# تكوين معرف ISE 3.0 REST باستخدام Azure Active Directory

## المحتويات



## المقدمة

يصف هذا المستند كيفية تكوين تكامل Cisco ISE 3.0 مع Azure AD الذي تم تنفيذه من خلال خدمة الهوية REST باستخدام بيانات اعتماد كلمة مرور المالك المورد.

## معلومات أساسية

يصف هذا المستند كيفية تكوين تكامل محرك خدمات الهوية (ISE) 3.0 مع Microsoft (MS) Azure Active Directory (AD) واستكشاف أخطائه وإصلاحها من خلال خدمة الهوية نقل الحالة التمثيلية (REST) (ID) بمساعدة بيانات اعتماد كلمة مرور المالك المورد (ROPC).

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- السيدة أوزر
- فهم تنفيذ بروتوكول ROPC والقيود المفروضة عليه؛ [الارتباط]

## المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

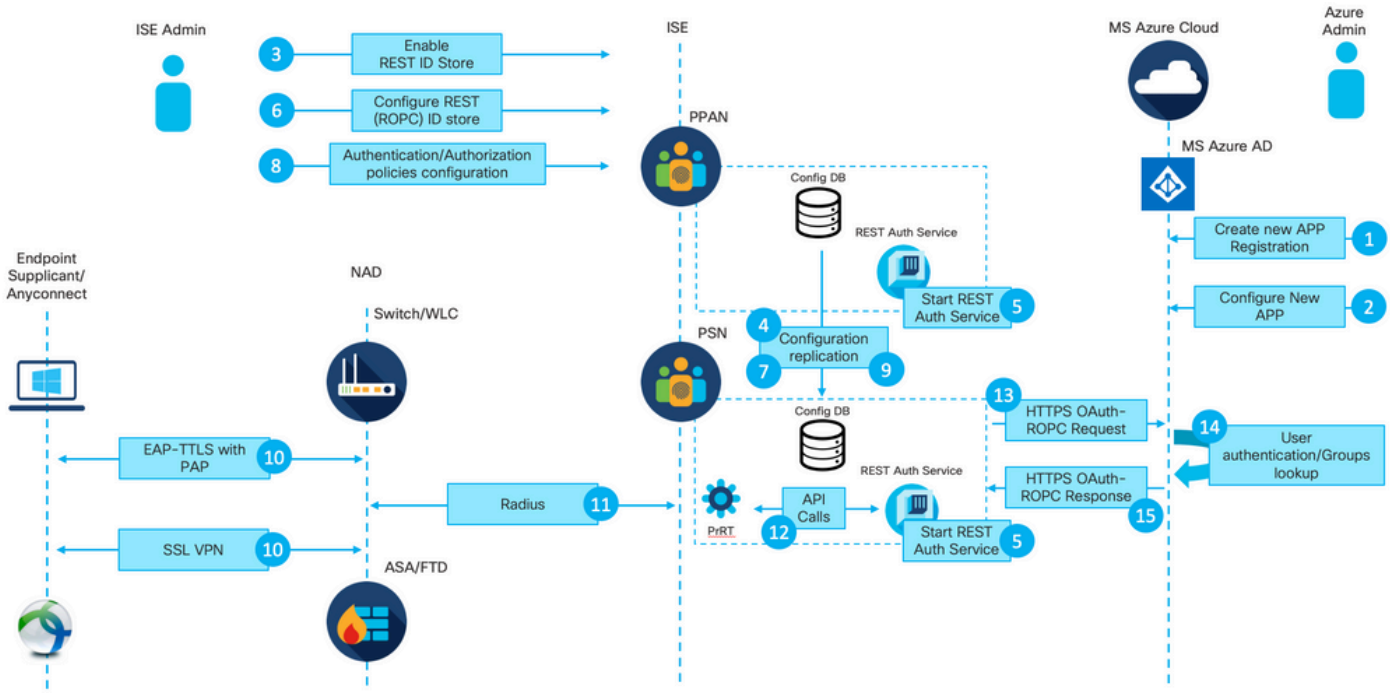
- ISE الإصدار 3.0 من Cisco
- السيدة أوزو
- WS-C3850-24P مع S/W 16.9.2
- ASAv مع 9.10 (1)
- Windows 10.0.18363

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# التكوين

تستند وظائف معرف ISE REST ID إلى الخدمة الجديدة التي تم تقديمها في ISE 3.0 - خدمة مصادقة REST. هذه الخدمة مسؤولة عن الاتصال ب Azure AD عبر التفويض المفتوح (OAuth) ROPC Exchange من أجل إجراء مصادقة المستخدم واستردادا المجموعة. يتم تعطيل خدمة مصادقة REST بشكل افتراضي، وبعد أن يقوم المسؤول بتمكينها، يتم تشغيلها على جميع عقد ISE في النشر. بما أن اتصال خدمة مصادقة REST بالسحابة يحدث عند وقت مصادقة المستخدم، فإن أي تأخيرات على المسار تجلب زمن وصول إضافي إلى تدفق المصادقة/التخويل. كما أن هذا زمن الوصول خارج نطاق التحكم في إختصاصات ISE، ويجب تخطيط أي تنفيذ لمصادقة REST واختباره بعناية لتجنب التأثير على خدمات ISE الأخرى.

## نظرة عامة على التدفق عالي المستوى



1. يقوم مسؤول سحابة Azure بإنشاء تسجيل تطبيق جديد (App). يتم إستخدام تفاصيل هذا التطبيق لاحقا على ISE لإنشاء اتصال مع Azure AD.

2. يجب على مسؤول سحابة Azure تكوين التطبيق باستخدام:

- إنشاء سر عميل
- تمكين ROPC
- إضافة مطالبات المجموعة
- تعريف أذونات واجهة برمجة التطبيقات (API)

3. يقوم مسؤول ISE بتشغيل خدمة مصادقة REST. يجب القيام بذلك قبل تنفيذ أي إجراء آخر.

4. تتم كتابة التغييرات في قاعدة بيانات التكوين ونسخها عبر نشر ISE بالكامل.

5. تبدأ خدمة مصادقة الراحة على جميع العقد.

6. يقوم مسؤول ISE بتكوين مخزن معرف REST بتفاصيل من الخطوة 2.

