Configuración de la autenticación de dos factores de máquina para el acceso del suplicante

Contenido

Introducción

Este documento describe los pasos necesarios para configurar la autenticación de dos factores con autenticación máquina y dot1x.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Cisco Identity Services Engine
- Configuración de Cisco Catalyst
- IEEE802.1X

Componentes Utilizados

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

- Windows Server 2019

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.

El nombre de dominio configurado en Windows Server 2019 es ad.rem-xxx.com, que se utiliza como ejemplo en este documento.

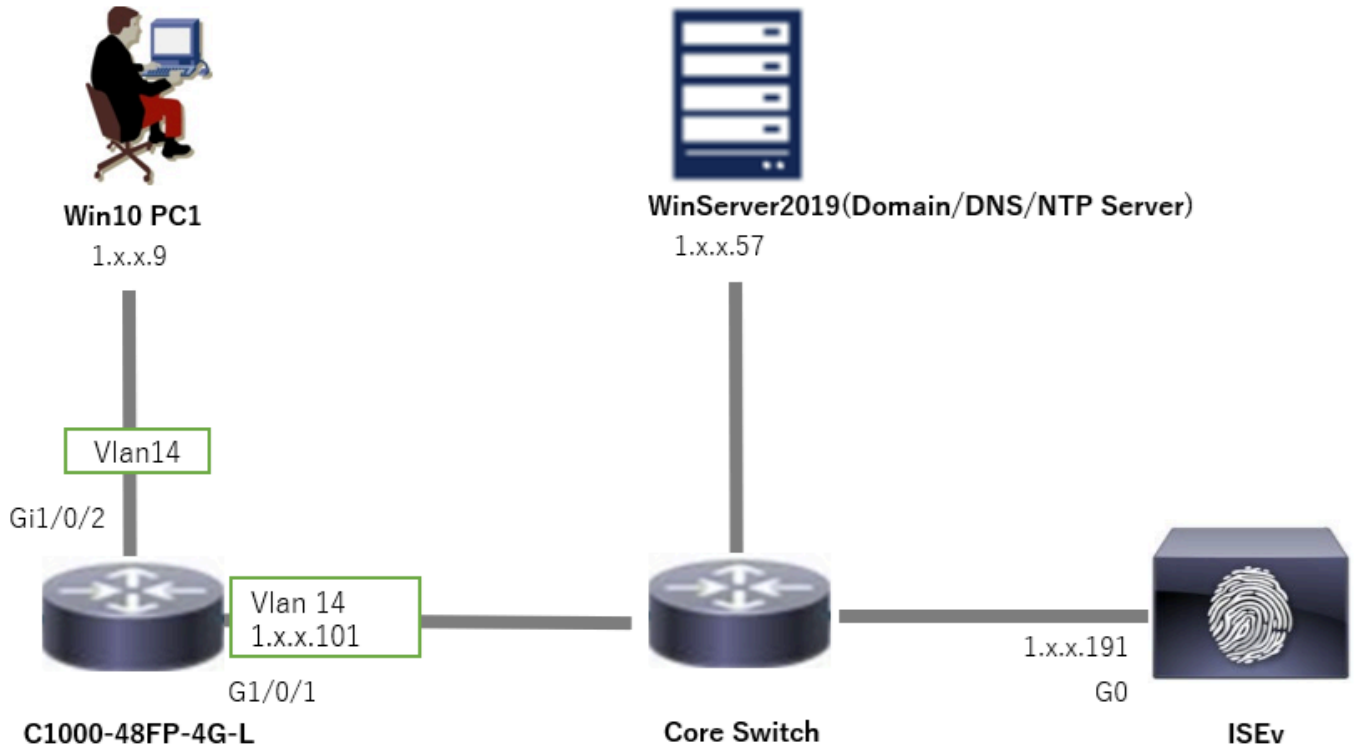


Diagrama de la red

Antecedentes

La autenticación de equipo es un proceso de seguridad que verifica la identidad de un dispositivo que solicita acceso a una red o sistema. A diferencia de la autenticación de usuario, que comprueba la identidad de una persona basándose en credenciales como un nombre de usuario y una contraseña, la autenticación de equipo se centra en validar el propio dispositivo. Esto se suele hacer mediante certificados digitales o claves de seguridad que son únicas para el dispositivo.

Mediante el uso conjunto de la autenticación de equipo y usuario, una organización puede garantizar que solo los dispositivos y usuarios autorizados puedan acceder a su red, lo que proporciona un entorno más seguro. Este método de autenticación de dos factores es especialmente útil para proteger la información confidencial y cumplir con estándares normativos estrictos.

Configuraciones

Configuración en C1000

Esta es la configuración mínima en C1000 CLI.

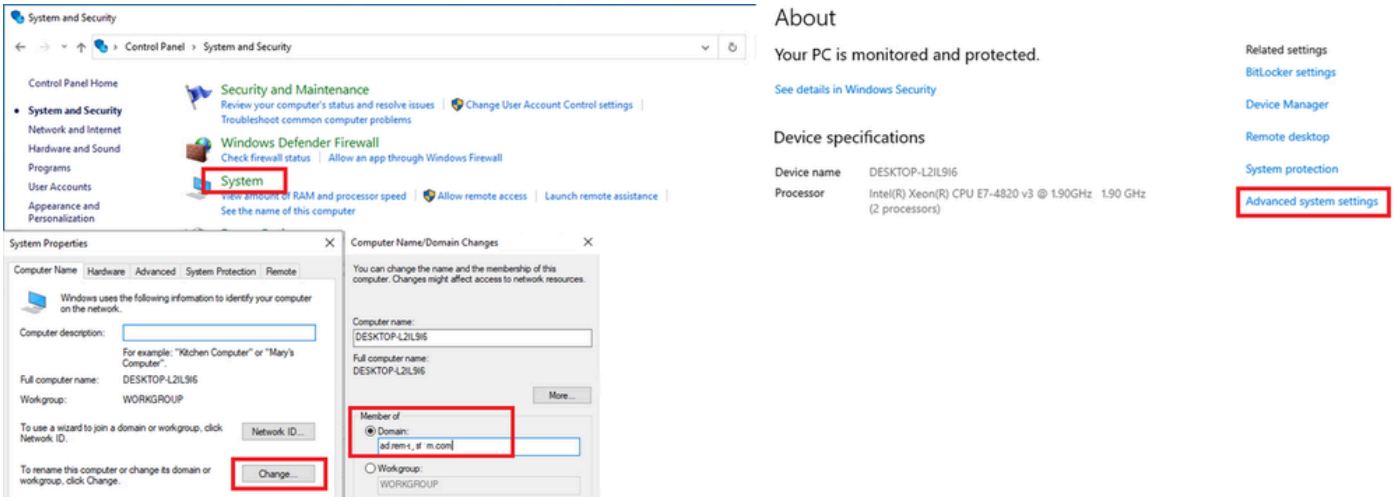
```
aaa new-model

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
```

Configuración en PC con Windows

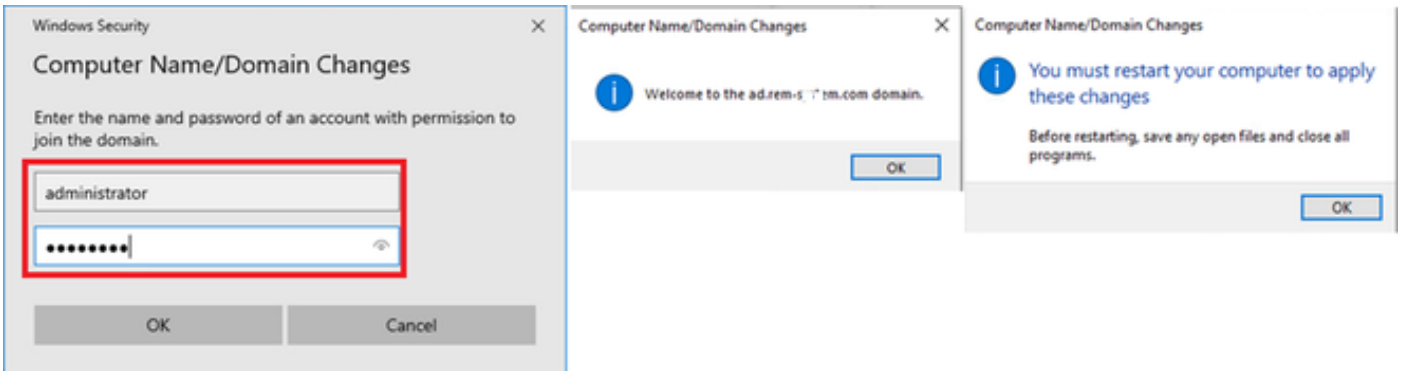
Paso 1. Agregar equipo al dominio AD

Vaya a Panel de control > Sistema y seguridad, haga clic en Sistema y, a continuación, haga clic en Configuración avanzada del sistema. En la ventana Propiedades del sistema, haga clic en Cambiar, seleccione Dominio e ingrese el nombre de dominio.



