

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Antecedentes](#)

[Configuraciones](#)

[Configuración en C1000](#)

[Configuración en PC con Windows](#)

[Paso 1. Agregar equipo al dominio AD](#)

[Paso 2. Configurar autenticación de usuario](#)

[Configuración en Windows Server](#)

[Paso 1. Confirmar equipos de dominio](#)

[Paso 2. Agregar usuario de dominio](#)

[Configuración en ISE](#)

[Paso 1. Agregar dispositivo](#)

[Paso 2. Agregar Active Directory](#)

[Paso 3. Confirmar configuración de autenticación de equipo](#)

[Paso 4. Agregar secuencias de origen de identidad](#)

[Paso 5. Agregar DACL y perfil de autorización](#)

[Paso 6. Agregar conjunto de políticas](#)

[Paso 7. Agregar política de autenticación](#)

[Paso 8. Agregar política de autorización](#)

[Verificación](#)

[Patrón 1. Autenticación de equipo y autenticación de usuario](#)

[Paso 1. Cerrar sesión en PC con Windows](#)

[Paso 2. Confirmar sesión de autenticación](#)

[Paso 3. Iniciar sesión en Windows PC](#)

[Paso 4. Confirmar sesión de autenticación](#)

[Paso 5. Confirmar registro en directo de Radius](#)

[Patrón 2. Sólo autenticación de usuario](#)

[Paso 1. Desactivar y activar NIC de PC con Windows](#)

[Paso 2. Confirmar sesión de autenticación](#)

[Paso 3. Confirmar registro en directo de Radius](#)

[Troubleshoot](#)

[Información Relacionada](#)

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.

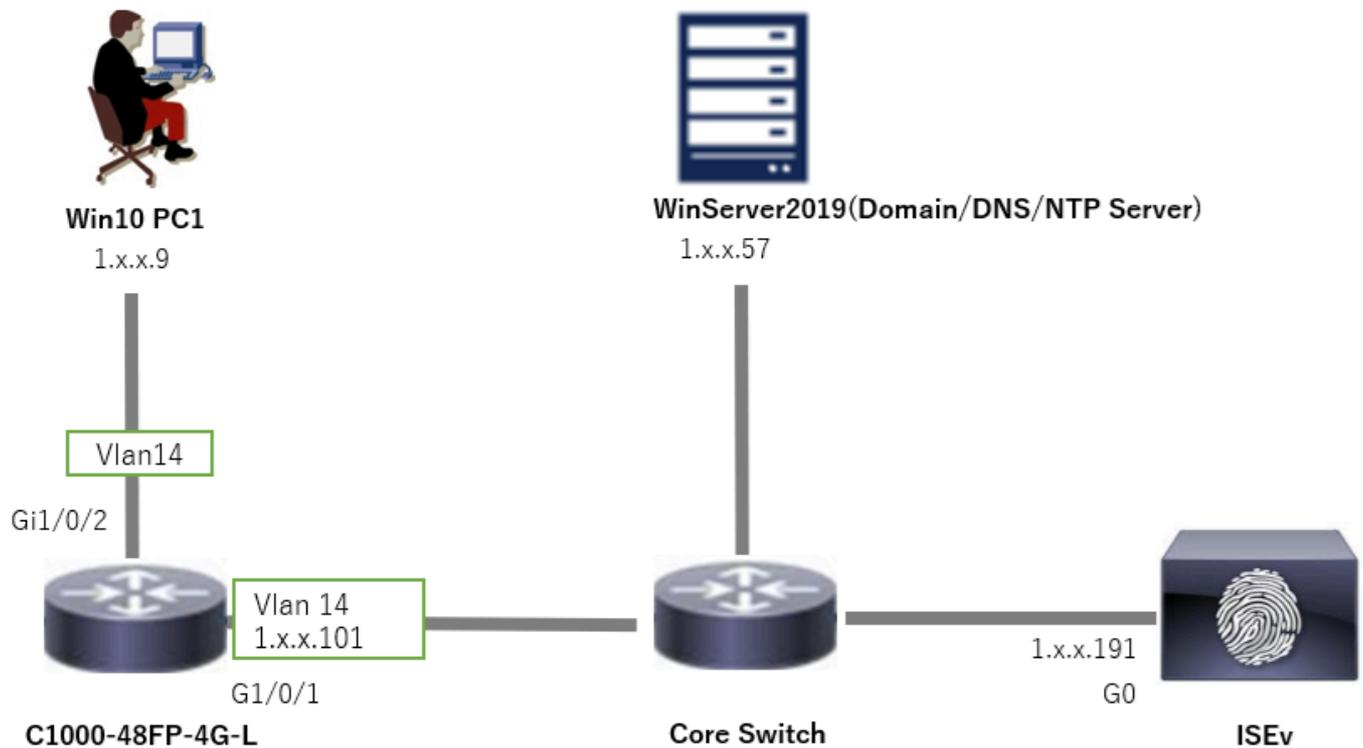


Diagrama de la red

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
```

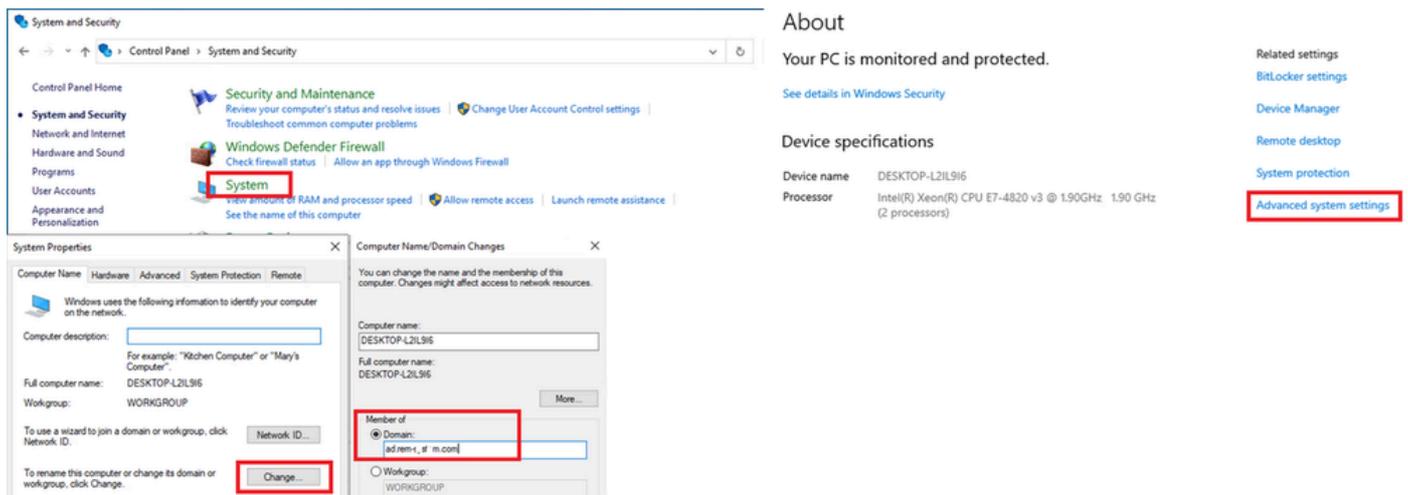
```
interface GigabitEthernet1/0/1  
switchport access vlan 14  
switchport mode access
```