7. تتم كتابة التغييرات في قاعدة بيانات التكوين ونسخها عبر نشر ISE بالكامل.

8. يقوم مسؤول ISE بإنشاء تسلسل مخزن هوية جديد أو يقوم بتعديل التسلسل الموجود بالفعل ويقوم بتكوين سياسات المصادقة/التفويض.

9. تتم كتابة التغييرات في قاعدة بيانات التكوين ونسخها عبر نشر ISE بالكامل.

10. تقوم نقطة النهاية بتهيئة المصادقة. وفقا لمواصفات بروتوكول ROPC، يجب توفير كلمة مرور المستخدم إلى النظام الأساسي لهوية Microsoft في نص واضح عبر اتصال HTTP مشفر؛ ونظرا لهذه الحقيقة، فإن خيارات المصادقة الوحيدة المتاحة المدعومة من قبل ISE هي:

- بروتوكول المصادقة الموسع-تأمين طبقة النقل النفقي (EAP-TTLS) مع بروتوكول مصادقة كلمة المرور (PAP) كطريقة داخلية
- مصادقة AnyConnect SSL VPN باستخدام PAP

11. التبادل مع عقدة خدمة سياسة ISE (PSN) عبر RADIUS.

12. يرسل وقت تشغيل العملية (PrRT) طلبا إلى خدمة معرف REST بتفاصيل المستخدم (اسم المستخدم/كلمة المرور) عبر واجهة برمجة التطبيقات (API) الداخلية.

13. ترسل خدمة REST ID طلب OAuth ROPC إلى Azure AD عبر بروتوكول نقل النص التشعبي الآمن (HTTPS).

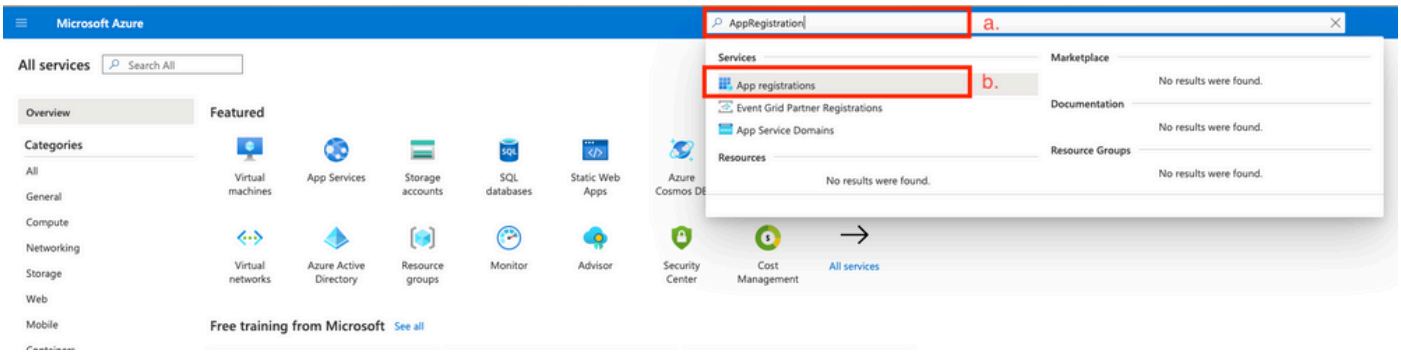
14. يقوم Azure AD بإجراء مصادقة المستخدم وجلب مجموعات المستخدمين.

15. تم إرجاع نتيجة المصادقة/التخويل إلى ISE.

بعد النقطة 15، يتم إرجاع نتائج المصادقة والمجموعات التي تم إحضارها إلى PrRT، والتي تتضمن تدفق تقييم السياسة وتعيين نتيجة المصادقة/التخويل النهائية. تم إرجاع إما Access-Accept بسمات من ملف تعريف التخويل أو Access-Reject إلى جهاز الوصول إلى الشبكة (NAD).

## تكوين Azure AD للتكامل

1. حدد موقع خدمة AppRegister كما هو موضح في الصورة.

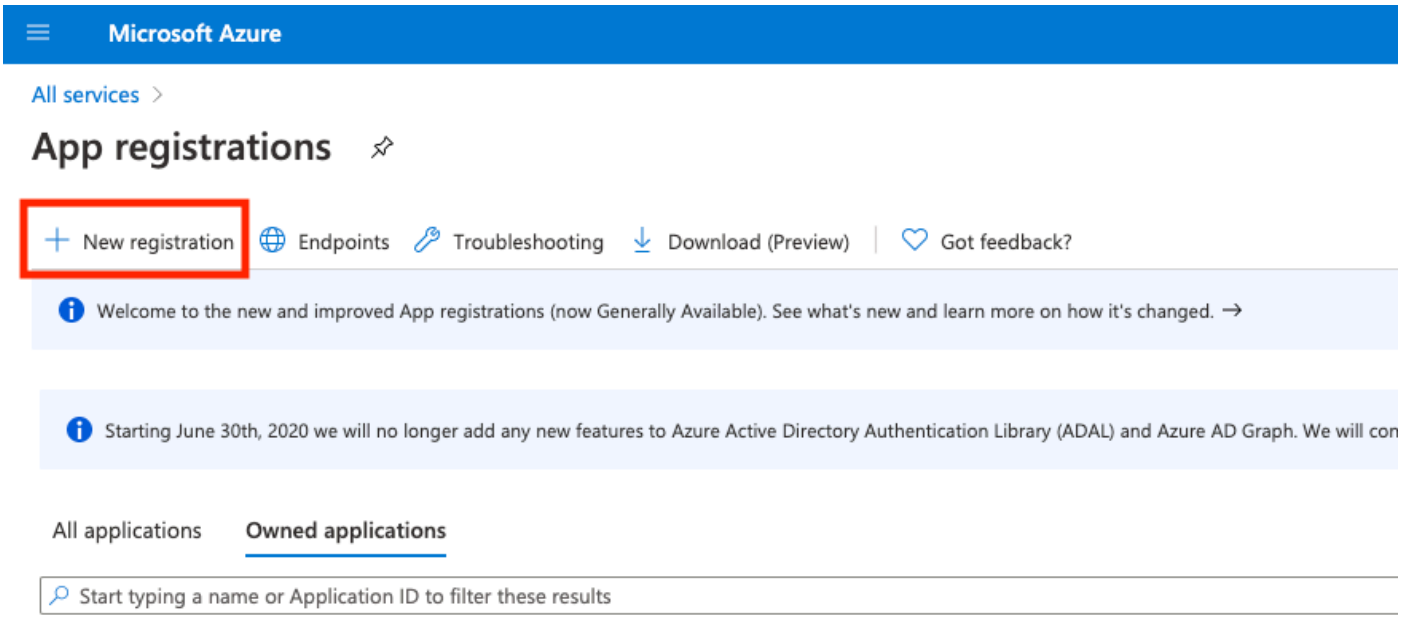



شكل 2.

