تكوين Cisco ISE 3.2 EAP-TLS باستخدام Microsoft Azure Active Directory

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين سياسات التخويل في ISE واستكشاف أخطائها وإصلاحها استنادا إلى عضوية Azure AD لمجموعة وسمات المستخدم الأخرى مع EAP-TLS أو TEAP كبروتوكولات مصادقة.

ساهم فيها إيمانويل كانو مهندس الاستشارات المهنية ورومي ميجيشا مهندس الاستشارات الفنية

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات الهوية (ISE)
- Microsoft Azure AD والاشتراك والتطبيقات
- EAP-TLS المصادقة

المكونات المستخدمة

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

- Cisco ISE 3.2
- Microsoft Azure AD

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.

معلومات أساسية

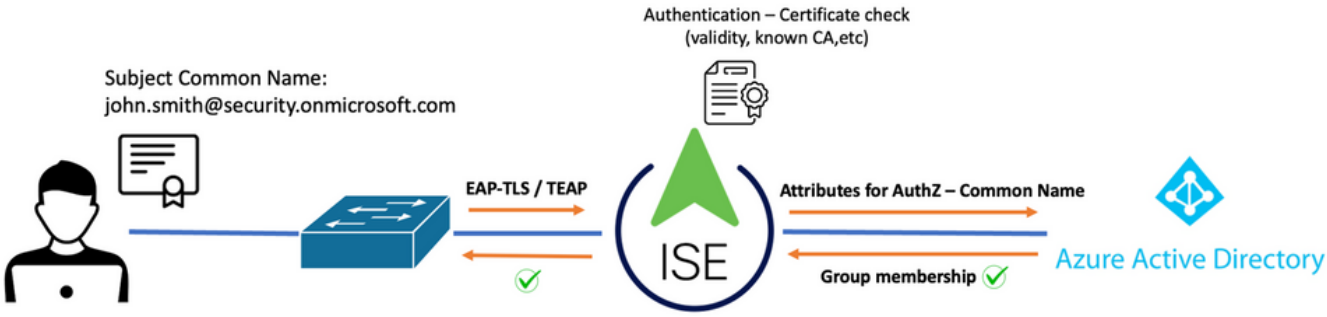
في ISE 3.0، من الممكن الاستفادة من التكامل بين ISE و Azure Active Directory (AAD) لمصادقة المستخدمين استنادا إلى مجموعات Azure AD والسمات من خلال اتصال بيانات اعتماد كلمة مرور مالك المورد (ROPC). باستخدام ISE 3.2، يمكنك تكوين المصادقة المستندة إلى الشهادة ويمكن تخويل المستخدمين استنادا إلى عضوية مجموعة Azure AD والسمات الأخرى. يستعلم ISE Azure through Graph API لجلب مجموعات وسمات للمستخدم الذي تمت مصادقته، فإنه يستخدم اسم الشهادة الشائع (CN) مقابل اسم المستخدم الأساسي (UPN) على جانب Azure.

ملاحظة: يمكن أن تكون المصادقات المستندة إلى الشهادة إما EAP-TLS أو TEAP مع EAP-TLS كطريقة داخلية. بعد ذلك، يمكنك تحديد سمات من Azure Active Directory وإضافتها إلى قاموس Cisco ISE. يمكن إستخدام هذه السمات للتخويل. مصادقة المستخدم فقط هي المدعومة.

التكوين

الرسم التخطيطي للشبكة

توفر الصورة التالية مثال لمخطط الشبكة وتدفق حركة مرور البيانات



التدفق:

1. ترسل الشهادة إلى ISE عبر EAP-TLS أو TEAP وتكون EAP-TLS هي الطريقة الداخلية.
2. يقيم ISE شهادة المستخدم (فترة الصلاحية، CA موثوق به، CRL، وهكذا.)
3. تأخذ ISE اسم موضوع الشهادة (CN) وتقوم بإجراء بحث على واجهة برمجة تطبيقات Microsoft Graph لجلب مجموعات المستخدم وسمات أخرى لذلك المستخدم. ويشار إليه باسم المستخدم الأساسي (UPN) على جانب Azure.
4. يتم تقييم نهج تخويل ISE مقابل سمات المستخدم التي تم إرجاعها من Azure.