```
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

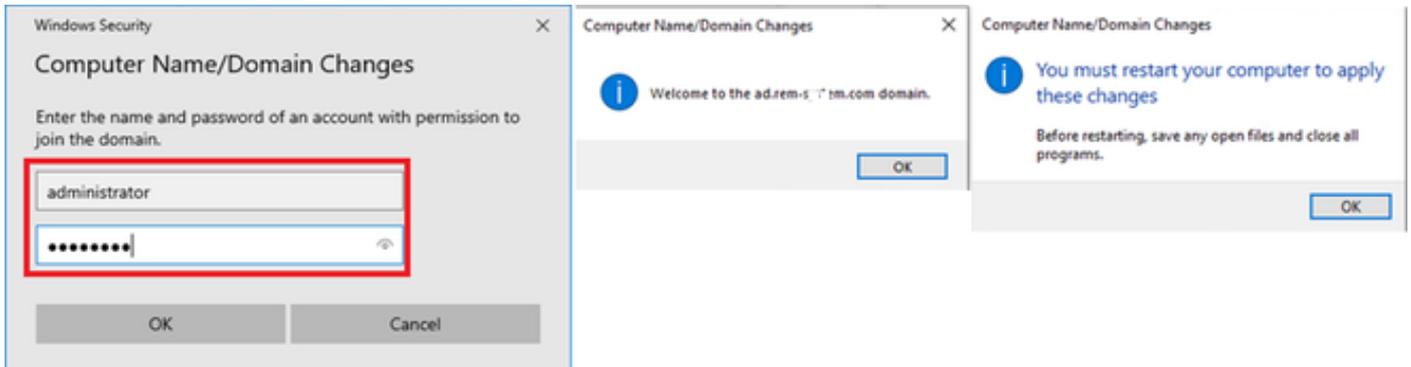
Paso 1. Agregar equipo al dominio AD

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

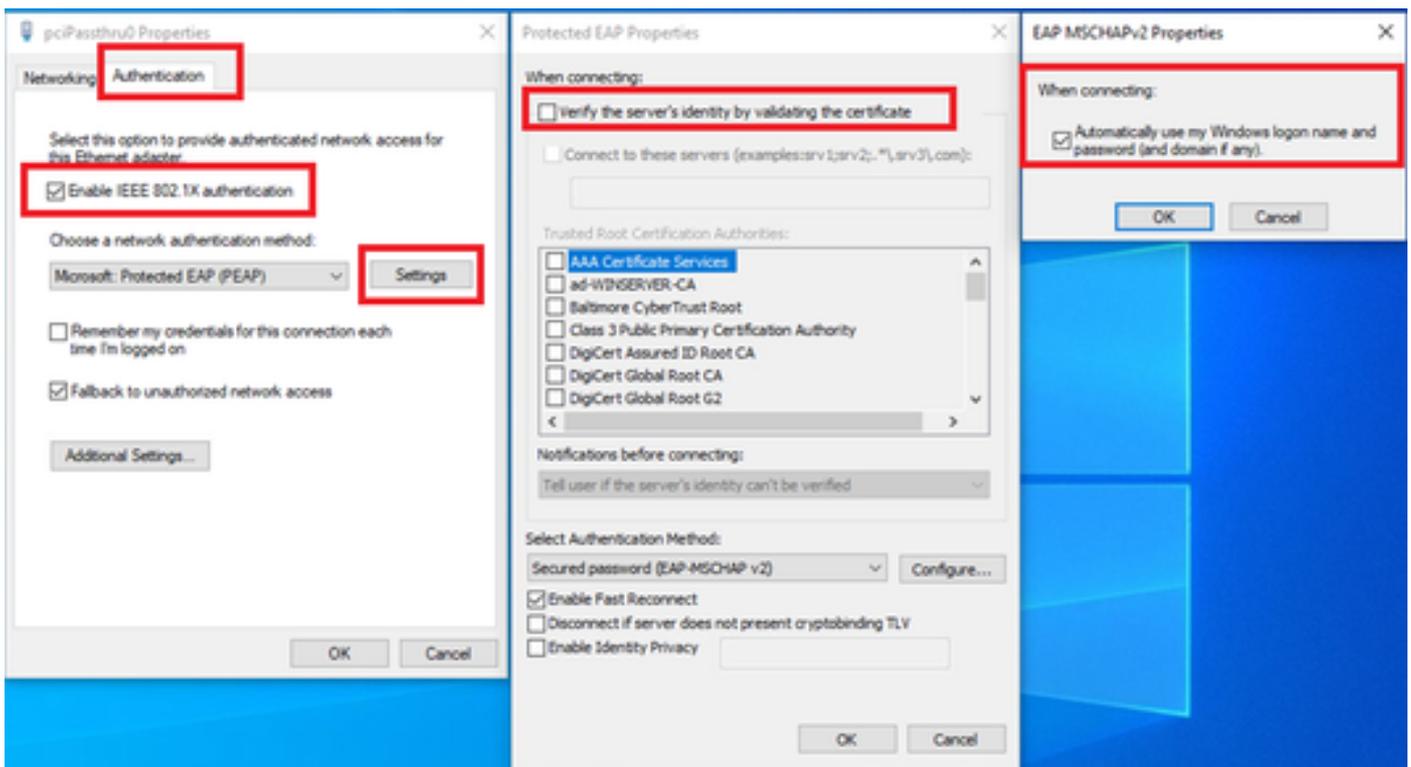
En la ventana Seguridad de Windows, introduzca el nombre de usuario y la contraseña del servidor de dominio.



