RADIUS Server Active Authentication LAB Using NPS

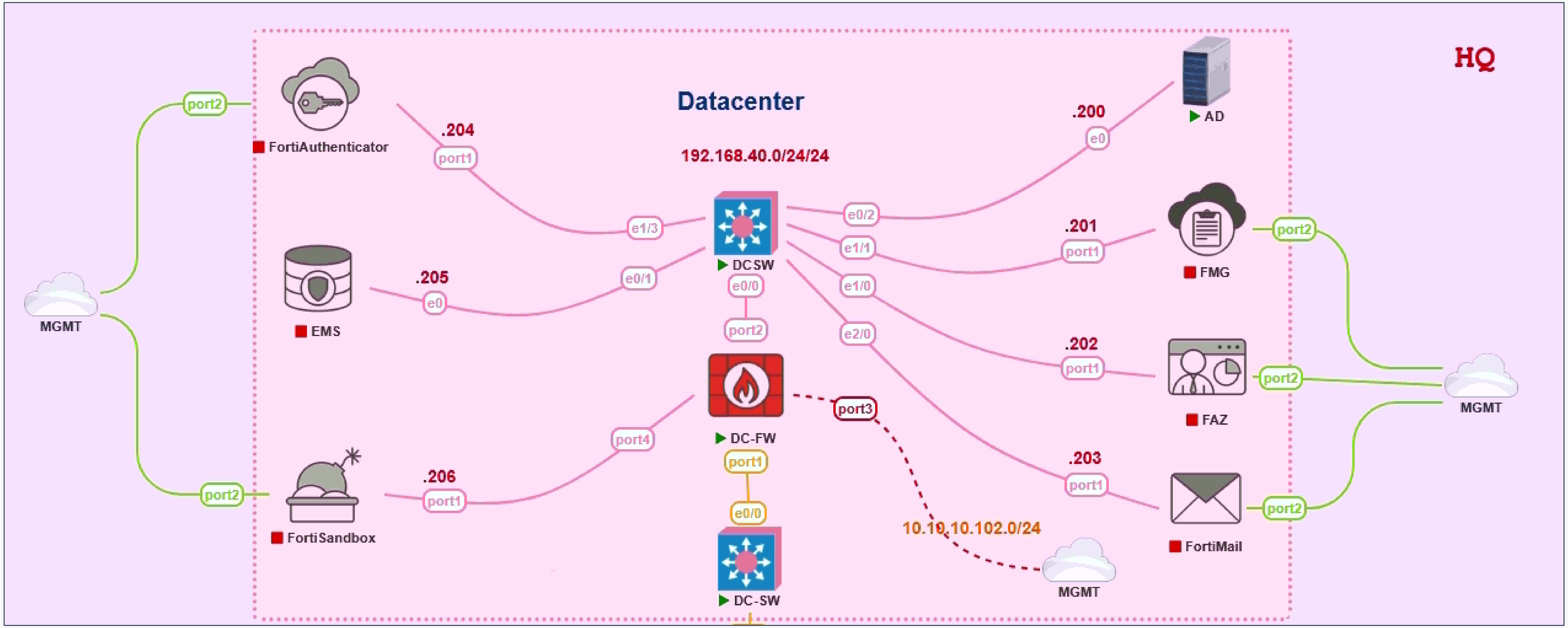
FCX_NSE8 : : FortiGate Administrator

MIAARI ACADEMY

EDUCATION & IT SOLUTIONS

FORTINET NSE 8 EXPERT

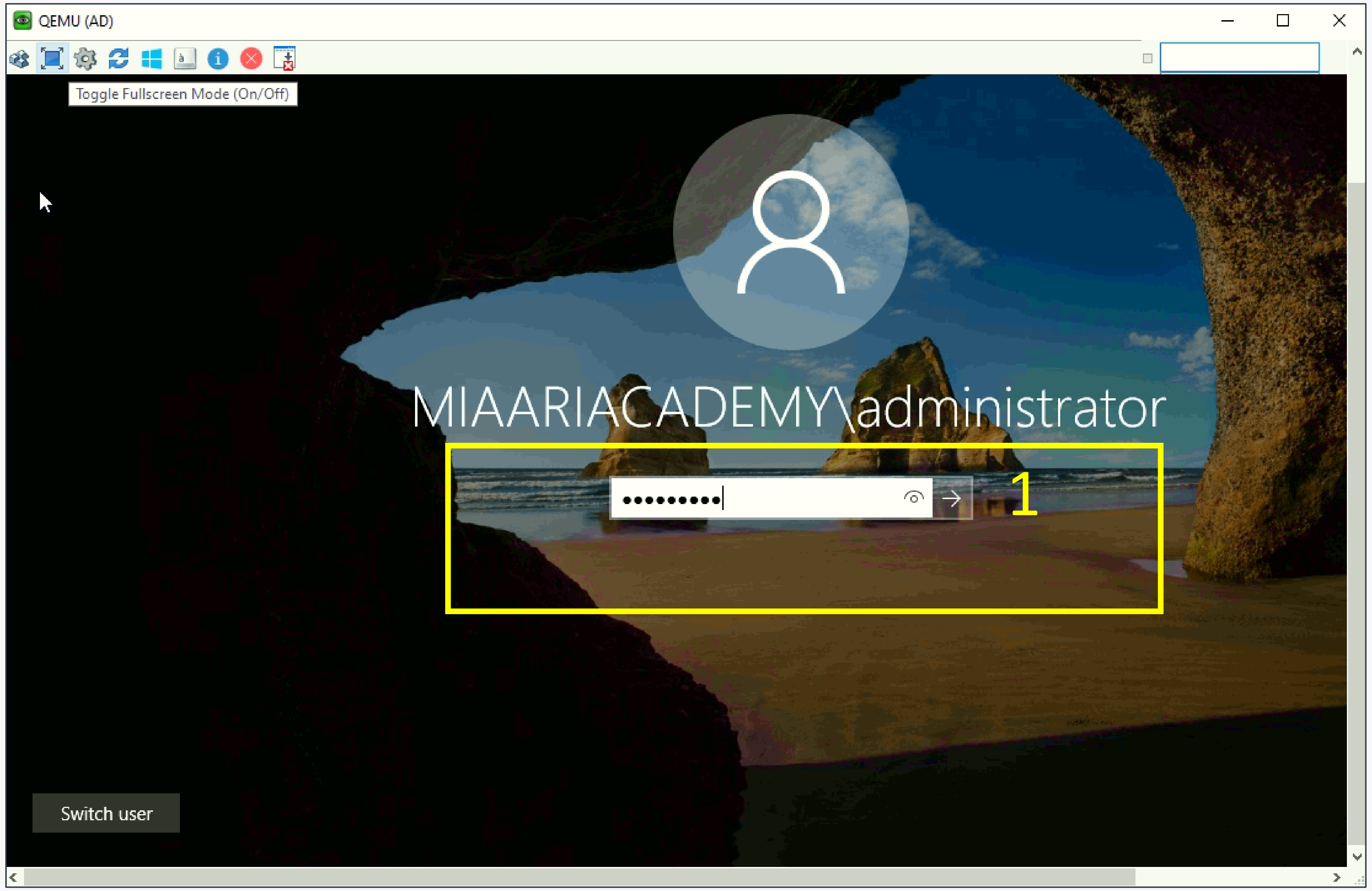
AD in Datacenter

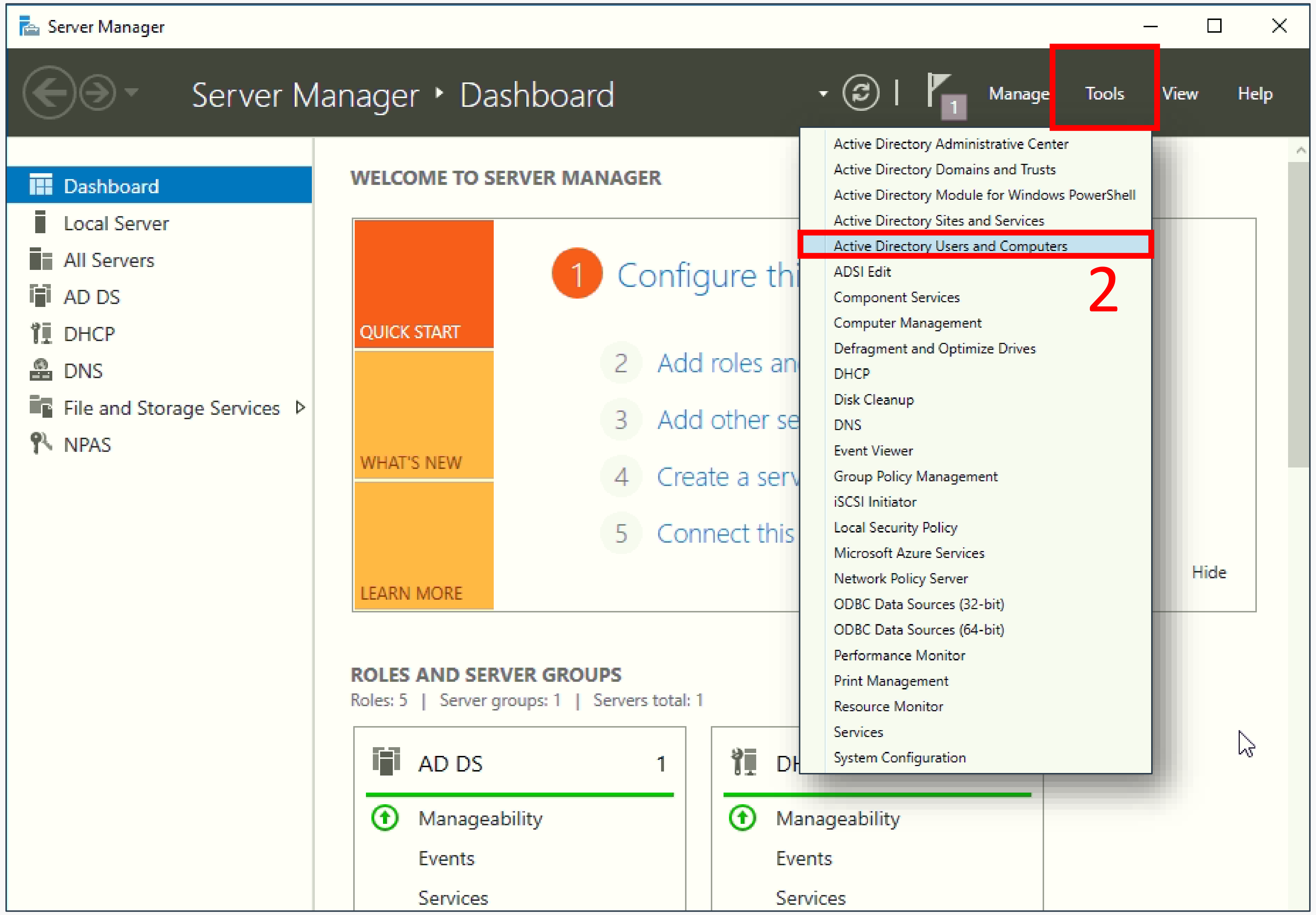


Access Active Directory Users and Computers

1. **Login to Windows Server (AD Server)**
   - Enter username: **MIAARIACADEMY\administrator**
   - Enter password **admin@123** and press Enter to login.

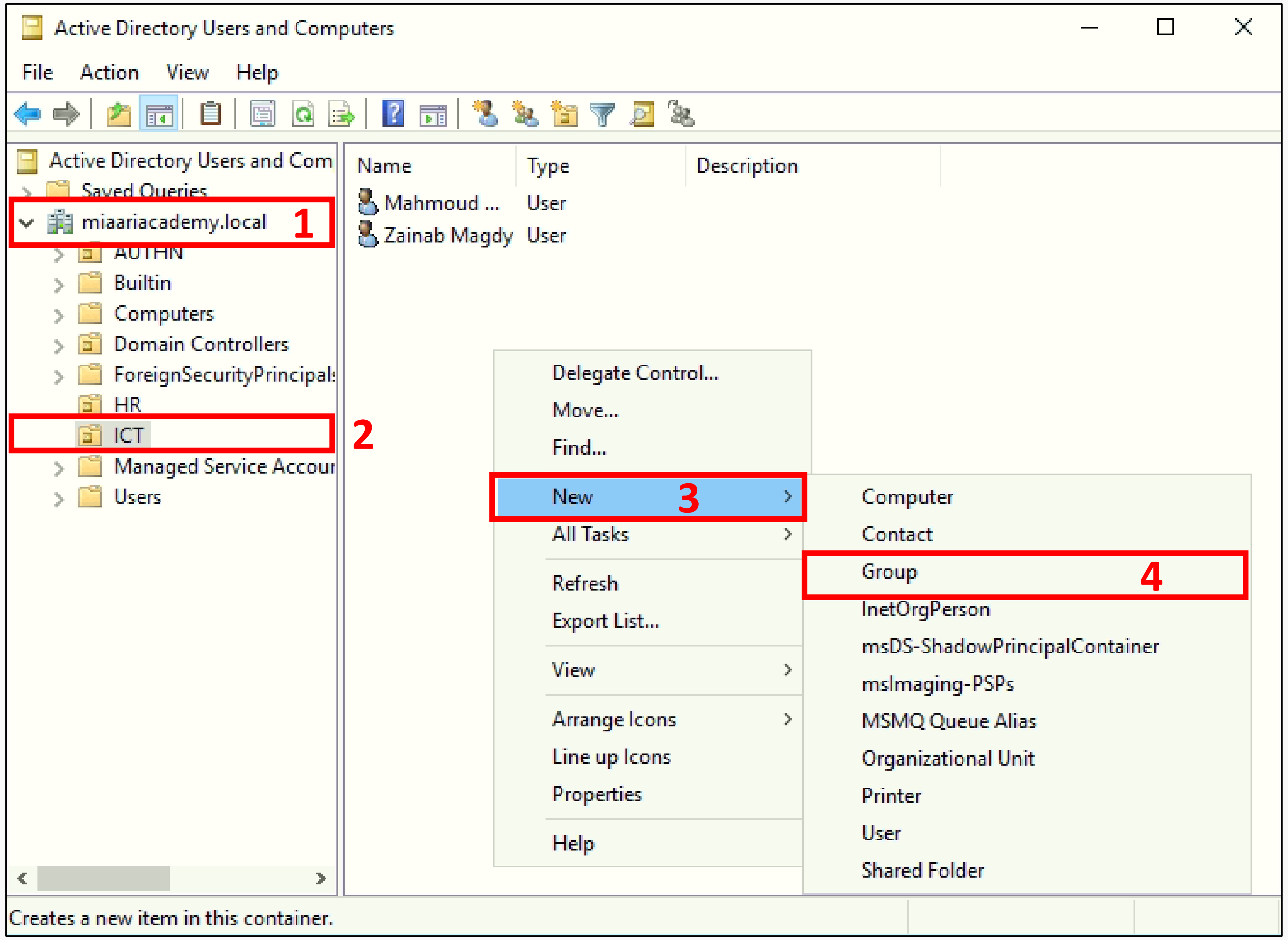
2. **Open** **Server Manager**, Click on **Tools** in the top-right menu and Select **Active Directory Users and Computers** from the drop-down list.



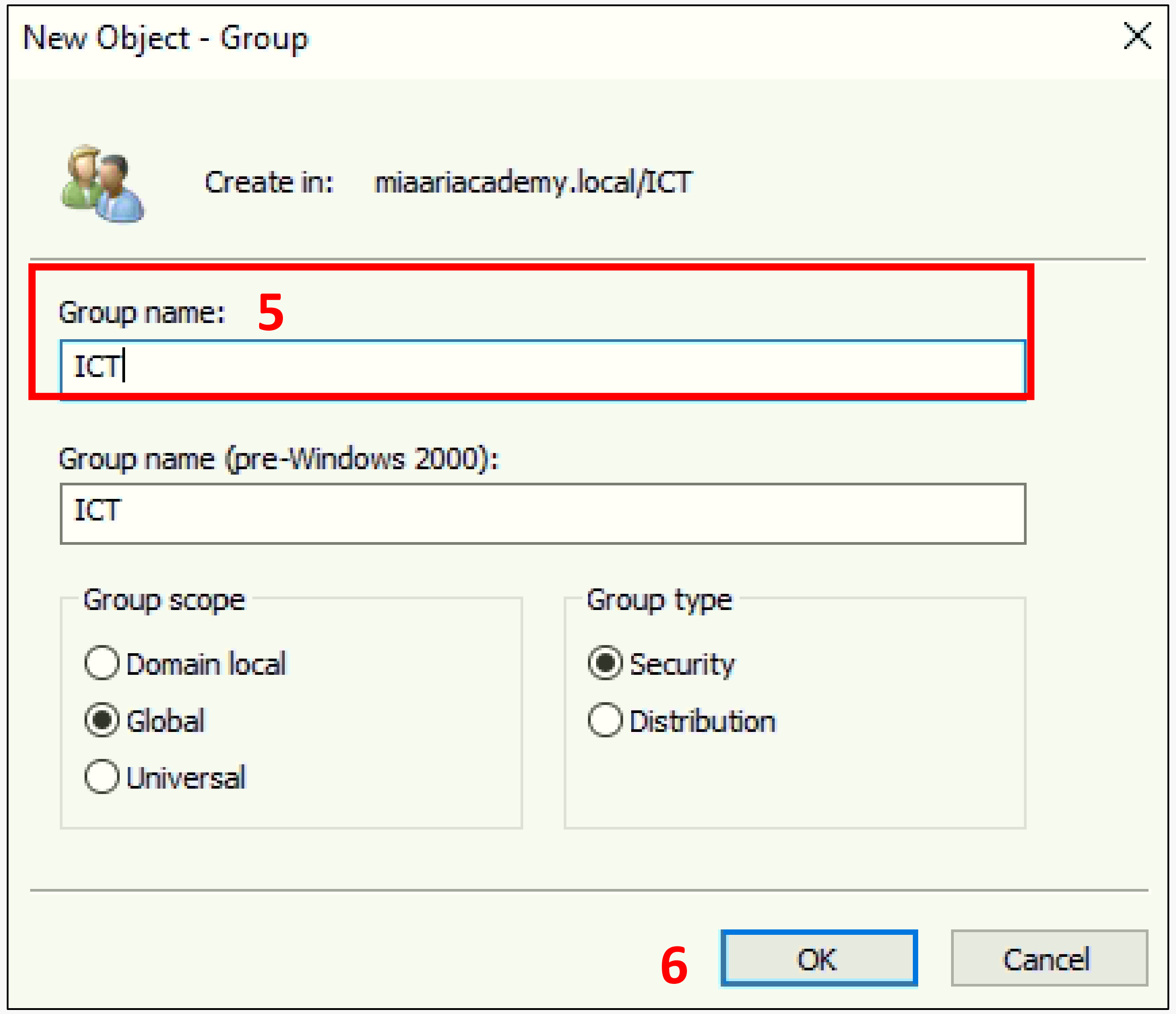


Creating a New Group ICT in Active Directory for RADIUS Authentication

1. Expand the domain `miaariacademy.local`.
2. Right-click on the `ICT` OU.
3. Navigate to `New`
4. Select `Group`.
5. Type the Group Name: `ICT`.
6. Click `OK` to create the group.



Creates a new item in this container.



Create in: miaariacademy.local/ICT

Group name: ICT

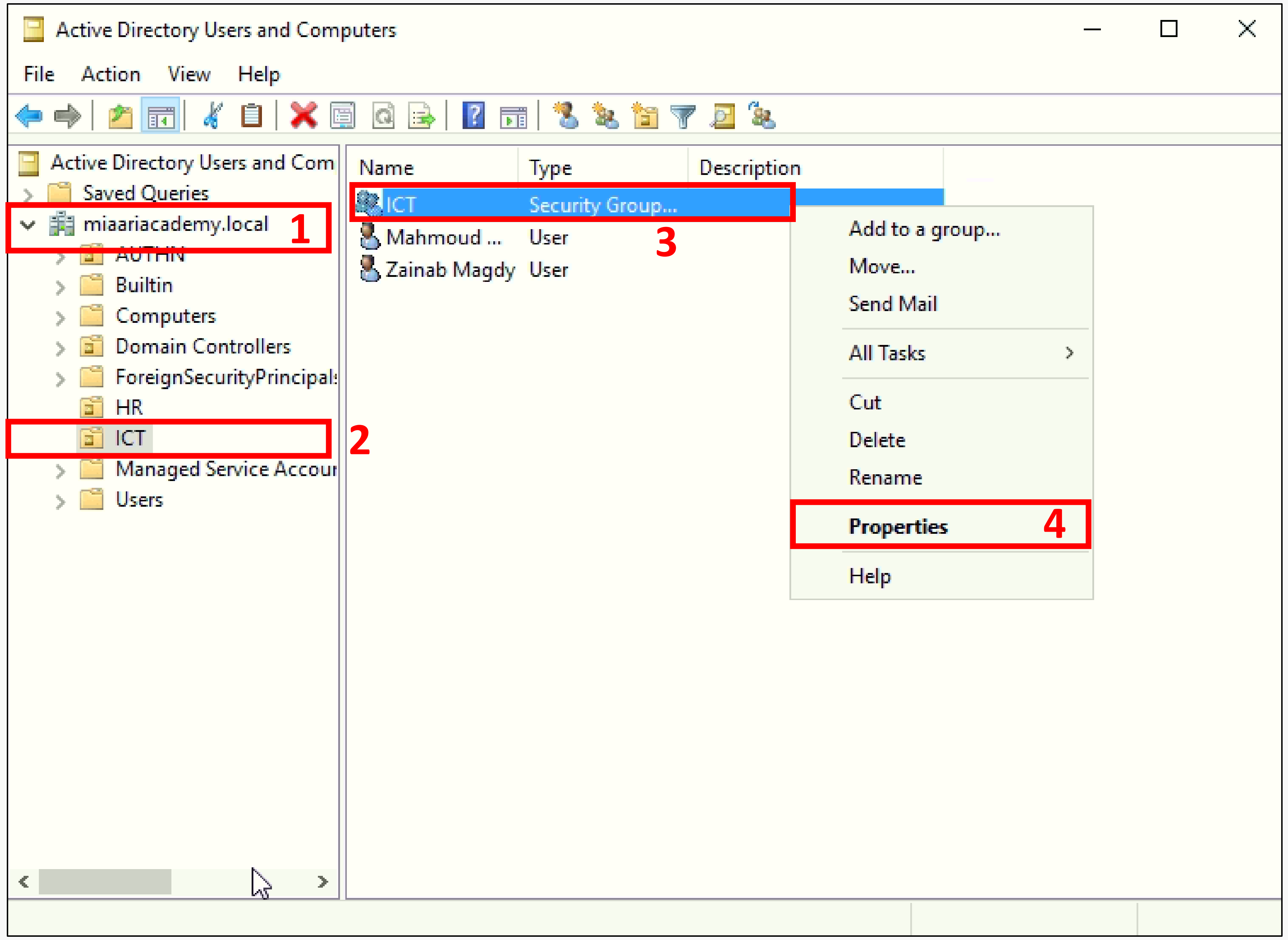
Group name (pre-Windows 2000): ICT

Group scope
○ Domain local
● Global
○ Universal

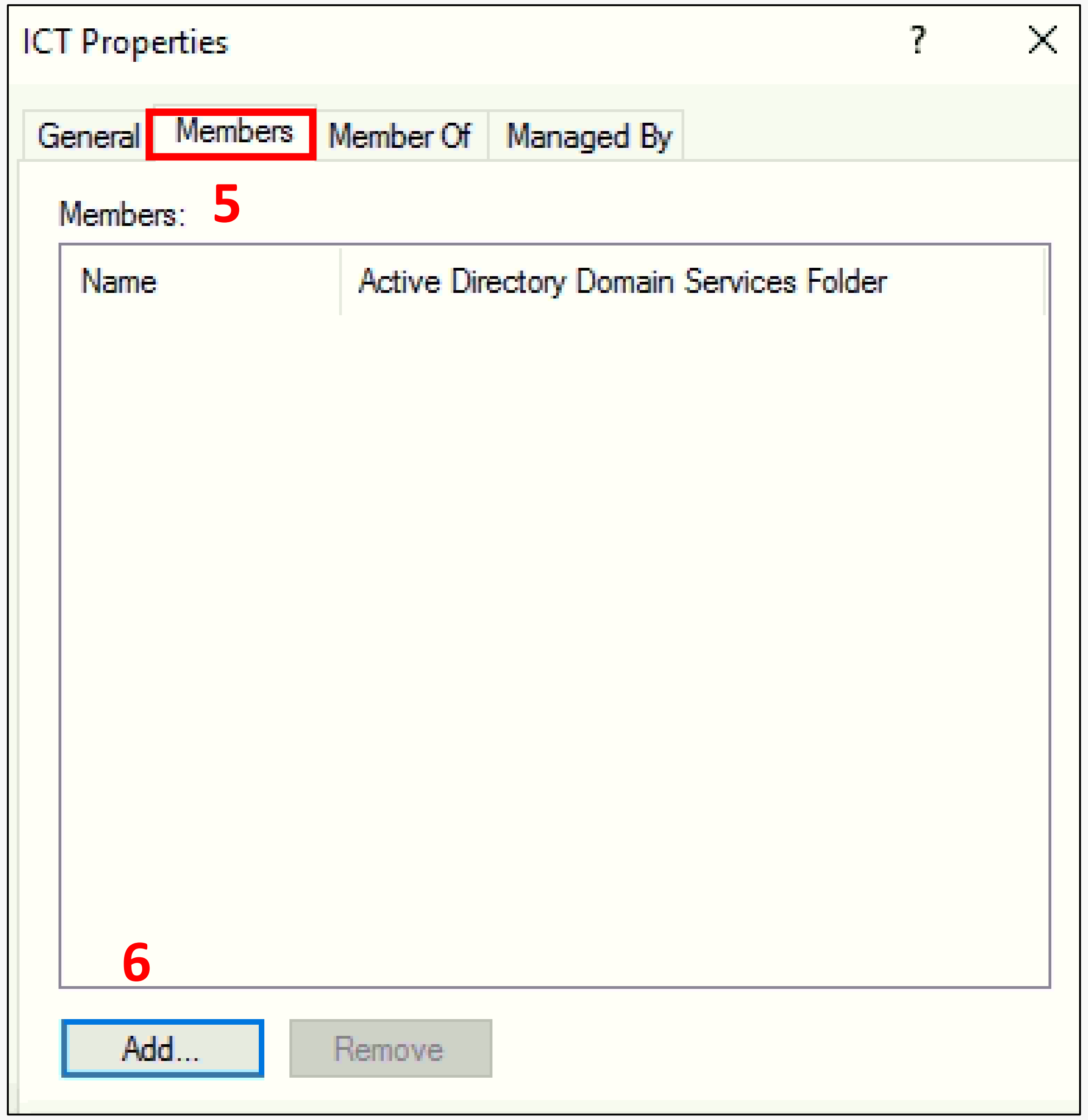
Group type
● Security
○ Distribution

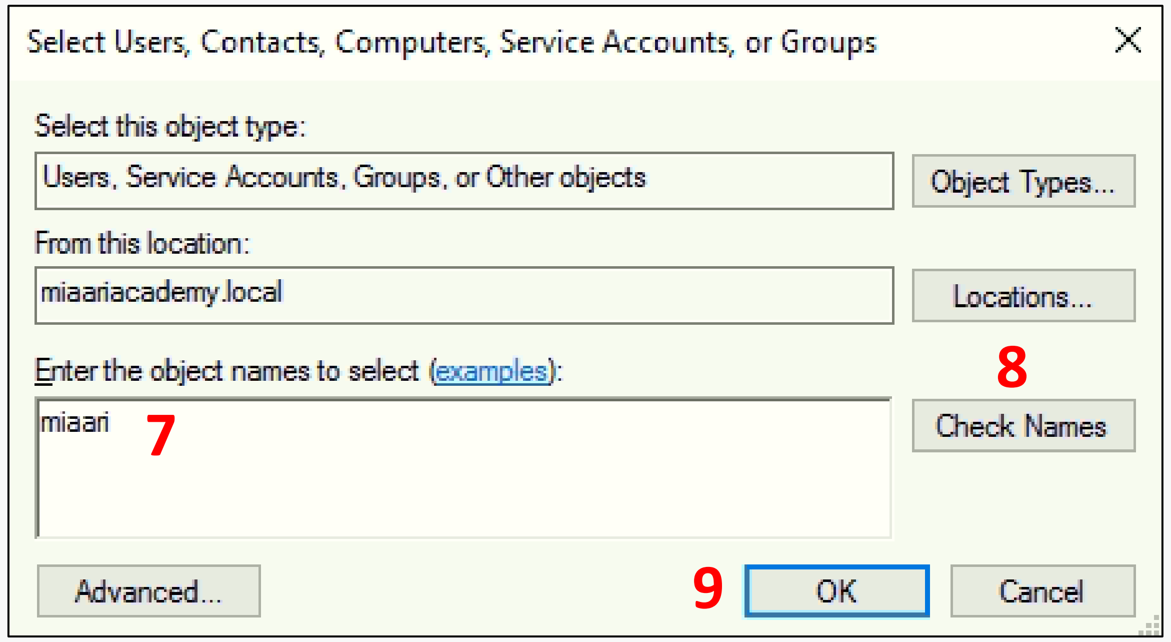
Adding Users miaari & zainab to Active Directory Group (ICT)

1. Expand the domain **miaariacademy.local**.
2. Select **ICT** Group under the respective Organizational Unit (OU).
3. Right-click on the **ICT** group
4. select **Properties**.
5. Go to the **Members** tab.
6. Click **Add** to add users into the group.
7. Type the desired username (Example: **miaari**).
8. Click **Check Names** to confirm the user exists.
9. Click **OK** to add the user to the group.



