使用Microsoft Azure Active Directory配置ISE 3.2 EAP-TLS

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 步骤
- 配置
  - ISE 配置
  - 配置证书身份验证配置文件
  - 用户配置

验证

- ISE验证

故障排除

- 在ISE上启用调试
- 日志片段

简介

本文档介绍如何根据EAP-TLS或TEAP的Azure AD组成员身份在ISE中配置授权策略并进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎 (ISE)
- Microsoft Azure AD、订阅和应用
- EAP-TLS身份验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE 3.2

- Microsoft Azure AD

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

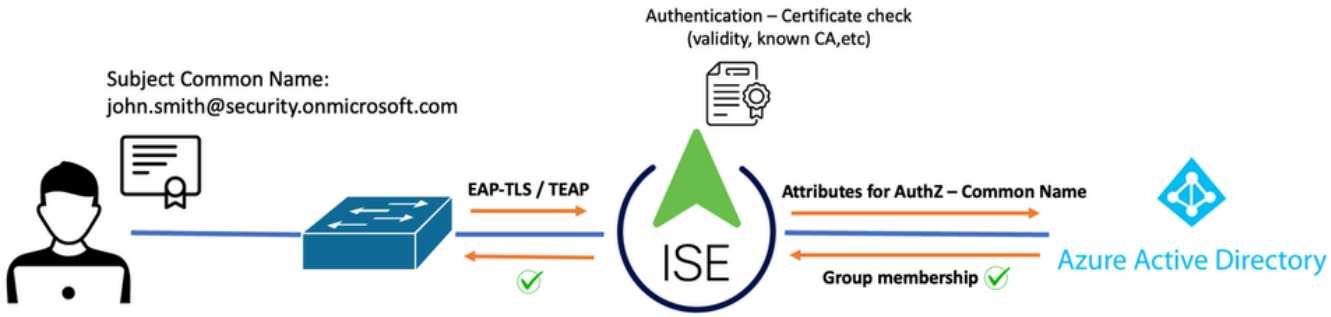
在ISE 3.0中，可以利用ISE与Azure Active Directory(AAD)之间的集成，通过资源所有者密码凭证(ROPC)通信根据Azure AD组和属性对用户进行身份验证。使用ISE 3.2，您可以配置基于证书的身份验证，用户可以根据Azure AD组成员身份和其他属性获得授权。ISE通过图形API查询Azure以获取经过身份验证的用户的组和属性，它根据Azure端的用户主体名称(UPN)使用证书的使用者公用名(CN)。

注意：基于证书的身份验证可以是EAP-TLS或EAP-TLS作为内部方法的TEAP。然后，您可以从Azure Active Directory选择属性并将其添加到思科ISE词典。这些属性可用于授权。仅支持用户身份验证。

配置

网络图

下图提供了网络图和流量传输的示例:



步骤

1. 证书通过EAP-TLS或TEAP发送到ISE，EAP-TLS作为内部方法。
2. ISE评估用户的证书（有效期、受信任CA、CRL等。）
3. ISE获取证书使用者名称(CN)并执行查找Microsoft Graph API以获取用户的组以及该用户的其它属性。这在Azure端称为用户主体名称(UPN)。
4. ISE授权策略根据从Azure返回的用户属性进行评估。

注意：您必须在Microsoft Azure中配置并授予ISE应用的图形API权限，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