Introducir nombre de usuario y contraseña

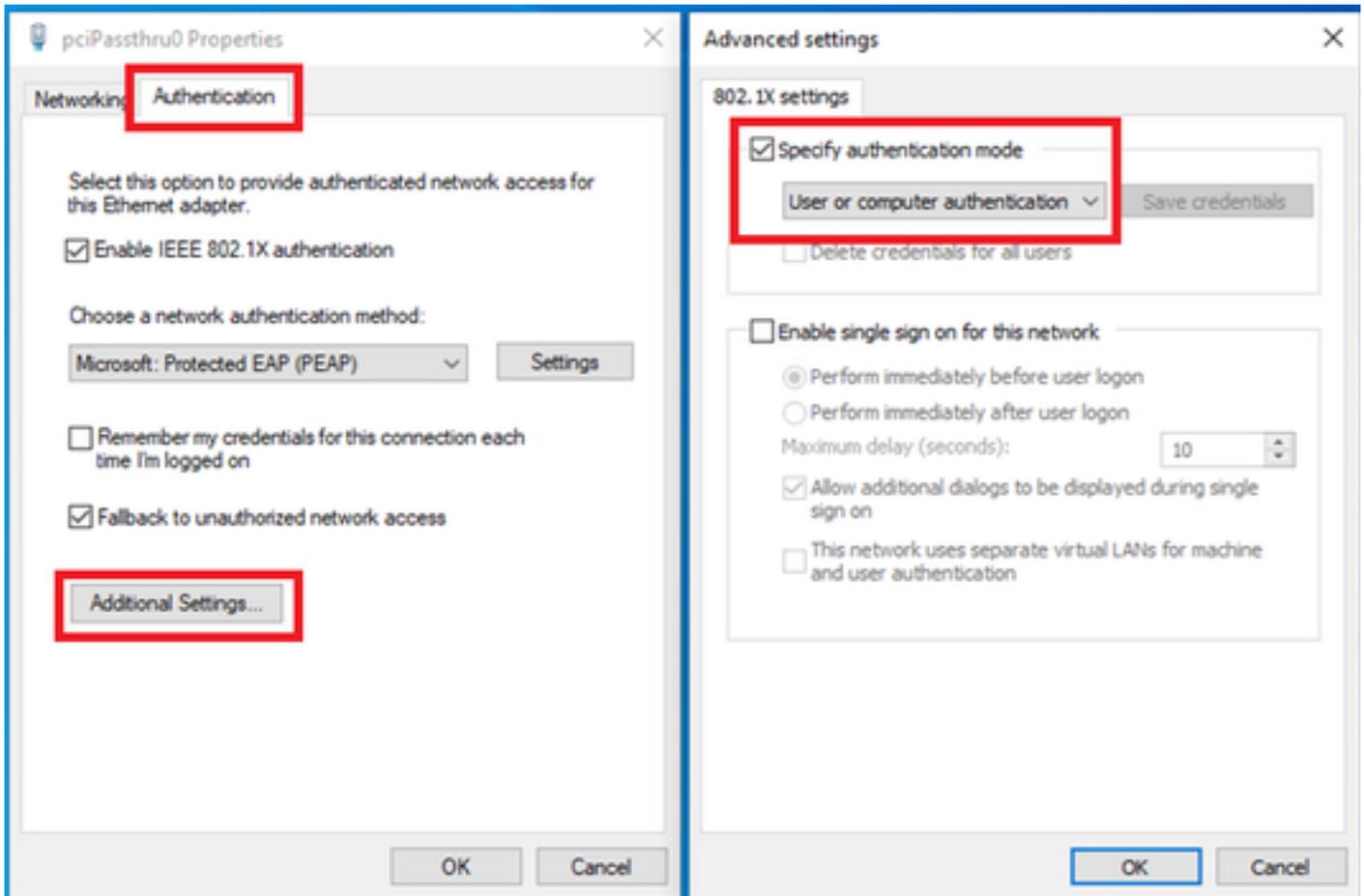
Paso 2. Configurar autenticación de usuario

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.

