

Externe verificatie op Catalyst Center configureren met Windows-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Rol van beheerder](#)

[Beleid inzake de rol van waarnemers.](#)

[Externe verificatie inschakelen](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u externe verificatie in Cisco DNA Center kunt configureren met behulp van Network Policy Server (NPS) in Windows Server als RADIUS.

Voorwaarden

Vereisten

Basiskennis over:

- Gebruikers en rollen van Cisco DNA Center
- Windows Server-netwerkbeleidsserver, RADIUS en actieve map

Gebruikte componenten

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server versie 2019 fungeert als domeincontroller, DNS-server, NPS en Active Directory

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.



Opmerking: het Cisco Technical Assistance Center (TAC) biedt geen technische ondersteuning voor de Microsoft Windows-server. Als u problemen ondervindt met de Microsoft Windows Server-configuratie, neemt u contact op met Microsoft Support voor technische assistentie.

Configureren

Rol van beheerder

1. Klik in het Windows Start menu en zoek naar NPS. Selecteer vervolgens Network Policy Server:

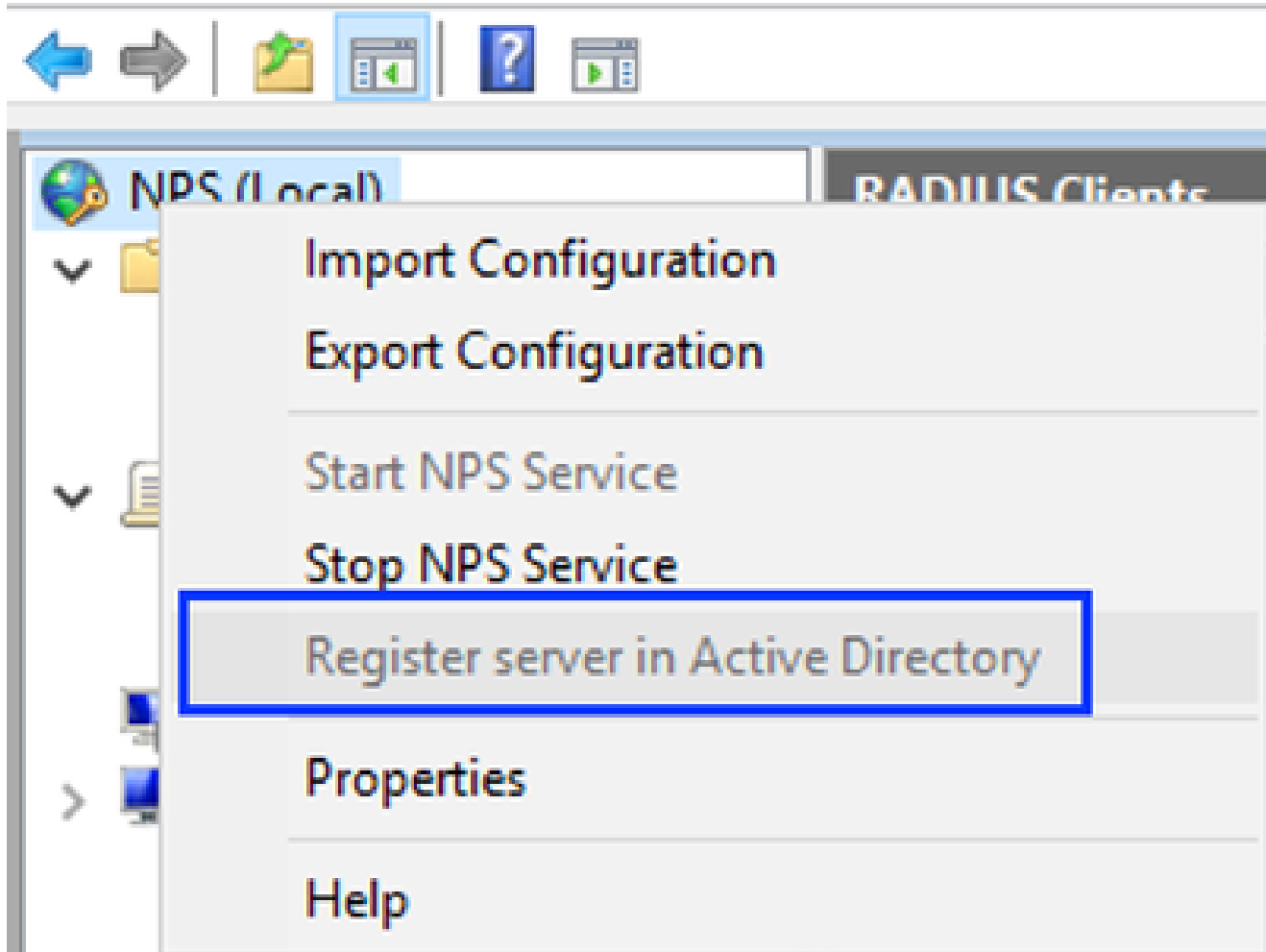


Network Policy Server

Desktop app

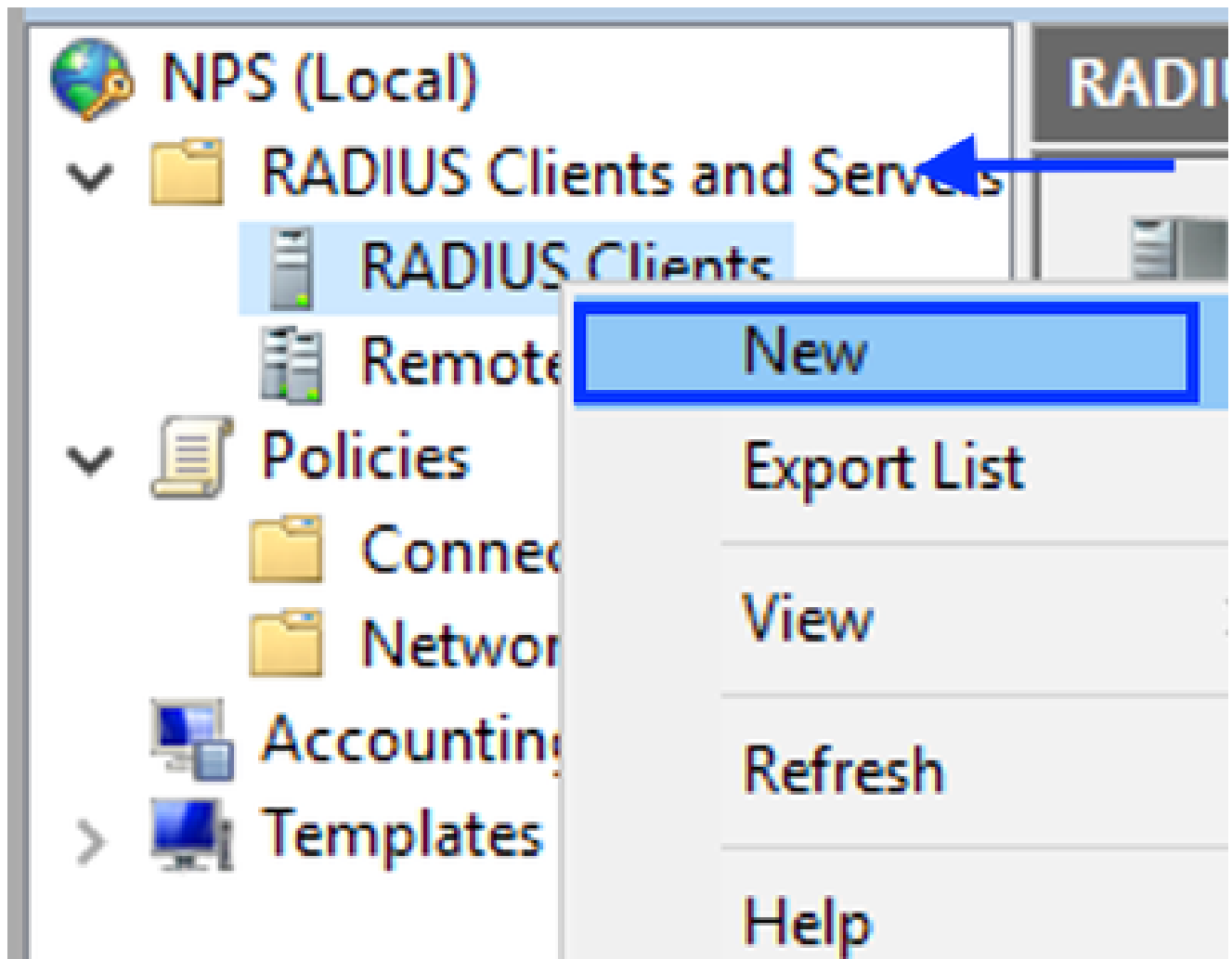
Network Policy Server

File Action View Help



Windows-netwerkbeleidsservice

3. Klik tweemaal op OK.
4. Breid RADIUS-clients en -servers uit, klik met de rechtermuisknop op RADIUS-clients en selecteer Nieuw:



