

Configurazione dell'autenticazione esterna in Catalyst Center tramite Windows Server

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Criteri ruolo di amministratore](#)

[Criterio del ruolo dell'osservatore.](#)

[Abilita autenticazione esterna](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna in Cisco DNA Center utilizzando Server dei criteri di rete in Windows Server come RADIUS.

Prerequisiti

Requisiti

Conoscenze di base su:

- Utenti e ruoli di Cisco DNA Center
- Server dei criteri di rete Windows Server, RADIUS e Active Directory

Componenti usati

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server versione 2019 con funzione di controller di dominio, server DNS, Server dei criteri di rete e Active Directory

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.



Nota: il Cisco Technical Assistance Center (TAC) non fornisce supporto tecnico per Microsoft Windows Server. Se si verificano problemi con la configurazione di Microsoft Windows Server, contattare il supporto tecnico Microsoft per assistenza tecnica.

Configurazione

Criteri ruolo di amministratore

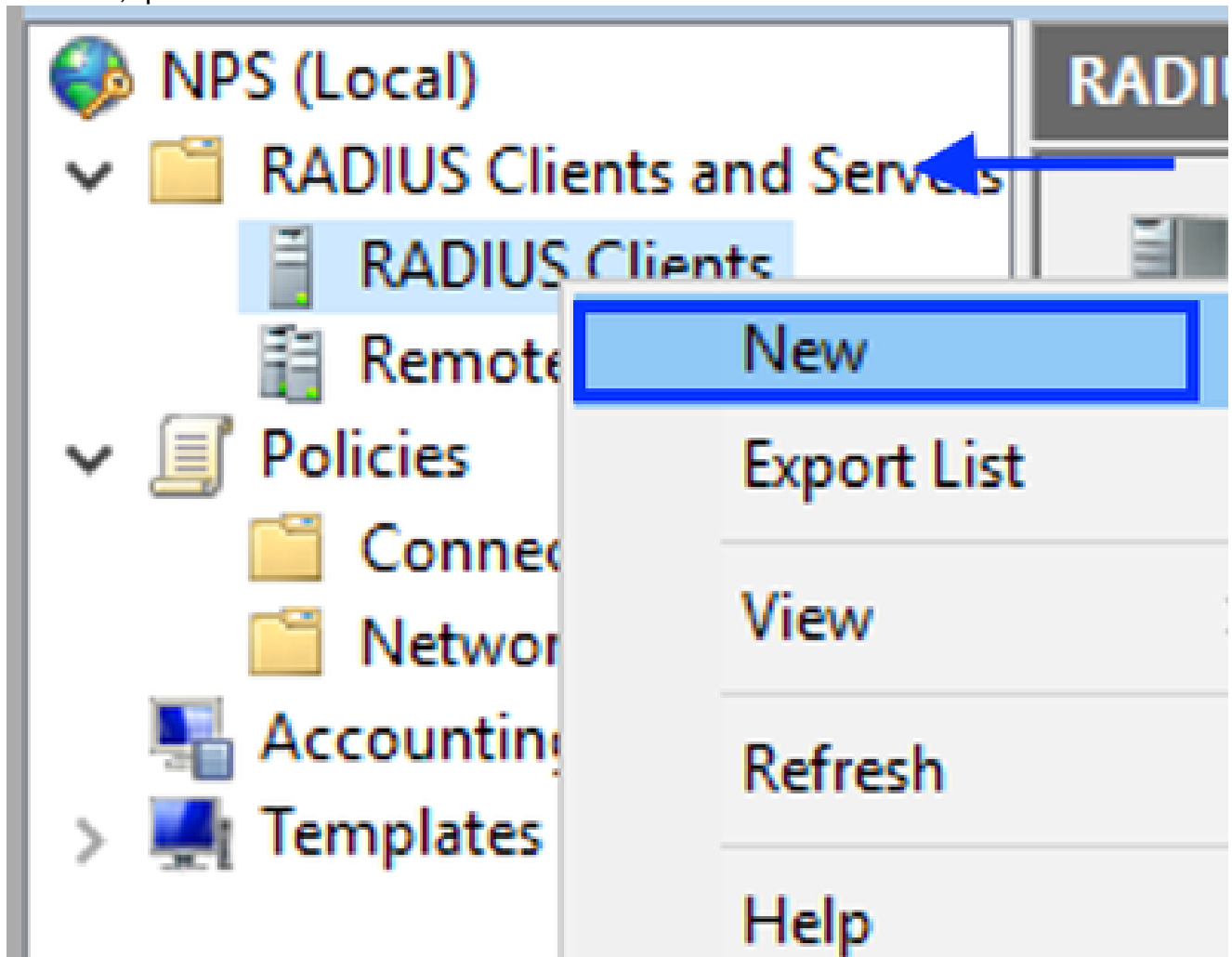
1. Fare clic su nel menu Start di Windows e cercare Server dei criteri di rete. Selezionare quindi Server dei criteri di rete:



Network Policy Server

Desktop app

4. Espandere Client e server RADIUS, fare clic con il pulsante destro del mouse su Client RADIUS, quindi selezionare Nuovo:



Aggiungi client RADIUS

5. Immettere il nome descrittivo, l'indirizzo IP di gestione di Cisco DNA Center e un segreto condiviso (utilizzabile in seguito):

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.

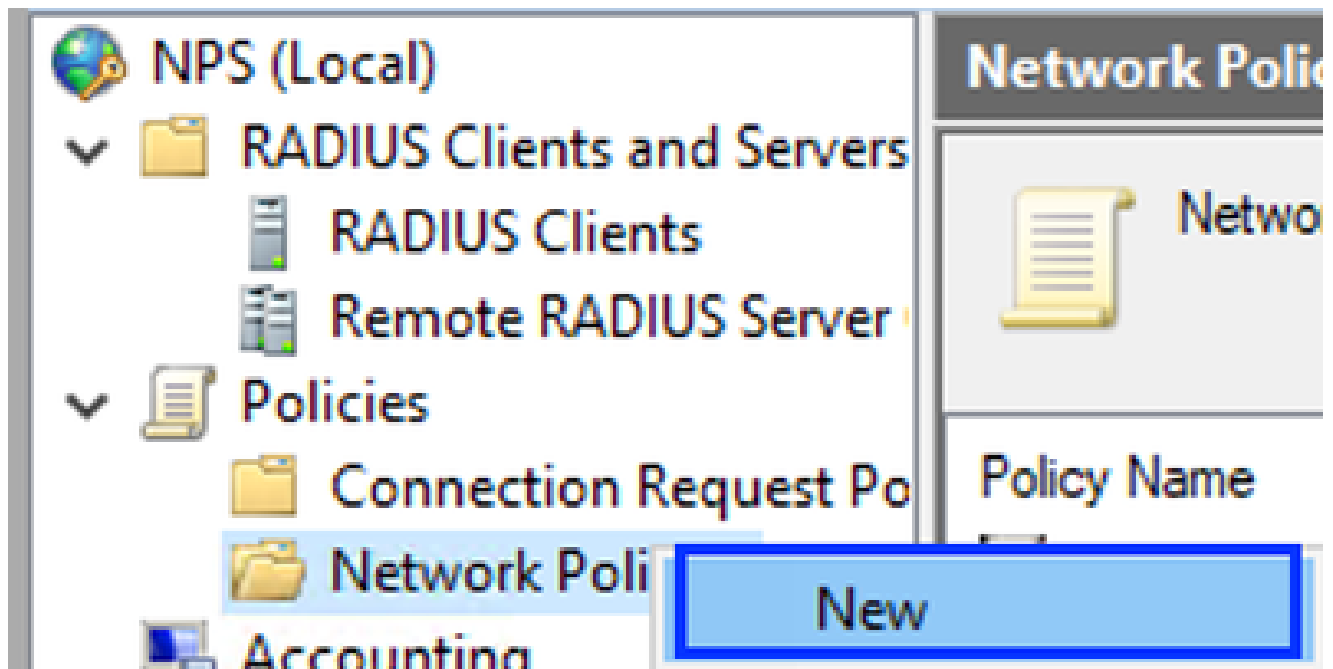
Manual Generate

Shared secret:

Confirm shared secret:

Configurazione client Radius

6. Fare clic su OK per salvarlo.
7. Espandere Criteri, fare clic con il pulsante destro del mouse su Criteri di rete e selezionare Nuovo:



Aggiungi nuovo criterio di rete

8. Immettere un nome di criterio per la regola e fare clic su Avanti:



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.