أ. اكتب AppRegister في شريط البحث العمومي.

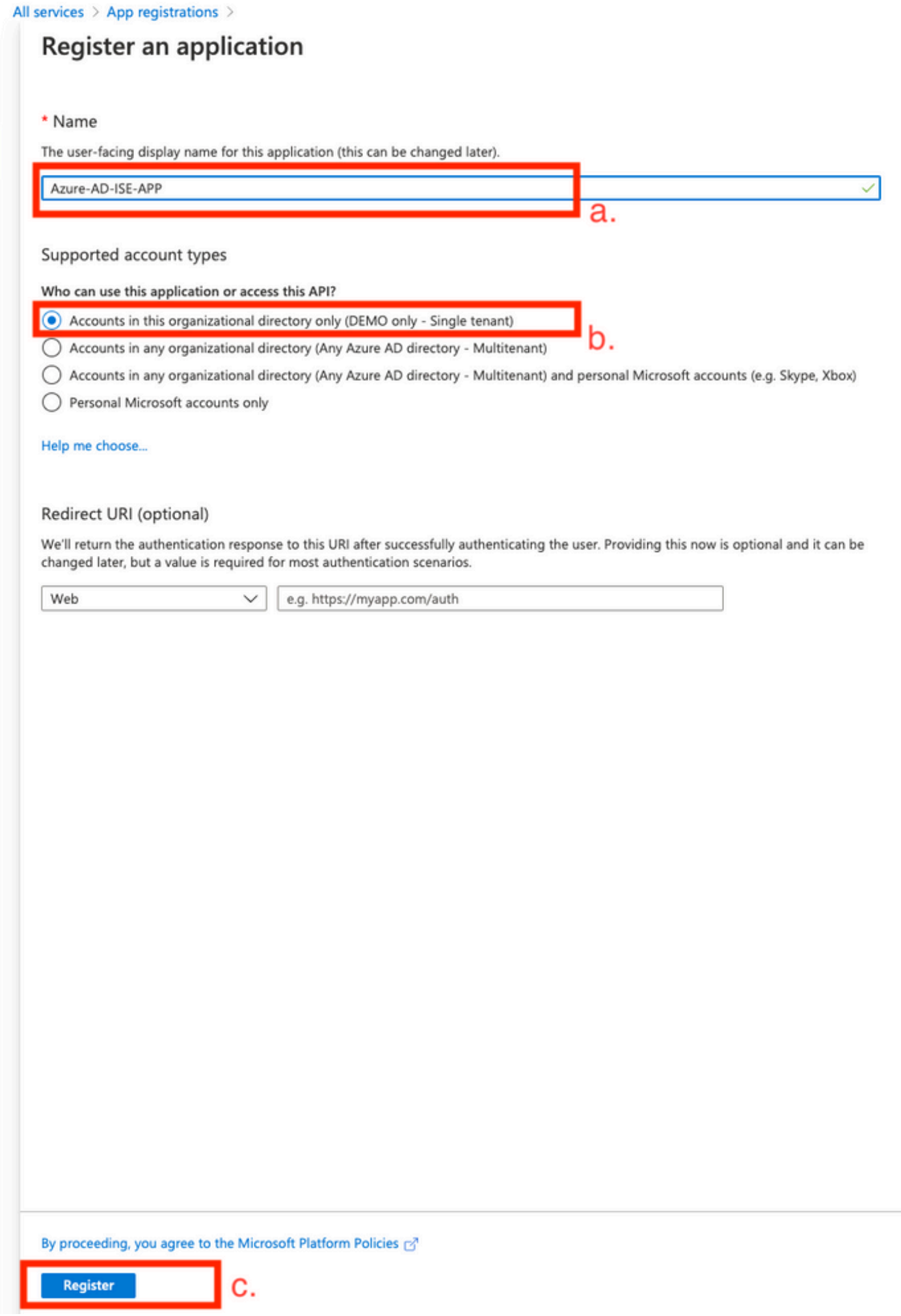
ب. انقر فوق خدمة تسجيل التطبيق.

2. إنشاء تسجيل تطبيق جديد.




شكل 3.

3. تسجيل تطبيق جديد.


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.

4. لكش

عند تكوين نهج التفويض. كما يتم عرض هذا الاسم في قائمة مخازن المعرفات المتاحة في إعدادات نهج المصادقة وفي قائمة مخازن المعرفات المتاحة في تكوين تسلسل مخزن الهوية.

ب. قم بتوفير معرف العميل (مأخوذ من Azure AD في الخطوة 8. من قسم تكوين Azure AD).

ج. توفير سر العميل (مأخوذ من Azure AD في الخطوة 7. من قسم تكوين كامل Azure AD).

د. توفير معرف المستأجر (مأخوذ من Azure AD في الخطوة 8. من قسم تكوين كامل Azure AD).

ه. تكوين اسم المستخدم Sufix - بشكل افتراضي، يستخدم ISE PSN اسم مستخدم تم توفيره من قبل المستخدم النهائي، والذي يتم توفيره في تنسيق sAMAccountName (اسم المستخدم المختصر، على سبيل المثال، بوب)؛ في مثل هذه الحالة، لا يمكن لـ Azure AD تحديد موقع المستخدم. Username Sufix هي القيمة المضافة إلى اسم المستخدم الذي يقدمه المستخدم لإحضار اسم المستخدم إلى تنسيق UPN.

