Configurar o EAP-TLS do Cisco ISE 3.2 com o Ative Diretory do Microsoft Azure

Contents

Introduction

Este documento descreve como configurar e solucionar problemas de políticas de autorização no ISE com base na associação de grupo do Azure AD e outros atributos de usuário com EAP-TLS ou TEAP como os protocolos de autenticação.

Contribuição de Emmanuel Cano, engenheiro de consultoria de segurança e Romeo Migisha, engenheiro de consultoria técnica

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity services engine (ISE)
- Microsoft Azure AD, assinatura e aplicativos
- EAP-TLS Autenticação

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE 3.2
- AD do Microsoft Azure

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

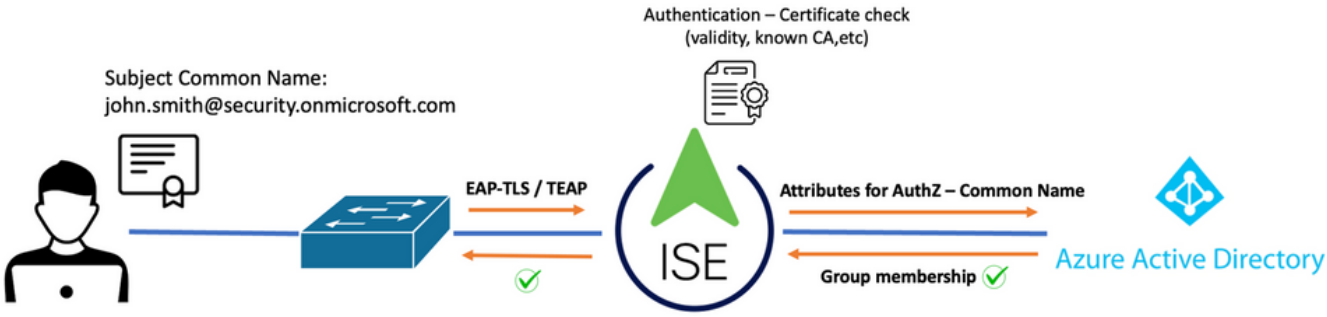
No ISE 3.0, é possível aproveitar a integração entre o ISE e o Azure Ative Diretory (AAD) para autenticar os usuários com base nos grupos e atributos do Azure AD por meio da comunicação ROPC (Resource Owner Password Credentials). Com o ISE 3.2, você pode configurar a autenticação baseada em certificado e os usuários podem ser autorizados com base em associações de grupo do Azure AD e outros atributos. O ISE consulta o Azure por meio da API de gráfico para buscar grupos e atributos para o usuário autenticado. Ele usa o Nome Comum do Requerente (CN) do certificado em relação ao Nome UPN no Azure.

> **Observação**: as autenticações baseadas em certificado podem ser EAP-TLS ou TEAP com EAP-TLS como o método interno. Em seguida, você pode selecionar atributos do Ative Diretory do Azure e adicioná-los ao dicionário do Cisco ISE. Esses atributos podem ser usados para autorização. Somente a autenticação de usuário é suportada.

Configurar

Diagrama de Rede

A próxima imagem fornece um exemplo de um diagrama de rede e fluxo de tráfego



Procedimento:

1. O certificado é enviado ao ISE por meio de EAP-TLS ou TEAP com EAP-TLS como o método interno.
2. O ISE avalia o certificado do usuário (período de validade, CA confiável, CRL e assim por diante).
3. O ISE pega o CN (nome da entidade) do certificado e faz uma pesquisa na API do Microsoft Graph para buscar os grupos do usuário e outros atributos para esse usuário. Isso é conhecido como nome UPN no Azure.
4. As políticas de Autorização do ISE são avaliadas em relação aos atributos do usuário retornados do Azure.