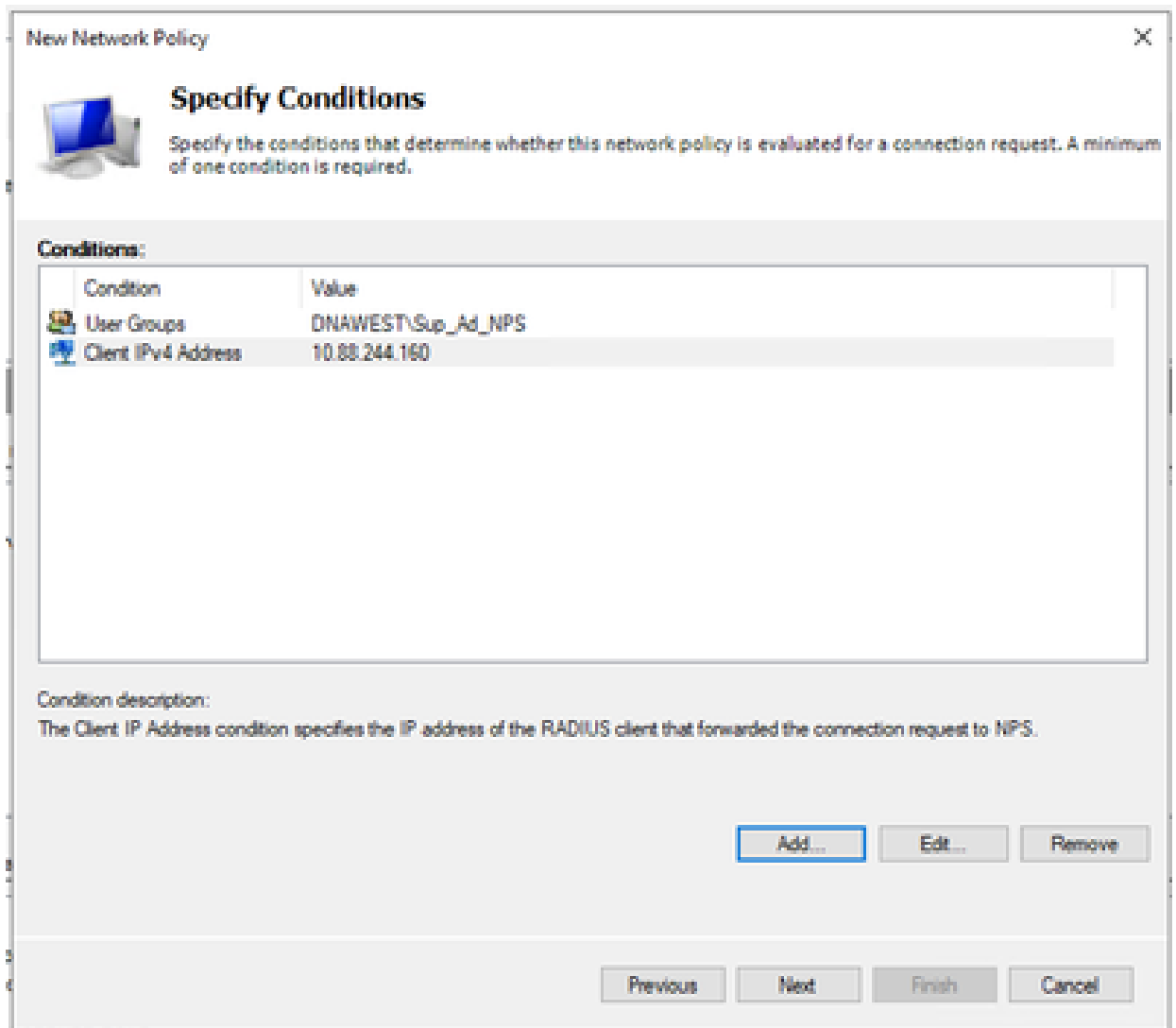
Type of network access server:

Vendor specific:

Nome criterio

9. Per consentire un gruppo di dominio specifico, aggiungere le due condizioni seguenti e fare clic su Avanti:


- Gruppo utenti: aggiungere il gruppo di dominio che può avere un ruolo di amministratore in Cisco DNA Center (per questo esempio viene utilizzato il gruppo Sup_Ad_NPS).
- Indirizzo IPv4client: aggiungere l'indirizzo IP di gestione di Cisco DNA Center.