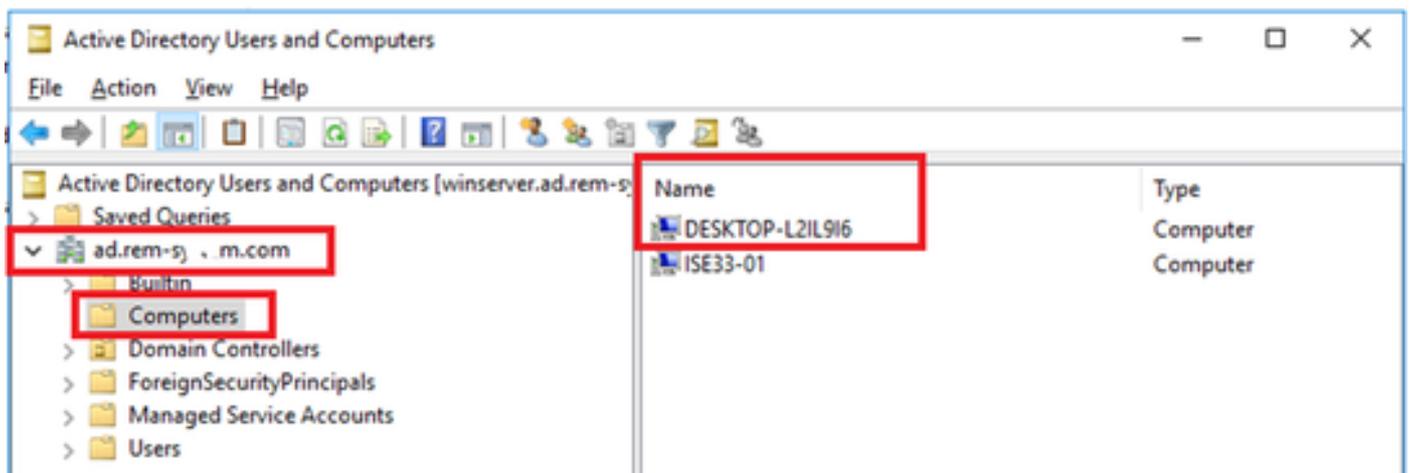


Especificar modo de autenticación

Configuración en Windows Server

Paso 1. Confirmar equipos de dominio

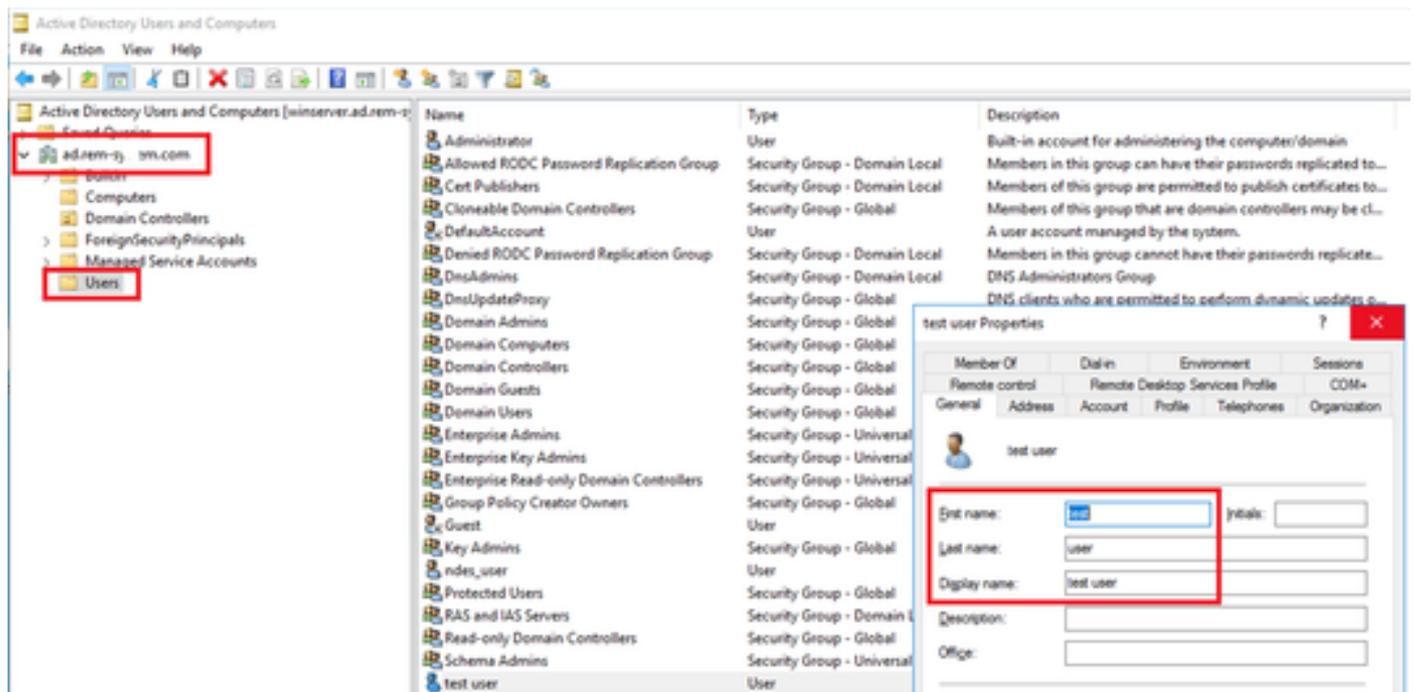
Vaya a Usuarios y equipos de Active Directory, haga clic en Equipos. Confirme que Win10 PC1 aparezca en el dominio.