配置

ISE 配置

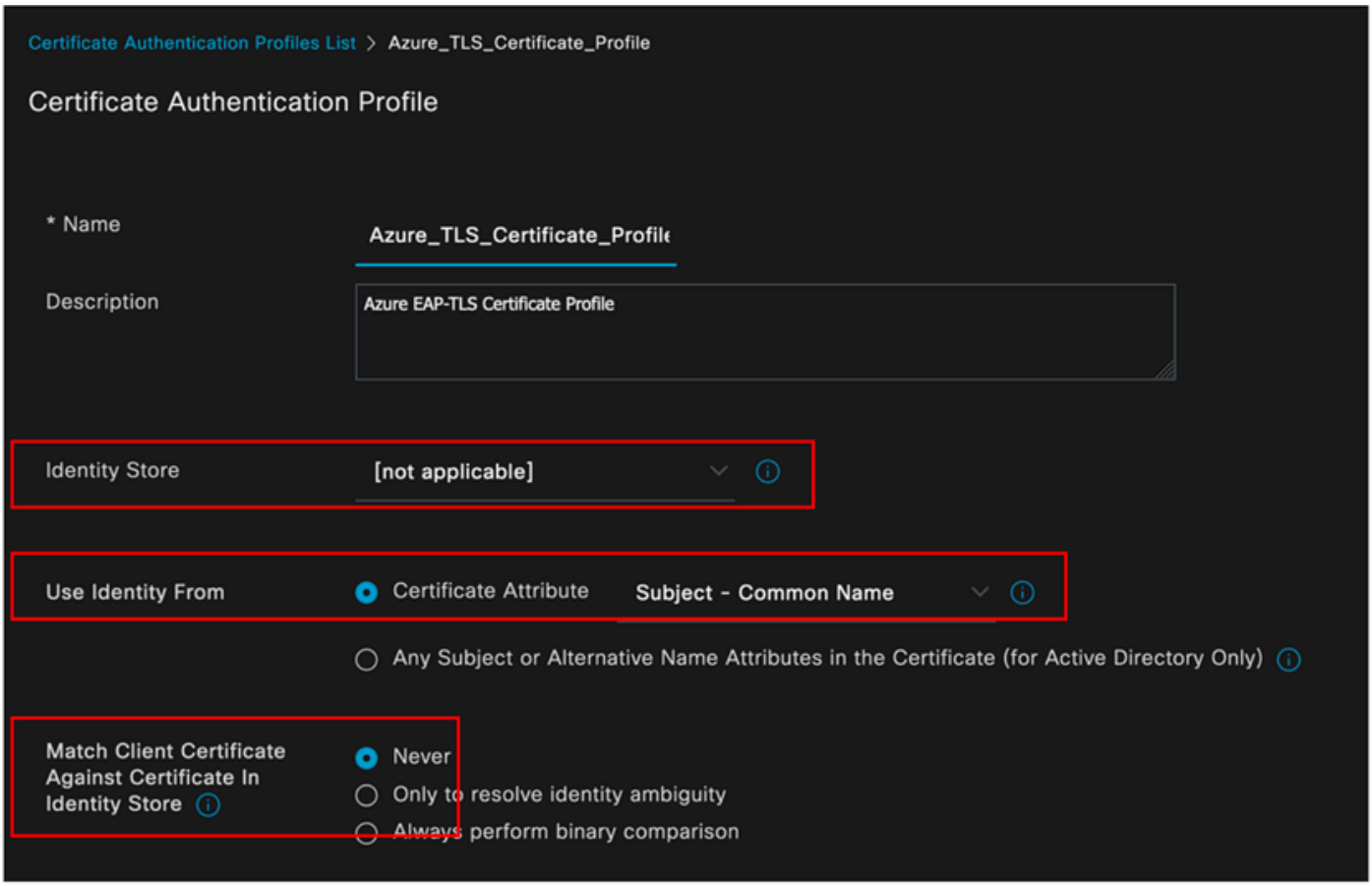
> 注意：ROPC功能和ISE与Azure AD之间的集成不在本文档的讨论范围之内。从Azure添加组和用户属性很重要。请参阅配置指南。