Condizioni criterio

10. Selezionare Accesso concesso e fare clic su Avanti:

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

Usa accesso concesso

11. Selezionare solo autenticazione non crittografata (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

Seleziona autenticazione non crittografata

12. Selezionare Successivo poiché vengono utilizzati i valori predefiniti:



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

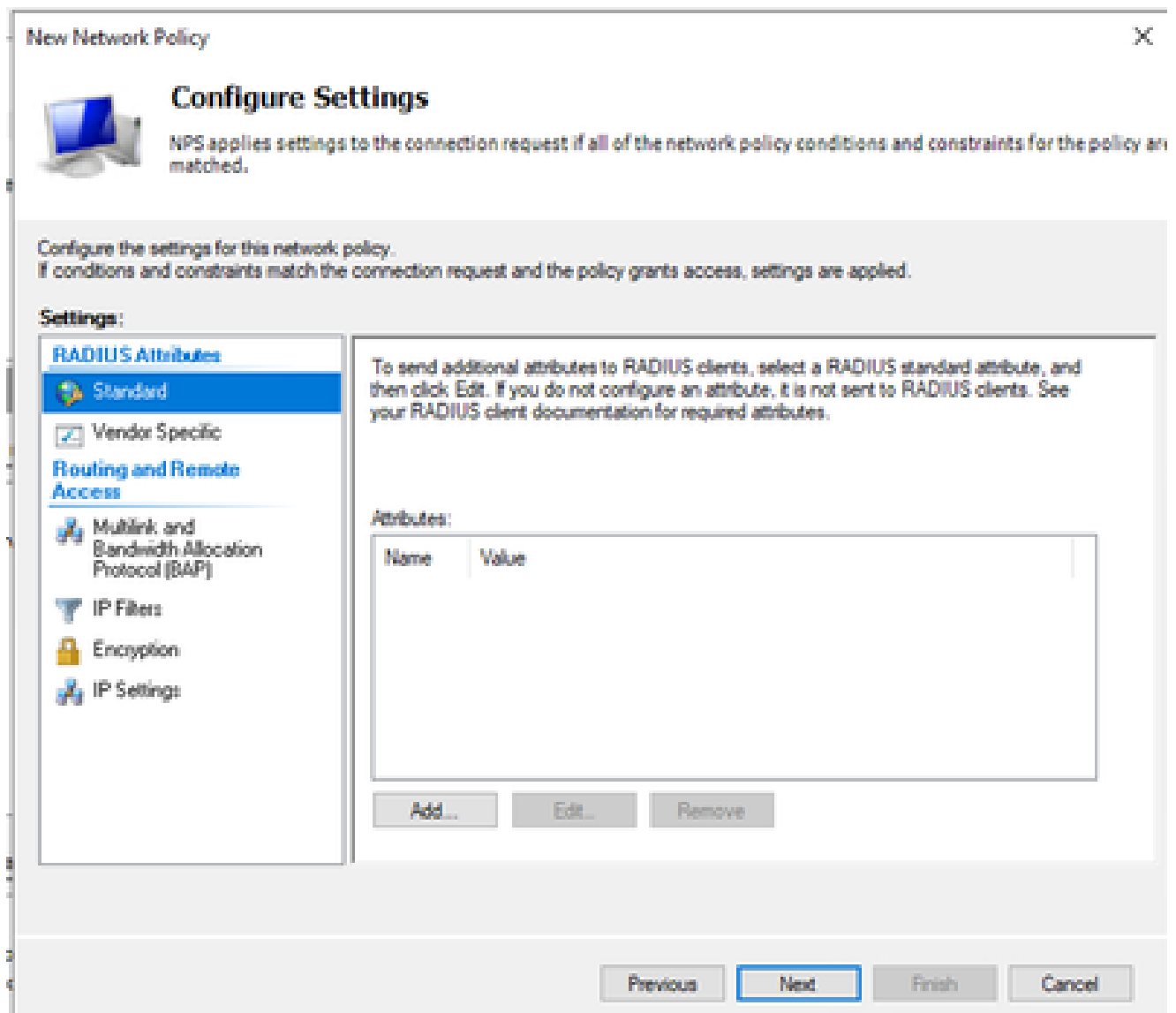
Next

Finish

Cancel

Finestra Configura vincolo

13. Rimuovi attributi standard:



Definisci attributi da utilizzare

