

Configuration de Cisco ISE 3.2 EAP-TLS avec Microsoft Azure Active Directory

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

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

Contribution d'Emmanuel Cano, Ingénieur-conseil en sécurité et de Romeo Migisha, Ingénieur-conseil technique

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE)
- Microsoft Azure AD, abonnement et applications
- EAP-TLS authentification

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

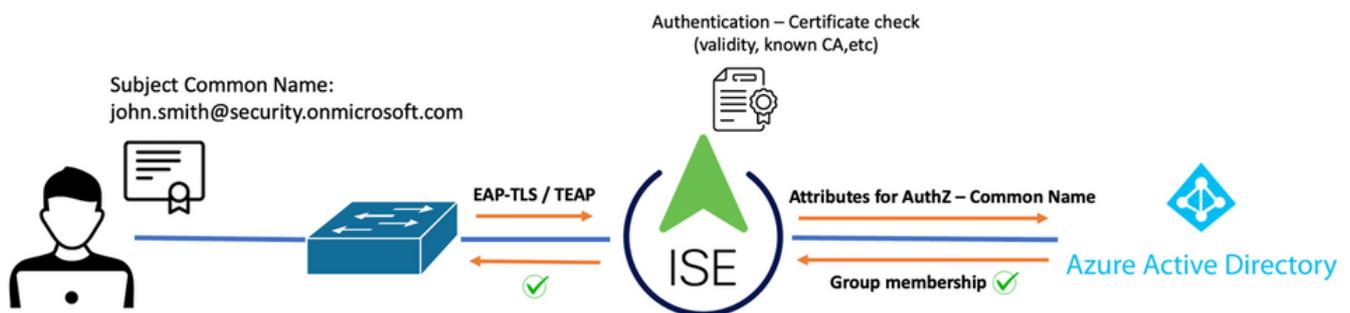
Dans ISE 3.0, il est possible de tirer parti de l'intégration entre ISE et Azure Active Directory (AAD) pour authentifier les utilisateurs en fonction des groupes et attributs Azure AD via la communication ROPC (Resource Owner Password Credentials). Avec ISE 3.2, vous pouvez configurer l'authentification 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 [ici](#).

Configurer le profil d'authentification du certificat

Étape 1. Naviguez jusqu'à l'icône Menu  dans l'angle supérieur gauche et sélectionnez **Administration > Gestion des identités > Sources d'identités externes**.

Étape 2. Sélectionner **Authentification du certificat Profil**, puis cliquez sur **Ajouter**.

Étape 3. Définissez le nom, Définissez le **Magasin d'identités** comme [Sans objet], et sélectionnez **Objet - Nom commun** sur **Utiliser l'identité de** champ. Sélectionnez **Jamais en correspondance** **Certificat client contre certificat dans le magasin d'identités** Champ.

Certificate Authentication Profiles List > Azure_TLS_Certificate_Profile

Certificate Authentication Profile

* Name Azure_TLS_Certificate_Profile

Description Azure EAP-TLS Certificate Profile

Identity Store [not applicable]

Use Identity From Certificate Attribute Subject - Common Name

Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Never

Only to resolve identity ambiguity

Always perform binary comparison

Étape 4. Cliquez sur Enregistrer

Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Certificate Authentication Profile

External Identity Sources

- Certificate Authentication
 - Azure_TLS_Certificate_Profile
 - Preloaded_Certificate_Profile
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST
 - Azure_AD

Edit + Add Duplicate Delete

Name	Description
<u>Azure_TLS_Certificate_Profile</u>	Azure EAP-TLS Certificate Profile
Preloaded_Certificate_Profile	Precreated Certificate Authorization...

Étape 5. Naviguez jusqu'à l'icône Menu dans l'angle supérieur gauche et sélectionnez Stratégie > Ensembles de stratégies.

