Configuration d'ISE 3.2 EAP-TLS avec Microsoft Azure Active Directory

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Procédure
  - Configurations
    - Configuration ISE
    - Configurer le profil d'authentification du certificat
    - Configuration utilisateur
- Vérifier
  - Vérification ISE
- Dépannage
  - Activer les débogages sur ISE
  - Extraits de journal

Introduction

Ce document décrit comment configurer et dépanner des stratégies d'autorisation dans ISE en fonction de l'appartenance au groupe Azure AD avec EAP-TLS ou TEAP.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Moteur du service de vérification des identités (ISE)
- Microsoft Azure AD, abonnement et applications
- authentification EAP-TLS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE 3.2
- Microsoft Azure AD

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

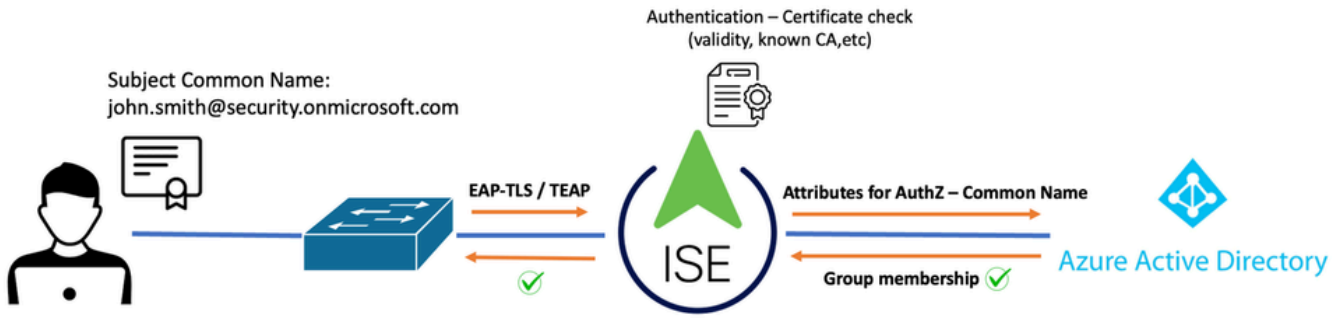
Dans ISE 3.0, il est possible de tirer parti de l'intégration entre ISE et Azure Active Directory (AAD) pour authentifier les utilisateurs en fonction des groupes et attributs Azure AD via la communication ROPC (Resource Owner Password Credentials). Avec ISE 3.2, vous pouvez configurer l'authentification basée sur les certificats et les utilisateurs peuvent être autorisés en fonction des appartenances aux groupes Azure AD et d'autres attributs. ISE interroge Azure via l'API graphique pour récupérer des groupes et des attributs pour l'utilisateur authentifié. Il utilise le nom commun de l'objet (CN) du certificat par rapport au nom principal de l'utilisateur (UPN) côté Azure.

Remarque : Les authentifications basées sur les certificats peuvent être EAP-TLS ou TEAP avec EAP-TLS comme méthode interne. Vous pouvez ensuite sélectionner des attributs dans Azure Active Directory et les ajouter au dictionnaire Cisco ISE. Ces attributs peuvent être utilisés pour l'autorisation. Seule l'authentification utilisateur est prise en charge.

Configurer

Diagramme du réseau

L'image suivante fournit un exemple de schéma de réseau et de flux de trafic :



Procédure

1. Le certificat est envoyé à ISE via EAP-TLS ou TEAP avec EAP-TLS comme méthode interne.
2. ISE évalue le certificat de l'utilisateur (période de validité, CA approuvée, CRL, etc.).
3. ISE prend le nom de sujet du certificat (CN) et effectue une recherche dans l'API Microsoft

Graph pour récupérer les groupes et autres attributs de l'utilisateur. Il s'agit du nom d'utilisateur principal (UPN) côté Azure.