Name	Type	Description
ICT	Security Group...	
Mahmoud ...	User	
Zainab Magdy	User	




Select Users, Contacts, Computers, Service Accounts, or Groups
Object Types...
Locations...
8
Check Names
7
Advanced...
9
OK
Cancel

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
miaariacademy.local

Enter the object names to select (examples):
miaari

Adding Users miaari & zainab to Active Directory Group (ICT) Cont..

10. Click Add to add a new user.

11. In the Select Users window →

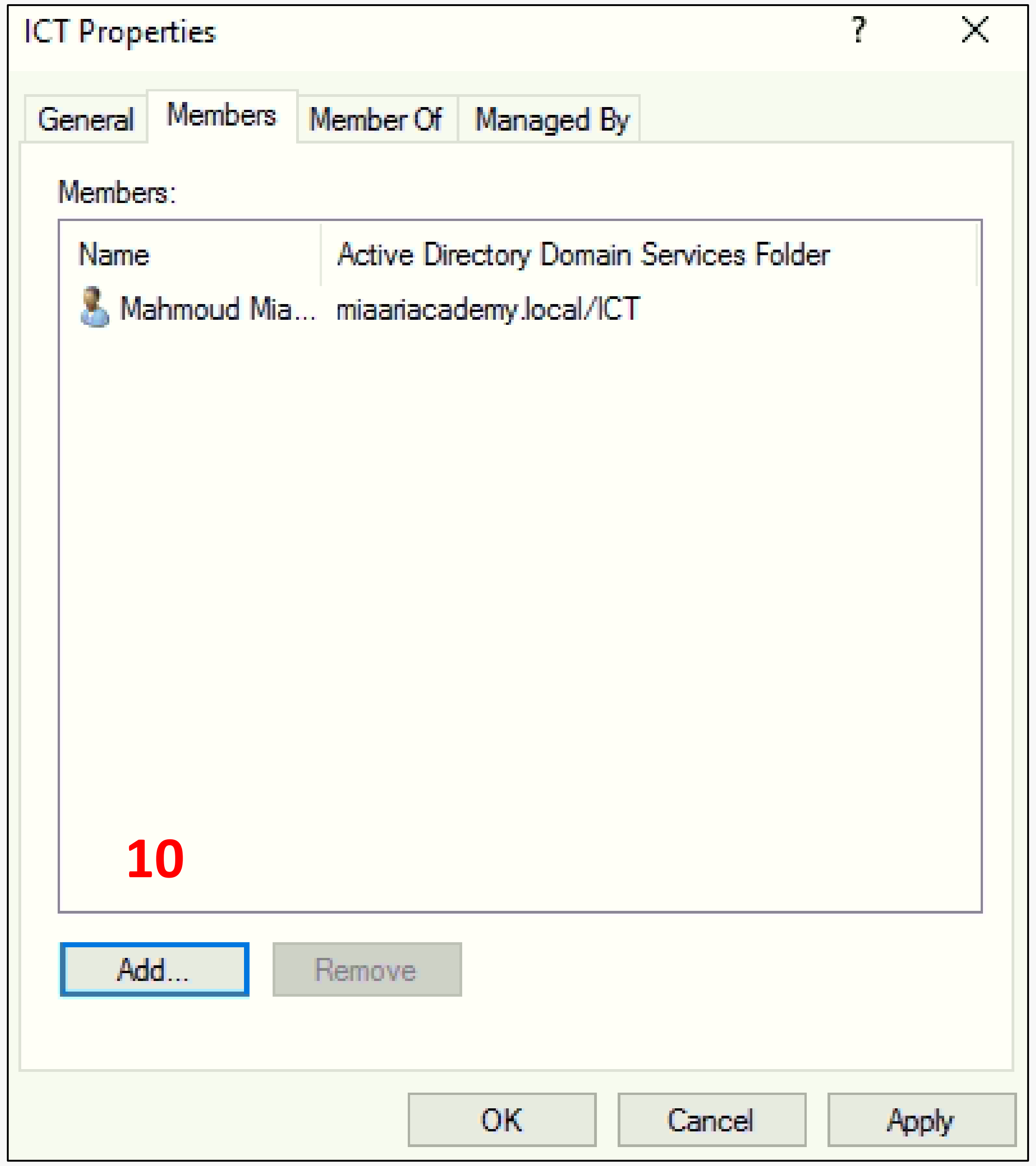
    Type zainab in the text box.

12. Click Check Names to verify the username.

13. Click OK to confirm adding the user.

14. Click Apply

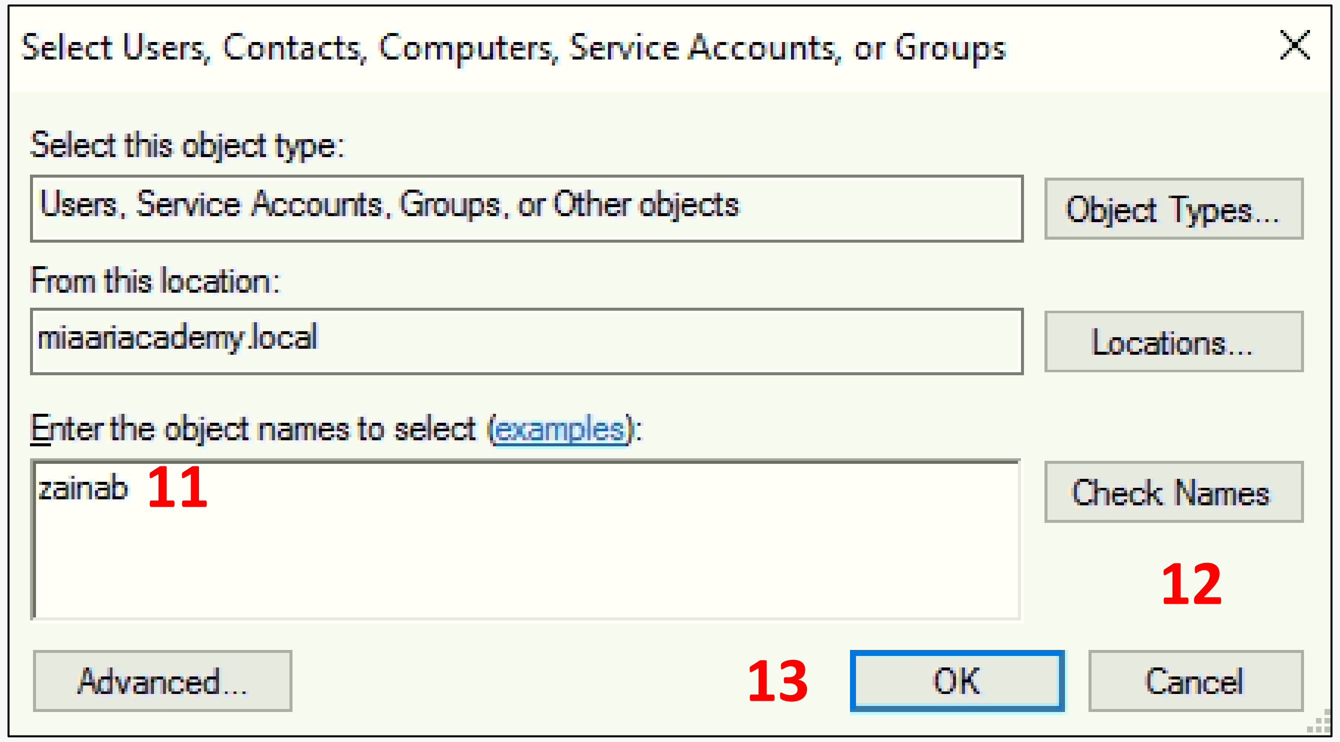
15. then OK to save the configuration.



ICT Properties

Members:

Name	Active Directory Domain Services Folder
Mahmoud Mia...	miaariacademy.local/ICT

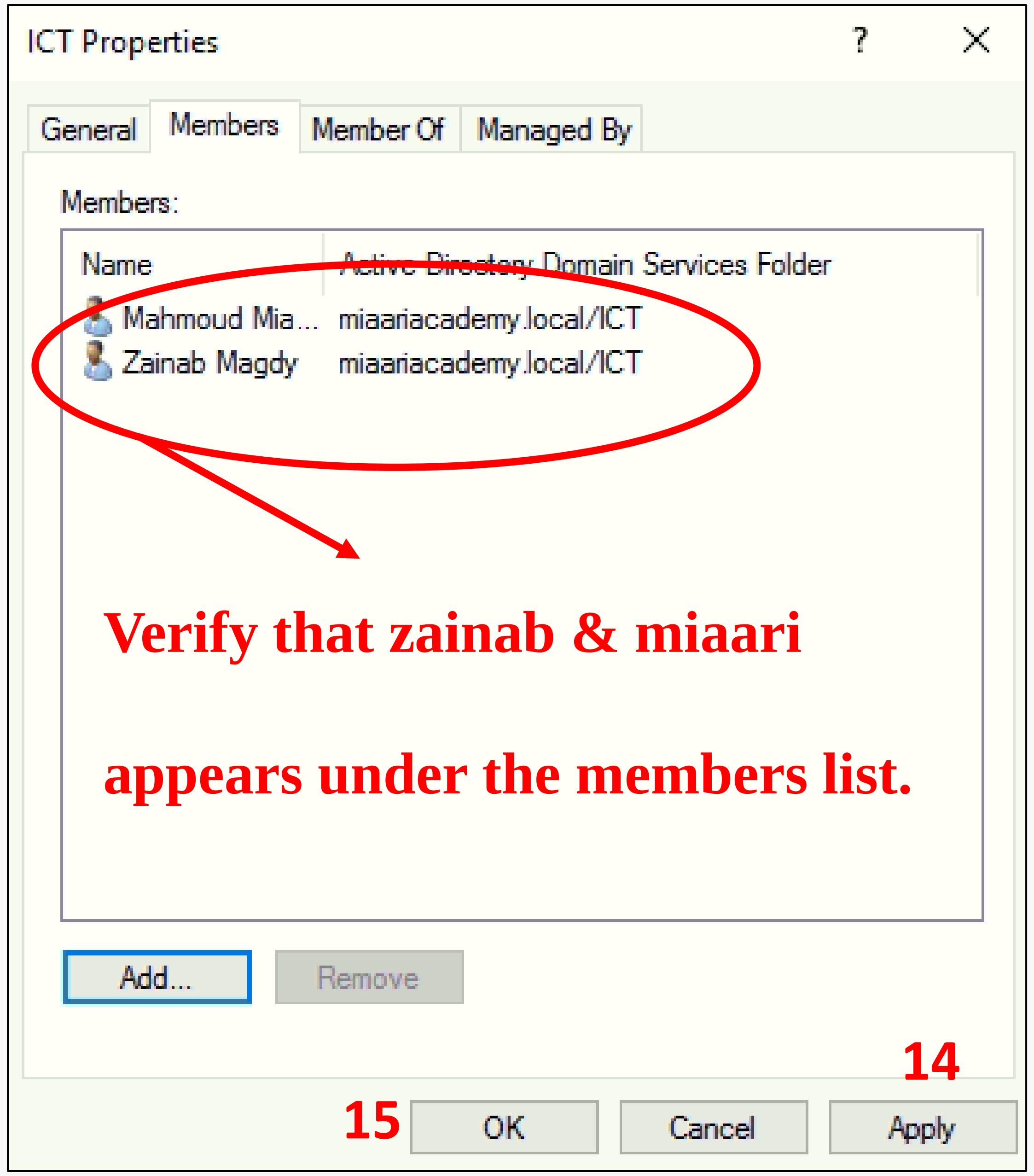


Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
miaariacademy.local

Enter the object names to select (examples):
zainab



ICT Properties

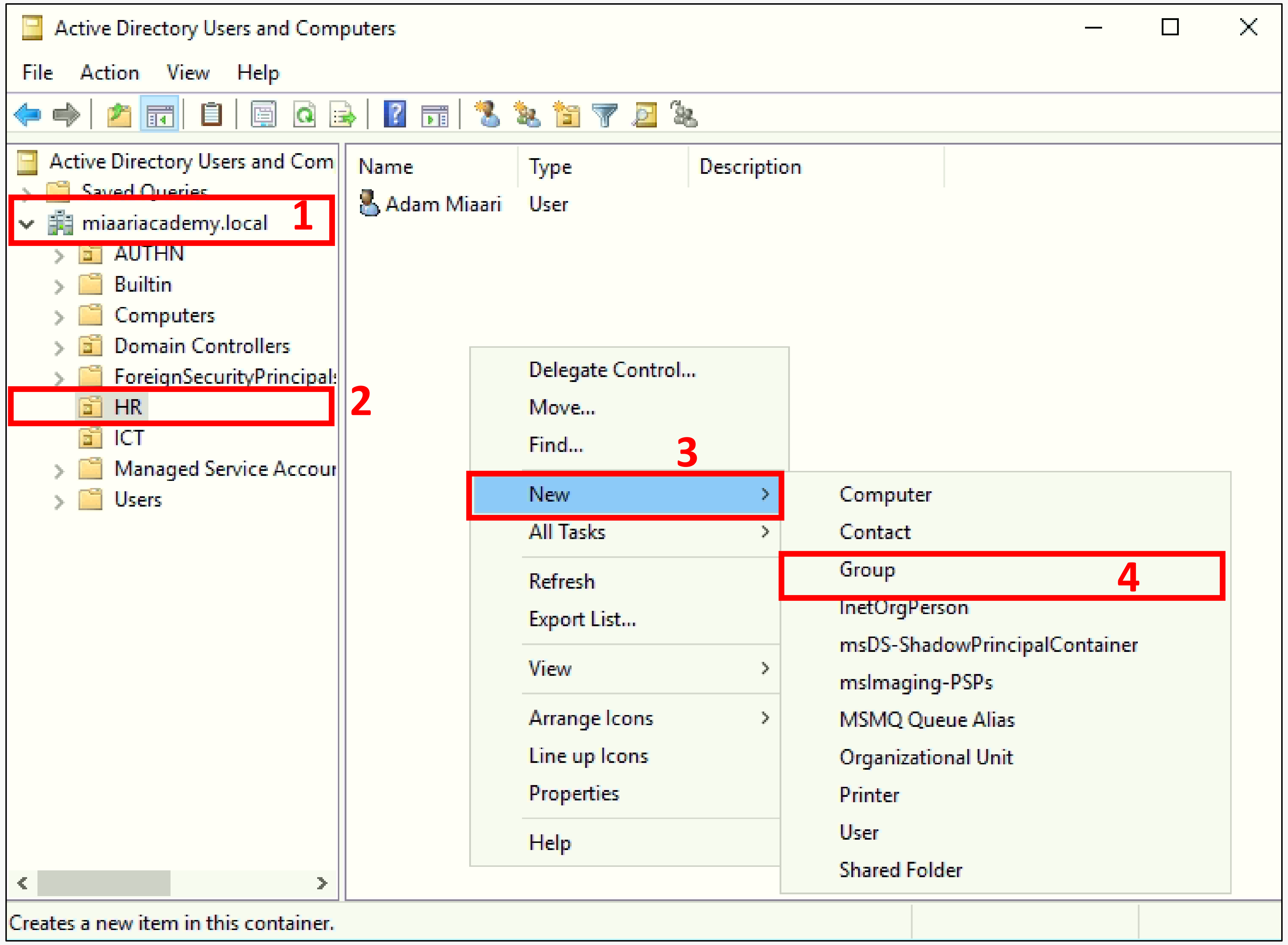
Members:

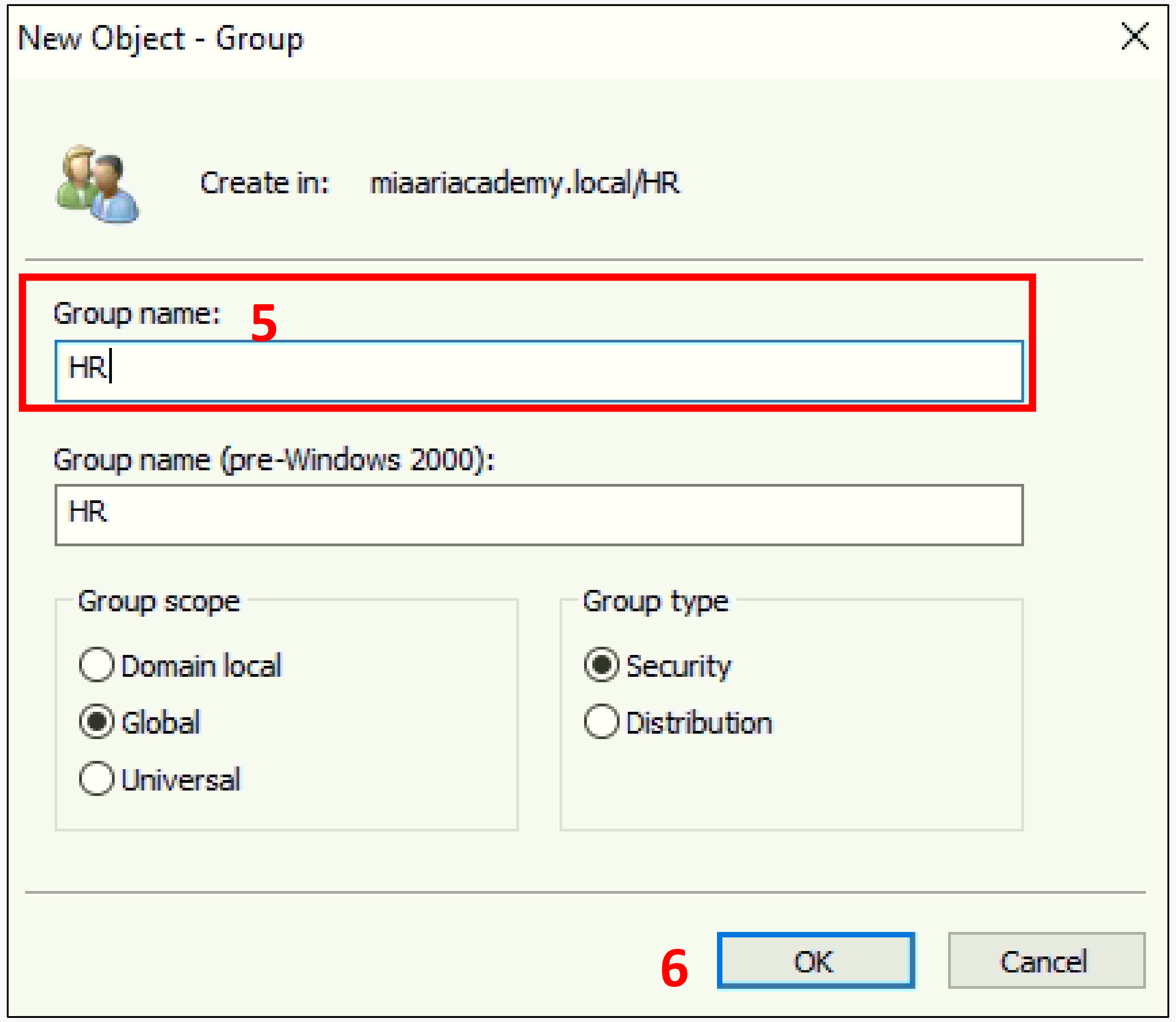
Name	Active Directory Domain Services Folder
Mahmoud Mia...	miaariacademy.local/ICT
Zainab Magdy	miaariacademy.local/ICT

Verify that zainab & miaari appears under the members list.

Creating a New Group HR in Active Directory for RADIUS Authentication

1. Expand the domain `miaariacademy.local`.
2. Right-click on the `HR` OU.
3. Navigate to `New`
4. Select `Group`.
5. Type the Group Name: `HR`.
6. Click `OK` to create the group.