配置证书身份验证配置文件

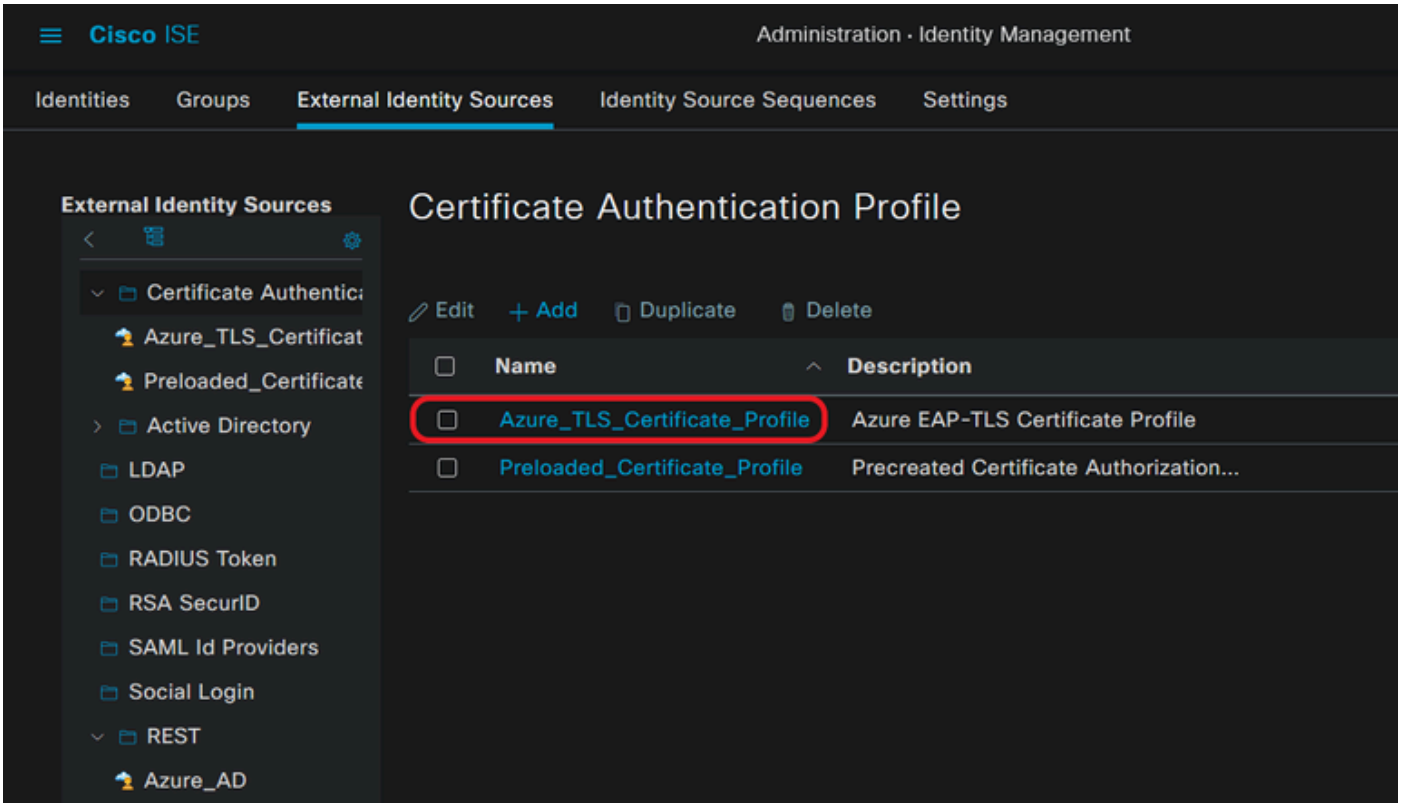
步骤1.导航到菜单图标 ☰ 位于左上角，然后选择Administration > Identity Management > External Identity sources。

第2步：选择Certificate Authentication Profile，然后点击Add。

步骤3.定义名称。将Identity Store设置为[不适用]，然后选择Subject - Common Name on Use Identity From字段。选择Never on Match Client Certificate against Certificate in Identity Store字段。



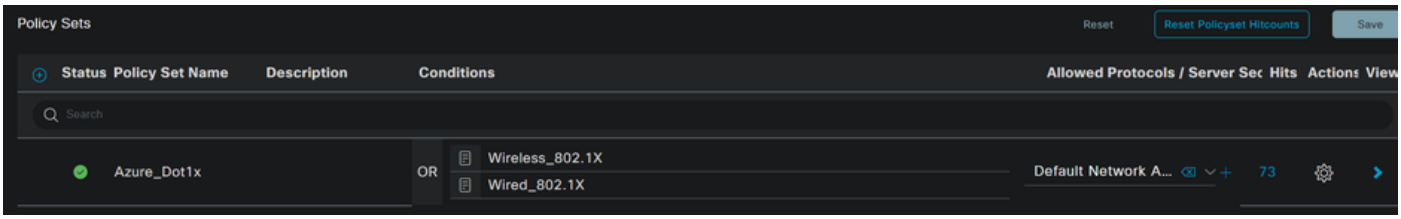
步骤4.单击保存:



步骤5.导航到菜单图标 位于左上角，然后选择Policy > Policy Sets。

步骤6.选择加号 图标以创建新的策略集。定义名称并选择无线802.1x或有线802.1x作为条件。

本示例中使用了Default Network Access选项:

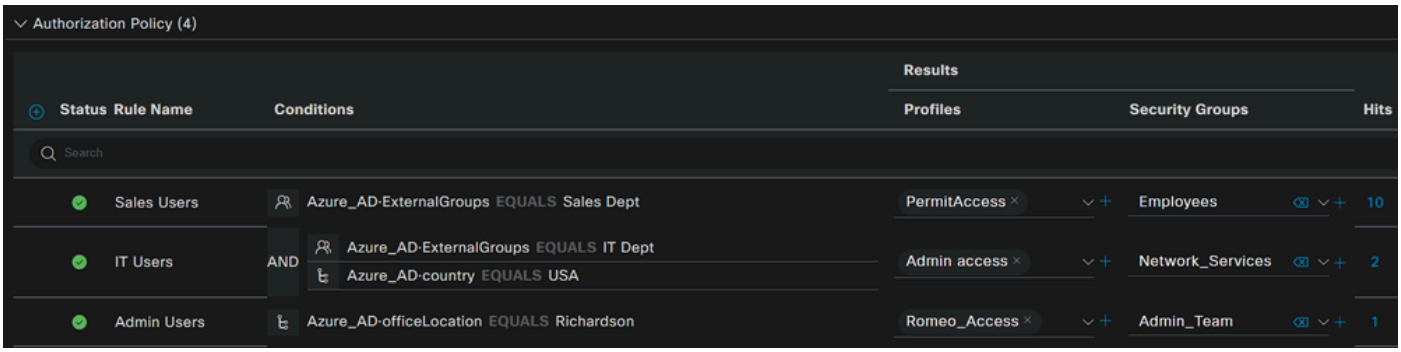


步骤7.选择箭头 › 在Default Network Access旁边，配置身份验证和授权策略。

第8步：选择Authentication Policy选项，定义名称并添加EAP-TLS作为网络访问EAPAuthentication，如果将TEAP用作身份验证协议，则可以添加TEAP作为网络访问EAPTunnel。选择在第3步中创建的证书身份验证配置文件，然后单击Save。



第9步：选择“授权策略”选项，定义名称并将Azure AD组或用户属性添加为条件。在“结果”(Results)下选择配置文件或安全组，具体取决于使用案例，然后单击保存。



用户配置

用户证书的主题公用名(CN)必须与Azure端上的用户主体名称(UPN)匹配，才能检索在授权规则中使用的AD组成员身份和用户属性。为使身份验证成功，根CA和任何中间CA证书必须位于ISE受信任库中。