4. Les stratégies d'autorisation ISE sont évaluées par rapport aux attributs de l'utilisateur renvoyés par Azure.

Remarque : Vous devez configurer et accorder les autorisations de l'API Graph à l'application ISE dans Microsoft Azure, comme indiqué ci-dessous :

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

Configurations

Configuration ISE

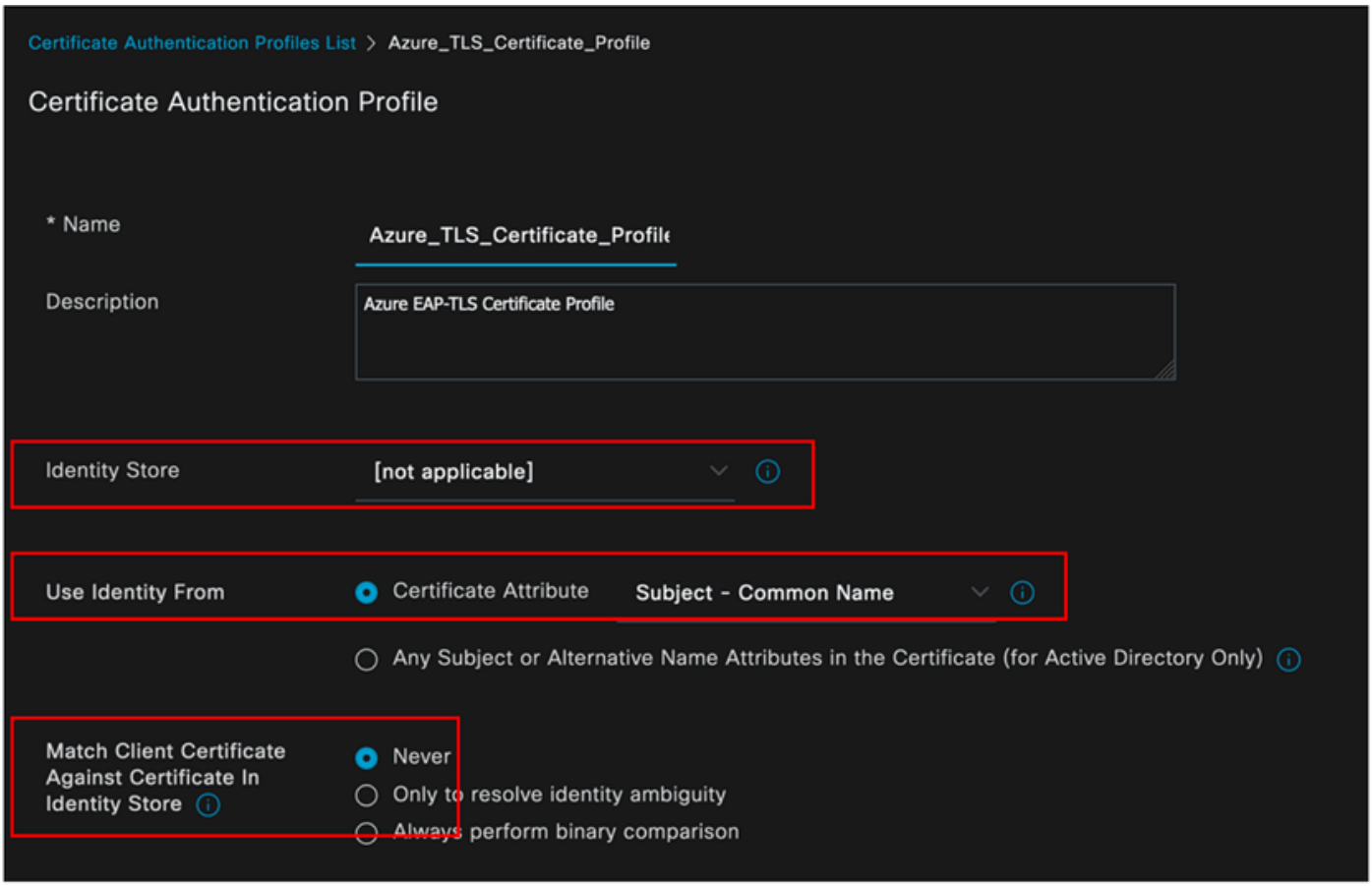
Remarque : La fonctionnalité ROPC et l'intégration entre ISE et Azure AD ne sont pas abordées dans ce document. Il est important que les groupes et les attributs d'utilisateur soient ajoutés à partir d'Azure. Reportez-vous au guide de configuration.