RADIUS-client toevoegen

5. Voer de Vriendelijke naam, het IP-adres van het Cisco DNA Center-beheer en een gedeeld geheim in (dit kan later worden gebruikt):

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.

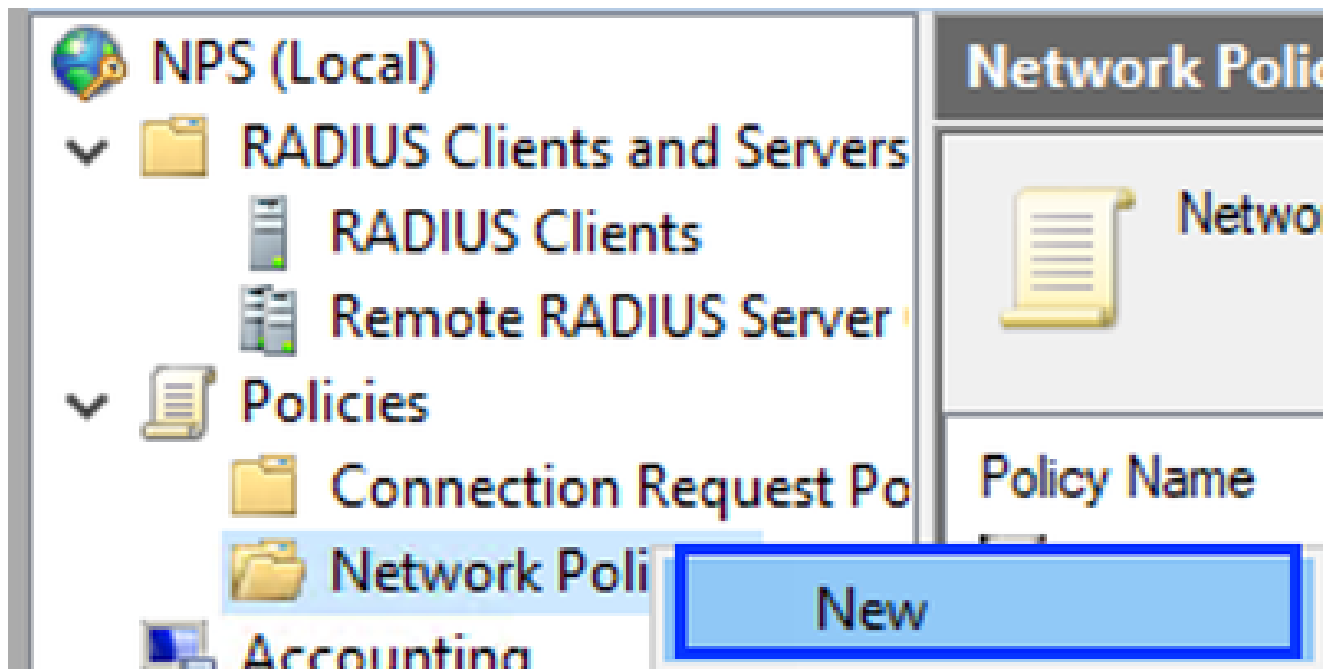
Manual Generate

Shared secret:

Confirm shared secret:

Configuratie van RADIUS-clients

- Klik op OK om het op te slaan.
- Breid Beleid uit, klik met de rechtermuisknop op Netwerkbeleid en selecteer Nieuw:



Nieuw netwerkbeleid toevoegen

8. Voer een beleidsnaam in voor de regel en klik op Volgende:



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:
DNAC-Admin-Policy

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.

