Konfigurieren von Cisco ISE 3.2 EAP-TLS mit Microsoft Azure Active Directory

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Autorisierungsrichtlinien in ISE auf der Grundlage der Azure AD-Gruppenmitgliedschaft und anderer Benutzerattribute mit EAP-TLS oder TEAP als Authentifizierungsprotokolle konfigurieren und Fehler in diesen Richtlinien beheben.

Beitrag von Emmanuel Cano, Security Consulting Engineer, und Romeo Migisha, Technical Consulting Engineer

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- Microsoft Azure AD, Abonnement und Apps
- EAP-TLS authentifizierung

Verwendete Komponenten

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

- Cisco ISE 3.2
- Microsoft Azure AD

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 verstehen.

Hintergrundinformationen

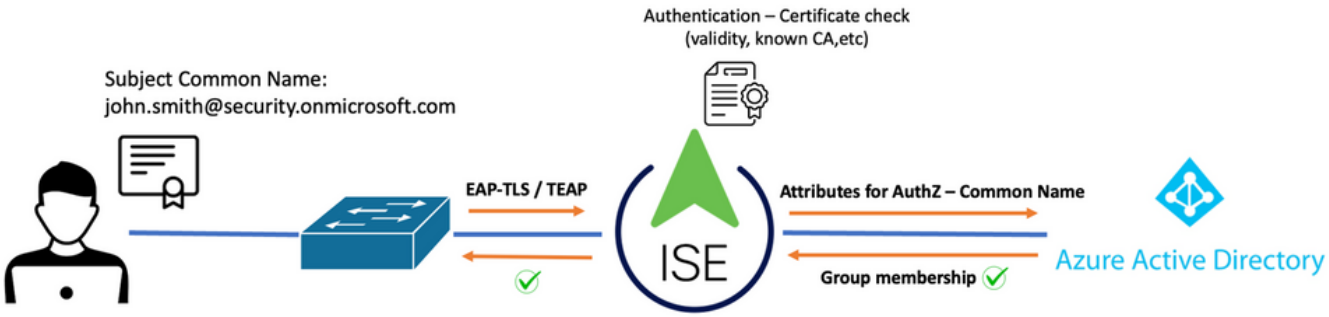
In ISE 3.0 ist es möglich, die Integration zwischen ISE und Azure Active Directory (AAD) zu nutzen, um die Benutzer basierend auf Azure AD-Gruppen und -Attributen über die ROPC-Kommunikation (Resource Owner Password Credentials) zu authentifizieren. Mit ISE 3.2 können Sie eine zertifikatbasierte Authentifizierung konfigurieren, und Benutzer können basierend auf Azure AD-Gruppenmitgliedschaften und anderen Attributen autorisiert werden. ISE fragt Azure über eine Grafik-API ab, um Gruppen und Attribute für den authentifizierten Benutzer abzurufen. Dabei wird der Common Name (CN) des Zertifikats mit dem UPN (User Principal Name) auf Azure-Seite verglichen.

> **Hinweis**: Bei den zertifikatbasierten Authentifizierungen kann es sich entweder um EAP-TLS oder um TEAP mit EAP-TLS als interner Methode handeln. Anschließend können Sie Attribute aus Azure Active Directory auswählen und sie dem Cisco ISE-Wörterbuch hinzufügen. Diese Attribute können für die Autorisierung verwendet werden. Nur die Benutzerauthentifizierung wird unterstützt.

Konfigurieren

Netzwerkdiagramm

Das nächste Bild zeigt ein Netzwerkdiagramm und einen Verkehrsfluss.



Vorgehensweise:

1. Das Zertifikat wird über EAP-TLS oder TEAP mit EAP-TLS als interner Methode an die ISE gesendet.
2. Die ISE wertet das Zertifikat des Benutzers aus (Gültigkeitsdauer, vertrauenswürdige Zertifizierungsstelle, Zertifikatsperrliste usw.).
3. Die ISE sucht anhand des Zertifikatssubjektnamens (CN) nach der Microsoft Graph-API, um die Benutzergruppen und andere Attribute für diesen Benutzer abzurufen. Dies wird auf der Azure-Seite als Benutzerprinzipalname (User Principal Name, UPN) bezeichnet.
4. ISE-Autorisierungsrichtlinien werden anhand der von Azure zurückgegebenen Benutzerattribute ausgewertet.

