

# Microsoft Azure Active Directoryを使用したCisco ISE 3.2 EAP-TLSの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Azure ADグループメンバーシップと、認証プロトコルとしてEAP-TLSまたはTEAPを使用するその他のユーザ属性に基づいて、ISEで認証ポリシーを設定し、トラブルシューティングする方法について説明します。

著者： Emmanuel Cano、セキュリティコンサルティングエンジニア、Romeo Migisha、テクニカルコンサルティングエンジニア

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine ( ISE )
- Microsoft Azure AD、サブスクリプション、アプリ
- EAP-TLS CA1 を関連付けます

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE 3.2
- Microsoft Azure AD

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 背景説明

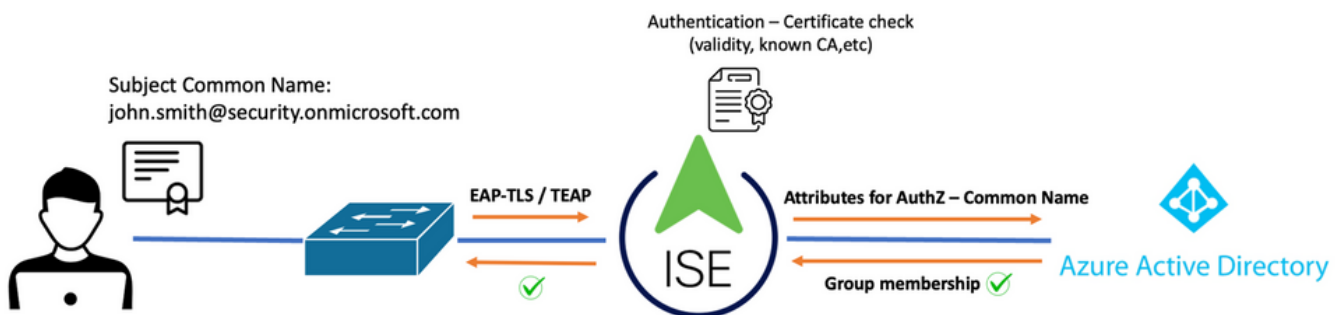
ISE 3.0では、ISEとAzure Active Directory (AAD)の統合を活用して、リソース所有者のパスワード資格情報(ROPC)通信を通じて、Azure ADのグループと属性に基づいてユーザーを認証することができます。ISE 3.2では、証明書ベースの認証を設定でき、Azure ADグループメンバーシップやその他の属性に基づいてユーザーを認証できます。ISEはGraph APIを使用してAzureにクエリを実行し、認証されたユーザーのグループと属性を取得します。Azure側のユーザープリンシパル名(UPN)に対して証明書のサブジェクト共通名(CN)を使用します。

注：証明書ベースの認証は、内部方式としてEAP-TLSまたはEAP-TLSを使用したTEAPのいずれかになります。次に、Azure Active Directoryから属性を選択し、Cisco ISEディクショナリに追加できます。これらの属性は認可に使用できます。ユーザ認証のみがサポートされます。

## 設定

### ネットワーク図

次の図に、ネットワークダイアグラムとトラフィックフローの例を示します



### 手順：

1. 証明書は、内部方式としてEAP-TLSまたはEAP-TLSを使用するTEAPを介してISEに送信されます。
2. ISEはユーザの証明書（有効期間、信頼できるCA、CRLなど）を評価します。
3. ISEは証明書サブジェクト名(CN)を取得し、Microsoft Graph APIをルックアップして、そのユーザのグループおよびその他の属性を取得します。これは、Azure側ではユーザープリンシパル名(UPN)と呼ばれます。
4. ISE認証ポリシーは、Azureから返されたユーザーの属性に対して評価されます。

注：次に示すように、Graph API権限を設定し、Microsoft AzureのISEアプリケーションに付与する必要があります。


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

## 設定

### ISE の設定

注:ROPCの機能とISEとAzure ADの統合については、このドキュメントの対象外です。グループとユーザー属性をAzureから追加することが重要です。設定ガイド[here](#)を参照してください。

### 証明書認証プロファイルの設定

ステップ 1： 移動先 Menuアイコン  を選択します。 [Administration] > [Identity Management] > [External Identity sources]

ステップ 2： 選択 **証明書認証** [Profile]をクリックし、 **追加**.

ステップ 3： 名前を定義し、 **IDストア** [Not applicable]を選択し、 [Subject - Common Name on]を選択します [Use Identity From] フィールドにプローブ間隔値を入力します。 [Never on Match]を選択します。 **IDストア内の証明書に対するクライアント証明書** フィールドにプローブ間隔値を入力します。

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

ステップ 4： クリック 保存します。

Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

### Certificate Authentication Profile


External Identity Sources

- ▼ Certificate Authentication Profiles
  - Azure\_TLS\_Certificate\_Profile
  - Preloaded\_Certificate\_Profile
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST
  - Azure\_AD

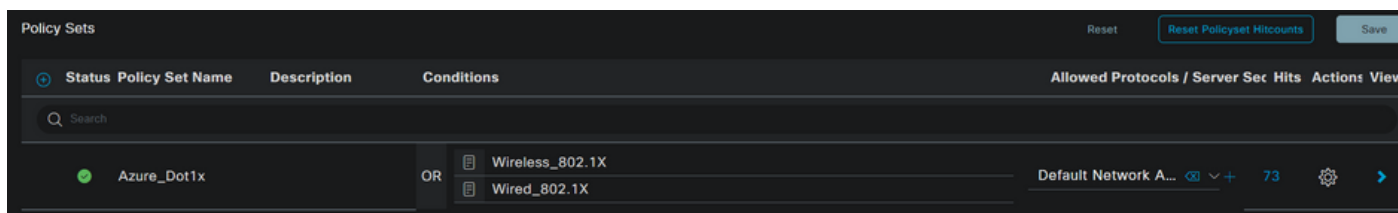
Edit  + Add  Duplicate  Delete

Name	Description
<input checked="" type="checkbox"/> Azure_TLS_Certificate_Profile	Azure EAP-TLS Certificate Profile
<input type="checkbox"/> Preloaded_Certificate_Profile	Precreated Certificate Authorization...