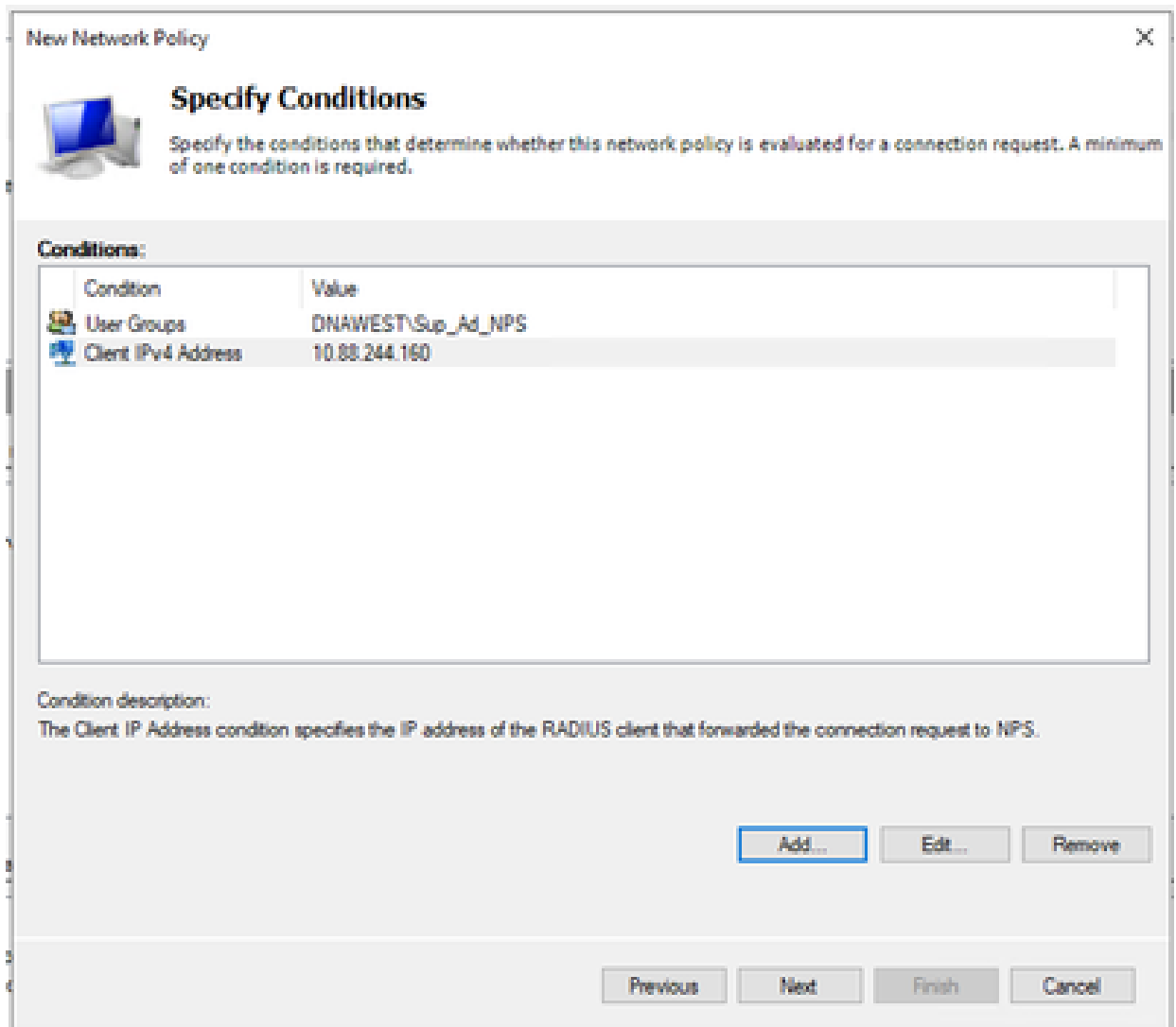
Type of network access server:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

Beleidsnaam


9. Als u een specifieke domeingroep wilt toestaan, voegt u deze twee voorwaarden toe en klikt u op Volgende:
- Gebruikersgroep - Voeg uw domeingroep toe die een Admin Rol kan hebben op Cisco DNA Center (voor dit voorbeeld wordt Sup_Ad_NPS-groep gebruikt).
 - ClientIPv4Address - Voeg uw IP-adres voor Cisco DNA Center-beheer toe.