14. In Attributi RADIUS selezionare Vendor Specific (Specifico del fornitore), fare clic su Add, selezionare Cisco come fornitore e fare clic su Add (Aggiungi):

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

Aggiungi Cisco AV-Pair

15. Fare clic su Add, write Role=SUPER-ADMIN-ROLE e fare clic su OK due volte:



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

Attributo Cisco AV-Pair aggiunto

16. Selezionare Chiudi, quindi Avanti.

17. Verificare le impostazioni dei criteri e selezionare Fine per salvarle.



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

Riepilogo criteri

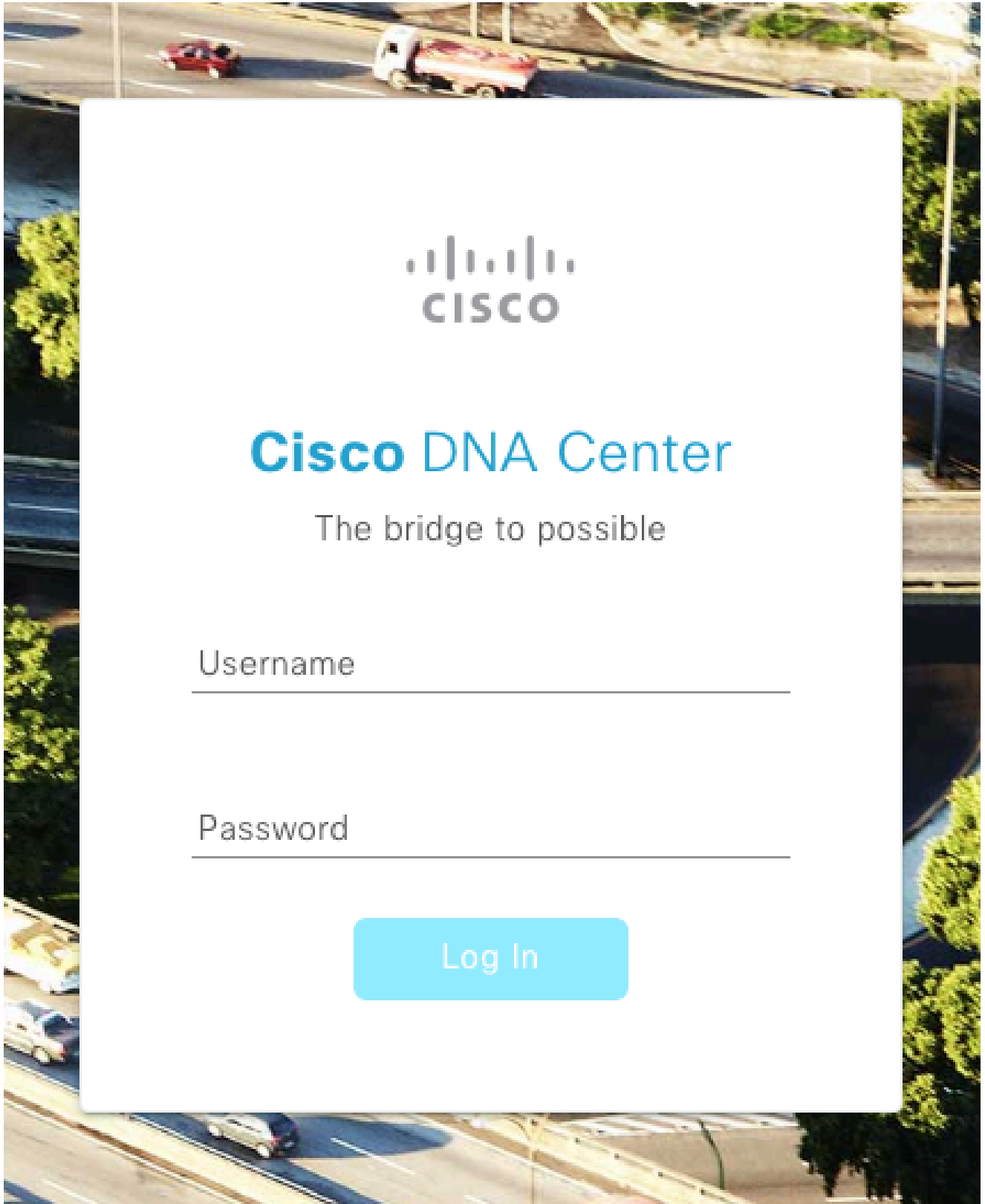
Criterio del ruolo dell'osservatore.