> **Hinweis**: Sie müssen die Graph API-Berechtigungen für die ISE-App in Microsoft Azure konfigurieren und erteilen, wie unten gezeigt:

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

Konfigurationen

ISE-Konfiguration

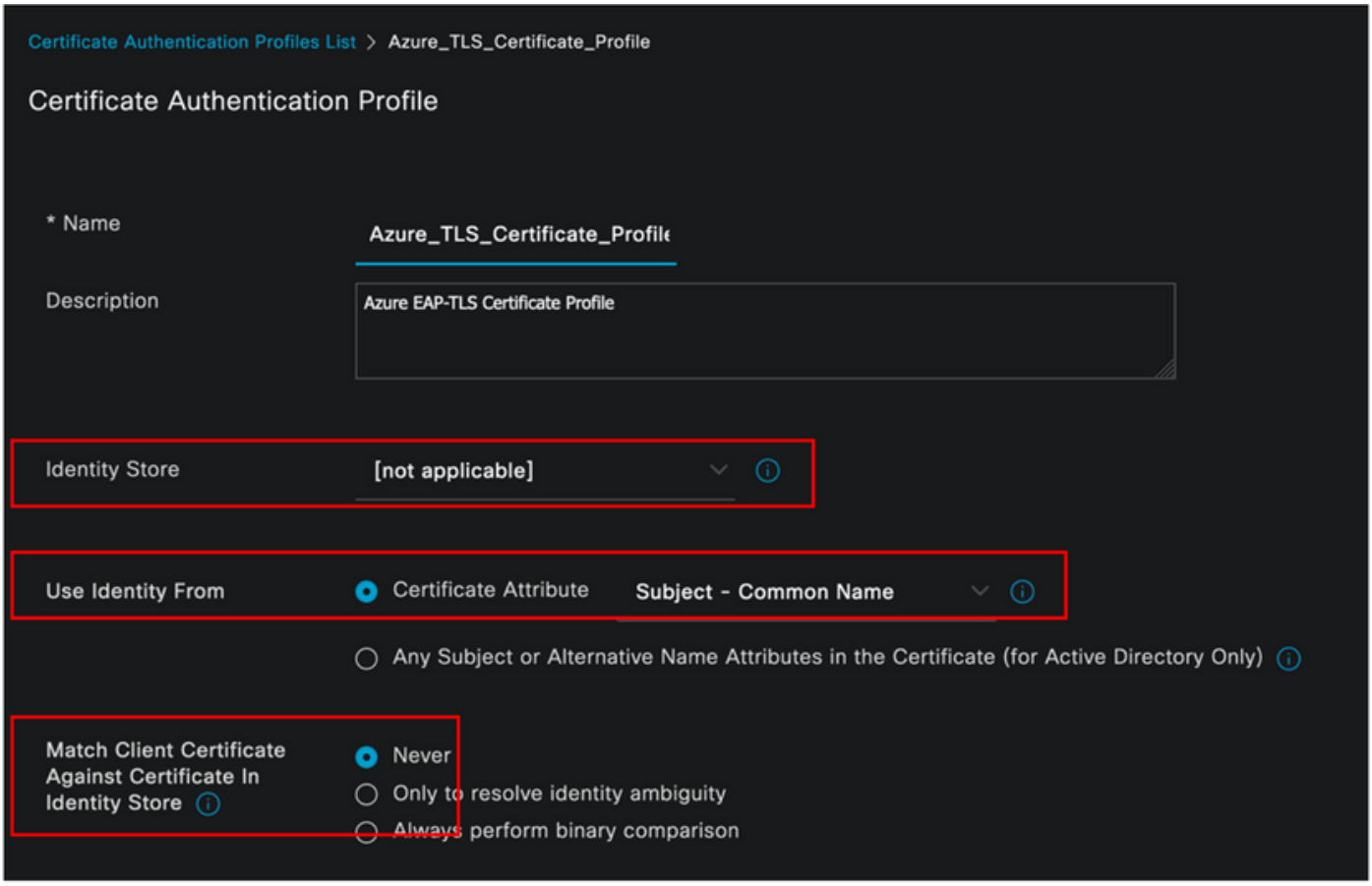
> **Hinweis**: Die ROPC-Funktionalität und die Integration zwischen der ISE und Azure AD werden in diesem Dokument nicht behandelt. Es ist wichtig, dass Gruppen und Benutzerattribute von Azure hinzugefügt werden. Siehe Konfigurationsleitfaden hier.

