

Konfigurieren der externen Authentifizierung in Catalyst Center mit Windows Server

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Richtlinie für Administratorrolle](#)

[Richtlinie zur Beobachterrolle](#)

[Externe Authentifizierung aktivieren](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie die externe Authentifizierung im Cisco DNA Center mithilfe des Netzwerkrichtlinienservers (Network Policy Server, NPS) in Windows Server als RADIUS konfiguriert wird.

Voraussetzungen

Anforderungen

Grundlegendes Wissen zu:

- Cisco DNA Center - Benutzer und Rollen
- Windows Server-Netzwerkrichtlinienserver, RADIUS und Active Directory

Verwendete Komponenten

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server Version 2019 als Domänencontroller, DNS-Server, NPS und Active Directory

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.



Hinweis: Das Cisco Technical Assistance Center (TAC) bietet keinen technischen Support für Microsoft Windows Server. Wenn Probleme mit der Microsoft Windows Server-Konfiguration auftreten, wenden Sie sich an den Microsoft-Support, um technische Unterstützung zu erhalten.

Konfigurieren

Richtlinie für Administratorrolle

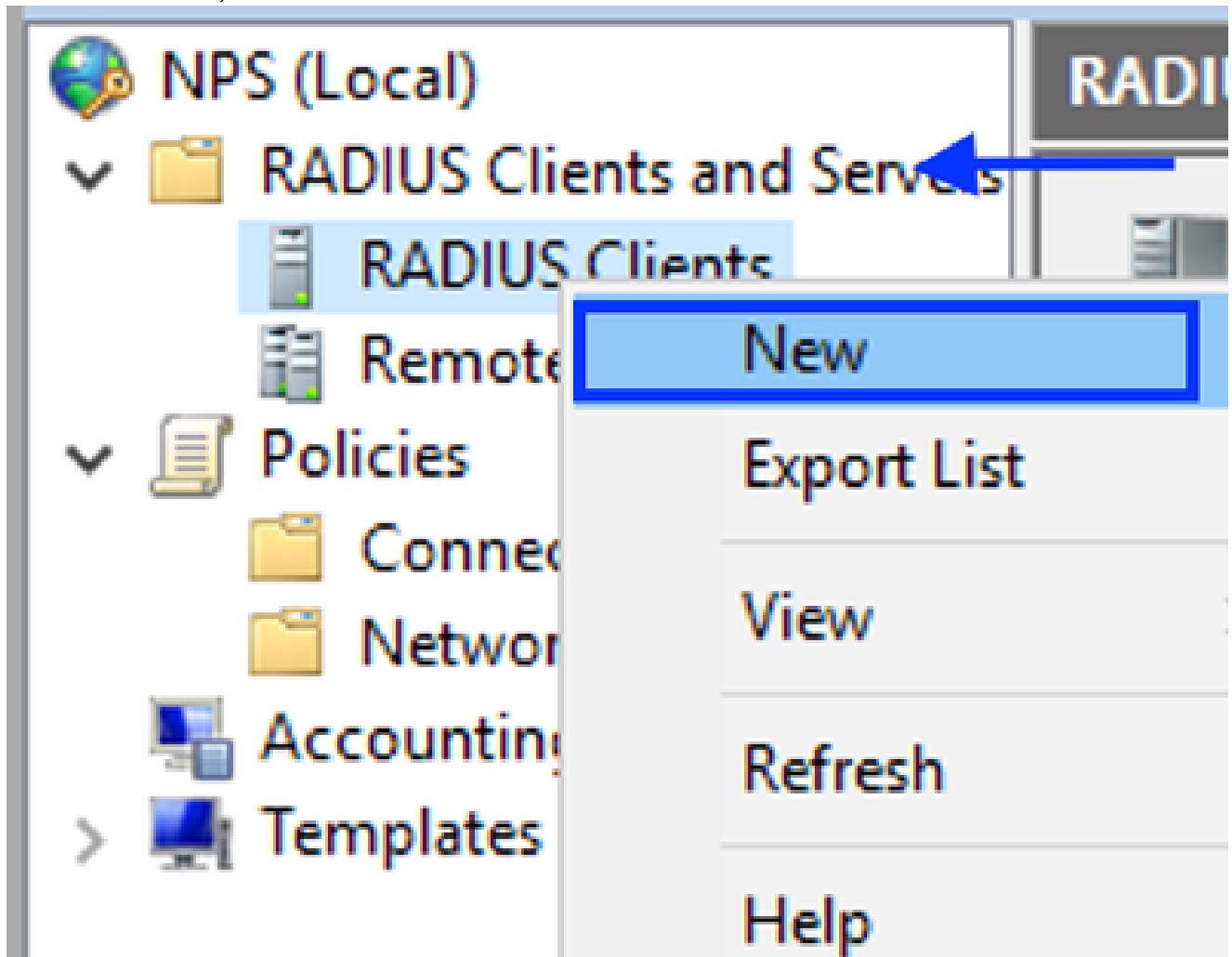
1. Klicken Sie in das Windows-Startmenü, und suchen Sie nach NPS. Wählen Sie dann Netzwerkrichtlinienserver aus:



Network Policy Server

Desktop app

4. Erweitern Sie RADIUS Clients and Servers, klicken Sie mit der rechten Maustaste auf RADIUS Clients, und wählen Sie Neu:



RADIUS-Client hinzufügen

5. Geben Sie den Anzeigenamen, die IP-Adresse für das Management von Cisco DNA Center und einen gemeinsamen geheimen Schlüssel ein (dieser kann später verwendet werden):

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.

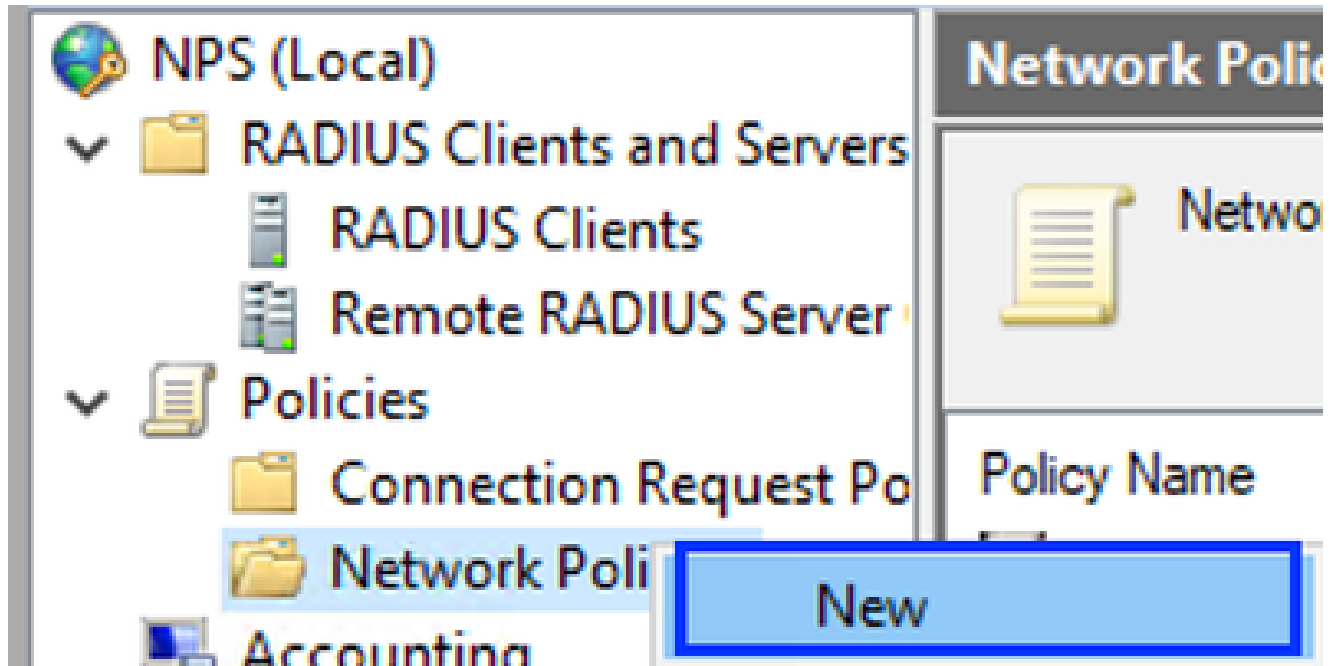
Manual Generate

Shared secret:

Confirm shared secret:

RADIUS-Client-Konfiguration

6. Klicken Sie auf OK, um sie zu speichern.
7. Erweitern Sie Richtlinien, klicken Sie mit der rechten Maustaste auf Netzwerkrichtlinien, und wählen Sie Neu aus:



Neue Netzwerkrichtlinie hinzufügen

8. Geben Sie einen Richtliniennamen für die Regel ein, und klicken Sie auf Weiter:



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

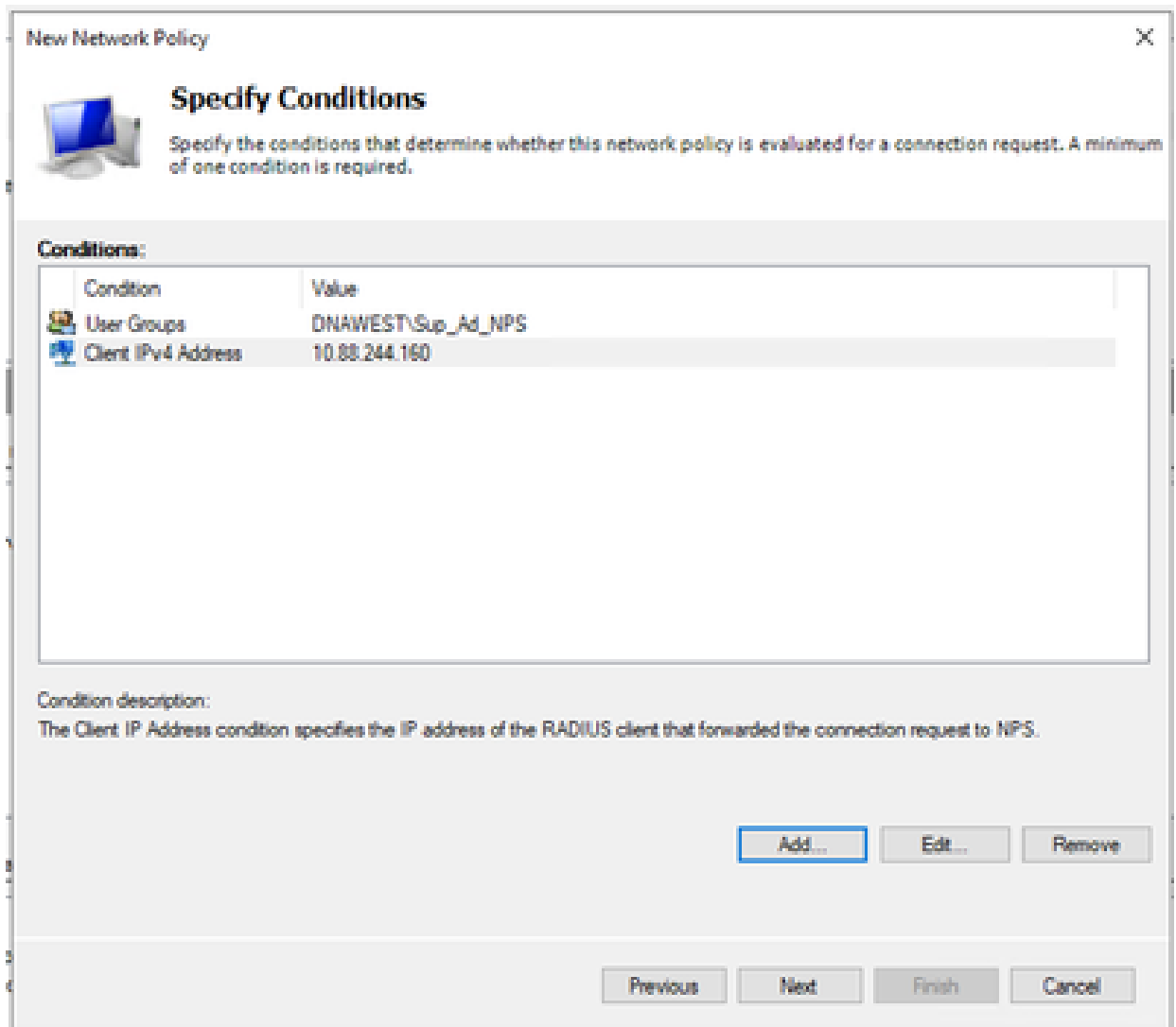
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Vendor specific:

Richtliniename


9. Um eine bestimmte Domänengruppe zuzulassen, fügen Sie diese beiden Bedingungen hinzu, und klicken Sie auf Weiter:
- Benutzergruppe - Fügen Sie Ihre Domänengruppe hinzu, die im Cisco DNA Center eine Administratorrolle übernehmen kann (für dieses Beispiel wird die Gruppe Sup_Ad_NPS verwendet).
 - ClientIPv4Address - Fügen Sie Ihre Cisco DNA Center Management IP-Adresse hinzu.



