Configurar a Autenticação de Fator da Máquina Dois para Acesso do Candidato

Contents

Introdução

Este documento descreve as etapas necessárias para configurar a autenticação de dois fatores com a máquina e a autenticação dot1x.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine
- Configuração do Cisco Catalyst
- IEEE802.1X

Componentes Utilizados

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2019

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

O nome de domínio configurado no Windows Server 2019 é ad.rem-xxx.com, usado como exemplo neste documento.

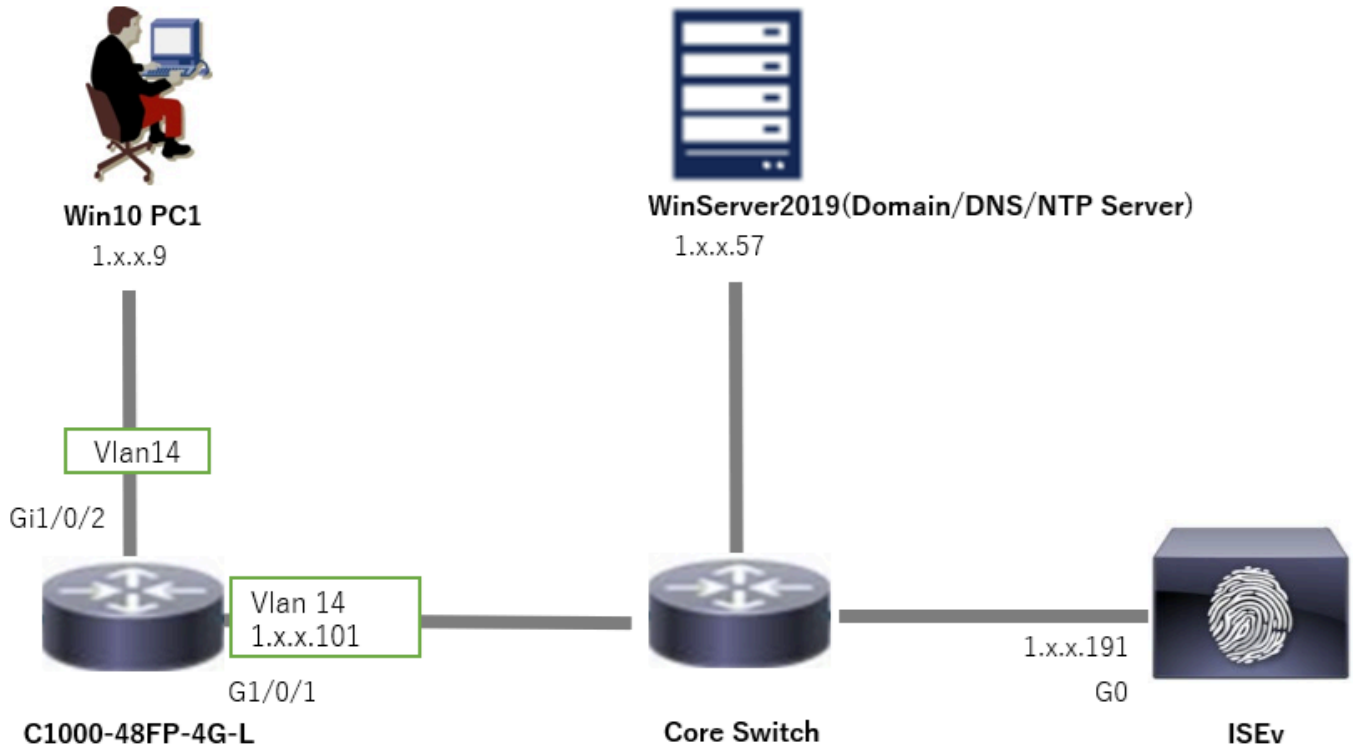


Diagrama de Rede

Informações de Apoio

A autenticação de máquina é um processo de segurança que verifica a identidade de um dispositivo que busca acesso a uma rede ou sistema. Diferentemente da autenticação de usuário, que verifica a identidade de uma pessoa com base em credenciais como um nome de usuário e senha, a autenticação de máquina se concentra na validação do próprio dispositivo. Isso é feito frequentemente usando certificados digitais ou chaves de segurança que são exclusivas do dispositivo.

Ao usar a autenticação de máquina e usuário em conjunto, uma organização pode garantir que apenas dispositivos e usuários autorizados possam acessar sua rede, fornecendo, assim, um ambiente mais seguro. Esse método de autenticação de dois fatores é particularmente útil para proteger informações confidenciais e estar em conformidade com padrões regulatórios rigorosos.

Configurações

Configuração no C1000

Essa é a configuração mínima na CLI do C1000.