Agregar equipo al dominio AD

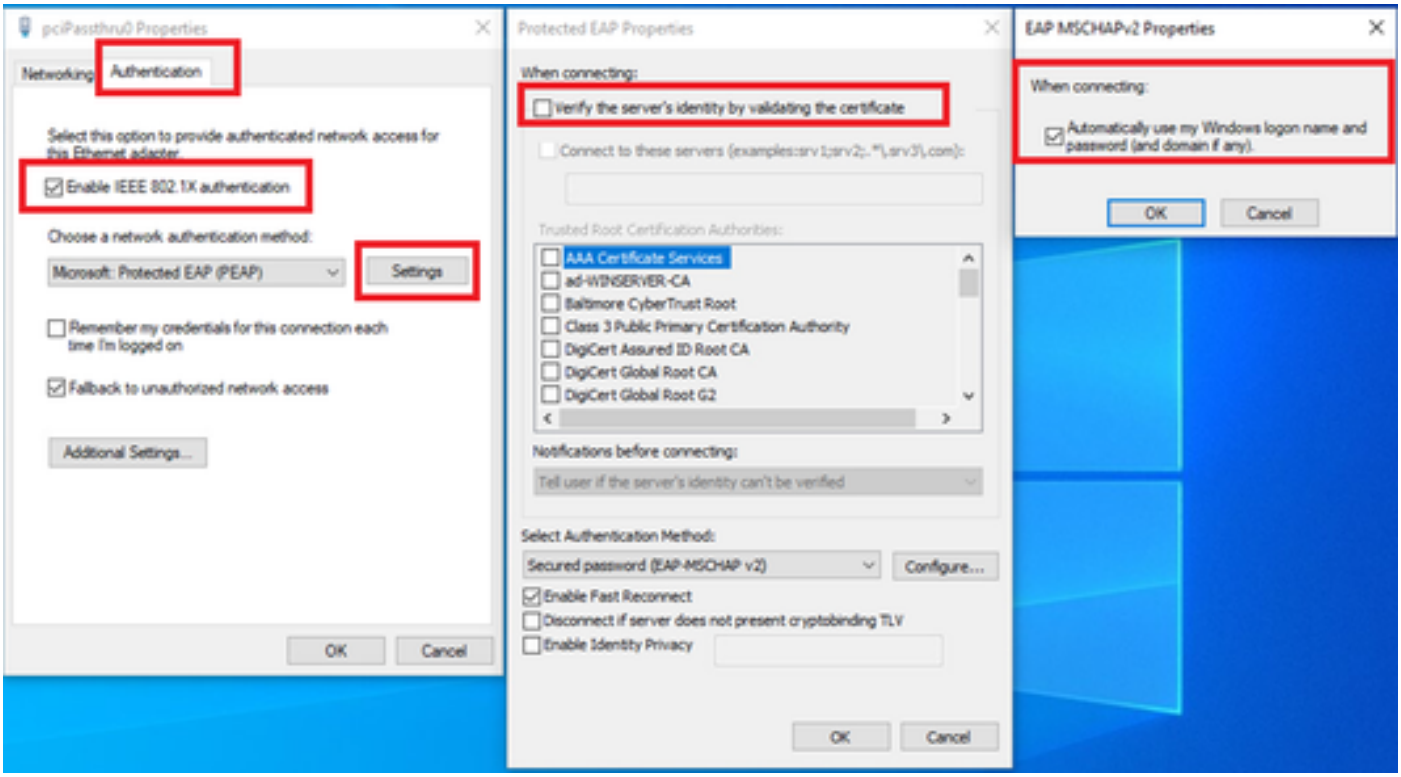
En la ventana Seguridad de Windows, introduzca el nombre de usuario y la contraseña del servidor de dominio.



Introducir nombre de usuario y contraseña

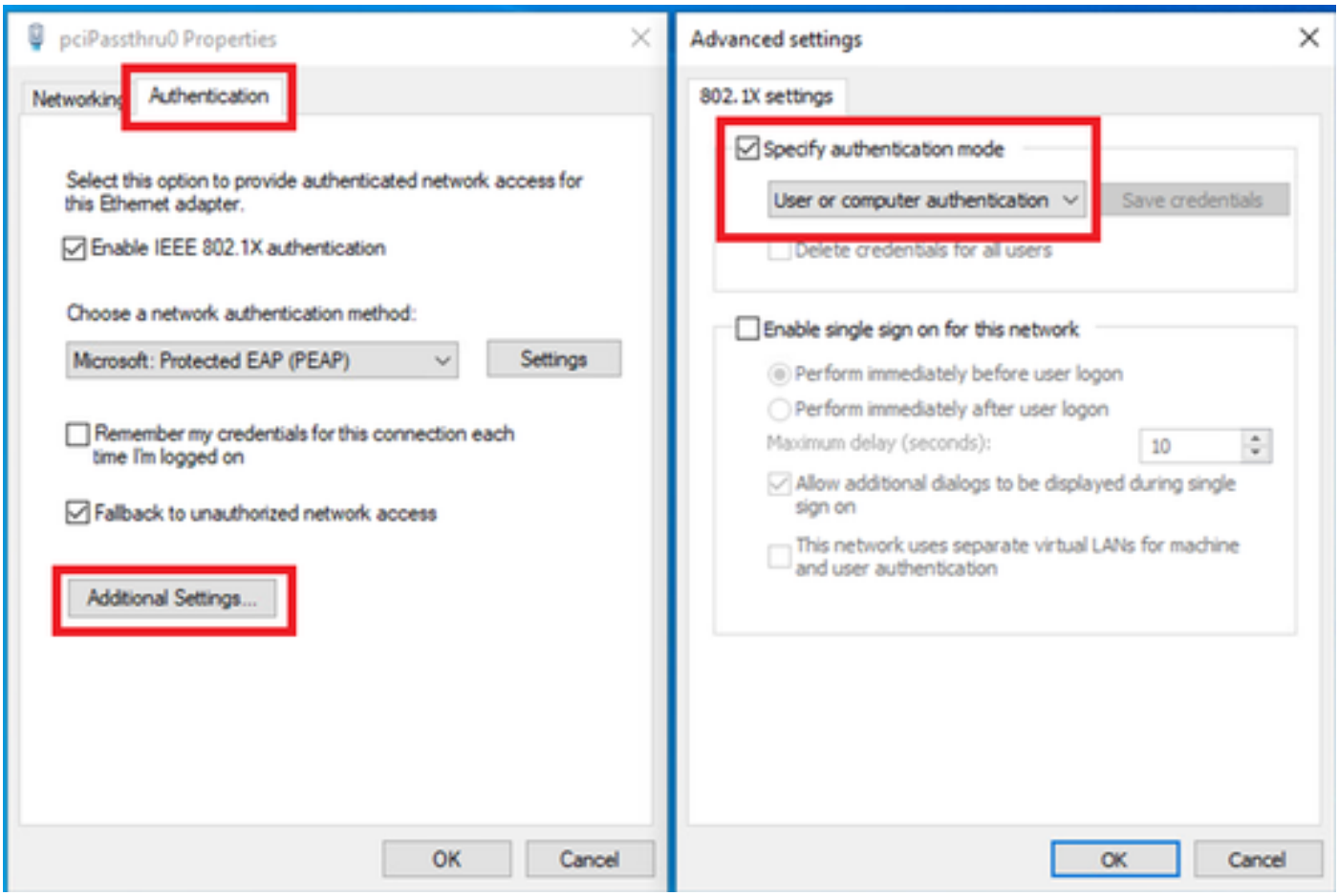
Paso 2. Configurar autenticación de usuario

Vaya a Authentication, marque Enable IEEE 802.1X authentication. Haga clic en Configuración en la ventana Propiedades de EAP protegido, desmarque Verificar la identidad del servidor validando el certificado y luego haga clic en Configurar. En la ventana Propiedades de EAP MSCHAPv2, marque Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows (y dominio si lo hubiera) para utilizar el nombre de usuario introducido durante el inicio de sesión de la máquina Windows para la autenticación de usuario.



Habilitar autenticación de usuario

Navegue hasta Autenticación, marque Configuración adicional. Seleccione Autenticación de usuario o equipo en la lista desplegable.

