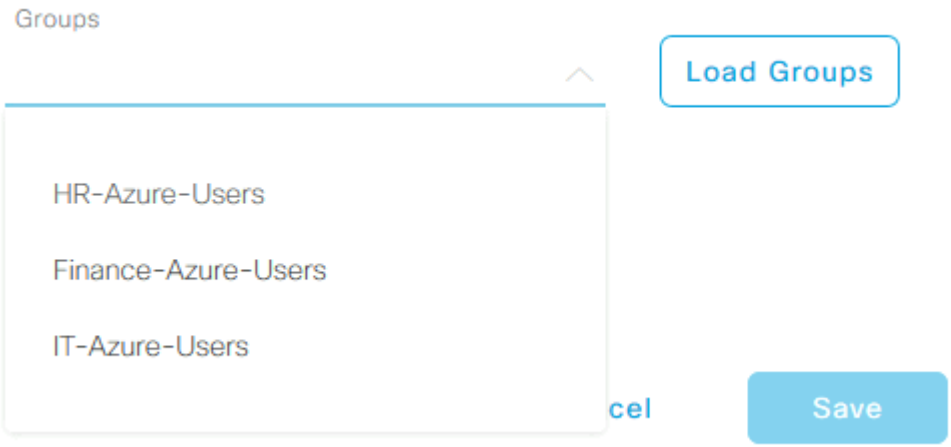


Abbildung 23:

h. Senden Sie Ihre Änderungen.

5. Bei diesem Schritt sollten Sie eine neue Identity Store-Sequenz erstellen, die einen neu erstellten REST-ID-Speicher enthält.

6. Ändern Sie zu dem Zeitpunkt, zu dem der REST-ID-Speicher oder die Identitätsspeichersequenz, die ihn enthält, der Authentifizierungsrichtlinie zugewiesen wurde, eine Standardaktion für Prozessfehler von DROP in REJECT, wie im Bild dargestellt.

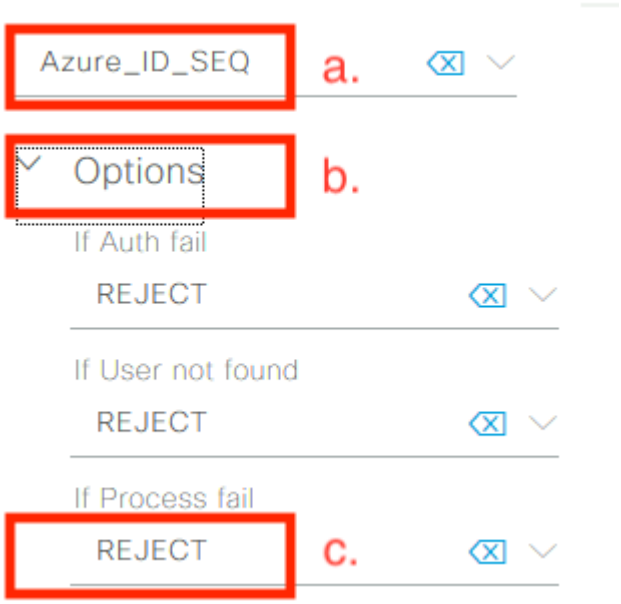


Abbildung 24:

antwort: Suchen Sie nach einer Authentifizierungsrichtlinie, die den REST-ID-Speicher verwendet.

b. Öffnen Sie die Dropdown-Liste Optionen.

c. Ändern Sie die Standardaktion für "Prozess fehlgeschlagen" von "DROP" in "REJECT".

Dies ist erforderlich, um zu vermeiden, dass PSN auf der NAD-Seite als ausgefallen markiert wird, und zwar zu einem Zeitpunkt, an dem bestimmte Fehler im REST-ID-Speicher auftreten, wie z. B.:

- Der Benutzer ist kein Mitglied einer Gruppe in Azure AD.
- Das Benutzerkennwort muss geändert werden.