---

ملاحظة: يقتصر ROPC على مصادقة المستخدم لأنه يعتمد على سمة اسم المستخدم أثناء المصادقة. لا تحتوي كائنات الجهاز في Azure AD على سمات اسم المستخدم.

---

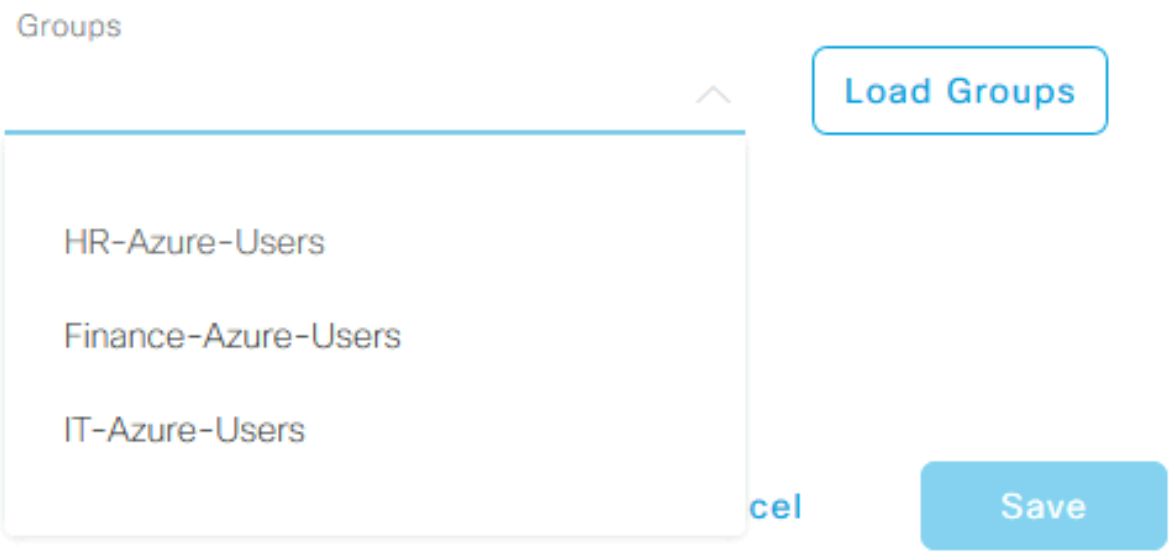
و. اضغط على اتصال الاختبار للتأكد من إمكانية استخدام ISE لتفاصيل التطبيق المقدمة لإنشاء اتصال مع Azure AD.

g. اضغط على مجموعات التحميل لإضافة المجموعات المتوفرة في مخزن معرف Azure AD إلى REST. يوضح المثال التالي كيفية ظهور تجربة المسؤول.

---

ملاحظة: يرجى الانتباه إلى الخلل في معرف تصحيح الأخطاء من Cisco CSCvx00345، لأنه يتسبب في عدم تحميل المجموعات. وقد تم إصلاح الخلل في حزمة ISE 3.0 2.

---

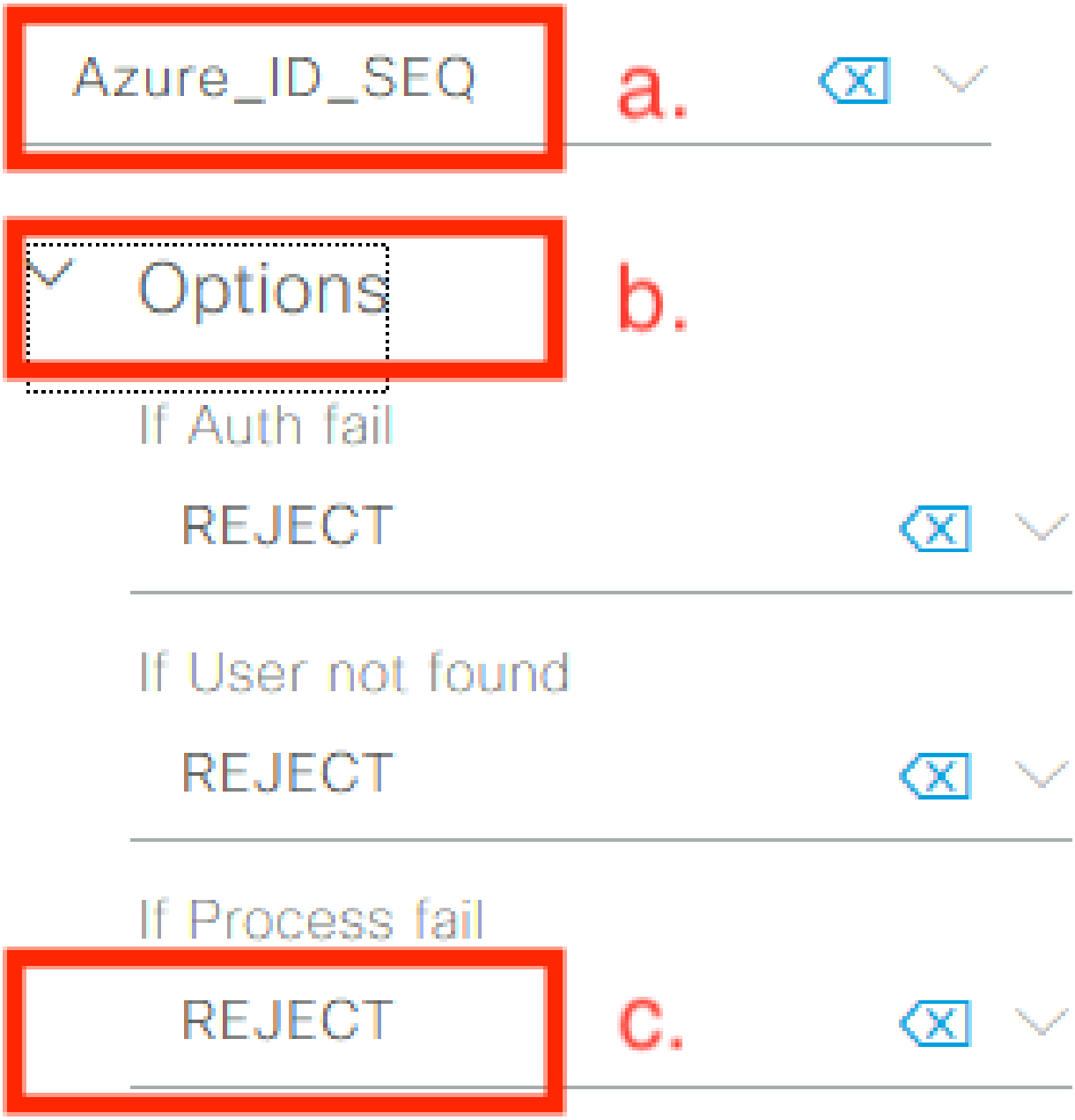



شكل 23.

