

Configuración de la autenticación externa en Catalyst Center mediante Windows Server

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Política de roles de administrador](#)

[Política de funciones de observador.](#)

[Habilitar autenticación externa](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar la autenticación externa en Cisco DNA Center mediante el Servidor de directivas de redes (NPS) en Windows Server como RADIUS.

Prerequisites

Requirements

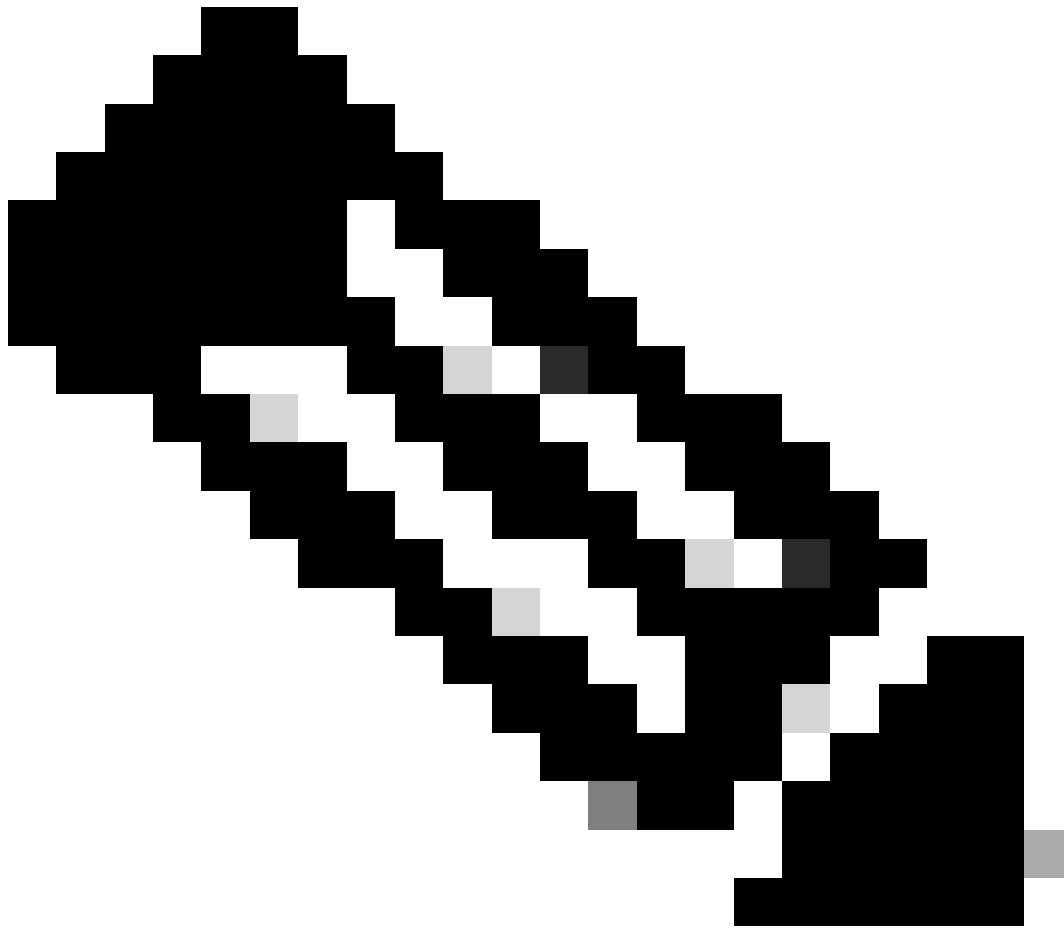
Conocimientos básicos sobre:

- Funciones y usuarios de Cisco DNA Center
- Servidor de directivas de red de Windows Server, RADIUS y Active Directory

Componentes Utilizados

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server versión 2019 que actúa como controlador de dominio, servidor DNS, NPS y Active Directory

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.



Nota: Cisco Technical Assistance Center (TAC) no proporciona asistencia técnica a Microsoft Windows Server. Si experimenta problemas con la configuración de Microsoft Windows Server, póngase en contacto con el soporte técnico de Microsoft para obtener asistencia técnica.