7. REST ID-Speicherwörterbuch zur Autorisierungsrichtlinie hinzufügen

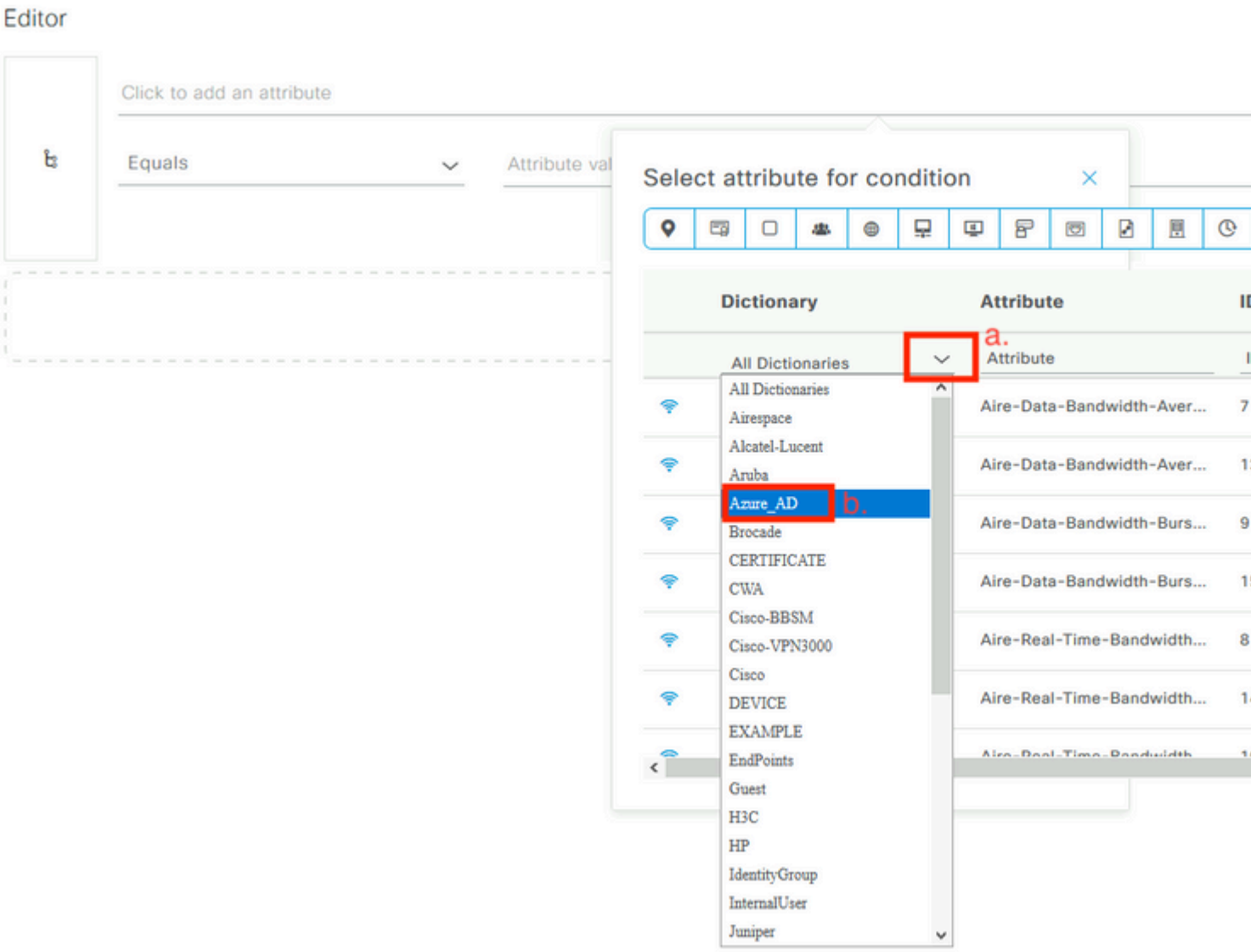


Abbildung 25:

antwort: Öffnen Sie die Dropdown-Liste All Dictionary.

b. Suchen Sie das Wörterbuch auf die gleiche Weise wie Ihre REST-ID.