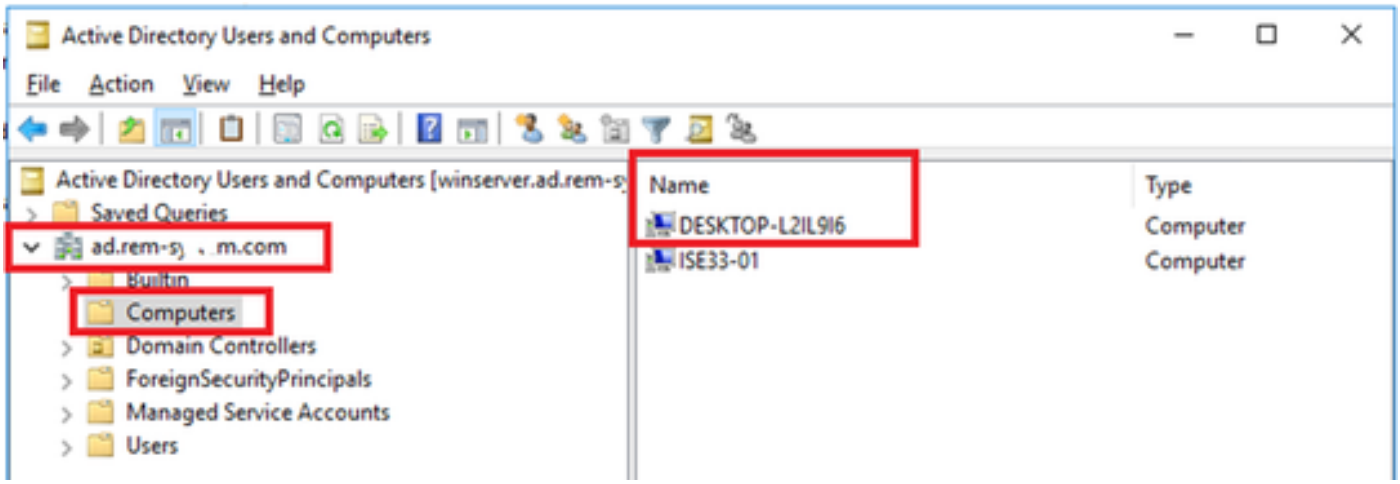


Especificar modo de autenticación

Configuración en Windows Server

Paso 1. Confirmar equipos de dominio

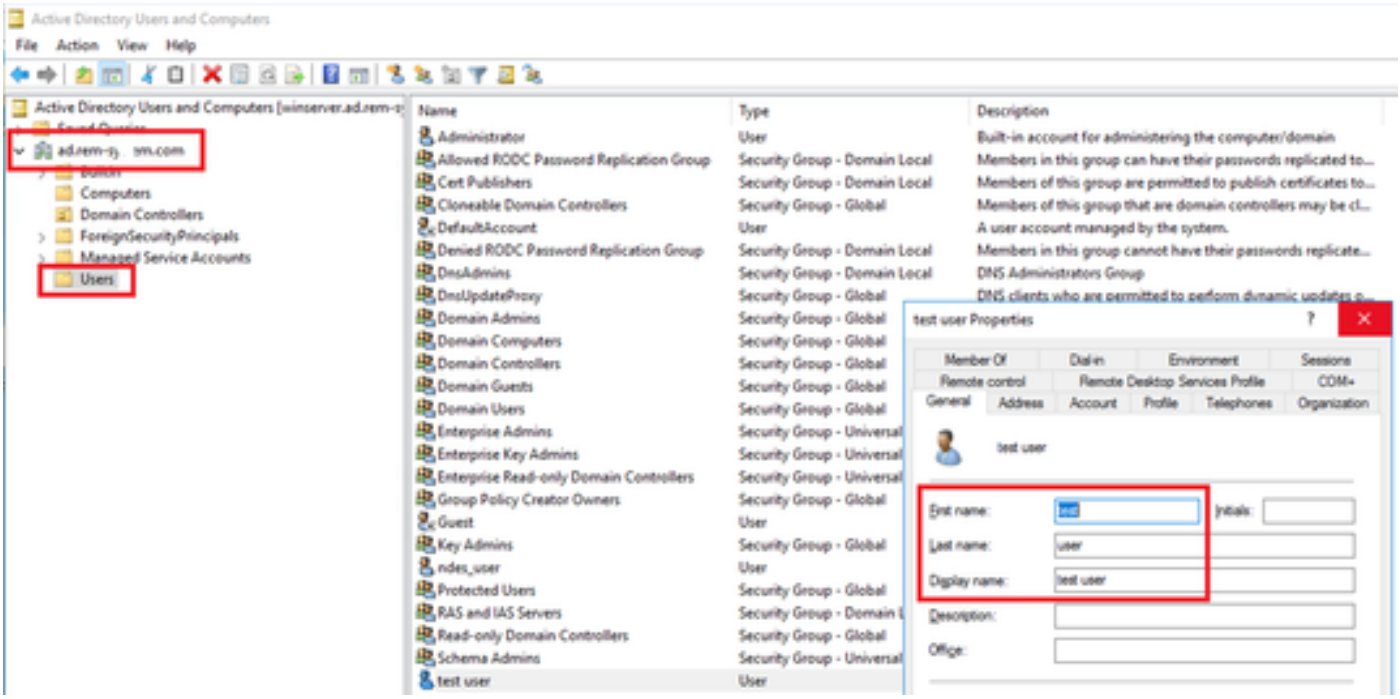
Vaya a Usuarios y equipos de Active Directory, haga clic en Equipos. Confirme que Win10 PC1 aparezca en el dominio.



Confirmar equipo de dominio

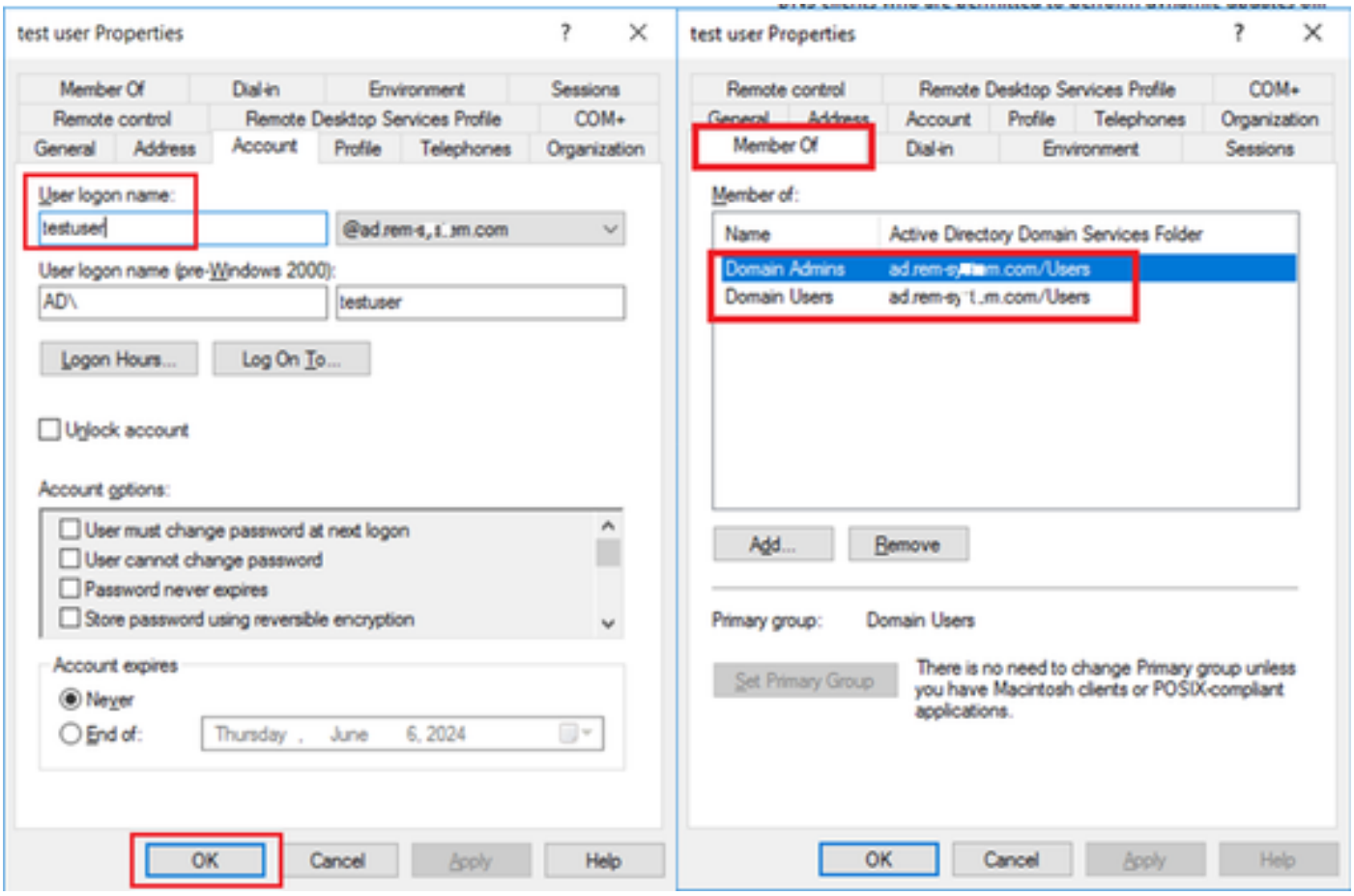
Paso 2. Agregar usuario de dominio

Navegue hasta Usuarios y equipos de Active Directory, haga clic en Usuarios. Agregue testuser como usuario de dominio.



Agregar usuario de dominio

Agregue el usuario de dominio a un miembro de Domain Admins y Domain Users.

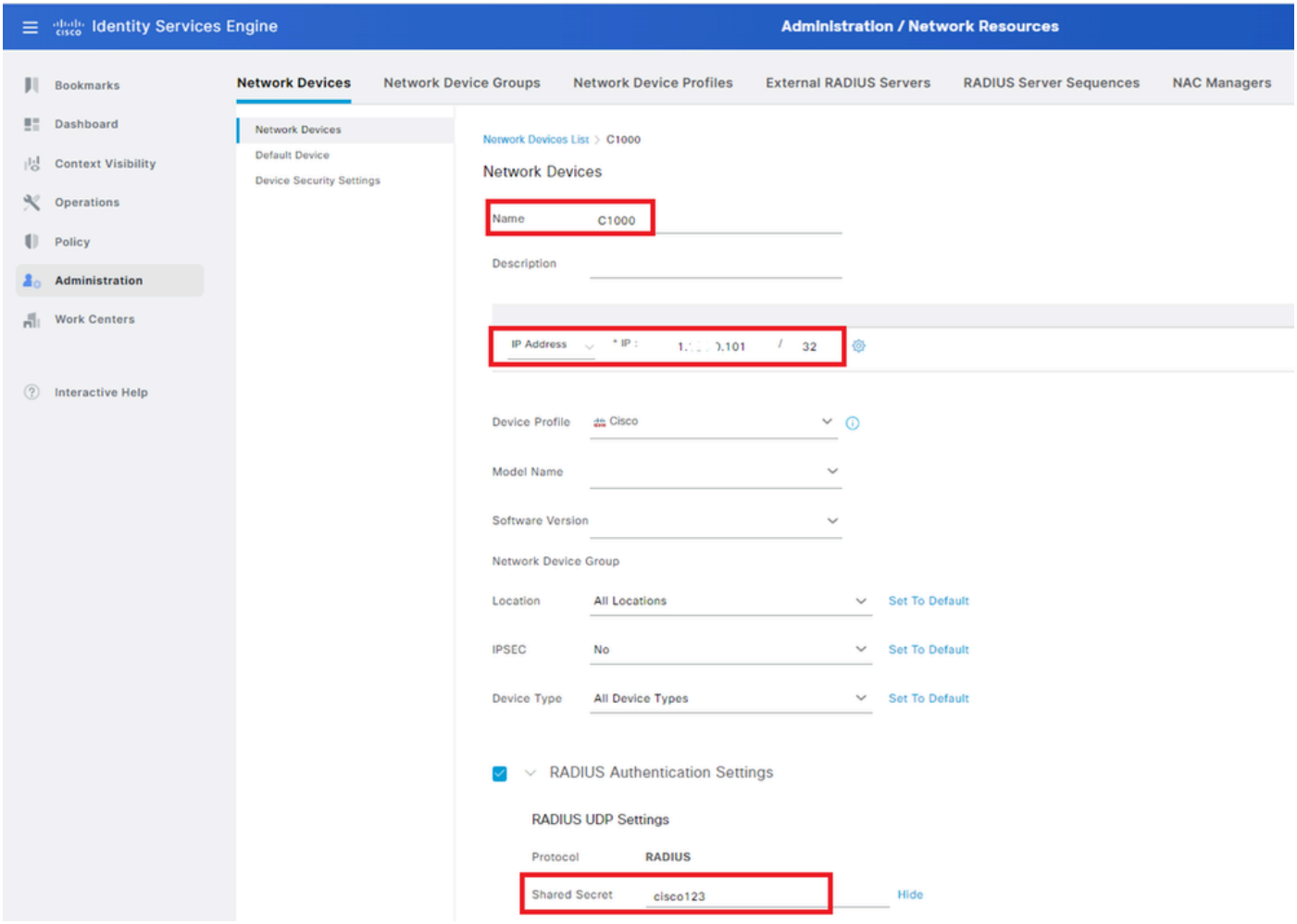


Administradores de dominio y usuarios de dominio

Configuración en ISE

Paso 1. Agregar dispositivo

Vaya a Administration > Network Devices, haga clic en el botón Add para agregar el dispositivo C1000.