> **Observação**: você deve configurar e conceder as permissões da API do Graph para o aplicativo ISE no Microsoft Azure como mostrado abaixo:

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

Configurações

Configuração do ISE

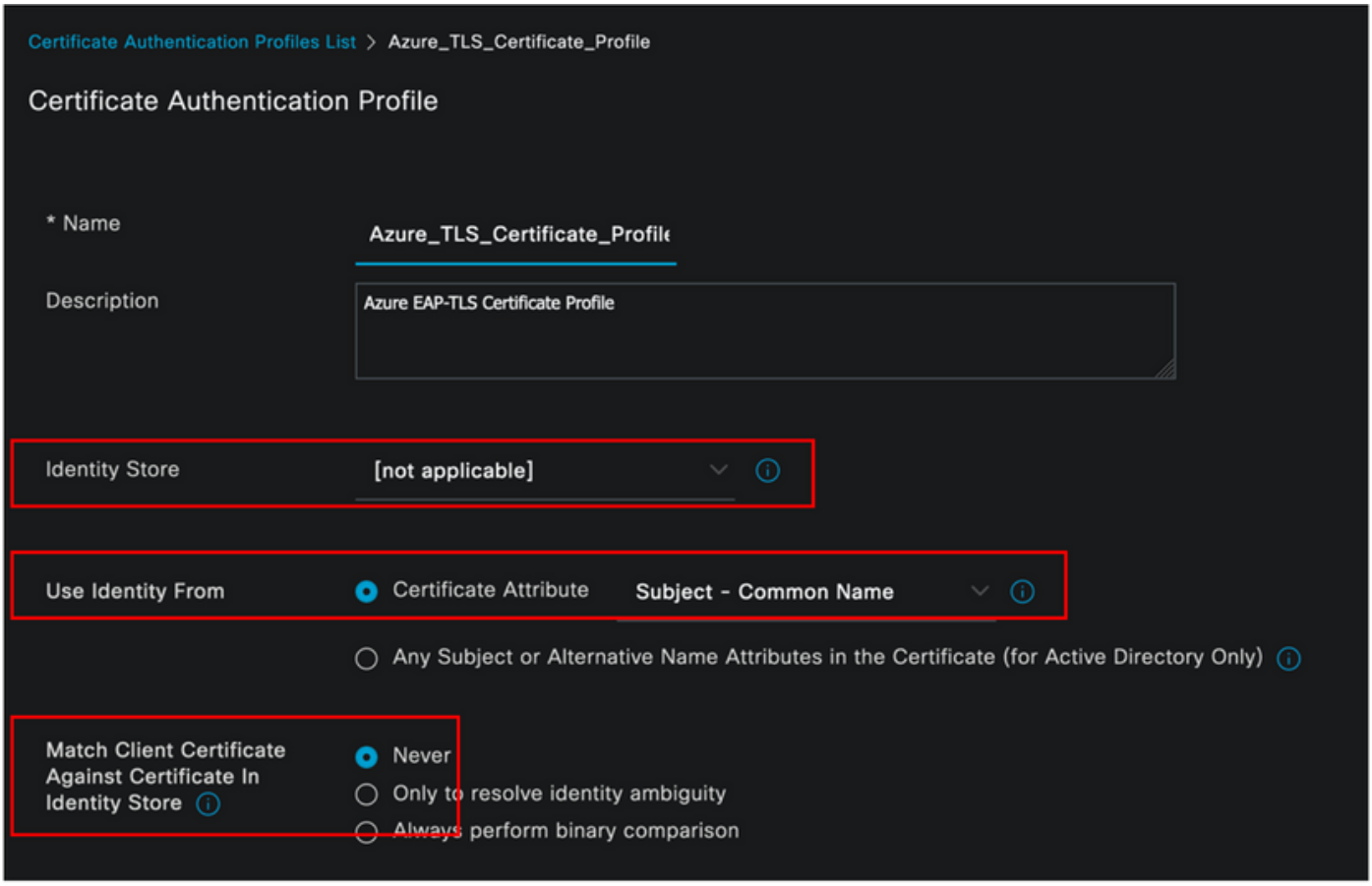
> **Observação**: a funcionalidade ROPC e a Integração entre o ISE e o Azure AD estão fora do escopo deste documento. É importante que grupos e atributos de usuário sejam adicionados do Azure. Consulte o guia de configuração aqui.