Konfigurieren des Zertifikatauthentifizierungsprofils

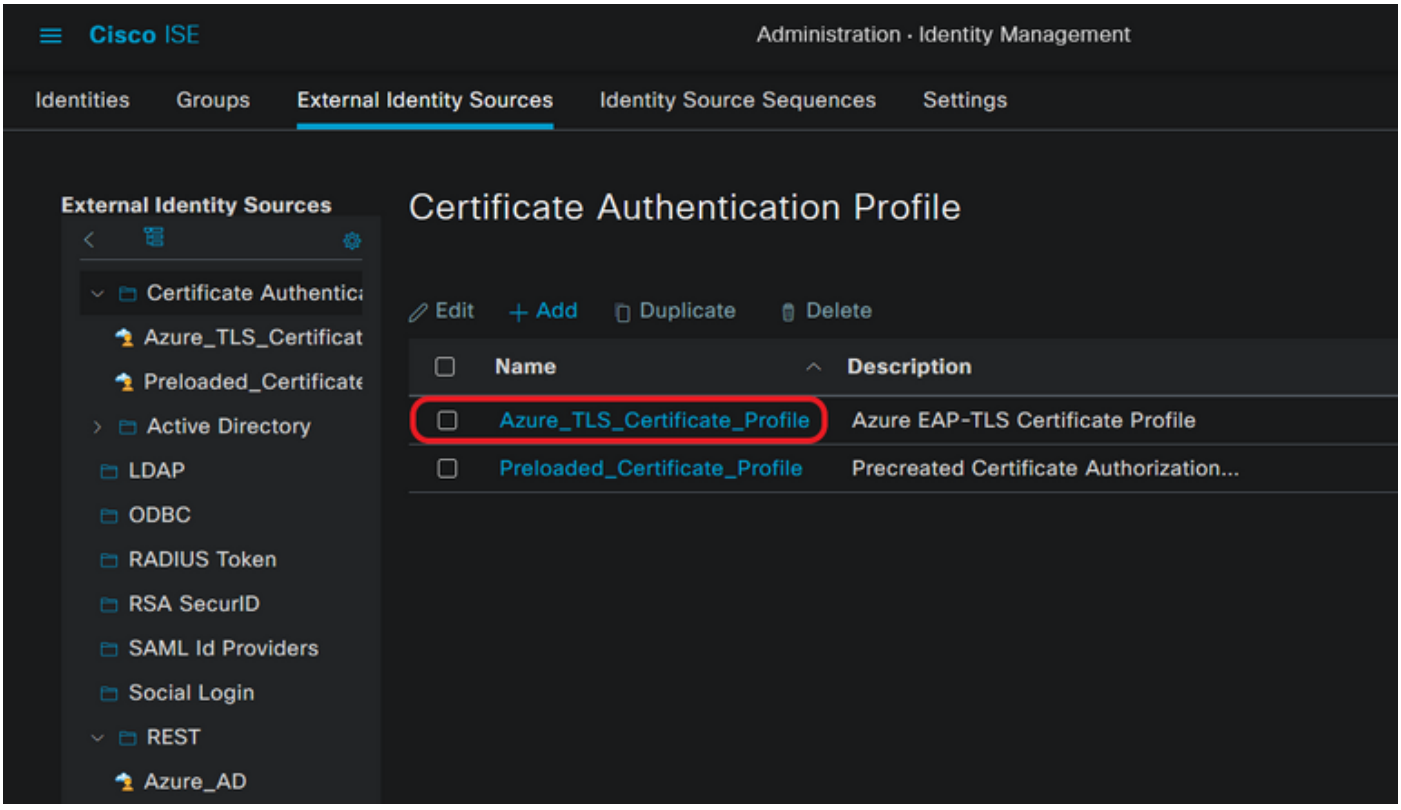
Schritt 1: Navigieren Sie zu das Menü-Symbol in der linken oberen Ecke befindet, und wählen Sie **Administration > Identity Management > Externe Identitätsquellen.**