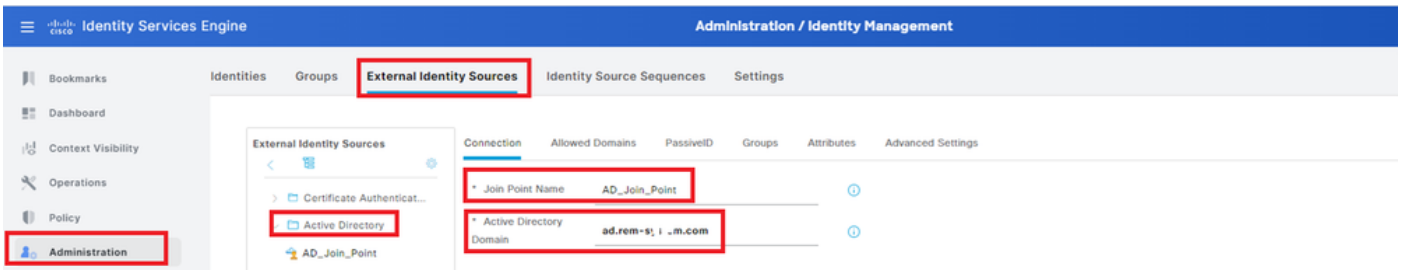


Agregar dispositivo

Paso 2. Agregar Active Directory

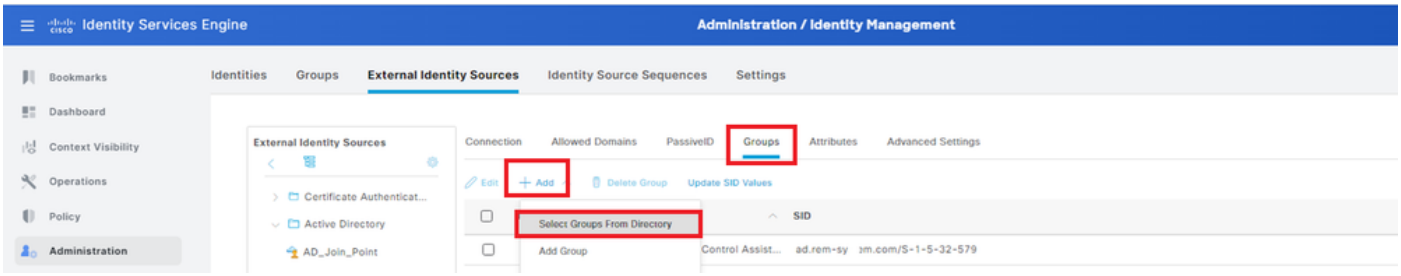
Vaya a Administration > External Identity Sources > Active Directory, haga clic en la pestaña Connection, agregue Active Directory a ISE.

- Nombre del punto de unión: AD_Join_Point
- Dominio de Active Directory: ad.rem-xxx.com



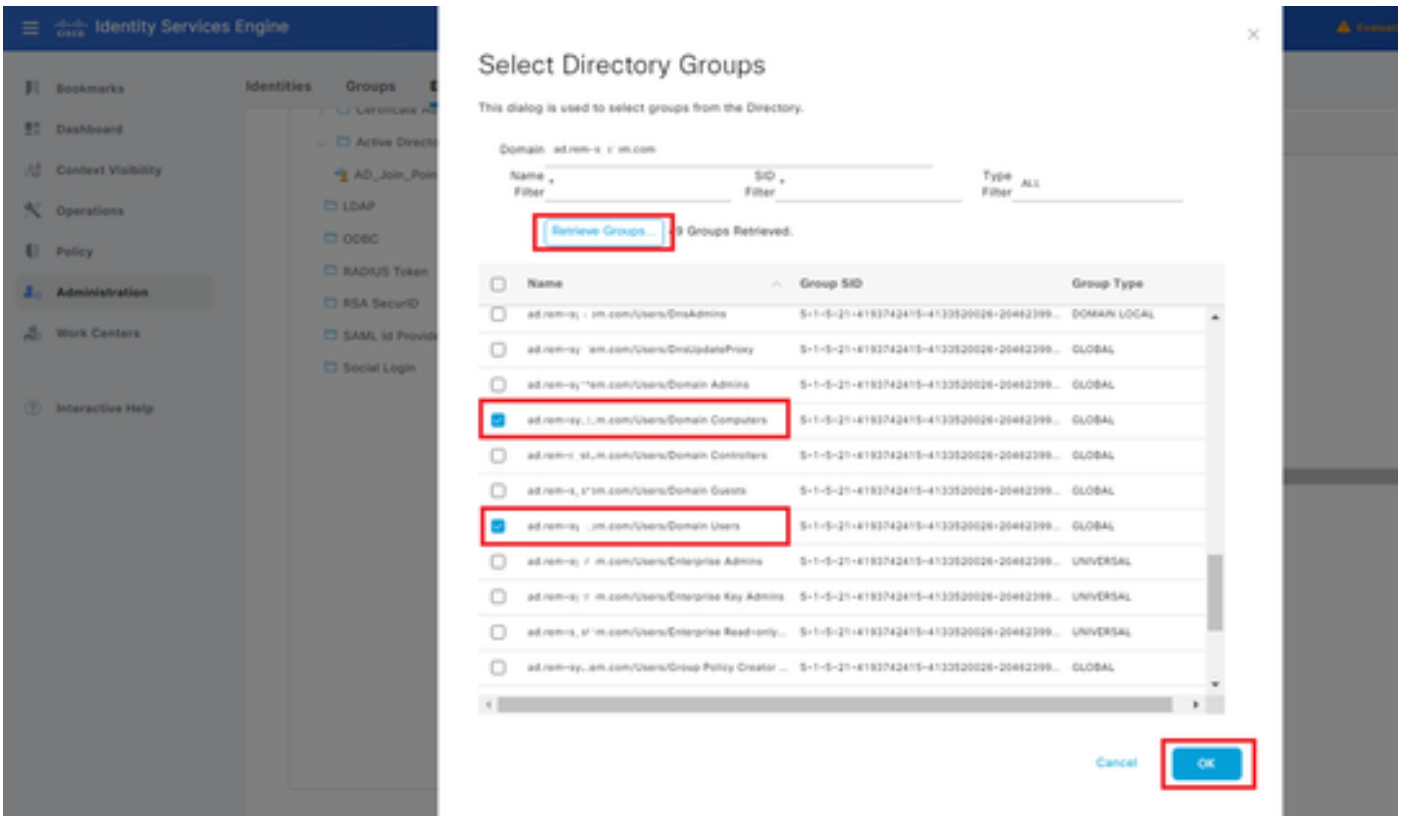
Agregar Active Directory

Vaya a la pestaña Grupos, seleccione Seleccionar grupos del directorio en la lista desplegable.



Seleccionar grupos del directorio

Haga clic en Recuperar grupos de la lista desplegable. Marque ad.rem-xxx.com/Users/Domain Computers y ad.rem-xxx.com/Users/Domain Users y haga clic en OK.



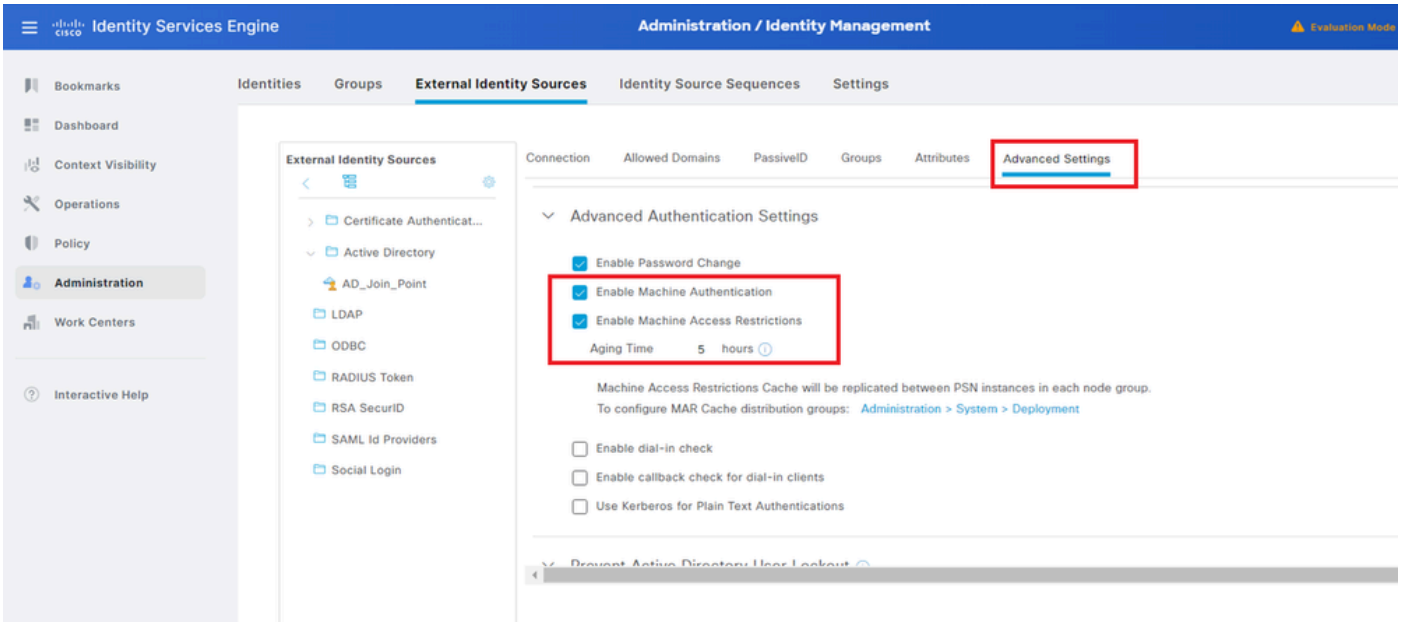
Agregar equipos y usuarios de dominio

Paso 3. Confirmar configuración de autenticación de equipo

Vaya a la pestaña Advanced Settings y confirme la configuración de la autenticación de la máquina.