Confirmar equipo de dominio

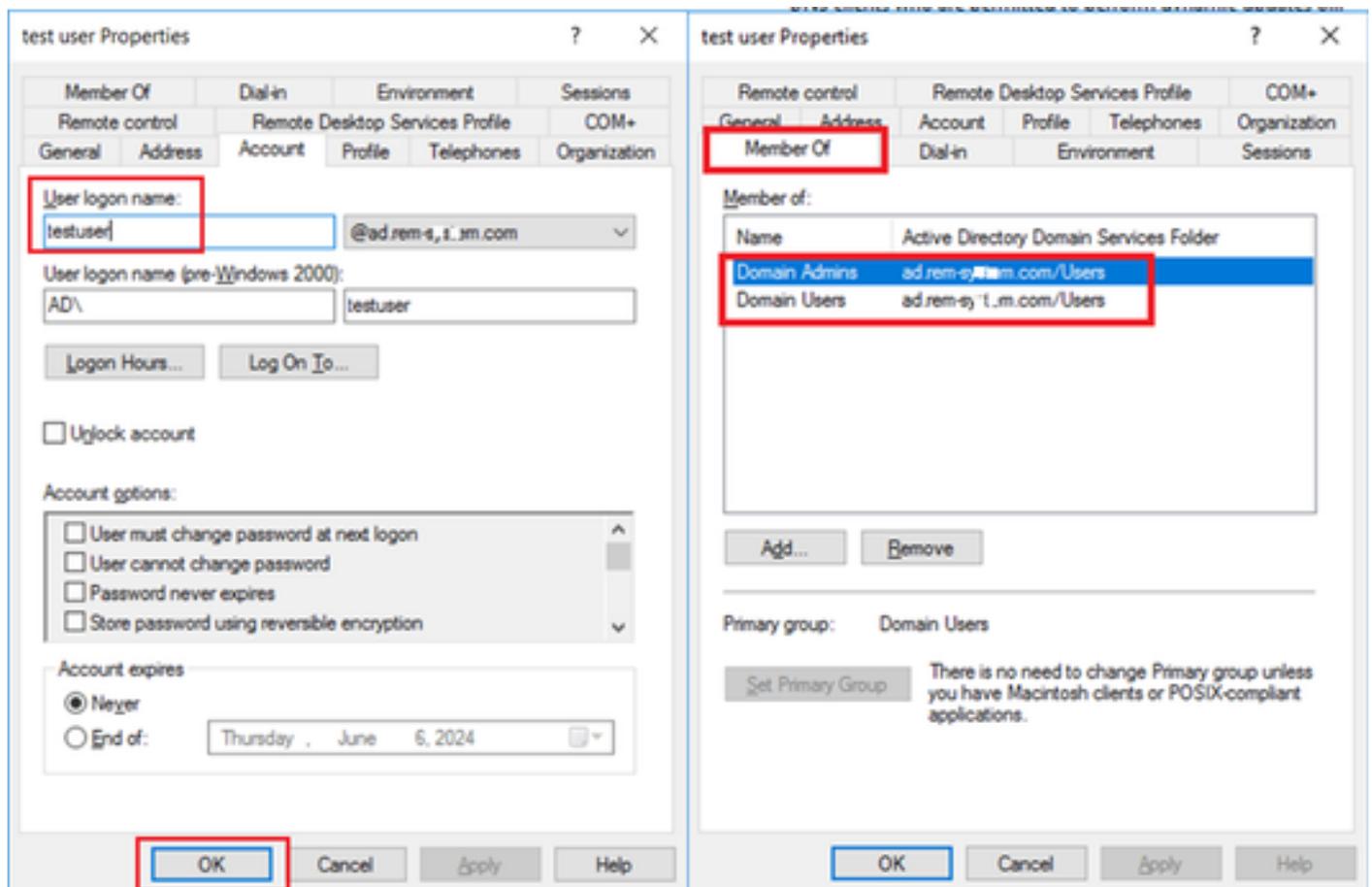
Paso 2. Agregar usuario de dominio

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.

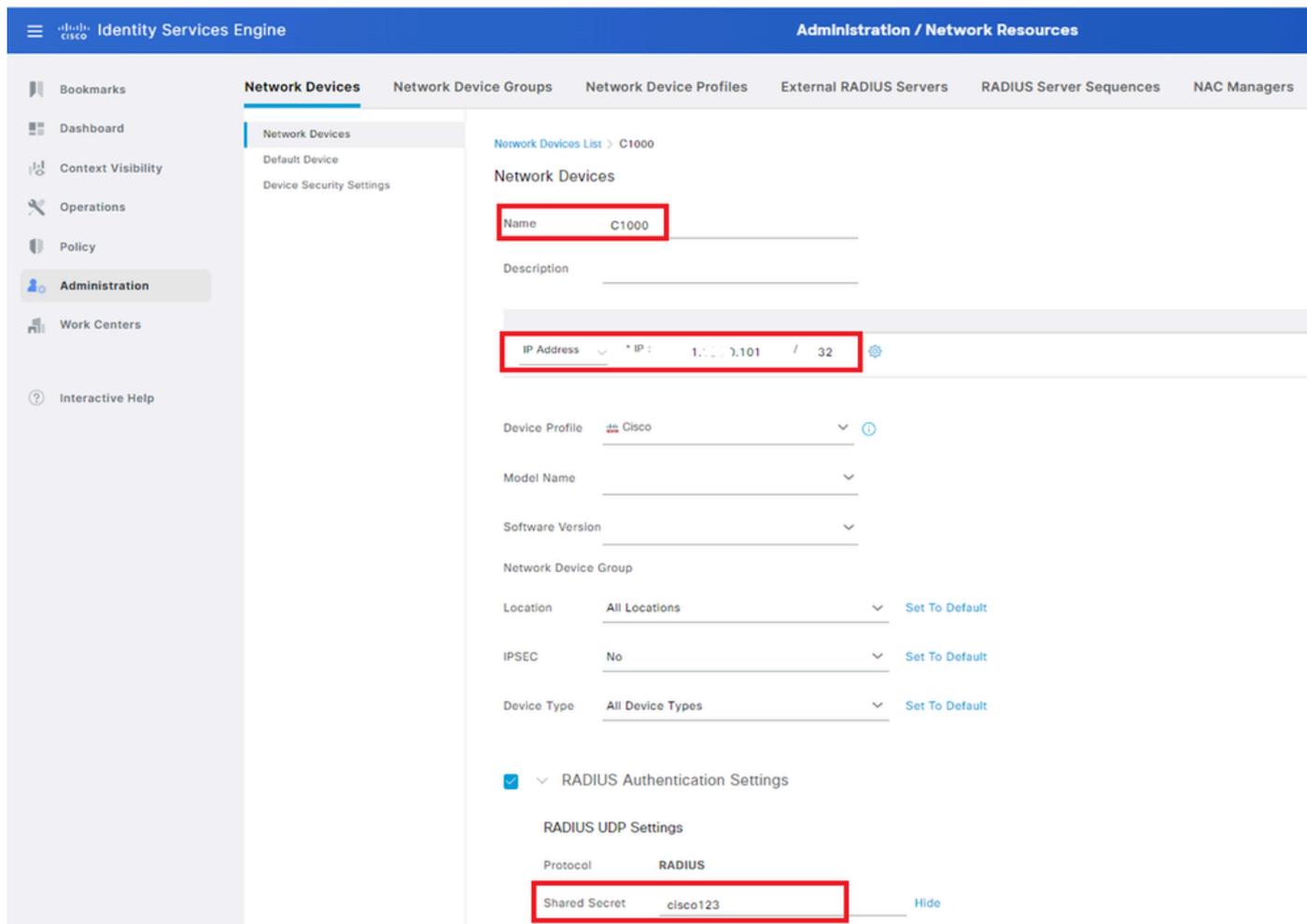


Administradores de dominio y usuarios de dominio

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

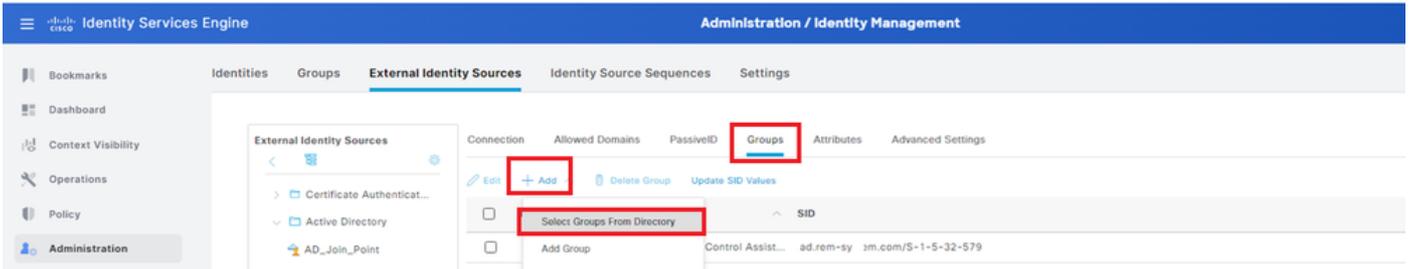
Vaya a Administration > External Identity Sources > Active Directory, haga clic en la pestaña Connection, agregue Active Directory a ISE.