ملاحظة: يجب تكوين أذونات واجهة برمجة تطبيقات الرسم البياني ومنحها لتطبيق ISE في Microsoft Azure كما هو موضح أدناه:

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

التكوينات

تكوين ISE

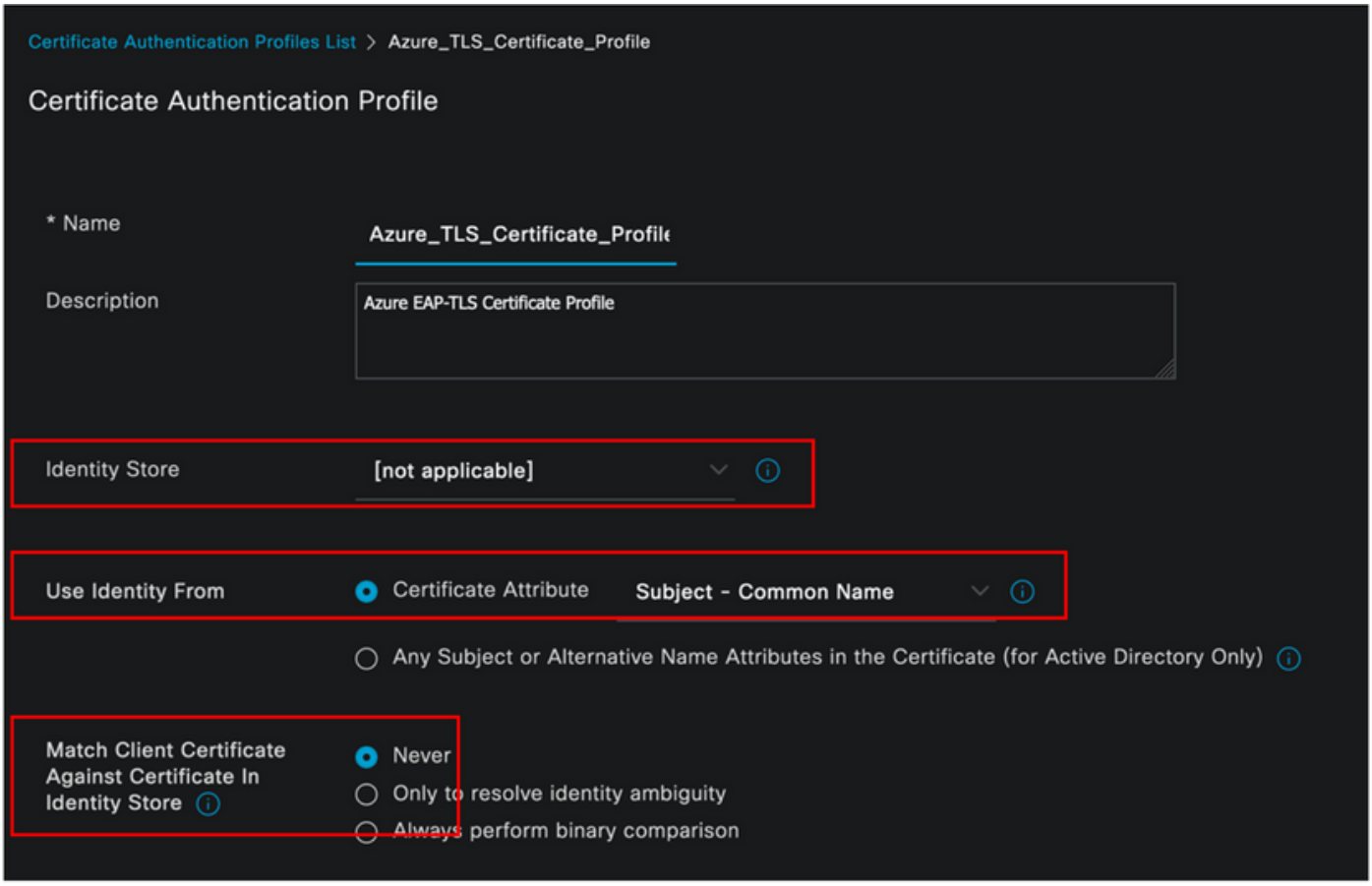
> **ملاحظة**: وظيفة ROPC والدمج بين ISE مع Azure AD خارج نطاق هذا المستند. من المهم أن تتم إضافة المجموعات وسمات المستخدم من Azure. رأيت تشكيل مرشد هنا.