New Object - Group

Create in: miaariacademy.local/HR

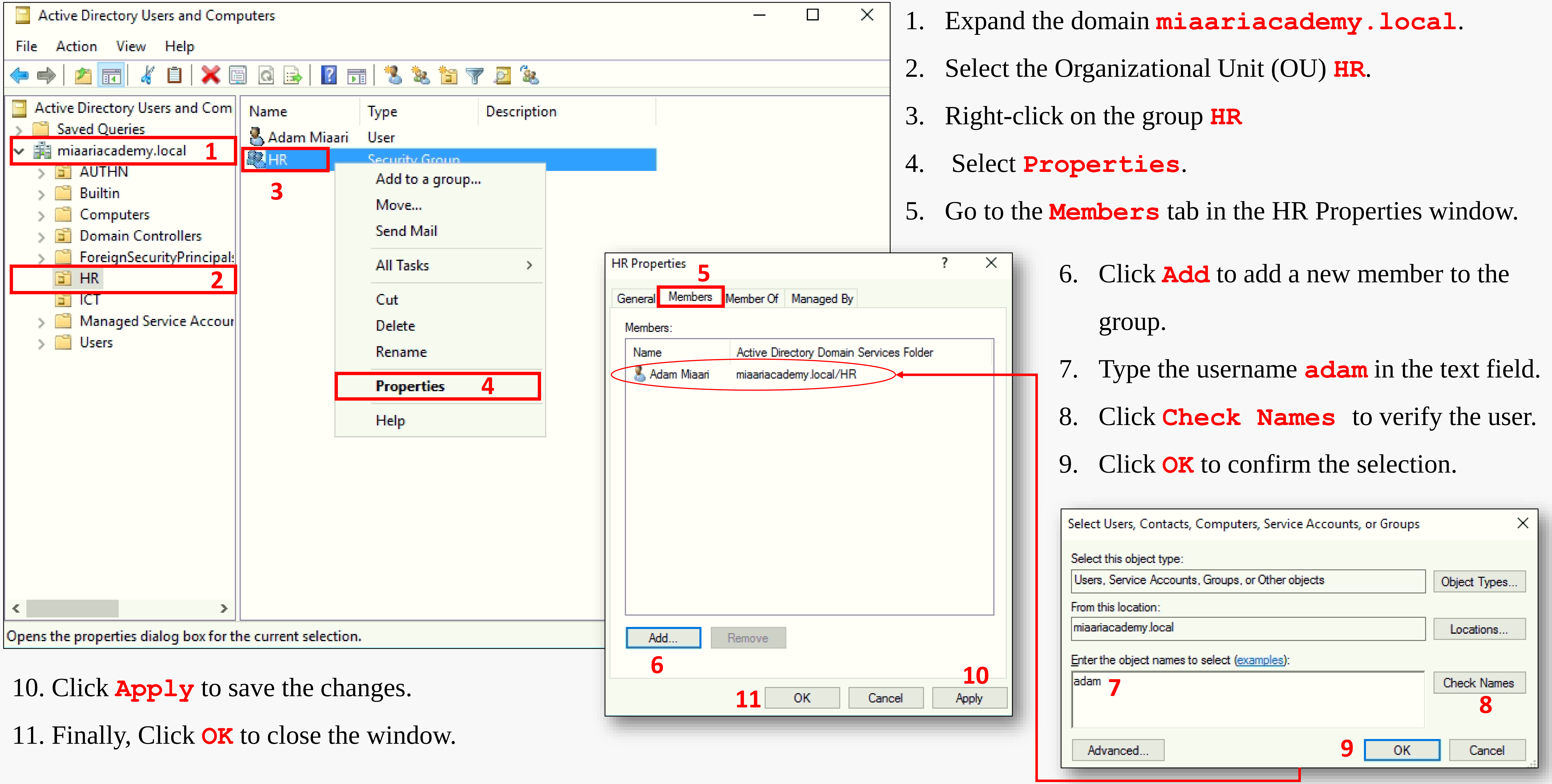
Group name: HR

Group name (pre-Windows 2000): HR

Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

Adding Users adam to Active Directory Group (ICT)



Members:

Name	Active Directory Domain Services Folder
Adam Miaari	miaariacademy.local/HR

Select this object type:
Users, Service Accounts, Groups, or Other objects

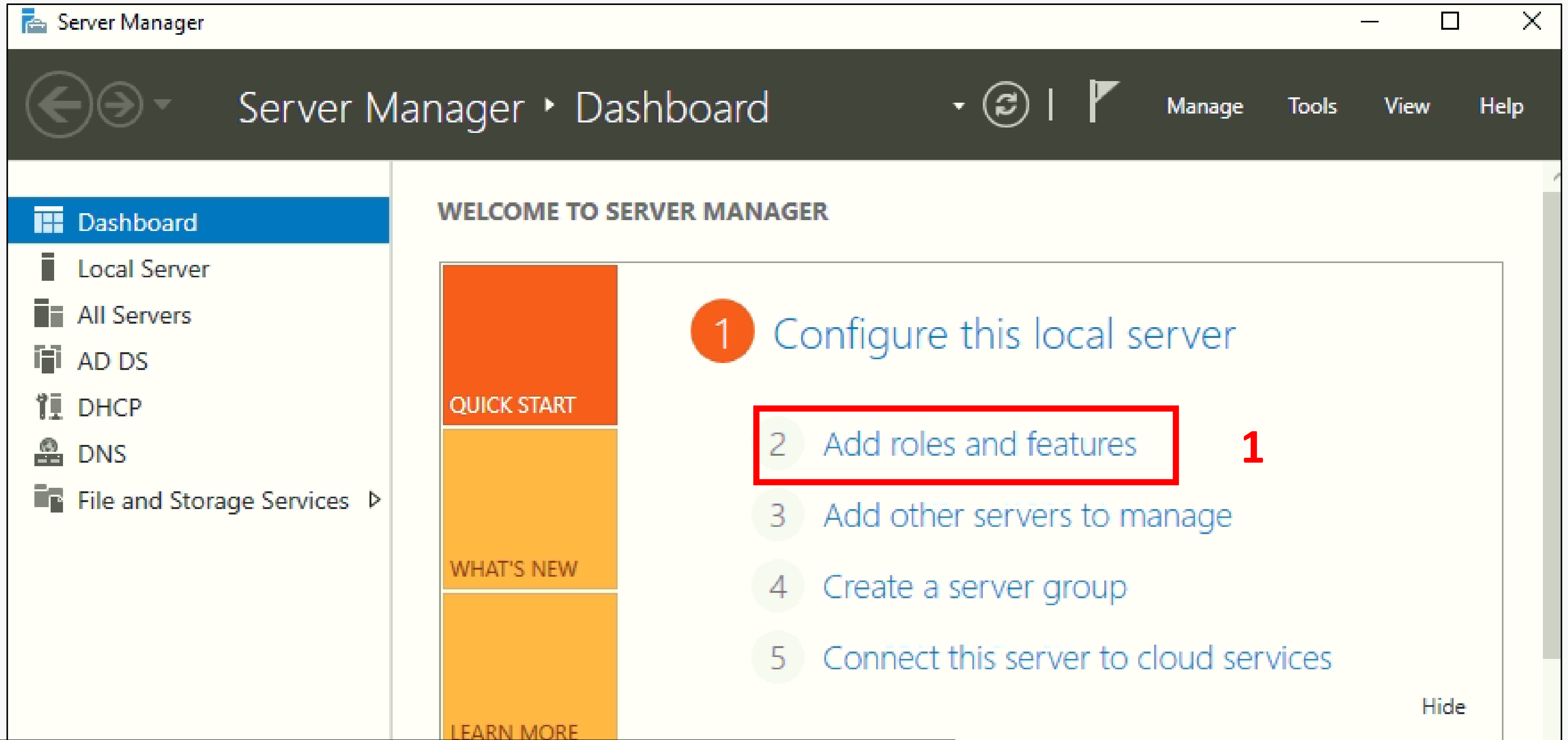
From this location:
miaariacademy.local

Enter the object names to select (examples):
adam

1. Expand the domain **miaariacademy.local**.
2. Select the Organizational Unit (OU) **HR**.
3. Right-click on the group **HR**
4. Select **Properties**.
5. Go to the **Members** tab in the HR Properties window.
6. Click **Add** to add a new member to the group.
7. Type the username **adam** in the text field.
8. Click **Check Names** to verify the user.
9. Click **OK** to confirm the selection.
10. Click **Apply** to save the changes.
11. Finally, Click **OK** to close the window.

Installing NPS Role on Windows Server

1. Open **Server Manager** → Click on **Add roles and features**.
2. Click **Next** on the "**Before you begin**" page.
3. Select **Role-based or feature-based installation** → Click **Next**.
4. Select the **destination server** from the server pool → Click **Next**.



WELCOME TO SERVER MANAGER

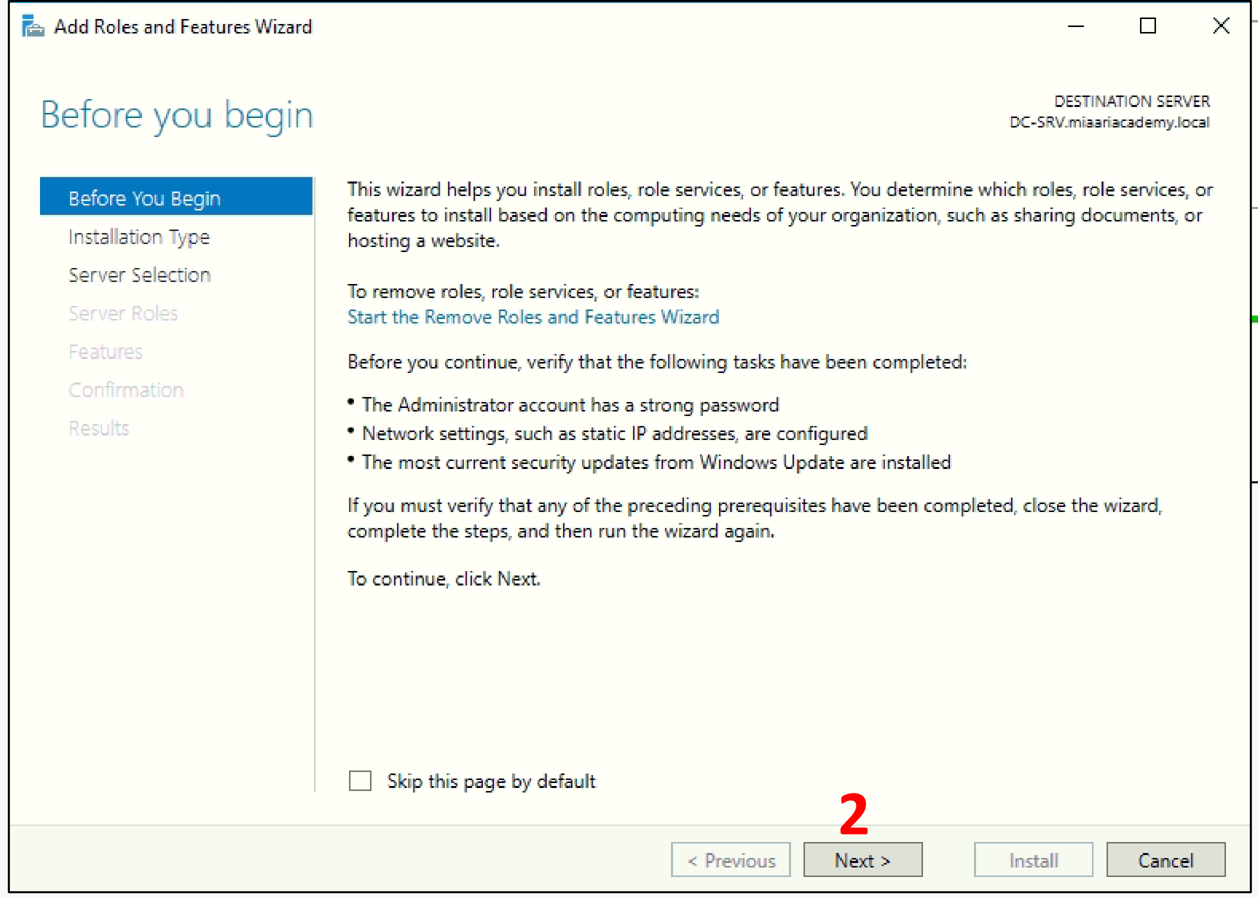
1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services



Before you begin

DESTINATION SERVER
DC-SRV.miaariacademy.local

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

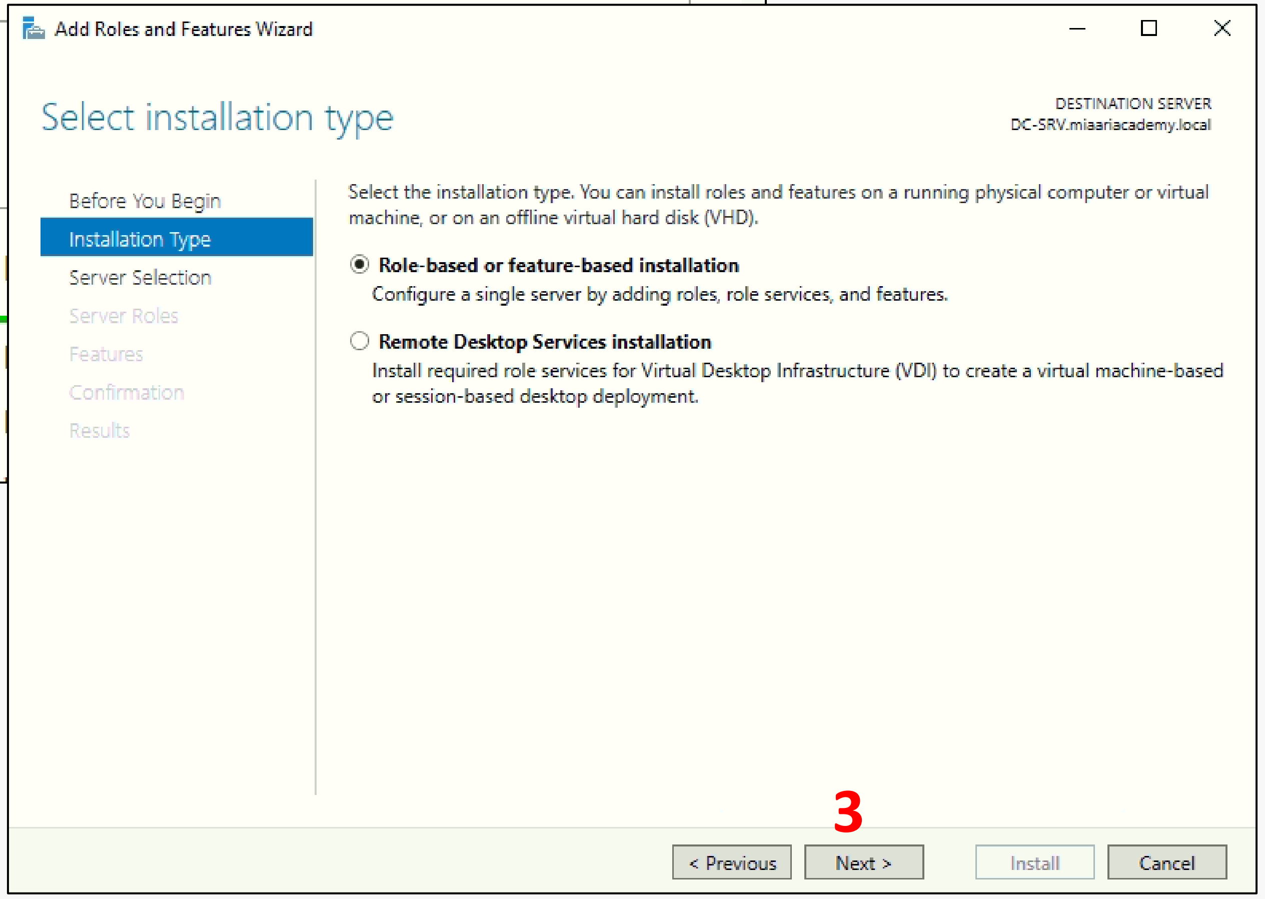
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default



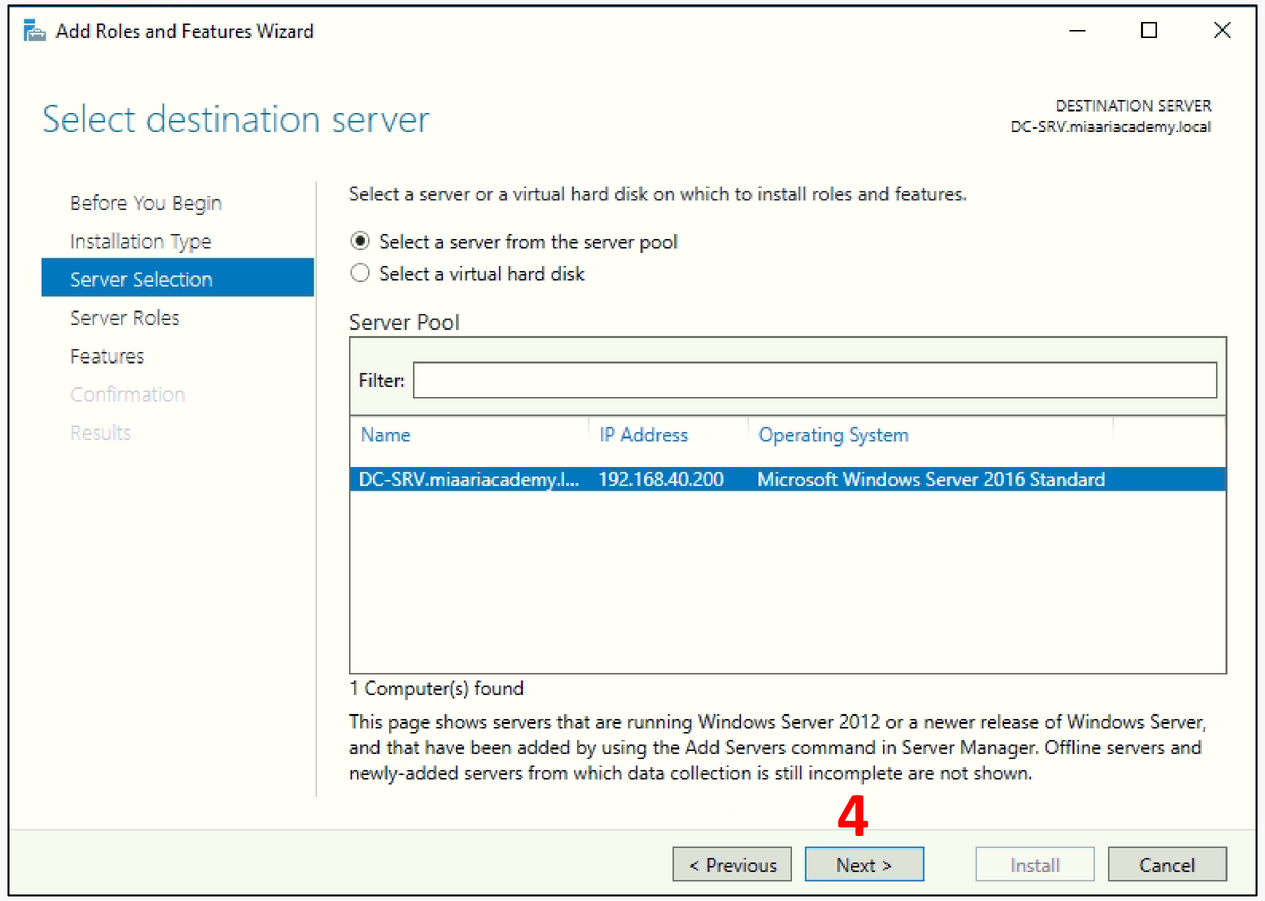
Select installation type

DESTINATION SERVER
DC-SRV.miaariacademy.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
DC-SRV.miaariacademy.local

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
DC-SRV.miaariacademy.l...	192.168.40.200	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Installing NPS Role on Windows Server Cont..

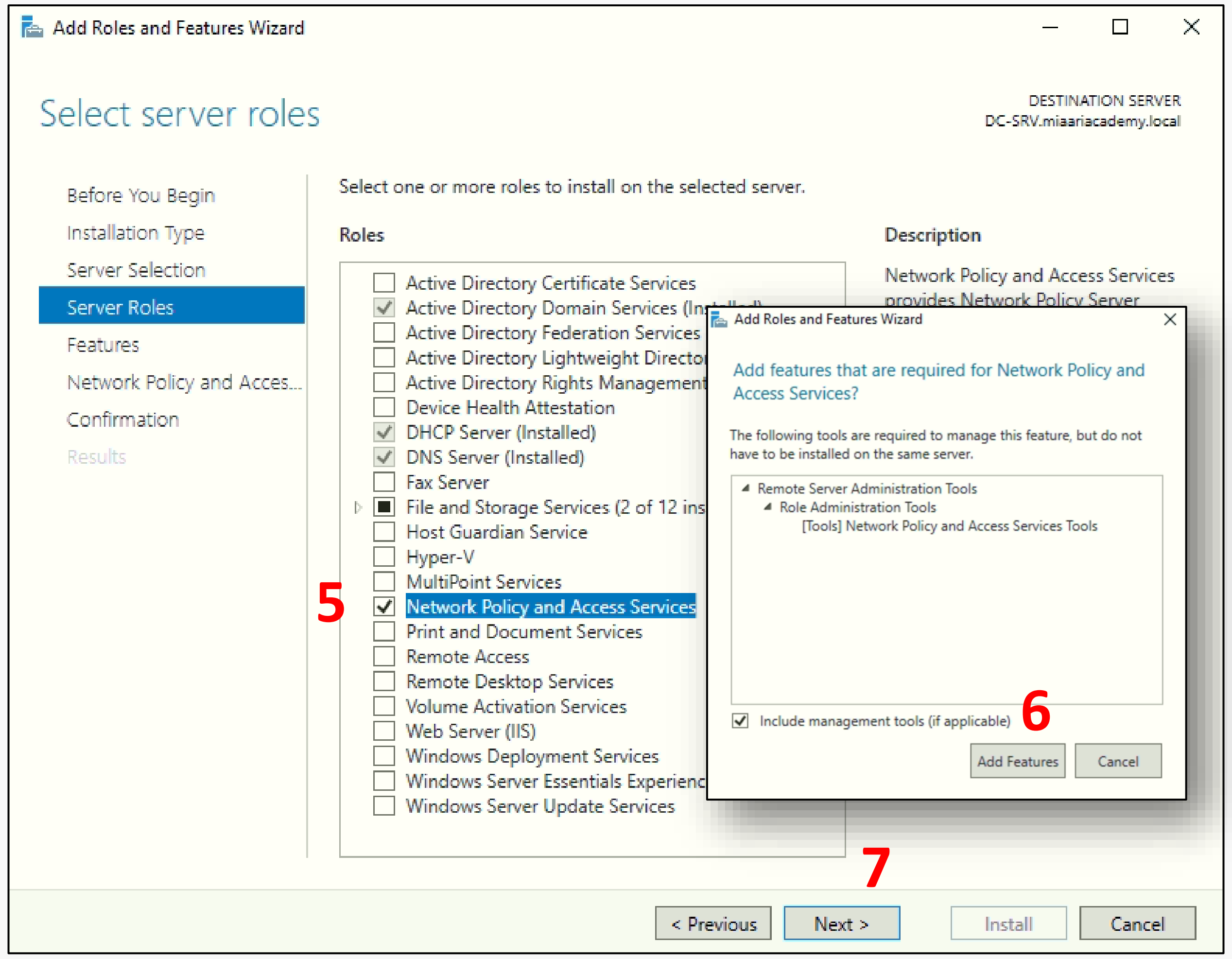
5. Select **Network Policy and Access Services** from the server roles.

6. Click **Add Features** when prompted to include required features.

7. Click **Next** to proceed.

8. Leave features selection as default → Click **Next**.

9. Read the NPS information summary → Click **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
DC-SRV.miaariacademy.local

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (In
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directo
- □ Active Directory Rights Management
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 ins
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- ☑ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experienc
- □ Windows Server Update Services

Description

Network Policy and Access Services provides Network Policy Server

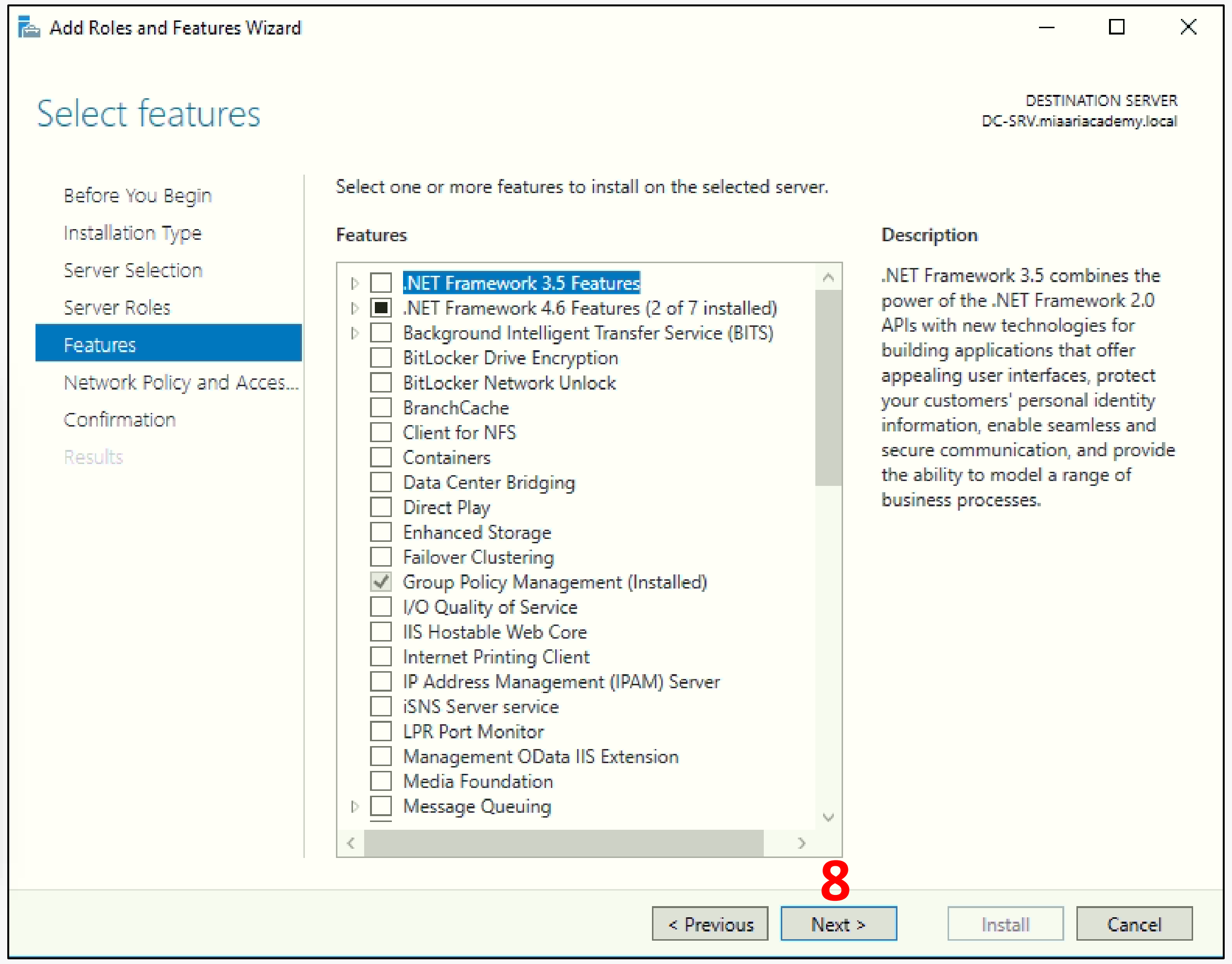
Add Roles and Features Wizard

Add features that are required for Network Policy and Access Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] Network Policy and Access Services Tools

☑ Include management tools (if applicable)



Add Roles and Features Wizard

Select features

DESTINATION SERVER
DC-SRV.miaariacademy.local

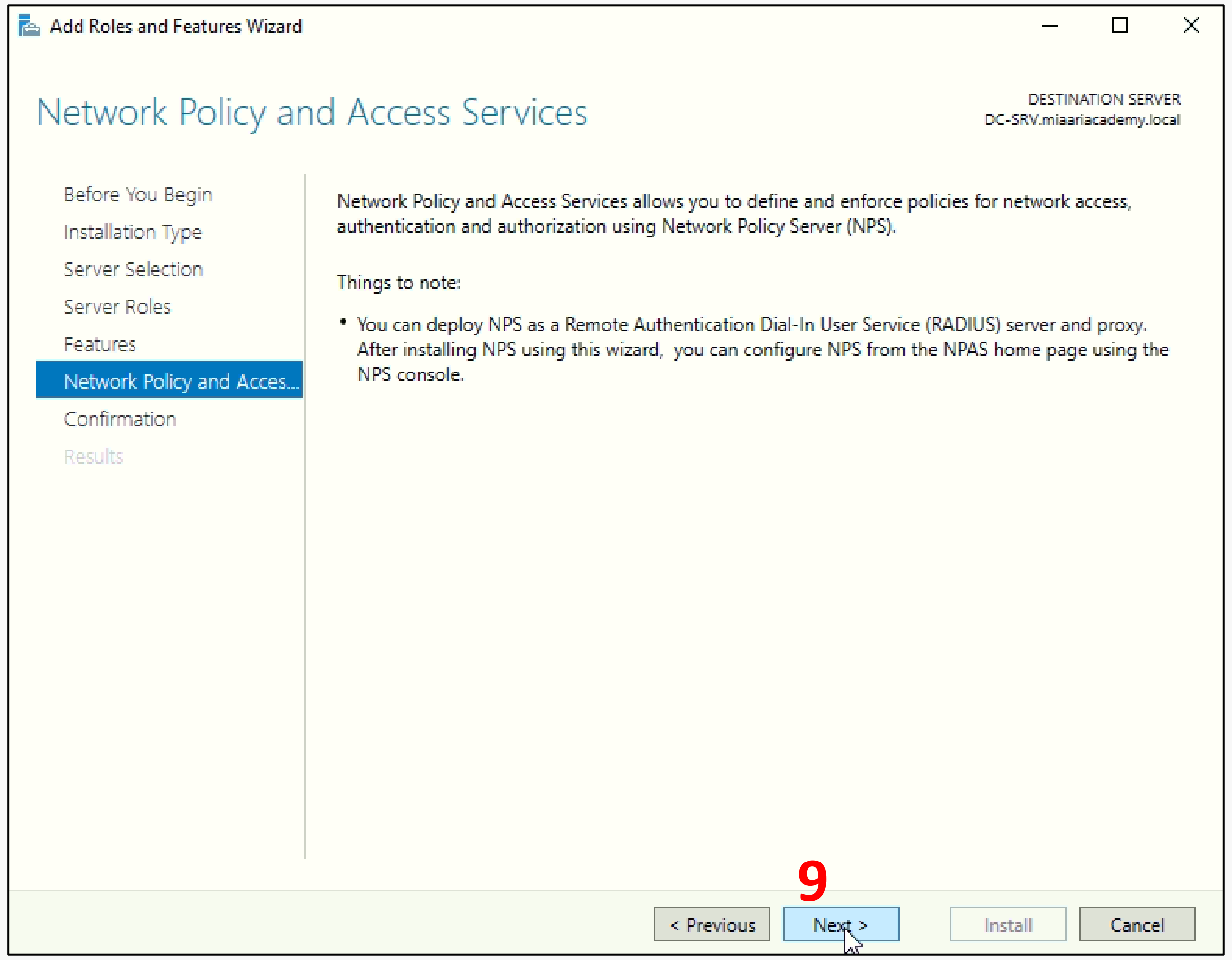
Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor
- □ Management OData IIS Extension
- □ Media Foundation
- □ Message Queuing

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.