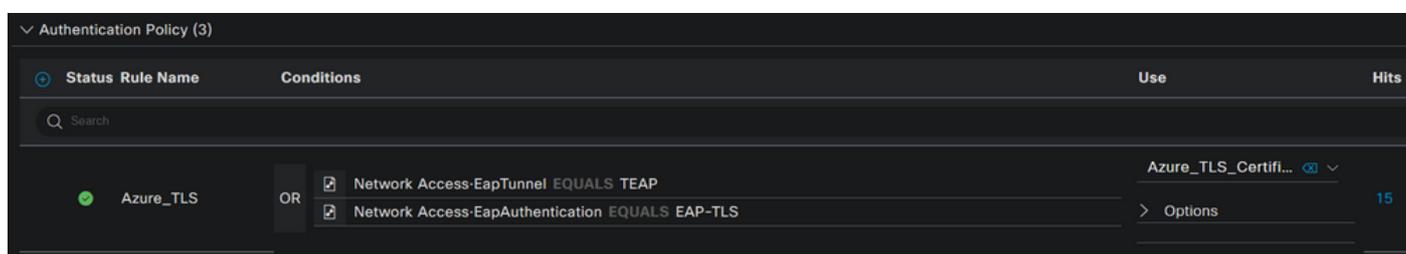
Étape 6. Sélectionnez le signe plus pour créer un nouvel ensemble de stratégies. Définissez

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

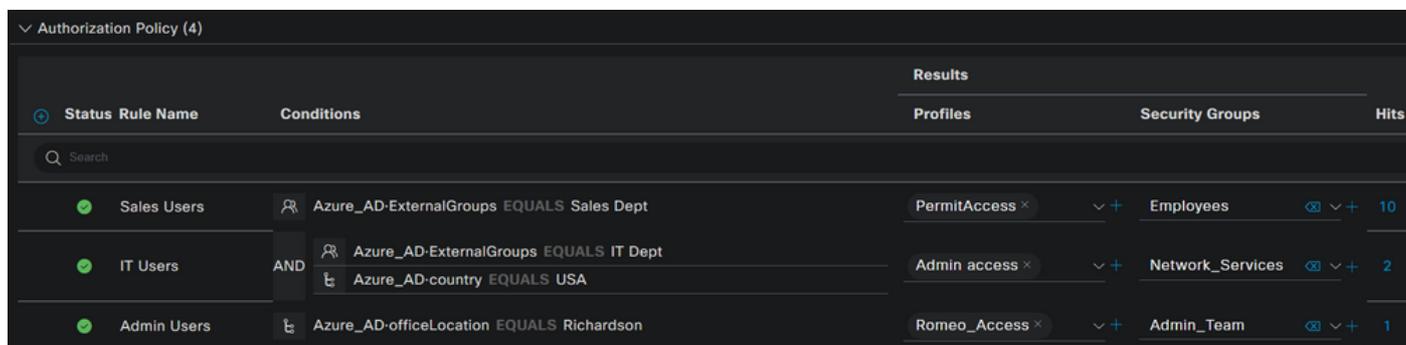


Étape 7. Sélectionnez la flèche  en regard de Default Network Access pour configurer les stratégies d'authentification et d'autorisation.

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. Sélectionnez le profil ou le groupe de sécurité sous Résultats, en fonction de l'exemple 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-ROME0-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-ROME0-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

Microsoft Azure Search resources, services, and docs (G+)

Home > romlab | Users > Users >

John Smith User

Search Edit properties Delete Refresh Reset password Revoke sessions Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods Troubleshooting + Support New support request

Overview Monitoring **Properties**

Identity

Display name	John Smith
First name	John
Last name	Smith
User principal name	john.smith@romlab.onmicrosoft.com
Object ID	4adde592-d6f9-4e67-8f1f-d3cc43ed400a
Identities	romlab.onmicrosoft.com
User type	Member
Creation type	
Created date time	Sep 16, 2022, 7:56 PM
Last password change date time	Sep 16, 2022, 8:08 PM
External user state	
External user state change date t...	
Assigned licenses	View
Password policies	
Password profile	
Preferred language	
Sign in sessions valid from date ...	Sep 16, 2022, 8:08 PM
Authorization info	View

Contact Information

Street address	
City	
State or province	
ZIP or postal code	
Country or region	
Business phone	
Mobile phone	
Email	
Other emails	
Proxy addresses	
Fax number	
IM addresses	
Mail nickname	john.smith

Parental controls

Age group	
Consent provided for minor	
Legal age group classification	

Settings

Account enabled	Yes
Usage location	
Preferred data location	
On-premises	

Job Information

Job title	
Company name	
Department	Sales 2nd Floor

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)**.