Beleidsvoorwaarden

10. Selecteer Toegang verleend en klik op Volgende:

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

Toegang verleend gebruik

11. Alleen verificatie versleutelen selecteren (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

Selecteer verificatie versleutelen

12. Selecteer Volgende omdat er standaardwaarden worden gebruikt:



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

1

Previous

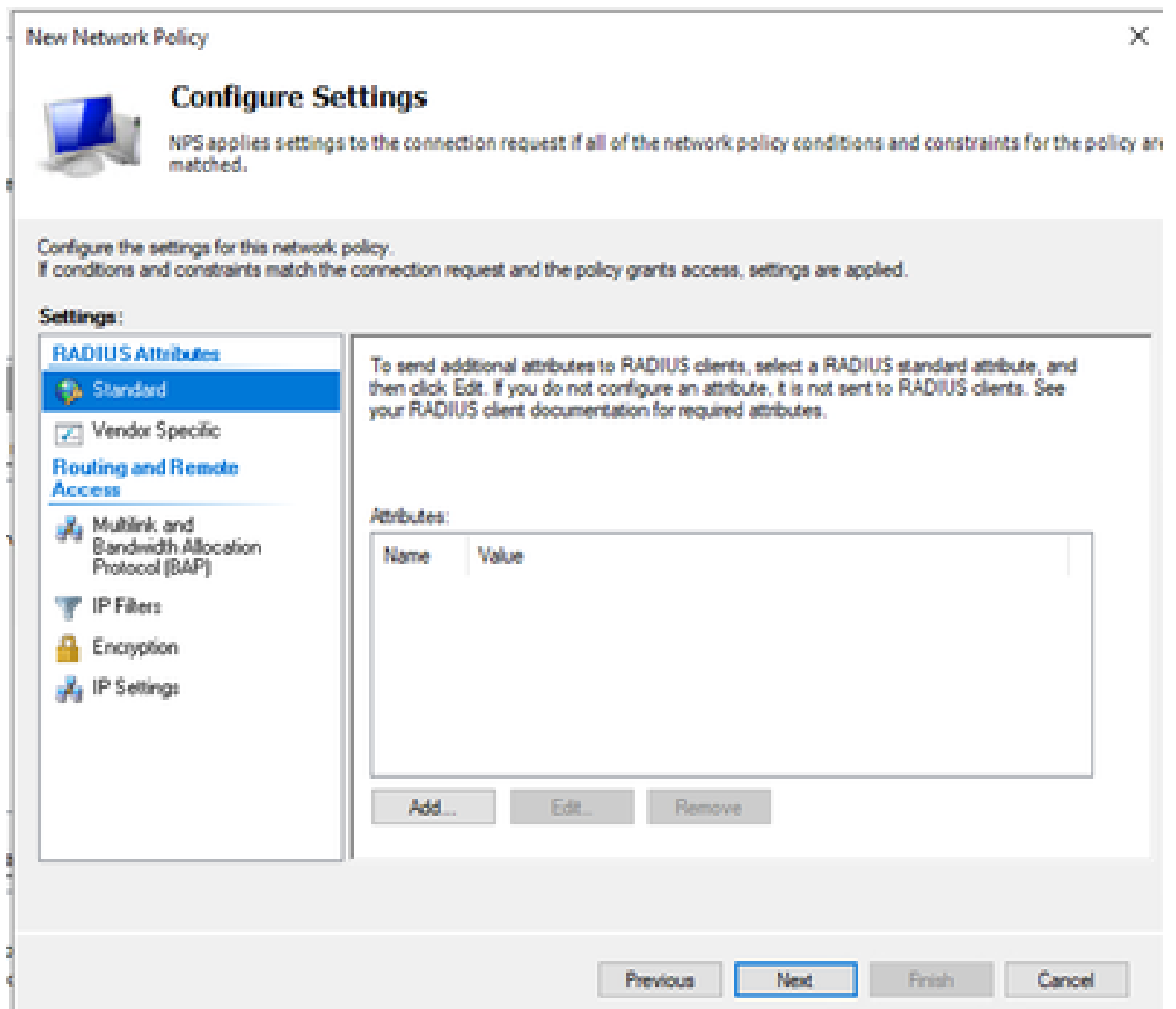
Next

Finish

Cancel

Constraint-venster configureren

13. Standaardkenmerken verwijderen:



Kenmerken definiëren voor gebruik