تكوين ملف تعريف مصادقة الشهادة

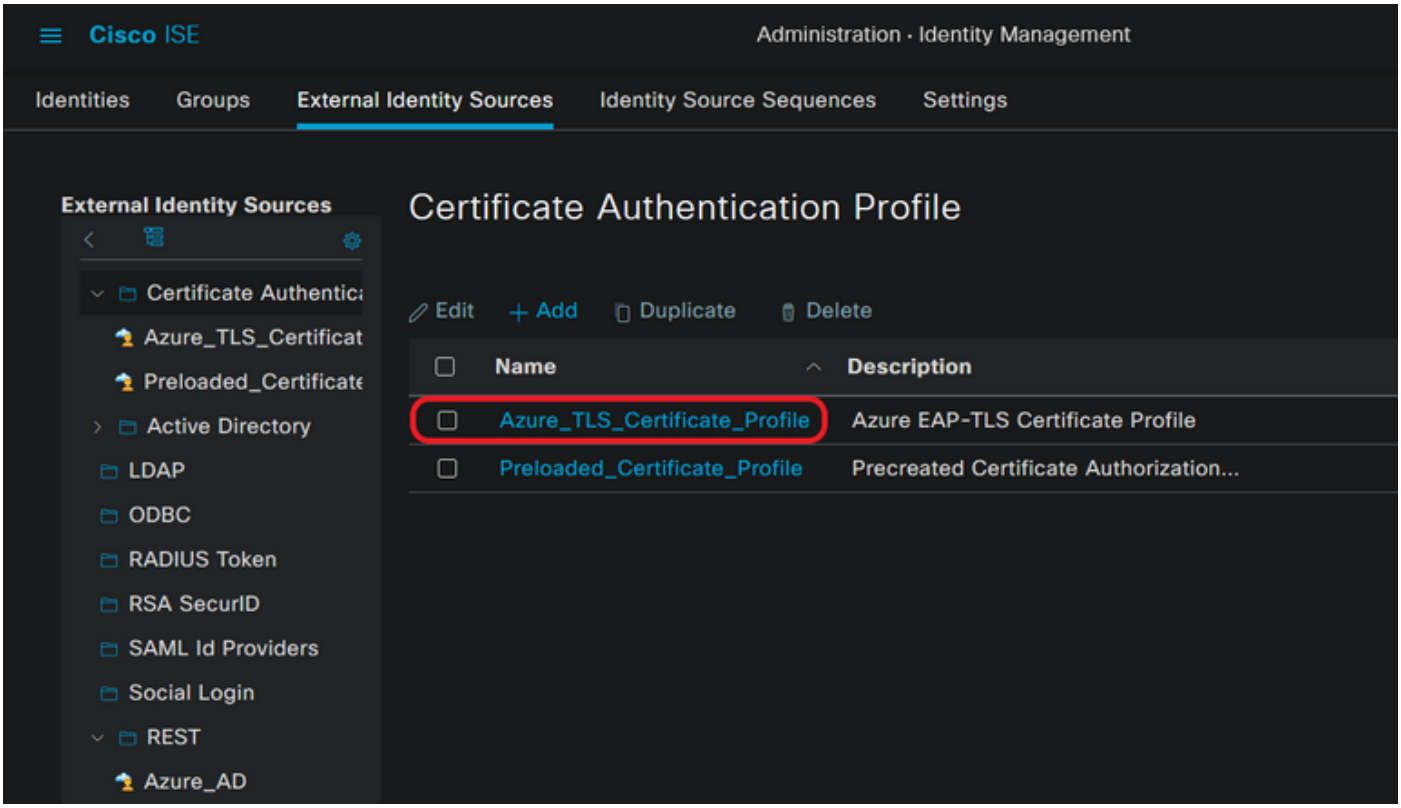
الخطوة 1. انتقل إلى أيقونة القائمة ☰ موجود في الزاوية العلوية اليسرى وحدد **إدارة > إدارة الهوية > مصادر الهوية الخارجية.**

الخطوة 2. تحديد **مصادقة الشهادة** ملف تخصيص ثم انقر على **إضافة.**

الخطوة 3. قم بتعريف الاسم، قم بتعيين **مخزن الهويات** ك [غير قابل للتطبيق]، وحدد موضوع - الاسم الشائع على **استخدام الهوية من** الحقل. تحديد عدم التطابق **شهادة العميل مقابل الشهادة في مخزن الهويات** الحقل.