ステップ 5： 移動先 Menuアイコン  を選択します。 [Policy] > [Policy Sets]。

手順 6： プラス記号を選択します  アイコンをクリックして、新しいポリシーセットを作成します。名前を定義し、条件として [Wireless 802.1x] または [Wired 802.1x] を選択します。この例で

は、[Default Network Access]オプションを使用します

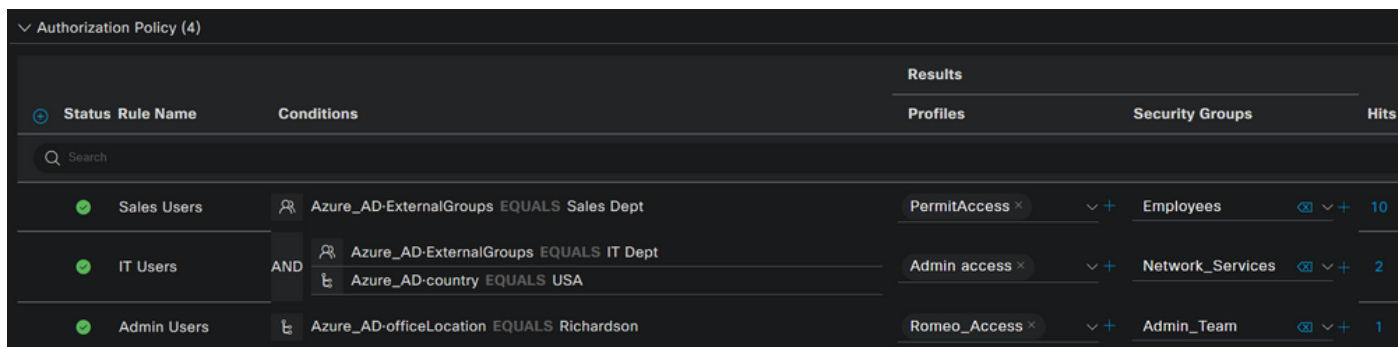


手順 7： 矢印を選択します ➡ [Default Network Access]の横に表示され、認証ポリシーと許可ポリシーを設定します。

ステップ 8： [Authentication Policy]オプションを選択し、名前を定義してEAP-TLSを[Network Access EAPAuthentication]として追加します。TEAPが認証プロトコルとして使用されている場合、TEAPを[Network Access EAPTunnel]として追加できます。ステップ3で作成した証明書認証プロファイルを選択し、保存します。



ステップ 9： [Authorization Policy]オプションを選択し、名前を定義して、Azure ADグループまたはユーザー属性を条件として追加します。[結果(Results)]でプロファイルまたはセキュリティグループを選択し、使用例に応じて、保存します。



## ユーザ設定.

認証ルールで使用されるADグループメンバーシップとユーザー属性を取得するには、ユーザー証明書のサブジェクト共通名(CN)がAzure側のユーザープリンシパル名(UPN)と一致する必要があります。認証を成功させるには、ルートCAおよび中間CA証明書がISE信頼ストアに存在する必要があります。



**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
<b>User principal name</b>	<b>john.smith@romlab.onmicrosoft.com</b>
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

## 確認

### ISEの検証

Cisco ISE GUIで、[Menu] アイコンをクリックします ☰ を選択し、[Operations] > [RADIUS] > [Live Logs for network authentications (RADIUS)]。

Reset Repeat Counts Export To

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

[Details]列の拡大鏡アイコンをクリックして詳細な認証レポートを表示し、フローが期待どおりに機能するかどうかを確認します。

1. 認証/認可ポリシーの確認
2. 認証方式/プロトコル

3. 証明書から取得されたユーザのサブジェクト名

4. Azureディレクトリからフェッチされたユーザーグループおよびその他の属性

## 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		

## トラブルシューティング

### ISEでのデバッグの有効化

移動先 **Administration > System > Logging > Debug Log Configuration** をクリックして、次の構成部品を指定したレベルに設定します。

ノード	コンポーネント名	ログレベル	ログファイル名
PSN	rest-id-store	デバッグ	rest-id-store.log
PSN	runtime-AAA	デバッグ	prrt-server.log

注：トラブルシューティングが終了したら、必ずデバッグをリセットしてください。これを行うには、関連するノードを選択し、「デフォルトにリセット」をクリックします。

## ログのスニペット

次の抜粋は、「ネットワークダイアグラム」セクションで前述したように、フローの最後の2つのフェーズを示しています。

1. ISEは証明書のサブジェクト名(CN)を取得し、Azure Graph APIのルックアップを実行して、そのユーザのグループおよびその他の属性を取得します。これは、Azure側ではユーザープリンシパル名(UPN)と呼ばれます。
2. ISE認証ポリシーは、Azureから返されたユーザの属性に対して評価されます。

### Rest-idログ:

```
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,department,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
```

### Prrtログ:

```
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
```

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。