14. Selecteer in het gedeelte RADIUS-kenmerken de optie Leverancier specifiek, klik vervolgens op Add, selecteer Cisco als leverancier en klik op 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

Cisco AV-paar toevoegen

15. Klik op Add, schrijf Role=SUPER-ADMIN-ROLE en klik tweemaal op OK:



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

Toegevoegd Cisco AV-paar attribuut

16. Selecteer Sluiten en selecteer vervolgens Volgende.

17. Bekijk uw beleidsinstellingen en selecteer Voltoeien om deze op te slaan.



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

Beleidsoverzicht

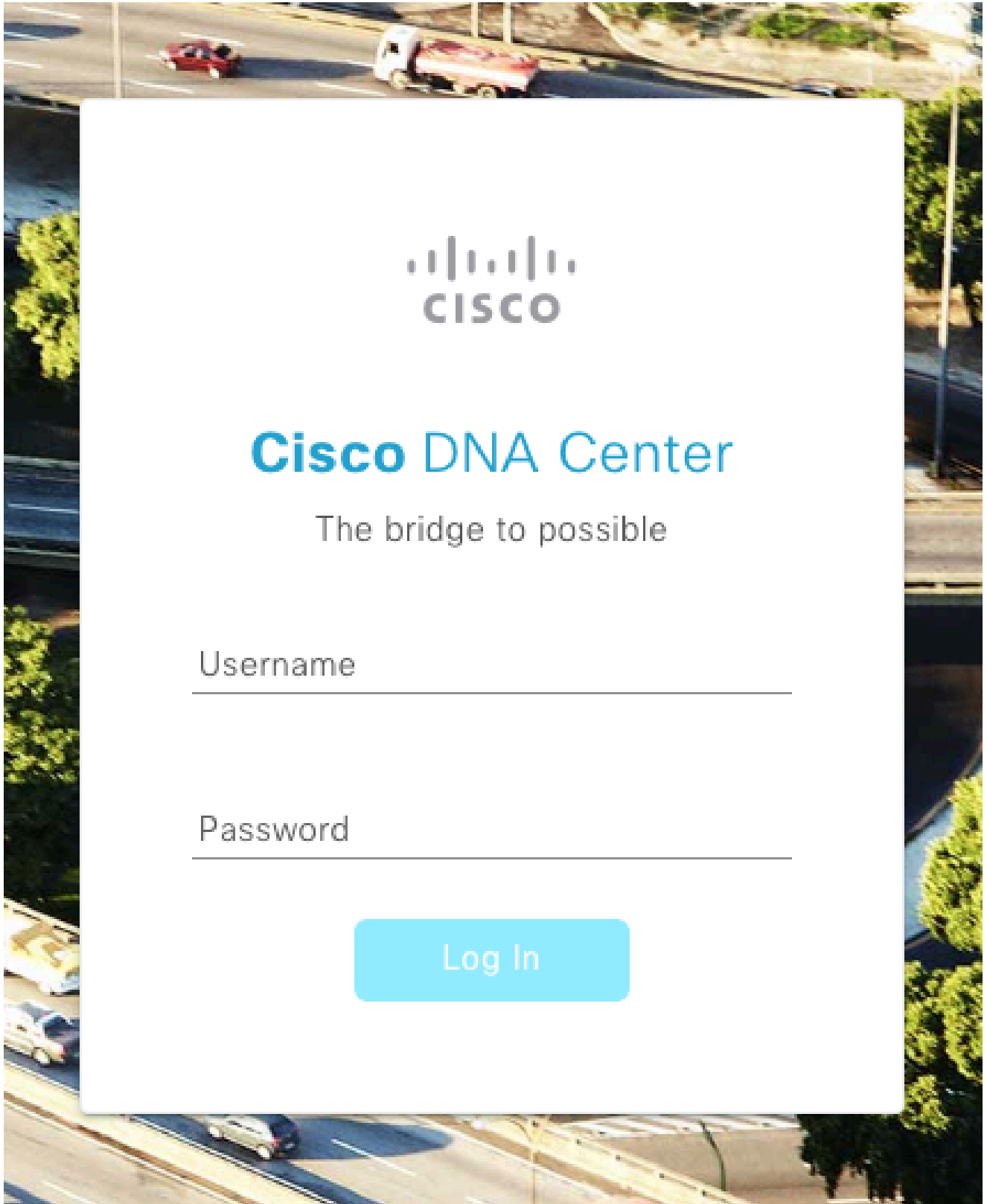
Beleid inzake de rol van waarnemers.