ح. إرسال التغييرات الخاصة بك.

5. في هذه الخطوة، ضع في الاعتبار إنشاء تسلسل مخزن هوية جديد، يتضمن مخزن معرف REST الذي تم إنشاؤه حديثا.

6. في اللحظة التي يتم فيها تعيين تسلسل مخزن معرف REST أو مخزن الهويات الذي يحتوي على نهج المصادقة، قم بتغيير الإجراء الافتراضي لفشل العملية من DROP إلى REJECT كما هو موضح في الصورة.




شكل 24.

أ. تحديد موقع نهج المصادقة الذي يستخدم مخزن معرف REST.

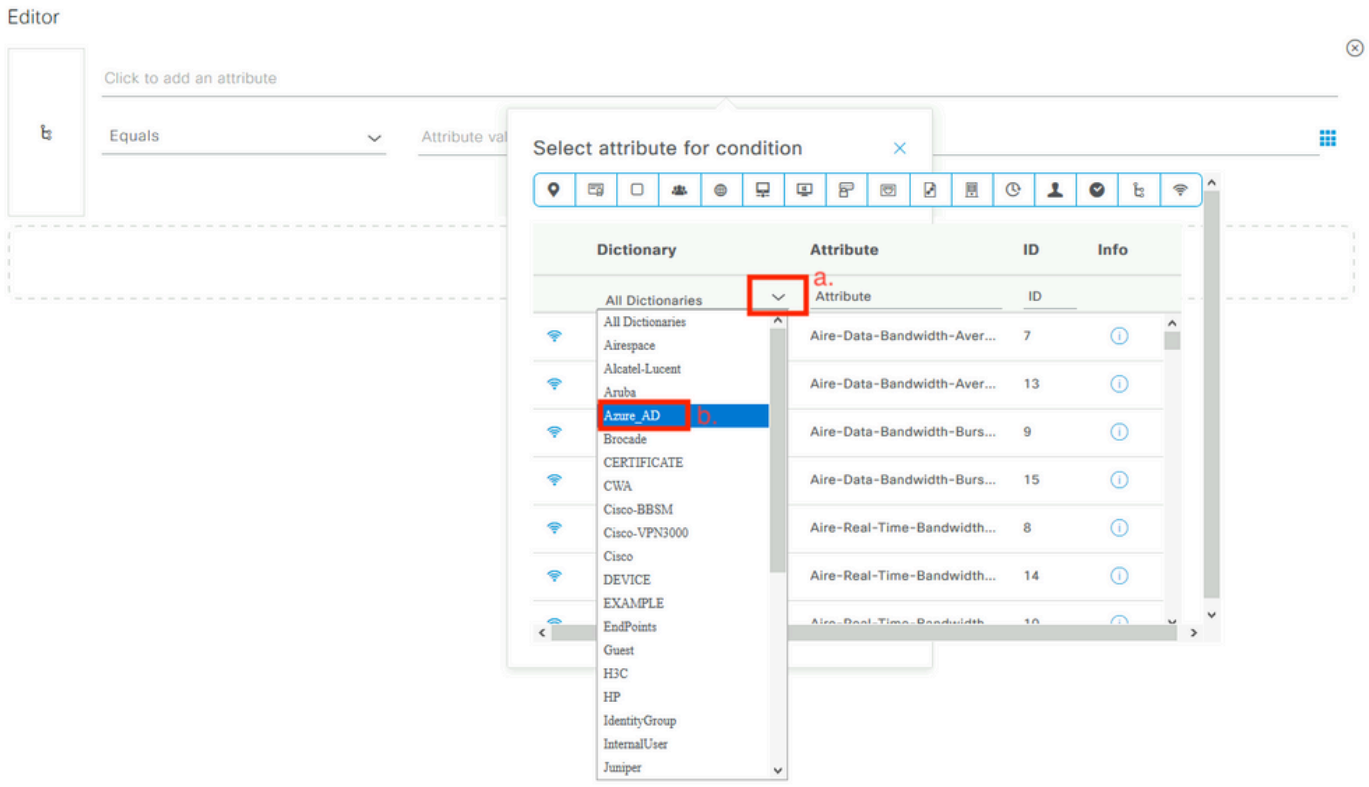
ب. فتح قائمة الخيارات المنسدلة.

ج. فشل إجراء التغيير الافتراضي للعملية من DROP إلى REJECT.

يلزم إجراء هذا لتجنب وضع علامة PSN كشيء ميت على جانب NAD في وقت تحدث فيه حالات فشل معينة داخل مخزن REST ID مثل:

- المستخدم ليس عضوا في أي مجموعة في Azure AD.
- يجب تغيير كلمة مرور المستخدم.

7. إضافة قاموس مخزن معرف REST إلى نهج التخويل.