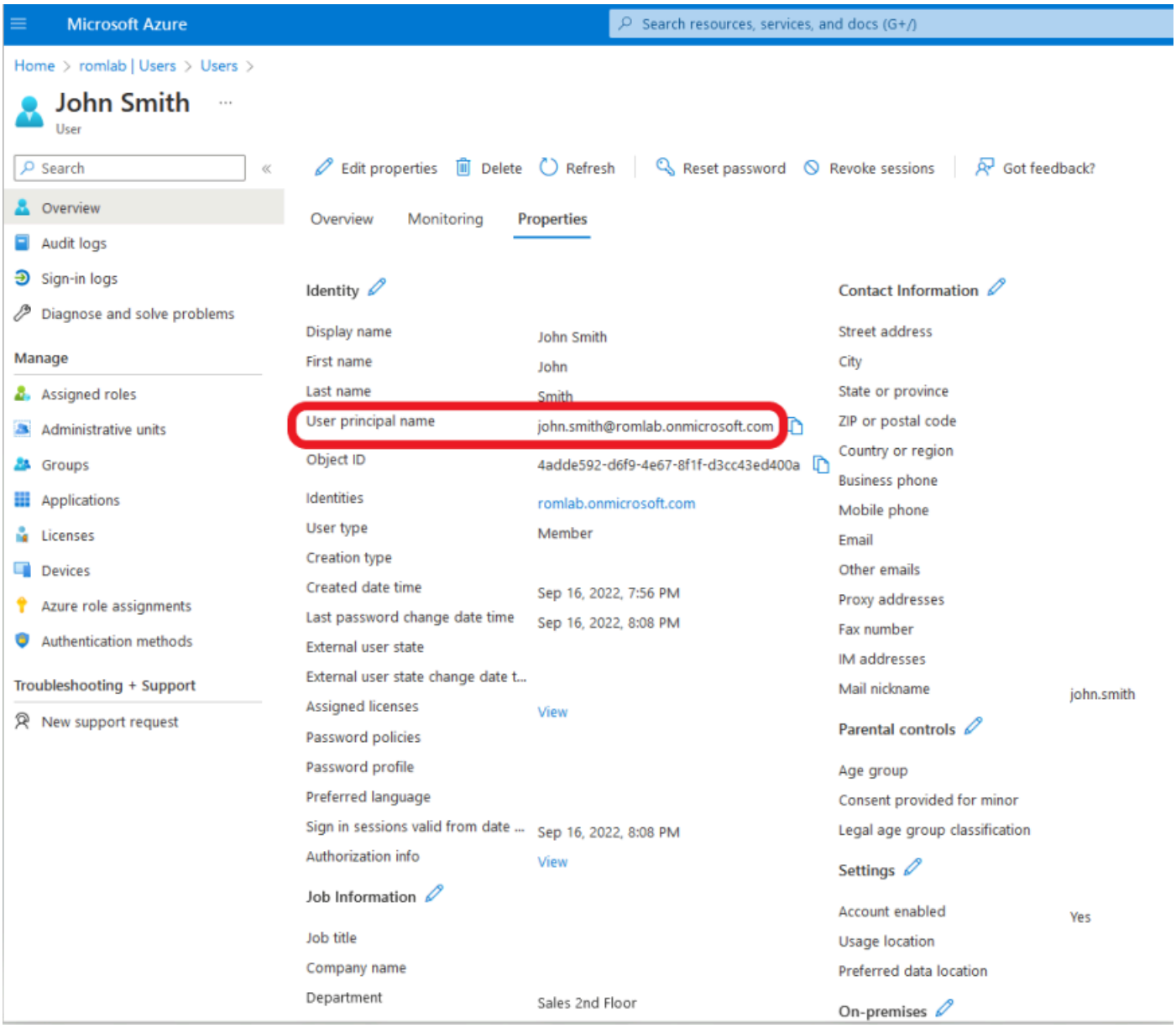


john.smith@romlab.onmicrosoft.com
Issued by: romlab-ROMEO-DC-CA
Expires: Sunday, December 17, 2023 at 6:27:52 PM Central Standard Time
This certificate is valid

Trust

Details

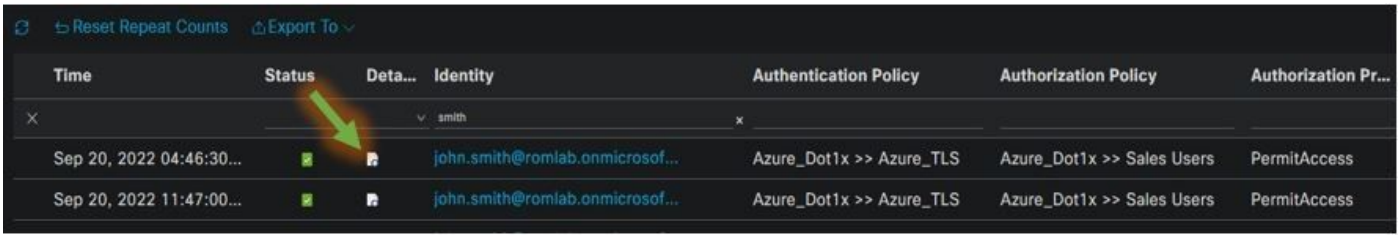
Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01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