- Habilitar autenticación de equipo: para habilitar la autenticación de equipo
- Habilitar restricción de acceso de equipo: para combinar la autenticación de usuario y equipo antes de la autorización

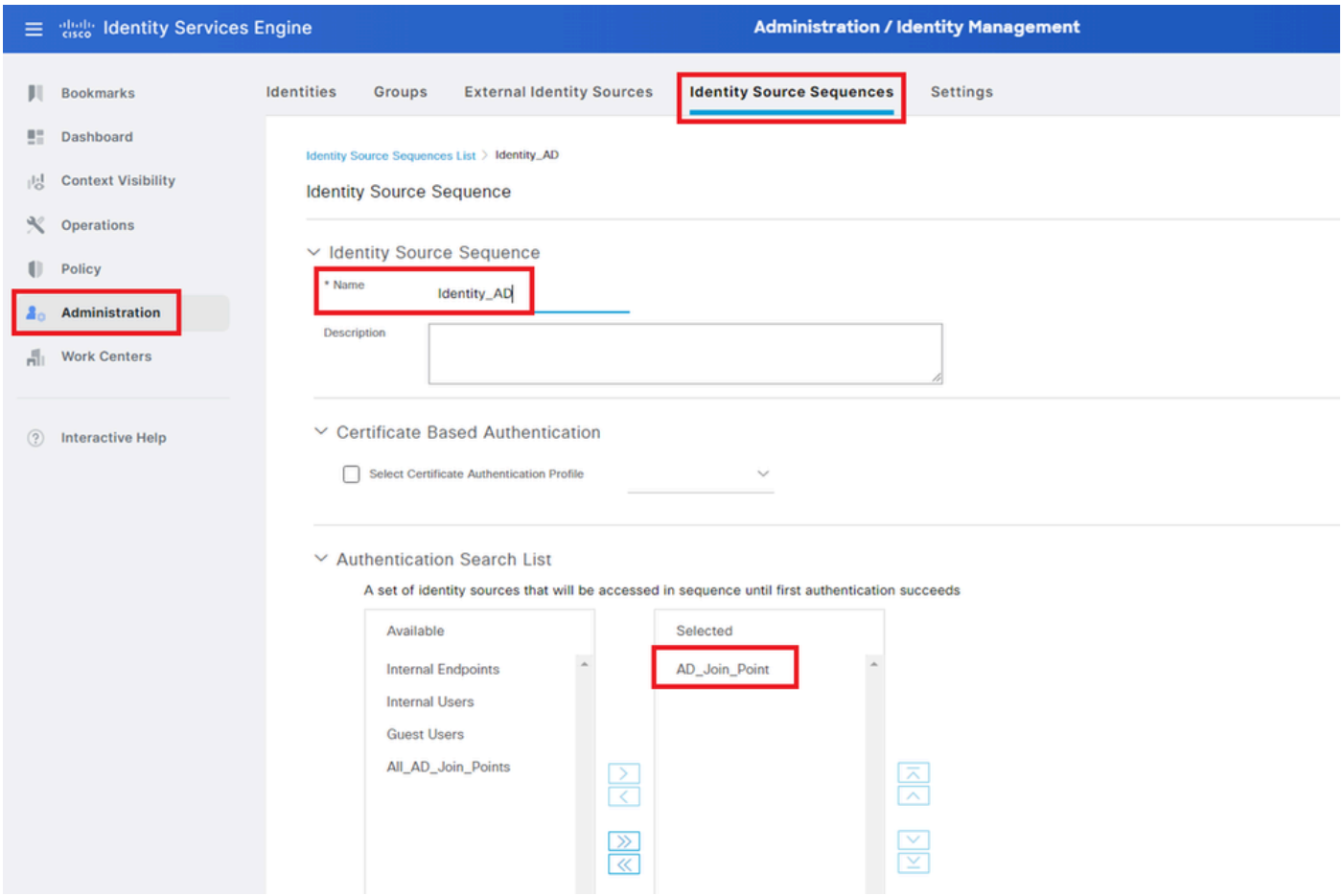
Nota: el intervalo válido de tiempo de caducidad es de 1 a 8760.



Paso 4. Agregar secuencias de origen de identidad

Vaya a Administration > Identity Source Sequences, agregue una secuencia de origen de identidad.

- Nombre: Identity_AD
- Lista de búsqueda de autenticación: AD_Join_Point

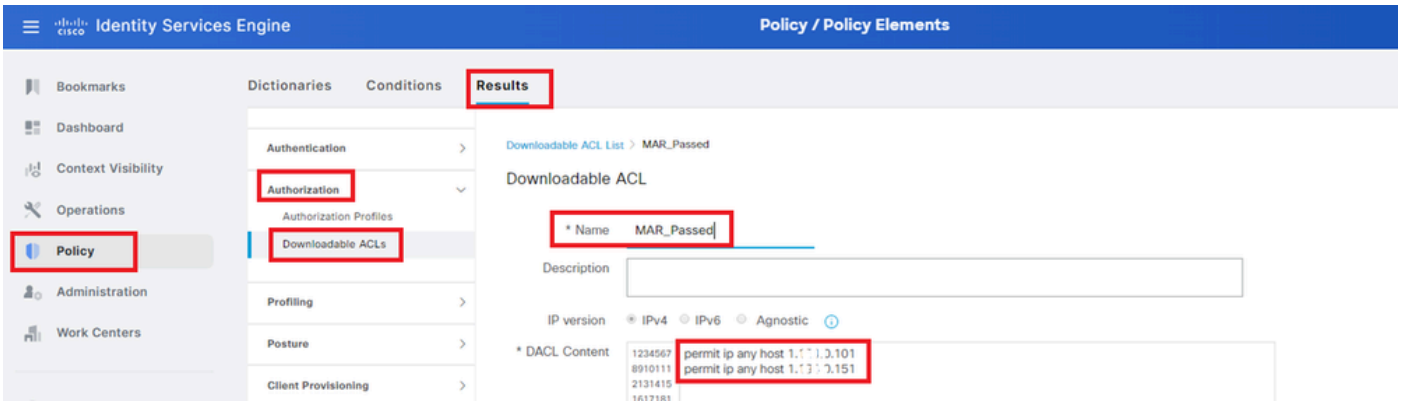


Agregar secuencias de origen de identidad

Paso 5. Agregar DACL y perfil de autorización

Navegue hasta Política > Resultados > Autorización > ACL descargables, agregue una DACL.

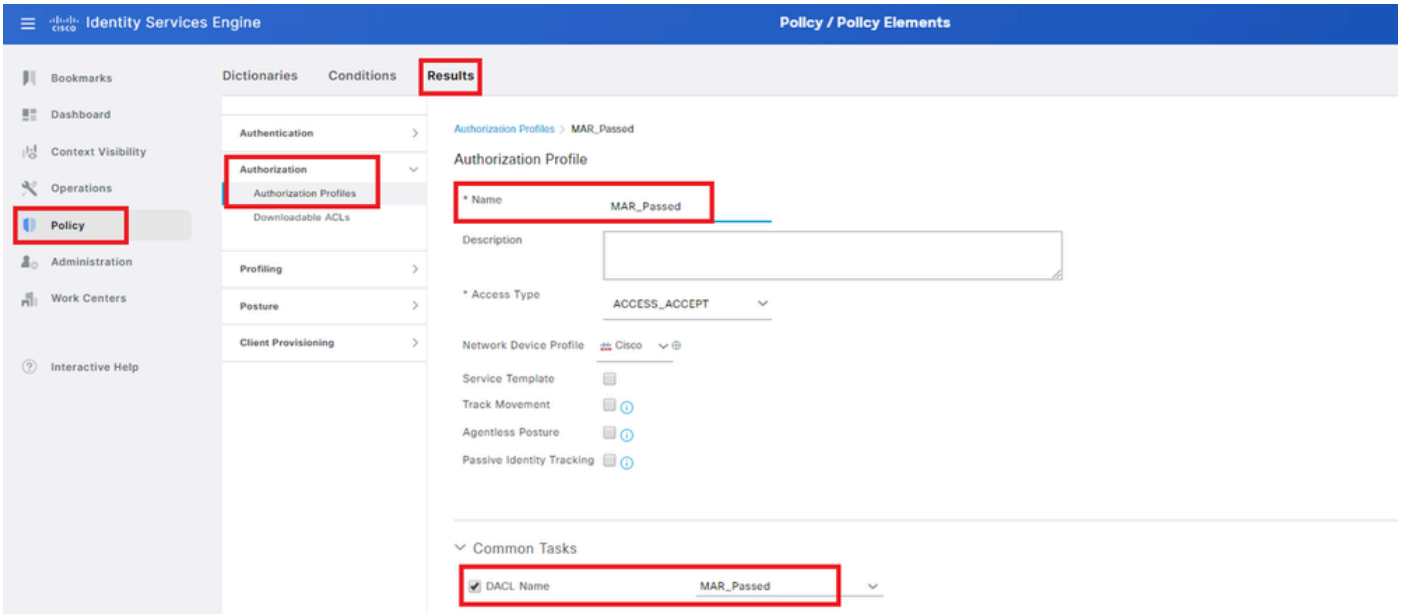
- Nombre: MAR_Passed
- Contenido DACL: permitir ip any host 1.x.x.101 y permitir ip any host 1.x.x.105



Agregar DACL

Vaya a Policy > Results > Authorization > Authorization Profiles, agregue un perfil de autorización.

- Nombre: MAR_Passed
- Nombre de DACL: MAR_Passed

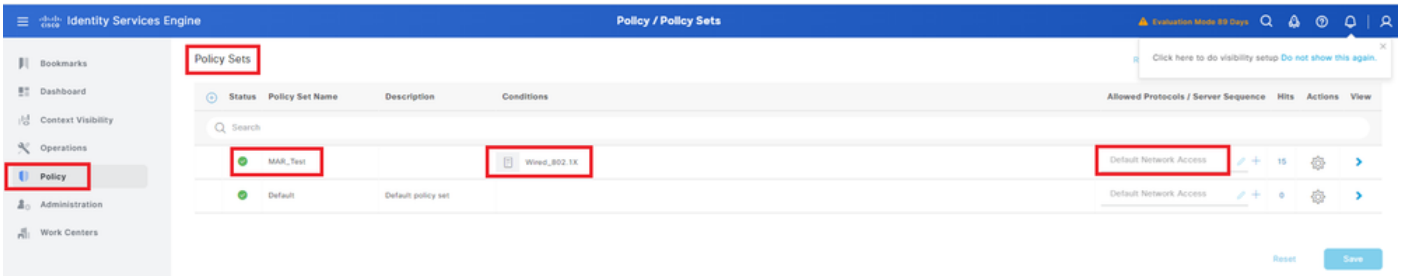


Agregar perfil de autorización

Paso 6. Agregar conjunto de políticas

Navegue hasta Policy > Policy Sets, haga clic en + para agregar un conjunto de políticas.