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



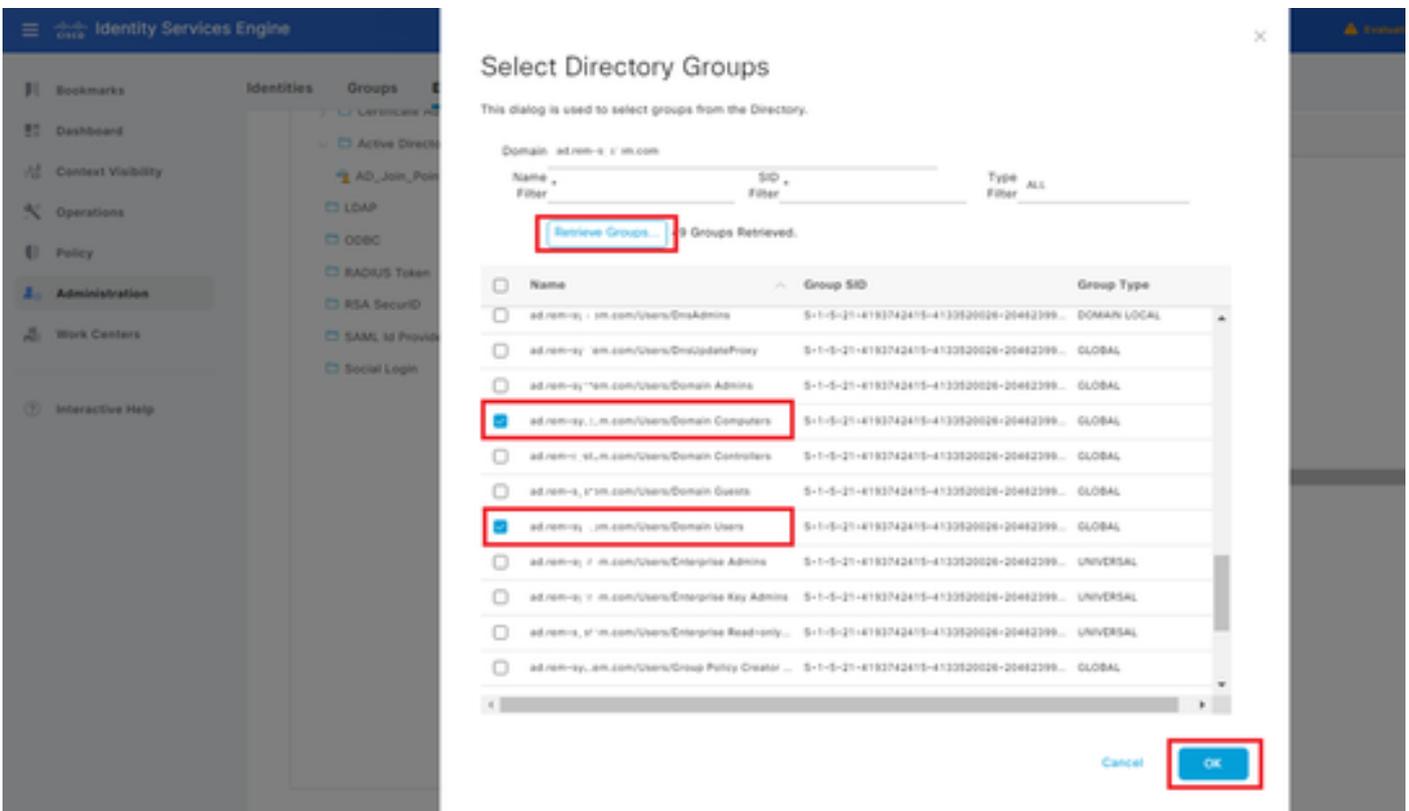
Agregar Active Directory

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.

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 content area is divided into several tabs: 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' tab is active, and the 'Advanced Settings' sub-tab is selected and highlighted with a red box. The 'Advanced Authentication Settings' section is expanded, showing the following options:

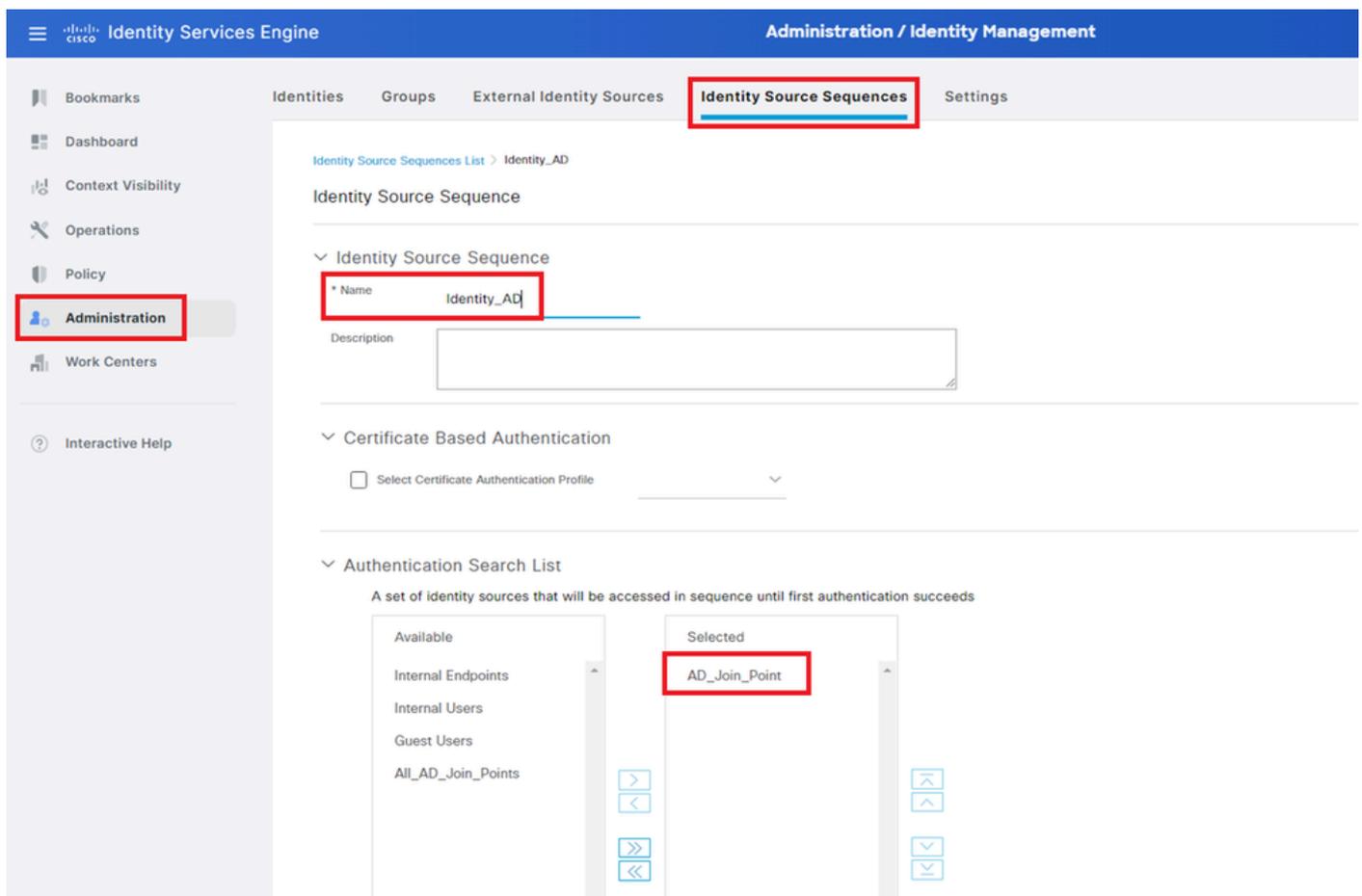
- Enable Password Change
- Enable Machine Authentication
- Enable Machine Access Restrictions
- Aging Time: 5 hours