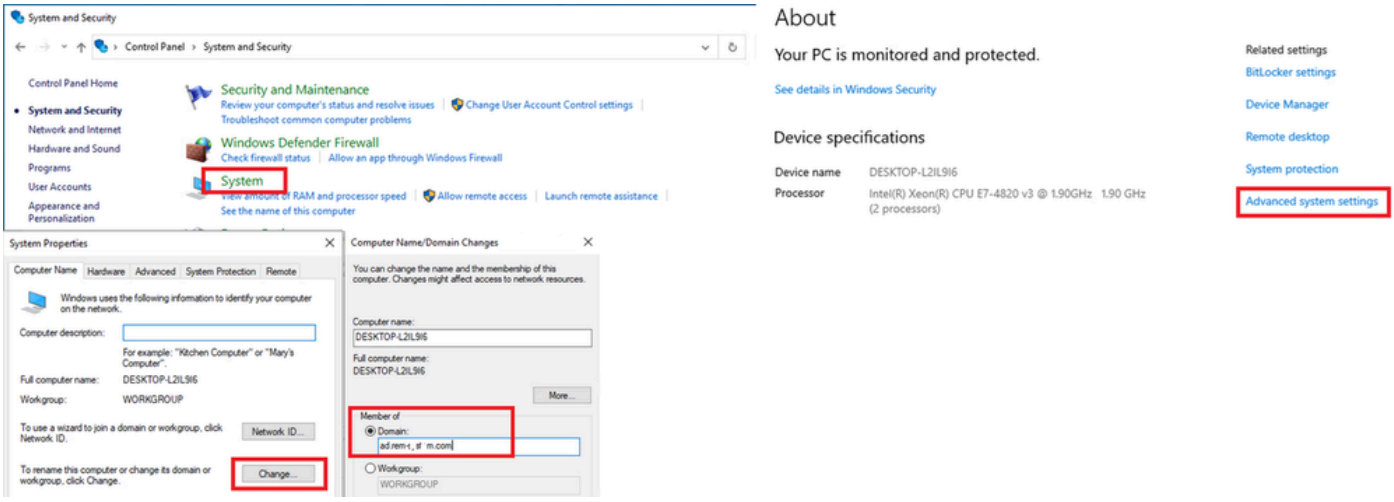
```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123
```

```
aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configuração no PC com Windows

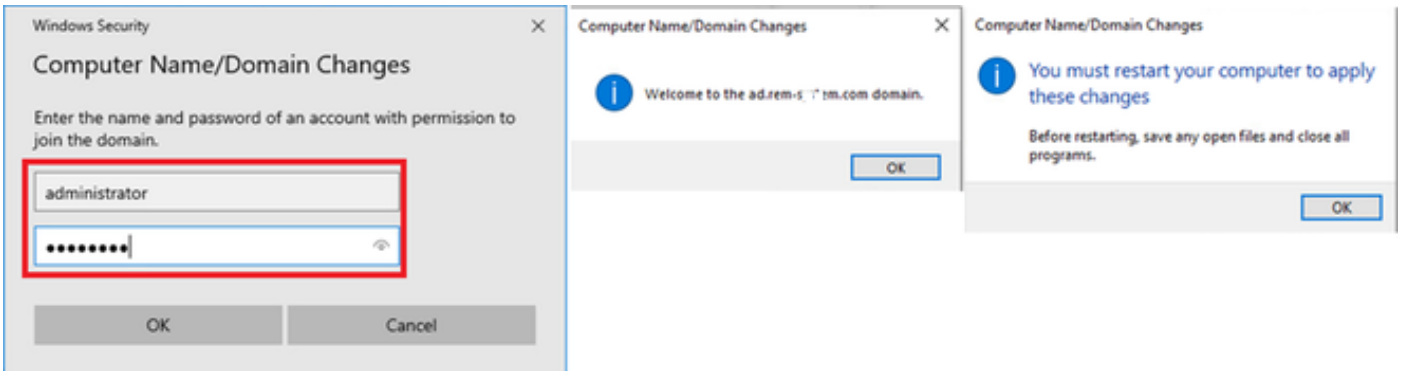
Etapa 1. Adicionar computador ao Domínio do AD

Navegue para Painel de controle > Sistema e segurança, clique em Sistema e em Configurações avançadas do sistema. Na janela Propriedades do sistema, clique em Alterar, selecione Domínio e insira o nome do domínio.



Adicionar computador ao Domínio do AD

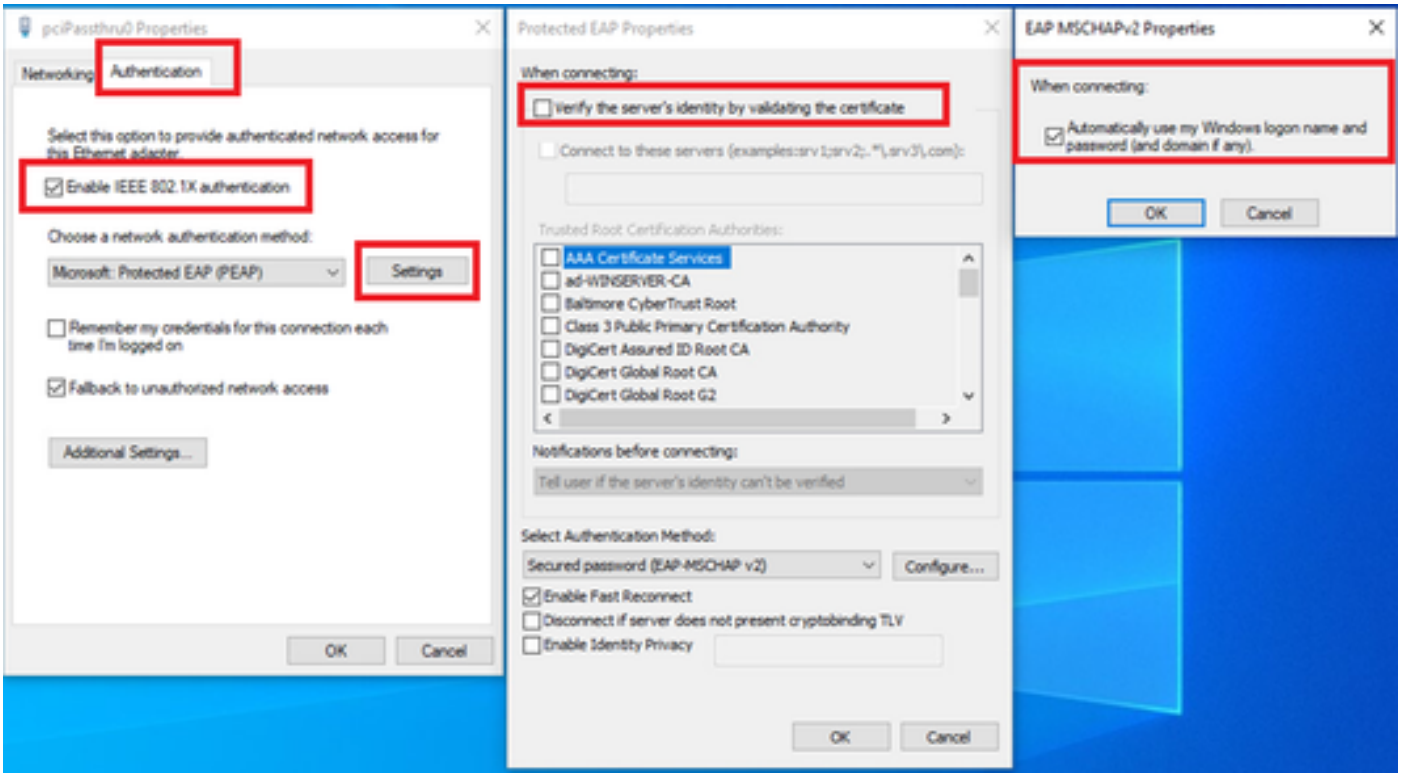
Na janela Segurança do Windows, insira o nome de usuário e a senha do servidor de domínio.



Inserir nome de usuário e senha

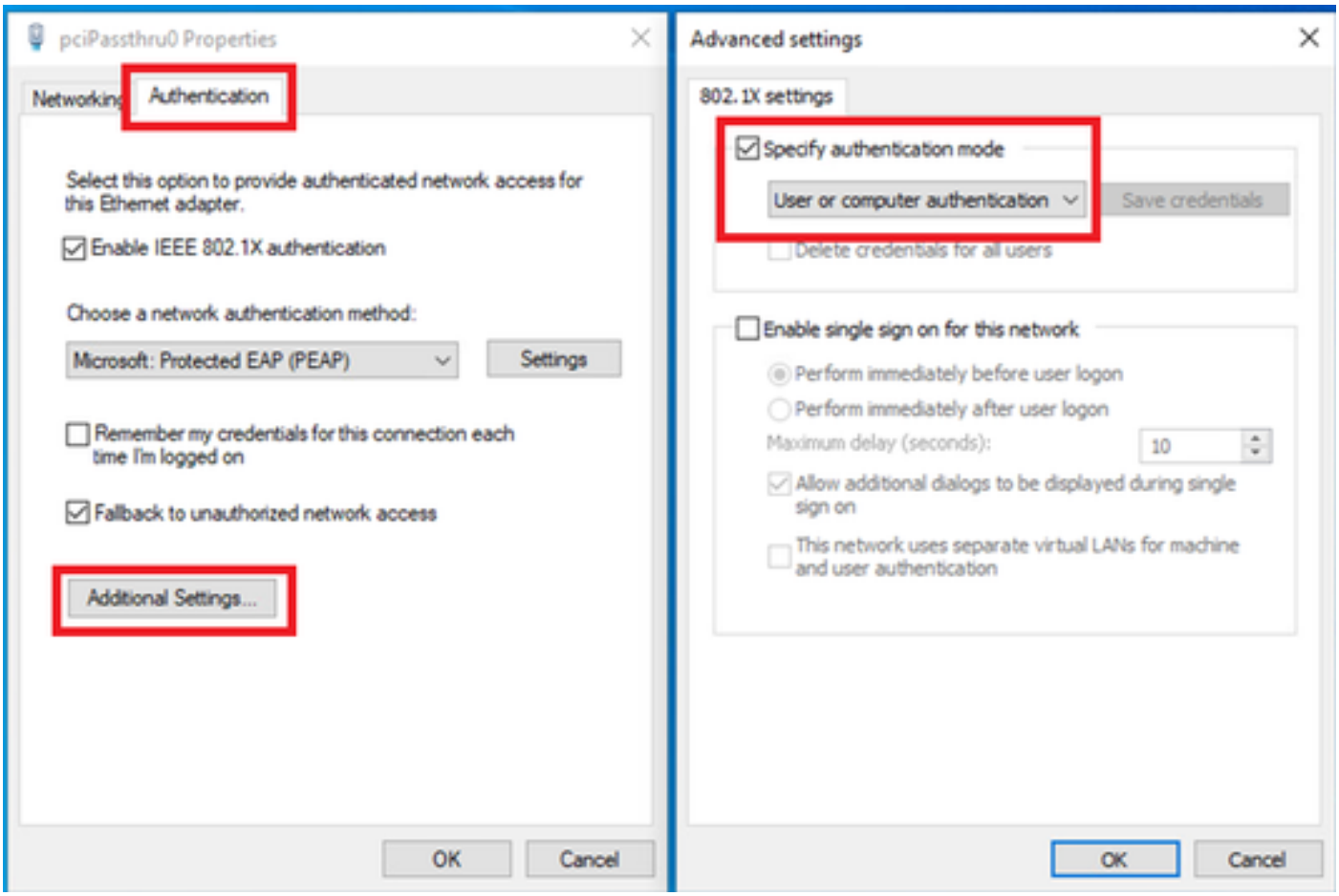
Etapa 2. Configurar autenticação de usuário

Navegue até Authentication, marque Enable IEEE 802.1X authentication. Clique em Settings na janela Protected EAP Properties, desmarque Verify the server's identity by validating the certificate e clique em Configure. Na janela Propriedades de EAP MSCHAPv2, marque Usar automaticamente meu nome e senha de logon do Windows (e o domínio, se houver) para usar o nome de usuário inserido durante o logon de máquina do Windows para autenticação de usuário.