Configurar o Perfil de Autenticação de Certificado

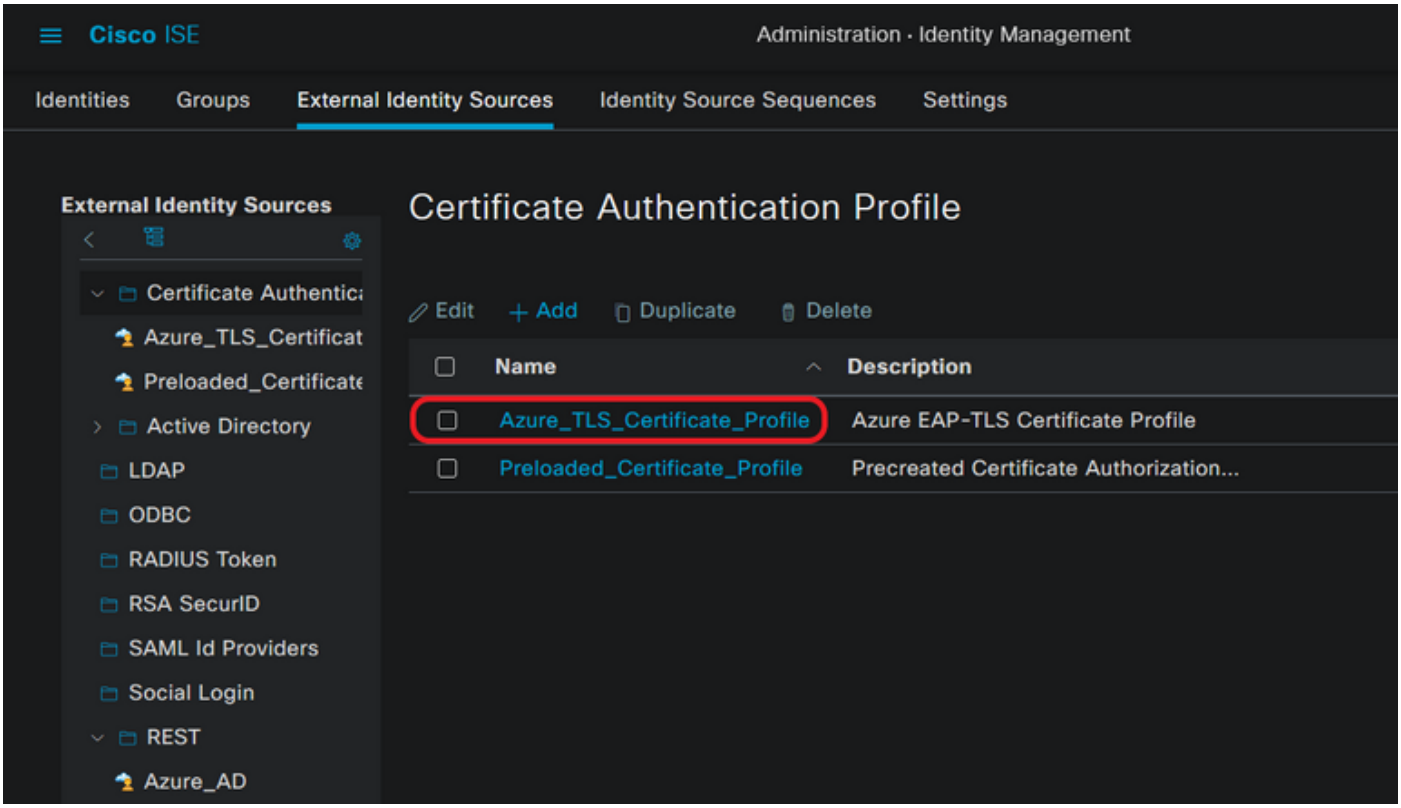
Etapa 1. Navegue até o ícone Menu localizado no canto superior esquerdo e selecione **Administração > Gerenciamento de Identidades > Origens de Identidades Externas.**