Below these options, 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](#)'. There are also three unchecked options: 'Enable dial-in check', 'Enable callback check for dial-in clients', and 'Use Kerberos for Plain Text Authentications'.

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.

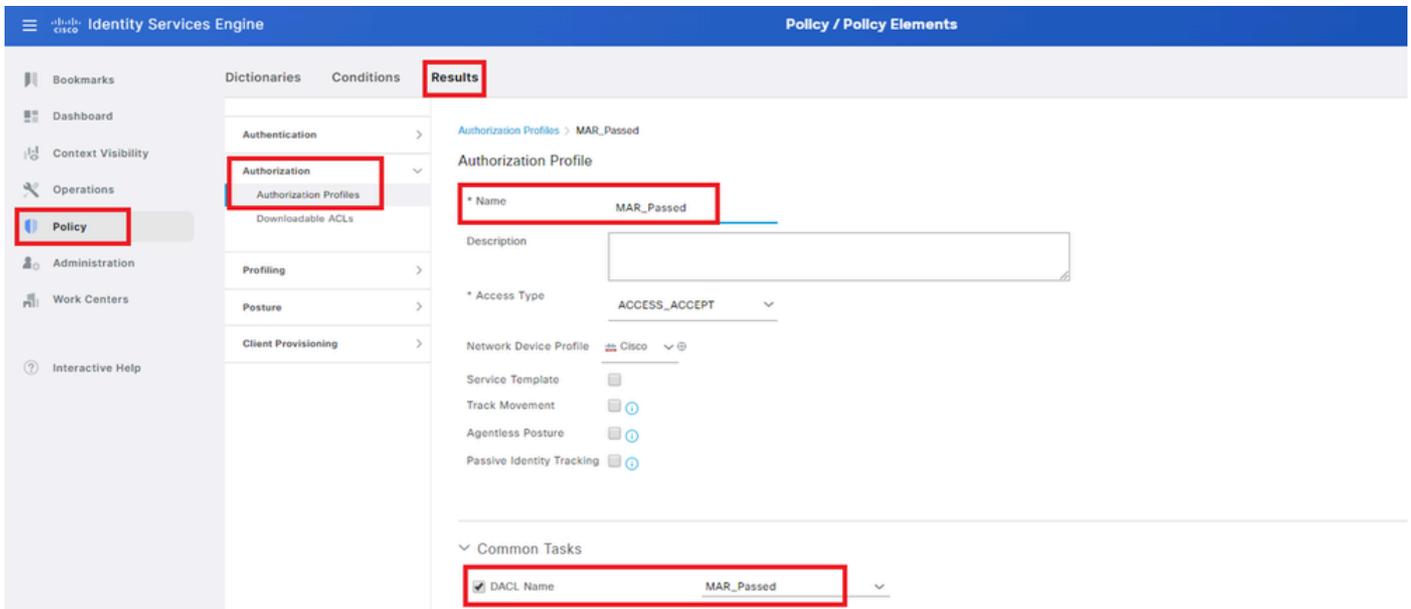
- Nombre: MAR_Passed
- Contenido DACL: permitir ip any host 1.x.x.101 y permitir ip any host 1.x.x.105