Habilitar Autenticação de Usuário

Navegue até Authentication, verifique Additional Settings. Selecione User or computer authentication na lista suspensa.

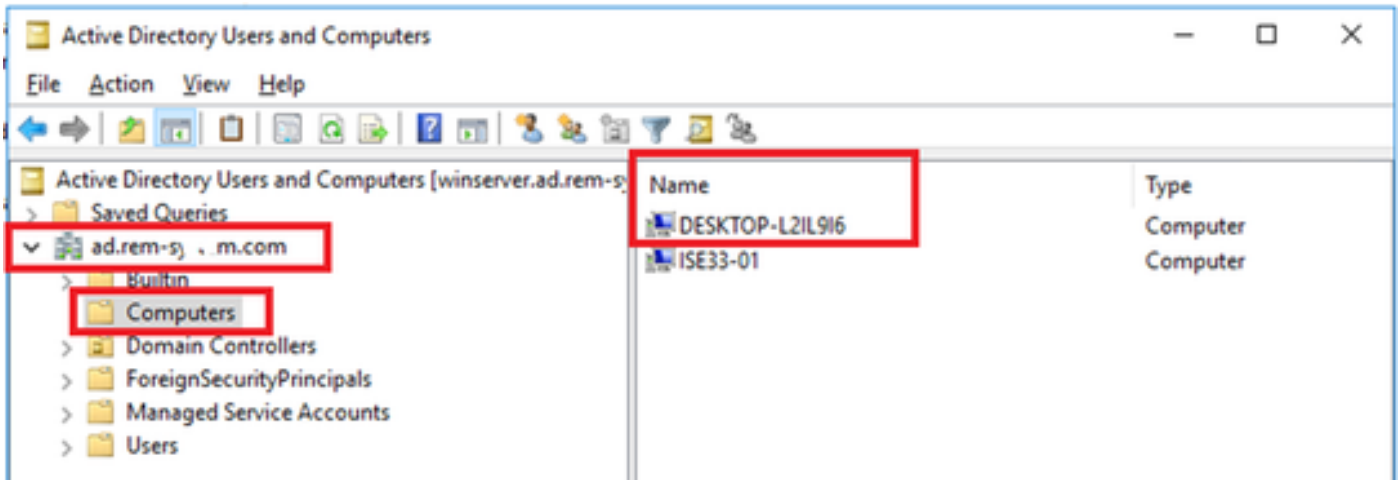


Especificar Modo de Autenticação

Configuração no Windows Server

Etapa 1. Confirmar computadores de domínio

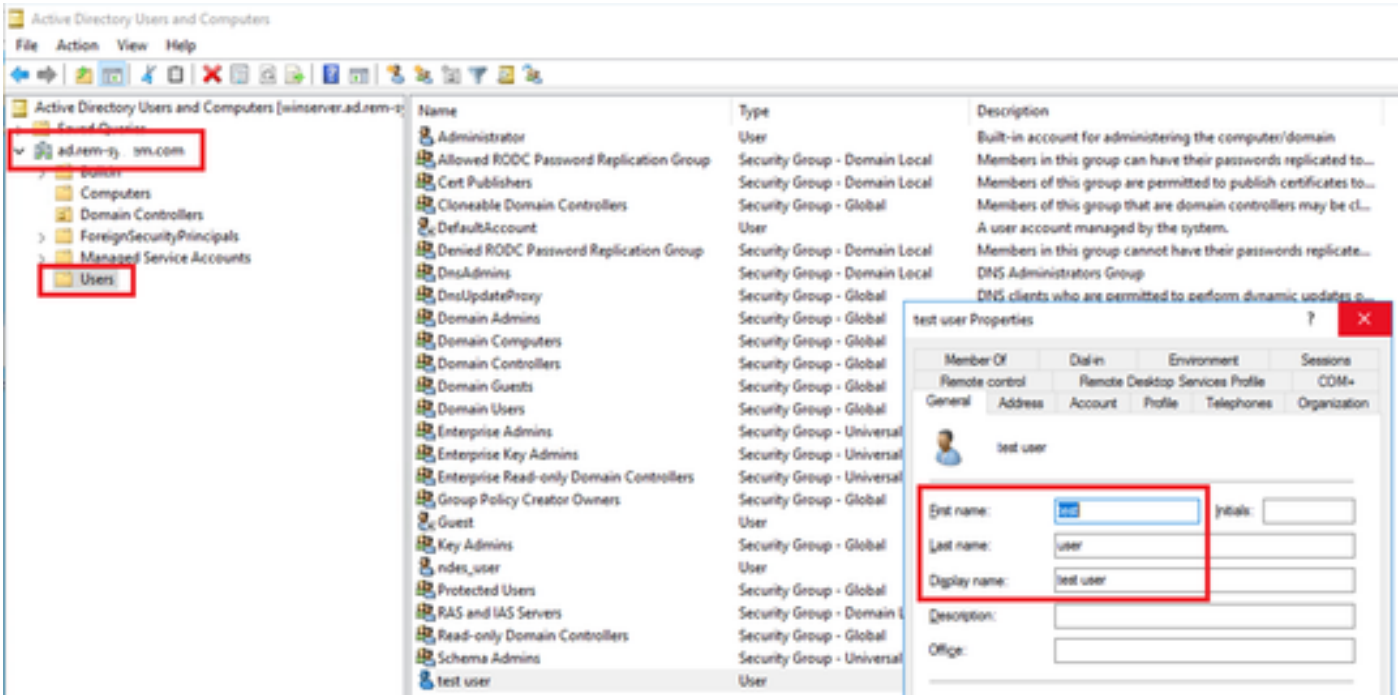
Navegue até Usuários e computadores do Ative Diretory, clique em Computadores. Confirme se o Win10 PC1 está listado no domínio.



Confirmar computador de domínio

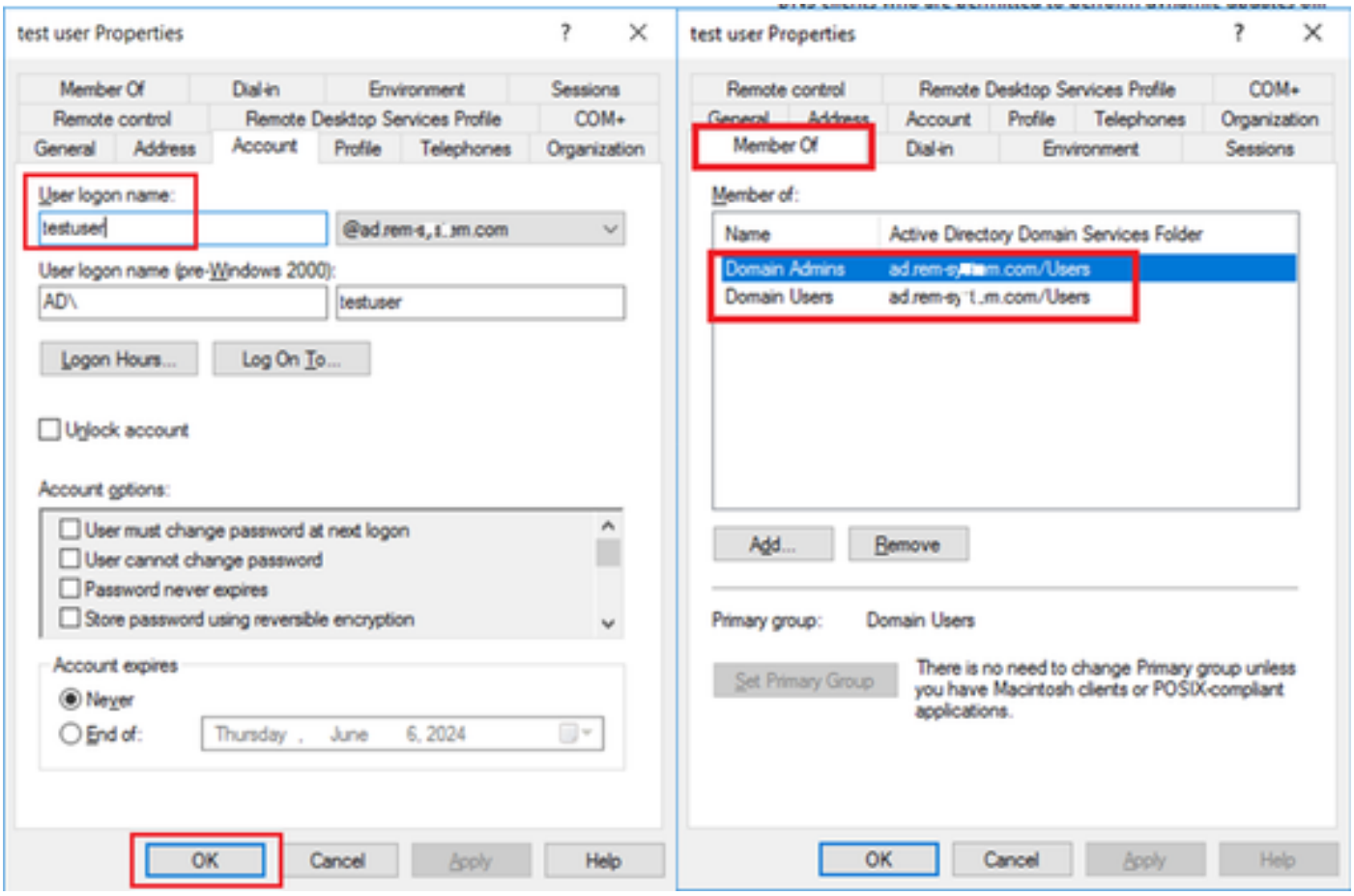
Etapa 2. Adicionar usuário de domínio

Navegue até Usuários e computadores do Ative Diretory, clique em Usuários. Adicionar usuário de teste como usuário de domínio.



Adicionar usuário de domínio

Adicione o usuário de domínio ao membro de Admins. do Domínio e Usuários do Domínio.

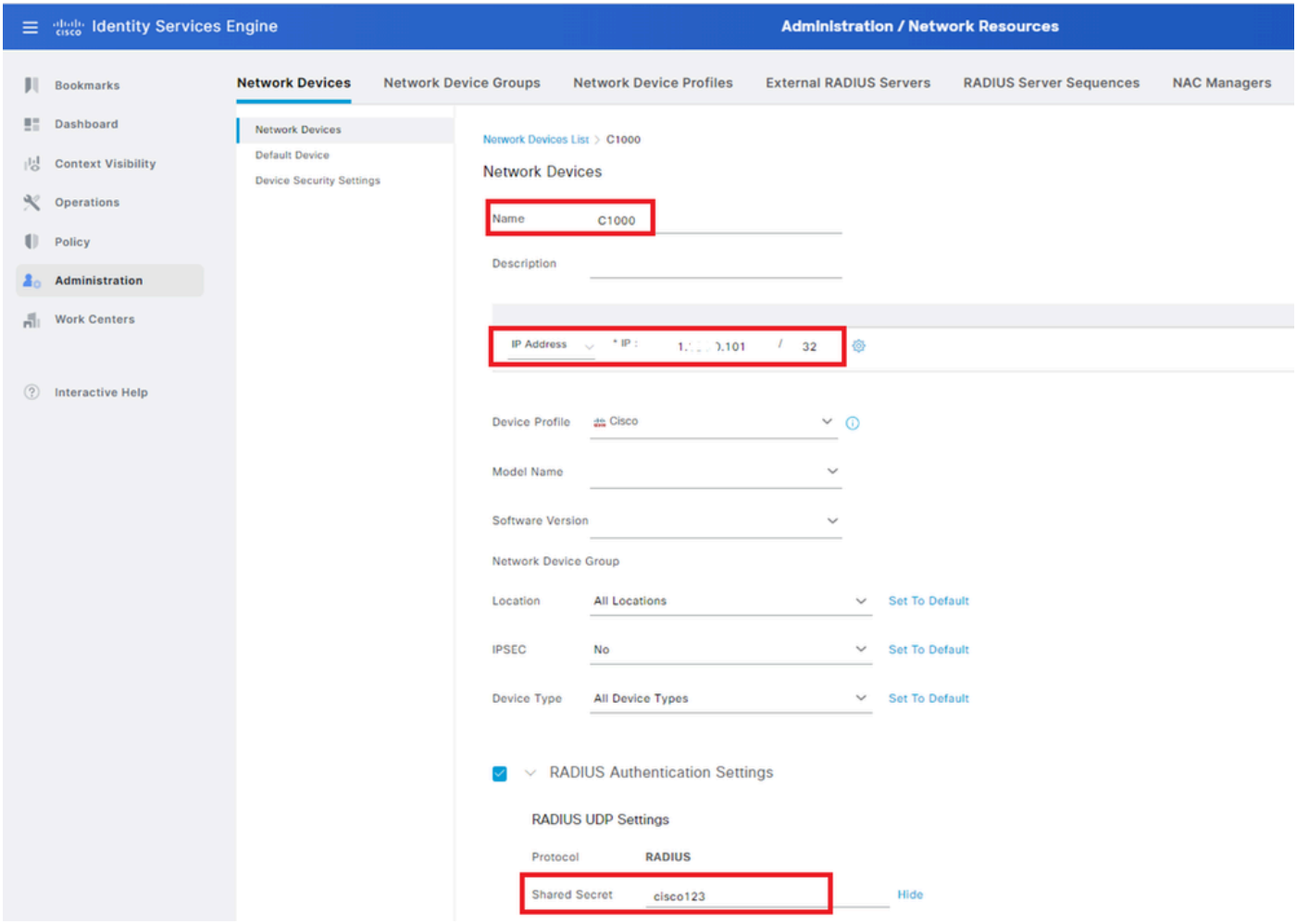


Admins. e Usuários do Domínio

Configuração no ISE

Etapa 1. Adicionar dispositivo

Navegue até Administração > Dispositivos de rede, clique no botão Adicionar para adicionar o dispositivo C1000.

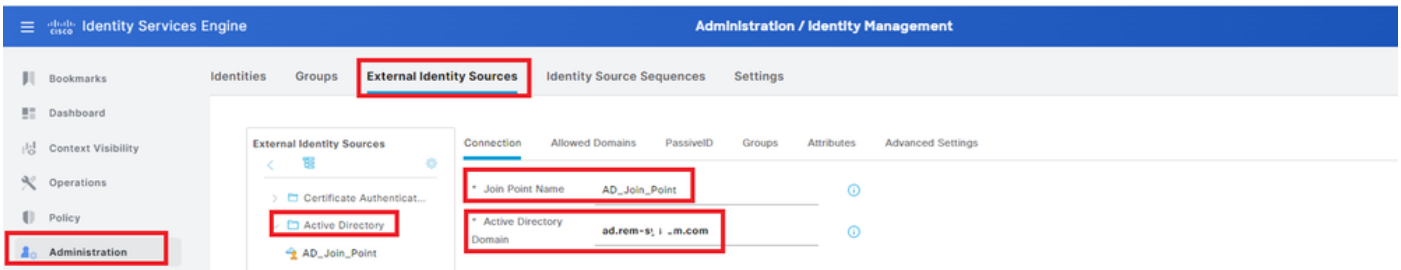


Adicionar dispositivo

Etapa 2. Adicionar Ative Diretory

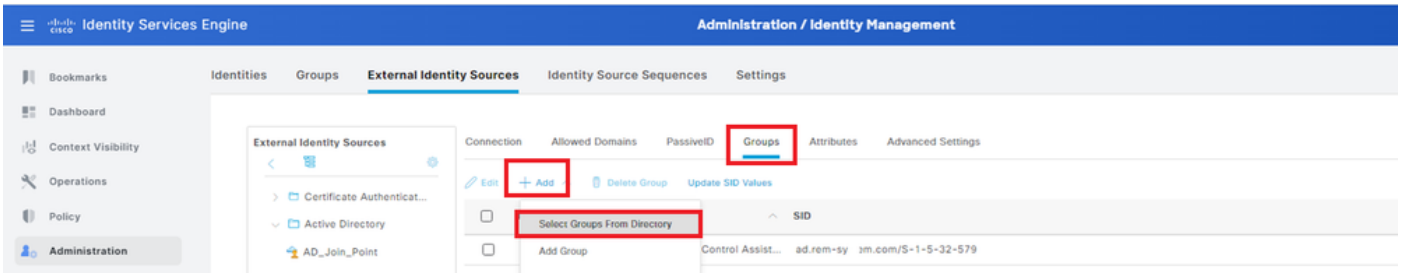