8. Fügen Sie externe Identitätsgruppen hinzu (Ab ISE 3.0 ist das einzige im REST-ID-Speicher-Dictionary verfügbare Attribut eine externe Gruppe).

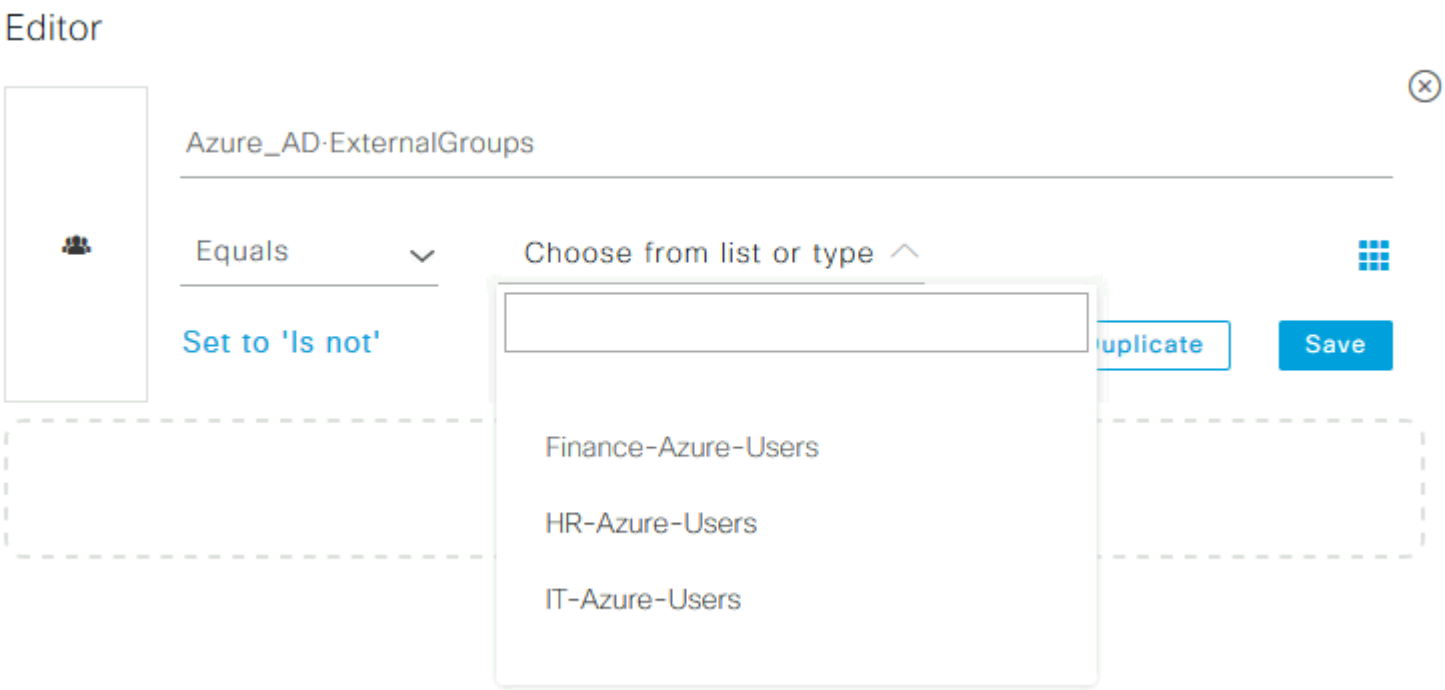


Abbildung 26:

ISE-Richtlinienbeispiele für verschiedene Anwendungsfälle

Bei der 802.1x-Authentifizierung kann die EAP-Tunnelbedingung aus dem Netzwerkzugriffs-Dictionary verwendet werden, um die EAP-TTLS-Versuche abzugleichen, wie im Bild gezeigt.