Add Roles and Features Wizard

Network Policy and Access Services

DESTINATION SERVER
DC-SRV.miaariacademy.local

Network Policy and Access Services allows you to define and enforce policies for network access, authentication and authorization using Network Policy Server (NPS).

Things to note:

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.

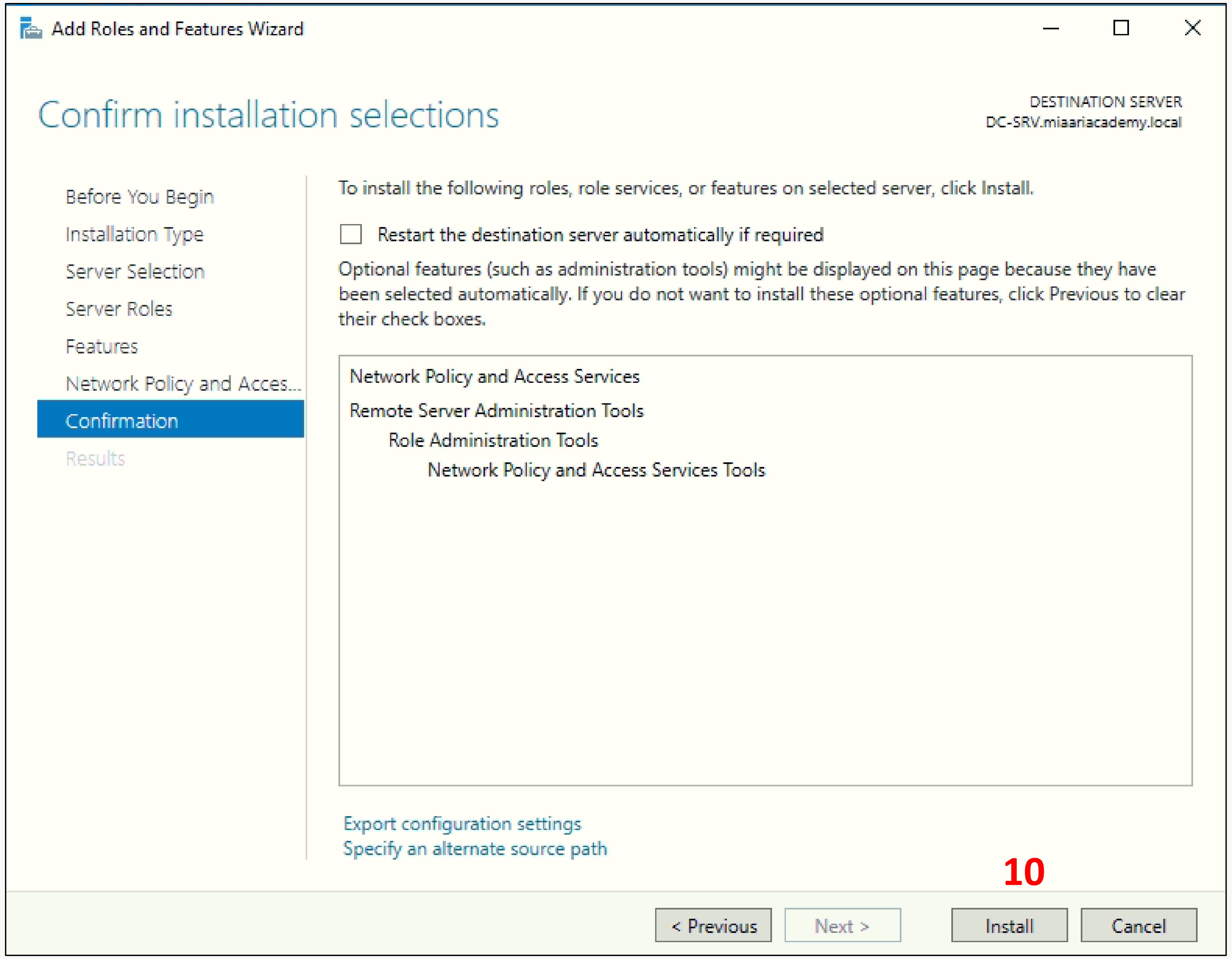
Installing NPS Role on Windows Server Cont..

10. Review the selected roles and features for installation.

    Click **Install** to start the installation process.

11. Wait until the installation progress reaches 100% and displays **Installation succeeded**.

    Click **Close** to finish the wizard.



Confirm installation selections

DESTINATION SERVER
DC-SRV.miaariacademy.local

To install the following roles, role services, or features on selected server, click Install.

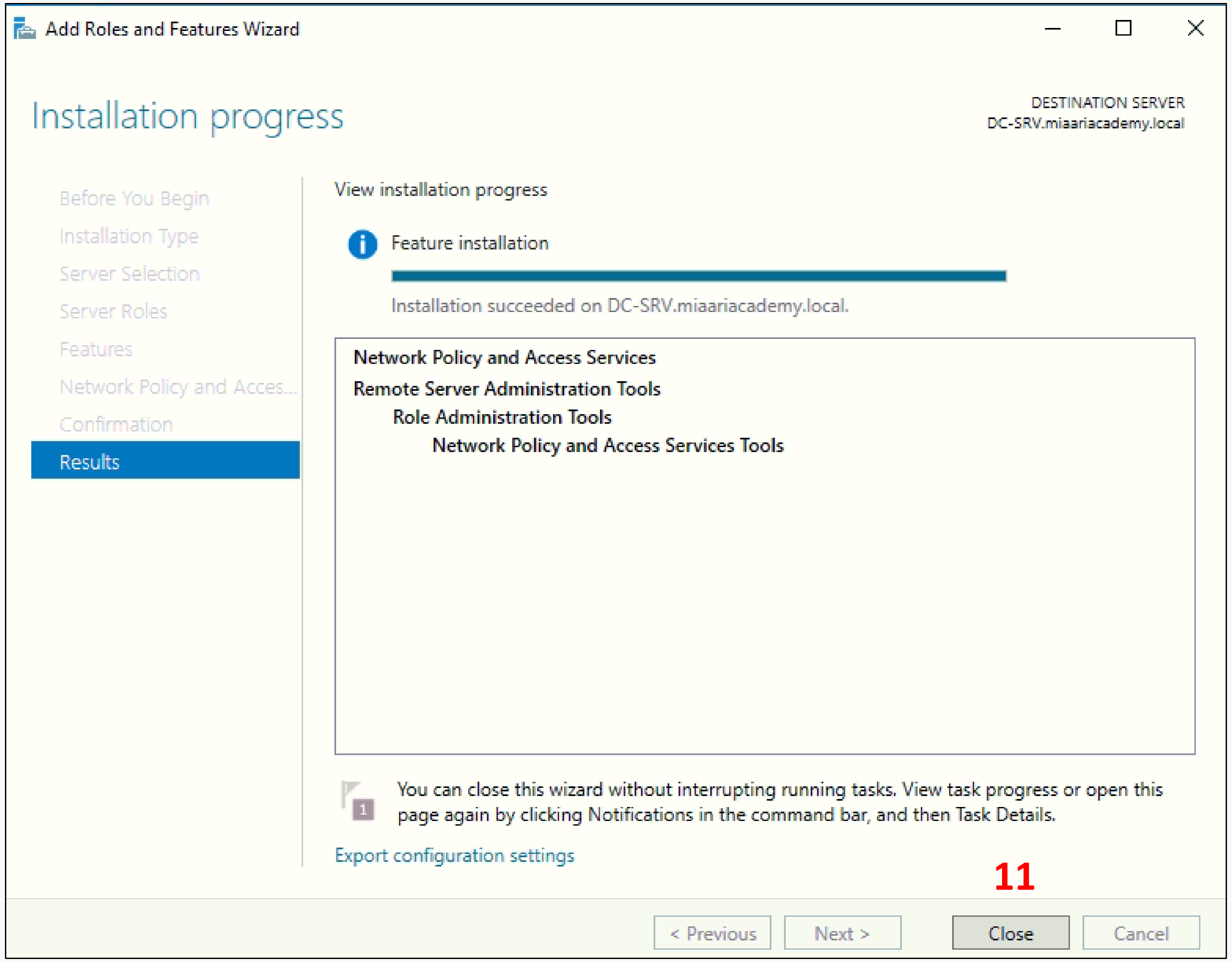
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Network Policy and Access Services
Remote Server Administration Tools
    Role Administration Tools
        Network Policy and Access Services Tools

Export configuration settings
Specify an alternate source path

10



Installation progress

DESTINATION SERVER
DC-SRV.miaariacademy.local

View installation progress

Feature installation

Installation succeeded on DC-SRV.miaariacademy.local.

Network Policy and Access Services
Remote Server Administration Tools
    Role Administration Tools
        Network Policy and Access Services Tools

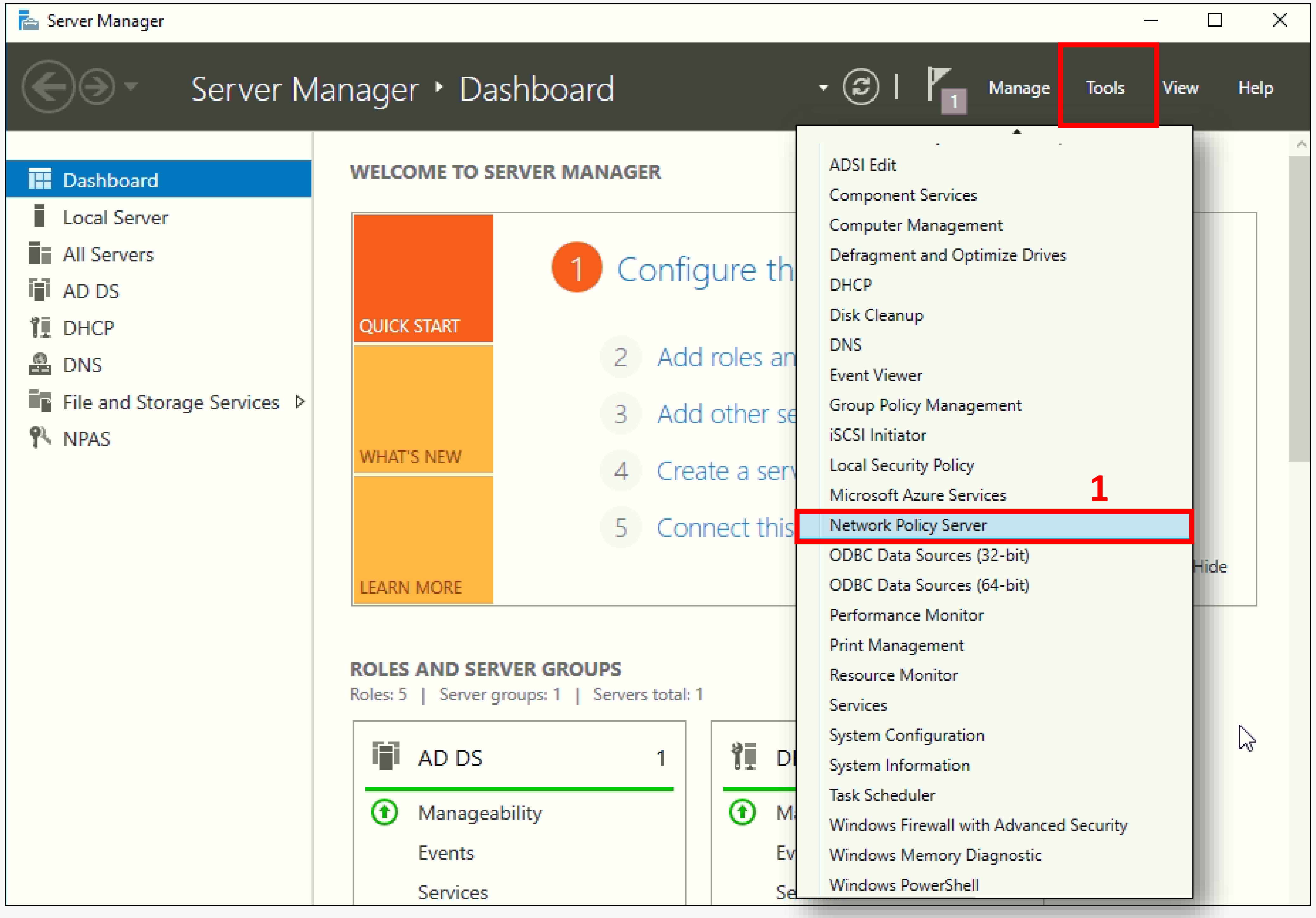
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

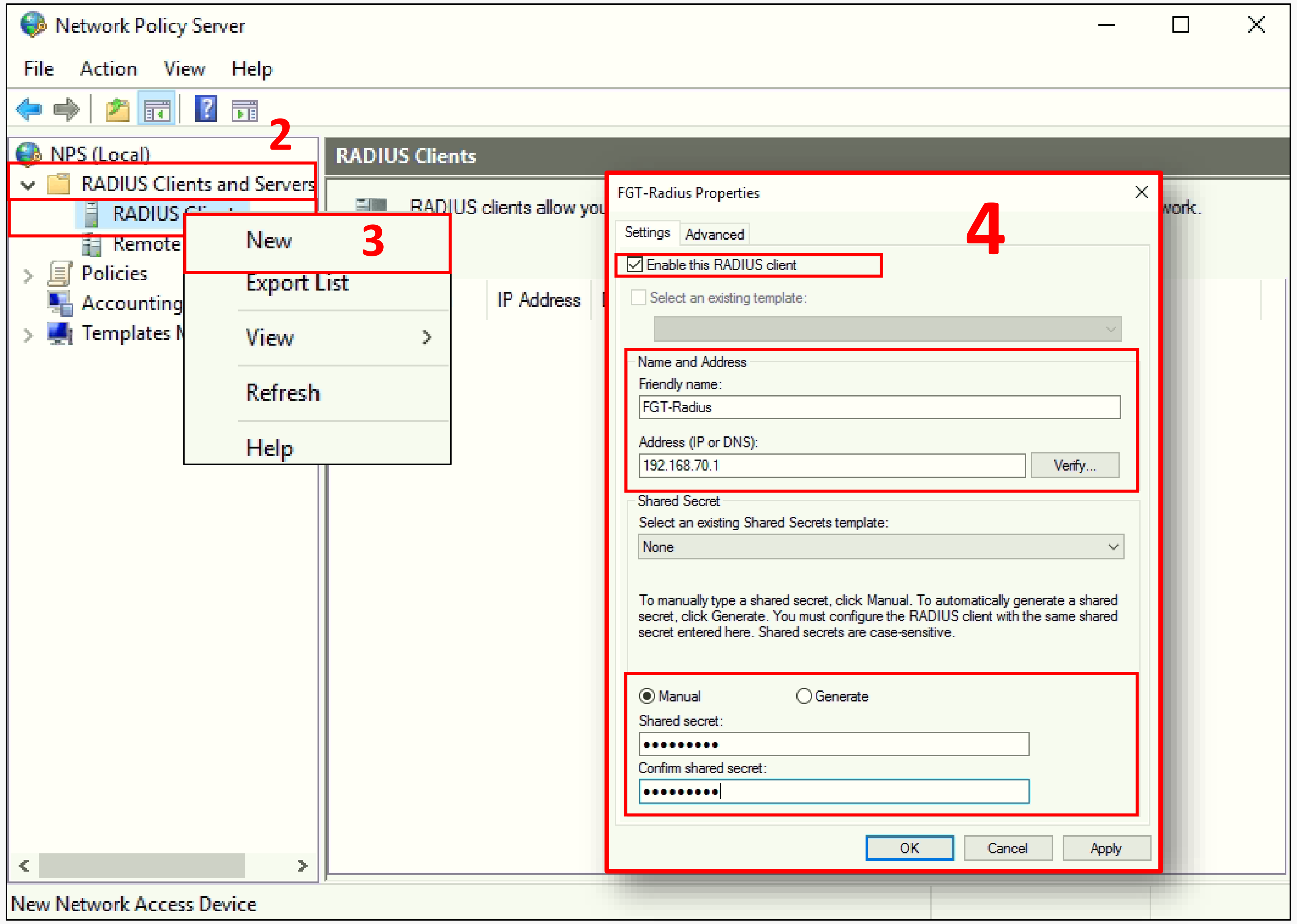
11

Configuring RADIUS Client in Network Policy Server (NPS)

1. From the **Server Manager** Dashboard, click on **Tools** and Select **Network Policy Server** from the dropdown menu.
2. In the **NPS** console, expand **RADIUS Clients and Servers**.
3. Right-click on **RADIUS Clients** and select **New**.



4. In the **New RADIUS Client** window:
   - Enable **RADIUS Client**.
   - Enter Friendly Name (e.g., **FGT-Radius**).
   - Enter the **IP Address 192.168.70.1** of the FortiGate device.
   - Enter and confirm the **Shared Secret admin@123** .
   - Click **Apply** then **OK** to save the RADIUS client configuration.



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: FGT-Radius

Address (IP or DNS): 192.168.70.1

Shared Secret

Select an existing Shared Secrets template: None

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.

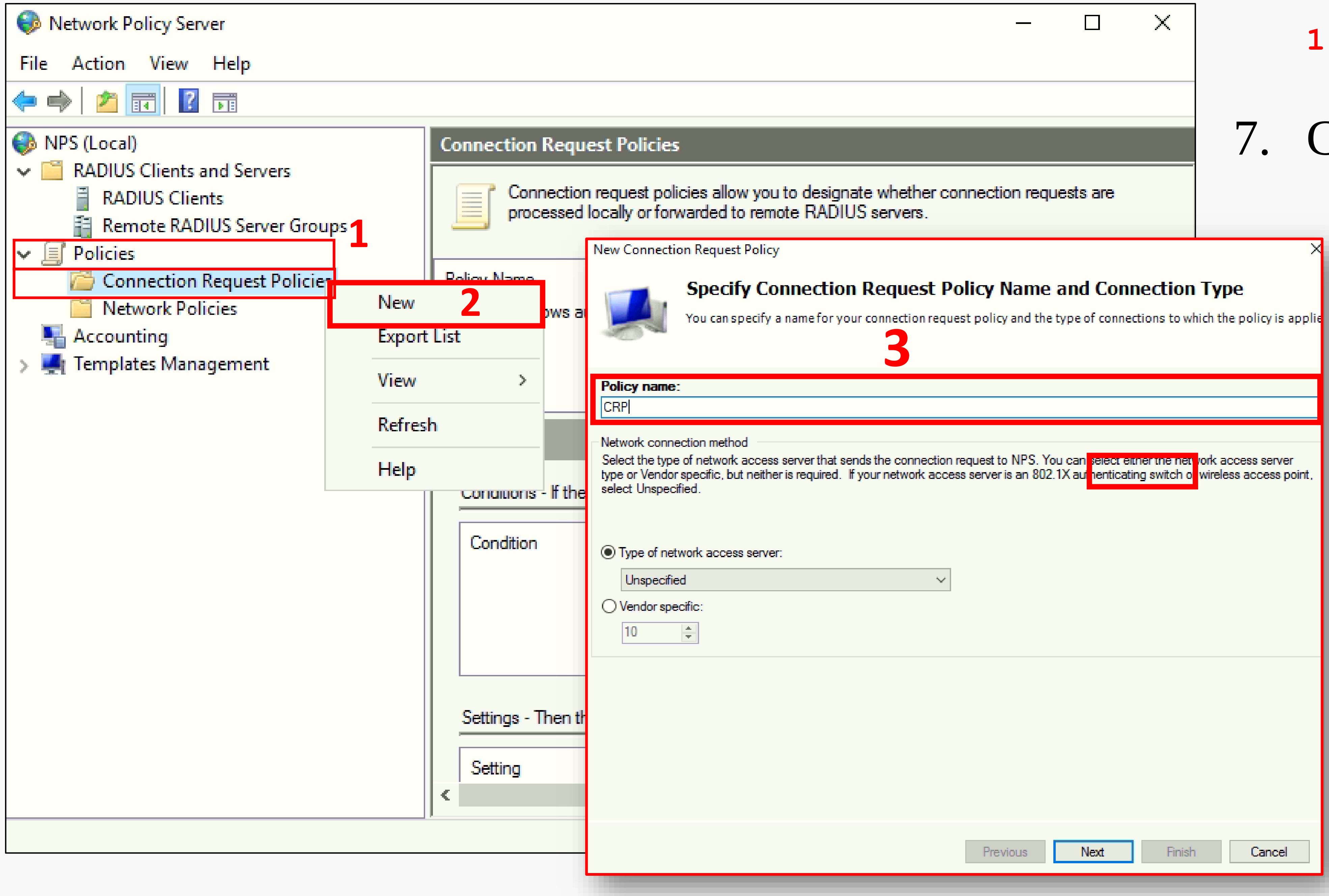
● Manual ○ Generate

Shared secret: •••••••••

Confirm shared secret: •••••••••

Creating Connection Request Policy CRP in NPS for RADIUS Client

1. In the NPS console, expand `Policies`.
2. Right-click on `Connection Request Policy` and select `New`.
3. Enter a `Policy Name` (e.g., `CRP`) and click `Next`.
4. In the `Specify Conditions` section, click `Add`.
5. Select `Access Client IPv4 Address` and click `Add`.
6. Enter the `IP Address` of the FortiGate device (e.g., `192.168.70.1`) and click `OK`.
7. Click `Next` to continue and complete the configuration.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applie

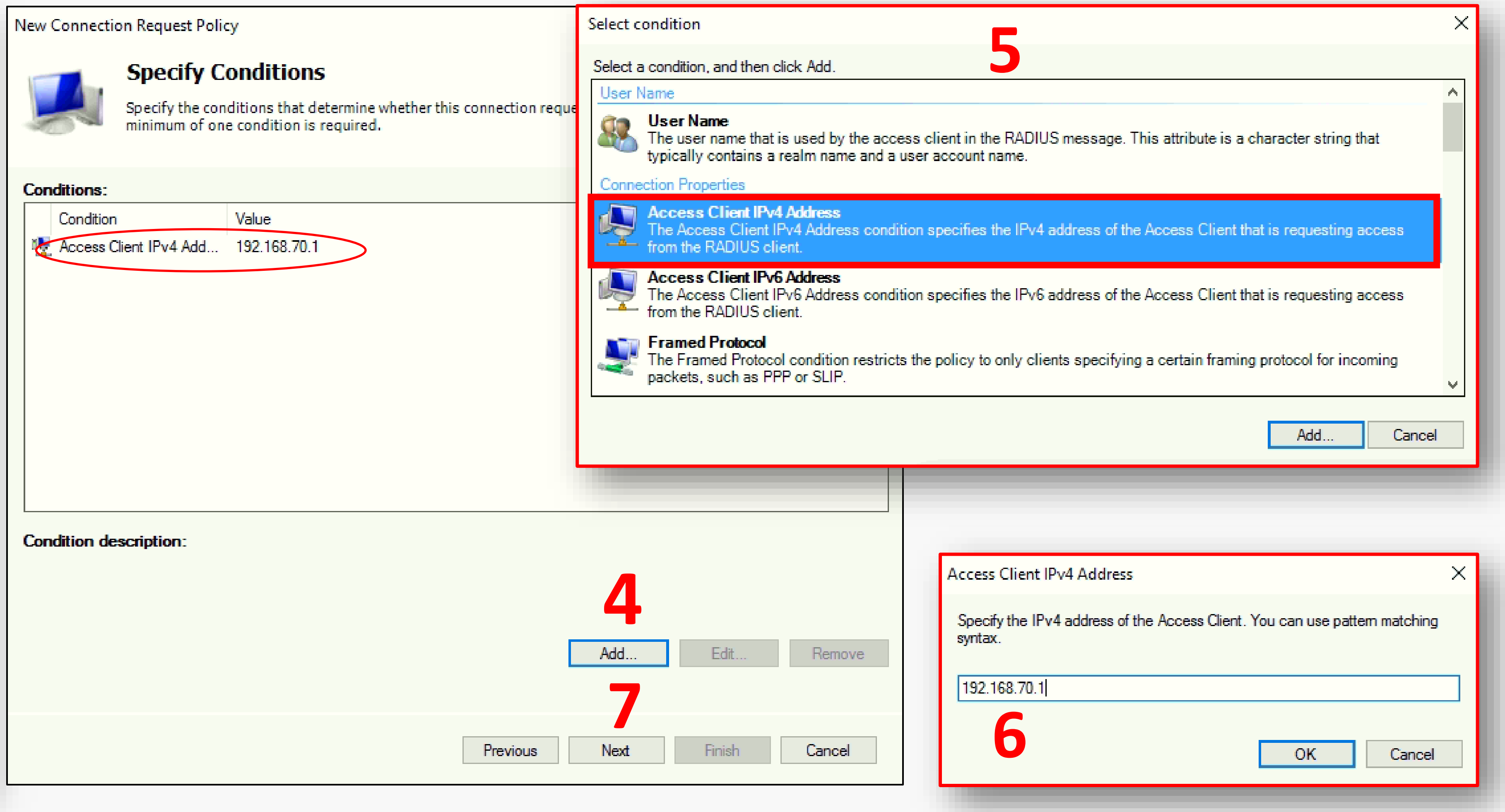
Policy name: CRP

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



New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection reque minimum of one condition is required.

