

使用Microsoft Azure Active Directory配置ISE 3.2 EAP-TLS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何根據EAP-TLS或TEAP的Azure AD組成員身份在ISE中配置授權策略並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 身分識別服務引擎 (ISE)
- Microsoft Azure AD、訂閱和應用
- EAP-TLS 驗證

採用元件

本文中的資訊係根據以下軟體和硬體版本：


- Cisco ISE 3.2
- Microsoft Azure AD

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在ISE 3.0中，可以利用ISE與Azure Active Directory(AAD)之間的整合，通過資源所有者密碼憑證

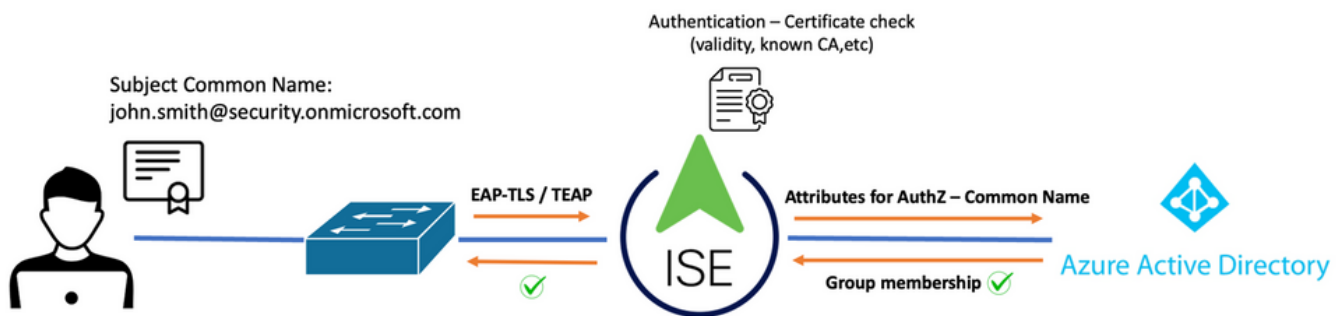
(ROPC)通訊基於Azure AD組和屬性對使用者進行身份驗證。使用ISE 3.2，您可以配置基於證書的身份驗證，並且使用者可以基於azure AD組成員身份和其他屬性獲得授權。ISE通過圖形API查詢Azure來獲取經過身份驗證的使用者的組和屬性，它根據Azure端的使用者主體名稱(UPN)使用證書的使用者公用名(CN)。

 註：基於證書的身份驗證可以是EAP-TLS或以EAP-TLS作為內部方法的TEAP。然後，您可以從Azure Active Directory選擇屬性並將其新增到思科ISE詞典。這些屬性可用於授權。僅支援使用者身份驗證。

設定


網路圖表

下一張圖提供網路圖表和流量傳輸的範例



過程:


1. 證書通過EAP-TLS或TEAP傳送到ISE，EAP-TLS作為內部方法。
2. ISE評估使用者證書（有效期、受信任CA、CRL等。）
3. ISE獲取證書使用者名稱(CN)並執行查詢Microsoft Graph API以獲取該使用者的組和其他屬性。這在Azure端稱為使用者主體名稱(UPN)。
4. 根據從Azure返回的使用者屬性評估ISE授權策略。

 注意：您必須配置圖形API許可權並將其授予Microsoft Azure中的ISE應用，如下所示：

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


組態

ISE 組態

 注意:ROPC功能和ISE與Azure AD之間的整合不在本文檔的範圍之內。從Azure新增組和使用者屬性很重要。請參閱此處的[配置指南](#)。

配置證書身份驗證配置檔案



步驟 1. 導航至  位於左上角，然後選擇 管理>身份管理>外部身份源。

步驟 2. 選擇 憑證驗證 配置式，然後按一下 新增。

步驟 3. 定義名稱，設定 身份庫 為[不適用]，然後選擇主題 — 通用名稱 使用身份源 欄位。選擇Never on Match 針對身份庫中的證書的客戶端證書 欄位。