Richtlinienbedingungen

10. Wählen Sie Zugriff gewährt aus, und klicken Sie auf Weiter:

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

Zugriff gewährt verwenden

11. Wählen Sie nur unverschlüsselte Authentifizierung (PAP, SPAP) aus:



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

Unverschlüsselte Authentifizierung auswählen

12. Wählen Sie Weiter aus, da Standardwerte verwendet werden:



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

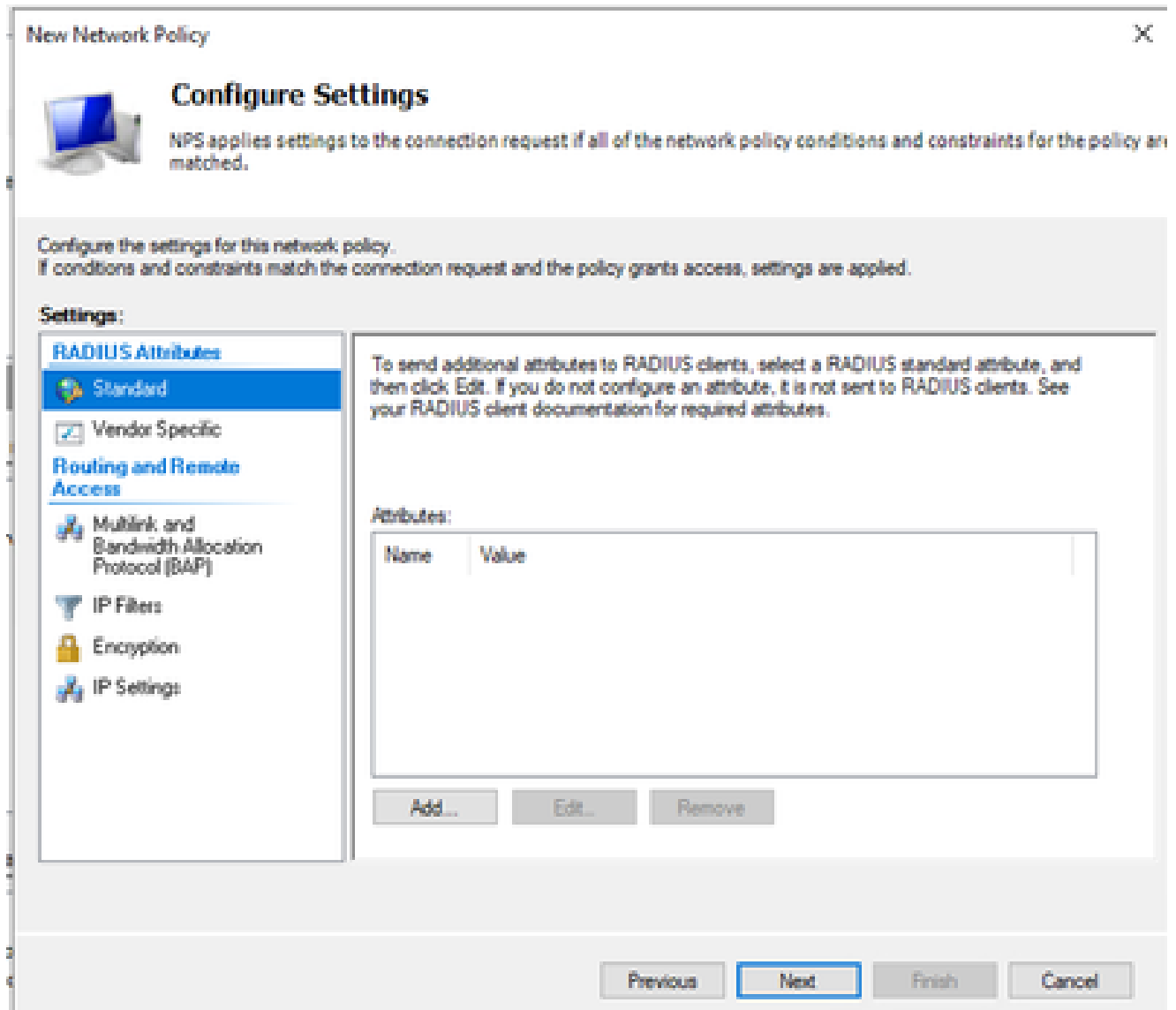
Next

Finish

Cancel

Constraint-Fenster konfigurieren

13. Standardattribute entfernen:



Zu verwendende Attribute definieren