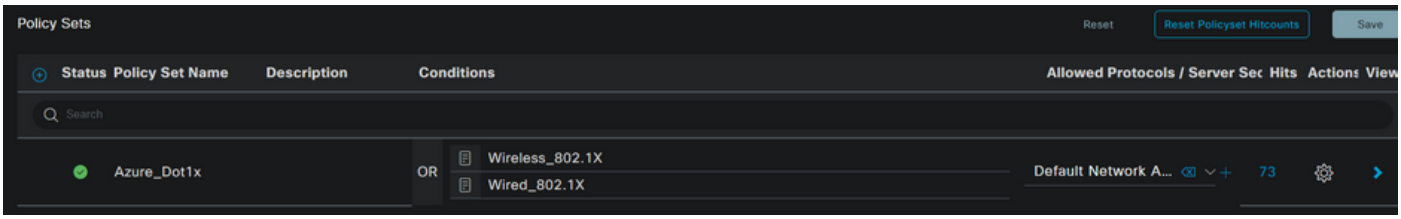
الخطوة 4. انقر فوق **حفظ**



الخطوة 5. انتقل إلى أيقونة القائمة موجود في الزاوية العلوية اليسرى وحدد **السياسة > مجموعات السياسات.**

الخطوة 6. تحديد علامة الجمع أيقونة لإنشاء مجموعة نهج جديدة. قم بتعريف اسم وحدد

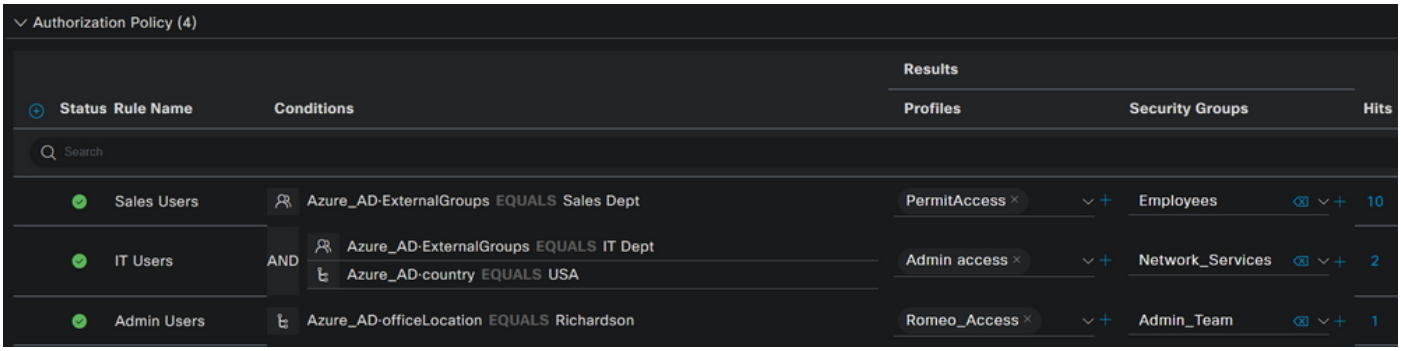
Wireless 802.1x أو 802.1x السلكي كشروط. يتم إستخدام الخيار الافتراضي للوصول إلى الشبكة في هذا المثال



الخطوة 7. حدد السهم التالي إلى الوصول الافتراضي إلى الشبكة لتكوين سياسات المصادقة والتفويض.

الخطوة 8. حدد خيار سياسة المصادقة، وحدد اسم وقم بإضافة EAP-TLS كمصادقة للوصول إلى الشبكة، ومن الممكن إضافة TEAP كمركز وصول إلى الشبكة إذا تم إستخدام TEAP كبروتوكول مصادقة. حدد ملف تعريف مصادقة الشهادة الذي تم إنشاؤه في الخطوة 3 وانقر فوق **حفظ**.

الخطوة 9. حدد خيار "نهج التخويل"، وقم بتحديد اسم وإضافة سمات Azure AD أو سمات المستخدم كشرط. أختر ملف التخصيص أو مجموعة التأمين تحت النتائج، حسب حالة الاستخدام، ثم انقر **حفظ**.



تكوين المستخدم.