Etapa 2. Selecionar **Autenticação de certificado** Perfil e clique em **Adicionar.**

Etapa 3. Defina o nome, defina o **Repositório de Identidades** como [Não aplicável] e selecione Assunto - Nome comum em **Usar Identidade de** campo. Selecionar Nunca na Correspondência **Certificado do Cliente em relação ao Certificado no Repositório de Identidades** Campo.



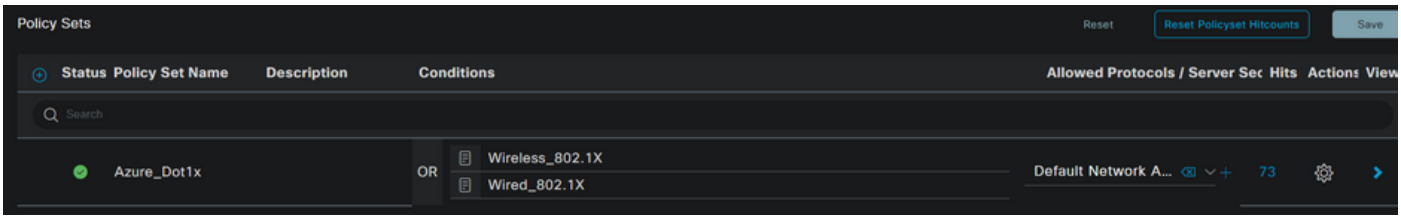
Etapa 4. Clique em **Save**



Etapa 5. Navegue até o ícone Menu localizado no canto superior esquerdo e selecione **Política > Conjuntos de Políticas.**

Etapa 6. Selecione o sinal de mais para criar um novo conjunto de políticas. Defina um nome

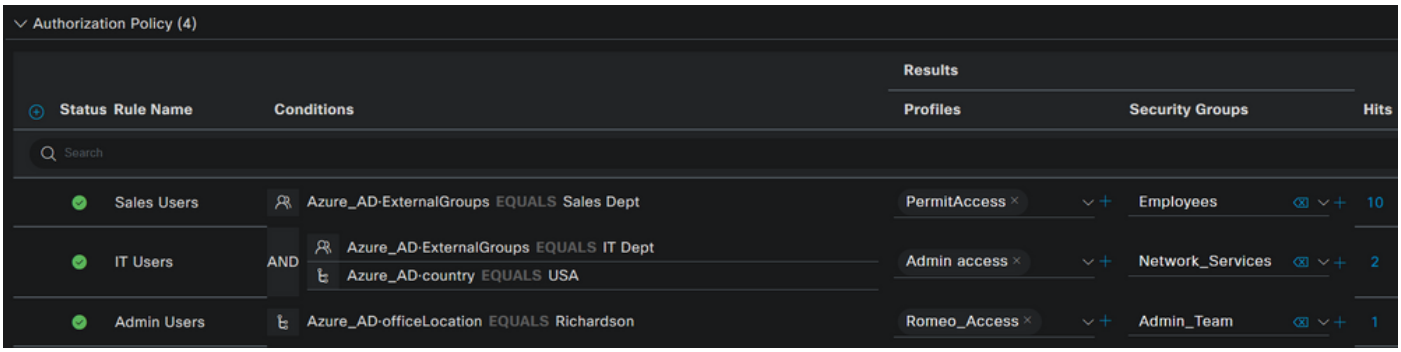
e selecione Wireless 802.1x ou wired 802.1x como condições. A opção Acesso à rede padrão é usada neste exemplo



Passo 7. Selecione a seta ao lado de Default Network Access (Acesso de rede padrão) para configurar Authentication and Authorization Policies (Políticas de autenticação e autorização).

