

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Informações de Apoio](#)

[Configurações](#)

[Configuração no C1000](#)

[Configuração no PC com Windows](#)

[Etapa 1. Adicionar computador ao Domínio do AD](#)

[Etapa 2. Configurar autenticação de usuário](#)

[Configuração no Windows Server](#)

[Etapa 1. Confirmar computadores de domínio](#)

[Etapa 2. Adicionar usuário de domínio](#)

[Configuração no ISE](#)

[Etapa 1. Adicionar dispositivo](#)

[Etapa 2. Adicionar Active Directory](#)

[Etapa 3. Confirmar Configuração de Autenticação do Computador](#)

[Etapa 4. Adicionar Sequências de Origem de Identidade](#)

[Etapa 5. Adicionar DACL e perfil de autorização](#)

[Etapa 6. Adicionar conjunto de políticas](#)

[Passo 7. Adicionar política de autenticação](#)

[Etapa 8. Adicionar Política de Autorização](#)

[Verificar](#)

[Padrão 1. Autenticação de máquina e autenticação de usuário](#)

[Etapa 1. Sair do Windows PC](#)

[Etapa 2. Confirmar sessão de autenticação](#)

[Etapa 3. Fazer login no Windows PC](#)

[Etapa 4. Confirmar sessão de autenticação](#)

[Etapa 5. Confirmar registro ao vivo do Radius](#)

[Padrão 2. Somente Autenticação de Usuário](#)

[Etapa 1. Desabilitar e Habilitar NIC de PC com Windows](#)

[Etapa 2. Confirmar sessão de autenticação](#)

[Etapa 3. Confirmar registro ao vivo do Radius](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

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.

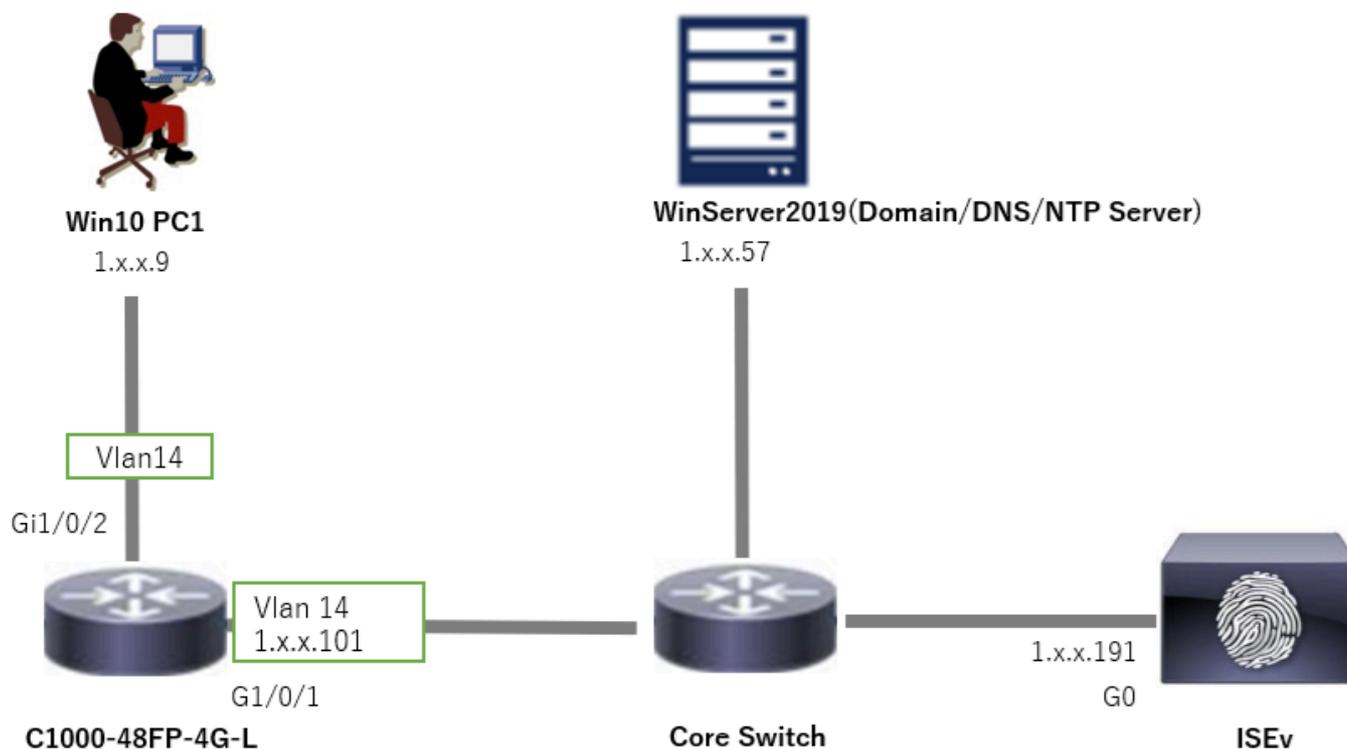


Diagrama de Rede

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
```

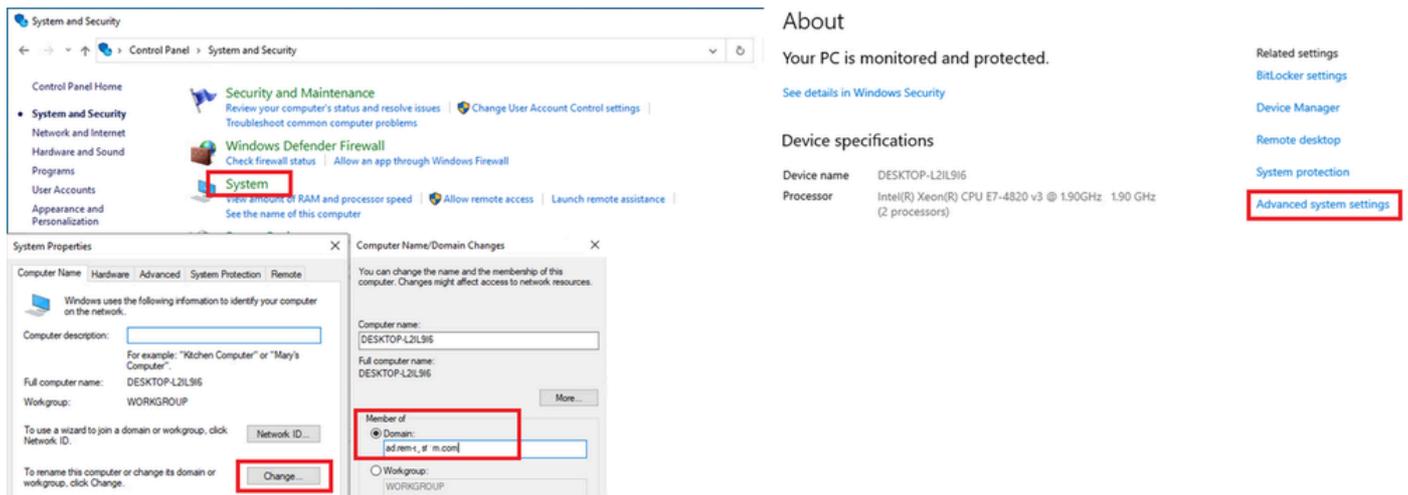
```
interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access
```