Conditions:

Condition	Value
Access Client IPv4 Add...	192.168.70.1

Condition description:

Select condition

Select a condition, and then click Add.

User Name

User Name
The user name that is used by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name.

Connection Properties

Access Client IPv4 Address
The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.

Access Client IPv6 Address
The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.

Framed Protocol
The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.

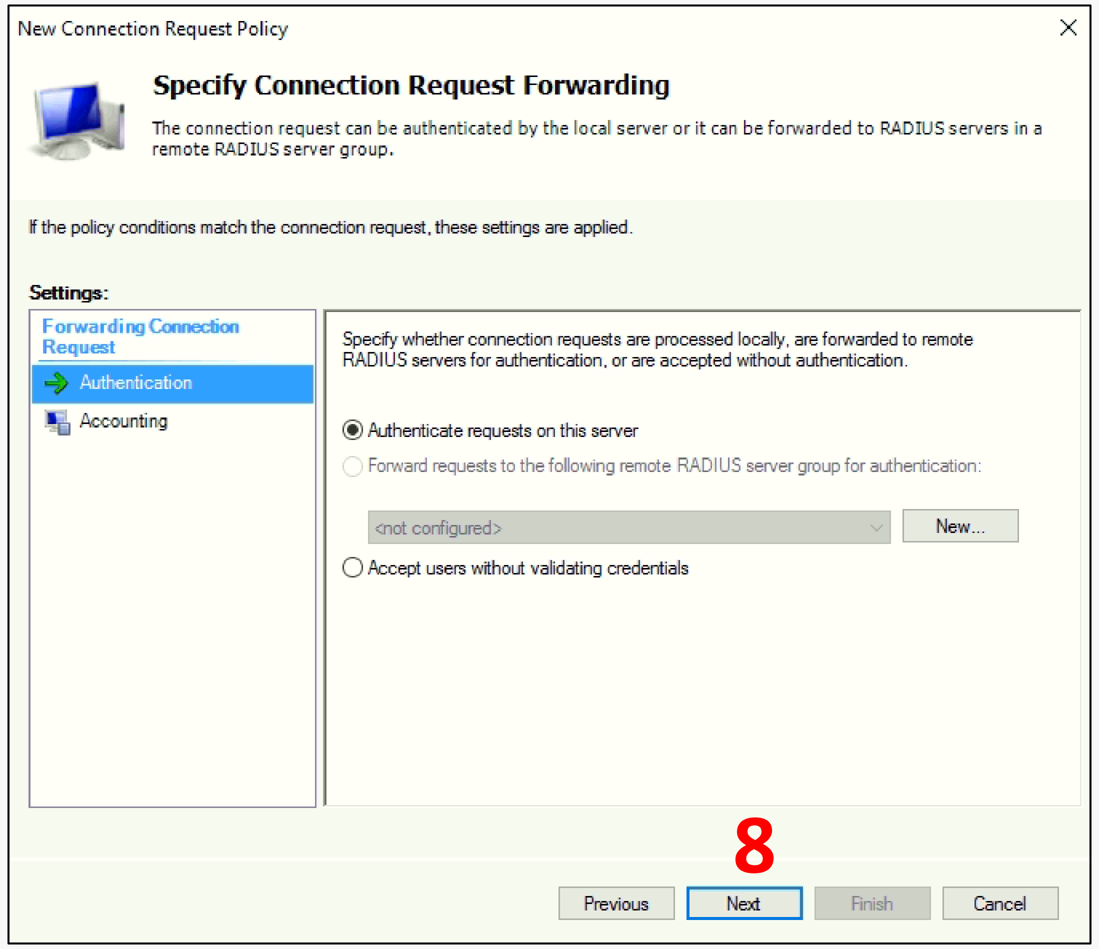
Access Client IPv4 Address

Specify the IPv4 address of the Access Client. You can use pattern matching syntax.

192.168.70.1

Creating Connection Request Policy CRP in NPS for RADIUS Client Cont..

1. In **Specify Connection Request Forwarding** window, select **Authenticate requests on this server** and click **Next**.
2. In **Specify Authentication Methods** window, leave the default settings and click **Next**.
3. In **Configure Settings** window, keep the default settings and click **Next**.
4. In **Completing Connection Request Policy Wizard** window, review your configuration and click **Finish** to save the policy.



New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

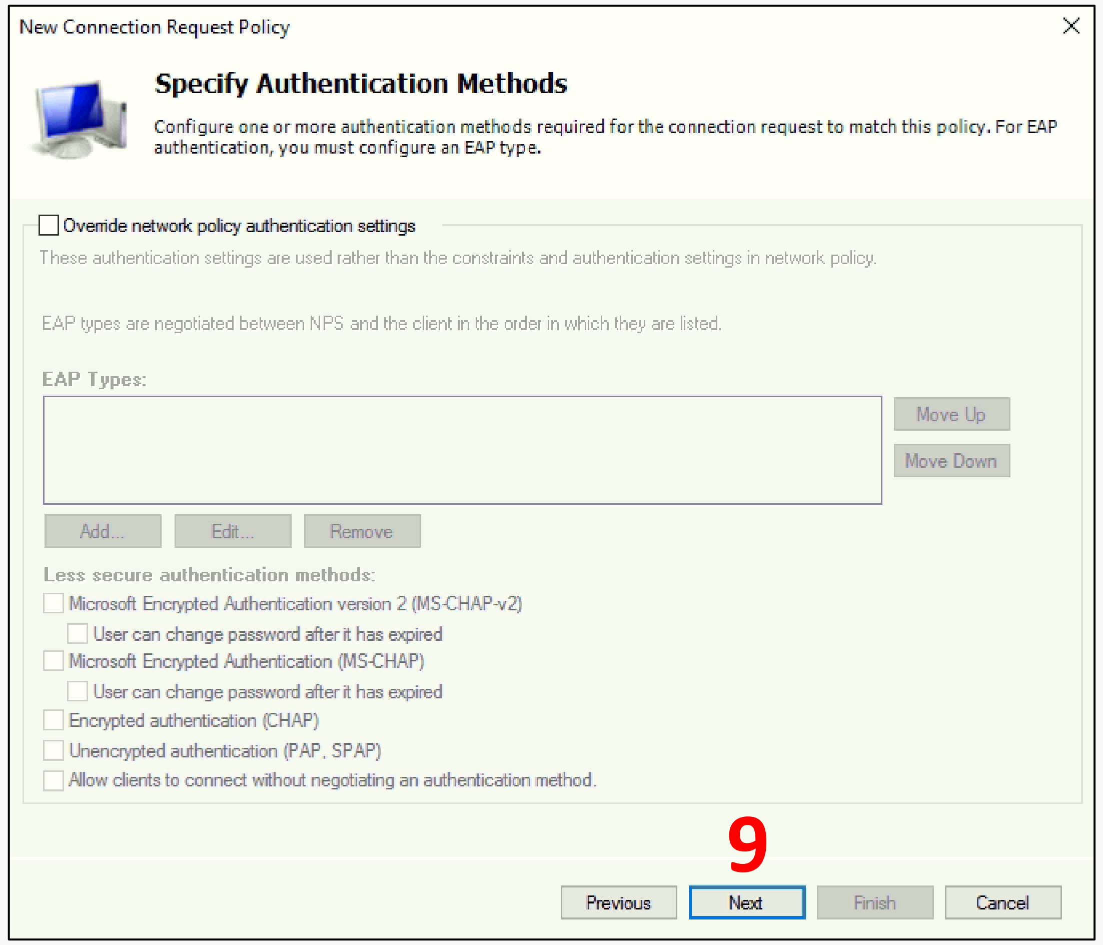
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials



New Connection Request Policy

Specify 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.

□ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy.

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

EAP Types:

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

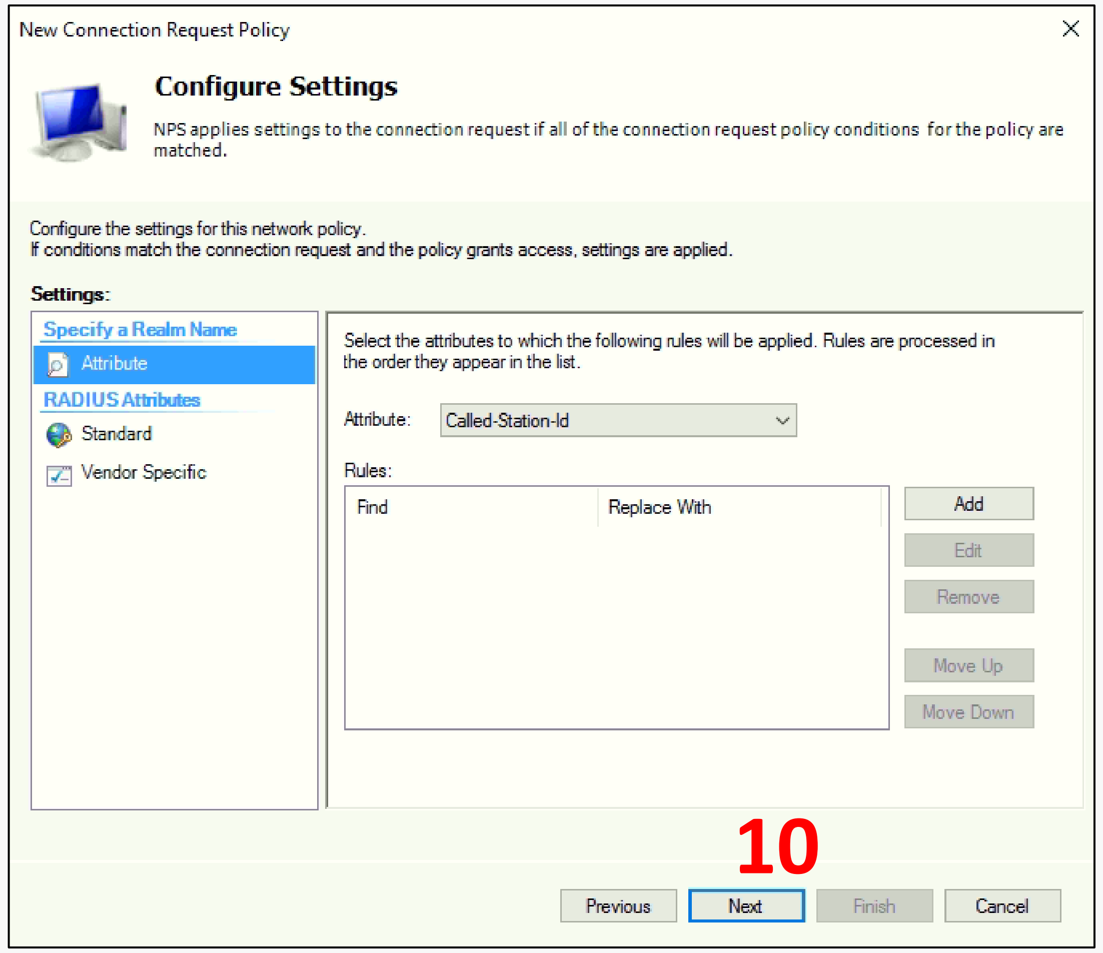
□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.



New Connection Request Policy

Configure Settings

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

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

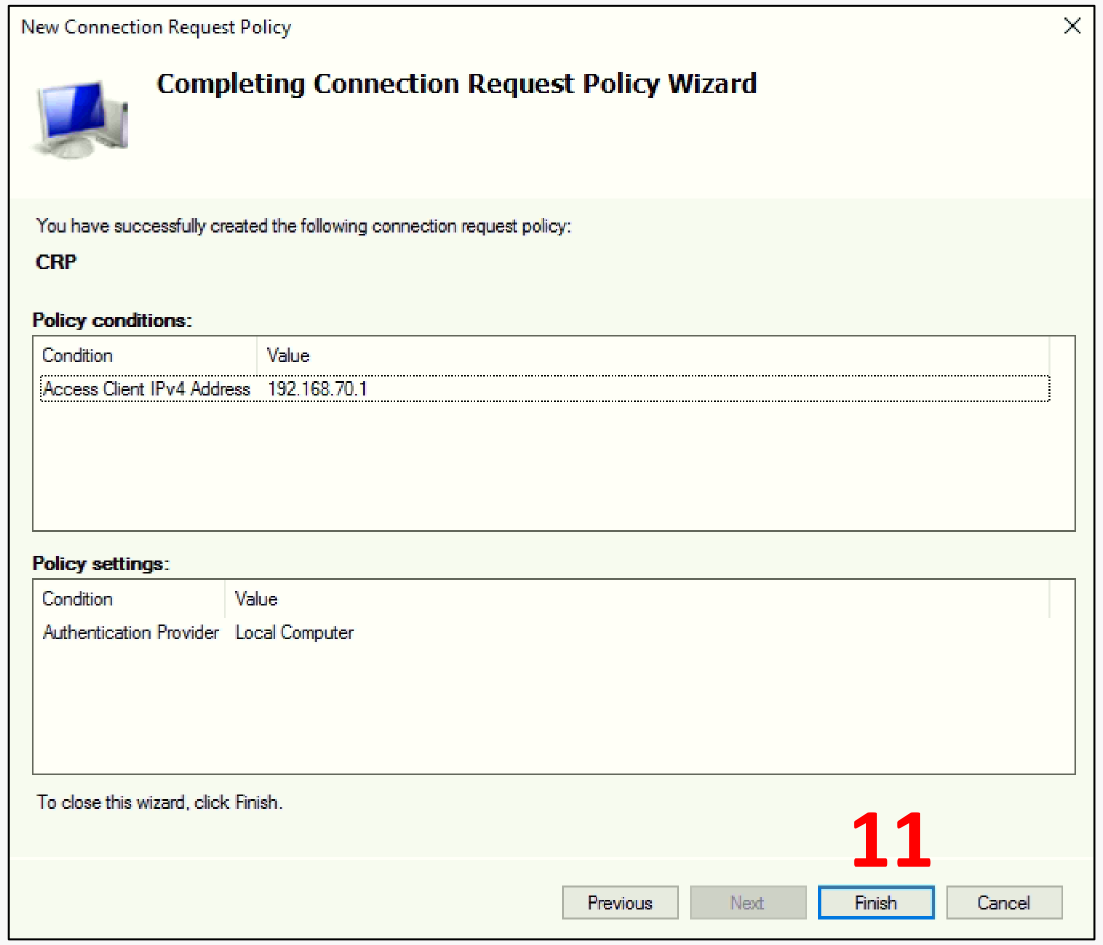
Settings:

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: Called-Station-Id

Rules:

Find	Replace With



New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

CRP

Policy conditions:

Condition	Value
Access Client IPv4 Address	192.168.70.1

Policy settings:

Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

Creating Network Policy (NPS) for Active Directory Groups (ICT & HR)

1. Navigate to **Network Policy Server (NPS)** → Expand **Policies** → Right-click **Network Policies** → Select **New**.

2. In **Specify Network Policy Name and Connection Type** window:
   - Enter Policy Name (e.g., **RADIUS-ICT-HR**).
   - Click **Next**.

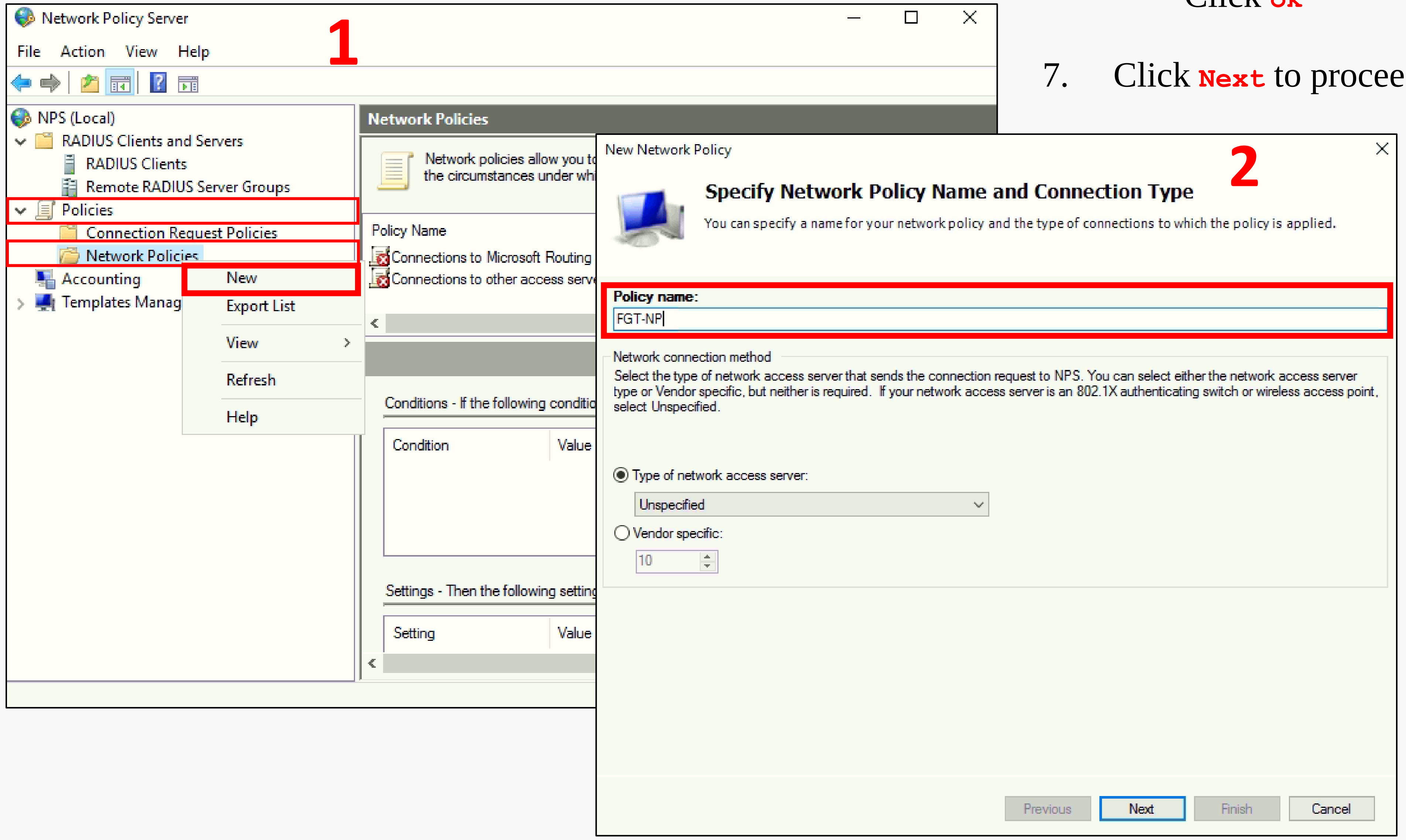
3. In **Specify Conditions** window: Click **Add**

4. Select **Windows Groups** → Click **Add Groups**.

5. In **Select Groups** window click **Add Groups** :
   - Add **ICT** Group → Click **OK**.
   - Add **HR** Group → Click **OK**.

6. Verify the added groups MIAARIACADEMY\ICT and MIAARIACADEMY\HR are listed.
   - Click **ok**

7. Click **Next** to proceed with policy configuration.



Network policies allow you to ... the circumstances under wh...

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.

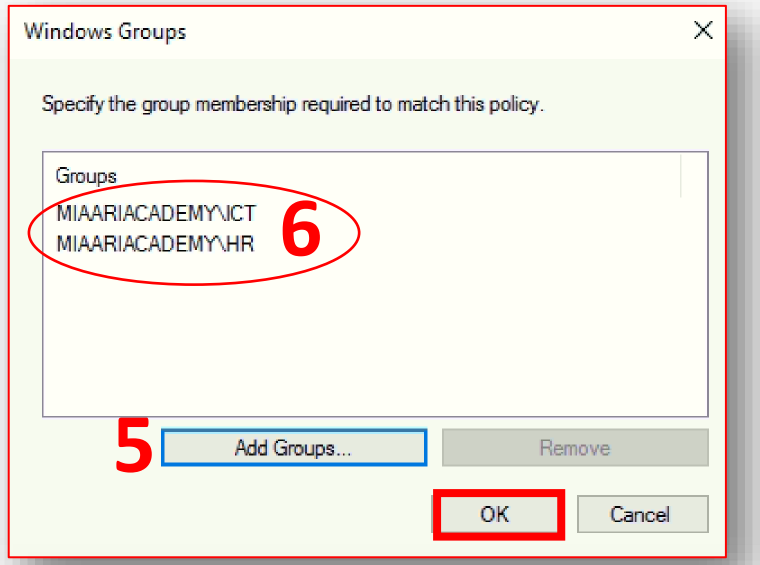
Policy name: FGT-NP

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

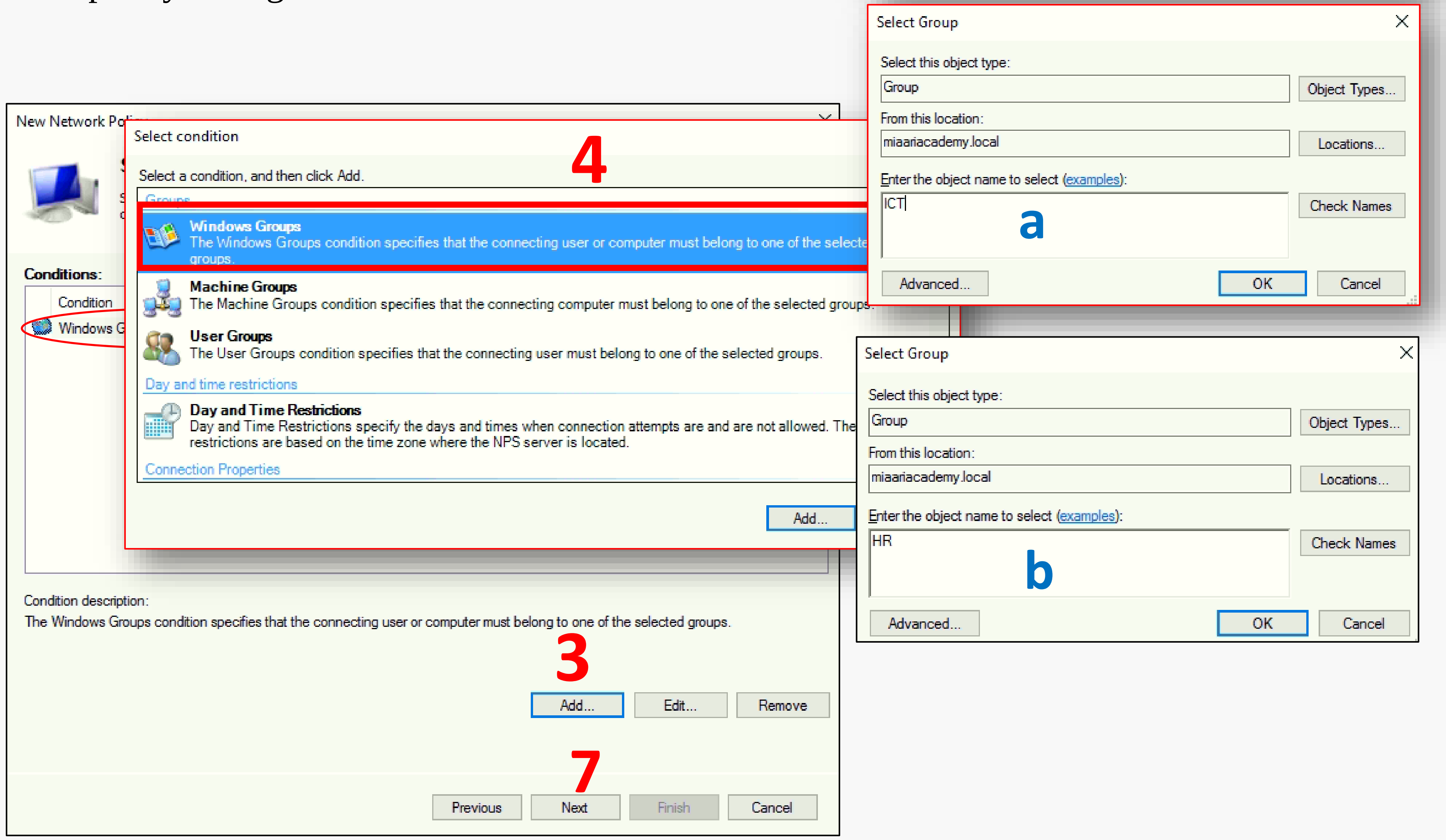
○ Vendor specific: 10



Windows Groups

Specify the group membership required to match this policy.