Navegue para Administração > Fontes de identidade externas > Ative Diretory, clique na guia Conexão e adicione o Ative Diretory ao ISE.

- Nome do ponto de junção: AD_Join_Point
- Domínio do Ative Diretory: ad.rem-xxx.com



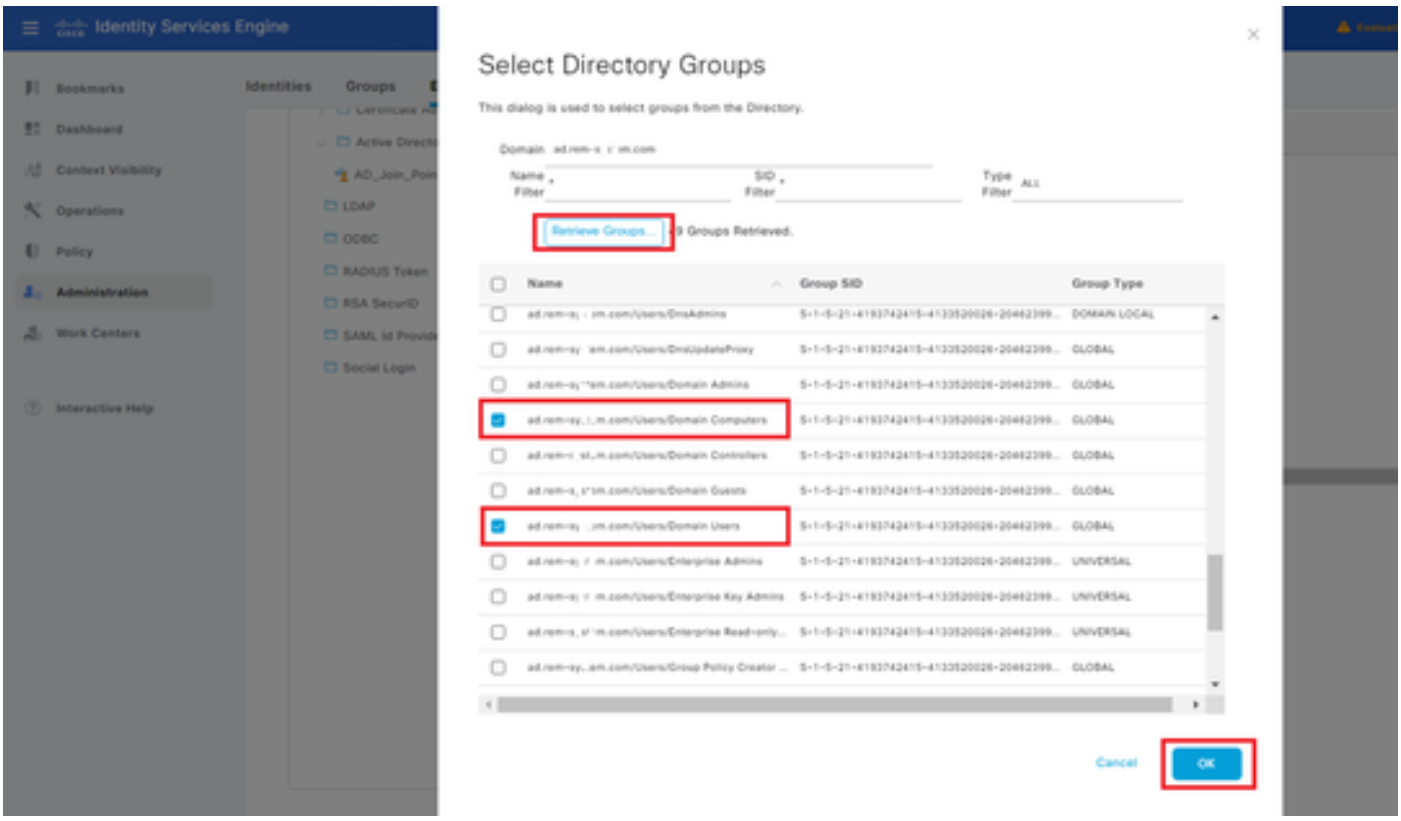
Adicionar Ative Diretory

Navegue até a guia Grupos e selecione Selecionar grupos do diretório na lista suspensa.



Selecionar grupos do diretório

Clique em Recuperar grupos na lista suspensa. Marque ad.rem-xxx.com/Users/Domain Computers e ad.rem-xxx.com/Users/Domain Users e clique em OK.



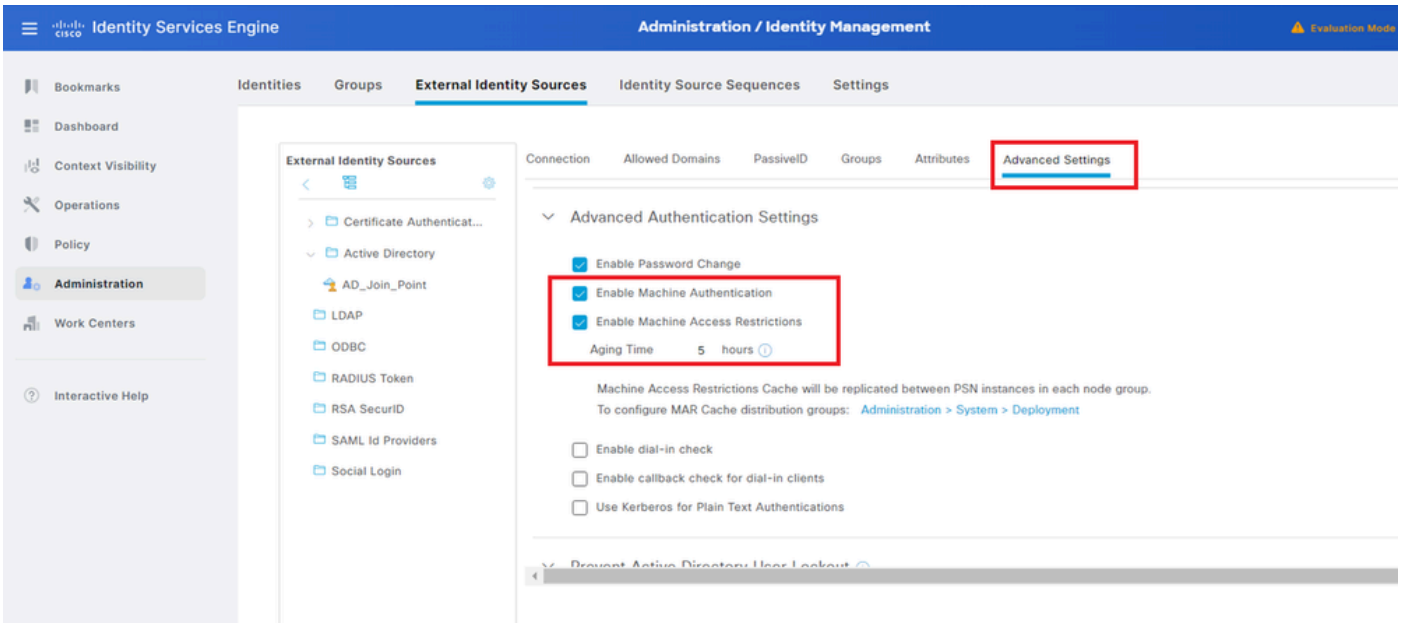
Adicionar computadores e usuários de domínio

Etapa 3. Confirmar Configuração de Autenticação do Computador

Navegue até a guia Advanced Settings, confirme a configuração de autenticação de máquina.

- Habilitar Autenticação da Máquina: para habilitar a autenticação da máquina
- Habilitar Restrição de Acesso à Máquina: para combinar autenticação de usuário e máquina antes da autorização

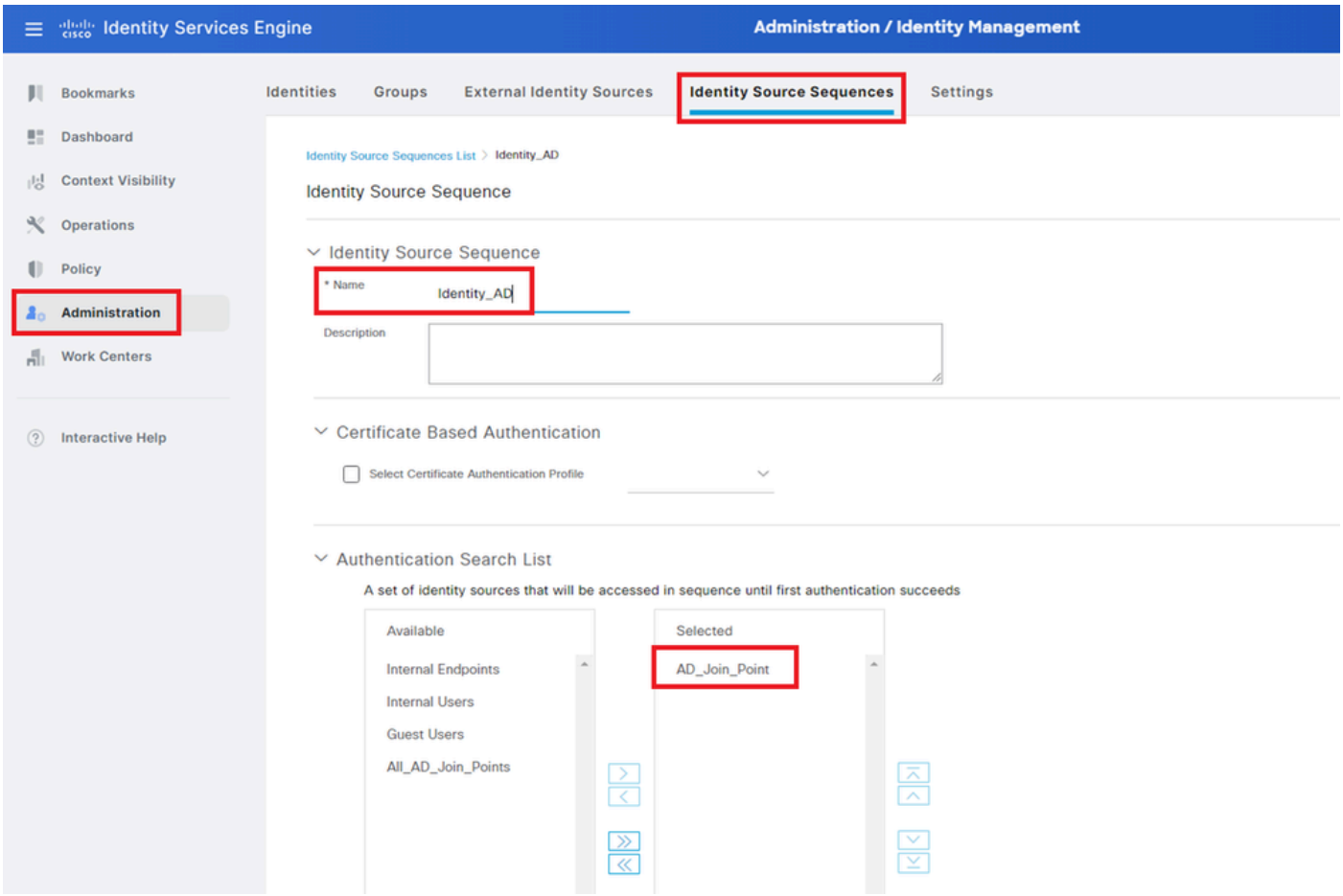
Observação: o intervalo válido de tempo de envelhecimento é de 1 a 8760.



Etapa 4. Adicionar Sequências de Origem de Identidade

Navegue até Administração > Sequências de origem de identidade, adicione uma Sequência de origem de identidade.