- Nombre del conjunto de políticas: MAR_Test
- Condiciones: Wired_802.1X
- Protocolos / Secuencia de servidor permitidos: acceso a red predeterminado



Agregar conjunto de políticas

Paso 7. Agregar política de autenticación

Navegue hasta Conjuntos de políticas, haga clic en MAR_Test para agregar una política de autenticación.

- Nombre de regla: MAR_dot1x
- Condiciones: Wired_802.1X
- Uso: Identity_AD

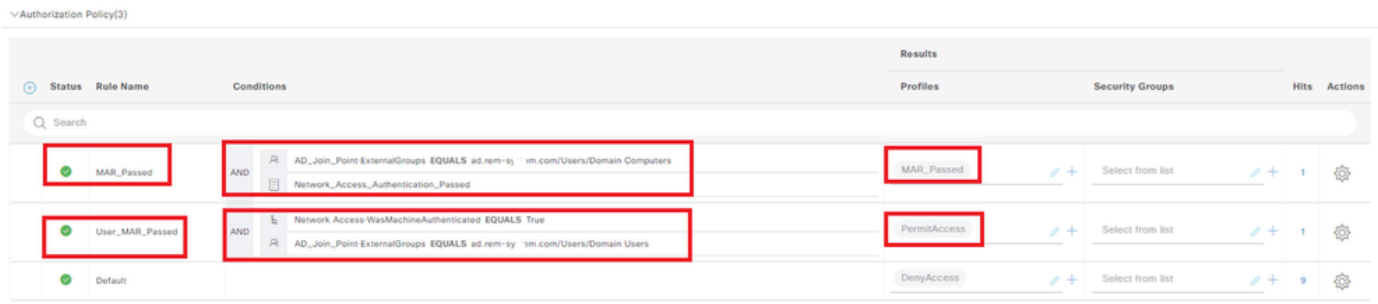
Agregar política de autenticación

Paso 8. Agregar política de autorización

Navegue hasta Conjuntos de políticas, haga clic en MAR_Test para agregar una política de autorización.

- Nombre de regla: MAR_Passed
- Condiciones: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- Resultados: MAR_Passed

- Nombre de regla: User_MAR_Passed
- Condiciones: Network Access·WasMachineAuthenticated EQUALS True Y AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Usuarios
- Resultados: PermitAccess



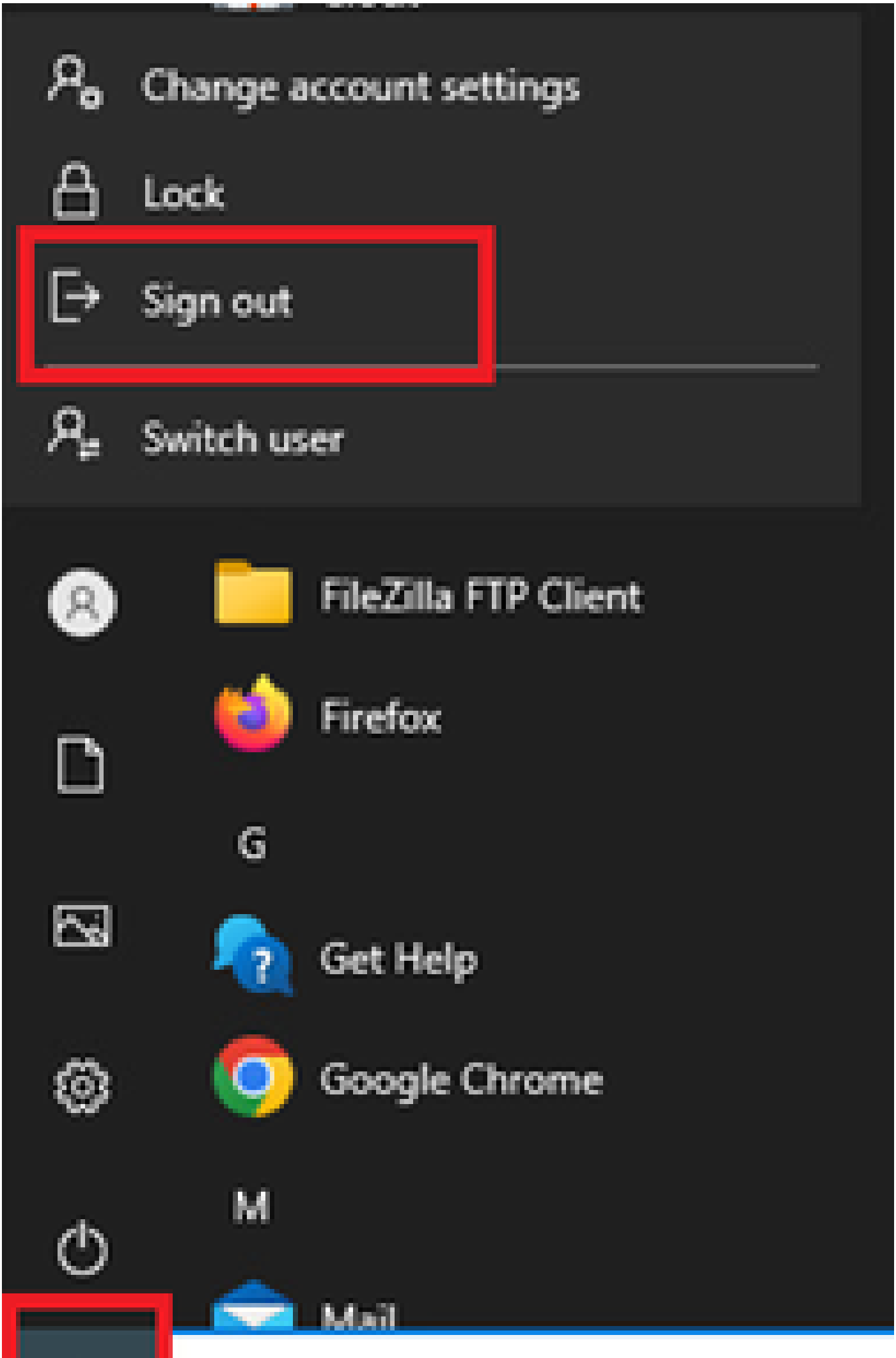
Agregar directiva de autorización

Verificación

Patrón 1. Autenticación de equipo y autenticación de usuario

Paso 1. Cerrar sesión en PC con Windows

Haga clic en el botón Sign out de Win10 PC1 para activar la autenticación del equipo.


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

show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de la máquina en 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:

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)

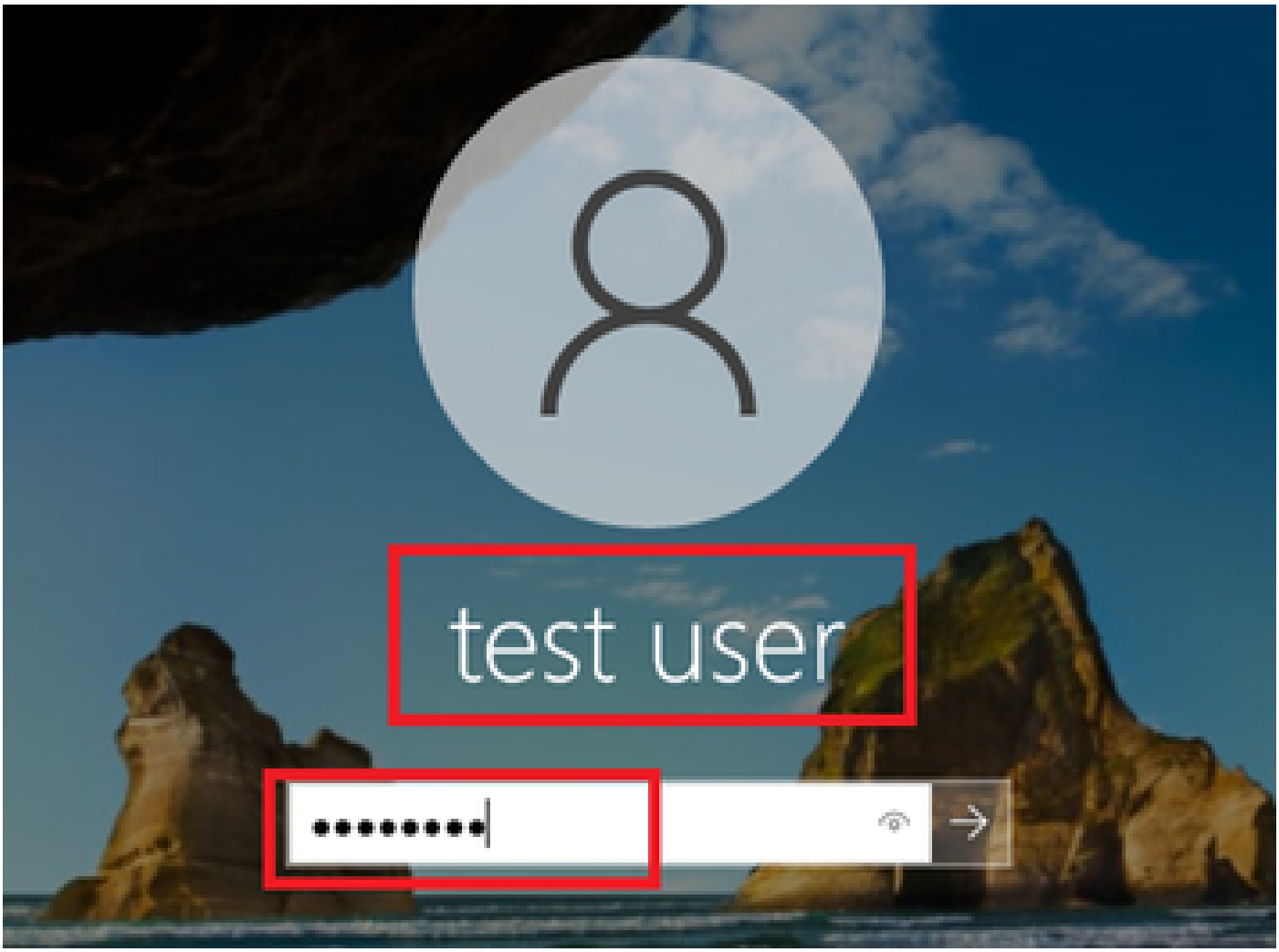
Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success

Paso 3. Iniciar sesión en Windows PC

Inicie sesión en Win10 PC1, introduzca el nombre de usuario y la contraseña para activar la autenticación de usuario.