Groups
MIAARIACADEMY\ICT
MIAARIACADEMY\HR



Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selecte groups.

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. The restrictions are based on the time zone where the NPS server is located.

Connection Properties

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Select Group

Select this object type: Group

From this location: miaariacademy.local

Enter the object name to select (examples): ICT

Select Group

Select this object type: Group

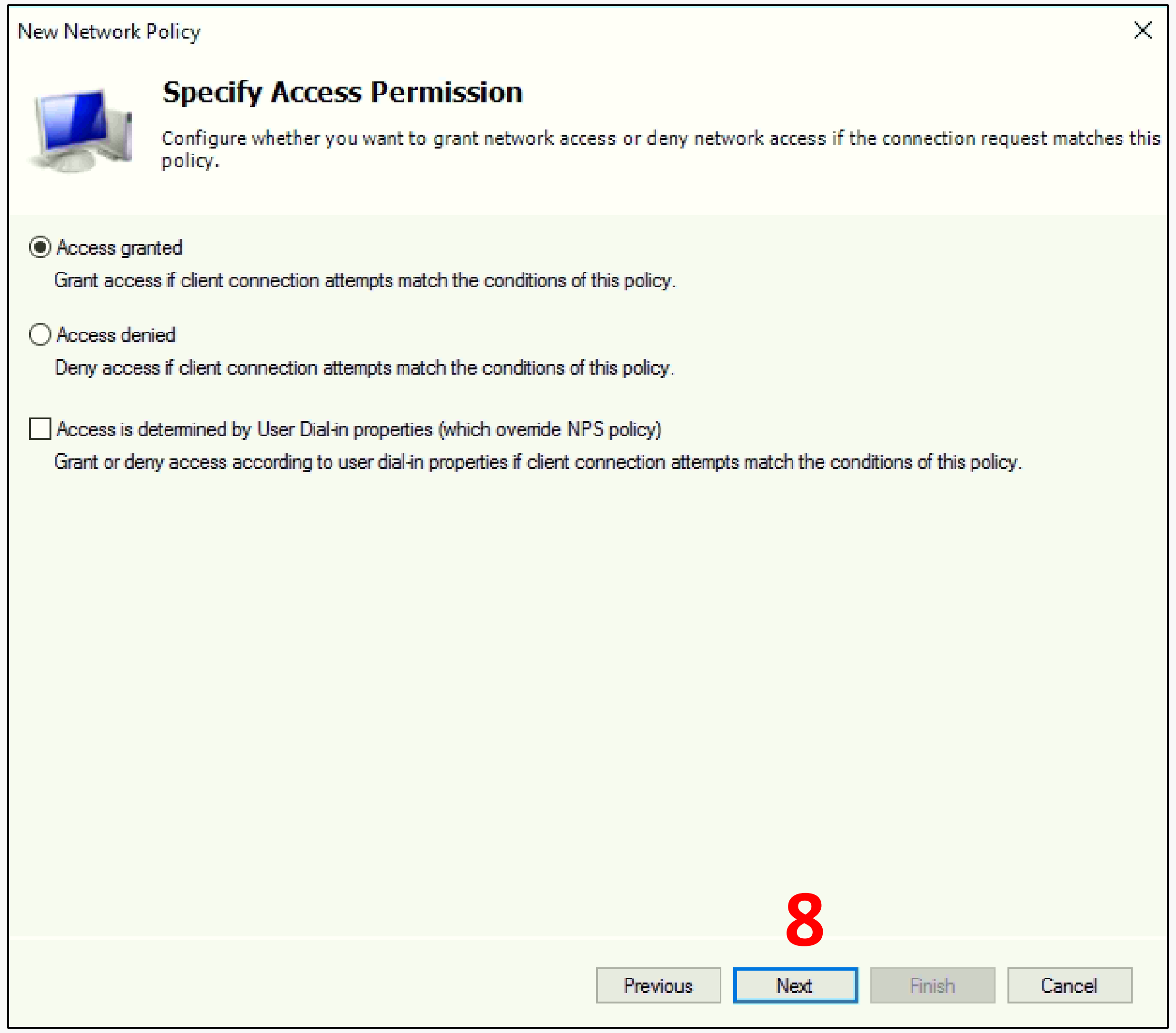
From this location: miaariacademy.local

Enter the object name to select (examples): HR

Creating Network Policy (NPS) for Active Directory Groups (ICT & HR) Cont..

8. Specify Access Permission

- In the `Specify Access Permission` window:
  - Select **`Access granted`** to allow network access for the users/groups that meet the policy conditions.
  - Click **`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.

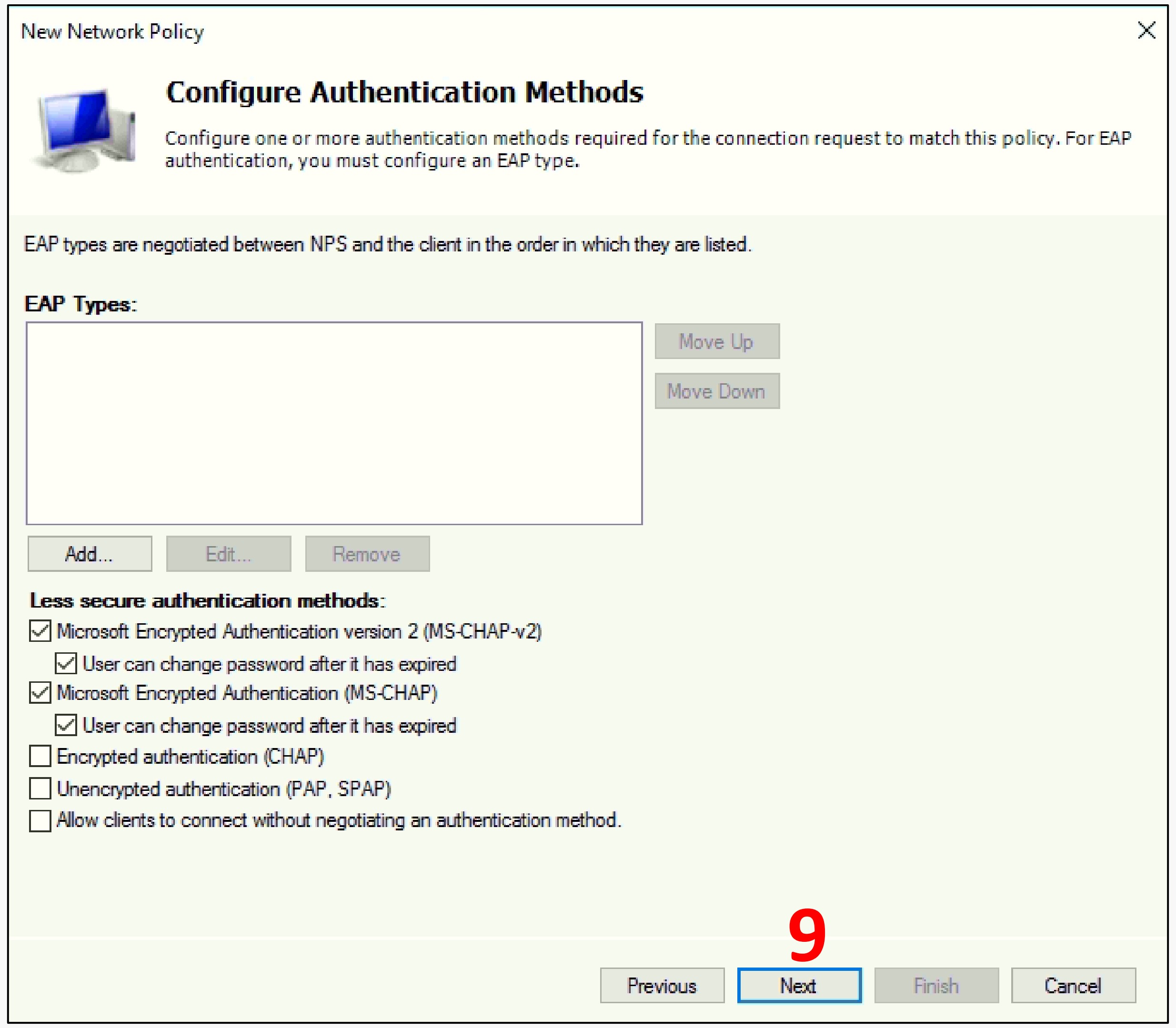
● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ 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.

9. Configure Authentication Methods

- In the `Configure Authentication Methods` window:
  - Select appropriate authentication methods.
  - Example:
    - Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
    - Microsoft Encrypted Authentication (MS-CHAP)
  - Click **`Next`**.



New Network Policy

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.

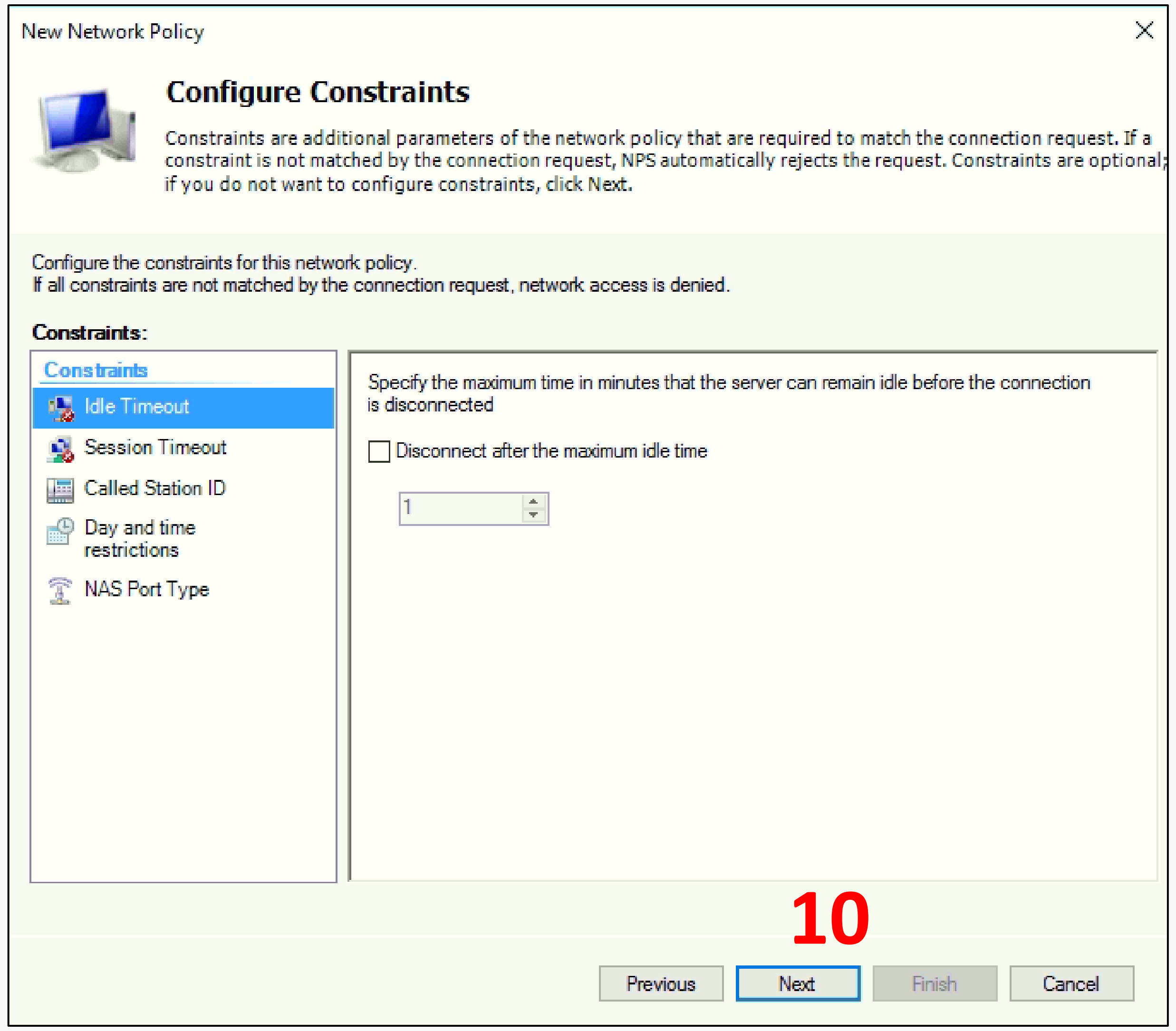
EAP Types:

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.

10. Configure Constraints

- In the `Configure Constraints` window:
  - Configure optional settings like `Idle Timeout` for the session.
  - Example: Specify idle time in minutes or leave default.
  - Click **`Next`** to proceed.



New Network Policy

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.

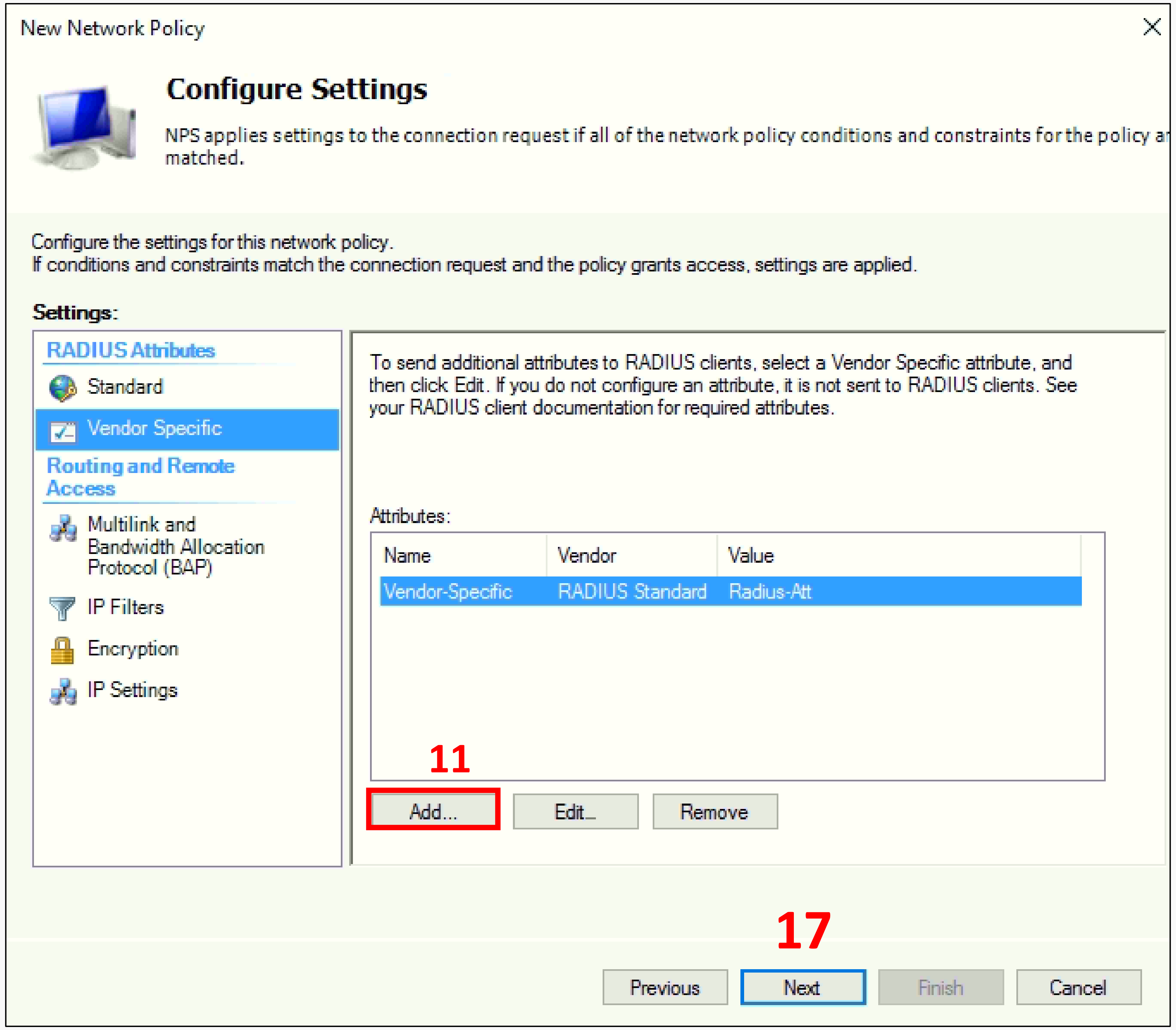
Constraints:

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

□ Disconnect after the maximum idle time

1

Creating Network Policy (NPS) for Active Directory Groups (ICT & HR) Cont..



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy ar 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

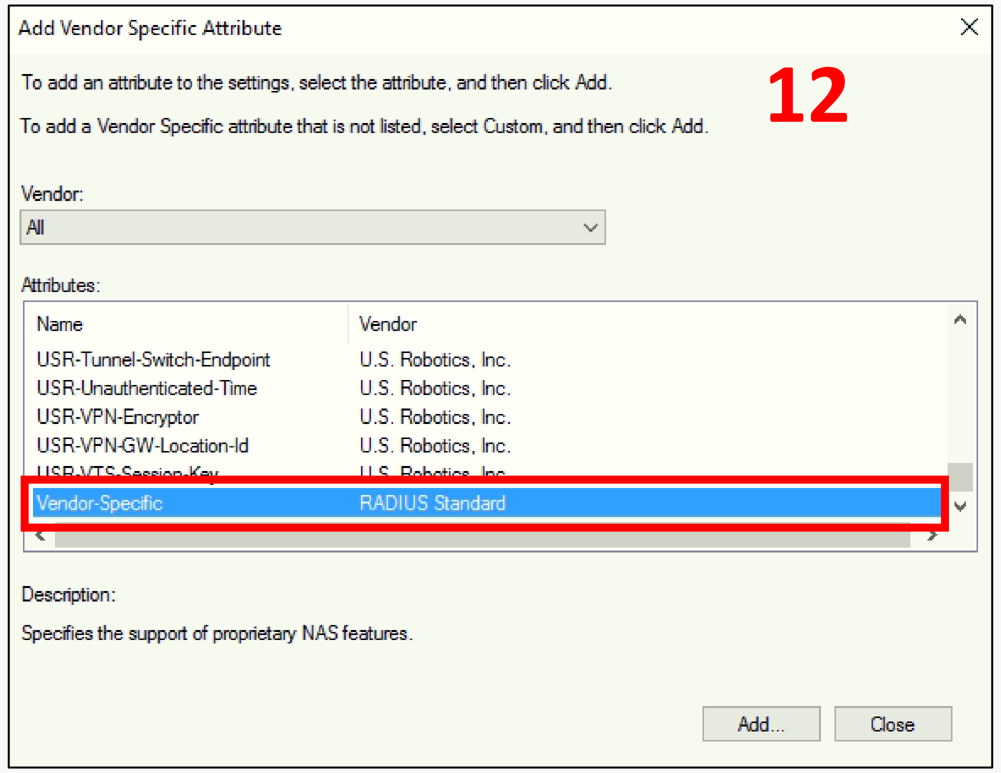
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	Radius-Att

11

17



Add Vendor Specific Attribute

12

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.

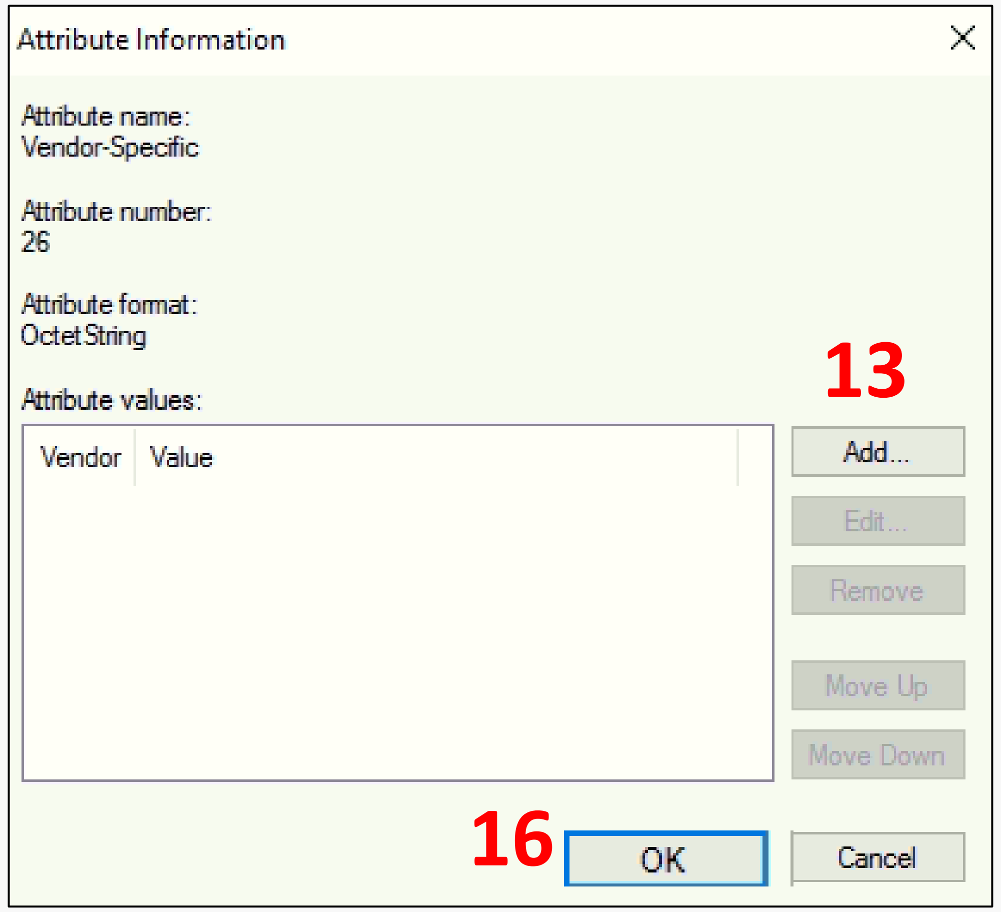
Vendor: All

Attributes:

Name	Vendor
USR-Tunnel-Switch-Endpoint	U.S. Robotics, Inc.
USR-Unauthenticated-Time	U.S. Robotics, Inc.
USR-VPN-Encryptor	U.S. Robotics, Inc.
USR-VPN-GW-Location-Id	U.S. Robotics, Inc.
USR-VTS-Session-Key	U.S. Robotics, Inc.
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

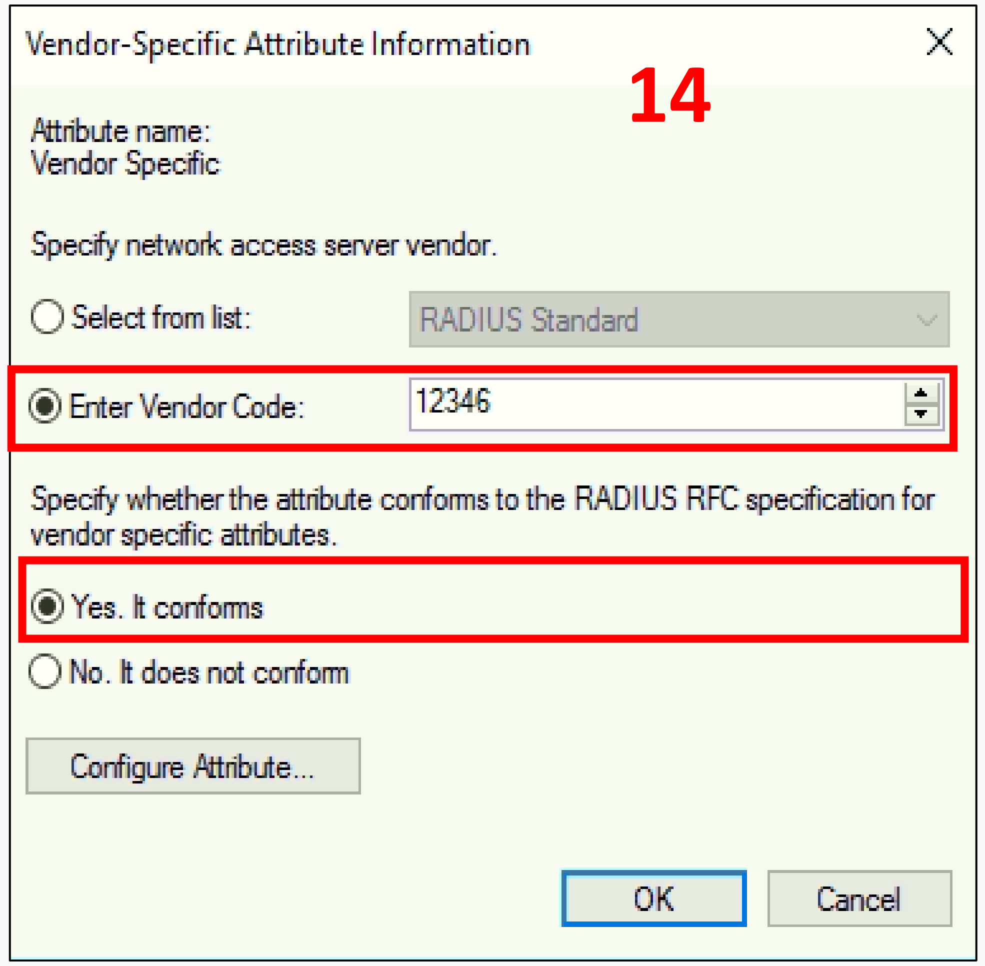
Attribute format:
OctetString

Attribute values:

Vendor	Value

13

16



Vendor-Specific Attribute Information

14

Attribute name:
Vendor Specific

Specify network access server vendor.