- Nome: Identity_AD
- Lista de pesquisa de autenticação: AD_Join_Point

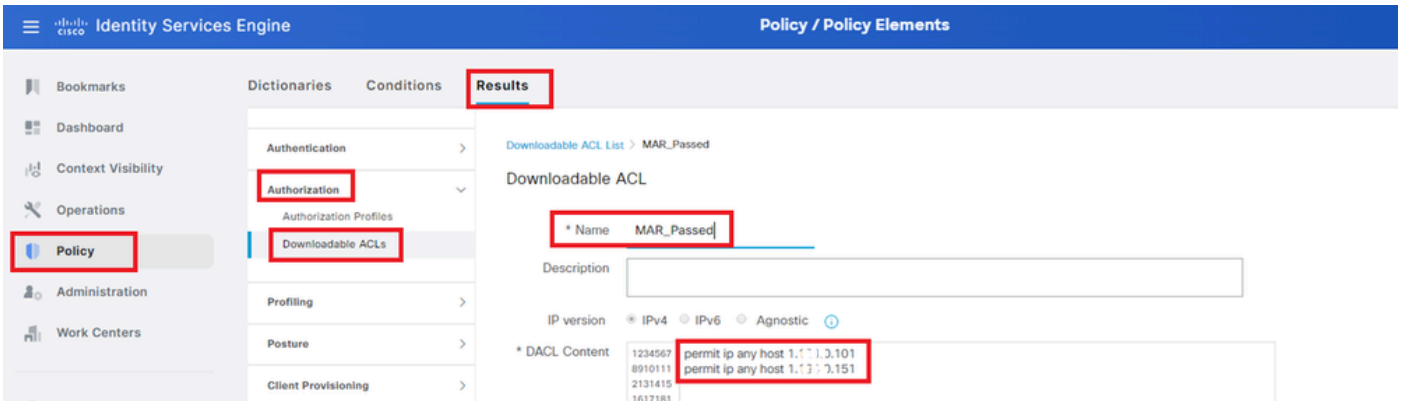


Adicionar Sequências de Origem de Identidade

Etapa 5. Adicionar DACL e perfil de autorização

Navegue até Policy > Results > Authorization > Downloadable ACLs e adicione um DACL.

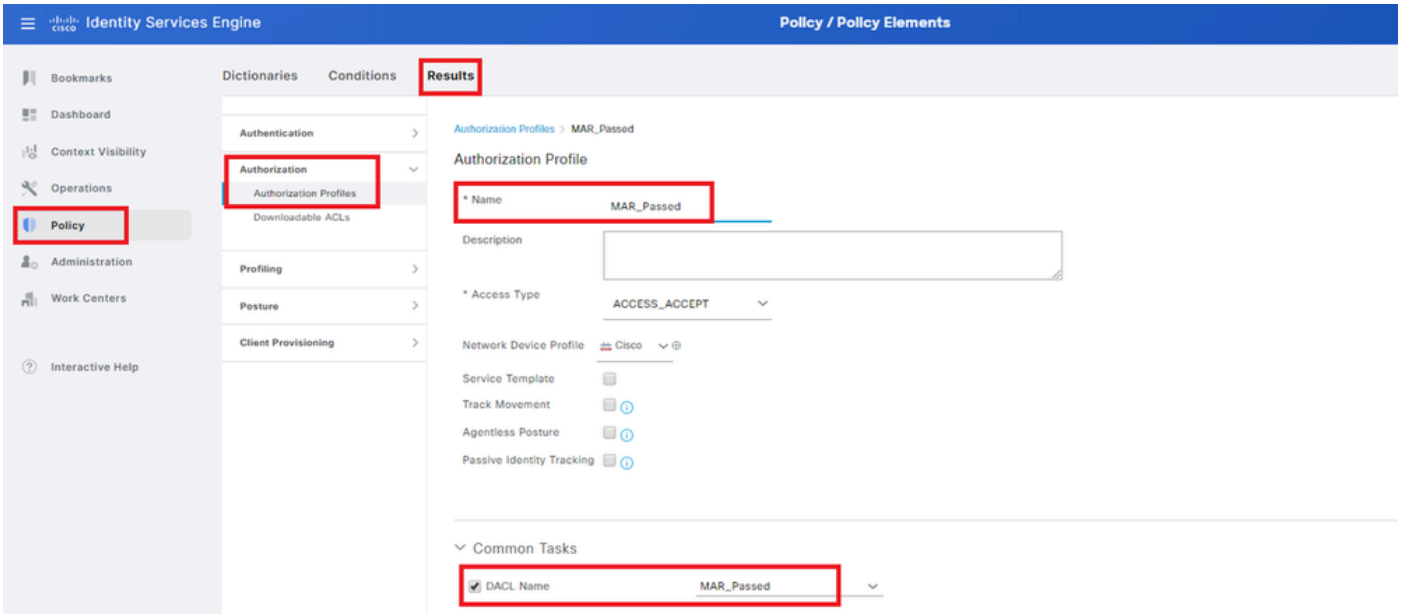
- Nome: MAR_Passed
- Conteúdo da DACL: permit ip any host 1.x.x.101 e permit ip any host 1.x.x.105



Adicionar DACL

Navegue até Política > Resultados > Autorização > Perfis de autorização, adicione um perfil de autorização.

- Nome: MAR_Passed
- Nome DACL: MAR_Passed

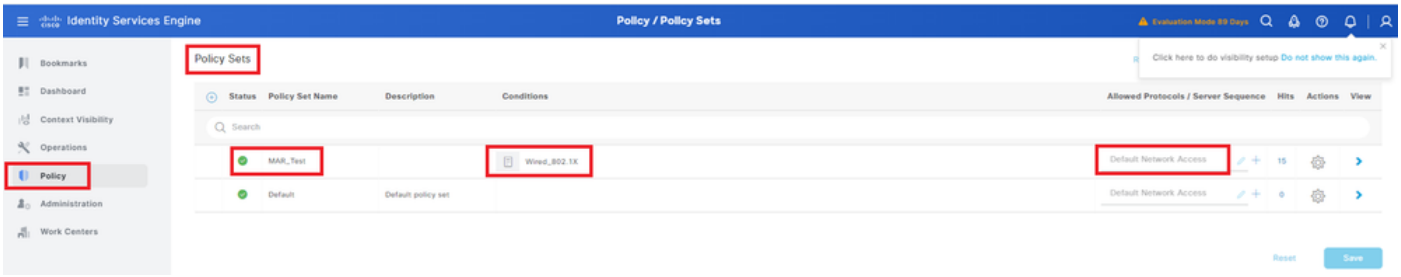


Adicionar perfil de autorização

Etapa 6. Adicionar conjunto de políticas

Navegue para Política > Conjuntos de políticas, clique em + para adicionar um conjunto de políticas.

- Nome do Conjunto de Políticas: MAR_Test
- Condições: Wired_802.1X
- Protocolos Permitidos/Sequência de Servidores: Acesso Padrão à Rede

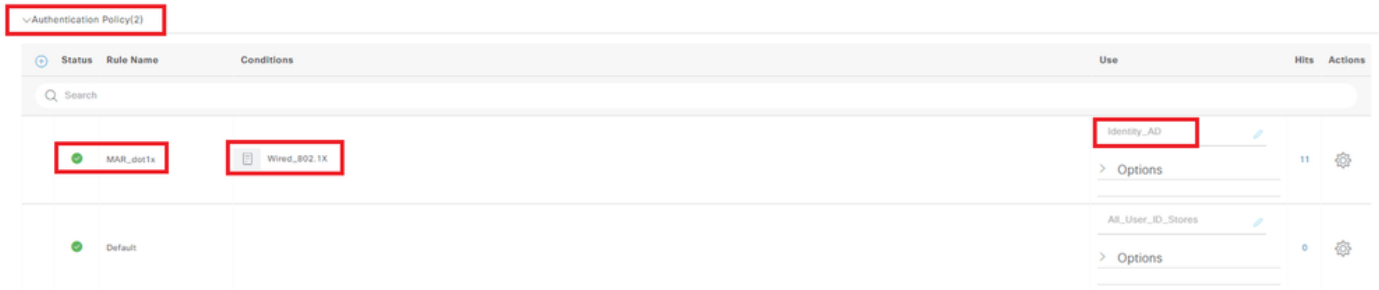


Adicionar conjunto de políticas

Passo 7. Adicionar política de autenticação

Navegue até Policy Sets, clique em MAR_Test para adicionar uma política de autenticação.