1. Klik in het Windows Start menu en zoek naar NPS. Selecteer vervolgens Network Policy Server.
2. Voer vanuit het navigatiedeelvenster aan de linkerkant een rechtsklik uit in de optie NPS (lokaal) en selecteer Server registreren in Active Directory.
3. Klik tweemaal op OK.
4. Breid RADIUS-clients en -servers uit, klik met de rechtermuisknop op RADIUS-clients en selecteer Nieuw.
5. Voer een Vriendelijke naam, het IP-adres van het Cisco DNA Center-beheer en een gedeeld geheim in (dit kan later worden gebruikt).
6. Klik op OK om het op te slaan.

7. Breid Beleid uit, klik met de rechtermuisknop op Netwerkbeleid en selecteer Nieuw.
8. Voer een beleidsnaam in voor de regel en klik op Volgende.
9. Om een specifieke domeingroep toe te staan, moet u deze twee voorwaarden toevoegen en Volgende selecteren.
 - Gebruikersgroep - Voeg uw domeingroep toe om een Observer Role toe te wijzen aan Cisco DNA Center (in dit voorbeeld wordt de Observer_NPS-groep gebruikt).
 - ClientIPv4Address - Voeg uw Cisco DNA Center management IP toe.
10. Selecteer Toegang verleend en selecteer vervolgens Volgende.
11. Alleen verificatie versleutelen selecteren (PAP, SPAP).
12. Selecteer Volgende omdat er standaardwaarden worden gebruikt.
13. Standaardkenmerken verwijderen.
14. Selecteer in RADIUS-kenmerken de optie Leverancier Specific, klik vervolgens op Add, selecteer Cisco als leverancier en klik op Add.
15. Selecteer Add, schrijf ROLE=OBSERVER-ROLE, en OK tweemaal.
16. Selecteer Sluiten en vervolgens Volgende.
17. Controleer uw beleidsinstellingen en selecteer Voltooien om deze op te slaan.

Externe verificatie inschakelen

1. Open de Cisco DNA Center Graphical User Interface (GUI) in een webbrowser en log in met een geprivilegieerde beheerdersaccount:



Aanmeldpagina voor Cisco DNA Center

2. Navigeer naar Menu > Systeem > Instelling > Verificatie- en beleidsservers en selecteer Toevoegen > 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

Windows-server toevoegen

3. Typ uw IP-adres van Windows Server en het gedeelde geheim dat in de vorige stappen is gebruikt en klik op Opslaan:

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Controleer of uw Windows Server-status actief is:

10.88.244.148

RADIUS

AAA

ACTIVE



Samenvatting van Windows-server

5. Ga naar Menu > Systeem > Gebruikers & Rollen > Externe Verificatie en selecteer uw AAA-server:

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

[Update](#)