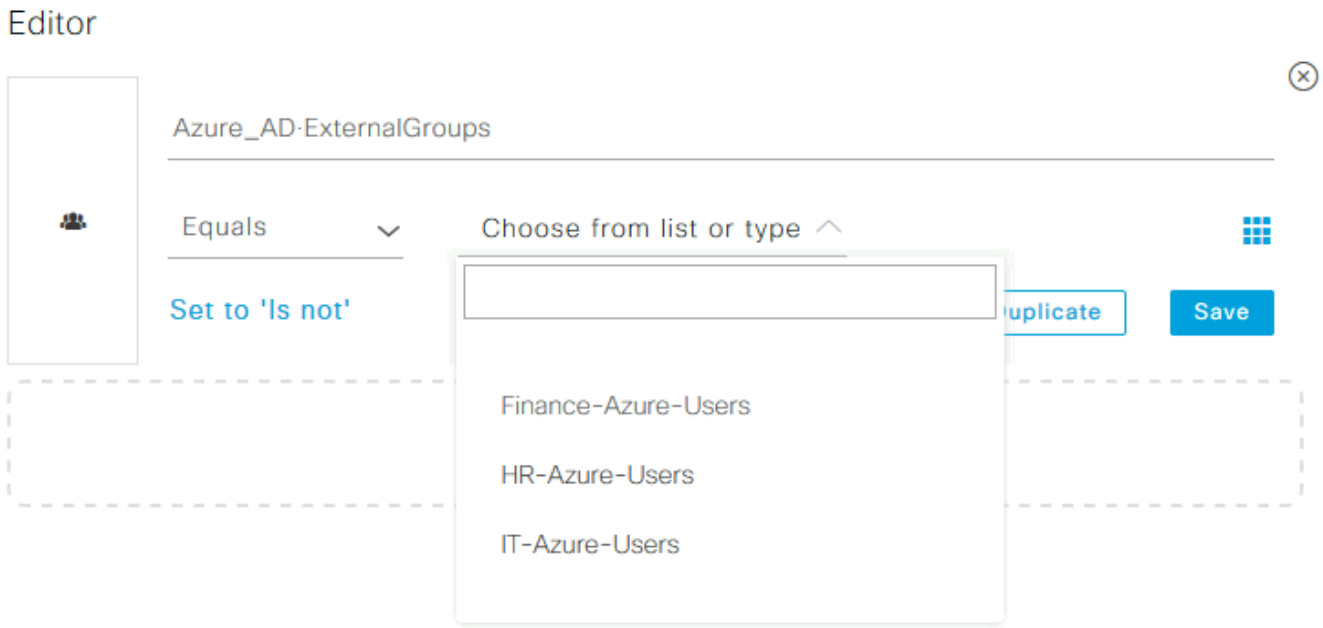



شكل 25.

أ. فتح كافة القوائم المنسدلة للقاموس.

ب. حدد مكان القاموس المسمى بنفس طريقة مخزن REST ID الخاص بك.

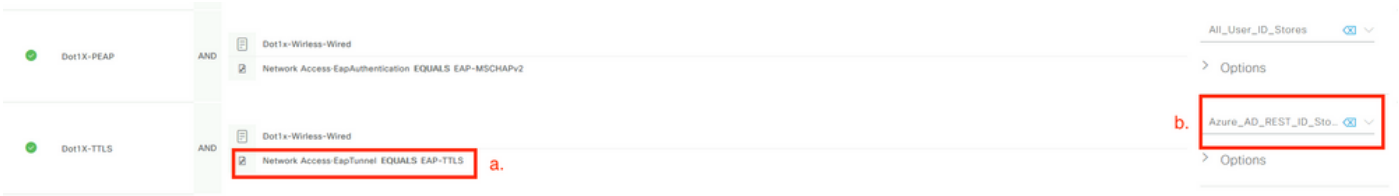
8. إضافة مجموعات هوية خارجية (حتى ISE 3.0، السمة الوحيدة المتوفرة في قاموس مخزن معرف REST هي مجموعة خارجية).




شكل 26.

## أمثلة سياسة ISE لحالات إستخدام مختلف

في حالة مصادقة Dot1x، يمكن إستخدام شرط نفق EAP من قاموس الوصول إلى الشبكة لمطابقة مجموعات EAP-TTLS كما هو موضح في الصورة.

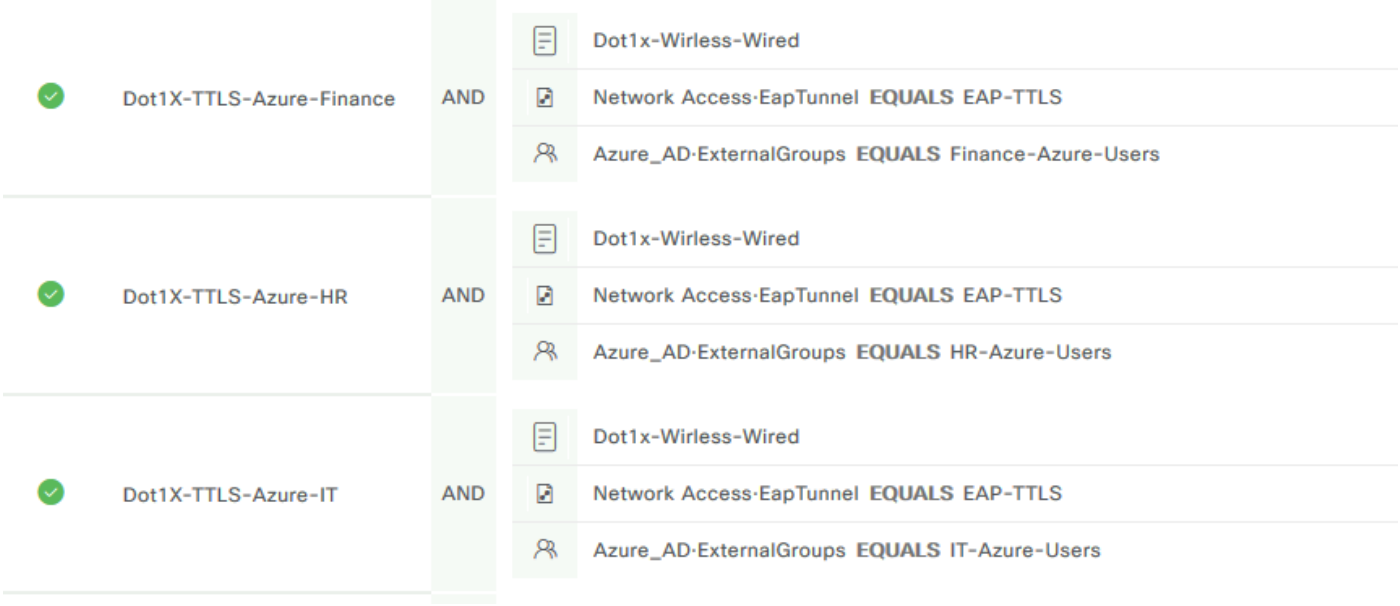



شكل 27.