14. Wählen Sie für RADIUS-Attribute "Herstellerspezifisch" aus, klicken Sie auf Hinzufügen, wählen Sie Cisco als Anbieter aus, und klicken Sie auf Hinzufügen:

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-Pair hinzufügen

15. Klicken Sie auf Hinzufügen, schreiben Sie Role=SUPER-ADMIN-ROLE und klicken Sie zweimal auf 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

Cisco AV-Pair-Attribut hinzugefügt

16. Wählen Sie Schließen und dann Weiter aus.

17. Überprüfen Sie Ihre Richtlinieninstellungen, und wählen Sie Beenden, um sie zu speichern.



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

Richtlinienübersicht

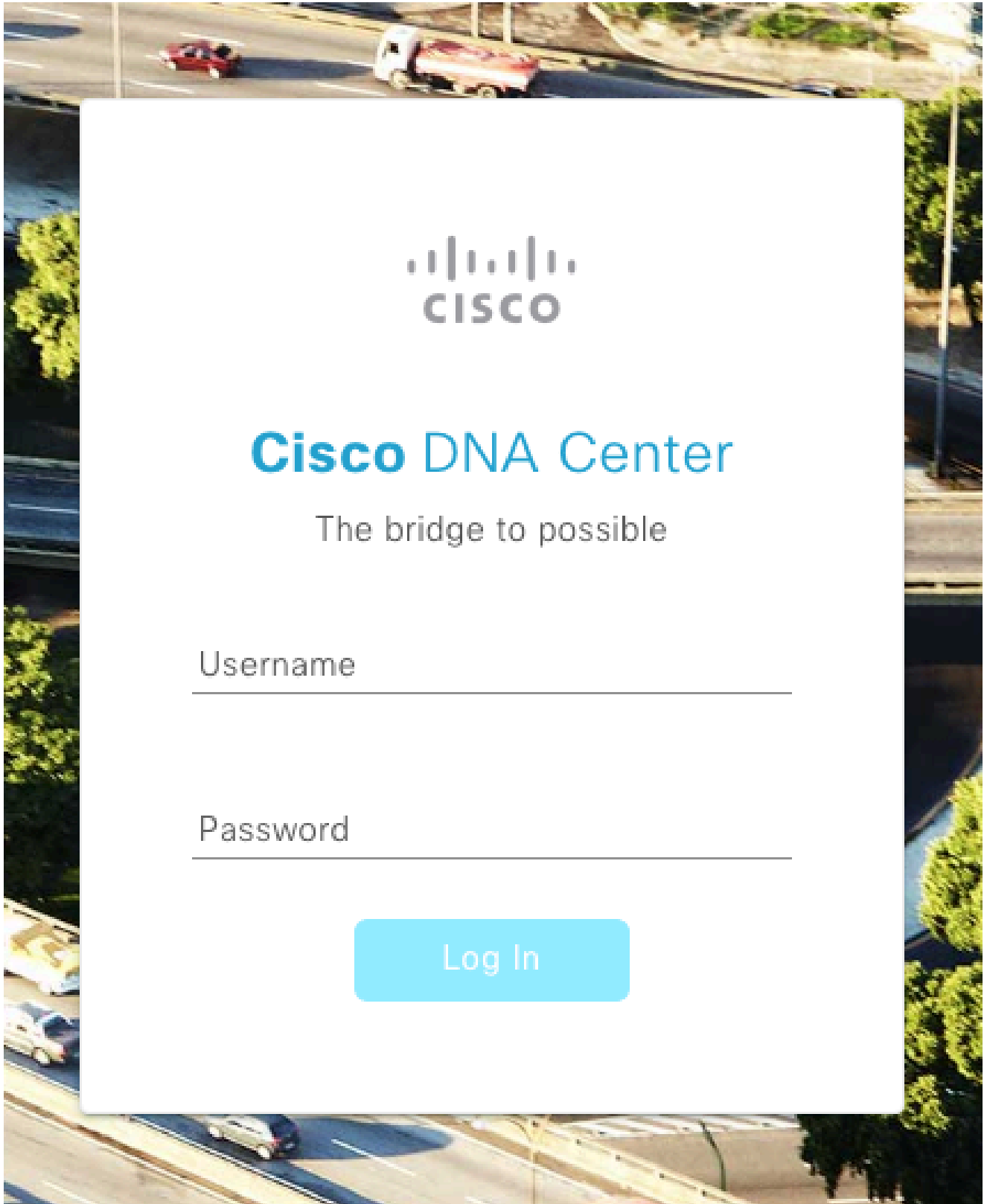
Richtlinie zur Beobachterrolle.