1. Fare clic su nel menu Start di Windows e cercare Server dei criteri di rete. Quindi selezionare Server dei criteri di rete.
2. Dal pannello di navigazione sul lato sinistro, fare clic con il pulsante destro del mouse sull'opzione Server dei criteri di rete (locale) , quindi selezionare Registra server in Active Directory.
3. Fare clic su OK due volte.
4. Espandere Client e server RADIUS, fare clic con il pulsante destro del mouse su Client RADIUS e selezionare Nuovo.
5. Immettere un nome descrittivo, l'indirizzo IP di gestione di Cisco DNA Center e un segreto condiviso (utilizzabile in seguito).

6. Fare clic su OK per salvarlo.
7. Espandere Criteri, fare clic con il pulsante destro del mouse su Criteri di rete e selezionare Nuovo.
8. Immettere un nome di criterio per la regola e fare clic su Avanti.
9. Per consentire un gruppo di dominio specifico, è necessario aggiungere queste due condizioni e selezionare Avanti.
 - Gruppo utenti: aggiungere il gruppo di dominio per assegnare un ruolo di osservatore al Cisco DNA Center (per questo esempio viene utilizzato il gruppo Observer_NPS).
 - Indirizzo IPv4client: aggiungere l'indirizzo IP di gestione di Cisco DNA Center.
10. Selezionare Accesso concesso, quindi Avanti.
11. Selezionare solo Autenticazione non crittografata (PAP, SPAP).
12. Selezionare Avanti poiché vengono utilizzati i valori predefiniti.
13. Rimuovere gli attributi standard.
14. In Attributi RADIUS selezionare Vendor Specific (Specifico del fornitore), fare clic su Add (Aggiungi), selezionare Cisco come fornitore e fare clic su Add (Aggiungi).
15. Selezionare Add, write ROLE=OBSERVER-ROLE e OK due volte.
16. Selezionare Chiudi, quindi Avanti.
17. Verificare le impostazioni dei criteri e selezionare Fine per salvarle.

Abilita autenticazione esterna

1. Aprire l'interfaccia grafica (GUI) di Cisco DNA Center in un browser Web ed effettuare l'accesso con un account con privilegi di amministratore:



Pagina di accesso a Cisco DNA Center

2. Passare a Menu > System > Setting > Authentication and Policy Server e selezionare Add > 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	RADIUS_TACACS

Aggiungi Windows Server

3. Digitare l'indirizzo IP del server Windows e il segreto condiviso utilizzati nei passaggi precedenti e fare clic su Salva:

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Verificare che lo stato di Windows Server sia Attivo:

10.88.244.148

RADIUS

AAA

ACTIVE



Riepilogo di Windows Server

5. Selezionare Menu > System > Users & Roles > External Authentication e selezionare il server AAA:

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

[Update](#)