Configurar

Política de roles de administrador

1. Haga clic en el menú Inicio de Windows y busque NPS. A continuación, seleccione Network Policy Server:

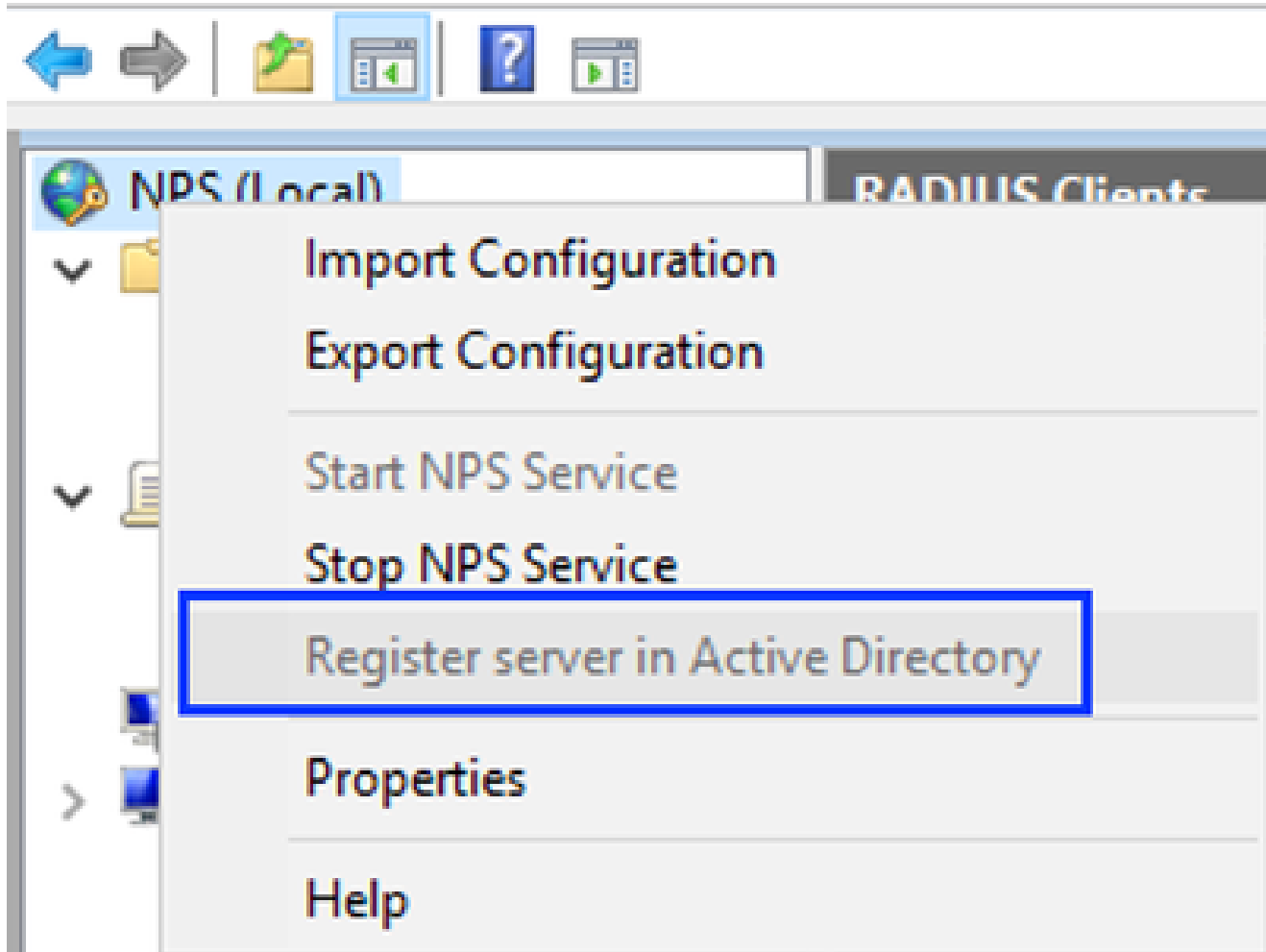


Network Policy Server

Desktop app

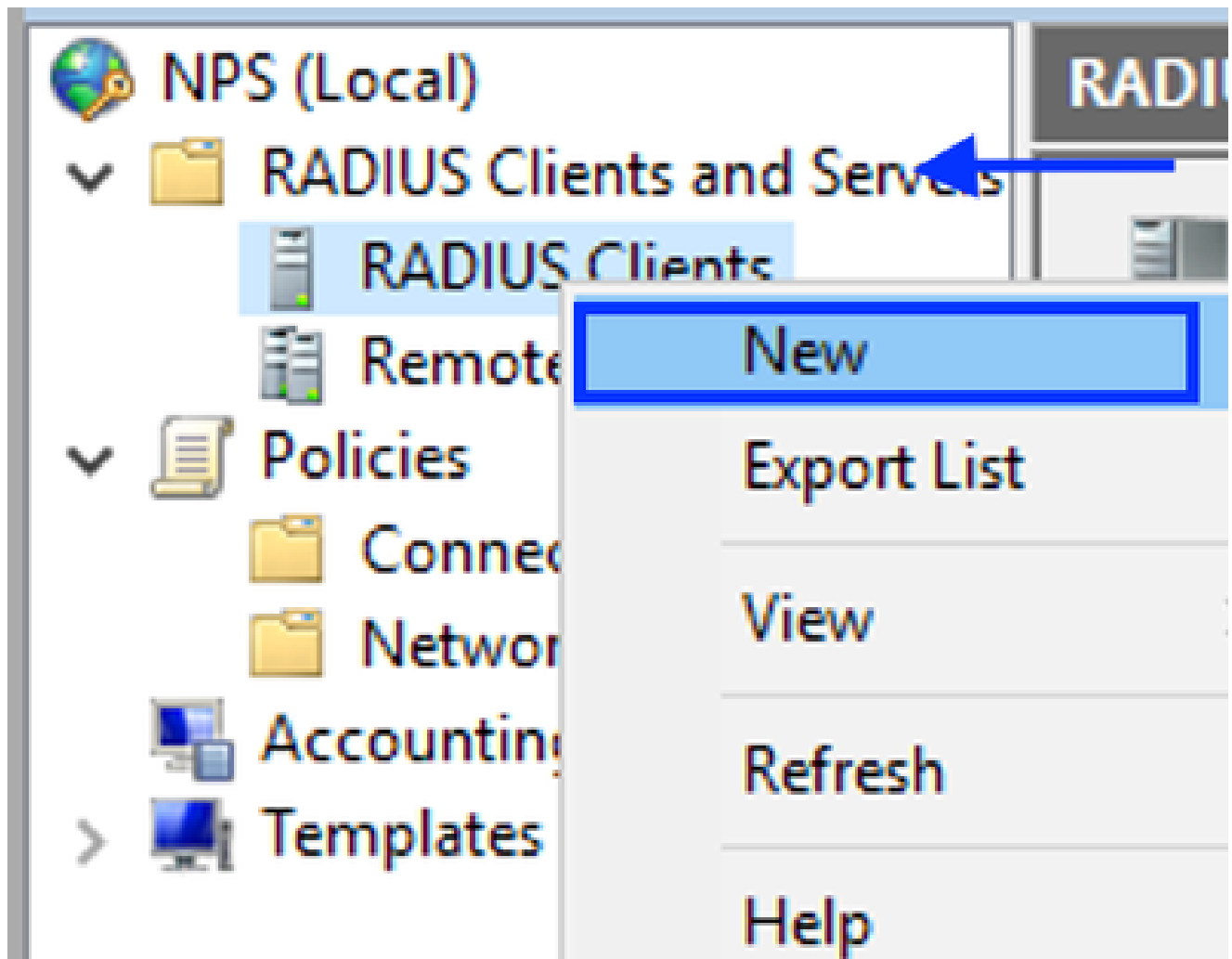
Network Policy Server

File Action View Help



Servicio de directivas de red de Windows

3. Haga clic en Aceptar dos veces.
4. Expanda RADIUS Clients and Servers, haga clic con el botón derecho en RADIUS Clients y seleccione New:



Agregar cliente RADIUS

5. Introduzca el nombre descriptivo, la dirección IP de administración del Cisco DNA Center y un secreto compartido (se puede utilizar más adelante):

DNAC Properties X

Settings **Advanced**

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template:

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

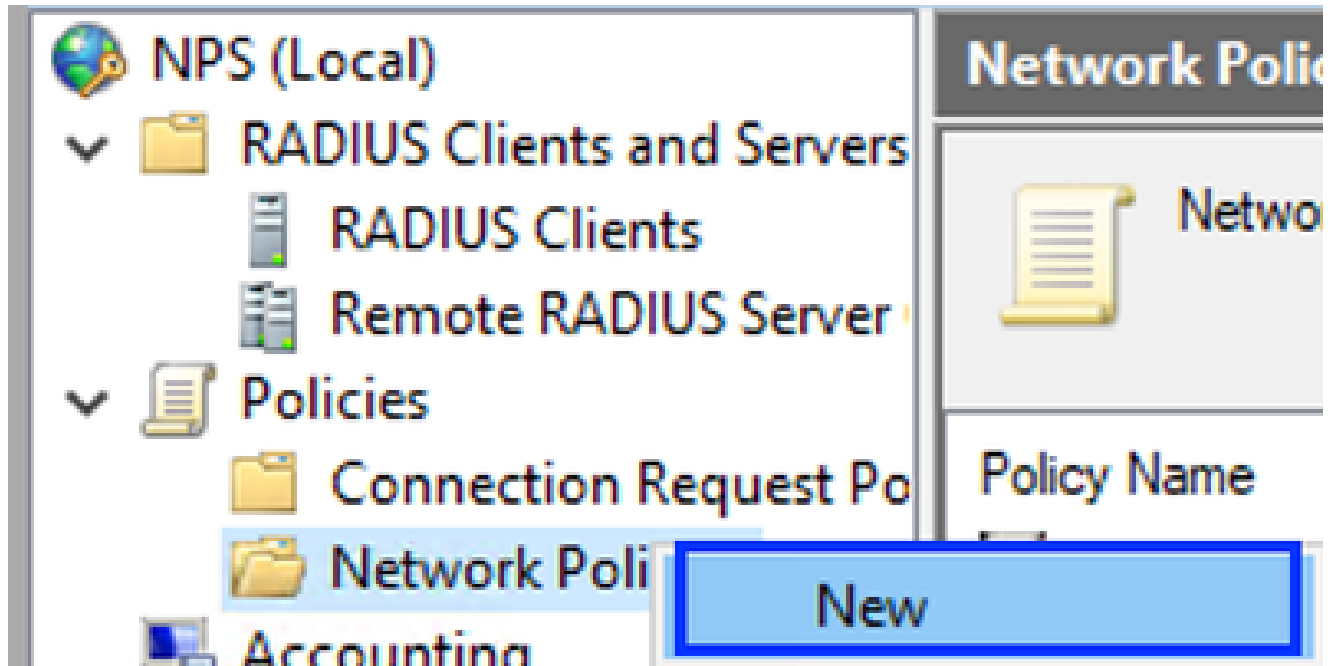
Manual Generate

Shared secret:

Confirm shared secret:

Configuración del cliente Radius

- Haga clic en Aceptar para guardarlo.
- Expanda Directivas, haga clic con el botón derecho