Iniciar sesión en Windows PC

Paso 4. Confirmar sesión de autenticación

Ejecute show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de usuario en 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:
```

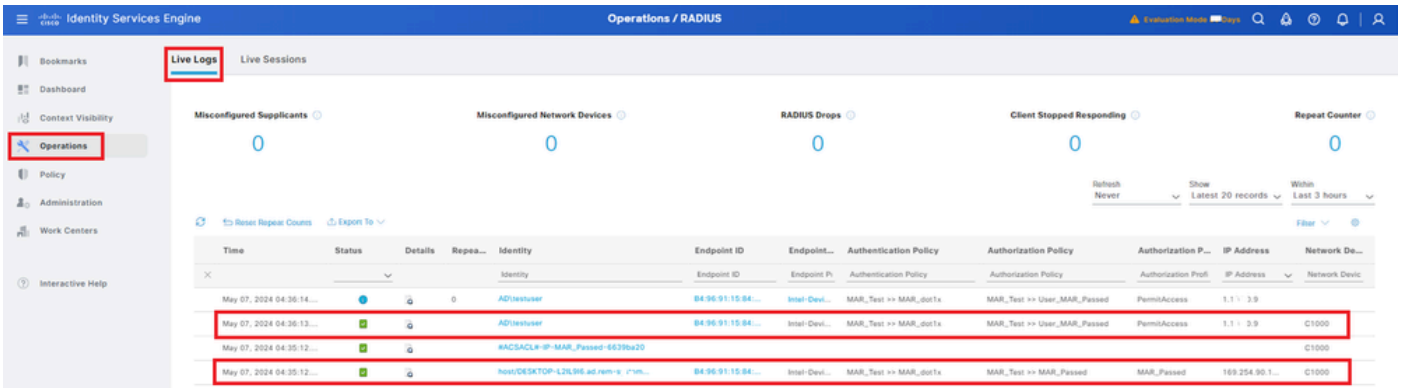
AD\testuser