Server Windows come server AAA

6. Digitare Cisco-AVPair come attributo AAA e fare clic su Aggiorna:

▼ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

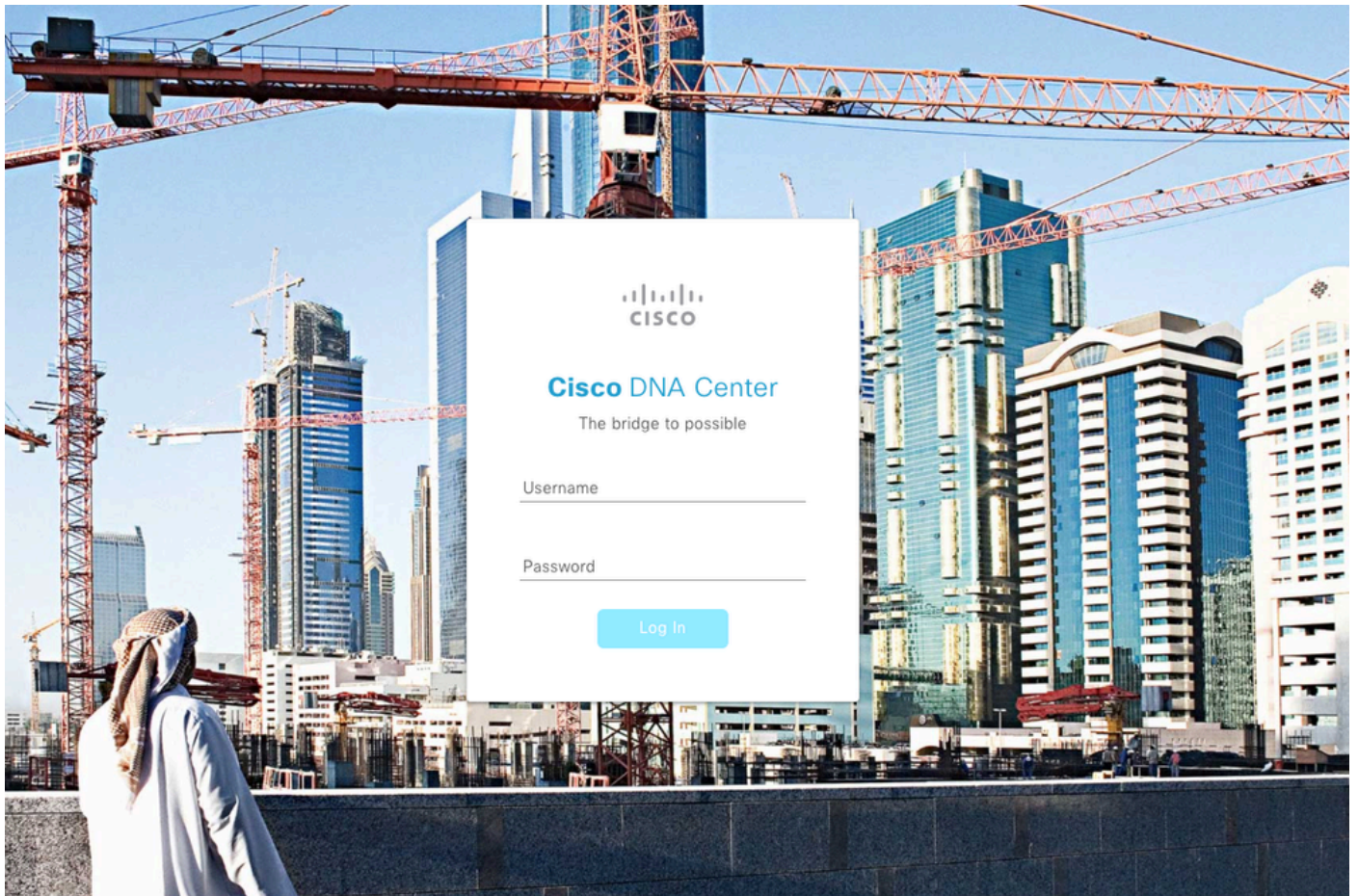
Coppia AV su utente esterno

7. Fare clic nella casella di controllo Abilita utente esterno per abilitare l'autenticazione esterna:

Enable External User 

Verifica

È possibile aprire l'interfaccia grafica utente (GUI) di Cisco DNA Center in un browser Web e accedere con un utente esterno configurato in Windows Server per verificare che sia possibile eseguire correttamente l'accesso utilizzando l'autenticazione esterna.



Pagina di accesso a Cisco DNA Center

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).