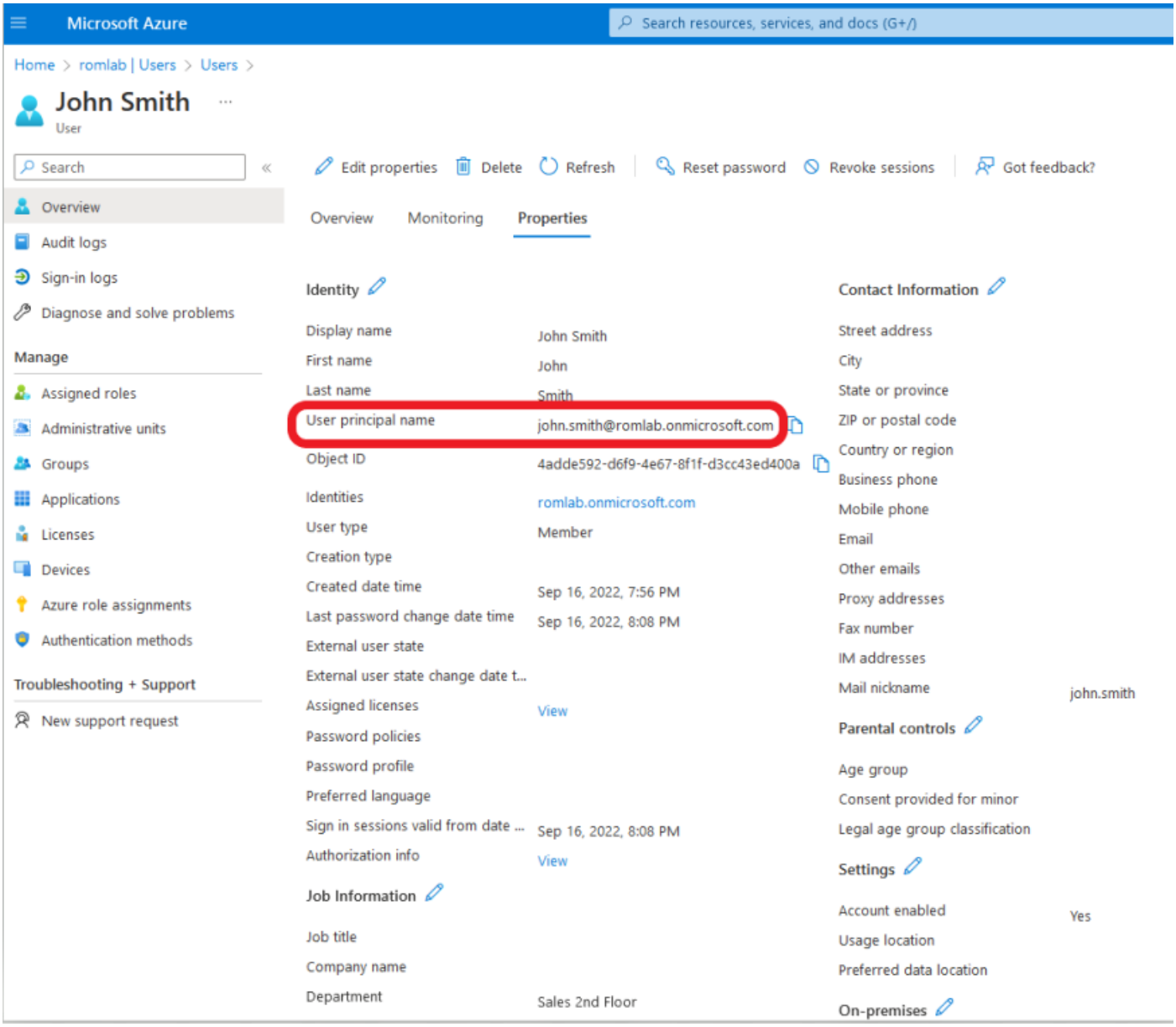
يجب أن يتطابق الاسم الشائع للموضوع (CN) من شهادة المستخدم مع اسم المستخدم الأساسي (UPN) على جانب Azure لاستيراد عضوية مجموعة AD وسمات المستخدم التي يتم إستخدامها في قواعد التخويل. لكي تكون المصادقة ناجحة، يجب أن يكون CA الجذر وأي شهادات CAs وسيطة في مخزن ISE الموثوق به.

john.smith@romlab.onmicrosoft.com
Issued by: romlab-ROMEO-DC-CA
Expires: Sunday, December 17, 2023 at 6:27:52 PM Central Standard Time
This certificate is valid

Trust

Details

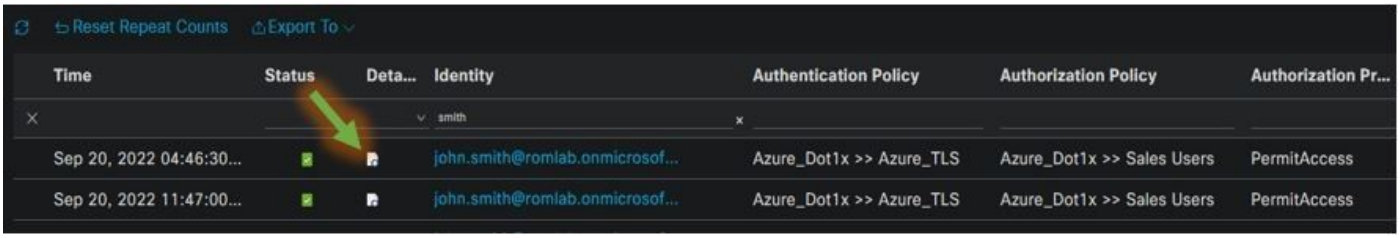
Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01 00 00 00 36
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None