Etapa 8. Selecione a opção Authentication Policy, defina um nome e adicione EAP-TLS como Network Access EAPAutenticação, será possível adicionar TEAP como Network Access EAPTunnel se TEAP for usado como o protocolo de autenticação. Selecione o perfil de autenticação de certificado criado na etapa 3 e clique em **Save**.

Etapa 9. Selecione a opção Política de Autorização, defina um nome e adicione atributos de usuário ou grupo do Azure AD como uma condição. Escolha o perfil ou o grupo de segurança em Resultados, dependendo do caso de uso e clique em **Save**.



User Configuration (Configuração do usuário).

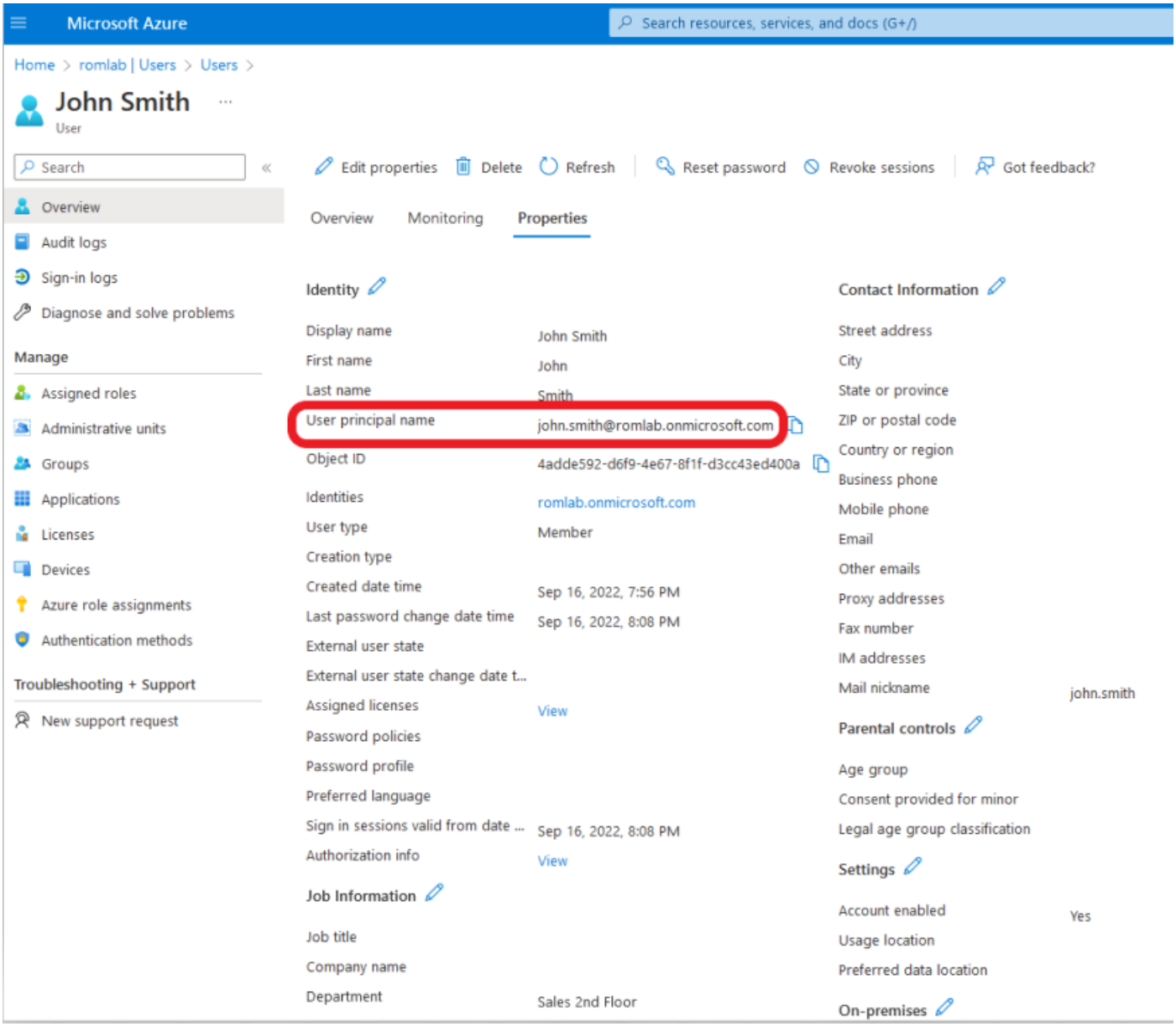
O Nome Comum do Requerente (CN) do certificado do usuário deve corresponder ao Nome UPN no Azure para recuperar a Associação de grupo do AD e os atributos do usuário que serão usados nas regras de autorização. Para que a autenticação seja bem-sucedida, a CA raiz e todos os certificados de CAs intermediários devem estar no ISE Trusted Store.