```
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
```

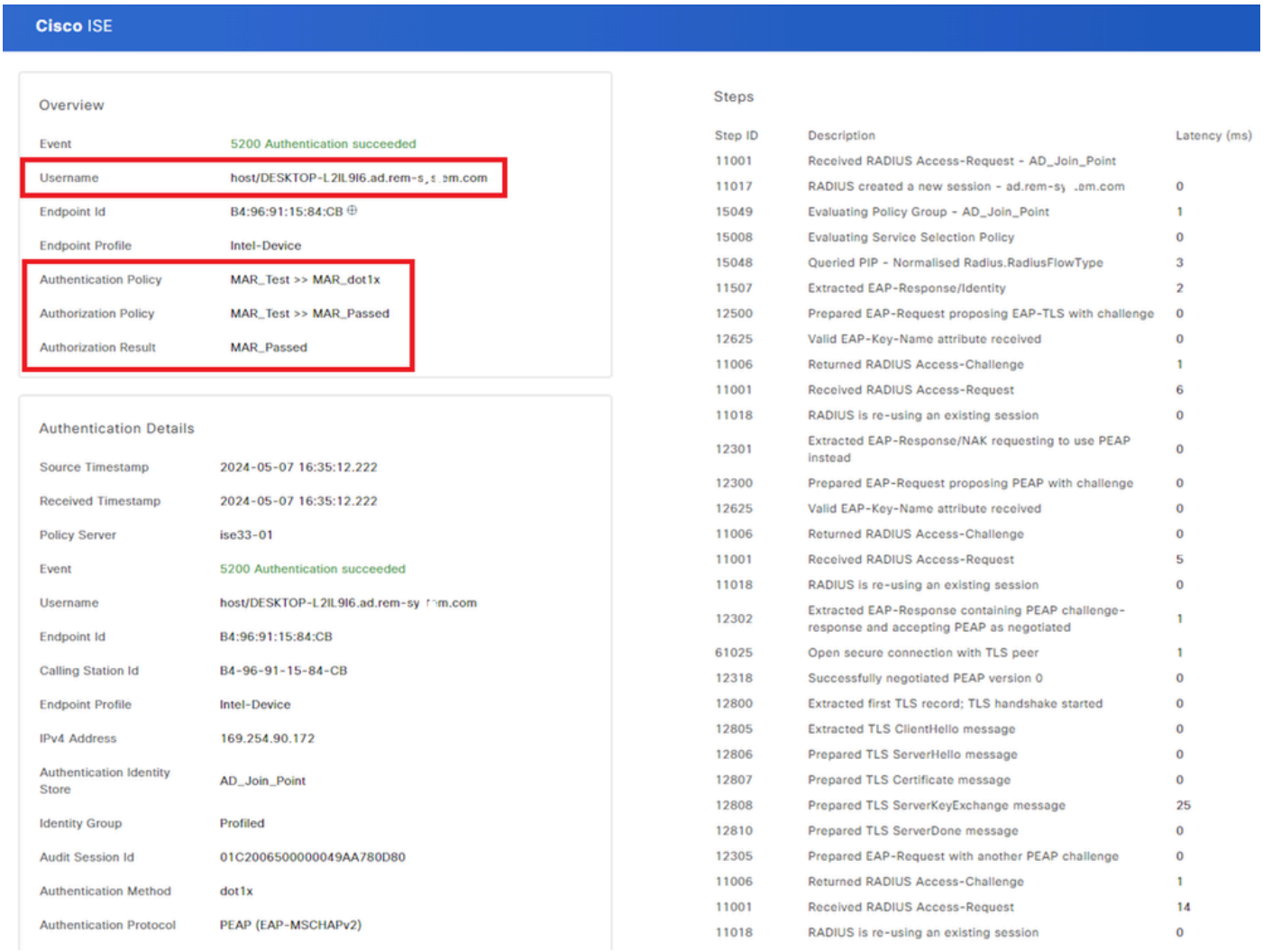
Paso 5. Confirmar registro en directo de Radius

Navegue hasta **Operaciones > RADIUS > Registros en vivo** en la GUI de ISE, confirme el registro en vivo para la autenticación de máquina y la autenticación de usuario.



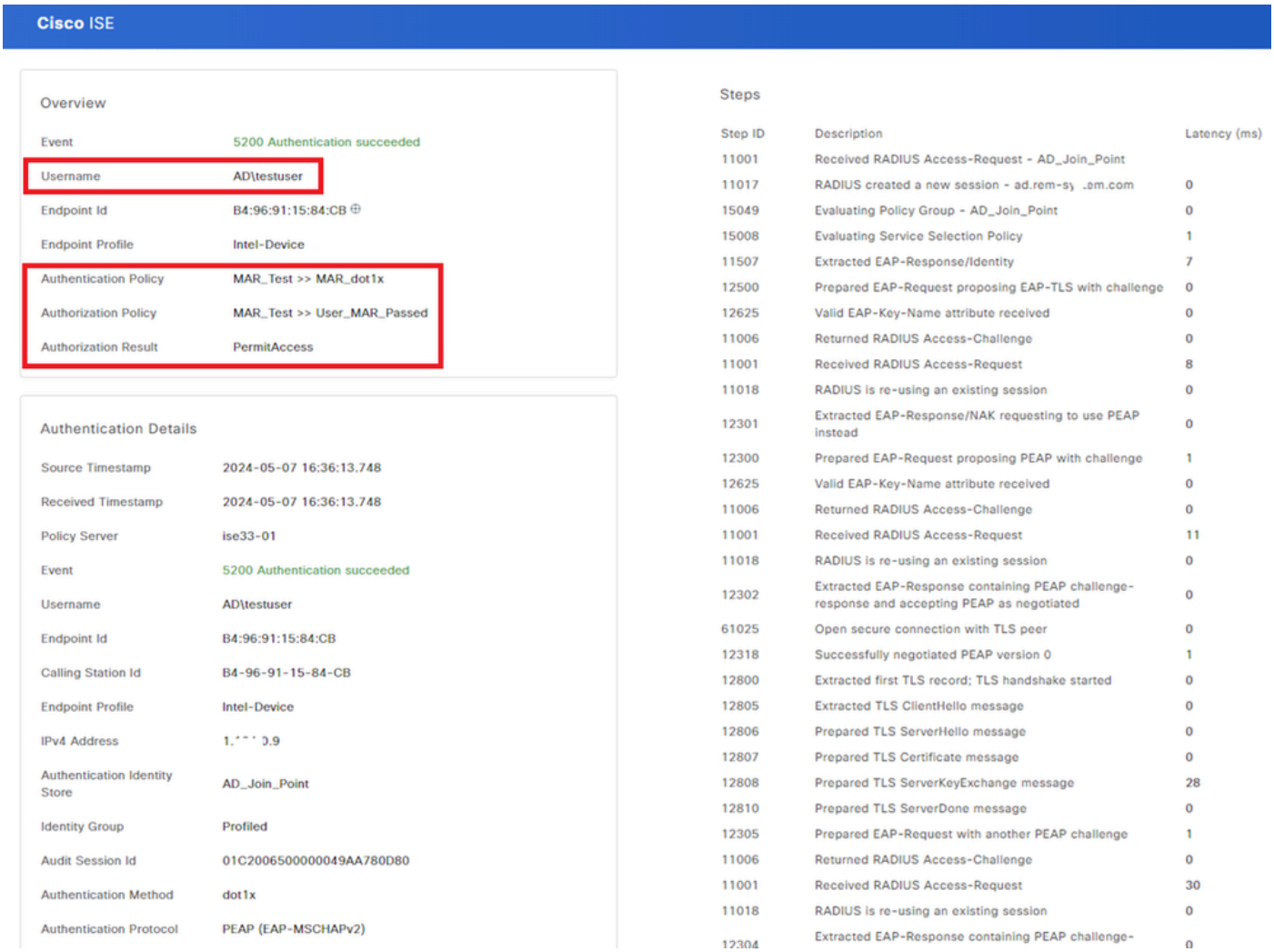
Registro en directo de Radius

Confirme el registro en vivo detallado de la autenticación de la máquina.



Detalle de autenticación de máquina

Confirme el registro en vivo detallado de la autenticación de usuario.



Detalle de la autenticación de usuario

Patrón 2. Sólo autenticación de usuario

Paso 1. Desactivar y activar NIC de PC con Windows

Para activar la autenticación de usuario, inhabilite y habilite la NIC de Win10 PC1.

Paso 2. Confirmar sesión de autenticación

Ejecute show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de usuario en C1000.

<#root>

Switch#

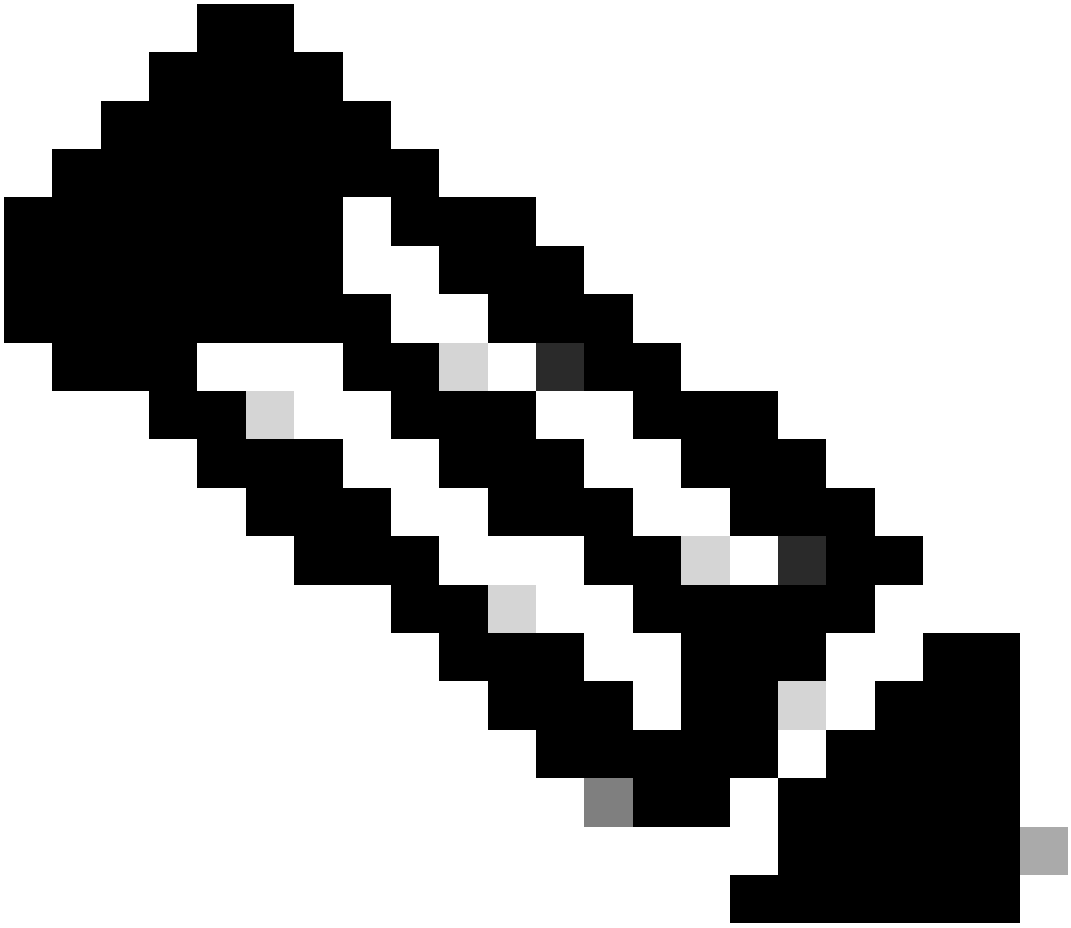
show authentication sessions interface GigabitEthernet1/0/2 details

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

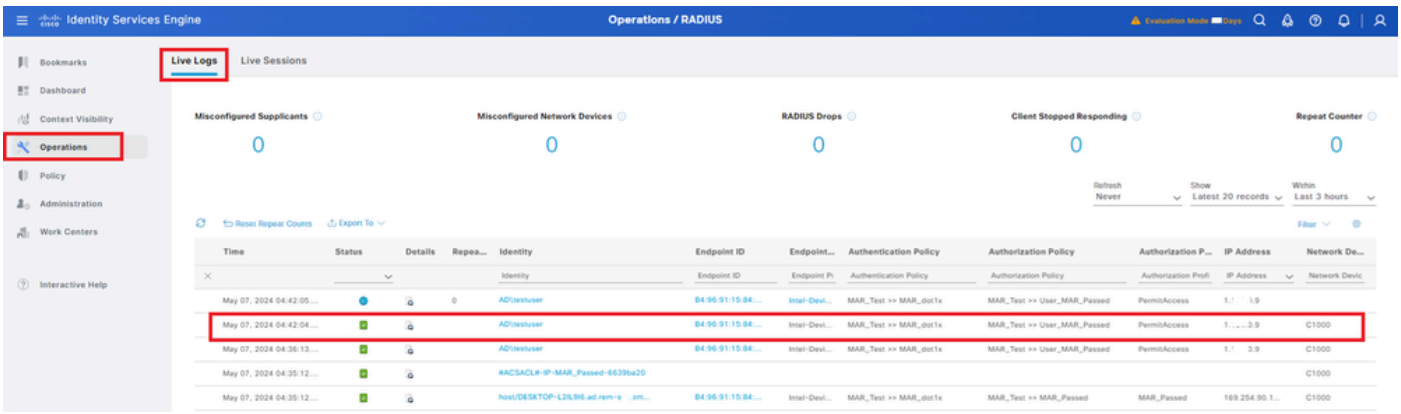
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: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

Paso 3. Confirmar registro en directo de Radius

Navegue hasta **Operaciones > RADIUS > Registros en vivo** en la GUI de ISE, confirme el registro en vivo para la autenticación del usuario.

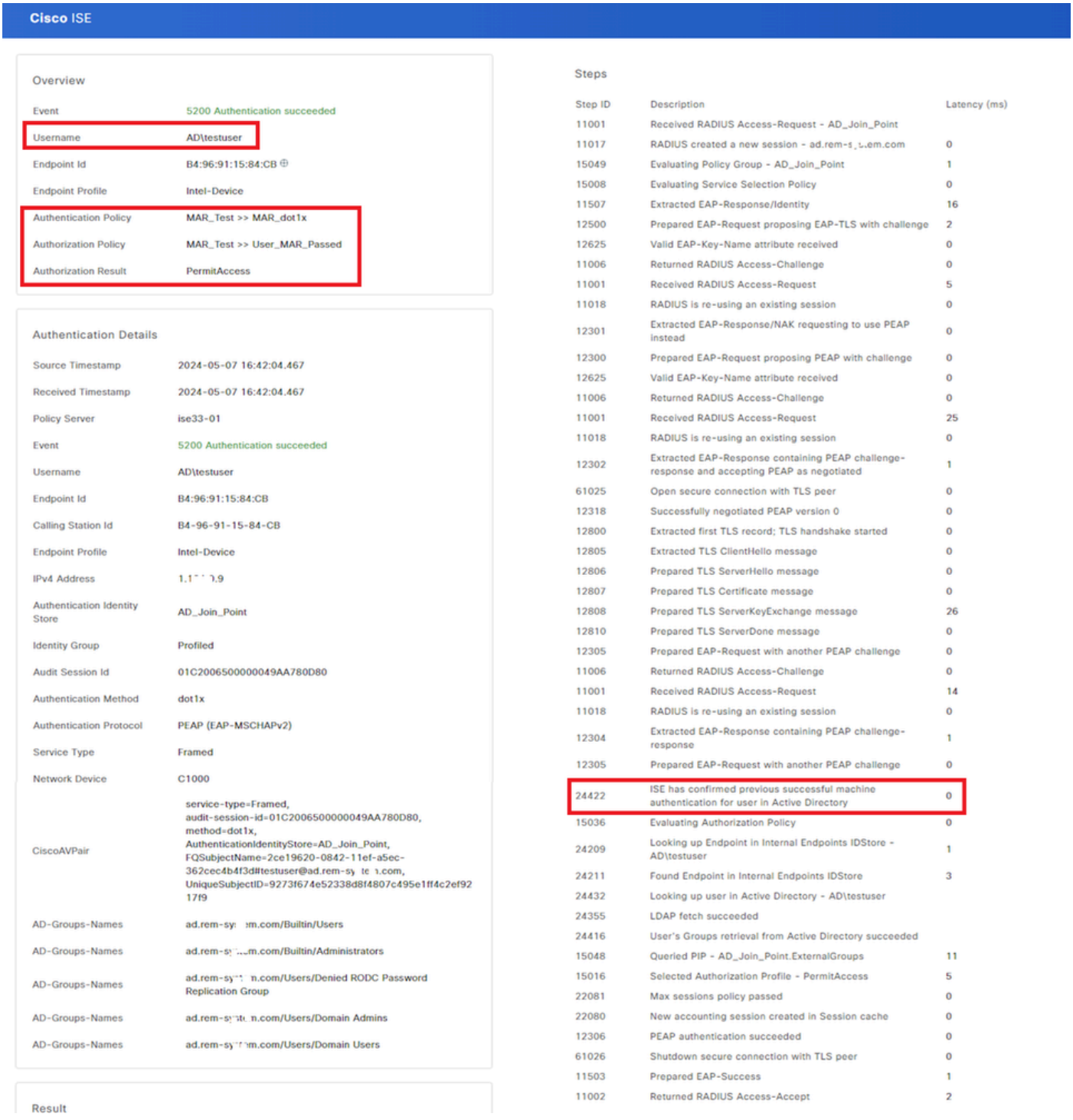


Nota: dado que la caché MAR se almacena en ISE, solo se necesita la autenticación de usuario.



Registro en directo de Radius

Confirme el registro en vivo detallado de la autenticación de usuario.



Detalle de la autenticación de usuario

Troubleshoot

Estos registros de depuración (port-server.log) le ayudan a confirmar el comportamiento detallado de la autenticación en ISE.

- runtime-config

- registro en tiempo de ejecución

- Runtime-AAA

Este es un ejemplo del registro de depuración para el **Patrón 1. Autenticación de máquina y Autenticación de usuario** en este 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

Información Relacionada

Ventajas y desventajas de la restricción de acceso a máquinas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).