验证

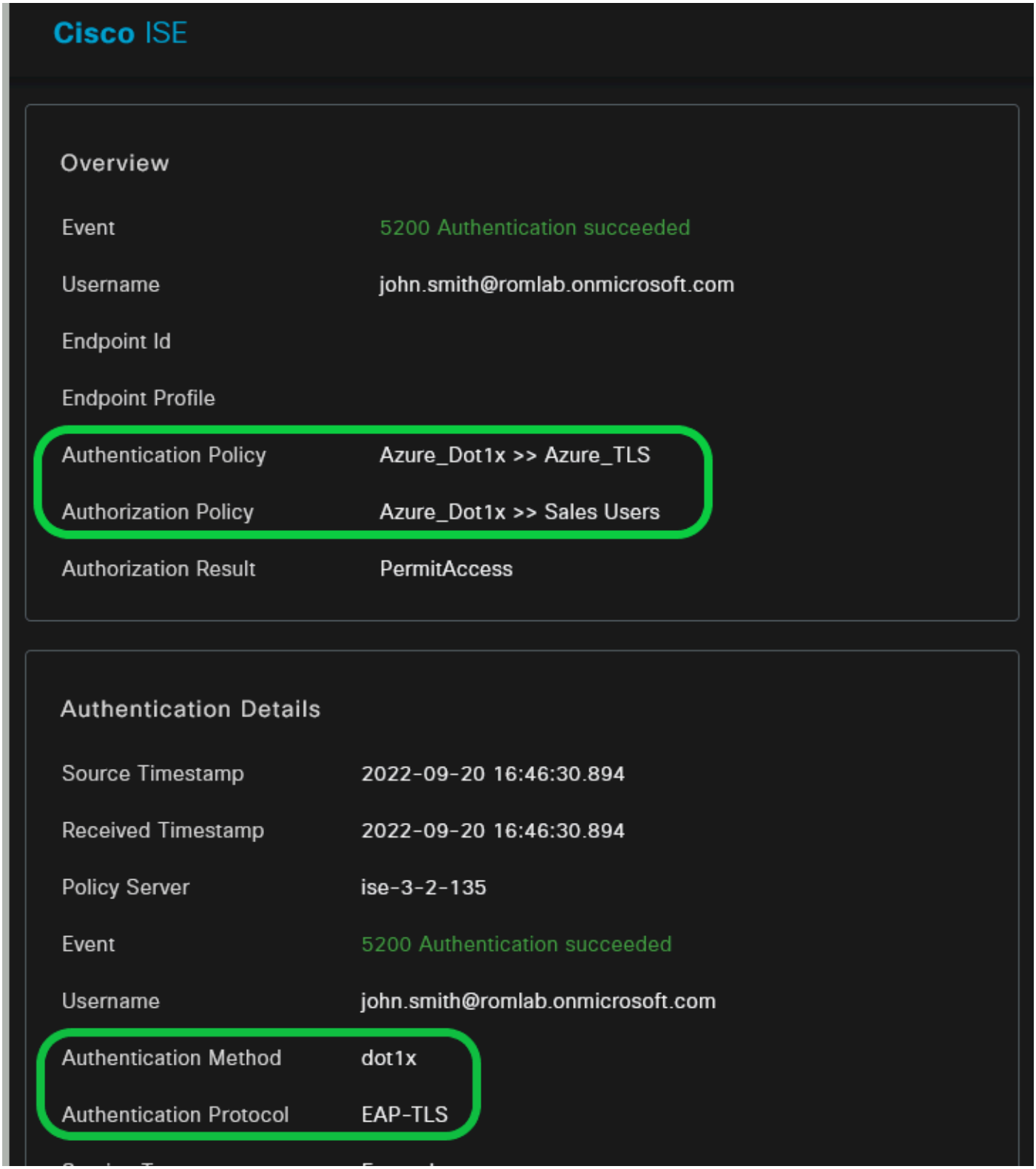
ISE验证

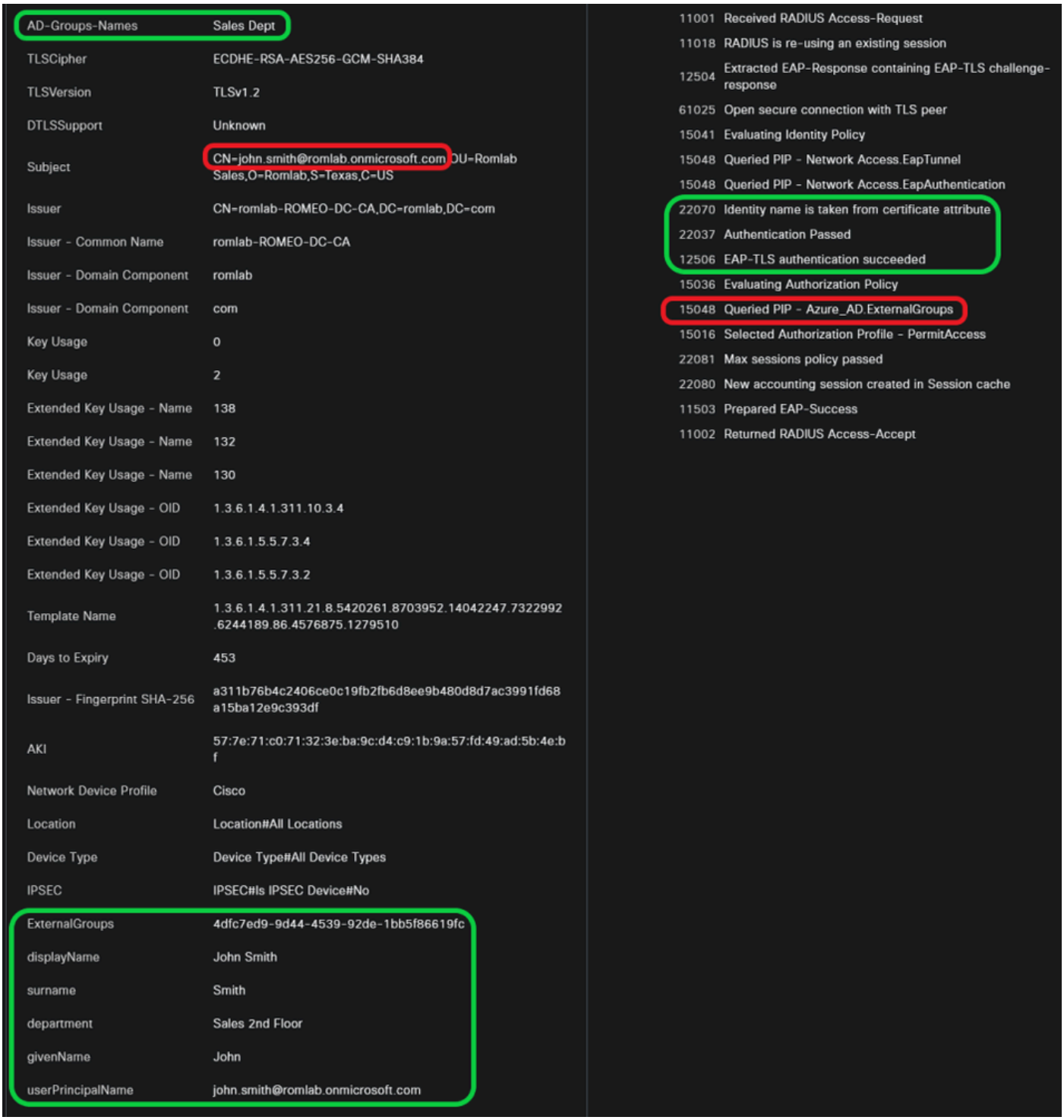
在Cisco ISE GUI中，点击Menu图标 ☰ 然后选择Operations > RADIUS > Live Logs进行网络身份验证(RADIUS)。



点击“详细信息”(Details)列中的放大镜图标，以查看详细的身份验证报告，并确认流是否按预期运行。

1. 验证身份验证/授权策略。
2. 身份验证方法/协议。
3. 从证书中获取的用户使用者名称。
4. 从Azure目录获取的用户组和其他属性。





故障排除

在ISE上启用调试

导航到Administration > System > Logging > Debug Log Configuration，将后续组件设置为指定级别。

节点	组件名称	日志级别	日志文件名

PSN	rest-id-store	调试	rest-id-store.log
PSN	运行时AAA	调试	prrt-server.log

注意：完成故障排除后，请记住重置调试。为此，请选择相关节点，然后单击重置为默认值。

日志片段

下面的摘录显示了流程的最后两个阶段，如前面的网络图部分所述。

1. ISE获取证书使用者名称(CN)并执行对Azure Graph API的查找，以获取用户的组以及该用户的其它属性。这在Azure端称为用户主体名称(UPN)。
2. ISE授权策略根据从Azure返回的用户属性进行评估。

Rest-id日志：

```
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
```

打印日志：

```
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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。