Schritt 2: Auswählen **Authentifizierung von Zertifikaten** Profil erstellen und dann auf klicken **Hinzufügen**

Schritt 3: Definieren Sie den Namen, legen Sie den **Identitätsspeicher** als [Nicht zutreffend] aus, und wählen Sie Subject - Common Name on **Identität verwenden von** feld. Nie zuordnen auswählen **Clientzertifikat für Zertifikat im Identitätsspeicher** Feld.



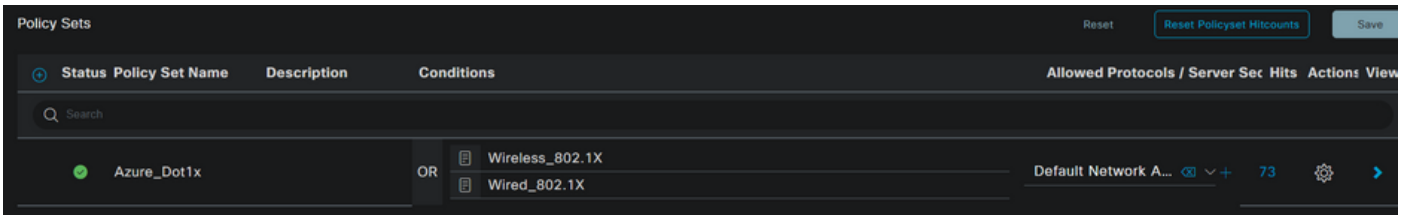
Schritt 4: Klicken Sie **Speichern**



Schritt 5: Navigieren Sie zu das Menü-Symbol in der linken oberen Ecke befindet, und wählen Sie **Richtlinie > Richtliniensätze.**

Schritt 6: Wählen Sie das Plus um einen neuen Richtliniensatz zu erstellen. Definieren Sie

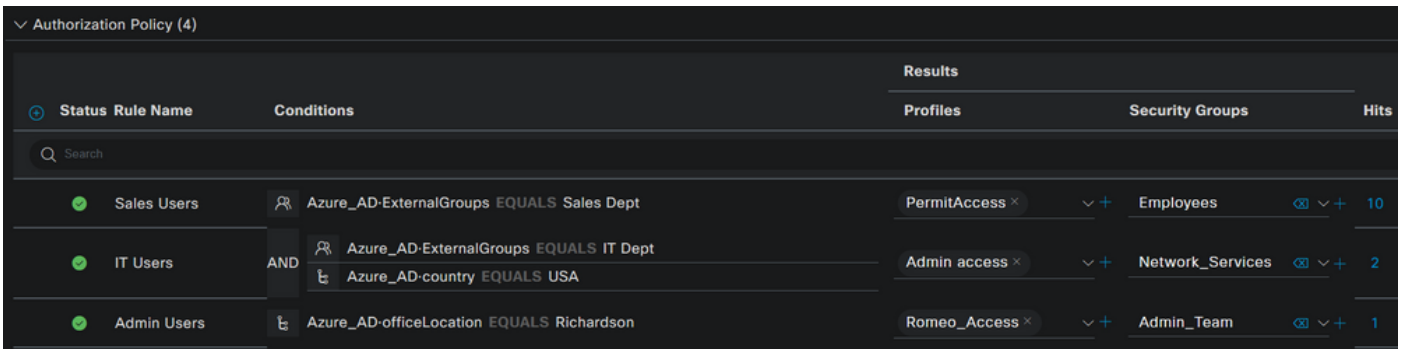
einen Namen, und wählen Sie als Bedingungen Wireless 802.1x oder kabelgebundene 802.1x-Verbindungen aus. In diesem Beispiel wird die Option Default Network Access (Standard-Netzwerkzugriff) verwendet



Schritt 7. Pfeil auswählen neben Standard-Netzwerkzugriff, um Authentifizierungs- und Autorisierungsrichtlinien zu konfigurieren.