Configurer le profil d'authentification du certificat

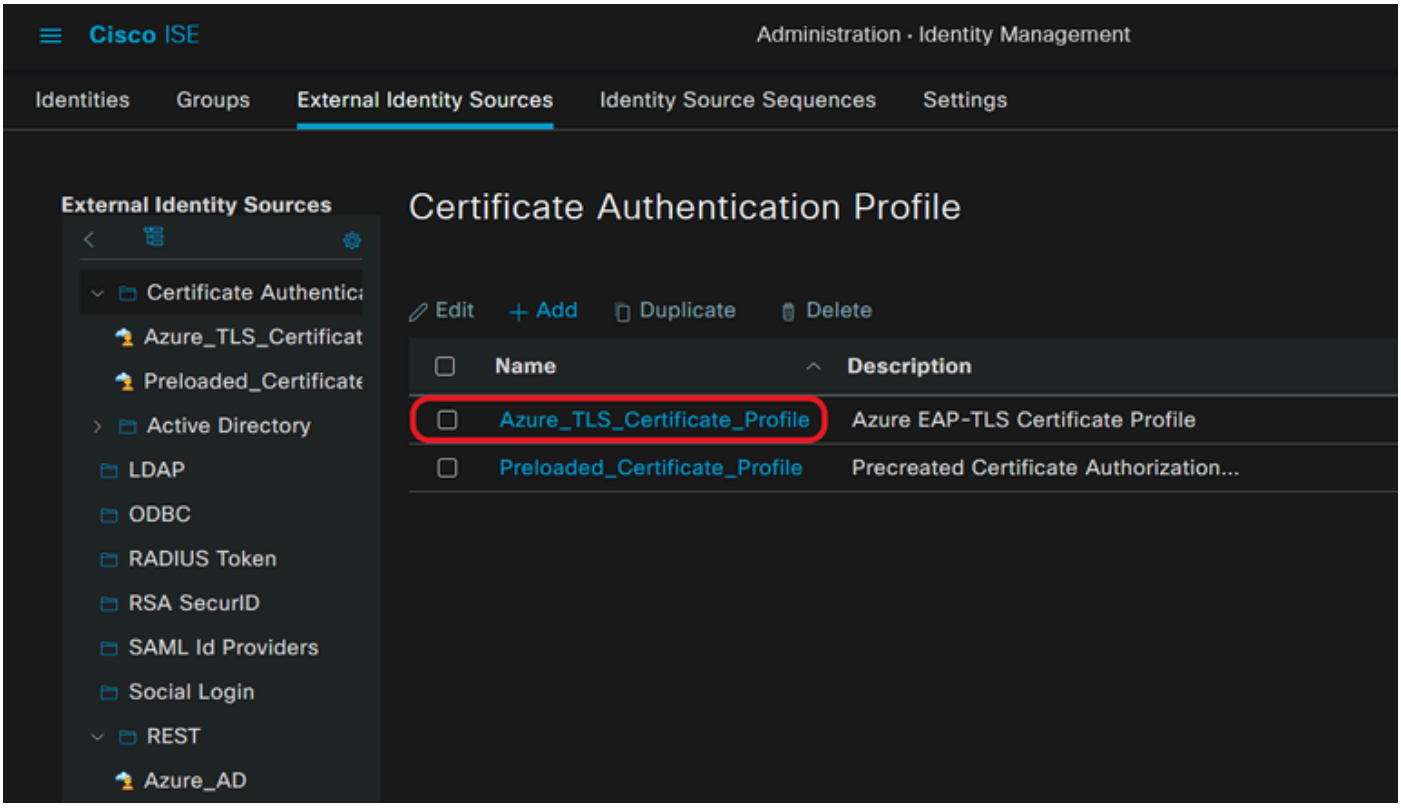
Étape 1. Accédez à l'icône Menu ☰ situé dans le coin supérieur gauche et sélectionnez Administration > Identity Management > External Identity sources.