en Directivas de red y seleccione Nuevo:



Agregar nueva política de red

8. Introduzca un nombre de directiva para la regla y haga clic en Next:



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

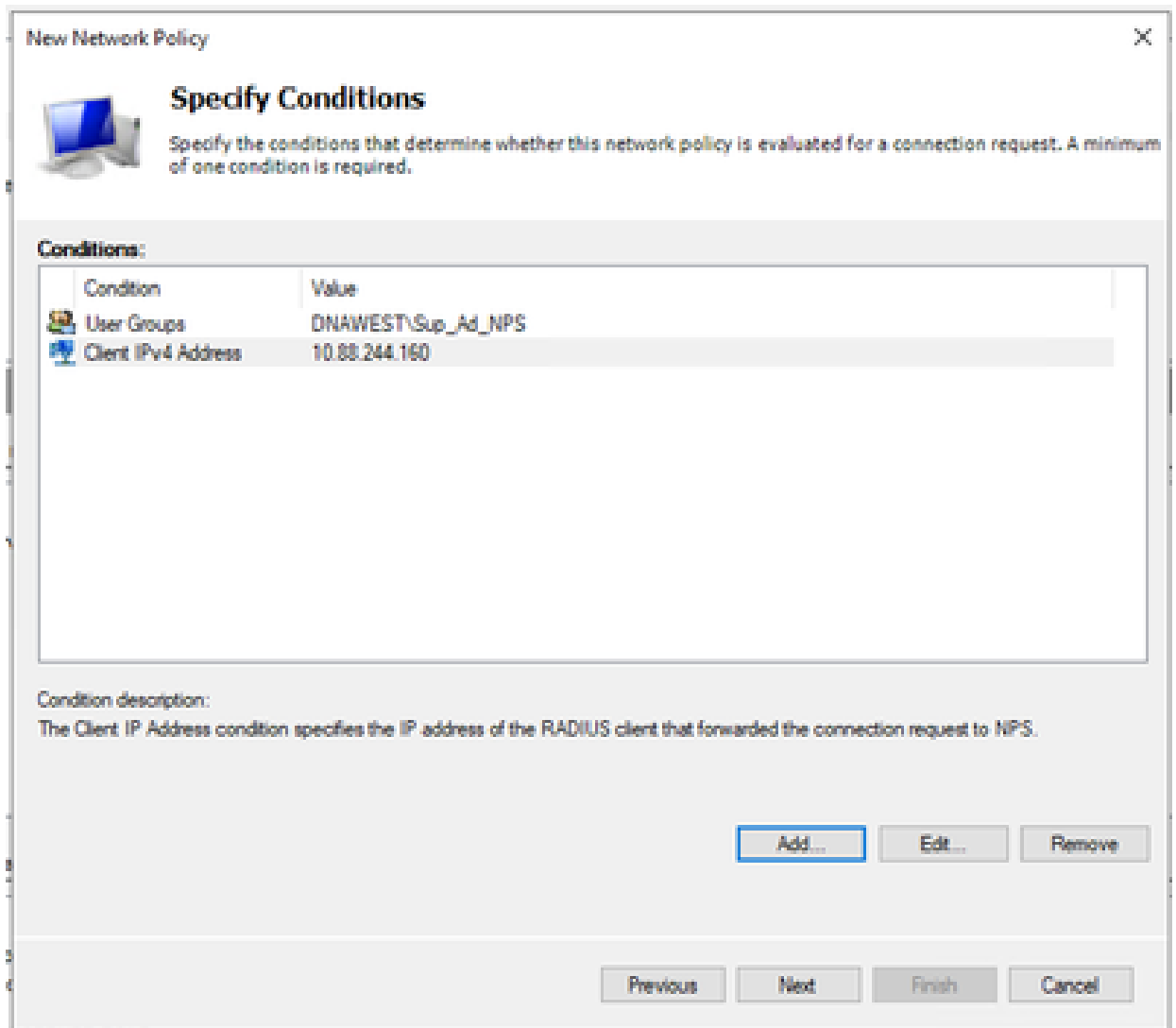
Type of network access server:

Vendor specific:

Nombre de política

9. Para permitir un grupo de dominio específico, agregue estas dos condiciones y haga clic en Next:


- Grupo de usuarios: agregue el grupo de dominio que puede tener un rol de administrador en el centro de DNA de Cisco (en este ejemplo, se utiliza el grupo Sup_Ad_NPS).
- ClientIPv4Address - Agregue su dirección IP de administración de Cisco DNA Center.



Condiciones de política

10. Seleccione Access Grant y haga clic en Next:

New Network Policy ✕



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

Acceso de uso concedido

11. Seleccione únicamente Autenticación sin cifrar (PAP, SPAP):



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Previous

Next

Finish

Cancel

Seleccionar autenticación no cifrada

12. Seleccione Next, ya que se utilizan los valores predeterminados:



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.

If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

Disconnect after the maximum idle time

Previous

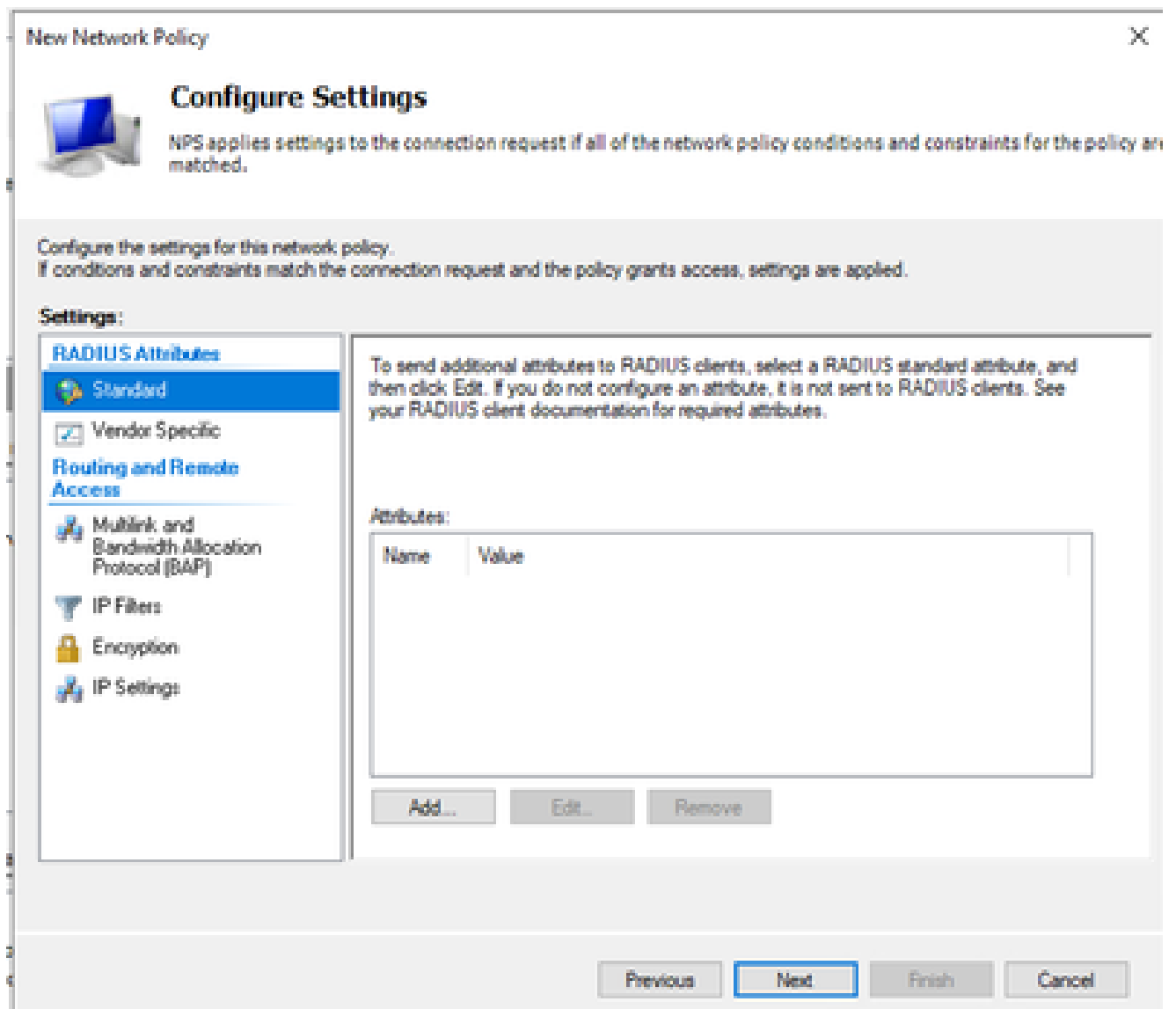
Next

Finish

Cancel

Ventana Configurar Restricción

13. Eliminar atributos estándar:



Definir atributos para utilizar

14. En RADIUS Attributes (Atributos RADIUS), seleccione Vendor Specific (Específicos del proveedor), luego haga clic en Add, seleccione Cisco como proveedor y haga clic en Add:

Add Vendor Specific Attribute



To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add...

Close

Agregar par AV de Cisco

15. Haga clic en Agregar, escriba Role=SUPER-ADMIN-ROLE y haga clic en Aceptar dos veces:



Configure Settings

NPS applies settings to the connection request if **all** of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	Role=SUPER-ADMIN-ROLE

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

Atributo de par AV de Cisco agregado

16. Seleccione Cerrar y, a continuación, Siguiente.

17. Revise la configuración de directiva y seleccione Finalizar para guardarla.



Completing New Network Policy

You have successfully created the following network policy:

DNAC-Admin-Policy

Policy conditions:

Condition	Value
User Groups	DNAWEST\Sup_Ad_NPS
Client IPv4 Address	10.88.244.160

Policy settings:

Condition	Value
Authentication Method	Encryption authentication (CHAP)
Access Permission	Grant Access
Ignore User Dial-In Properties	False
Cisco-AV-Pair	Role=SUPER-ADMIN-ROLE

To close this wizard, click Finish.