- Nome da regra: MAR_dot1x
- Condições: Wired_802.1X
- Uso: Identity_AD



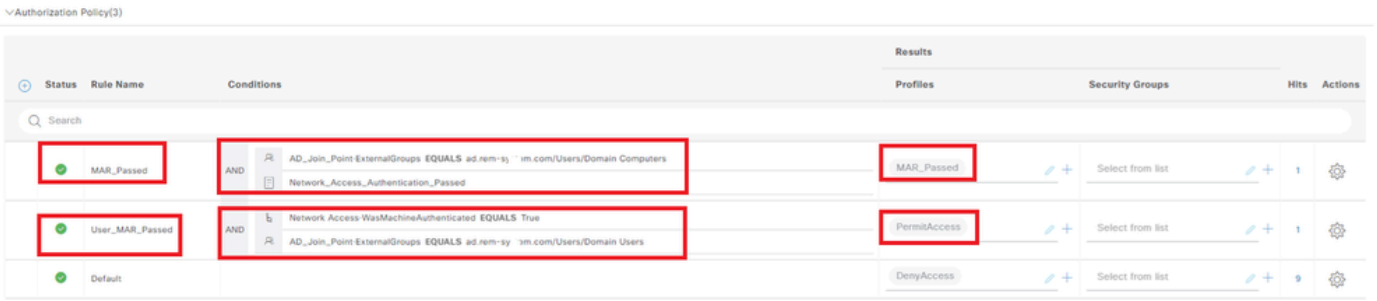
Adicionar política de autenticação

Etapa 8. Adicionar Política de Autorização

Navegue até Policy Sets, clique em MAR_Test para adicionar uma política de autorização.

- Nome da Regra: MAR_Passed
- Condições: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computadores AND Network_Access_Authentication_Passed
- Resultados: MAR_Passed

- Nome da regra: User_MAR_Passed
- Condições: Network Access·WasMachineAuthenticated EQUALS True AND AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Usuários
- Resultados: PermitAccess



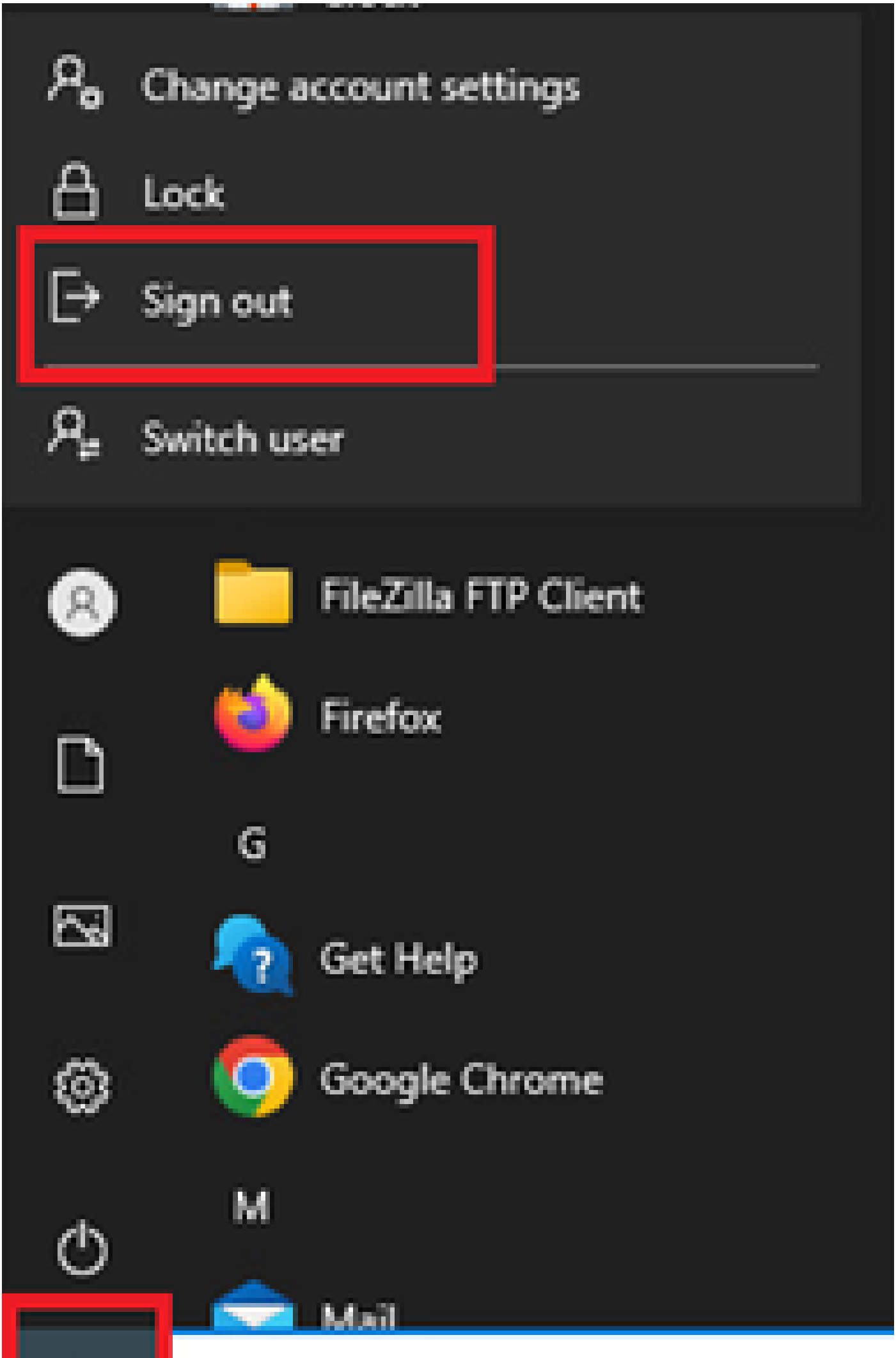
Adicionar política de Autorização

Verificar

Padrão 1. Autenticação de máquina e autenticação de usuário

Etapa 1. Sair do Windows PC

Clique no botão Sair do Win10 PC1 para disparar a autenticação da máquina.


Change account settings
Lock
Sign out
Switch user
FileZilla FTP Client
Firefox
G
Get Help
Google Chrome
M
Mail

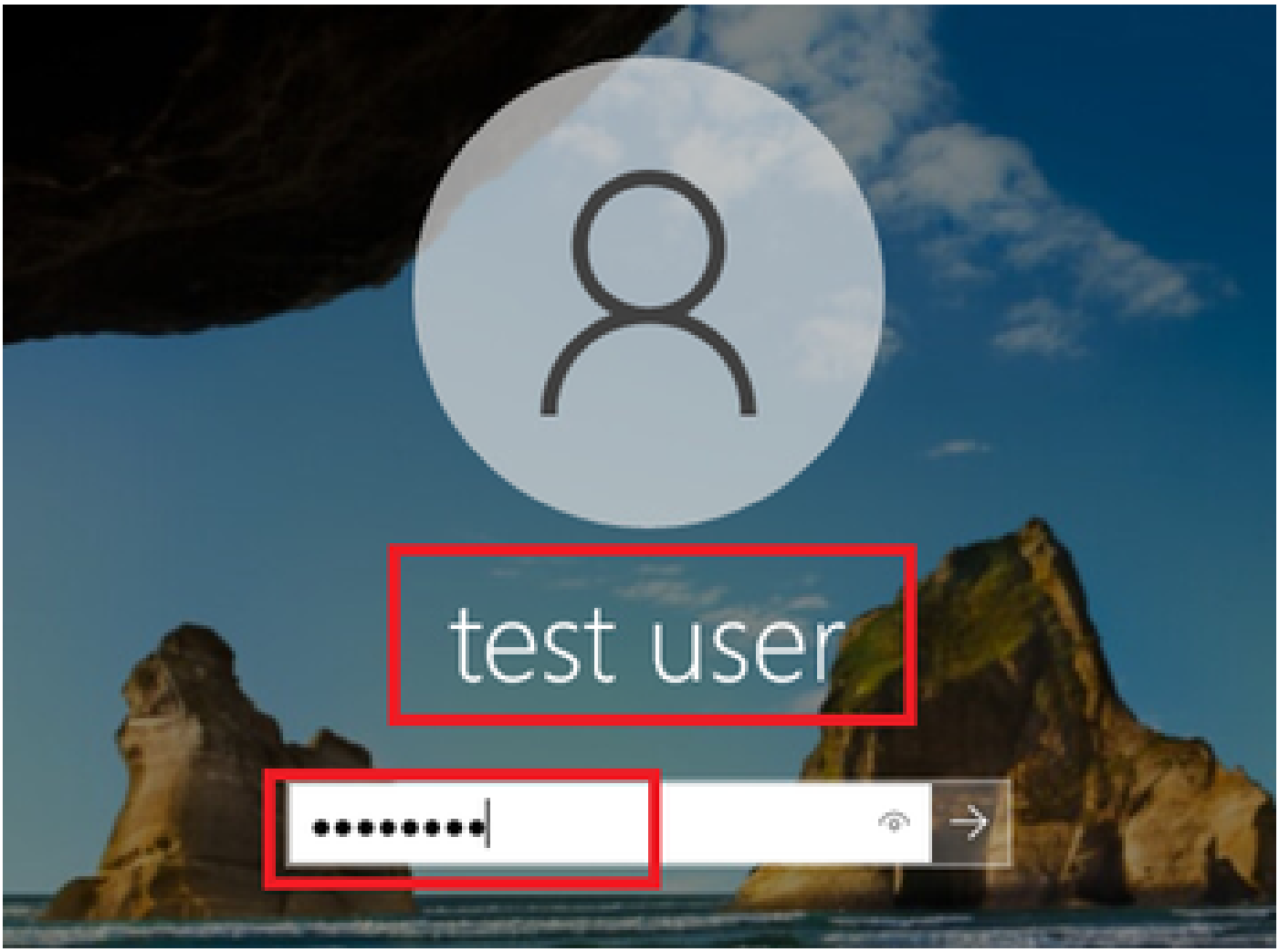
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 5s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003C
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success
```