Reset Repeat Counts Export To

Time	Status	Deta...	Identity	Authentication Policy	Authorization Policy	Authorization Pr...
Sep 20, 2022 04:46:30...			john.smith@romlab.onmicrosof...	Azure_Dot1x >> Azure_TLS	Azure_Dot1x >> Sales Users	PermitAccess
Sep 20, 2022 11:47:00...			john.smith@romlab.onmicrosof...	Azure_Dot1x >> Azure_TLS	Azure_Dot1x >> Sales Users	PermitAccess

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. Vérifier les stratégies d'authentification/autorisation
2. Méthode/protocole d'authentification

3. Nom du sujet de l'utilisateur extrait du certificat

4. Groupes d'utilisateurs et autres attributs extraits du répertoire Azure

Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	john.smith@romlab.onmicrosoft.com
Endpoint Id	
Endpoint Profile	
Authentication Policy	Azure_Dot1x >> Azure_TLS
Authorization Policy	Azure_Dot1x >> Sales Users
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-09-20 16:46:30.894
Received Timestamp	2022-09-20 16:46:30.894
Policy Server	ise-3-2-135
Event	5200 Authentication succeeded
Username	john.smith@romlab.onmicrosoft.com
Authentication Method	dot1x
Authentication Protocol	EAP-TLS

AD-Groups-Names	Sales Dept	11001	Received RADIUS Access-Request
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384	11018	RADIUS is re-using an existing session
TLSVersion	TLSv1.2	12504	Extracted EAP-Response containing EAP-TLS challenge-response
DTLSSupport	Unknown	61025	Open secure connection with TLS peer
Subject	CN=John.smith@romlab.onmicrosoft.com OU=Romlab Sales,O=Romlab,S=Texas,C=US	15041	Evaluating Identity Policy
Issuer	CN=romlab-ROME0-DC-CA,DC=romlab,DC=com	15048	Queried PIP - Network Access.EapTunnel
Issuer - Common Name	romlab-ROME0-DC-CA	15048	Queried PIP - Network Access.EapAuthentication
Issuer - Domain Component	romlab	22070	Identity name is taken from certificate attribute
Issuer - Domain Component	com	22037	Authentication Passed
Key Usage	0	12506	EAP-TLS authentication succeeded
Key Usage	2	15036	Evaluating Authorization Policy
Extended Key Usage - Name	138	15048	Queried PIP - Azure_AD.ExternalGroups
Extended Key Usage - Name	132	15016	Selected Authorization Profile - PermitAccess
Extended Key Usage - Name	130	22081	Max sessions policy passed
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4	22080	New accounting session created in Session cache
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4	11503	Prepared EAP-Success
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2	11002	Returned RADIUS Access-Accept
Template Name	1.3.6.1.4.1.311.21.8.5420261.8703952.14042247.7322992.6244189.86.4576875.1279510		
Days to Expiry	453		
Issuer - Fingerprint SHA-256	a311b76b4c2406ce0c19fb2fb6d8ee9b480d8d7ac3991fd68a15ba12e9c393df		
AKI	57:7e:71:c0:71:32:3e:ba:9c:d4:c9:1b:9a:57:fd:49:ad:5b:4e:b f		
Network Device Profile	Cisco		
Location	Location#All Locations		
Device Type	Device Type#All Device Types		
IPSEC	IPSEC#Is IPSEC Device#No		
ExternalGroups	4dfc7ed9-9d44-4539-92de-1bb5f86619fc		
displayName	John Smith		
surname	Smith		
department	Sales 2nd Floor		
givenName	John		
userPrincipalName	john.smith@romlab.onmicrosoft.com		

Dépannage

Activer les débogages sur ISE

Naviguez jusqu'à **Administration > System > Logging > Debug Log Configuration** pour définir les composants suivants sur le 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	pvt-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 journaux

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 de l'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.LdpKeyValueCacheInitializer -:- 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.prvt.impl.PrRTCpmBridge -::::- ---- Running Authorization Policy ----

2022-09-20 16:46:30,252 DEBUG [Thread-759][()] cisco.cpm.prvt.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.prvt.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.prvt.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.prvt.pip.RestIdentityProviderPIP -::::- Username from the Context
john.smith@romlab.onmicrosoft.com

2022-09-20 16:46:30,880 DEBUG [Thread-759][()] cisco.cpm.prvt.pip.RestIdentityProviderPIP -::::- userAttr size 11
...
2022-09-20 16:46:30,881 DEBUG [Thread-759][()] cisco.cpm.prvt.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.prvt.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.prvt.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.prvt.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.prvt.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.prvt.pip.RestIdentityProviderPIP -::::- userGroup 1

2022-09-20 16:46:30,882 DEBUG [Thread-759][()] cisco.cpm.prvt.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.