أ. تحديد نفق EAP المساوي ل EAP-TTLS لمطابقة المحاولات التي يلزم إعادة توجيهها إلى مخزن معرف REST.

ب. حدد في مخزن معرف REST مباشرة أو تسلسل مخزن الهويات، الذي يحتوي عليه في عمود "الاستخدام".

داخل سياسات التخويل الفردية، يمكن إستخدام المجموعات الخارجية من Azure AD مع نوع نفق EAP:




شكل 28.

بالنسبة للتدفق المستند إلى شبكة VPN، يمكنك إستخدام اسم مجموعة نفق كمميز:

نهج المصادقة:


نهج التخويل:


شكل 29.

# التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. تأكد من تشغيل خدمة مصادقة REST على عقدة ISE.

للتحقق من ذلك، يلزمك تنفيذ الأمر show application status ise في طبقة طبقة الأمان

(SSH) من عقدة ISE الهدف:

<#root>

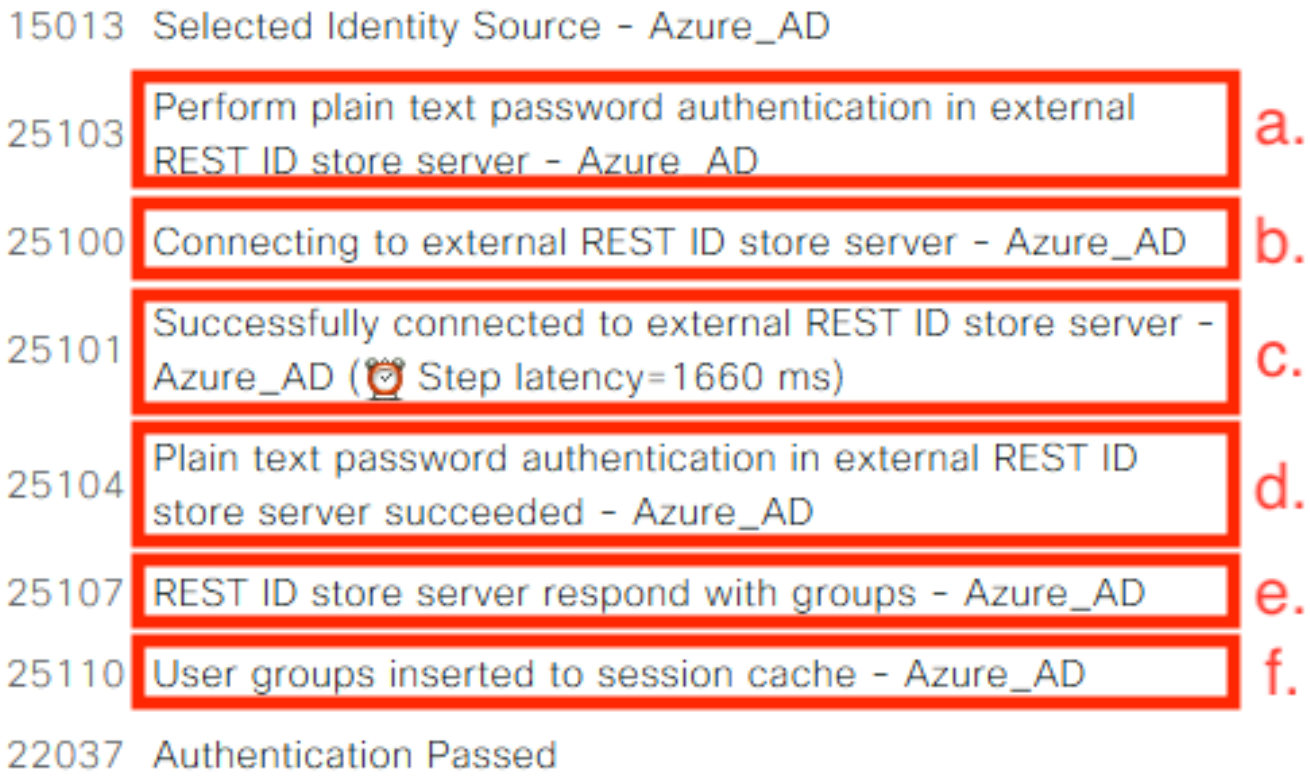
```
skuchere-ise30-1/admin# show application status ise

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. تحقق من إستخدام مخزن معرف REST في وقت المصادقة (تحقق من الخطوات. قسم من تقرير المصادقة التفصيلي).




أ. يبدأ PSN مصادقة النص العادي مع مخزن معرف REST المحدد.

ب. الاتصال المنشأ مع Azure Cloud.

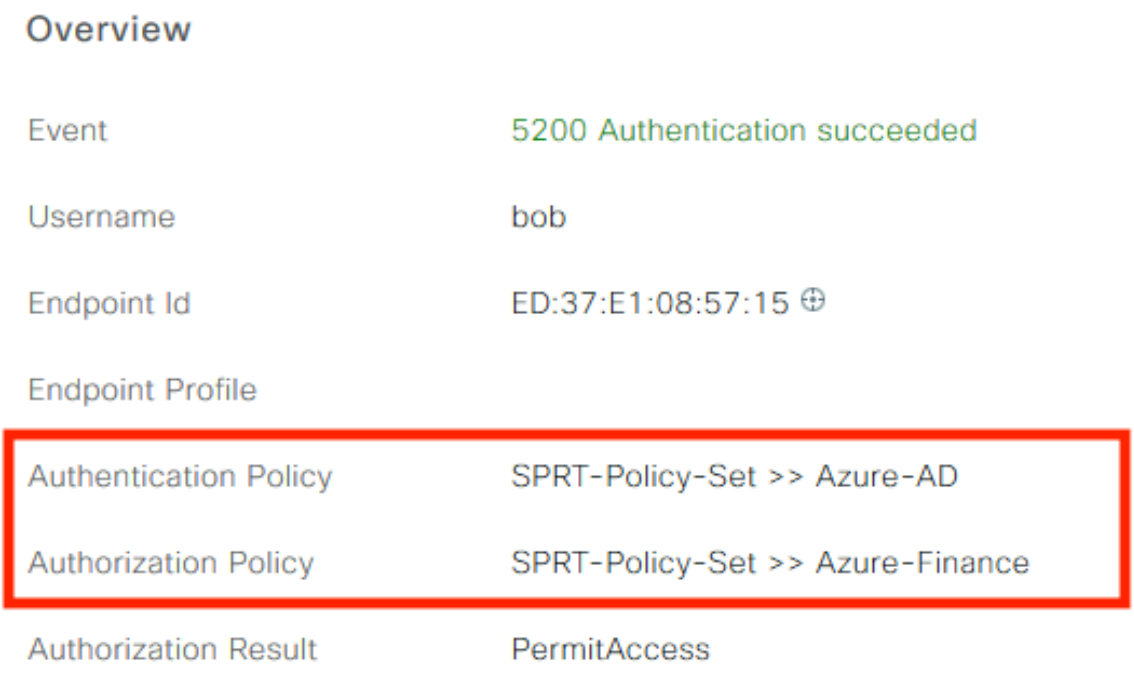
ج. خطوة المصادقة الفعلية - انتبه إلى قيمة زمن الانتقال المعروضة هنا. في حالة مواجهة جميع المصادقات الخاصة بك مع سحابة Aure لزمن وصول كبير، يؤثر هذا على تدفق ISE الآخر، وتتيجة لذلك، يصبح نشر ISE بالكامل غير مستقر.

د - تأكيد نجاح المصادقة.

ه - تأكيد بيانات المجموعة المقدمة ردا على ذلك.

و - سياق جلسة العمل المأهول ببيانات مجموعة المستخدمين. لمزيد من التفاصيل حول عملية إدارة جلسة عمل ISE، راجع مراجعة هذا المقال - [ارتباط.]

3. تأكد من تحديد سياسات المصادقة/التخويل المتوقعة (لقسم "التحقق من النظرة العامة" هذا في تقرير المصادقة التفصيلي).




شكل 30.

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم المعلومات التي يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

### المشاكل المتعلقة بخدمة مصادقة REST

لاستكشاف أخطاء أي مشاكل تتعلق بخدمة مصادقة REST وإصلاحها، يلزمك البدء بمراجعة ملف ADE.log. موقع مجموعة الدعم - /الدعم/adeos/ade

كلمة البحث الرئيسية لخدمة مصادقة REST هي - التحكم في ROPC.

يوضح هذا المثال كيفية بدء تشغيل خدمة مصادقة REST:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

في الحالات التي تفشل فيها الخدمة في البدء أو تنخفض بشكل غير متوقع، من المنطقي دائما البدء من خلال مراجعة ADE.Log حول إطار زمني مثير للمشاكل.

## مشاكل مصادقة معرف REST

في حالة فشل المصادقة عند إستخدام مخزن معرف REST، يلزمك دائما البدء من تقرير مصادقة مفصل. في منطقة "السمات الأخرى"، يمكنك رؤية مقطع - RestAuthErrorMsg يحتوي على خطأ تم إرجاعه من قبل سحابة Azure:

| | |
|---|---|
| RestAuthErrorMsg | Error Key - invalid_client \| Error Description - AADSTS7000218: The request body must contain the following parameter: 'client_assertion' or 'client_secret'. Trace ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID: 519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp: 2020-09-13 19:11:47Z \| Error Codes - [7000218] \| Error URI - https://login.microsoftonline.com/error?code=7000218 |

شكل 31.

## العمل باستخدام ملفات السجل

في ISE 3.0 بسبب التقديم المتحكم به لميزة REST ID، يتم تمكين تصحيح الأخطاء لها بشكل افتراضي. يتم تخزين جميع السجالت المتعلقة بمعرف REST في ملفات ROPC التي يمكن عرضها عبر CLI (واجهة سطر الأوامر):