```
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

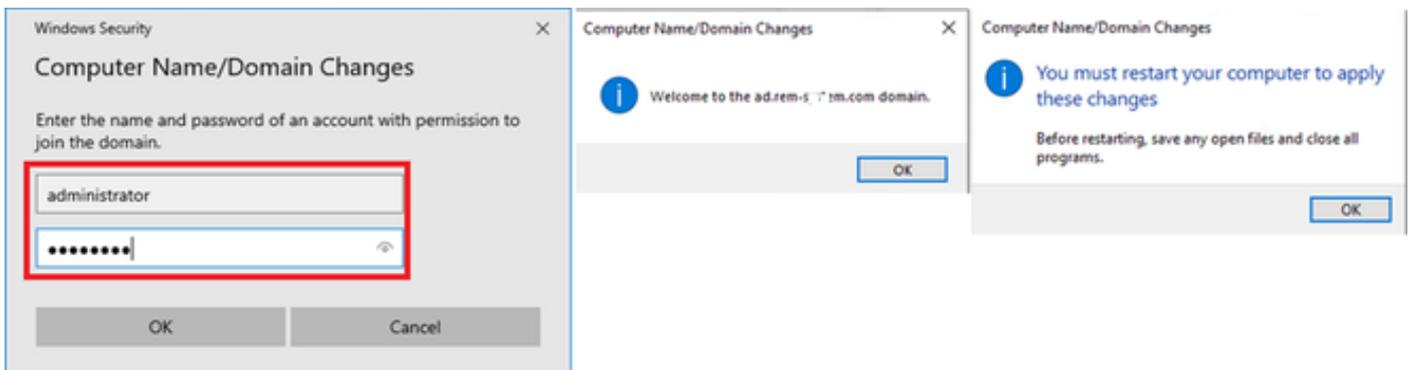
Etapa 1. Adicionar computador ao Domínio do AD

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

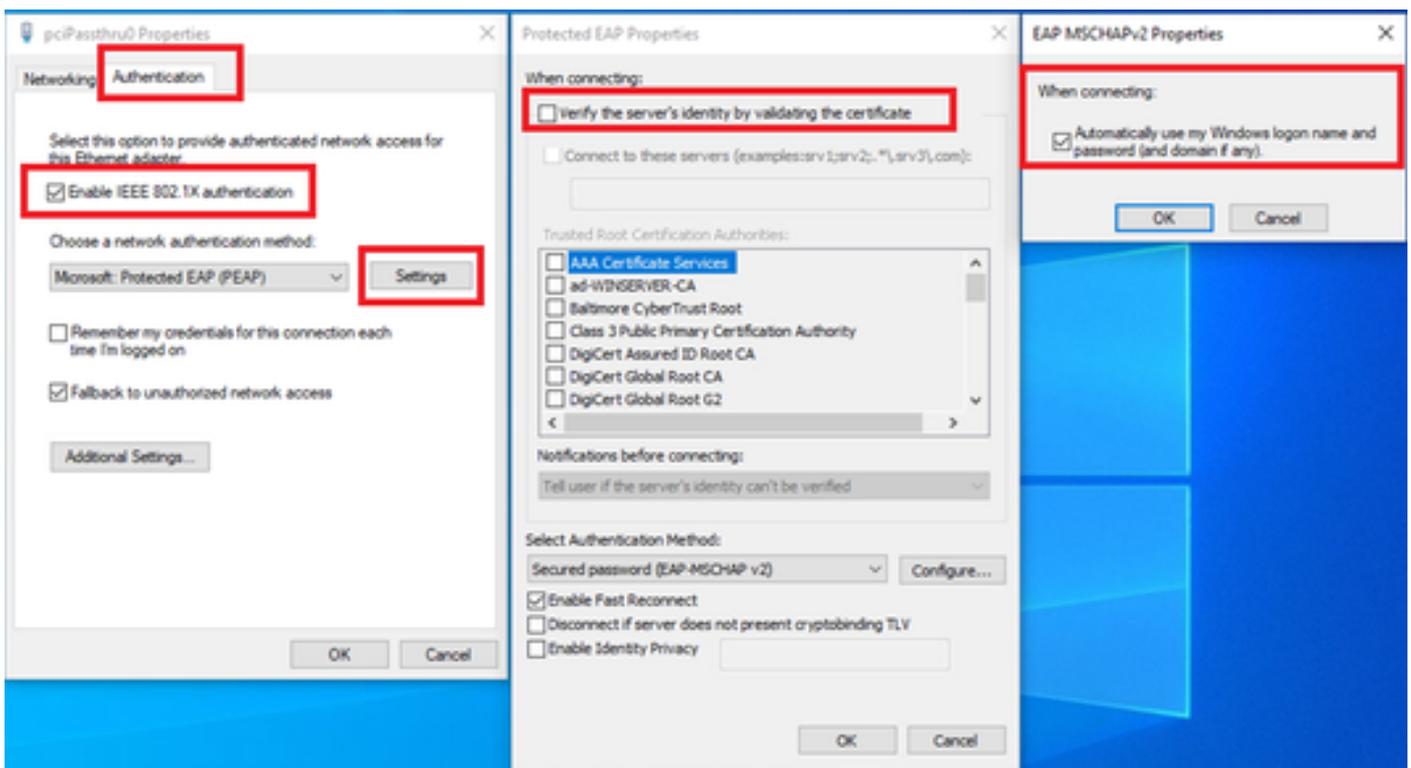
Na janela Segurança do Windows, insira o nome de usuário e a senha do servidor de domínio.