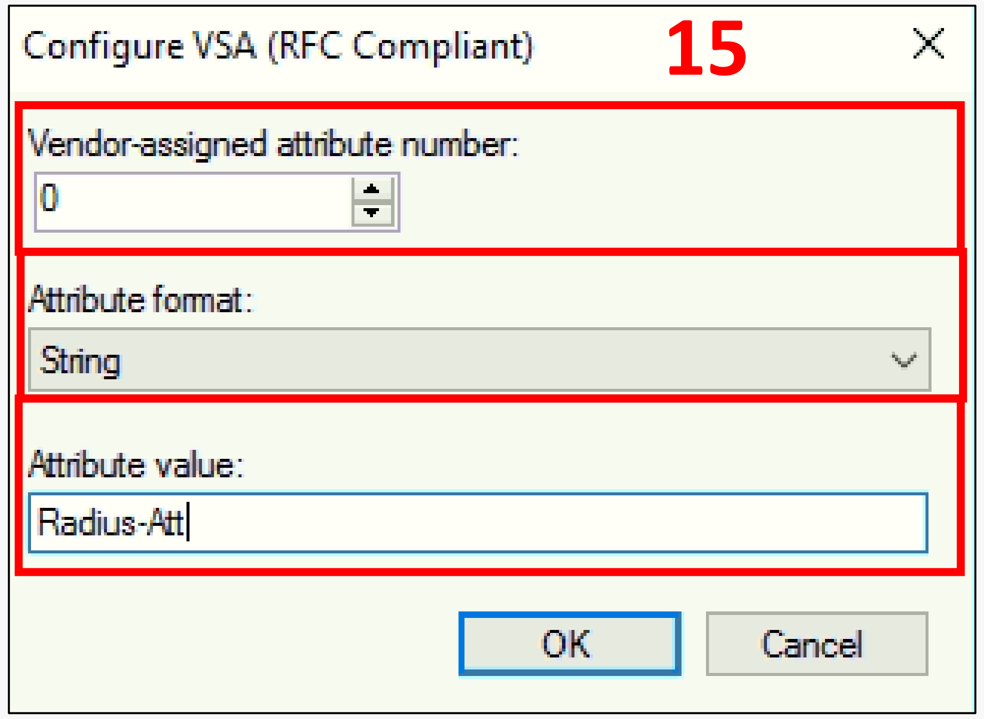
○ Select from list: RADIUS Standard

● Enter Vendor Code: 12346

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform



Configure VSA (RFC Compliant)

15

Vendor-assigned attribute number: 0

Attribute format: String

Attribute value: Radius-Att

Creating Network Policy (NPS) for Active Directory Groups (ICT & HR) Cont..

11. In the `Configure Settings` window of the New Network Policy: Click **`Add`** to add a new Vendor-Specific Attribute.

12. In the `Add Vendor Specific Attribute` window:
    - Select **`Vendor-Specific`** from the list and Click **`Add`**.

13. In the `Attribute Information` window : Click **`Add`**.

14. In the `Vendor-Specific Attribute Information` window:
    - Select `Enter Vendor Code` and type **`12346`**.
    - Ensure **`Yes, It conforms`** is selected.
    - Click **`Configure Attribute`**.

15. In the `Configure VSA (RFC Compliant)` window:
    - Set `Vendor-assigned attribute number` to **`0`**.
    - Set `Attribute format` to **`String`**.
    - Set `Attribute value` to **`Radius-Attr`**.
    - Click **`OK`**.

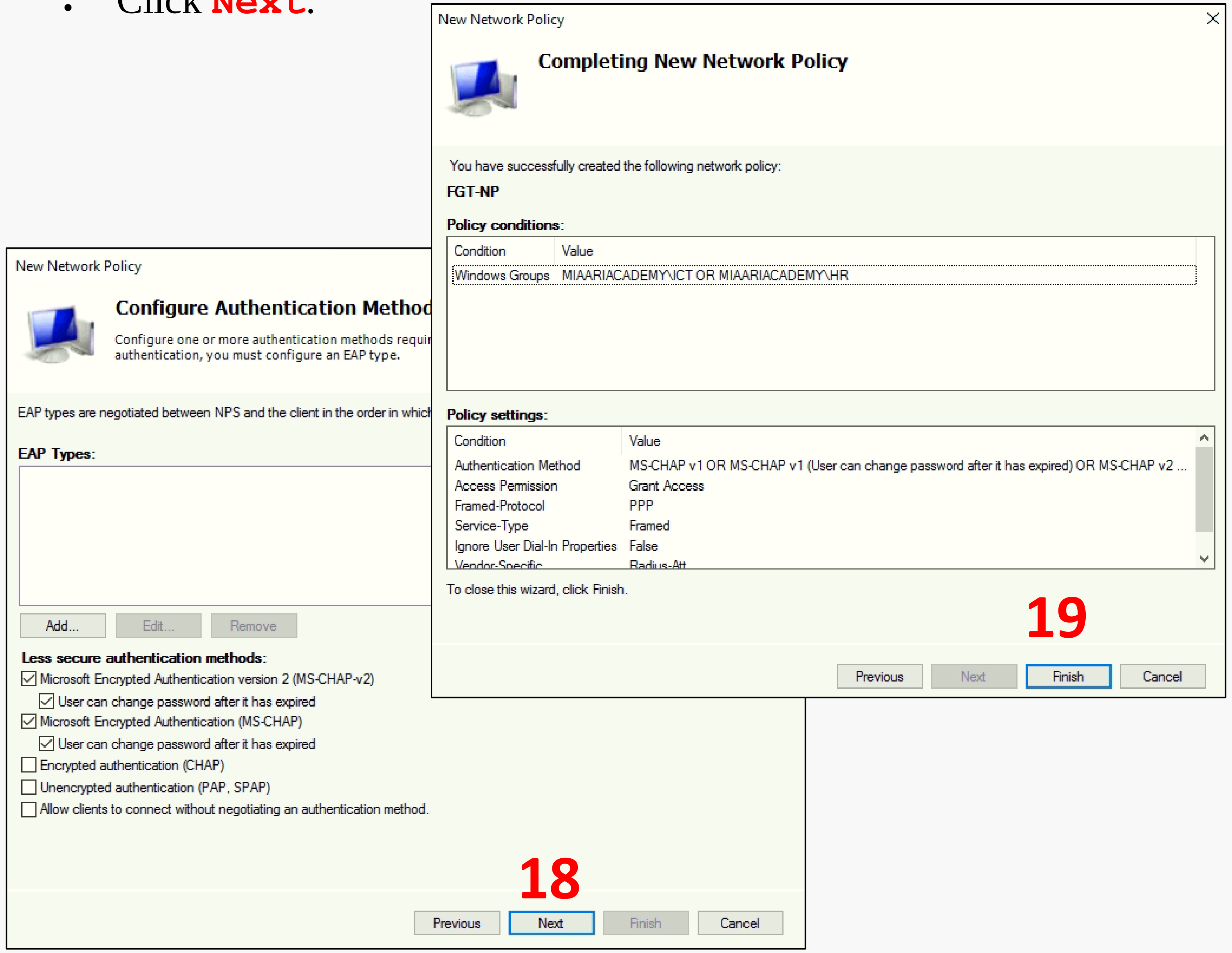
16. Click **`OK`** again to close the Attribute Information window.

17. In the `Configure Settings` window:
    - Verify that the new Vendor Specific Attribute has been added.
    - Click **`Next`** to proceed.

Creating Network Policy (NPS) for Active Directory Groups (ICT & HR) Cont..

18. In the `Configure Authentication Methods` window:
    - Select the required authentication methods:
        - MS-CHAPv2
        - MS-CHAPv1
        - Allow users to change passwords after expiry if needed.
    - Click **Next**.

19. In the `Completing New Network Policy` window:
    - Review the Policy Conditions:
        - Ensure `Windows Groups` includes `MIAARIACADEMY\ICT` OR `MIAARIACADEMY\HR`.
    - Click **Finish**.



New Network Policy

Configure Authentication Method

Configure one or more authentication methods requi
authentication, you must configure an EAP type.

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

EAP Types:

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.

18

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

FGT-NP

Policy conditions:

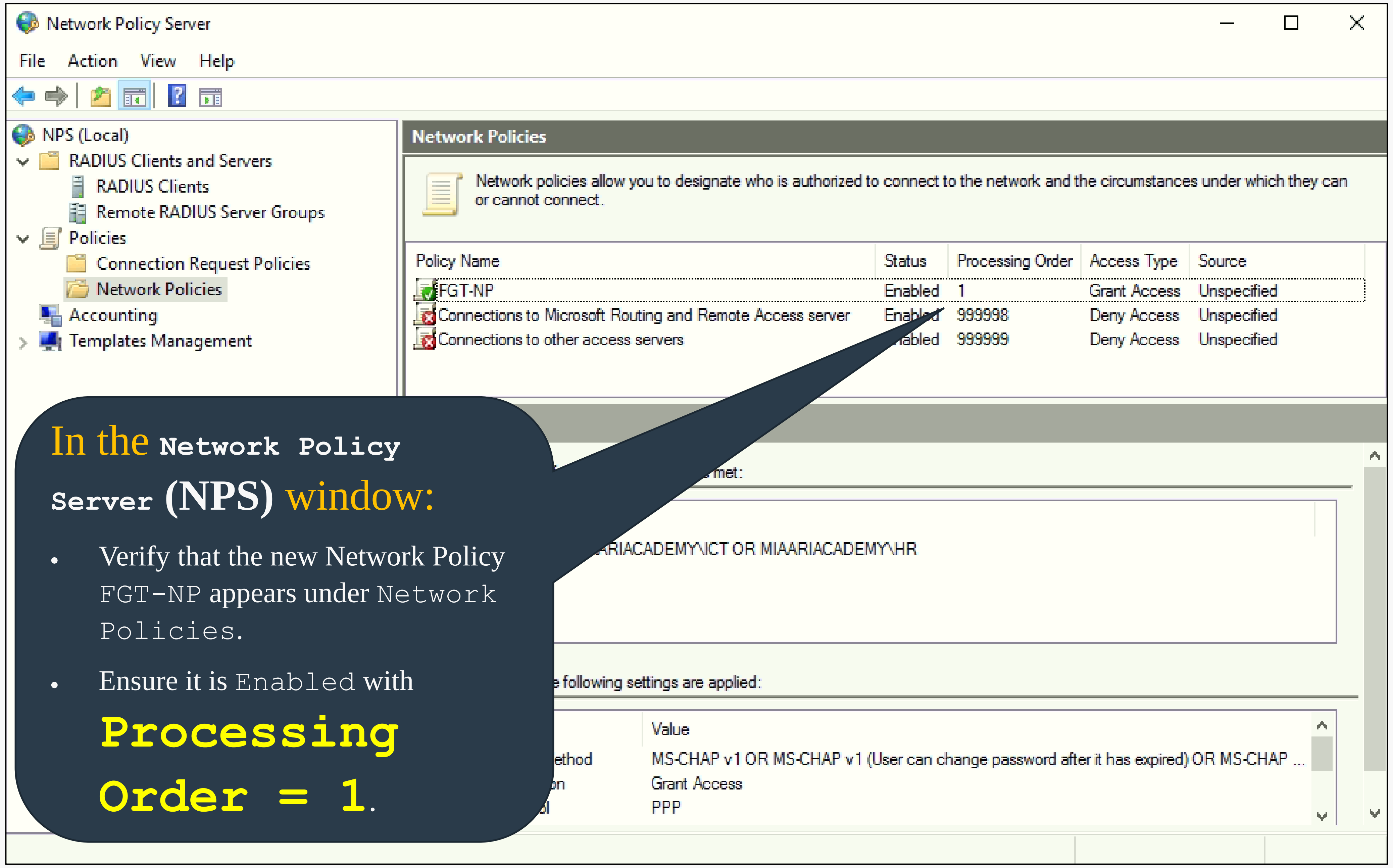
Condition	Value
Windows Groups	MIAARIACADEMY\ICT OR MIAARIACADEMY\HR

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Vendor-Specific	Radius-Att

To close this wizard, click Finish.

19



Network Policy Server

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
FGT-NP	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	abled	999999	Deny Access	Unspecified

met:

RIACADEMY\ICT OR MIAARIACADEMY\HR

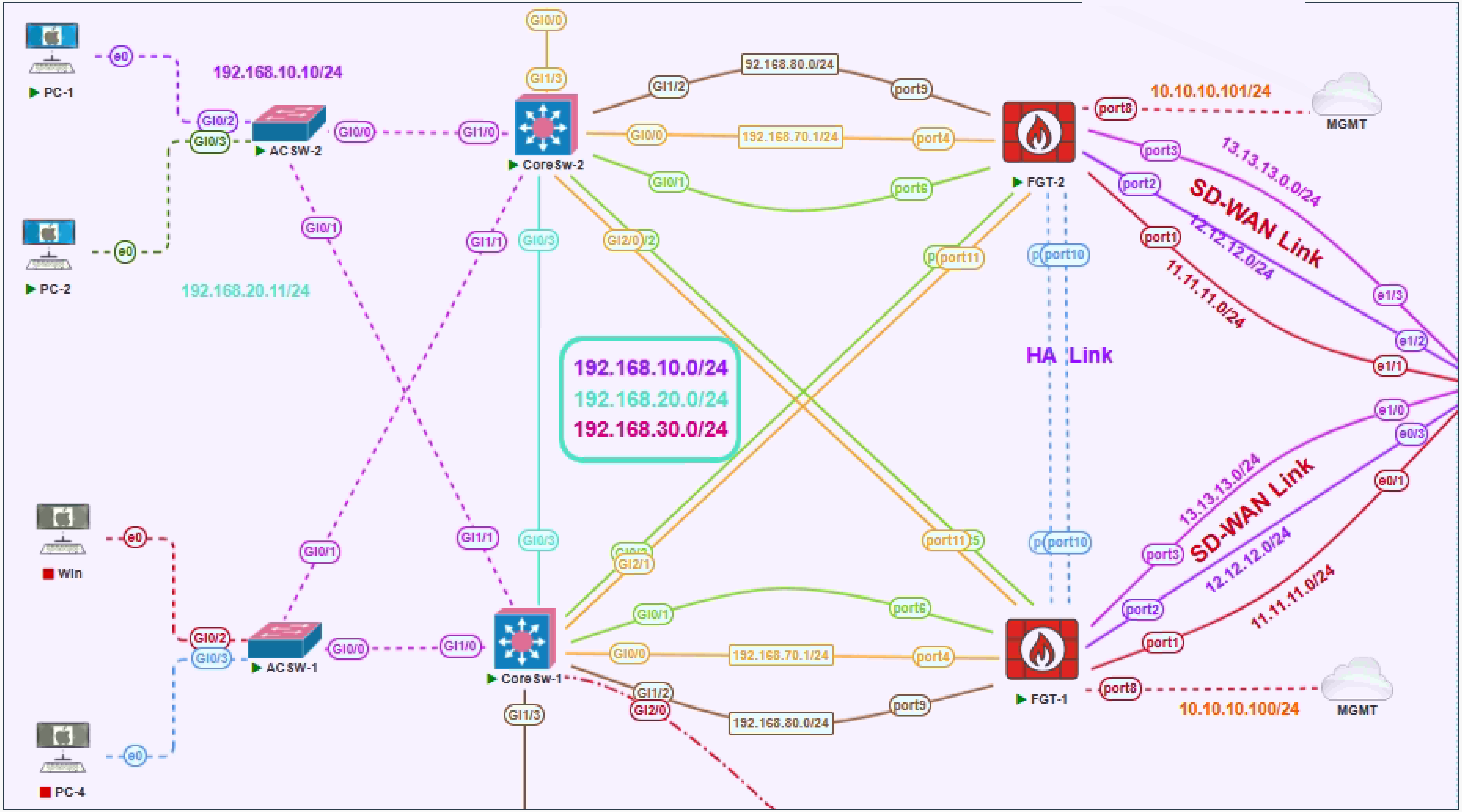
following settings are applied:

	Value
ethod	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP ...
on	Grant Access
ol	PPP

In the `Network Policy Server` (NPS) window:

- Verify that the new Network Policy `FGT-NP` appears under `Network Policies`.
- Ensure it is `Enabled` with **`Processing Order = 1`**.

Head Quarter



Steps to Log in to **FGT-1 of HQ** Web GUI

1. **Enter IP Address**

   Open a web browser and type : : `https://10.10.10.100`

2. **Enter Username**

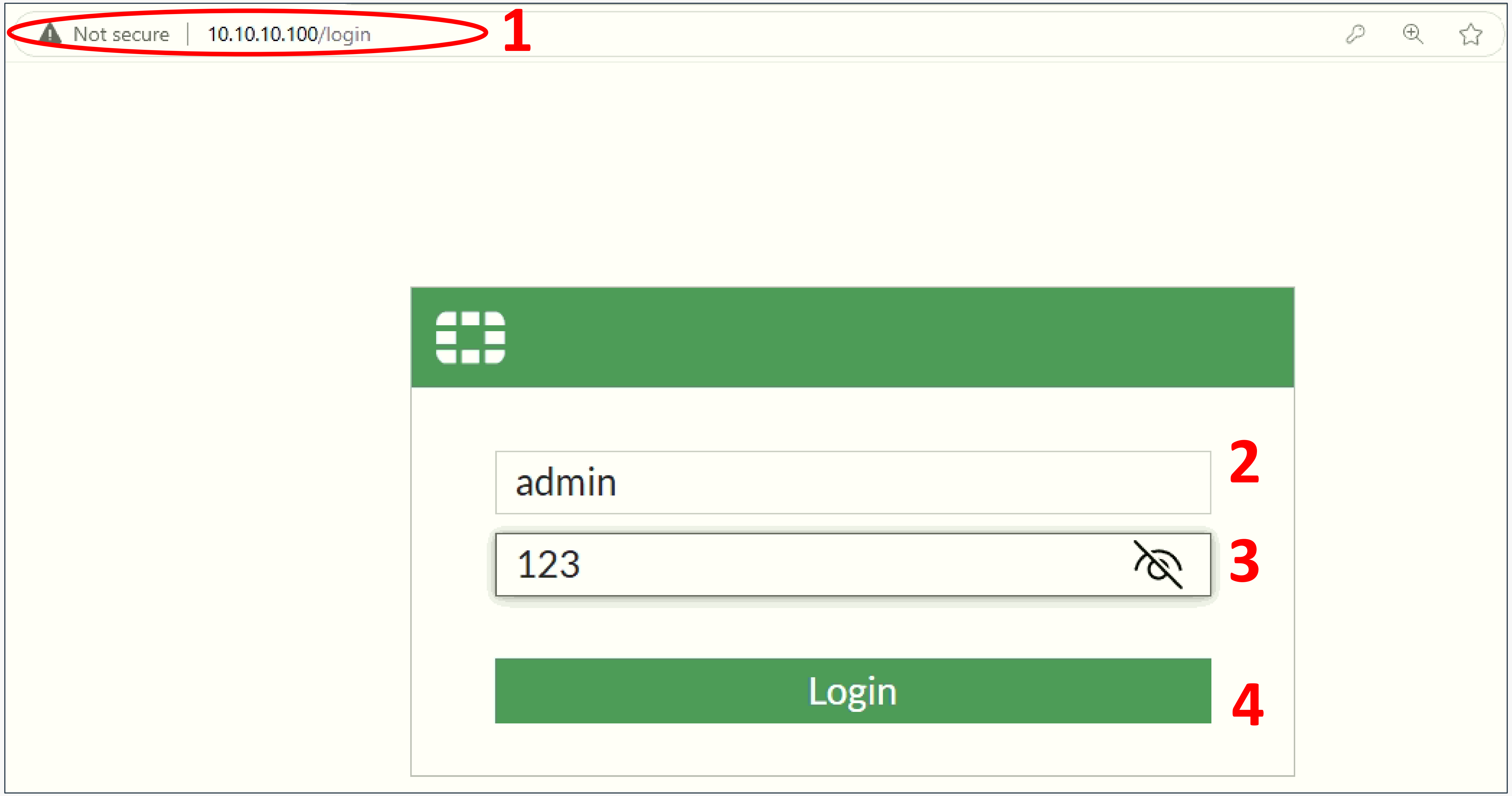
   Type: `admin` (default username)

3. **Enter Password**

   Type the password (e.g., `123` if you set it earlier).

4. **Click "Login"**

   Press the "**Login**" button to access the FortiGate Dashboard.



Not secure | 10.10.10.100/login

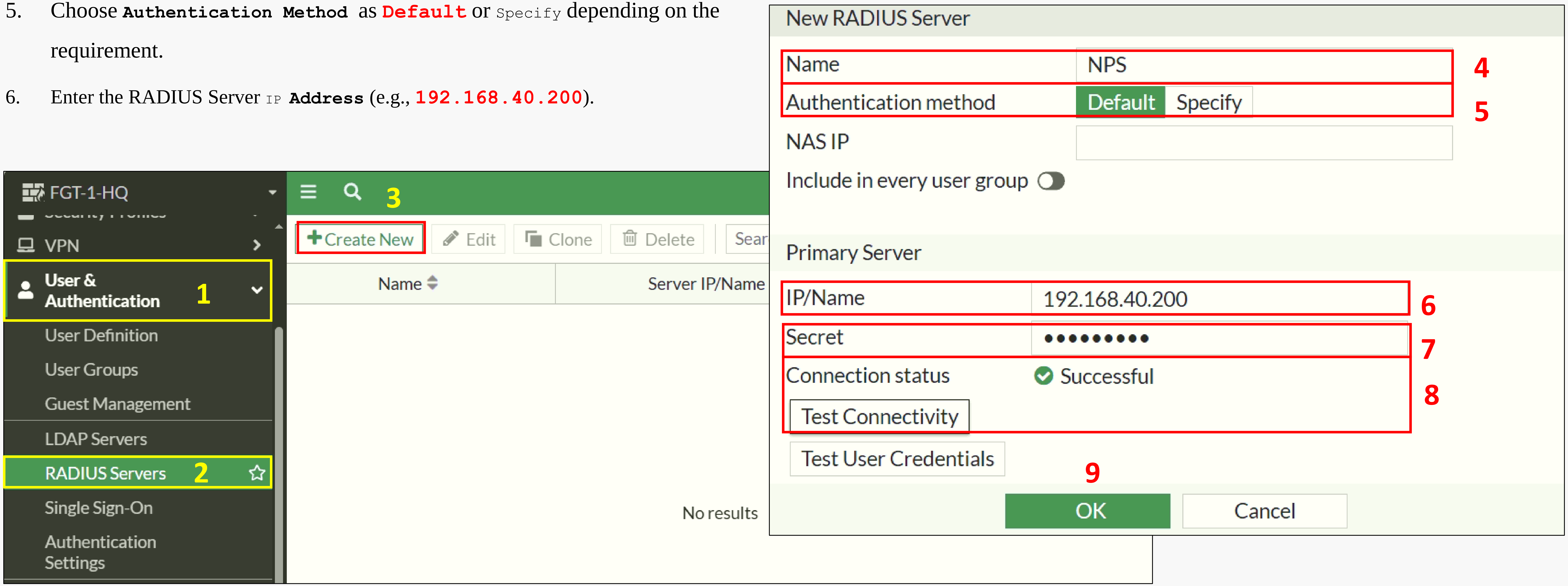
admin

123

Adding RADIUS Server (NPS) in FortiGate Firewall

1. Navigate to **User & Authentication** from the FortiGate GUI menu.
2. Select **RADIUS Servers**.
3. Click **Create New** to add a new RADIUS server.
4. Enter the **Name** of the RADIUS server (e.g., **NPS**).
5. Choose **Authentication Method** as **Default** or Specify depending on the requirement.
6. Enter the RADIUS Server IP **Address** (e.g., **192.168.40.200**).
7. Enter the **Secret** (**admin@123** must match the shared secret configured on NPS server).
8. Click **Test Connectivity** to verify the connection with the RADIUS Server.

   Ensure **Connection Status** is **Successful**.
9. Click **OK** to save the configuration.