```
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 filte
```

في ISE 3.0 مع التصحيح المثبت، لاحظ أن اسم الملف هو rest-id-store.log وليس ropc.log. يعمل مثال البحث السابق الذي تم توفيره لأن اسم المجلد لم يتغير.

أو أن هذا مبرد يستطيع كنت استخرجت من ال ISE دعم حزمة.

فيما يلي بعض أمثلة السجل التي تظهر سيناريوهات عمل وغير عمل مختلفة:

1. خطأ في الشهادة عندما ال تكون Azure Graph موثوق بها من قبل عقدة ISE. يمكن مالحظة هذا الخطأ عندما ال يتم تحميل المجموعات في إعداد مخزن معرف 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 appl
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
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)
```

تشير هذه المشكلة إلى أن شهادة واجهة برمجة تطبيقات Microsoft Graph غير موثوق بها من قبل ISE. الـ ISE 3.0.0.458 يحتوي على مرجع مصدق G2 جذر عمومي من DigiCert مثبت في المخزن الموثوق به. وهذا موثق في الخلل

- عرف تصحيح الأخطاء من Cisco CSCvv80297 لمعالجة هذه المشكلة، يلزمك تثبيت المرجع المصدق DigiCert Global Root G2 في المخزن الموثوق به لـ ISE ووضعه العامة كموثوق به لخدمات Cisco.

يمكن تنزيل الشهادة من هنا - https://www.digicert.com/kb/digicert-root-certificates.htm

2. سر تطبيق خاطئ.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
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 s
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(AzureIdentity
```

3. عرف تطبيق غير صحيح.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
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
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. لم يتم العثور على المستخدم.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
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_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
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. انتهت صلاحية كلمة مرور المستخدم - عادة ما يمكن أن يحدث للمستخدم الذي تم إنشاؤه حديثا حيث أن كلمة المرور التي تم تعريفها بواسطة مسؤول Azure يجب تغييرها في وقت تسجيل الدخول إلى Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
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_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
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. لا يمكن تحميل المجموعات بسبب أذونات API غير صحيحة.

```
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. تفشل المصادقة عندما يتم السماح بـ ROPC على جانب Azure.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
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_des
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
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. تفشل المصادقة نظرا لأن المستخدم ال ينتمي إلى أي مجموعة على جانب Azure.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
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 tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. مصادقة المستخدم الناجحة واستعادة المجموعة.

```
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 filte
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
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.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
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" : [ ]
}
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).