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

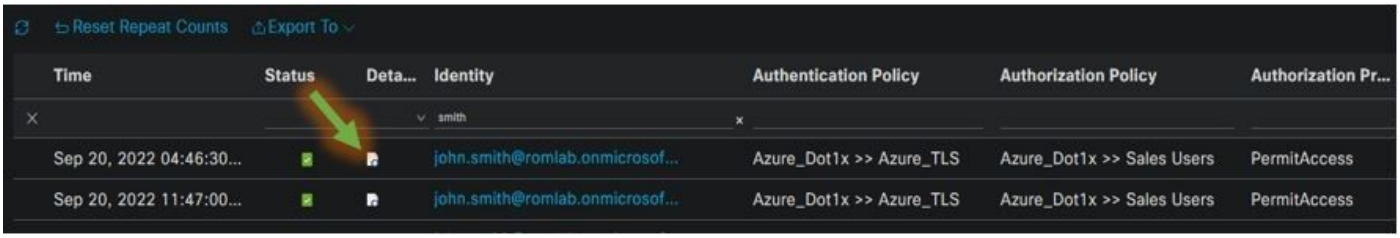
Subject Name	
Country or Region	US
State/Province	Texas
Organization	Romlab
Organizational Unit	Romlab Sales
Common Name	john.smith@romlab.onmicrosoft.com
Issuer Name	
Domain Component	com
Domain Component	romlab
Common Name	romlab-ROMEO-DC-CA
Serial Number	2C 00 00 00 36 00 3F CB D3 F1 52 B3 C2 00 01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