Inserir nome de usuário e senha

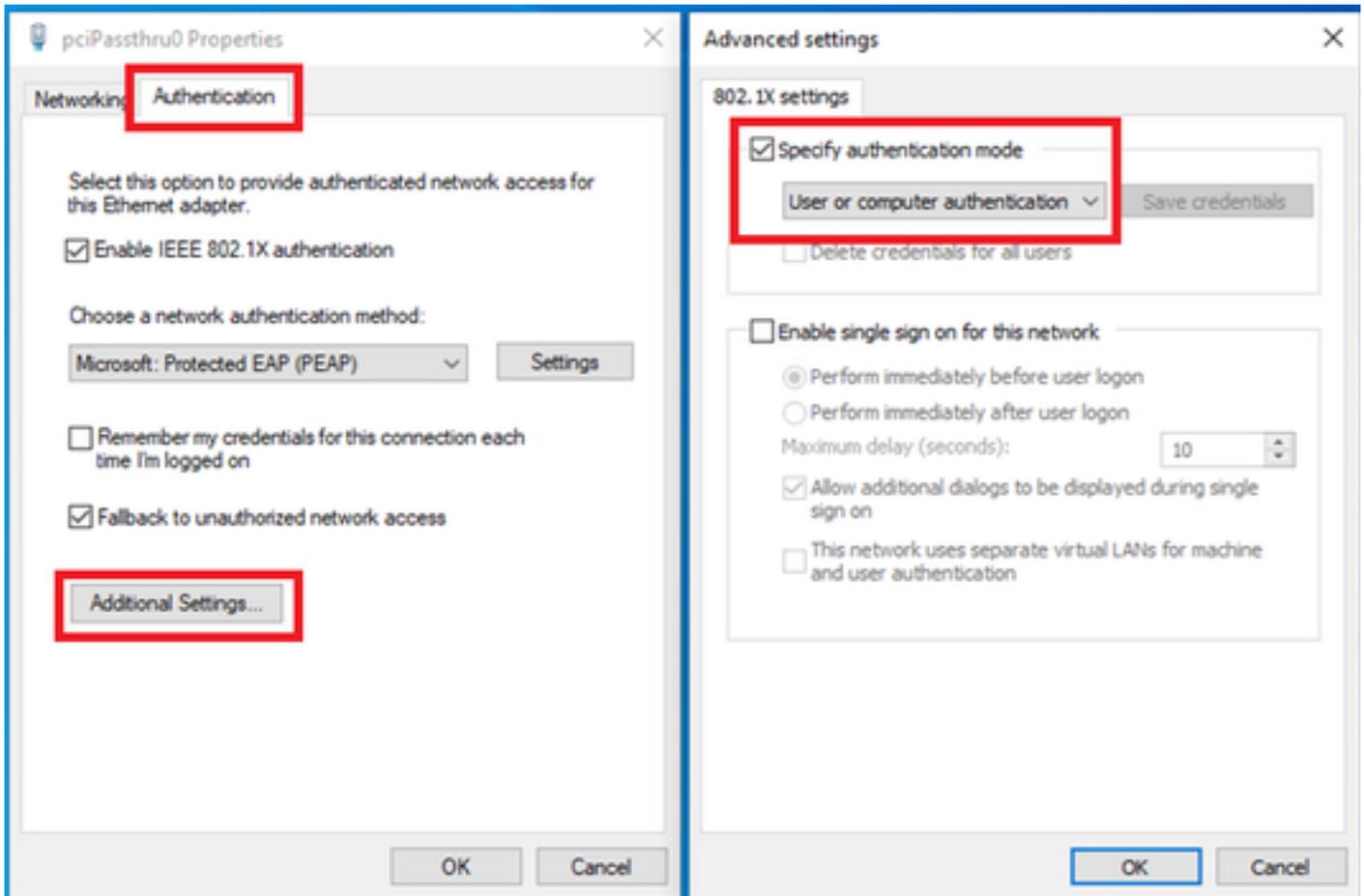
Etapa 2. Configurar autenticação de usuário

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.

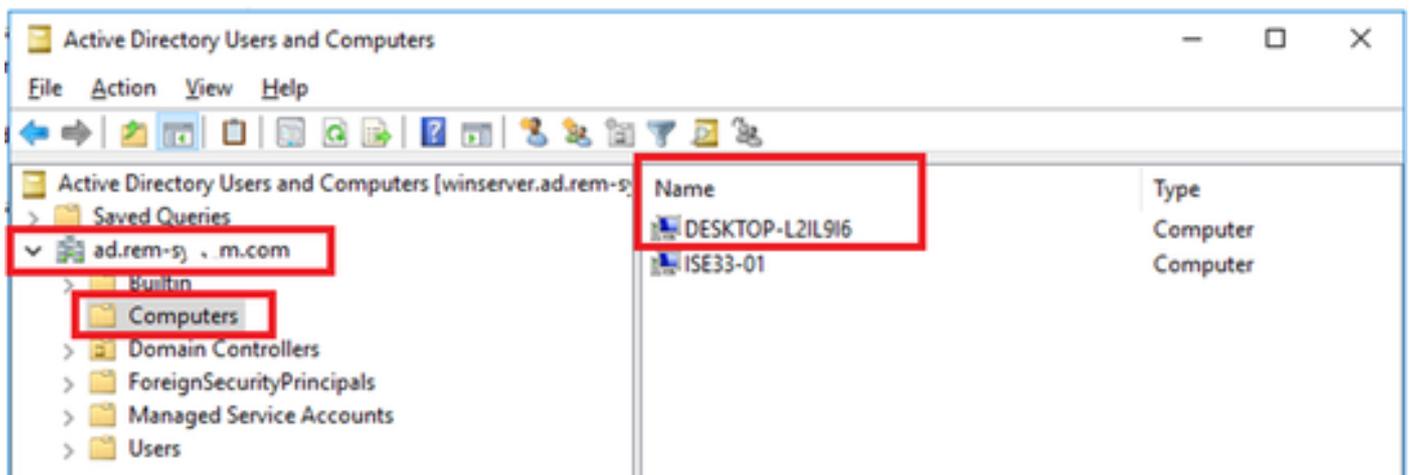


Especificar Modo de Autenticação

Configuração no Windows Server

Etapa 1. Confirmar computadores de domínio

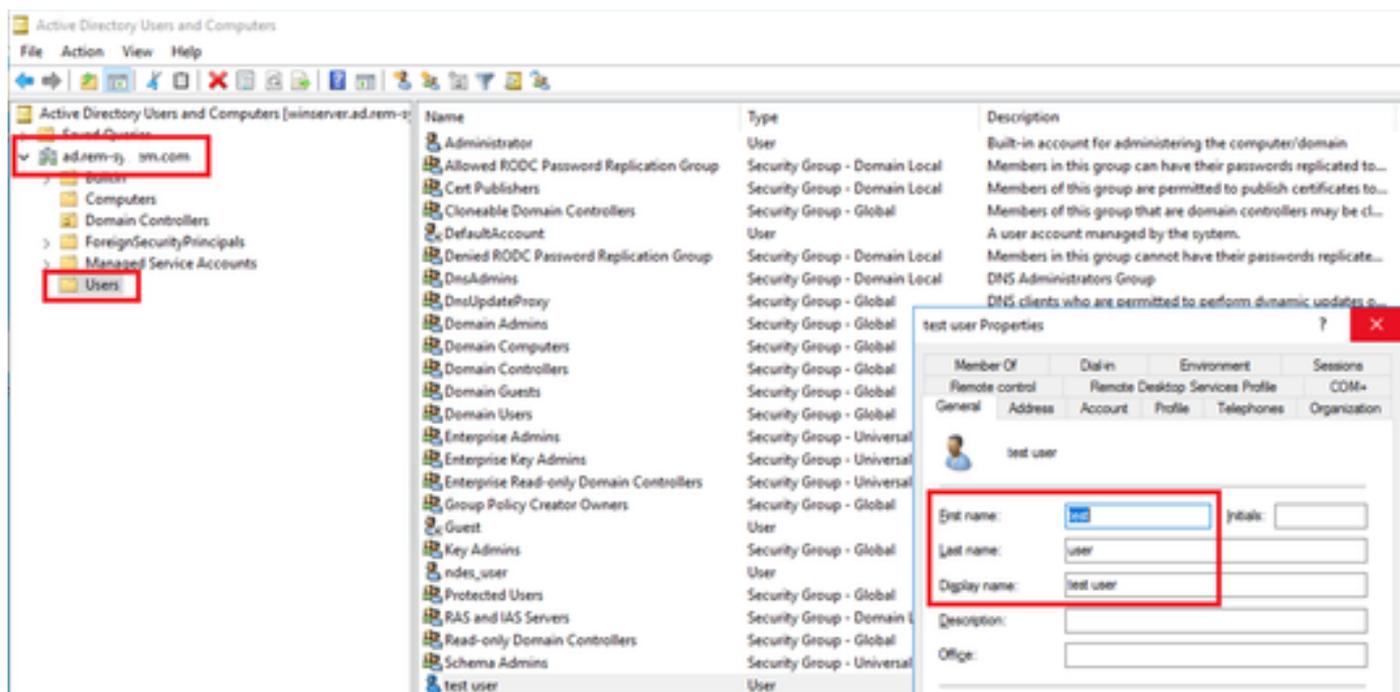
Navegue até Usuários e computadores do Active Directory, clique em Computadores. Confirme se o Win10 PC1 está listado no domínio.