Abbildung 27:

antwort: Definieren Sie EAP Tunnel EQUAL to EAP-TTLS, um die Versuche abzugleichen, die an den REST-ID-Speicher weitergeleitet werden müssen.

b. Wählen Sie direkt im REST-ID-Speicher oder in der Identity Store Sequence aus, die diese in der Spalte "Use" (Verwenden) enthält.

Innerhalb einzelner Autorisierungsrichtlinien können externe Gruppen aus Azure AD zusammen mit dem EAP-Tunneltyp verwendet werden:

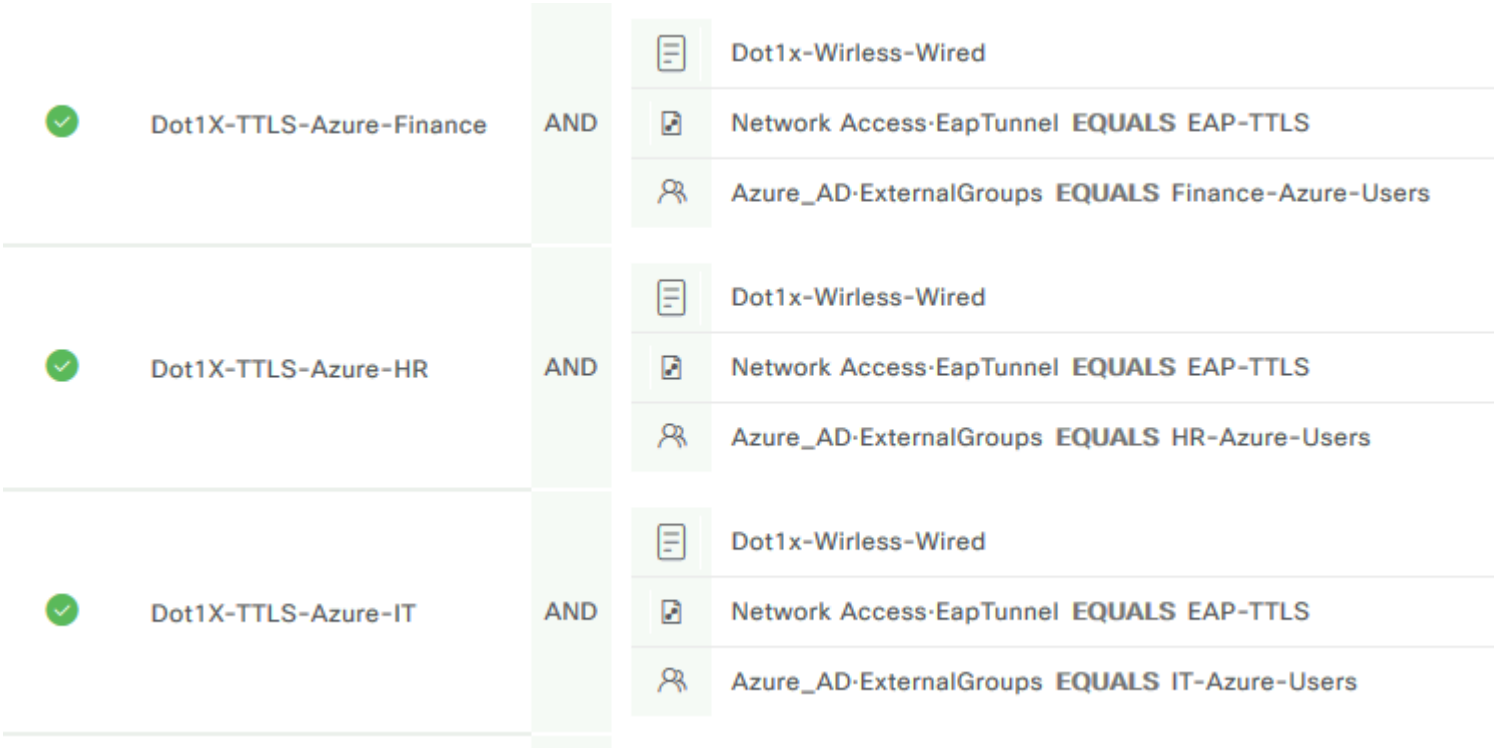


Abbildung 28:

Für VPN-basierten Datenfluss können Sie einen Tunnelgruppennamen als Differenzierungsmerkmal verwenden:

Authentifizierungsrichtlinie:

Autorisierungsrichtlinien:

Abbildung 29:

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Vergewissern Sie sich, dass der REST-Auth-Service auf dem ISE-Knoten ausgeführt wird.

Um dies zu überprüfen, müssen Sie den Befehl **show application status ise** in der Secure Shell (SSH)-Shell eines ISE-Zielknotens ausführen:

<#root>

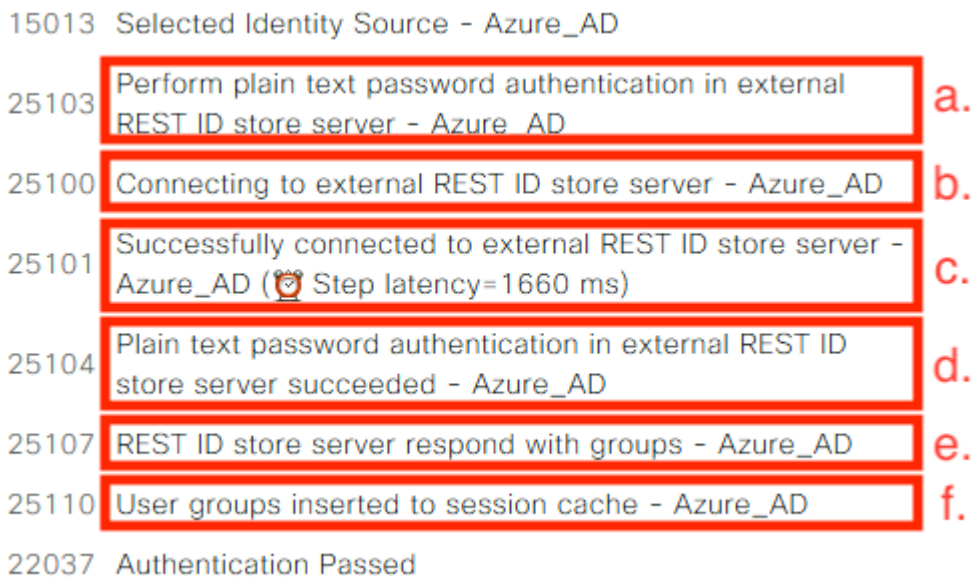
```
skuchere-ise30-1/admin# show application status ise

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. Überprüfen Sie, ob der REST-ID-Speicher zum Zeitpunkt der Authentifizierung verwendet wird (siehe Abschnitt "Schritte" im detaillierten Authentifizierungsbericht).



antwort: PSN startet die Nur-Text-Authentifizierung mit dem ausgewählten REST-ID-Speicher.

b. Verbindung mit Azure Cloud hergestellt.

c. Tatsächlicher Authentifizierungsschritt - Achten Sie auf den hier angegebenen Latenzwert. Wenn alle Ihre Authentifizierungen mit der Aure Cloud mit einer erheblichen Latenz zu kämpfen haben, wirkt sich dies auf den anderen ISE-Fluss aus, und infolgedessen wird die gesamte ISE-Bereitstellung instabil.

d. Bestätigung der erfolgreichen Authentifizierung.

e. Bestätigung der als Antwort angezeigten Gruppendaten.

f. Der Sitzungskontext wird mit den Daten der Benutzergruppe aufgefüllt. Weitere Informationen zum ISE-Sitzungsmanagement finden Sie in diesem Artikel - link.

3. Vergewissern Sie sich, dass Authentifizierungs-/Autorisierungsrichtlinien ausgewählt sind (hierzu wird der Abschnitt "Übersicht" des detaillierten Authentifizierungsberichts untersucht).

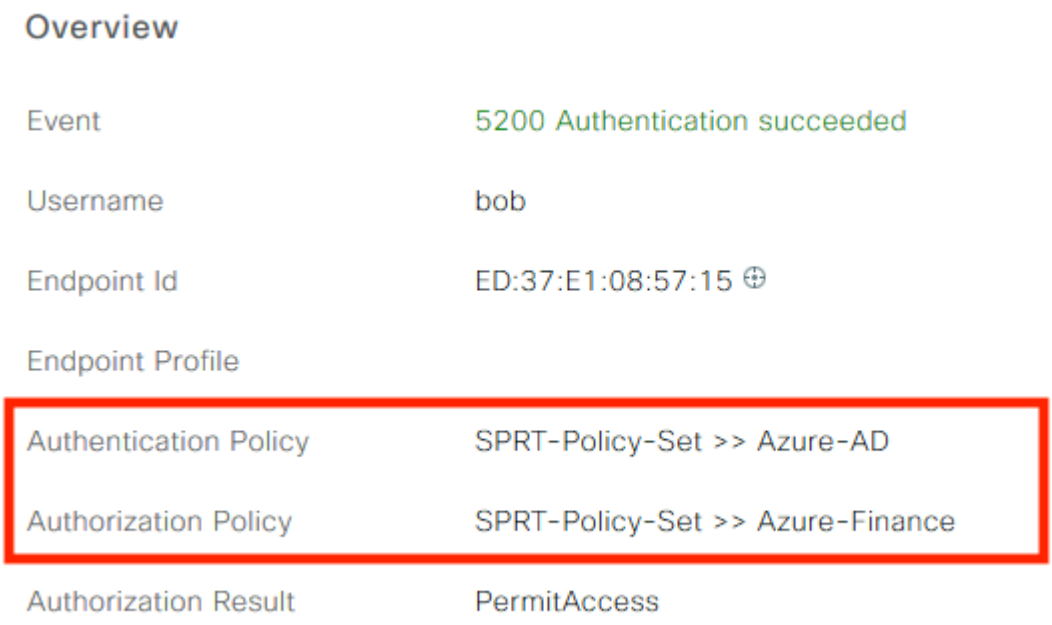


Abbildung 30:

Fehlerbehebung

In diesem Abschnitt finden Sie die Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Probleme mit dem REST-Authentifizierungsdienst

Um Probleme mit dem REST-Auth-Dienst zu beheben, müssen Sie mit der Überprüfung der Datei **ADE.log** beginnen. Standort des Support-Pakets: **/support/adeos/ade**

Ein Suchbegriff für REST Auth Service ist - **ROPC-control**.

Dieses Beispiel zeigt, wie der REST-Auth-Dienst gestartet wird:

```
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
```

Wenn der Dienst nicht startet oder unerwartet abstürzt, ist es immer sinnvoll, die **ADE.log** um einen problematischen Zeitraum zu überprüfen.

Probleme mit der REST-ID-Authentifizierung

Bei Authentifizierungsfehlern, wenn der REST-ID-Speicher verwendet wird, müssen Sie immer mit einem detaillierten Authentifizierungsbericht beginnen. Im Bereich "Other Attributes" (Andere Attribute) wird der Abschnitt "**RestAuthErrorMsg"** angezeigt, der einen von Azure Cloud zurückgegebenen Fehler enthält:

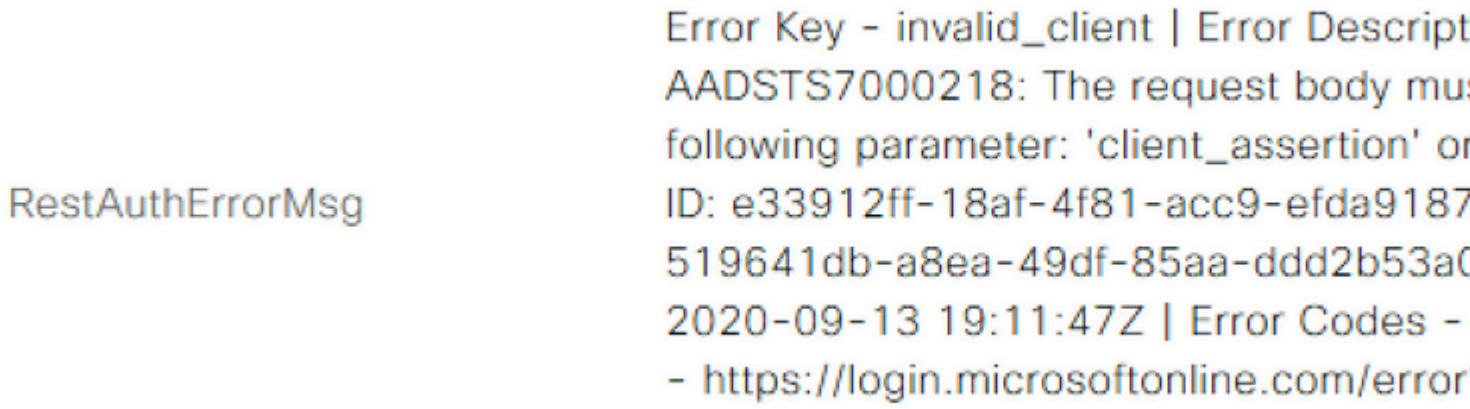


Abbildung 31:

Arbeiten mit den Protokolldateien

In ISE 3.0 ist Debug aufgrund der Funktion "Controlled Introduction of REST ID" standardmäßig aktiviert. Alle Protokolle der REST-ID werden in ROPC-Dateien gespeichert, die über die CLI angezeigt werden können:

```
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
```

Beachten Sie auf ISE 3.0 mit dem installierten Patch, dass der Dateiname rest-id-store.log und nicht ropc.log lautet. Das vorherige Suchbeispiel funktioniert, da der Ordnername nicht geändert wurde.

Diese Dateien können auch aus dem ISE-Supportpaket extrahiert werden.

Im Folgenden finden Sie einige Protokollbeispiele, die verschiedene Arbeits- und Nichtszenarien zeigen:

1. Zertifikatfehler, wenn Azure Graph vom ISE-Knoten nicht vertrauenswürdig ist. Dieser Fehler tritt auf, wenn Gruppen in der REST-ID-Speichereinstellung nicht geladen werden.

```
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)
```

Dieses Problem weist darauf hin, dass das Microsoft Graph-API-Zertifikat von ISE nicht vertrauenswürdig ist. ISE 3.0.0.458 verfügt nicht über eine DigiCert Global Root G2 CA, die im vertrauenswürdigen Speicher installiert ist. Dies ist im Mangel dokumentiert

- Cisco Bug-ID CSCvv80297 Um dieses Problem zu beheben, müssen Sie die DigiCert Global Root G2 CA im ISE Trusted Store installieren und als vertrauenswürdig für Cisco Services markieren.

Das Zertifikat kann hier heruntergeladen werden: https://www.digicert.com/kb/digicert-root-certificates.htm

2. Falscher Anwendungsgeheimnis.

```
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. Falsche APP-ID.

```
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. Benutzer nicht gefunden.

```
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. Benutzerkennwort abgelaufen - In der Regel kann es für den neu erstellten Benutzer passieren, da das von Azure Admin definierte Kennwort bei der Anmeldung bei Office365 geändert werden muss.

```
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. Gruppen können aufgrund falscher API-Berechtigungen nicht geladen werden.

```
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. Die Authentifizierung schlägt fehl, wenn ROPC auf Azure-Seite nicht zulässig ist.

```
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. Fehler bei der Authentifizierung, da der Benutzer keiner Azure-Gruppe angehört.

```
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: "n
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. Erfolgreiche Benutzerauthentifizierung und Gruppenabruf

```
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" : [ ]
}
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.