Agregar DACL

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

- Nombre: MAR_Passed
- Nombre de DACL: MAR_Passed

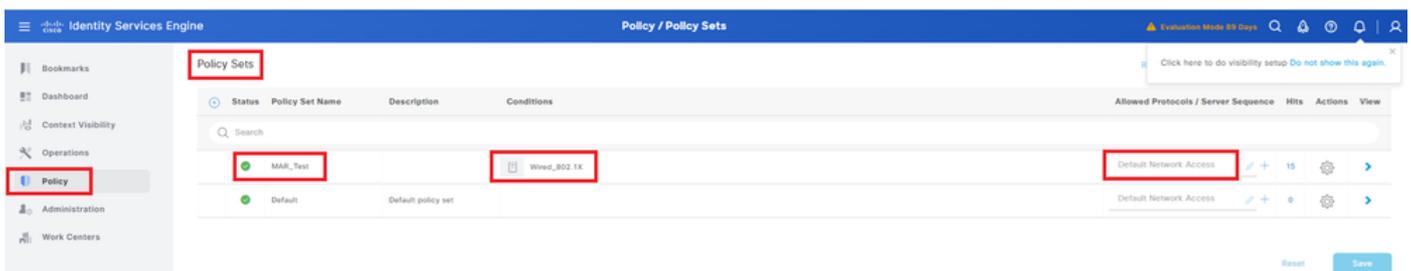


Agregar perfil de autorización

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

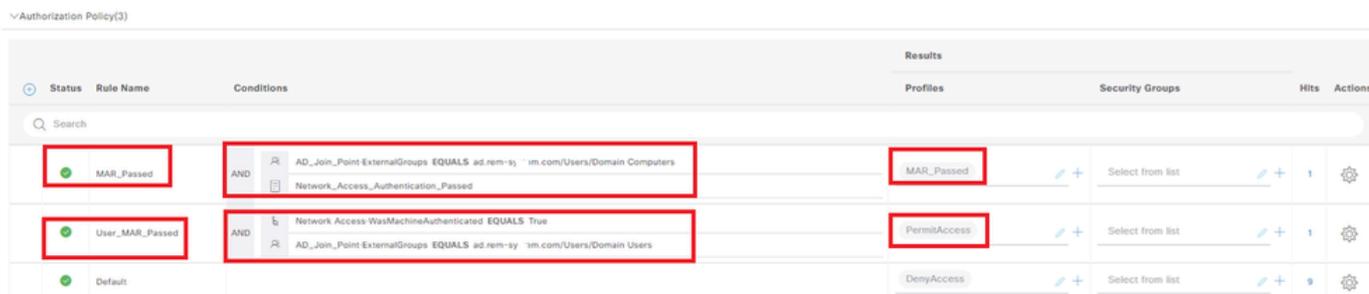


Agregar política de autenticación

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

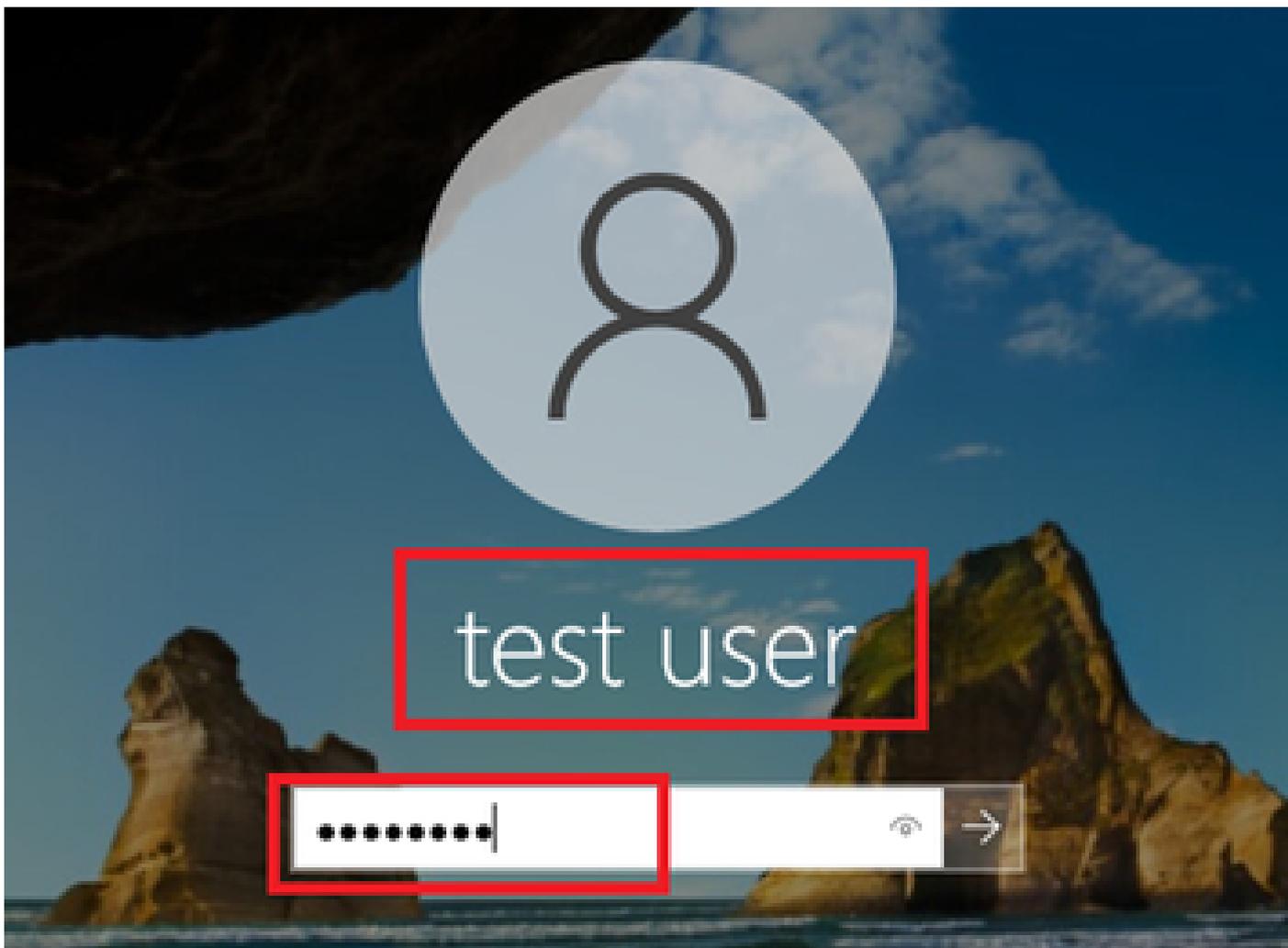
Method status list:

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: 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

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.

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...	Success		0	AD/tesuser	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...	Success		0	AD/tesuser	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...	Success		0	hsoi/DESKTOP-L2696-4d-rem-...	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Registro en directo de Radius

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

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL916.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-L2IL916.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

Detalle de autenticación de máquina

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

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

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.

The screenshot shows the Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / RADIUS'. The left sidebar has 'Operations' selected. The main area shows a 'Live Logs' section with a table of RADIUS events. A red box highlights a log entry for 'AD\testuser' at 'May 07, 2024 04:42:04'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05...	Success		0	AD\testuser	84-96:91:15:84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:42:04...	Success		0	AD\testuser	84-96:91:15:84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:36:13...	Success		0	AD\testuser	84-96:91:15:84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:35:12...	Success		0	WACSACLW-IP-MAR_Passed-6639a20							C1000
May 07, 2024 04:35:12...	Success		0	host/DESKTOP-L2L96.ad.rem-n..._sm...	84-96:91:15:84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == MAR_Passed	MAR_Passed	169.254.90.1...	C1000

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

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

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$@ad.rem-xxx.com,MARCache.cpp:105
// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8
user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com
,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,
Inserting new entry to cache
CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@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=01C2006500000049AA780D8
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=01C2006500000049AA780D8
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=01C2006500000049AA780D8
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).