Étape 2. Sélectionnez Certificate Authentication Profile, puis cliquez sur Add.

Étape 3 : définition du nom Définissez le magasin d'identités sur [Sans objet], puis sélectionnez Objet - Nom commun dans le champ Utiliser l'identité de. Sélectionnez Ne jamais faire correspondre le certificat client au certificat dans le champ Magasin d'identités.

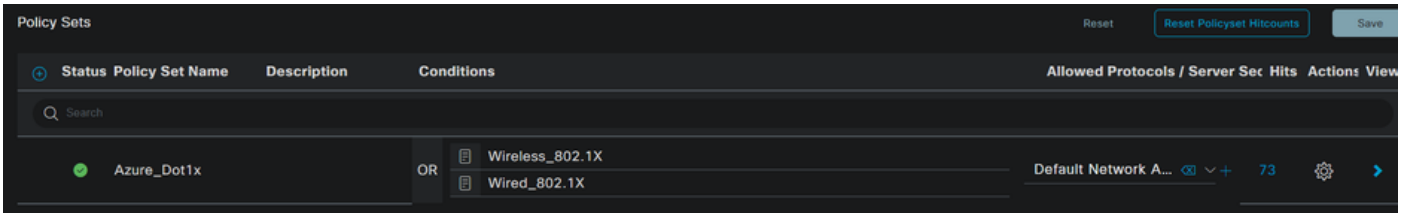


Étape 4. Cliquez sur Save :



Étape 5. Accédez à l'icône Menu dans l'angle supérieur gauche et sélectionnez Policy > Policy Sets.

Étape 6. Sélectionnez le signe plus pour créer un nouvel ensemble de stratégies. Définissez un nom et sélectionnez Wireless 802.1x (Sans fil 802.1x) ou wired 802.1x (Filaire 802.1x) comme conditions. L'option Accès réseau par défaut est utilisée dans cet exemple :

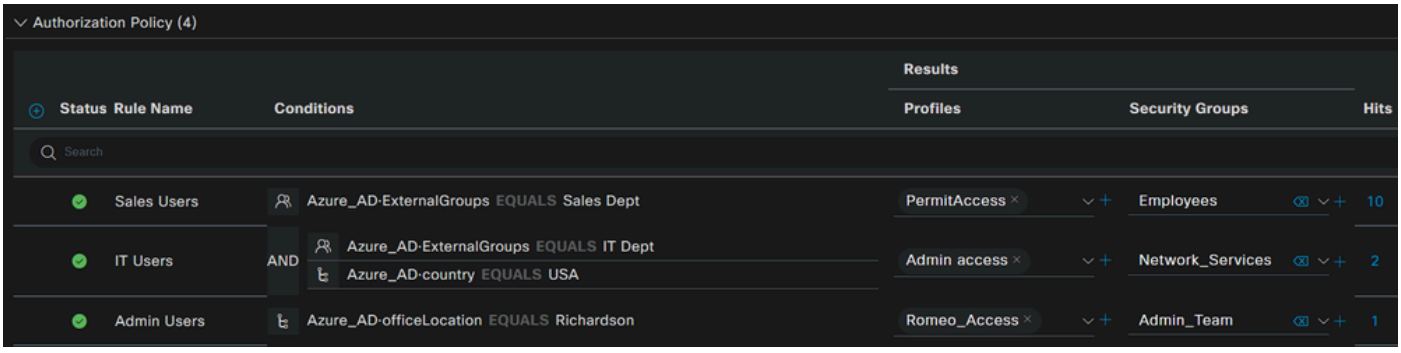


Étape 7. Sélectionnez la flèche en regard de Default Network Access pour configurer les stratégies d'authentification et d'autorisation.