التحقق من الصحة

التحقق من ISE

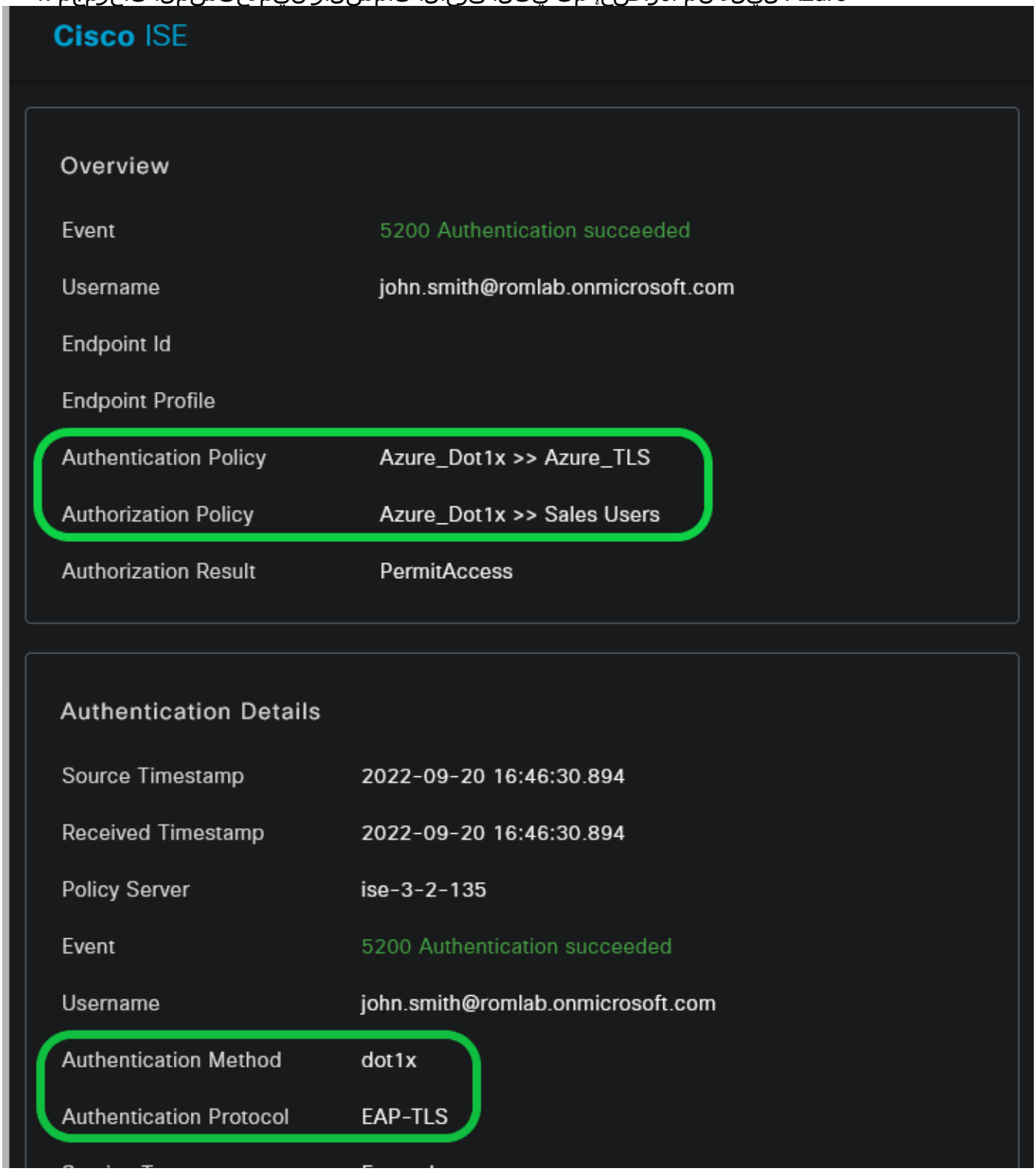
في واجهة المستخدم الرسومية Cisco ISE، انقر فوق رمز القائمة وتختار **العمليات > RADIUS > السجلات المباشرة لمصادقة الشبكة (RADIUS).**