Verificar

verificação de ISE

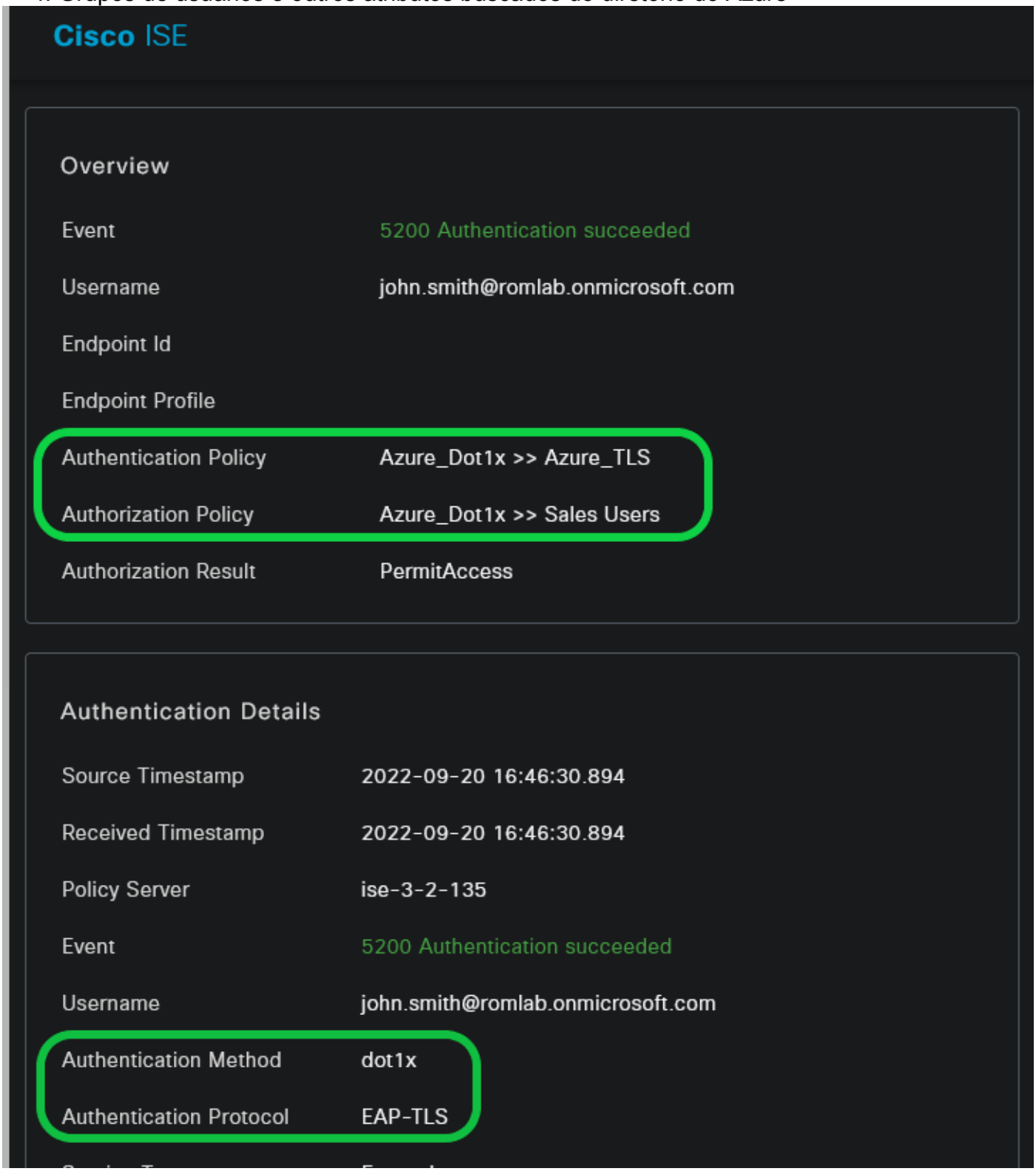
Na GUI do Cisco ISE, clique no ícone Menu e escolher **Operations > RADIUS > Live Logs para autenticações de rede (RADIUS).**