Étape 8. Sélectionnez l'option Authentication Policy, définissez un nom et ajoutez EAP-TLS comme Network Access EAPAuthentication. Il est possible d'ajouter TEAP comme Network Access EAPTunnel si TEAP est utilisé comme protocole d'authentification. Sélectionnez le profil d'authentification de certificat créé à l'étape 3 et cliquez sur Enregistrer.



Étape 9. Sélectionnez l'option Stratégie d'autorisation, définissez un nom et ajoutez des attributs de groupe ou d'utilisateur Azure AD comme condition. Choisissez le profil ou le groupe de sécurité sous Résultats, selon le cas d'utilisation, puis cliquez sur Enregistrer.



Configuration utilisateur

Le nom commun d'objet (CN) du certificat d'utilisateur doit correspondre au nom principal d'utilisateur (UPN) côté Azure afin de récupérer l'appartenance au groupe AD et les attributs d'utilisateur qui seront utilisés dans les règles d'autorisation. Pour que l'authentification réussisse, l'autorité de certification racine et tous les certificats d'autorités de certification intermédiaires doivent se trouver dans le magasin de confiance ISE.

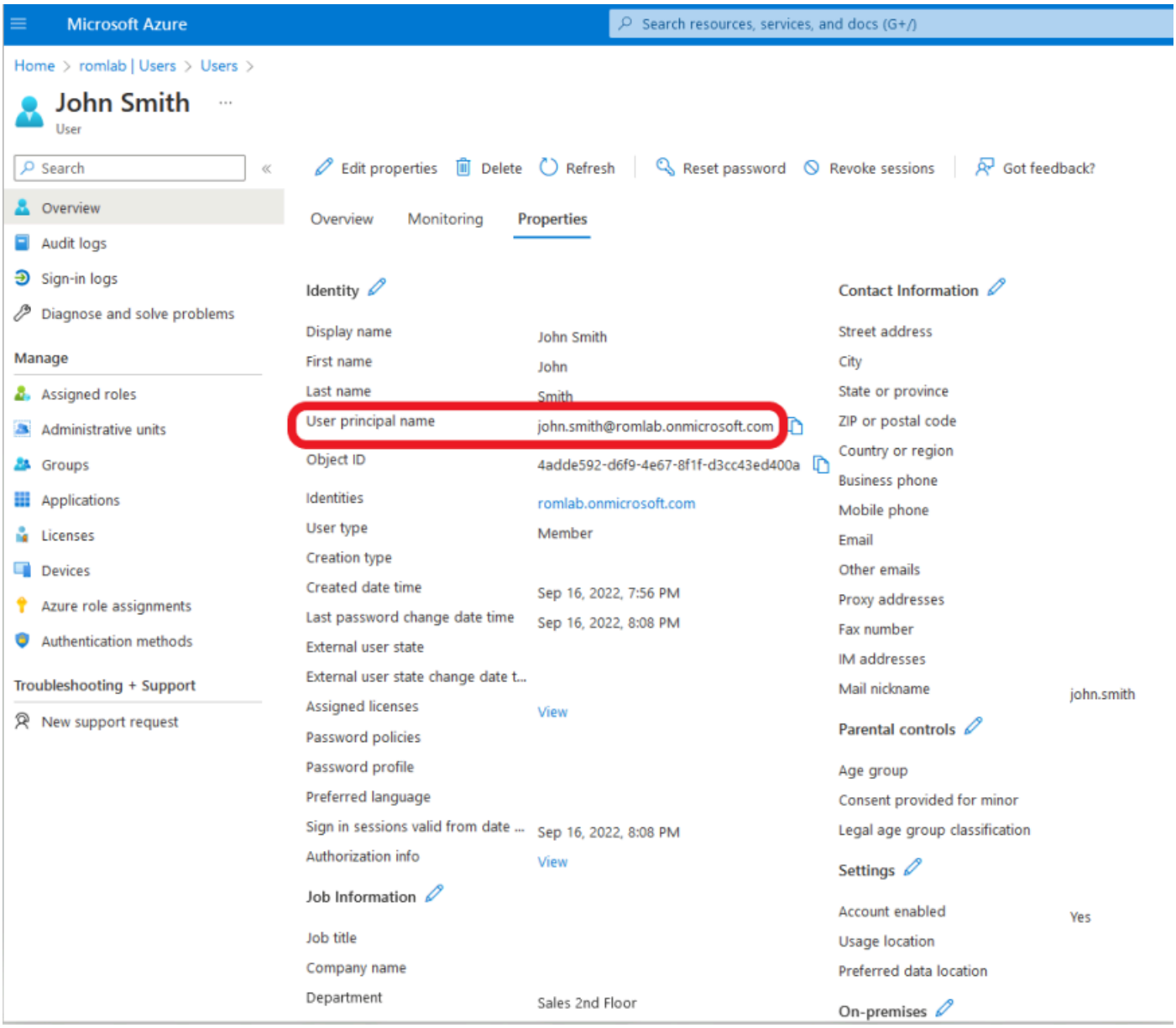


john.smith@romlab.onmicrosoft.com
Issued by: romlab-ROMEO-DC-CA
Expires: Sunday, December 17, 2023 at 6:27:52 PM Central Standard Time
This certificate is valid

Trust

Details

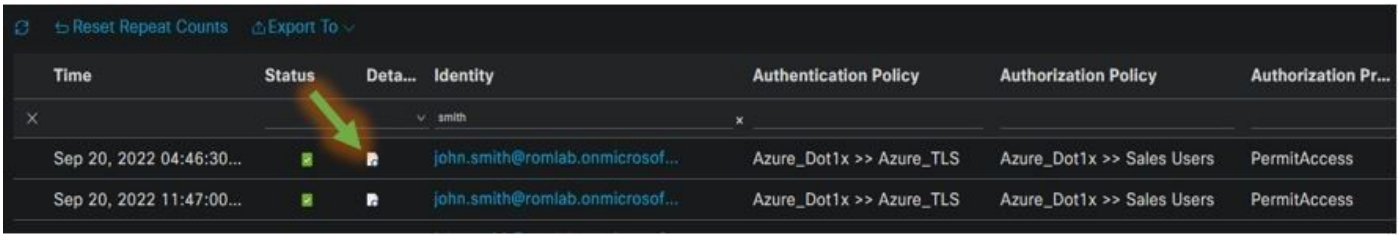
Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01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