Confirmar computador de domínio

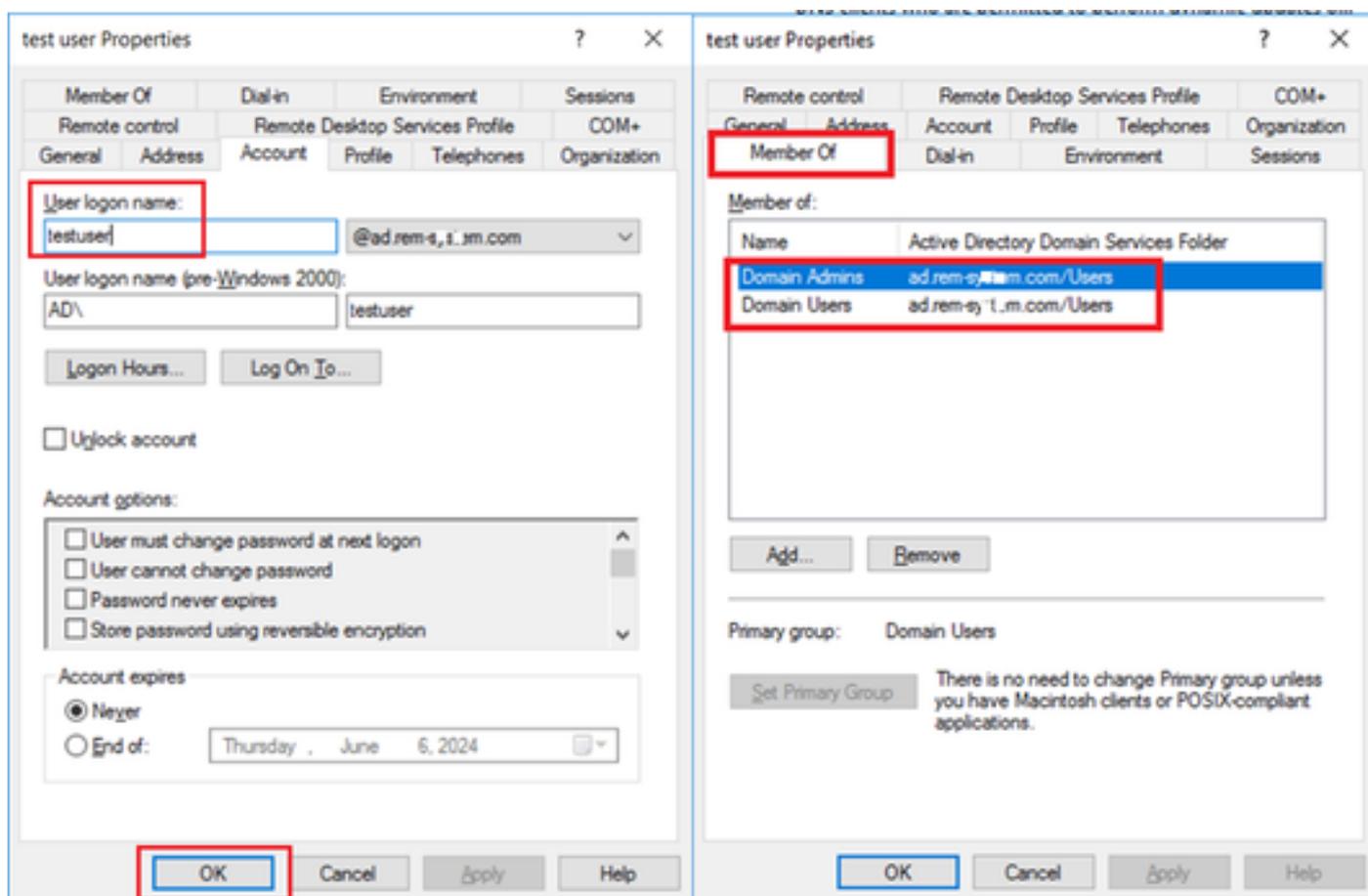
Etapa 2. Adicionar usuário de domínio

Navegue até Usuários e computadores do Ative Diretorio, 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.