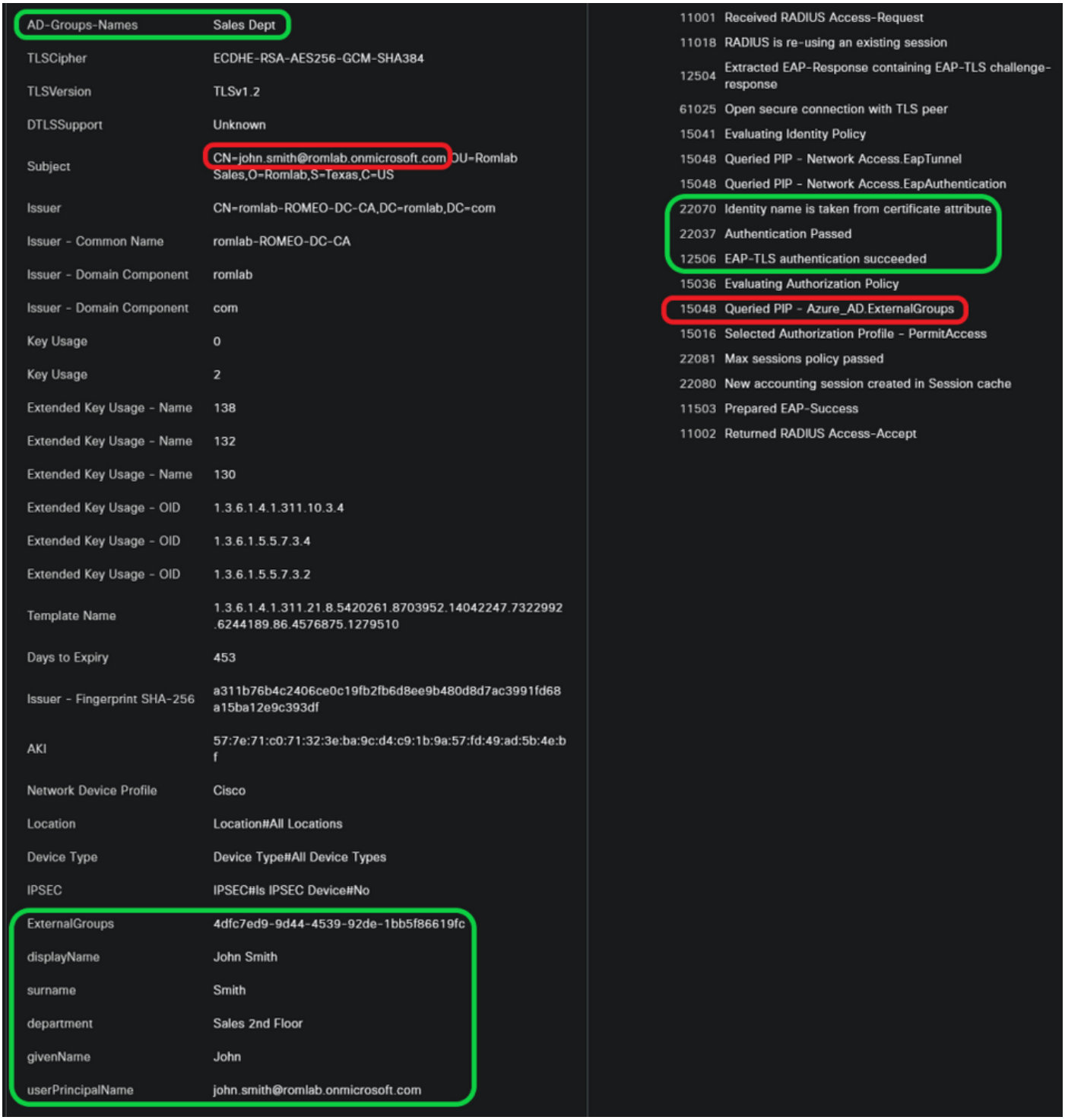


انقر فوق أيقونة المكبر في عمود التفاصيل لعرض تقرير مصادقة مفصل وتأكيد ما إذا كان التدفق يعمل كما هو متوقع.

1. التحقق من سياسات المصادقة/التفويض
2. أسلوب/بروتوكول المصادقة

3. اسم موضوع المستخدم مأخوذ من الشهادة
4. مجموعات المستخدمين والسمات الأخرى التي تم إحضارها من دليل Azure





استكشاف الأخطاء وإصلاحها

تمكين تصحيح الأخطاء على ISE

انتقل إلى **الإدارة > النظام > التسجيل > تكوين سجل التصحيح** لتعيين المكونات التالية إلى المستوى المحدد.