Vérifier

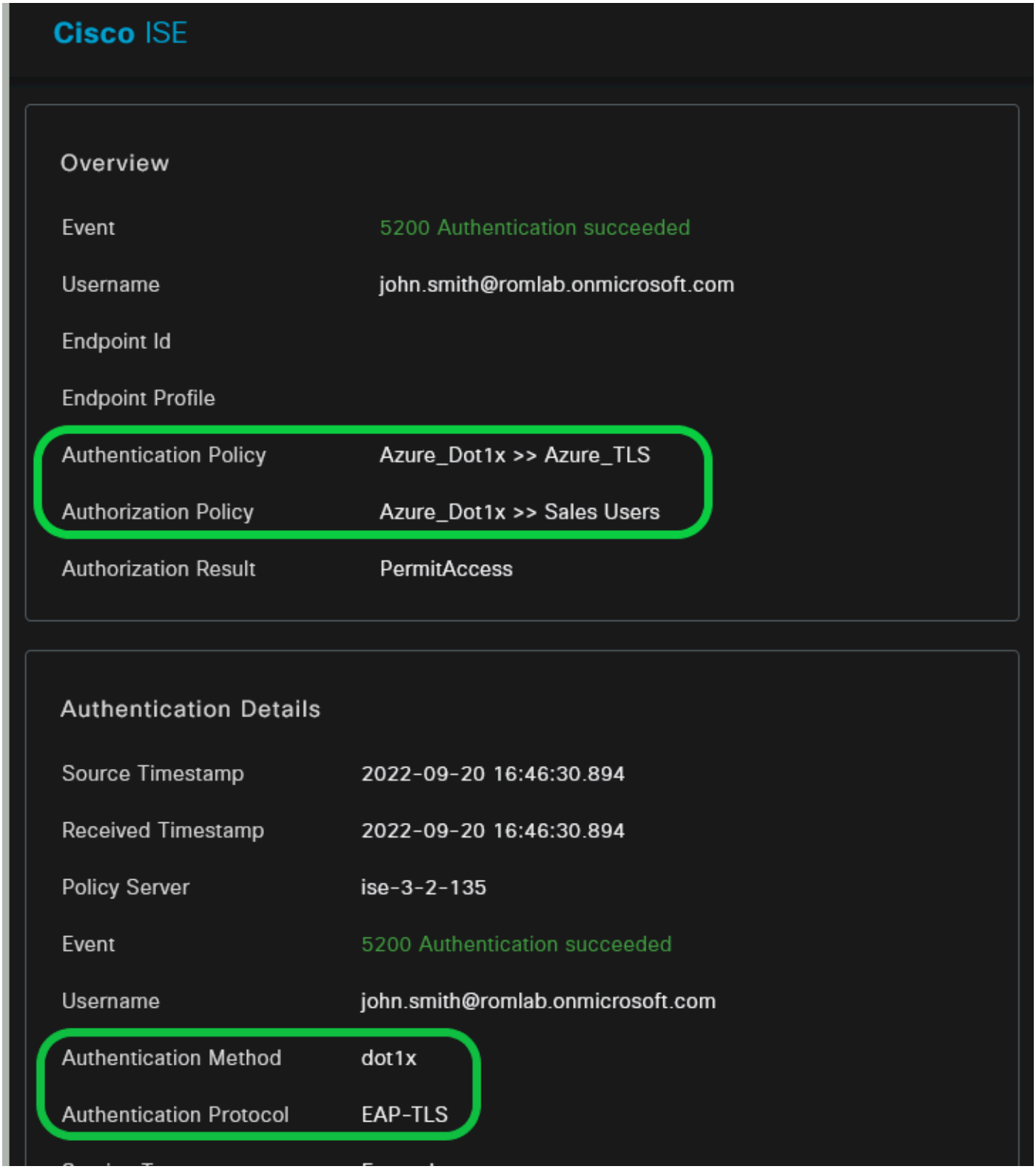
Vérification ISE

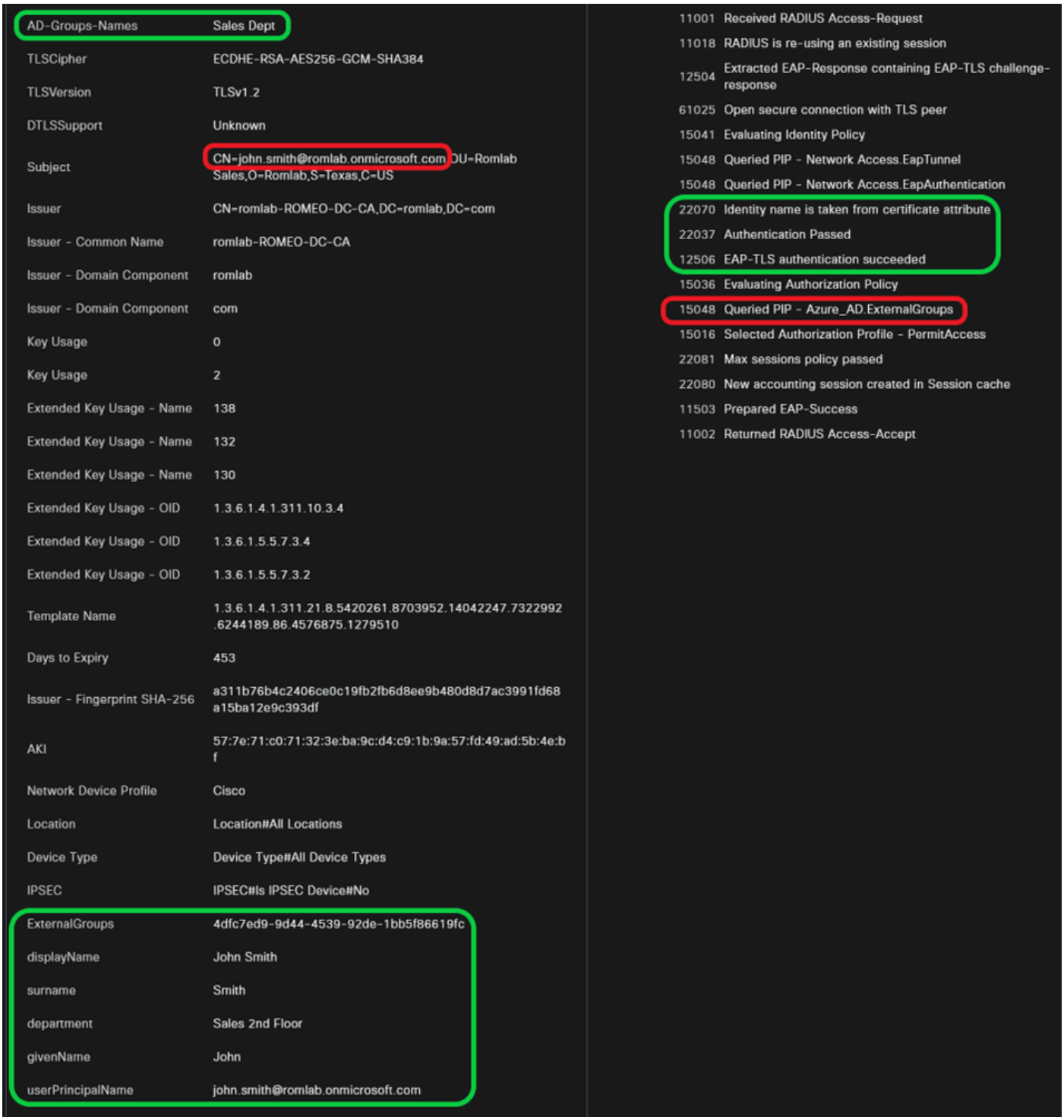
Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu ☰ et choisissez Operations > RADIUS > Live Logs for network authentications (RADIUS).



Cliquez sur l'icône de la loupe dans la colonne Détails pour afficher un rapport d'authentification détaillé et vérifier si le flux fonctionne comme prévu.

1. Vérifiez les stratégies d'authentification/autorisation.
2. Méthode/protocole d'authentification.
3. Nom de l'objet de l'utilisateur extrait du certificat.
4. Groupes d'utilisateurs et autres attributs extraits du répertoire Azure.





Dépannage

Activer les débogages sur ISE

Accédez à Administration > System > Logging > Debug Log Configuration pour définir les composants suivants au niveau spécifié.

Noeud	Nom du composant	Niveau de consignation	Nom du fichier journal

PSN	rest-id-store	Déboguer	rest-id-store.log
PSN	runtime-AAA	Déboguer	prt-server.log

Remarque : Lorsque vous avez terminé le dépannage, n'oubliez pas de réinitialiser les débogages. Pour ce faire, sélectionnez le noeud associé et cliquez sur Reset to Default.

Extraits de journal

Les extraits suivants montrent les deux dernières phases du flux, comme indiqué précédemment dans la section du schéma de réseau.

1. ISE prend le nom du sujet du certificat (CN) et effectue une recherche dans l'API Azure Graph pour récupérer les groupes et autres attributs de l'utilisateur. Il s'agit du nom d'utilisateur principal (UPN) côté Azure.
2. Les stratégies d'autorisation ISE sont évaluées par rapport aux attributs d'utilisateur renvoyés par Azure.

Journaux Rest-id :

```
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
```

Journaux de port :

```
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,userPrincipalNa
me

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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.