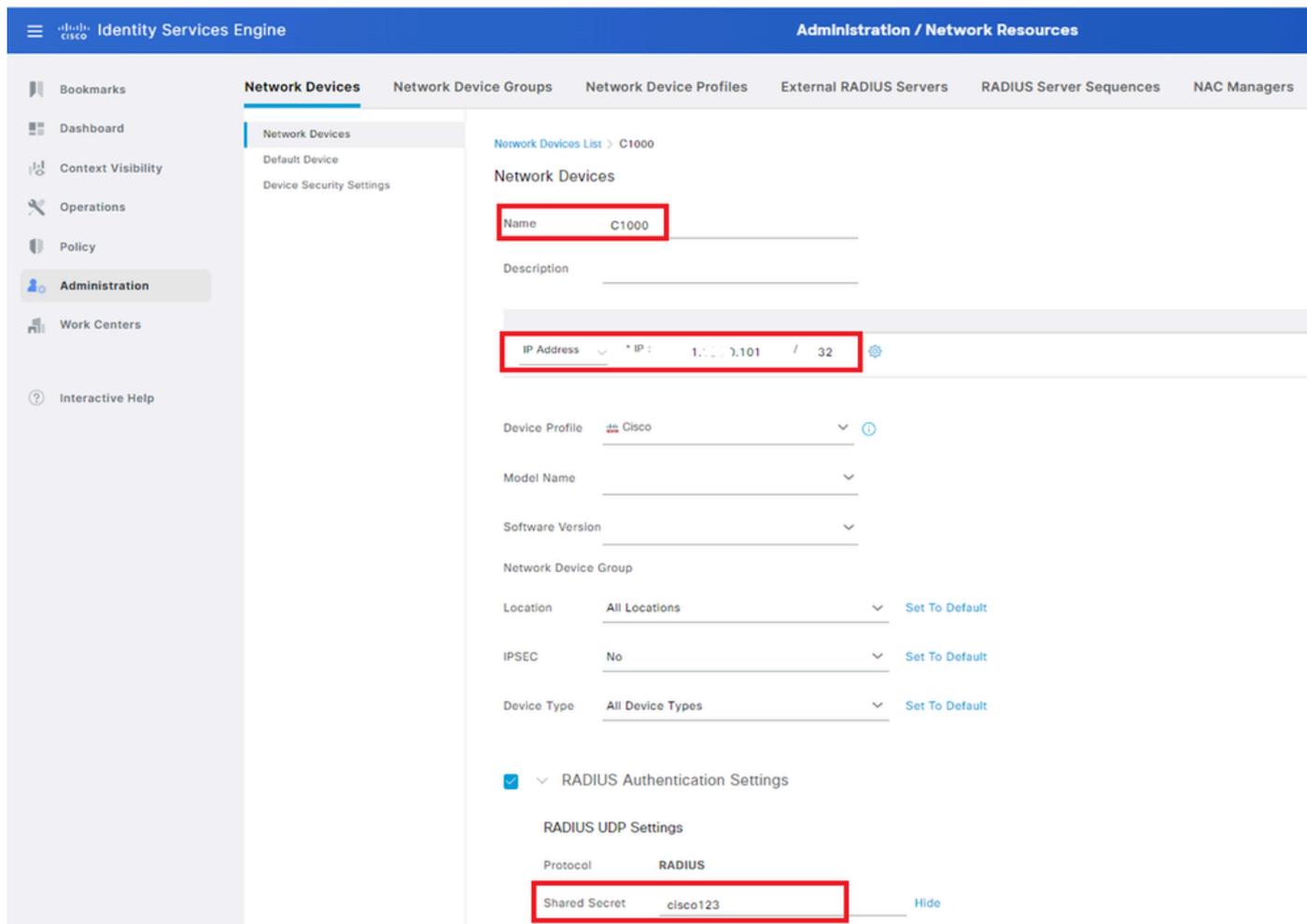


Admins. e Usuários do Domínio

Configuração no ISE

Etapa 1. Adicionar dispositivo

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

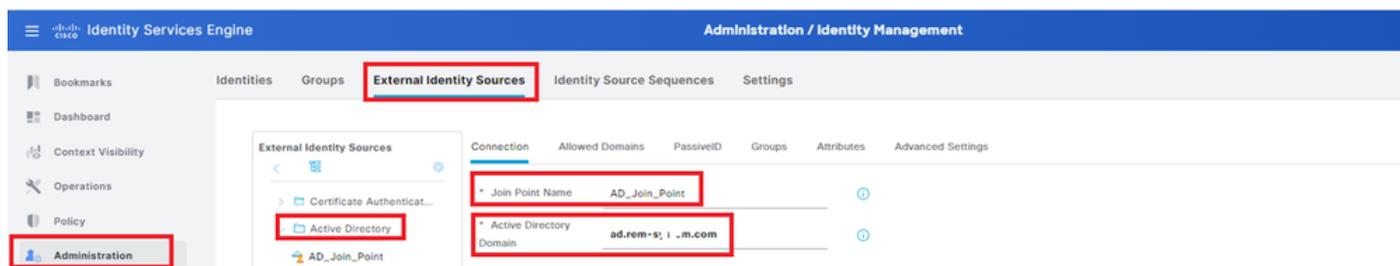


Adicionar dispositivo

Etapa 2. Adicionar Active Directory

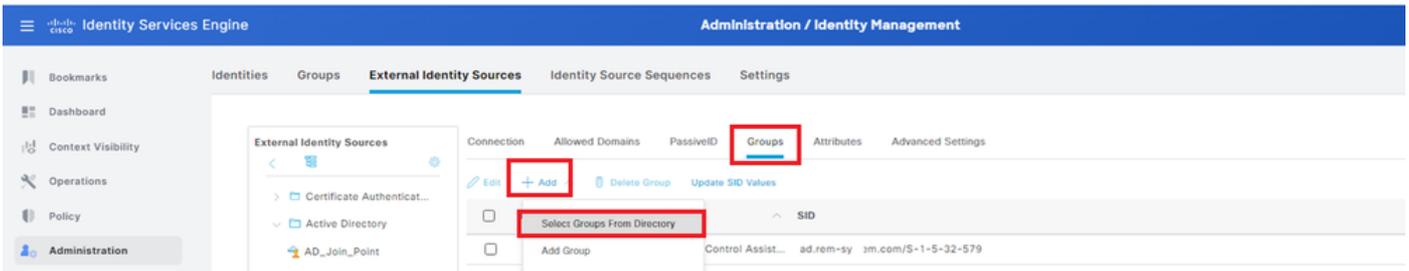
Navegue para Administração > Fontes de identidade externas > Active Directory, clique na guia Conexão e adicione o Active Directory ao ISE.

- Nome do ponto de junção: AD_Join_Point
- Domínio do Active Directory: ad.rem-xxx.com



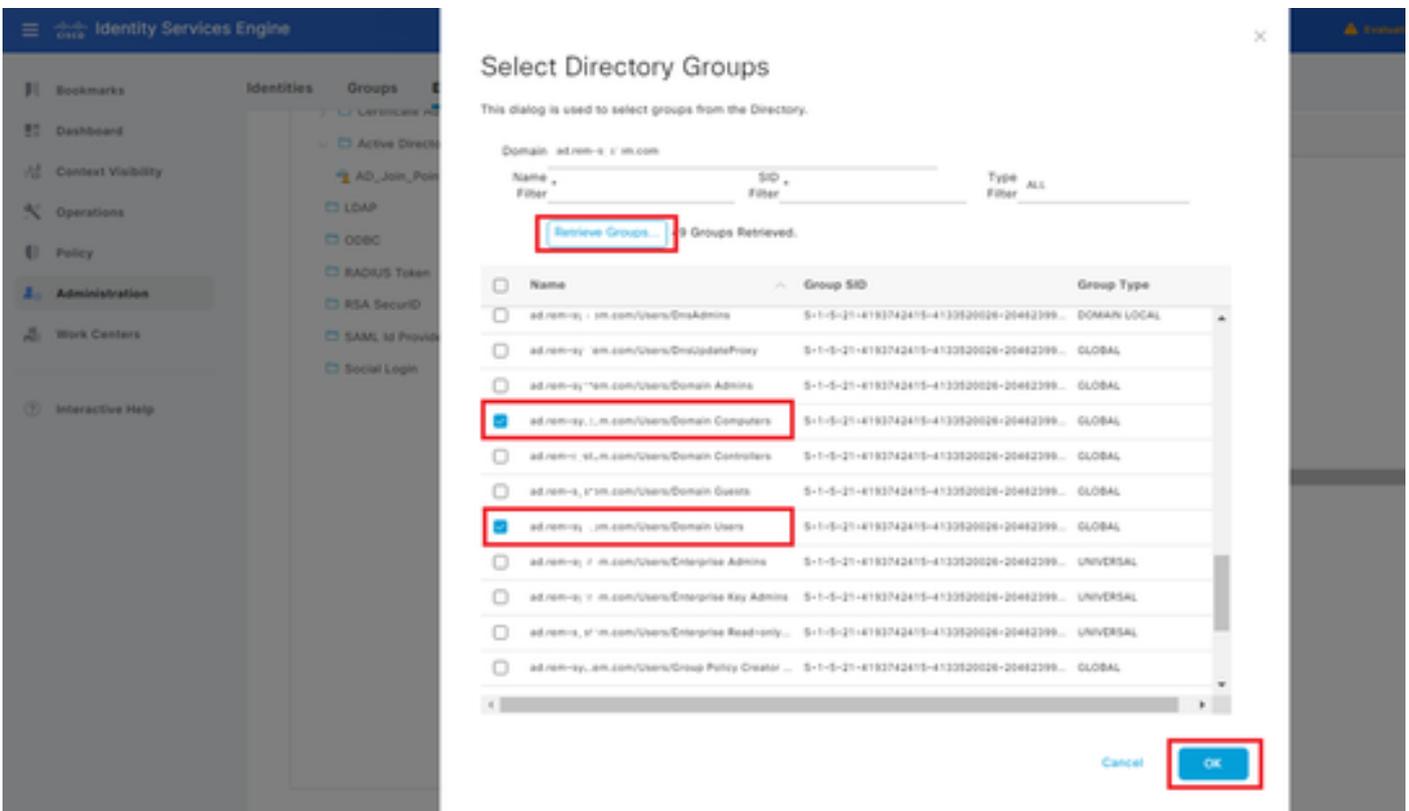
Adicionar Ative Directory

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.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar shows 'Identity Services Engine' and 'Administration / Identity Management'. The main navigation menu on the left includes 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is selected, and the 'External Identity Sources' page is active. The 'Advanced Settings' tab is highlighted with a red box. The 'Advanced Authentication Settings' section is expanded, showing the following options:

- Enable Password Change
- Enable Machine Authentication
- Enable Machine Access Restrictions
- Aging Time: 5 hours

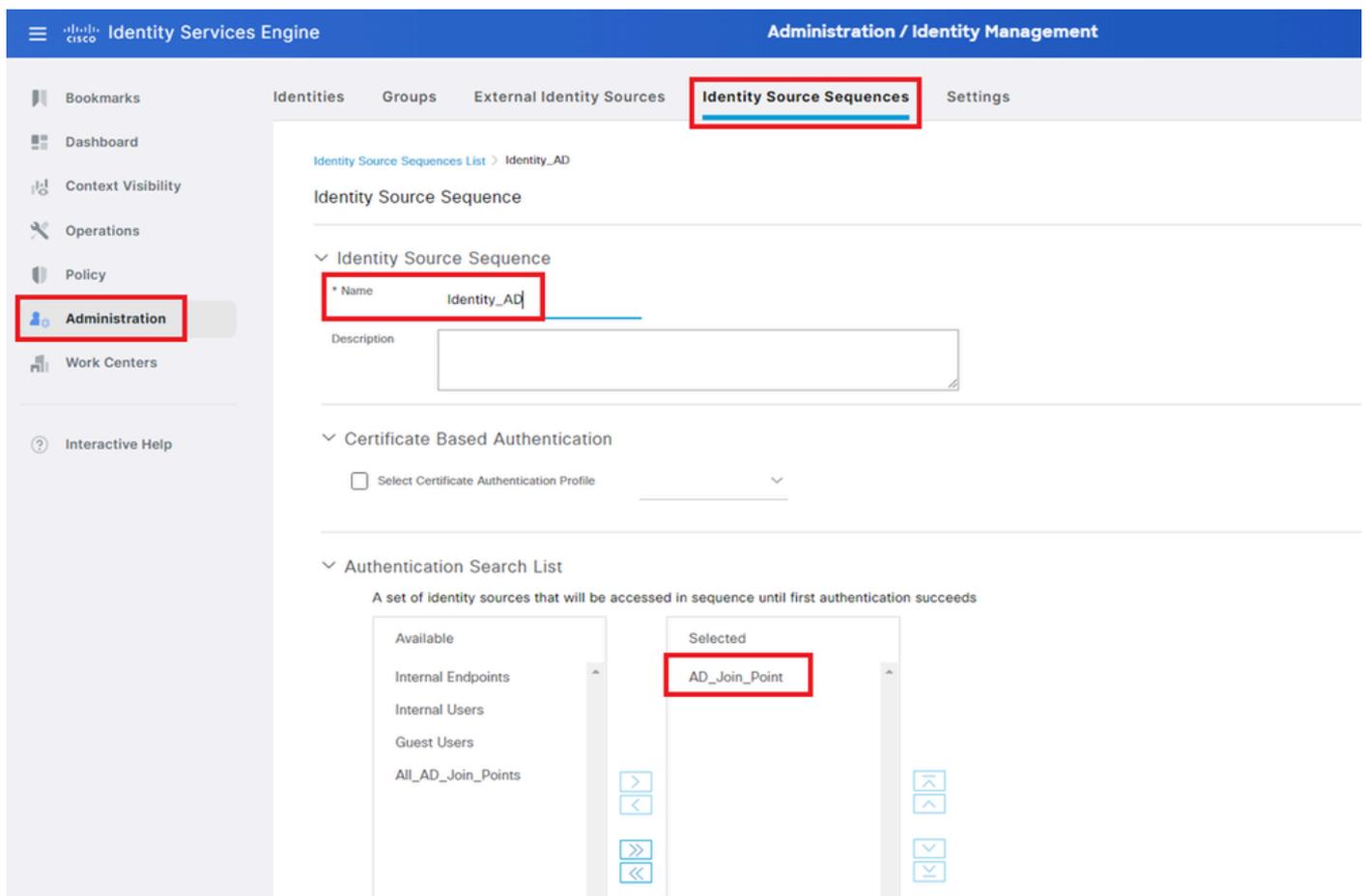
Below these settings, there is a note: 'Machine Access Restrictions Cache will be replicated between PSN instances in each node group. To configure MAR Cache distribution groups: [Administration > System > Deployment](#)'. Other options include:

- Enable dial-in check
- Enable callback check for dial-in clients
- Use Kerberos for Plain Text Authentications