Schritt 8: Wählen Sie die Authentifizierungsrichtlinie Option, definieren Sie einen Namen und fügen Sie EAP-TLS als Network Access EAPAuthentication, es ist möglich, TEAP als Network Access EAPTunnel hinzuzufügen, wenn TEAP als Authentifizierungsprotokoll verwendet wird. Wählen Sie das in Schritt 3 erstellte Zertifikatauthentifizierungsprofil aus, und klicken Sie auf **Speichern**.

Schritt 9. Wählen Sie die Option Autorisierungsrichtlinie aus, definieren Sie einen Namen, und fügen Sie Azure AD-Gruppen- oder Benutzerattribute als Bedingung hinzu. Wählen Sie das Profil oder die Sicherheitsgruppe unter "Ergebnisse" aus, hängt vom Anwendungsfall ab, und klicken Sie dann auf **Speichern**.



Benutzerkonfiguration.

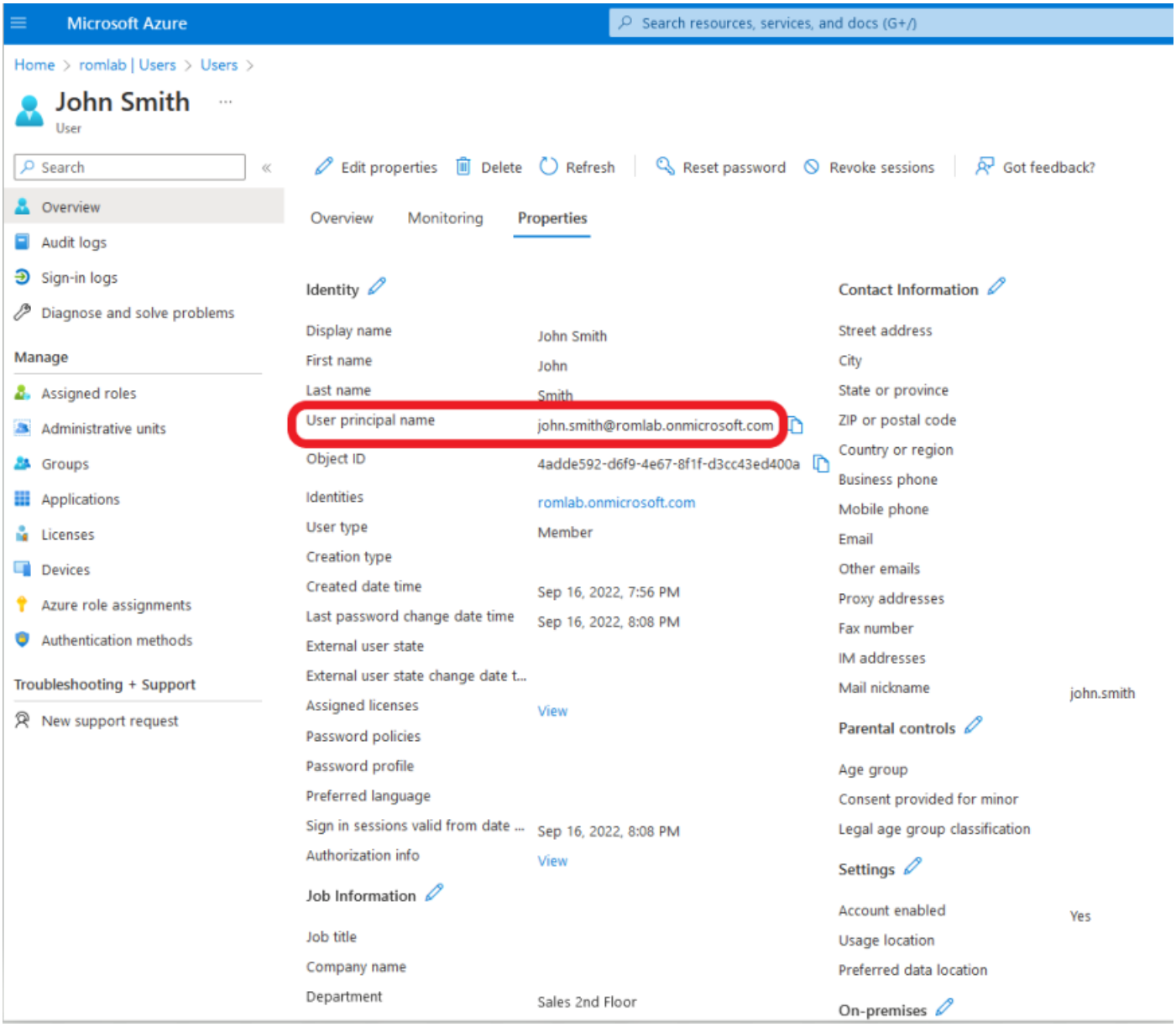
Der Common Name (CN) des Antragstellers aus dem Benutzerzertifikat muss mit dem UPN (User Principal Name) auf Azure-Seite übereinstimmen, damit die AD-Gruppenmitgliedschaft und die Benutzerattribute abgerufen werden können, die in Autorisierungsregeln verwendet werden. Damit die Authentifizierung erfolgreich ist, müssen sich die Stammzertifizierungsstelle und alle zwischengeschalteten Zertifizierungsstellenzertifikate im vertrauenswürdigen ISE-Speicher befinden.