Etapa 3. Fazer login no Windows PC

Faça login no Win10 PC1, insira o nome de usuário e a senha para disparar a autenticação de usuário.



Fazer login no Windows PC

Etapa 4. Confirmar sessão de autenticação

Execute show authentication sessions interface GigabitEthernet1/0/2 details o comando para confirmar a sessão de autenticação de usuário no C1000.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

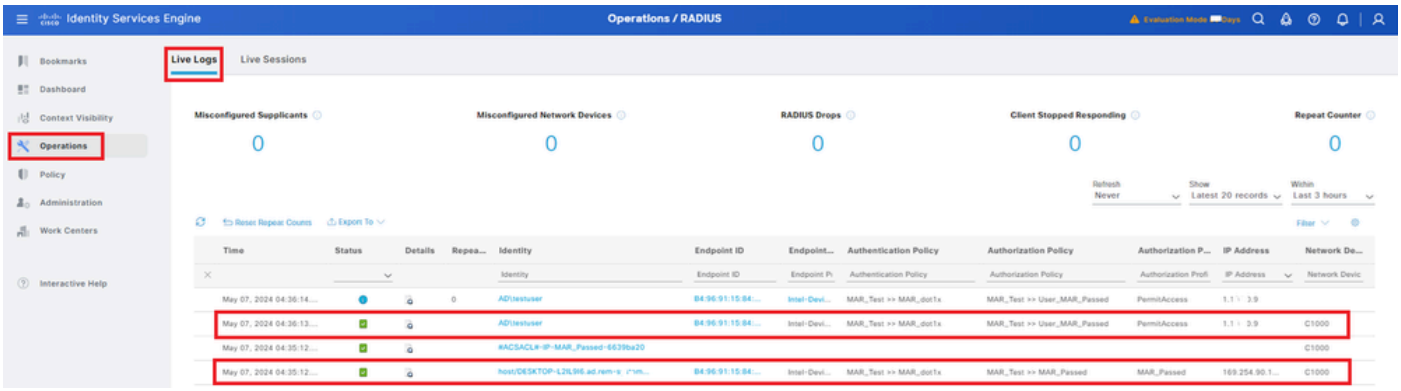
AD\testuser

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
```

```
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

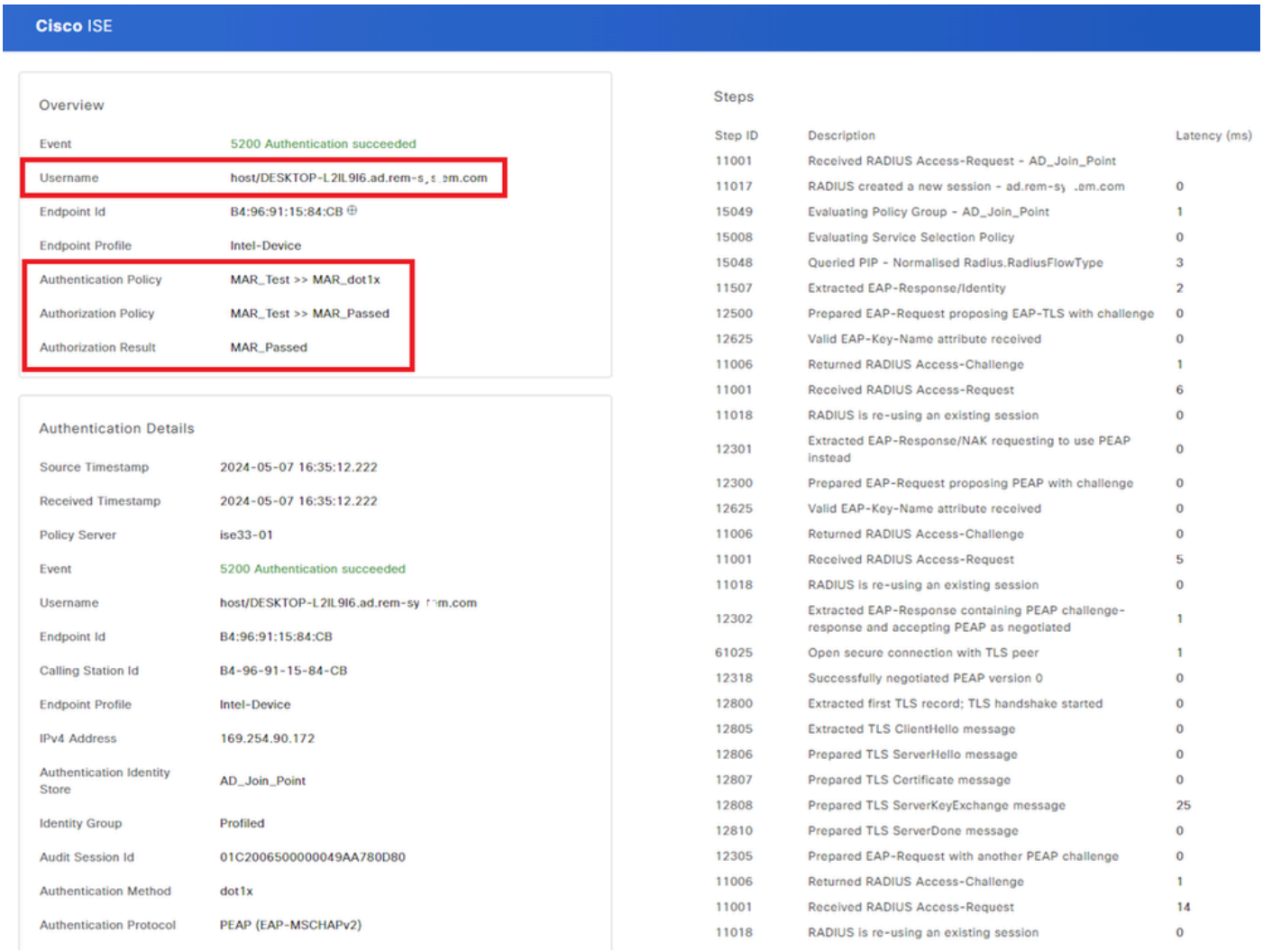
Etapa 5. Confirmar registro ao vivo do Radius

Navegue para **Operations > RADIUS > Live Logs** na GUI do ISE, confirme o registro em tempo real para autenticação da máquina e autenticação do usuário.



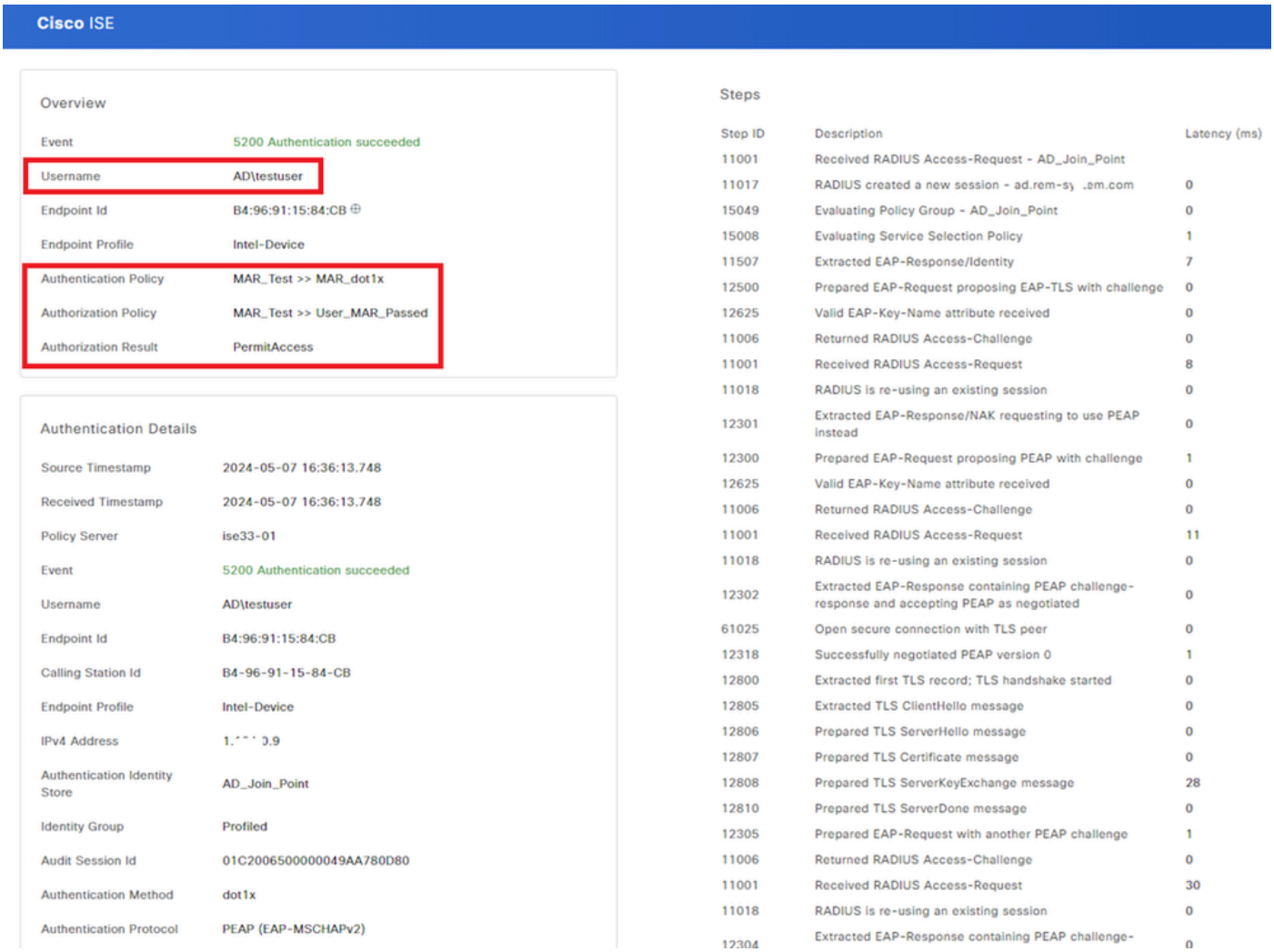
Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação da máquina.