Previous

Next

Finish

Cancel

Resumen de políticas

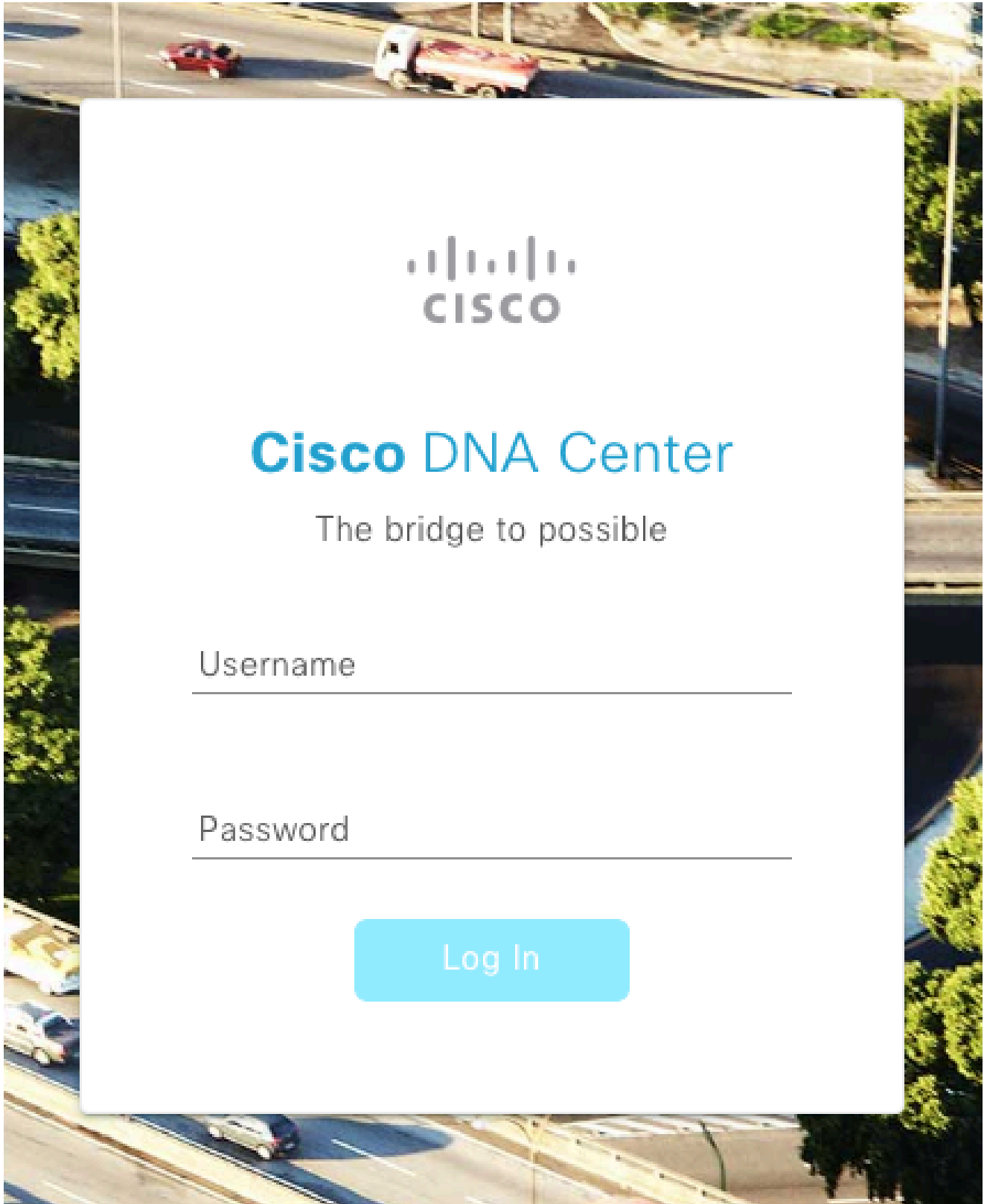
Política de funciones de observador.

1. Haga clic en el menú Inicio de Windows y busque NPS. A continuación, seleccione Servidor de directivas de red.
2. En el panel de navegación del lado izquierdo, haga clic con el botón derecho en la opción NPS (Local) y seleccione Registrar servidor en Active Directory.
3. Haga clic en Aceptar dos veces.
4. Expanda RADIUS Clients and Servers, haga clic con el botón derecho en RADIUS Clients y seleccione New.
5. Introduzca un nombre descriptivo, la dirección IP de administración del Cisco DNA Center y un secreto compartido (se puede utilizar más adelante).
6. Haga clic en Aceptar para guardarlo.

7. Expanda Directivas, haga clic con el botón derecho en Directivas de red y seleccione Nuevo.
8. Introduzca un nombre de directiva para la regla y haga clic en Siguiente.
9. Para permitir un grupo de dominio específico, debe agregar estas dos condiciones y seleccionar Next.
 - Grupo de usuarios: agregue su grupo de dominio para asignar un rol de observador en el centro de DNA de Cisco (en este ejemplo, se utiliza el grupo Observer_NPS).
 - ClientIPv4Address - Agregue su dirección IP de administración de Cisco DNA Center.
10. Seleccione Acceso concedido y, a continuación, Siguiente.
11. Seleccione únicamente Autenticación sin cifrar (PAP, SPAP).
12. Seleccione Next, ya que se utilizan los valores predeterminados.
13. Elimine los atributos estándar.
14. En RADIUS Attributes (Atributos RADIUS), seleccione Vendor Specific, luego haga clic en Add (Agregar), seleccione Cisco como proveedor y haga clic en Add.
15. Seleccione Add, write ROLE=OBSERVER-ROLE y OK dos veces.
16. Seleccione Cerrar y, a continuación, Siguiente.
17. Revise la configuración de directiva y seleccione Finalizar para guardarla.

Habilitar autenticación externa

1. Abra la interfaz gráfica de usuario (GUI) de Cisco DNA Center en un navegador web e inicie sesión con una cuenta con privilegios de administrador:



Página de inicio de sesión de Cisco DNA Center

2. Navegue hasta Menú > Sistema > Configuración > Servidores de autenticación y políticas y seleccione Agregar > AAA:

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[+ Add ^](#) [↑ Export](#)

AAA	Protocol
ISE 4.189	RADIUS_TACACS

Agregar Windows Server

3. Escriba la dirección IP de Windows Server y la clave secreta compartida utilizada en los pasos anteriores y haga clic en Guardar:

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Valide que su estado de Windows Server es Activo:

10.88.244.148

RADIUS

AAA

ACTIVE



Resumen de Windows Server

5. Navegue hasta Menú > Sistema > Usuarios y roles > Autenticación externa y seleccione su servidor AAA:

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

Update

Windows Server como servidor AAA

6. Escriba Cisco-AVPair como el atributo AAA y haga clic en Update:

✓ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

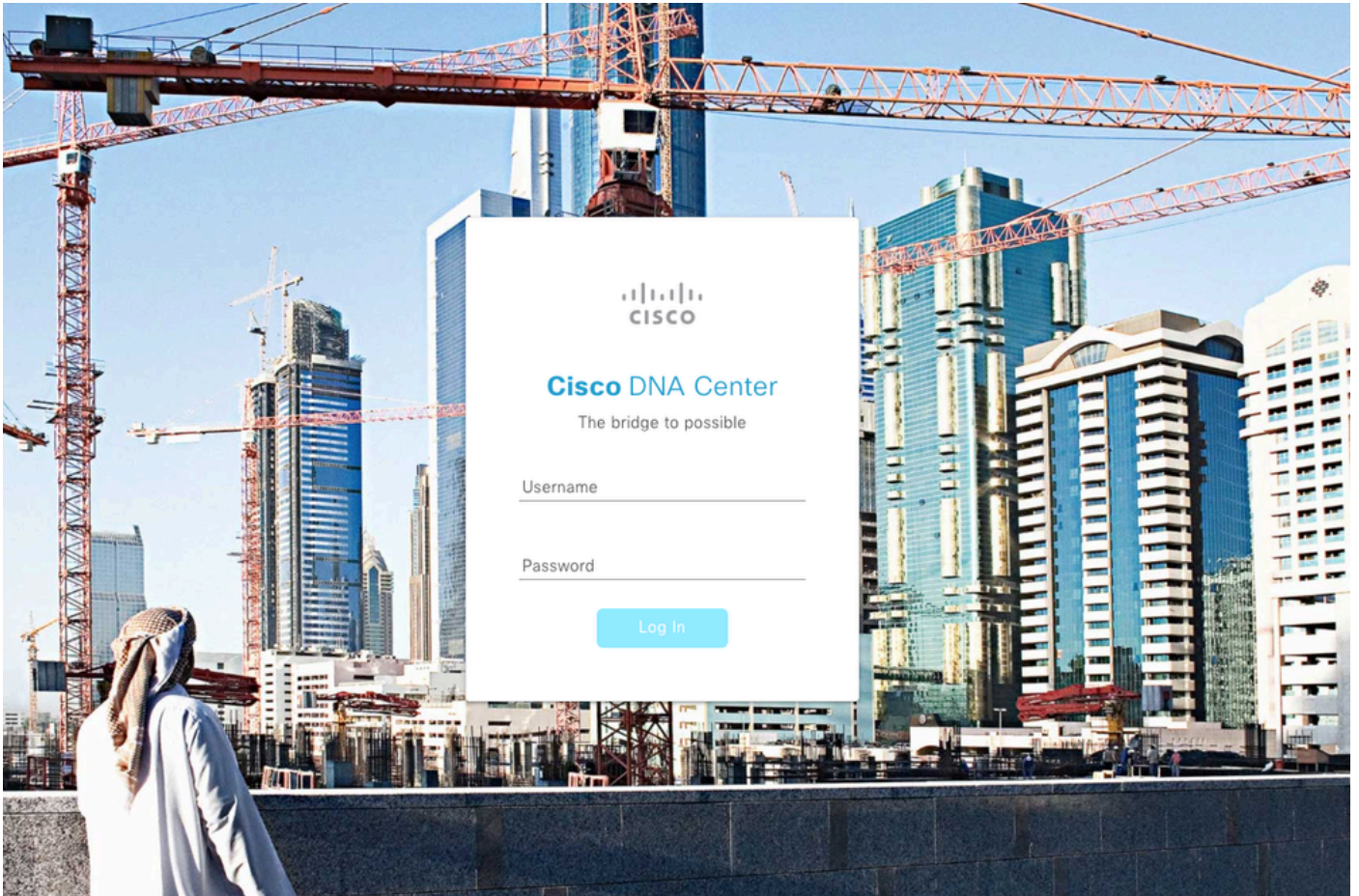
Par AV en usuario externo

7. Haga clic en la casilla de verificación Enable External User para habilitar la autenticación externa:

Enable External User 

Verificación

Puede abrir la interfaz gráfica de usuario (GUI) de Cisco DNA Center en un navegador web e iniciar sesión con un usuario externo configurado en Windows Server para validar que puede iniciar sesión correctamente mediante la autenticación externa.



Página de inicio de sesión de Cisco DNA Center

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).