Windows-server als AAA-server

6. Typ Cisco-AVPair als AAA-kenmerk en klik op Bijwerken:

✓ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

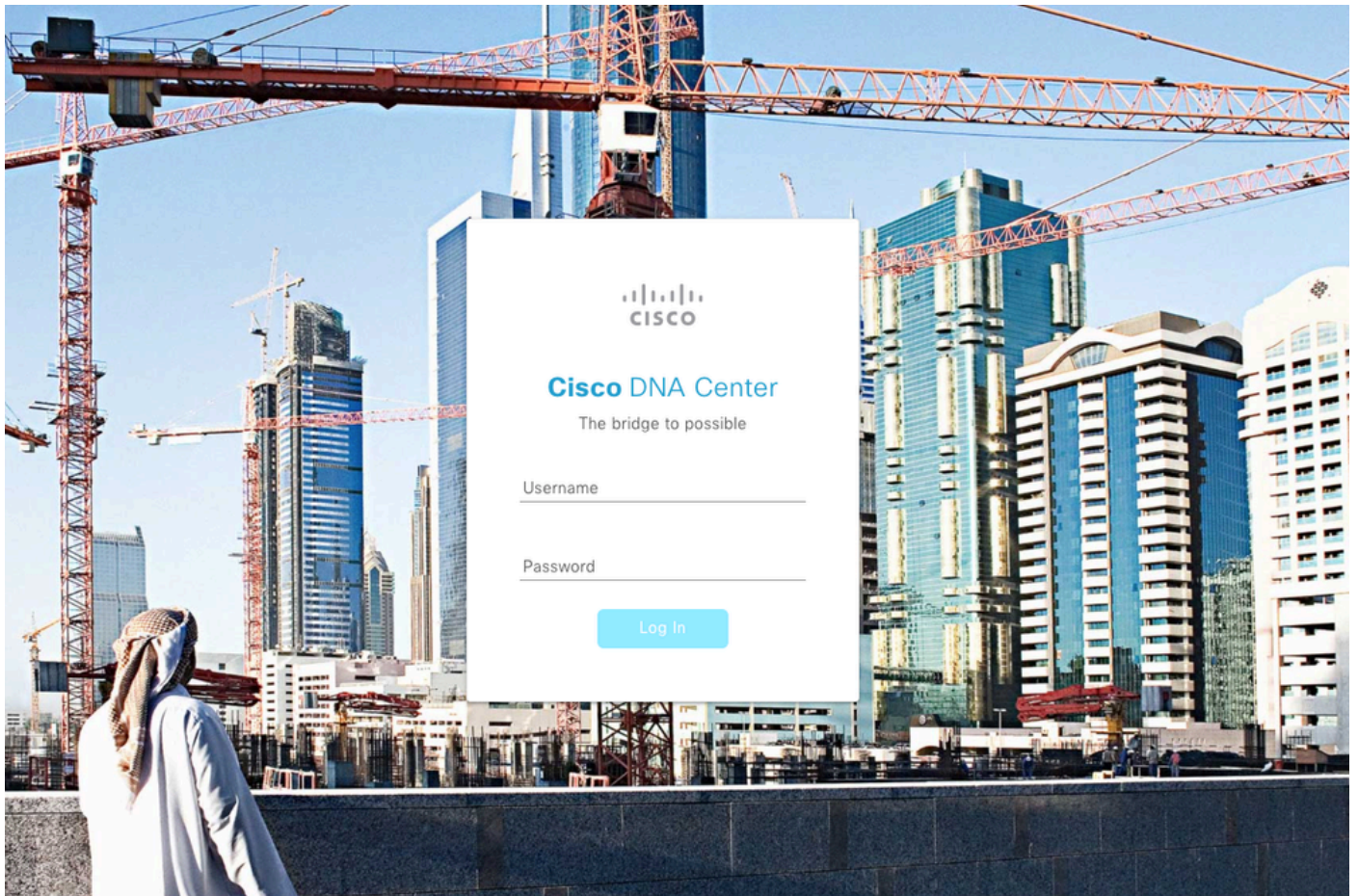
AV-paar op externe gebruiker

7. Klik in het aanvinkvakje Externe gebruiker inschakelen om externe verificatie in te schakelen:

Enable External User 

Verifiëren

U kunt de grafische gebruikersinterface van Cisco DNA Center (GUI) openen in een webbrowser en u kunt inloggen met een externe gebruiker die in de Windows-server is geconfigureerd om te bevestigen dat u met succes kunt inloggen met behulp van externe verificatie.



Aanmeldpagina voor Cisco DNA Center

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.