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

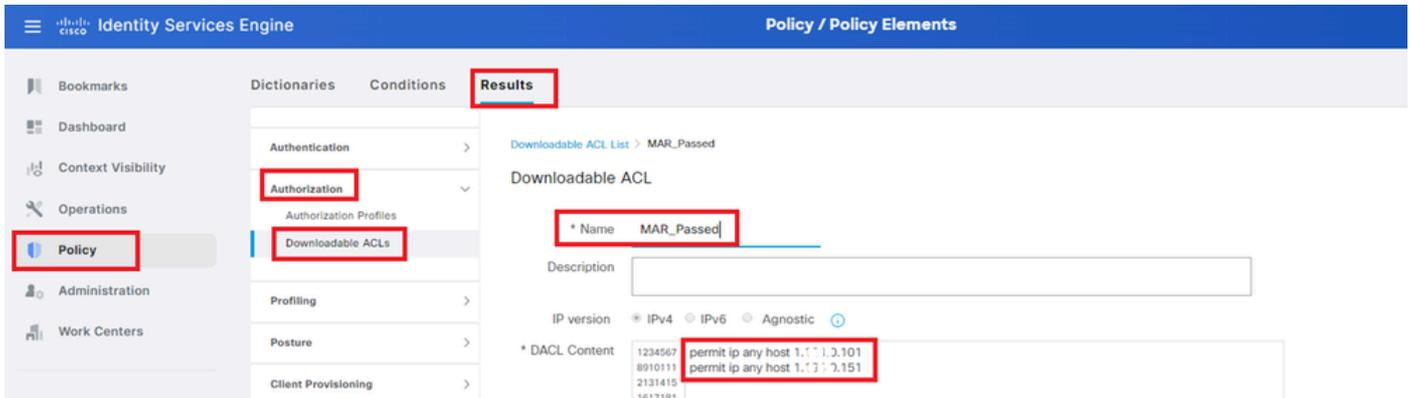


Adicionar Sequências de Origem de Identidade

Etapa 5. Adicionar DACL e perfil de autorização

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

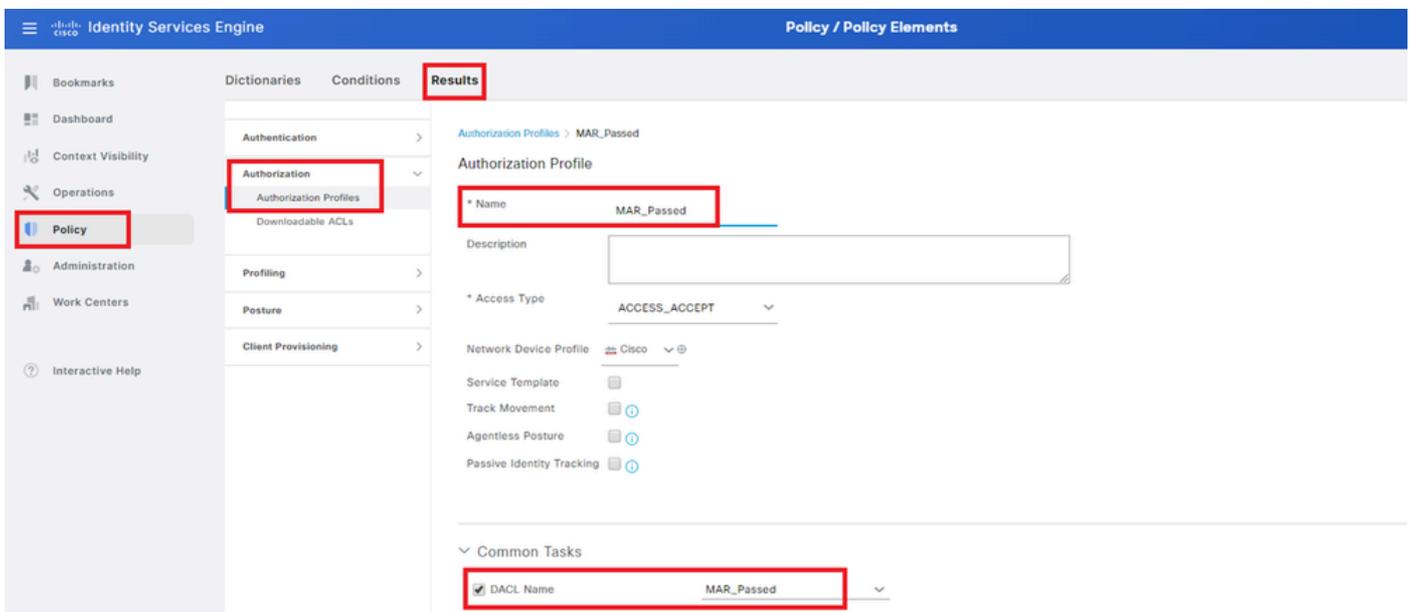
- Nome: MAR_Passed
- Conteúdo da DACL: permit ip any host 1.x.x.101 e permit ip any host 1.x.x.105



Adicionar DACL

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

- Nome: MAR_Passed
- Nome DACL: MAR_Passed

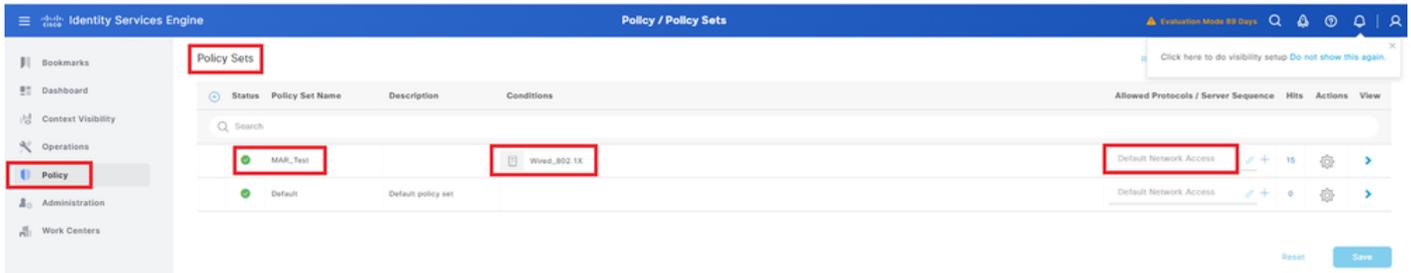


Adicionar perfil de autorização

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

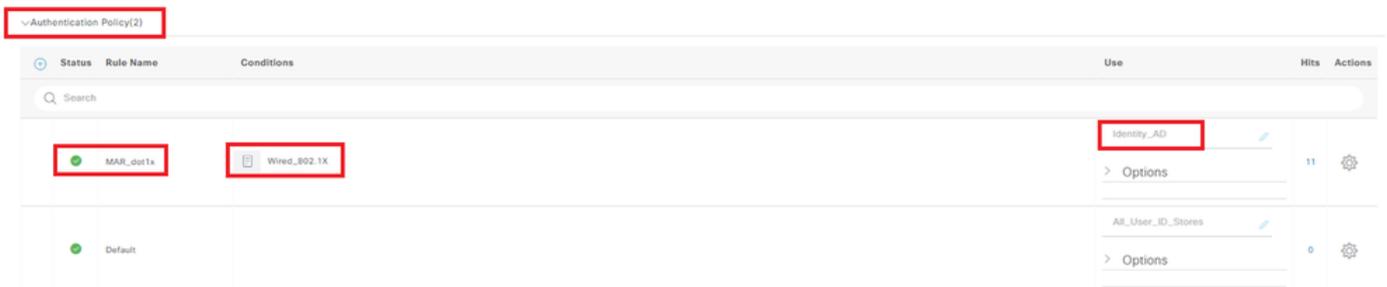


Adicionar conjunto de políticas

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

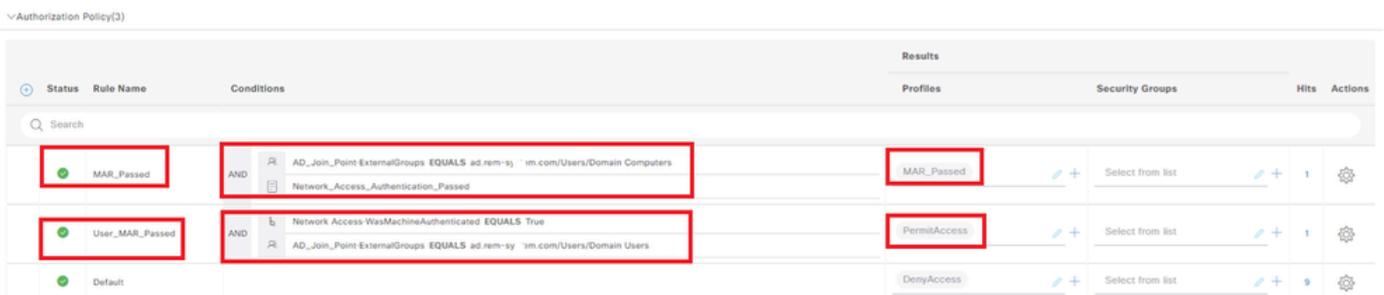


Adicionar política de autenticação

Etapas 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

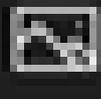
 Lock

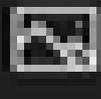
 Sign out

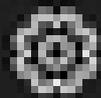
 Switch user

  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)