عقدة	اسم المكون	مستوى التسجيل	اسم ملف السجل
PSN	حفظ-معرف المخزن	تصحيح الأخطاء	rest-id-store.log
PSN	Runtime-AAA	تصحيح الأخطاء	prrt-server.log

ملاحظة: عند الانتهاء من أستكشاف الأخطاء وإصلاحها، تذكر إعادة تعيين تصحيح الأخطاء. للقيام بذلك، حدد العقدة ذات الصلة وانقر فوق "إعادة التعيين إلى

الافتراضي".

قصاصات السجلات

تظهر المقتطفات التالية المرحلتين الأخيرتين في التدفق، كما هو مذكور سابقا في قسم الرسم التخطيطي للشبكة.

1. تأخذ ISE اسم موضوع الشهادة (CN) وتقوم بعمل بحث على API الخاص برسم Azure البياني لجلب مجموعات المستخدمين وسمات أخرى لذلك المستخدم. ويشار إليه باسم المستخدم الأساسي (UPN) على جانب Azure.
2. يتم تقييم نهج تخويل ISE مقابل سمات المستخدم التي تم إرجاعها من Azure.

سجلات معرف الرامز:

```
2022-09-20 16:46:30,424 INFO  [http-nio-9601-exec-10] cisco.ise.ropc.controllers.ClientCredController -::- UPN:
john.smith@romlab.onmicrosoft.com , RestIdStoreName: Azure_AD, Attrname: ExternalGroups,city,companyName,country,department,
displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,424 DEBUG [http-nio-9601-exec-10]ise.ropc.providers.cache.IdpKeyValueCacheInitializer -::::- Found access token

2022-09-20 16:46:30,424 DEBUG [http-nio-9601-exec-10] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- User Lookup by UPN
john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,425 DEBUG [http-nio-9601-exec-10]ise.ropc.providers.azure.AzureIdentityProviderFacade -::- Lookup url
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com?$select=ExternalGroups,city,companyName,country,depart
ment,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,425 DEBUG [http-nio-9601-exec-10]cisco.ise.ropc.utilities.HttpClientWrapper -::- Start building http client for uri
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com?$select=ExternalGroups
,city,companyName,country,department,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,660 DEBUG [http-nio-9601-exec-10] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- UserAttribute size 11

2022-09-20 16:46:30,661 DEBUG [http-nio-9601-exec-10] cisco.ise.ropc.utilities.HttpClientWrapper -::- Start building http client for uri
https://graph.microsoft.com/v1.0/users/john.smith@romlab.onmicrosoft.com/transitiveMemberOf/microsoft.graph.group

2022-09-20 16:46:30,876 DEBUG [http-nio-9601-exec-10][[]] ise.ropc.providers.azure.AzureIdentityProviderFacade -::- UserGroups size 1
```

سجلات المنتج:

2022-09-20 16:46:30,182 DEBUG [Thread-759][[]] cisco.cpm.prrt.impl.PrRTCpmBridge -::::- ---- Running Authorization Policy ----

2022-09-20 16:46:30,252 DEBUG [Thread-759][[]] cisco.cpm.prrt.impl.PrRTCpmBridge -::::- setting sessionCache attribute CERTIFICATE.Subject - Common Name to john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,253 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- [RestIdentityProviderPIP] has been called by PIP manager: dictName: Azure_AD attrName: Azure_AD.ExternalGroups context: NonStringifiableExecutionContext inputs:

2022-09-20 16:46:30,408 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- checking attrList ExternalGroups,city,companyName,country,department,displayName,employeeId,givenName,officeLocation,state,surname,userPrincipalName

2022-09-20 16:46:30,408 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- Username from the Context john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,880 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr size 11
...
2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr update in context & map, Key : Azure_AD.department value Sales 2nd Floor

2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr update in context & map, Key : Azure_AD.displayName value John Smith
2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr update in context & map, Key : Azure_AD.givenName value John
2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr update in context & map, Key : Azure_AD.surname value Smith

2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userAttr update in context & map, Key : Azure_AD.userPrincipalName value john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,881 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- userGroup 1

2022-09-20 16:46:30,882 DEBUG [Thread-759][[]] cisco.cpm.prrt.pip.RestIdentityProviderPIP -::::- Group value 4dfc7ed9-9d44-4539-92de-1bb5f86619fc group name Sales Dept

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).