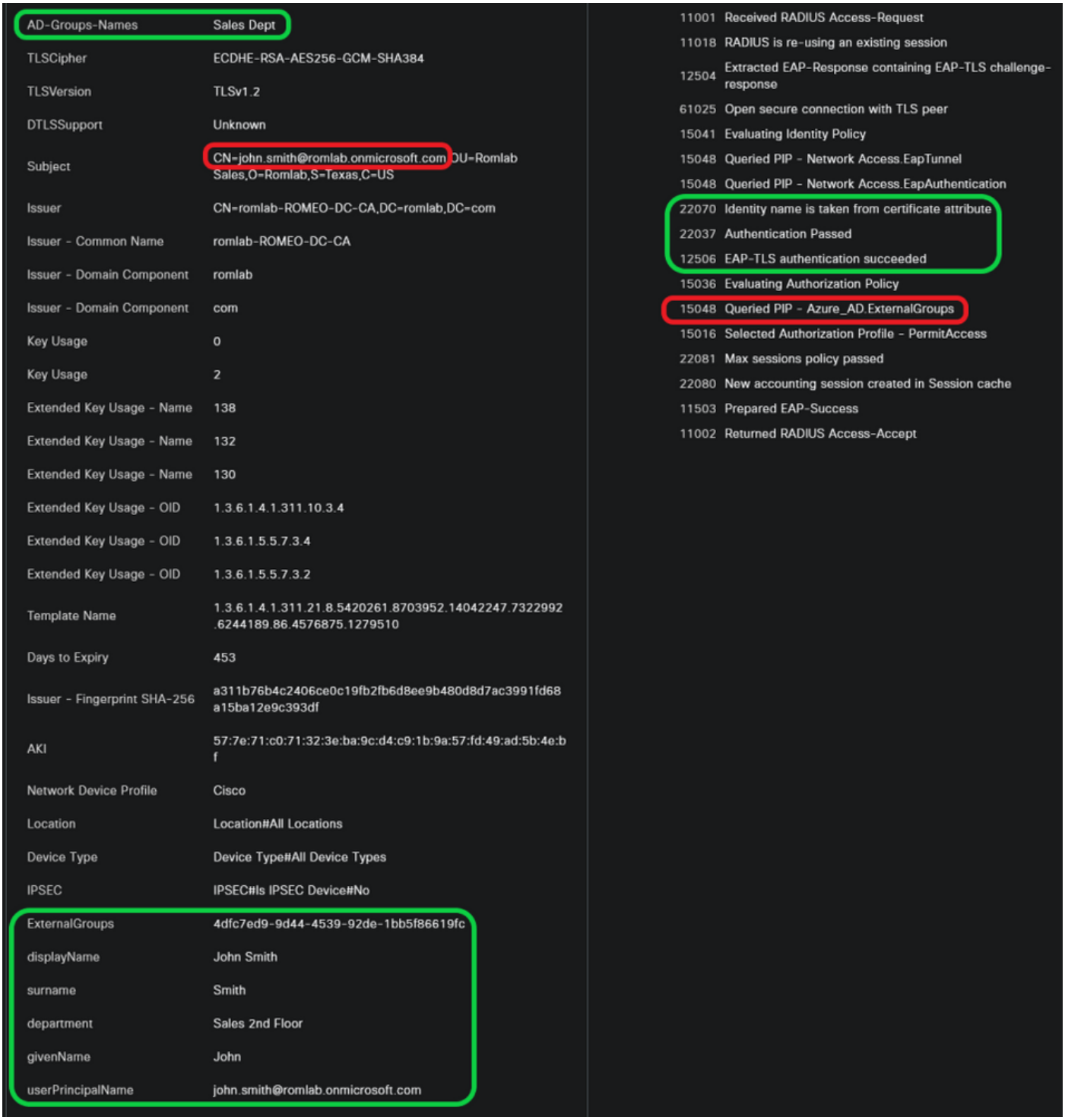


Clique no ícone de lupa na coluna Detalhes para exibir um relatório de autenticação detalhado e confirme se o fluxo funciona como esperado.

1. Verificar as políticas de autenticação/autorização
2. Método/protocolo de autenticação

3. Nome da entidade do usuário obtido do certificado
4. Grupos de usuários e outros atributos buscados do diretório do Azure





Troubleshoot

Habilitar depurações no ISE

Navegue até **Administração > Sistema > Registro > Configuração do Log de Depuração** para definir os próximos componentes para o nível especificado.

Nó	Nome do componente	Nível de log	Nome do arquivo de log
PSN	rest-id-store	Debug	rest-id-store.log
PSN	runtime-AAA	Debug	prt-server.log

> **Observação**: quando terminar de solucionar problemas, lembre-se de redefinir as depurações. Para fazer isso, selecione o nó relacionado e clique em "Redefinir para

padrão".

Registra trechos

Os próximos trechos mostram as duas últimas fases do fluxo, como mencionado anteriormente na seção do diagrama de rede.

1. O ISE pega o CN (nome da entidade) do certificado e executa uma pesquisa na API do Azure Graph para buscar grupos de usuários e outros atributos para esse usuário. Isso é conhecido como nome UPN no Azure.
2. As políticas de Autorização do ISE são avaliadas em relação aos atributos do usuário retornados do Azure.

Logs 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
```

Logs de porta:

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,userPrincipalName

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.