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

步驟 4. 按一下 儲存

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

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

Certificate Authentication Profile

Edit + Add Duplicate Delete

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

步驟 5. 導航至 Menu 圖示

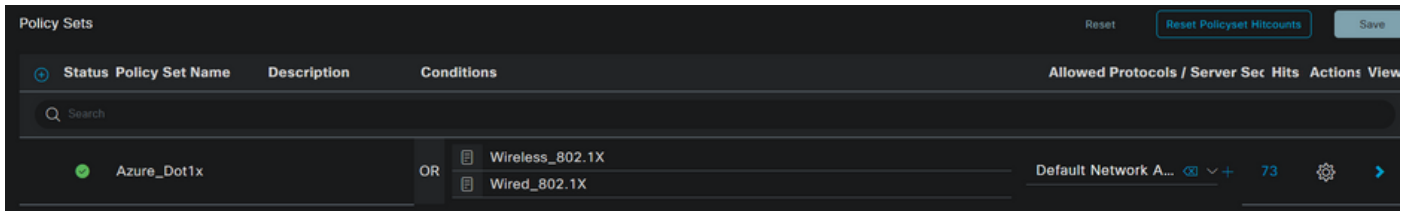


位於左上角，然後選擇 策略>策略集。

步驟 6. 選擇加號



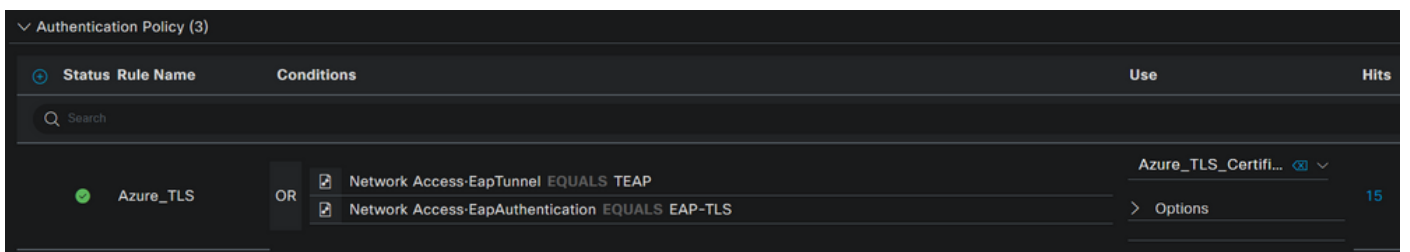
圖示以建立新的策略集。定義名稱並選擇無線802.1x或有線802.1x作為條件。本示例中使用了 Default Network Access 選項



步驟 7. 選取箭頭

在Default Network Access旁，配置身份驗證和授權策略。

步驟 8. 選擇Authentication Policy選項，定義名稱並新增EAP-TLS作為網路訪問EAPAuthentication，如果將TEAP用作身份驗證協定，則可能新增TEAP作為網路訪問EAPTunnel。選擇步驟3中建立的證書身份驗證配置檔案，然後按一下 儲存。




步驟 9. 選擇「授權策略」選項，定義名稱並將Azure AD組或使用者屬性新增為條件。選擇結果下的配置檔案或安全組（取決於用例），然後按一下 儲存。

Authorization Policy (4)		Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits
●	Sales Users	Azure_AD-ExternalGroups EQUALS Sales Dept	PermitAccess ×	Employees	10
●	IT Users	AND Azure_AD-ExternalGroups EQUALS IT Dept Azure_AD-country EQUALS USA	Admin access ×	Network_Services	2
●	Admin Users	Azure_AD-officeLocation EQUALS Richardson	Romeo_Access ×	Admin_Team	1

使用者配置。

使用者證書中的使用者公用名稱(CN)必須與Azure端上的使用者主體名稱(UPN)匹配，才能檢索在授權規則中使用的AD組成員身份和使用者屬性。為使身份驗證成功，根CA和任何中間CA證書必須位於ISE受信任儲存中。



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

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

驗證

ISE 驗證

在Cisco ISE GUI中，按一下Menu圖示



選擇 Operations > RADIUS > Live Logs for network authentications(RADIUS)。

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

按一下Details列中的放大鏡圖示以檢視詳細的身份驗證報告，並確認流是否按預期運行。

1. 驗證身份驗證/授權策略
2. 驗證方法/協定
3. 從證書中獲取的使用者使用者名稱
4. 從Azure目錄提取的使用者組和其他屬性

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		
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384		11001 Received RADIUS Access-Request
TLSVersion	TLSv1.2		11018 RADIUS is re-using an existing session
DTLSSupport	Unknown		12504 Extracted EAP-Response containing EAP-TLS challenge-response
Subject	CN=John.smith@romlab.onmicrosoft.com OU=Romlab Sales,O=Romlab,S=Texas,C=US		61025 Open secure connection with TLS peer
Issuer	CN=romlab-ROME0-DC-CA,DC=romlab,DC=com		15041 Evaluating Identity Policy
Issuer - Common Name	romlab-ROME0-DC-CA		15048 Queried PIP - Network Access.EapTunnel
Issuer - Domain Component	romlab		15048 Queried PIP - Network Access.EapAuthentication
Issuer - Domain Component	com		22070 Identity name is taken from certificate attribute
Key Usage	0		22037 Authentication Passed
Key Usage	2		12506 EAP-TLS authentication succeeded
Extended Key Usage - Name	138		15036 Evaluating Authorization Policy
Extended Key Usage - Name	132		15048 Queried PIP - Azure_AD.ExternalGroups
Extended Key Usage - Name	130		15016 Selected Authorization Profile - PermitAccess
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4		22081 Max sessions policy passed
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4		22080 New accounting session created in Session cache
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2		11503 Prepared EAP-Success
Template Name	1.3.6.1.4.1.311.21.8.5420261.8703952.14042247.7322992.6244189.86.4576875.1279510		11002 Returned RADIUS Access-Accept
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		


疑難排解

在ISE上啟用調試

導航至 管理>系統>記錄>調試日誌配置 將下一個元件設定為指定級別。

節點	元件名稱	日誌級別	日誌檔名
PSN	rest-id-store	偵錯	rest-id-store.log

PSN	運行時AAA	偵錯	prrt-server.log
-----	--------	----	-----------------

 注意：完成故障排除後，請記住重置調試。為此，請選擇相關節點，然後按一下「重置為預設值」。

日誌片段

接下來的摘錄顯示了流程的最後兩個階段，如前面網路圖部分所述。

1. ISE獲取證書使用者名稱(CN)並執行對Azure Graph API的查詢，以獲取該使用者的組和其他屬性。這在Azure端稱為使用者主體名稱(UPN)。
2. 根據從Azure返回的使用者屬性評估ISE授權策略。

Rest-id日誌:

```
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,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
```

埠日誌:

```
2022-09-20 16:46:30,182 DEBUG [Thread-759][()] cisco.cpm.pr.rt.impl.PrRTCPmBridge -::::- ---- Running Authorization Policy ----

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

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

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。