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

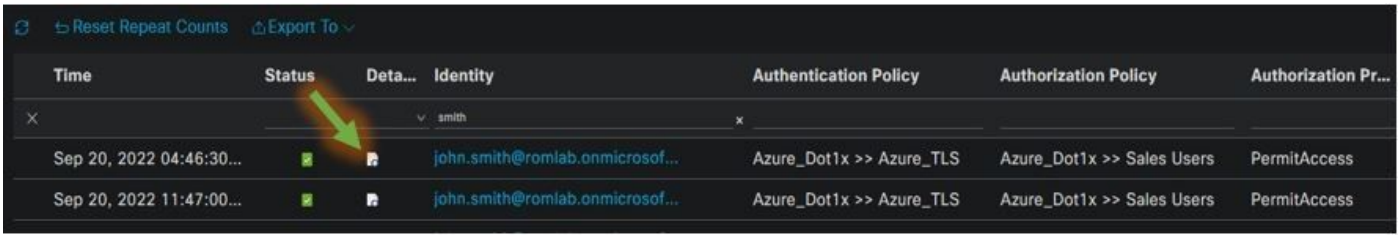
Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01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



Überprüfung

ISE-Verifizierung

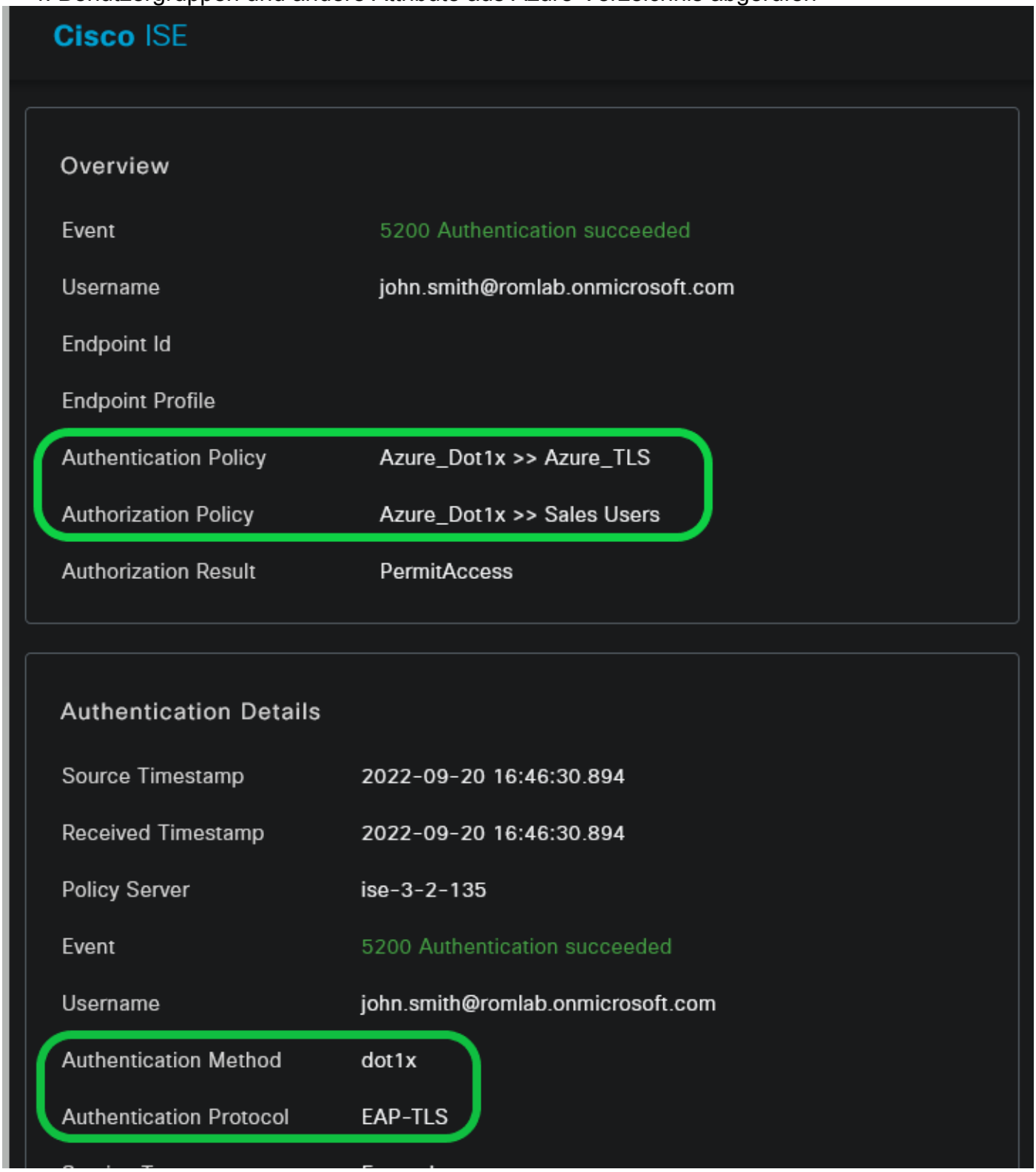
Klicken Sie in der Cisco ISE-GUI auf das Menü-Symbol und wählen **Vorgänge > RADIUS > Live-Protokolle für Netzwerkauthentifizierungen (RADIUS).**