1. Klicken Sie in das Windows-Startmenü, und suchen Sie nach NPS. Wählen Sie dann Netzwerkrichtlinienserver aus.
2. Klicken Sie im Navigationsbereich auf der linken Seite mit der rechten Maustaste auf die Option NPS (Lokal), und wählen Sie Server in Active Directory registrieren aus.
3. Klicken Sie zweimal auf OK.
4. Erweitern Sie RADIUS Clients and Servers, klicken Sie mit der rechten Maustaste auf RADIUS Clients, und wählen Sie Neu.
5. Geben Sie einen Anzeigenamen, die IP-Adresse für das Management von Cisco DNA Center und einen gemeinsamen geheimen Schlüssel ein (dieser kann später verwendet werden).

6. Klicken Sie auf OK, um sie zu speichern.
7. Erweitern Sie Richtlinien, klicken Sie mit der rechten Maustaste auf Netzwerkrichtlinien, und wählen Sie Neu aus.
8. Geben Sie einen Richtliniennamen für die Regel ein, und klicken Sie auf Weiter.
9. Um eine bestimmte Domänengruppe zuzulassen, müssen Sie diese beiden Bedingungen hinzufügen und Weiter auswählen.
 - Benutzergruppe - Fügen Sie Ihre Domänengruppe hinzu, um eine Beobachterrolle im Cisco DNA Center zuzuweisen (in diesem Beispiel wird die Gruppe Observer_NPS verwendet).
 - ClientIPv4Address - Fügen Sie Ihre Cisco DNA Center Management-IP.
10. Wählen Sie Zugriff gewährt und dann Weiter aus.
11. Wählen Sie nur unverschlüsselte Authentifizierung (PAP, SPAP) aus.
12. Wählen Sie Weiter aus, da Standardwerte verwendet werden.
13. Entfernen Sie Standard-Attribute.
14. Wählen Sie unter RADIUS-Attribute die Option Herstellerspezifisch aus, klicken Sie dann auf Hinzufügen, wählen Sie Cisco als Anbieter aus, und klicken Sie auf Hinzufügen.
15. Wählen Sie Hinzufügen, schreiben Sie ROLE=OBSERVER-ROLE und OK zweimal.
16. Wählen Sie Schließen und dann Weiter aus.
17. Überprüfen Sie Ihre Richtlinienereinstellungen, und wählen Sie Beenden, um sie zu speichern.

Externe Authentifizierung aktivieren

1. Öffnen Sie die grafische Benutzeroberfläche (GUI) von Cisco DNA Center in einem Webbrowser, und melden Sie sich mit einem privilegierten Administratorkonto an:



Cisco DNA Center Anmeldeseite

2. Navigieren Sie zu Menü > System > Setting > Authentication and Policy Servers, und wählen Sie Add > AAA aus:

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 hinzufügen

3. Geben Sie Ihre Windows Server-IP-Adresse und den in den vorherigen Schritten verwendeten geheimen Schlüssel ein, und klicken Sie auf Speichern:

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Überprüfen Sie, ob Ihr Windows Server-Status Aktiv ist:

10.88.244.148

RADIUS

AAA

ACTIVE



Windows Server - Zusammenfassung

5. Navigieren Sie zu Menü > System > Benutzer & Rollen > Externe Authentifizierung, und wählen Sie Ihren AAA-Server aus:

▼ 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. Geben Sie Cisco-AVPair als AAA-Attribut ein, und klicken Sie auf Aktualisieren:

✓ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

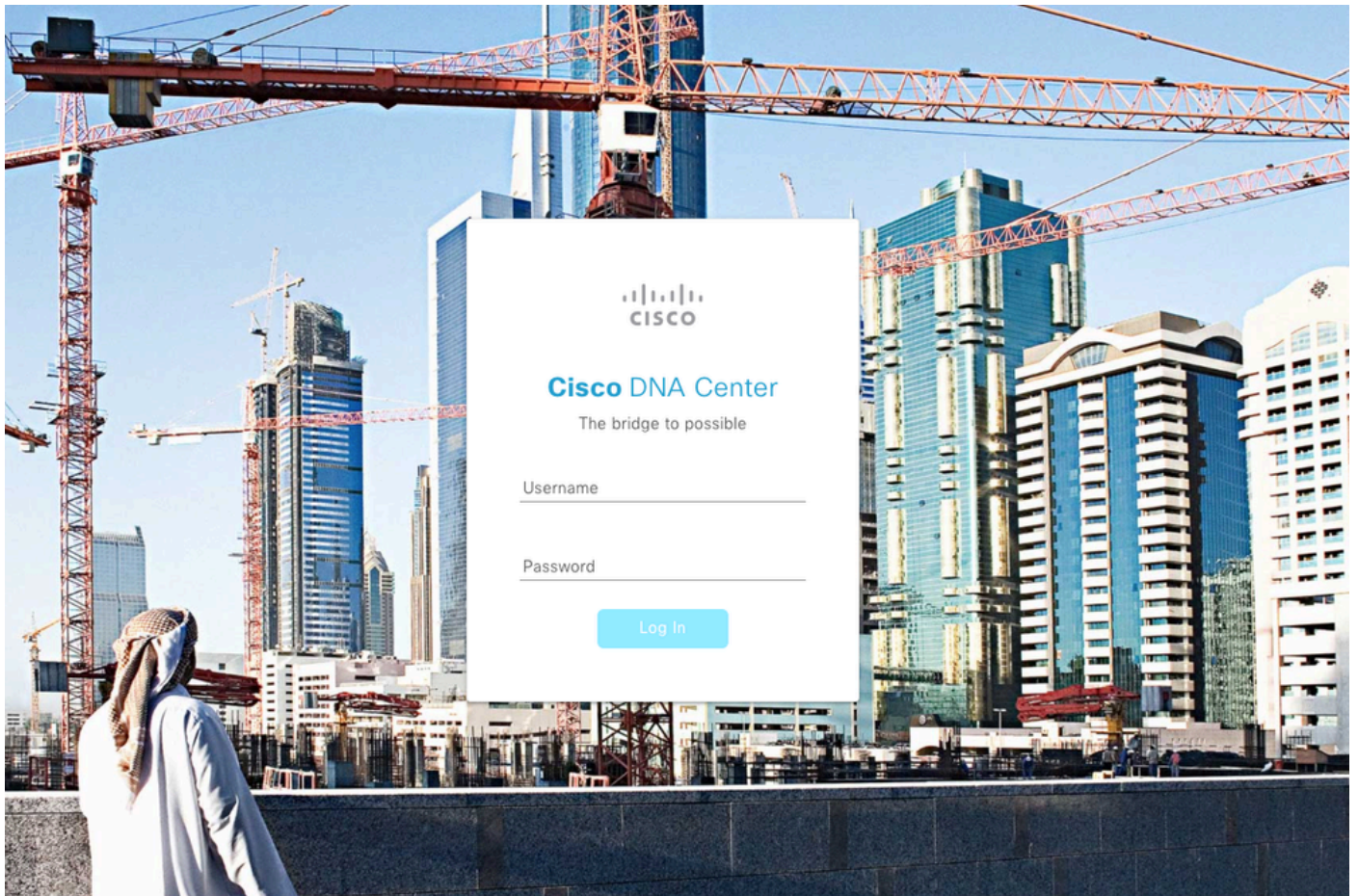
AV-Pair auf externem Benutzer

7. Klicken Sie in das Kontrollkästchen Externen Benutzer aktivieren, um die externe Authentifizierung zu aktivieren:

Enable External User 

Überprüfung

Sie können die grafische Benutzeroberfläche (GUI) von Cisco DNA Center in einem Webbrowser öffnen und sich mit einem externen Benutzer anmelden, der in Windows Server konfiguriert wurde, um zu überprüfen, ob Sie sich erfolgreich über die externe Authentifizierung anmelden können.



Cisco DNA Center Anmeldeseite

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.