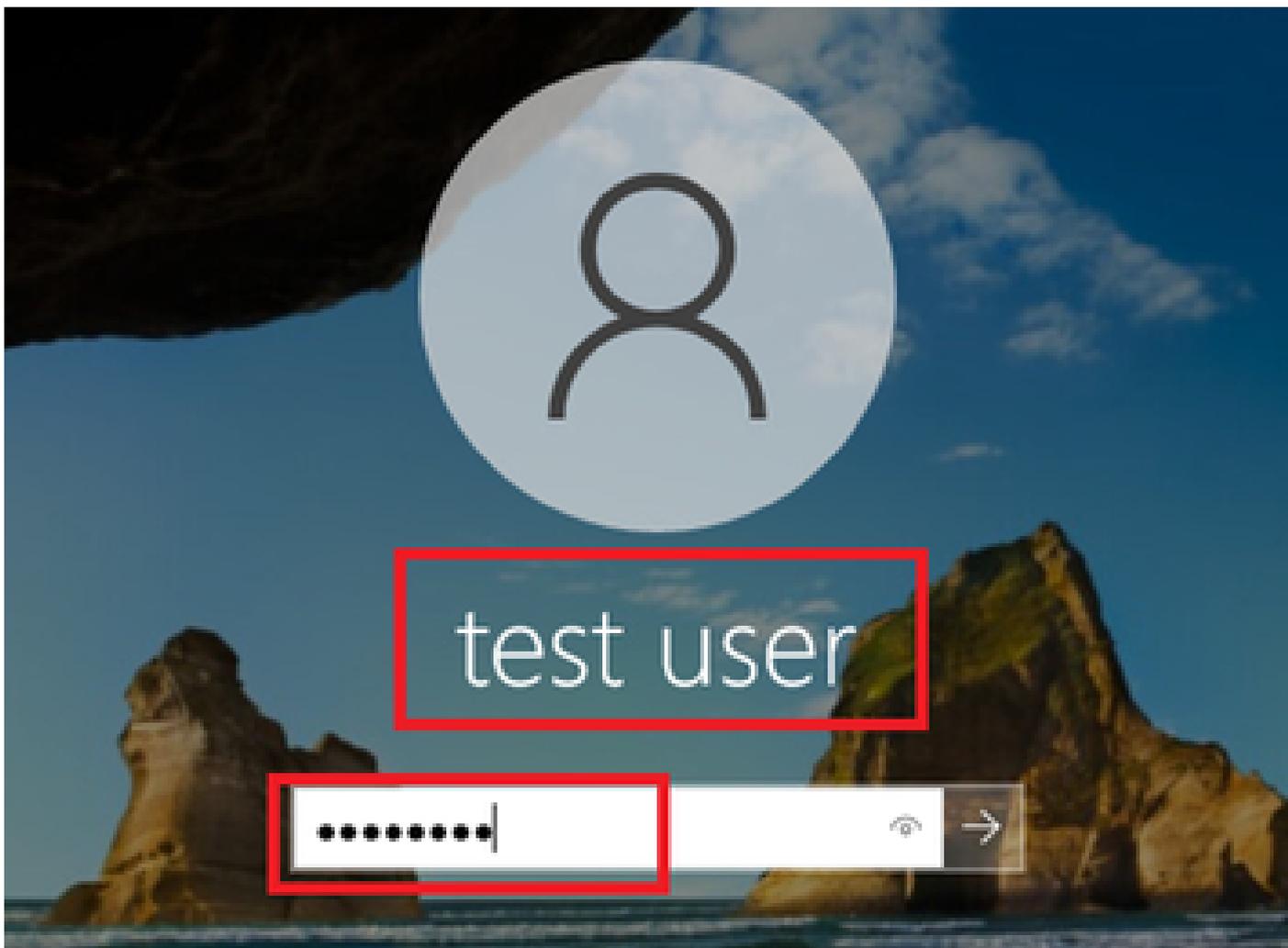
Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

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: 01C200650000049AA780D80
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.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:36:14...	●		0	AD\testuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermitAccess	1.1.1.39	
May 07, 2024 04:36:13...	●		0	AD\testuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermitAccess	1.1.1.39	C1000
May 07, 2024 04:35:12...	●		0	WACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12...	●		0	host\DESKTOP-L2696-ad-rem-1-r1m...	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação da máquina.

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy. em.com
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details

Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy. em.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy. em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

Detalhes da autenticação da máquina

Confirme o registro ao vivo detalhado da autenticação do usuário.

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.x.x.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .am.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

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.

The screenshot shows the Identity Services Engine (ISE) interface. The 'Operations / RADIUS' section is active, displaying a 'Live Logs' view. The interface includes a sidebar with navigation options like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Help'. The main area shows several summary cards for 'Misconfigured Supplicants', 'Misconfigured Network Devices', 'RADIUS Drops', 'Client Stopped Responding', and 'Repeat Counter', all showing zero counts. Below these is a table of log entries. A red box highlights a log entry for a successful authentication of 'AD\testuser'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05...			0	AD\testuser	84-96-91-15-84...	Intnl-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:42:04...			0	AD\testuser	84-96-91-15-84...	Intnl-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:36:13...			0	AD\testuser	84-96-91-15-84...	Intnl-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:35:12...			0	WACSACLW-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12...			0	hos\DESKTOP-L2L96-ad.rem-s..._sm...	84-96-91-15-84...	Intnl-Devi...	MAR_Test == MAR_dot1x	MAR_Test == MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Confirme o registro ao vivo detalhado da autenticação do usuário.

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: AD\testuser

Endpoint Id: B4:96:91:15:84:CB

Endpoint Profile: Intel-Device

Authentication Policy: MAR_Test >> MAR_dot1x

Authorization Policy: MAR_Test >> User_MAR_Passed

Authorization Result: PermitAccess

Authentication Details

Source Timestamp: 2024-05-07 16:42:04.467

Received Timestamp: 2024-05-07 16:42:04.467

Policy Server: ise33-01

Event: 5200 Authentication succeeded

Username: AD\testuser

Endpoint Id: B4:96:91:15:84:CB

Calling Station Id: B4-96-91-15-84-CB

Endpoint Profile: Intel-Device

IPv4 Address: 1.1.1.9

Authentication Identity Store: AD_Join_Point

Identity Group: Profiled

Audit Session Id: 01C2006500000049AA780D80

Authentication Method: dot1x

Authentication Protocol: PEAP (EAP-MSCHAPv2)

Service Type: Framed

Network Device: C1000

CiscoAVPair: service-type=Framed, audit-session-id=01C2006500000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d@testuser@ad.rem-sy.te.m.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9

AD-Groups-Names: ad.rem-sy.te.m.com/Builtin/Users

AD-Groups-Names: ad.rem-sy.te.m.com/Builtin/Administrators

AD-Groups-Names: ad.rem-sy.te.m.com/Users/Denied RODC Password Replication Group

AD-Groups-Names: ad.rem-sy.te.m.com/Users/Domain Admins

AD-Groups-Names: ad.rem-sy.te.m.com/Users/Domain Users

Result

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy.te.m.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
11507	Extracted EAP-Response/Identity	16
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	25
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
24432	Looking up user in Active Directory - AD\testuser	
24355	LDAP fetch succeeded	
24416	User's Groups retrieval from Active Directory succeeded	
15048	Queried PIP - AD_Join_Point.ExternalGroups	11
15016	Selected Authorization Profile - PermitAccess	5
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
12306	PEAP authentication succeeded	0
61026	Shutdown secure connection with TLS peer	0
11503	Prepared EAP-Success	1
11002	Returned RADIUS Access-Accept	2

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=01C200650000049AA780D8

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,CPMSessionID

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 and

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

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

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

// user authentication

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

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,CPMSessionID

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.