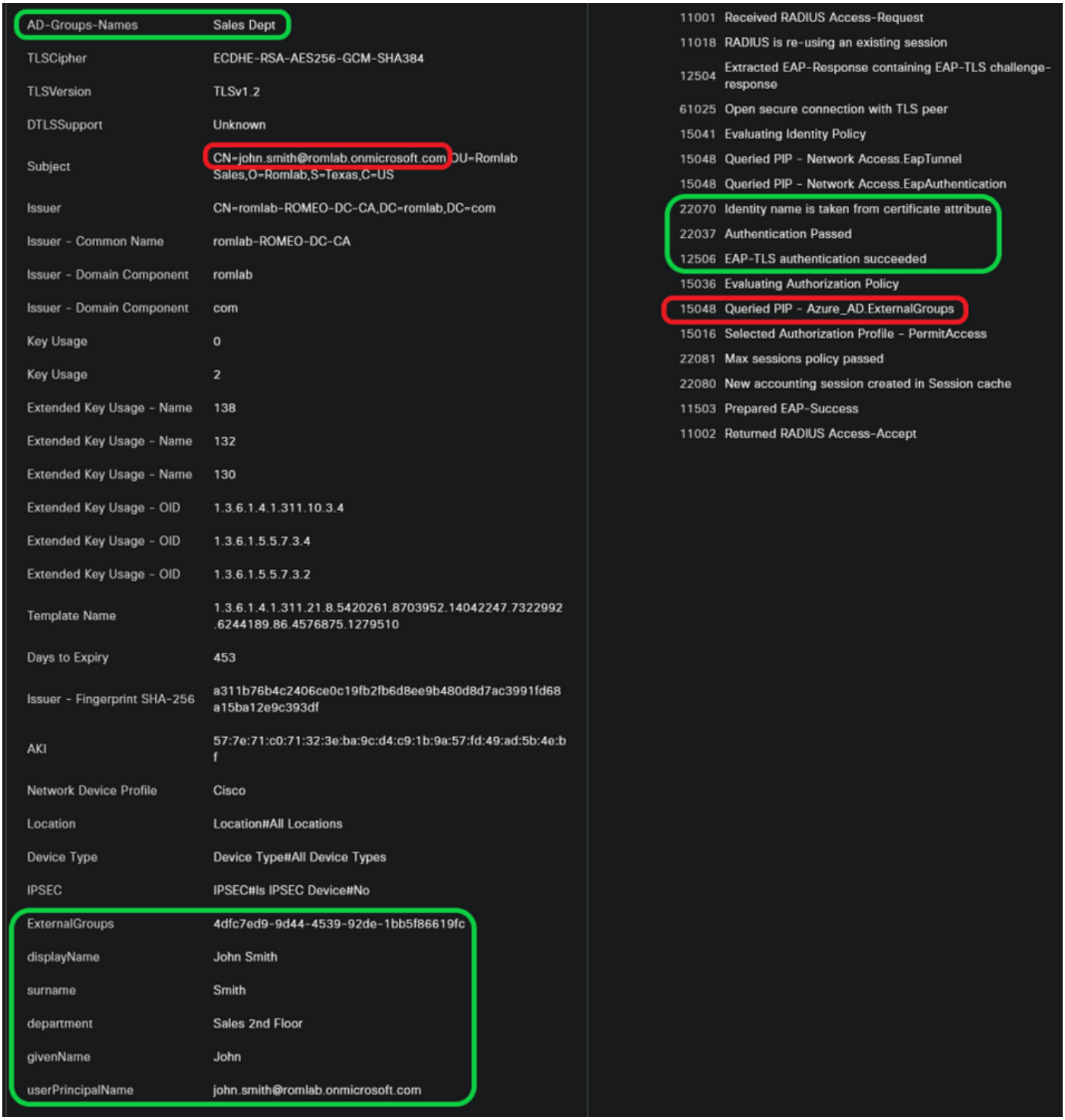


Klicken Sie in der Spalte "Details" auf das Lupensymbol, um einen detaillierten Authentifizierungsbericht anzuzeigen und zu überprüfen, ob der Fluss wie erwartet funktioniert.

1. Überprüfen von Authentifizierungs-/Autorisierungsrichtlinien
2. Authentifizierungsmethode/Protokoll

3. Dem Zertifikat entnommener Benutzername
4. Benutzergruppen und andere Attribute aus Azure-Verzeichnis abgerufen





Fehlerbehebung

Debuggen auf ISE aktivieren

Navigieren Sie zu **Administration > System > Protokollierung > Konfiguration des Debug-Protokolls** , um die nächsten Komponenten auf die angegebene Ebene zu setzen.

Knoten	Komponentenname	Protokollstufe	Protokolldateiname
PSN	Ruhestandslager	Fehlersuche	rest-id-store.log
PSN	Laufzeit-AAA	Fehlersuche	prrt-server.log

> **Hinweis**: Wenn Sie mit der Fehlerbehebung fertig sind, sollten Sie die Fehlerbehebungen zurücksetzen. Wählen Sie dazu den entsprechenden Knoten aus und klicken Sie auf "Reset

to Default".

Protokolle Ausschnitte

Die nächsten Auszüge zeigen die letzten beiden Phasen im Fluss, die bereits im Netzwerkdiagrammabschnitt erwähnt wurden.

1. ISE verwendet den Zertifikatssubjektnamen (CN) und führt eine Suche in der Azure Graph-API durch, um Benutzergruppen und andere Attribute für diesen Benutzer abzurufen. Dies wird auf Azure-Seite als Benutzerprinzipalname (UPN) bezeichnet.
2. ISE-Autorisierungsrichtlinien werden anhand der von Azure zurückgegebenen Benutzerattribute ausgewertet.

REST-ID-Protokolle:

```
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
```

Port-Protokolle:

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

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.