Detalhes da autenticação da máquina

Confirme o registro ao vivo detalhado da autenticação do usuário.



Detalhes da autenticação de usuário

Padrão 2. Somente Autenticação de Usuário

Etapa 1. Desabilitar e Habilitar NIC de PC com Windows

Para disparar a autenticação de usuário, desabilite e habilite a placa de rede do Win10 PC1.

Etapa 2. Confirmar sessão de autenticação

Execute show authentication sessions interface GigabitEthernet1/0/2 details o comando para confirmar a sessão de autenticação de usuário no C1000.

<#root>

Switch#

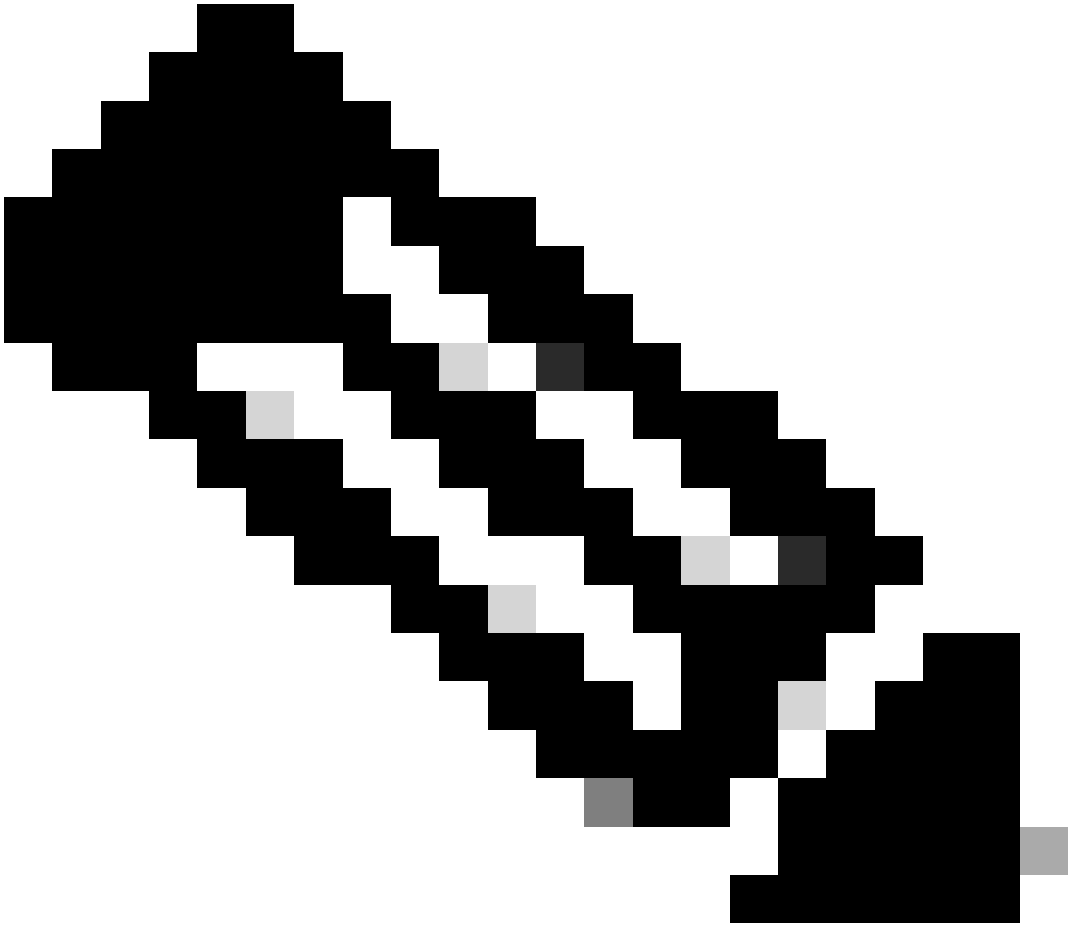
show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
```

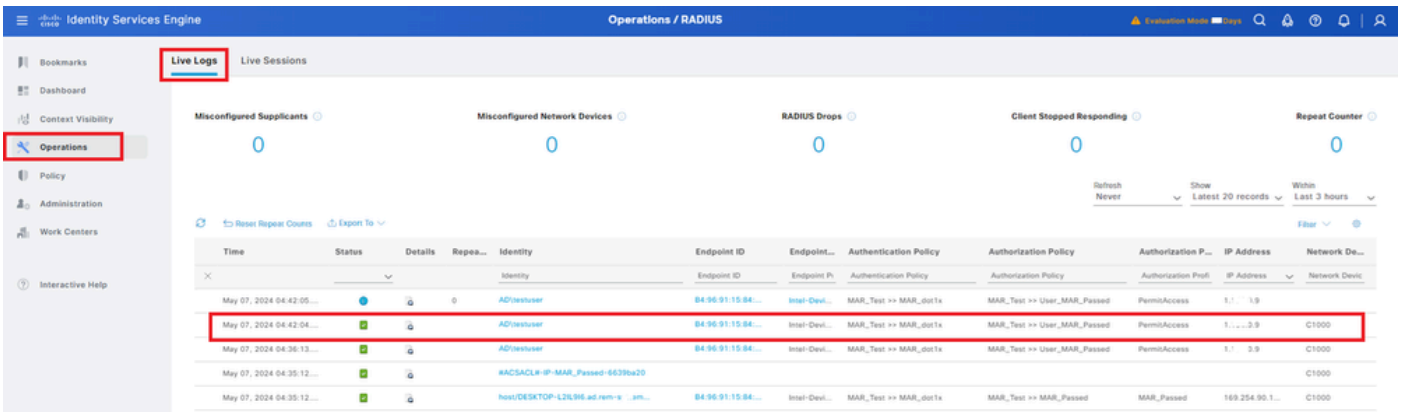
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

Etapa 3. Confirmar registro ao vivo do Radius

Navegue até **Operations > RADIUS > Live Logs** na GUI do ISE e confirme o registro em tempo real para a autenticação do usuário.

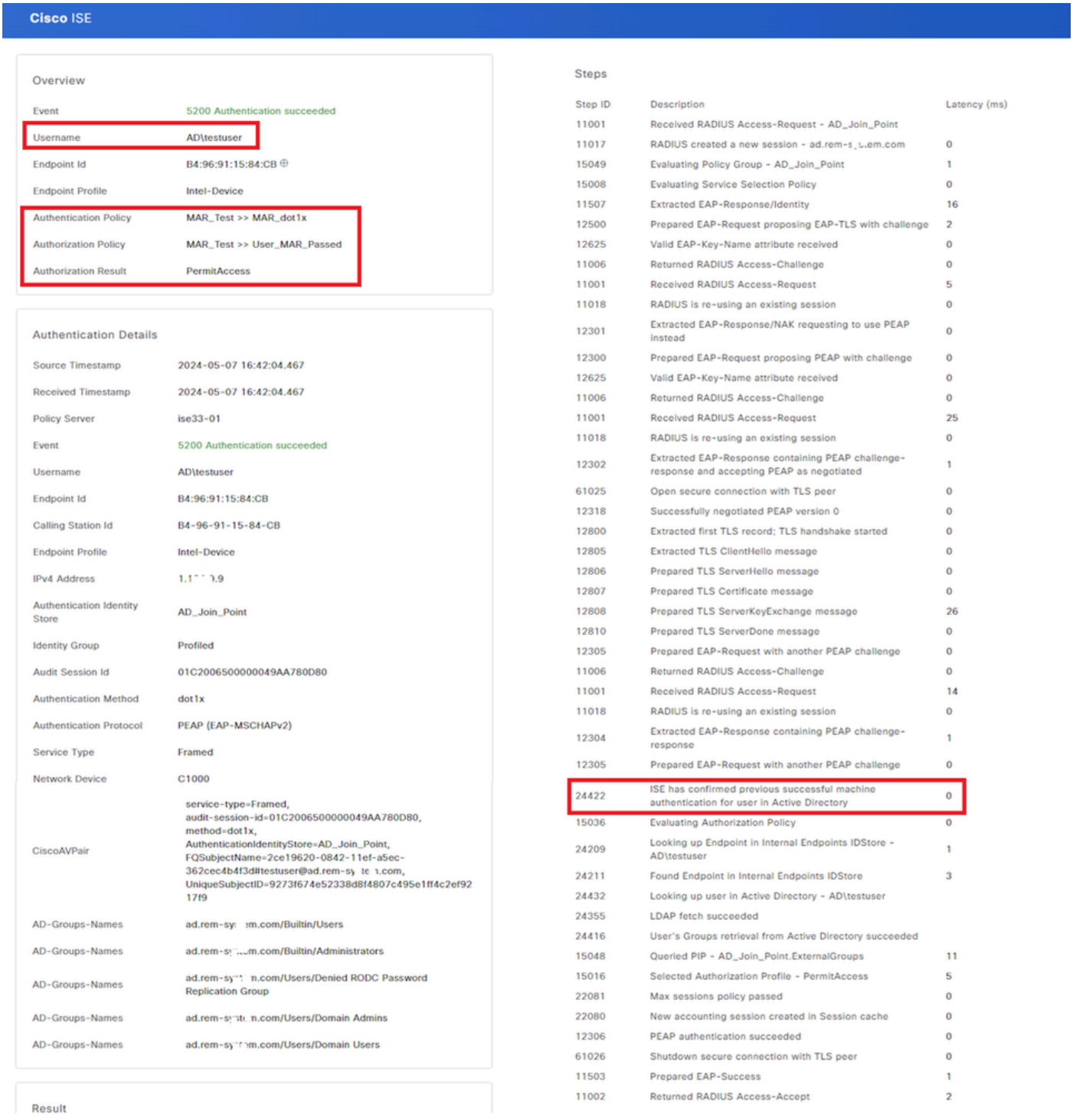


Observação: como o cache MAR é armazenado no ISE, somente a autenticação do usuário é necessária.



Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação do usuário.



Detalhes da autenticação de usuário

Troubleshooting

Esses logs de depuração (prt-server.log) ajudam a confirmar o comportamento detalhado da autenticação no ISE.

- runtime-config

- runtime-logging
- runtime-AAA

Este é um exemplo do log de depuração para o **Padrão 1. Autenticação de máquina e autenticação de usuário** neste documento.

<#root>

// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com, IDStore=AD_Join_Point an
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222
MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

Informações Relacionadas

Prós e contras da restrição de acesso à máquina

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.