New RADIUS Server

Name: NPS

Authentication method: [✓ Default] Specify

NAS IP:

Include in every user group: ○

Primary Server

IP/Name: 192.168.40.200

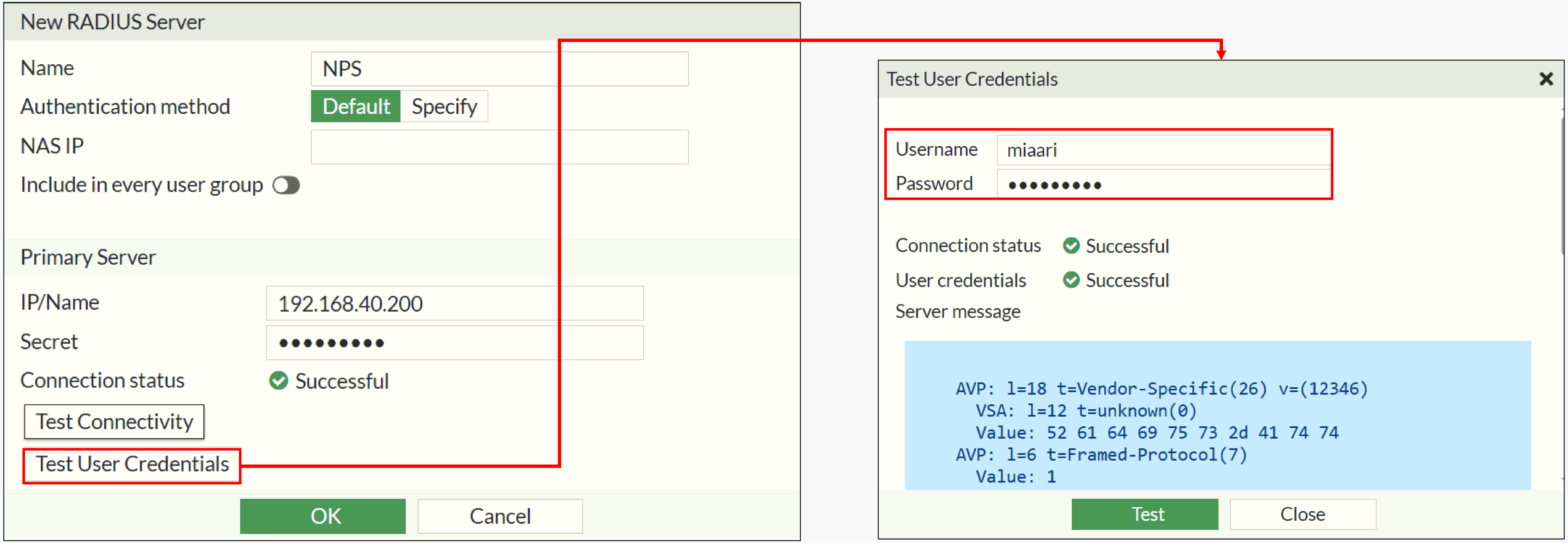
Secret: ●●●●●●●●●

Connection status: ✓ Successful

Test Connectivity

Testing User Authentication with RADIUS Server (NPS) in FortiGate

1. After configuring the RADIUS Server settings (IP, Secret, etc.), click on `Test User Credentials`.
2. Enter the Username (e.g., `miaari`).
3. Enter the corresponding Password (e.g., `admin@123`).
4. Click on `Test` to verify the credentials.
5. Ensure both Connection Status and User Credentials show Successful.



New RADIUS Server

Name	NPS
Authentication method	Default Specify
NAS IP	
Include in every user group	

Primary Server

IP/Name	192.168.40.200
Secret	●●●●●●●●●
Connection status	✓ Successful

Test User Credentials

Username	miaari
Password	●●●●●●●●●

Connection status	✓ Successful
User credentials	✓ Successful
Server message	

```
AVP: l=18 t=Vendor-Specific(26) v=(12346)
  VSA: l=12 t=unknown(0)
  Value: 52 61 64 69 75 73 2d 41 74 74
AVP: l=6 t=Framed-Protocol(7)
  Value: 1
```

Creating Remote RADIUS User miaari in FortiGate for NPS Authentication

1. Navigate to **User & Authentication** from the FortiGate dashboard.

2. Click on **User Definition**.

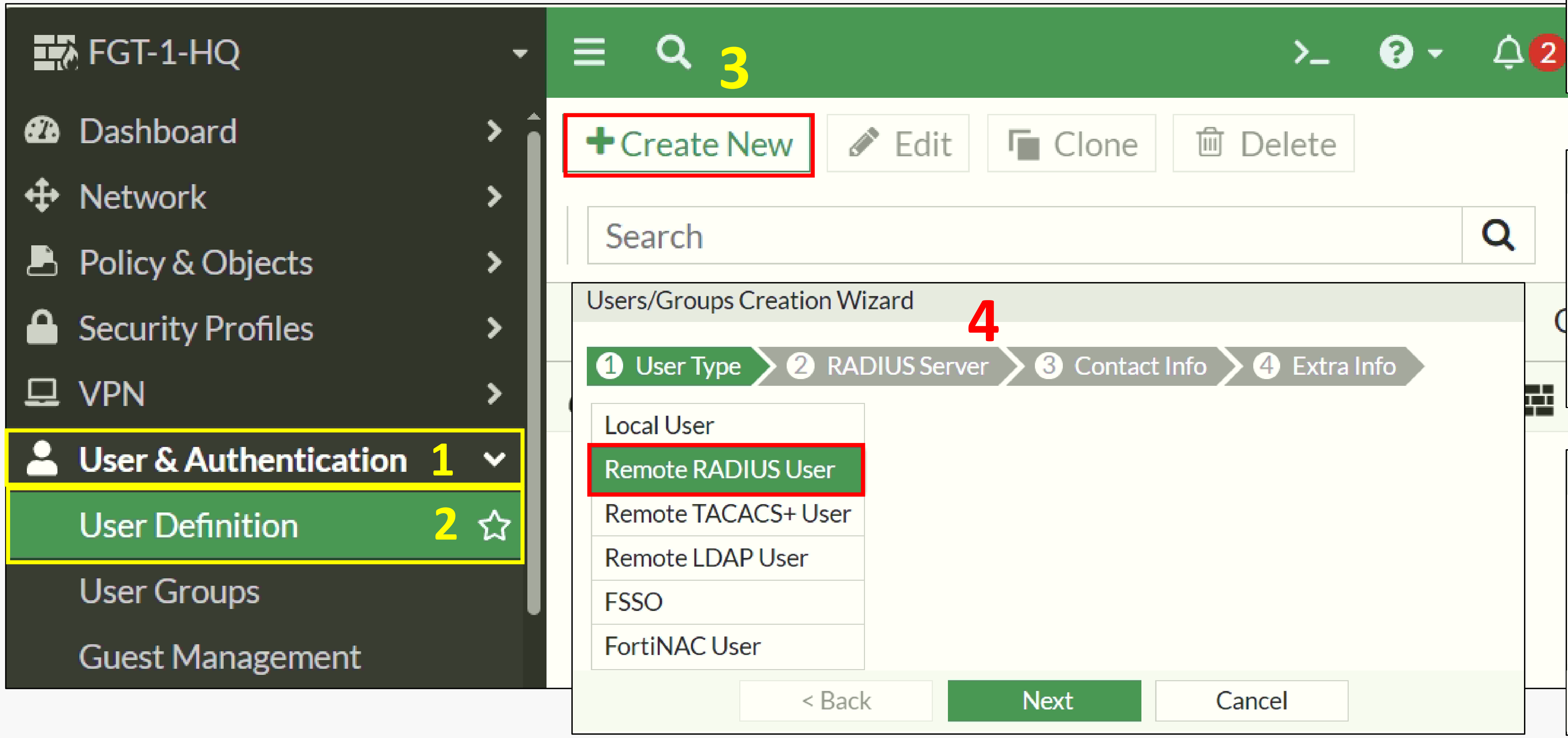
3. Click **Create New** to start the user creation wizard.

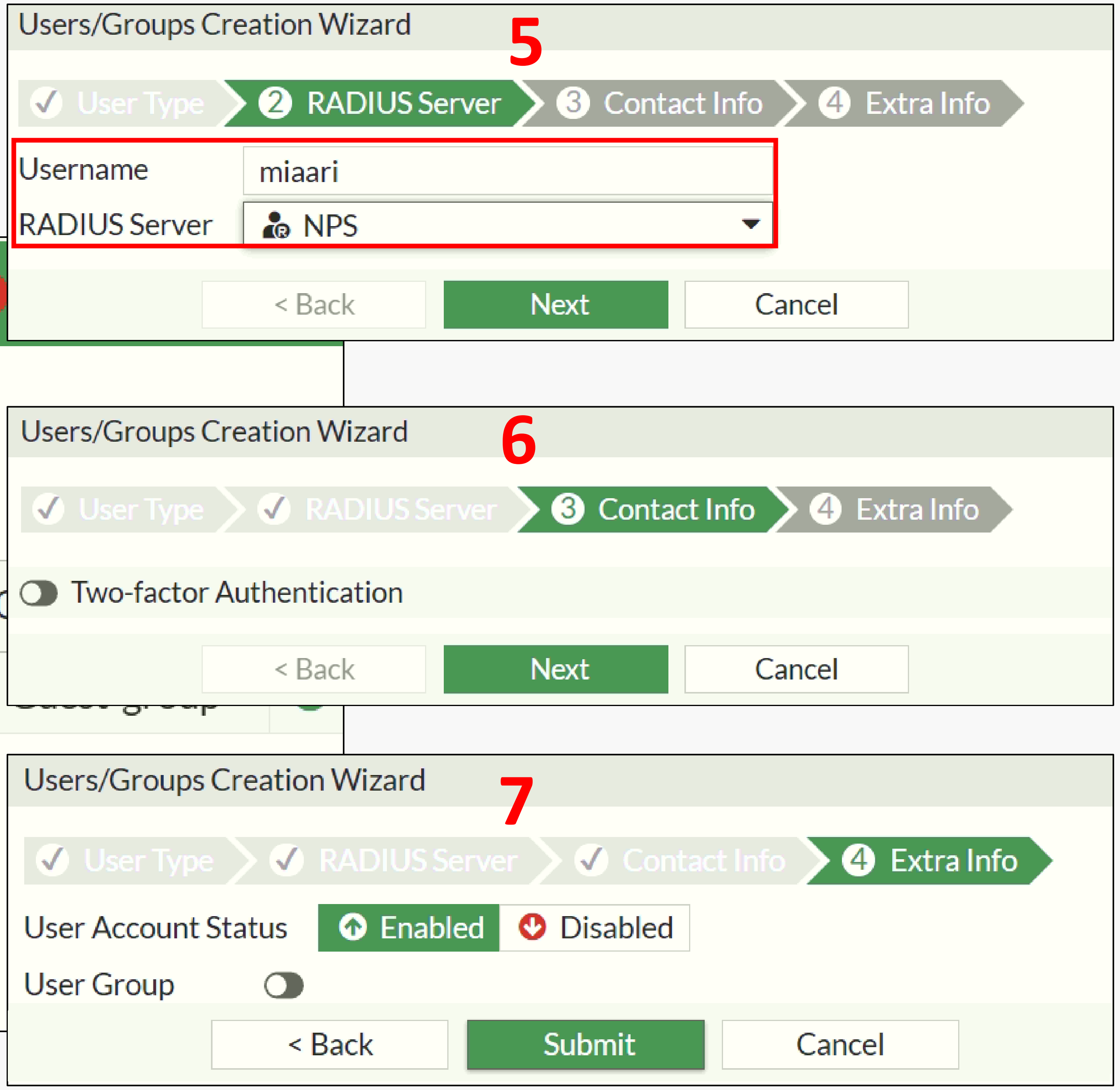
4. Select **Remote RADIUS User** from the User Type options.

5. Enter the Username (e.g., **miaari**) , select the configured RADIUS Server (e.g., **NPS**) and click **Next**.

6. (Optional) Configure Two-factor Authentication or leave it unchecked based on the requirement and click **Next** .

7. Set the User Account Status to Enabled and click **Submit** to create the Remote RADIUS User.





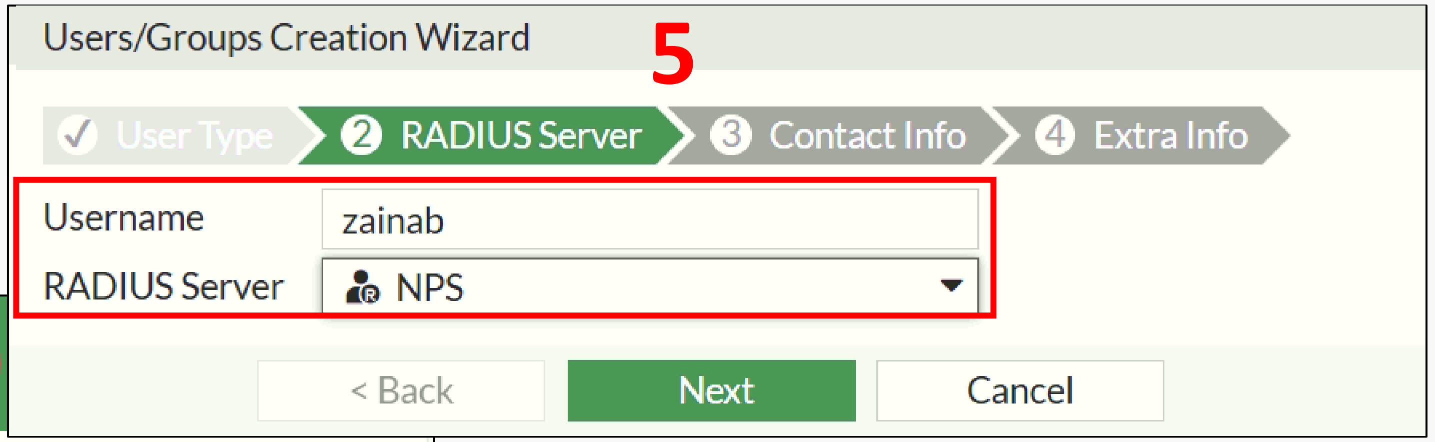
Username: miaari
RADIUS Server: NPS

○ Two-factor Authentication

User Account Status: ● Enabled ○ Disabled
User Group: ○

Creating Remote RADIUS User zainab in FortiGate for NPS Authentication

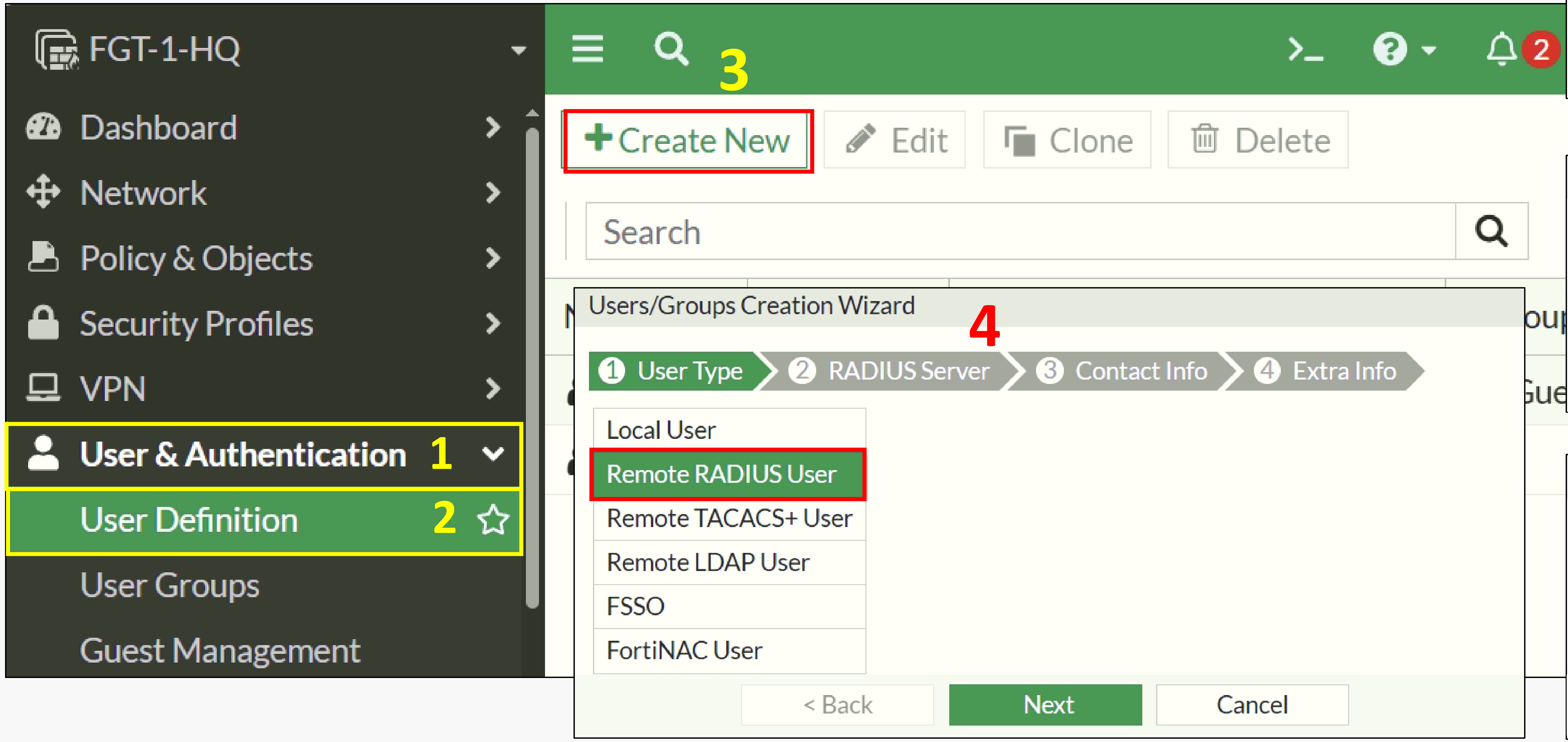
1. Navigate to **User & Authentication** from the FortiGate dashboard.
2. Click on **User Definition**.
3. Click **Create New** to start the user creation wizard.
4. Select **Remote RADIUS User** from the User Type options.
5. Enter the Username (e.g., **zainab**) , select the configured RADIUS Server (e.g., **NPS**) and click **Next**.
6. (Optional) Configure Two-factor Authentication or leave it unchecked based on the requirement and click **Next** .
7. Set the User Account Status to Enabled and click **Submit** to create the Remote RADIUS User.



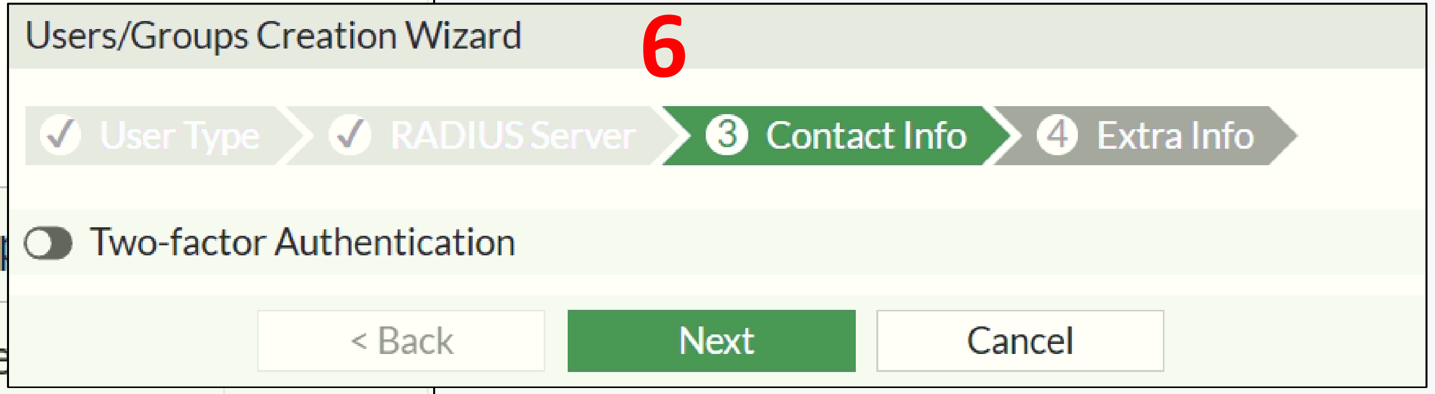
Users/Groups Creation Wizard

Username: zainab

RADIUS Server: NPS

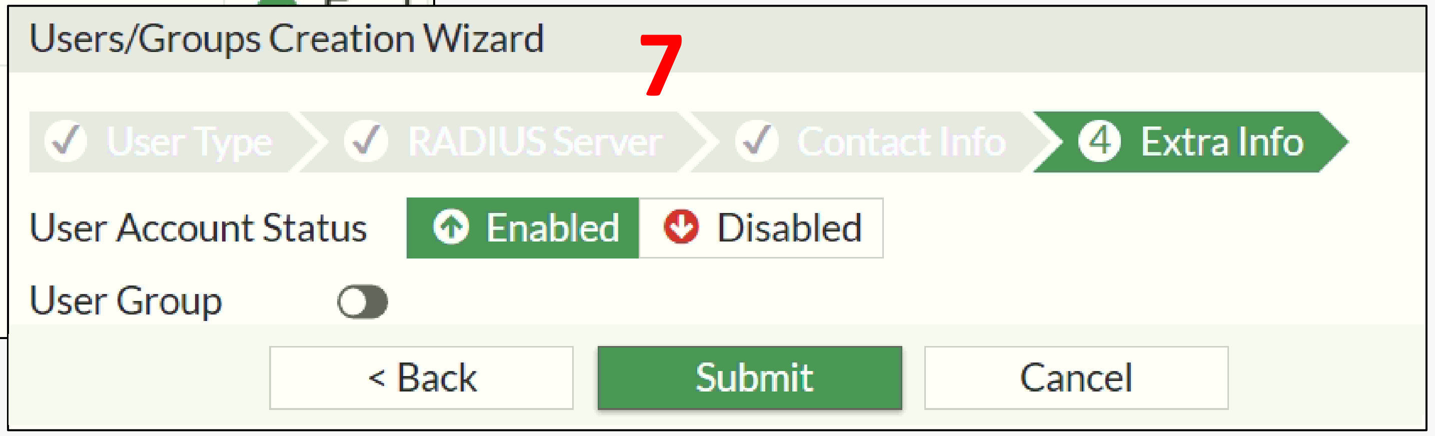


Users/Groups Creation Wizard



Users/Groups Creation Wizard

○ Two-factor Authentication



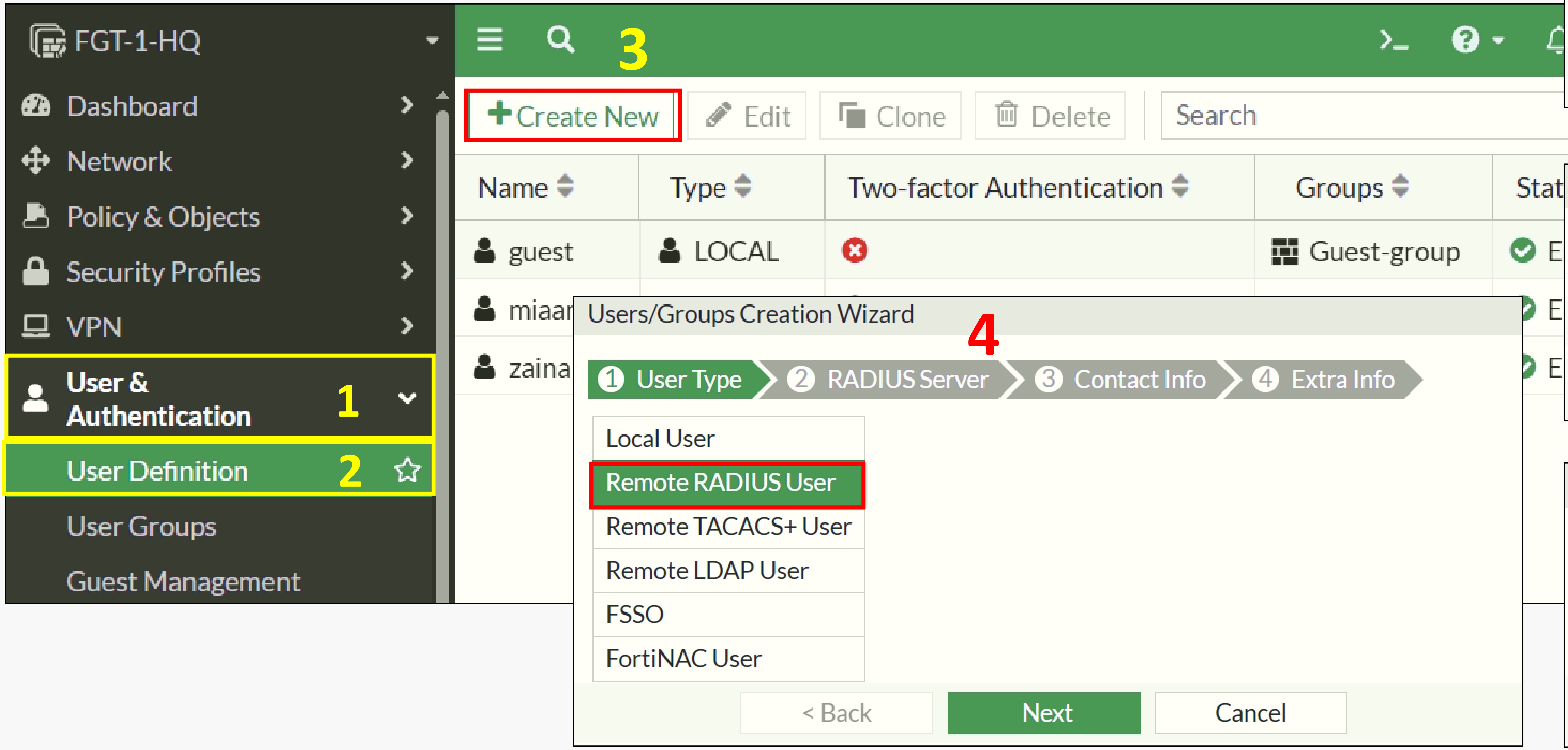
Users/Groups Creation Wizard

User Account Status: [✓ Enabled] Disabled

User Group ○

Creating Remote RADIUS User adam in FortiGate for NPS Authentication

1. Navigate to **User & Authentication** from the FortiGate dashboard.
2. Click on **User Definition**.
3. Click **Create New** to start the user creation wizard.
4. Select **Remote RADIUS User** from the User Type options.
5. Enter the Username (e.g., **adam**) , select the configured RADIUS Server (e.g., **NPS**) and click **Next**.
6. (Optional) Configure Two-factor Authentication or leave it unchecked based on the requirement and click **Next** .
7. Set the User Account Status to Enabled and click **Submit** to create the Remote RADIUS User.



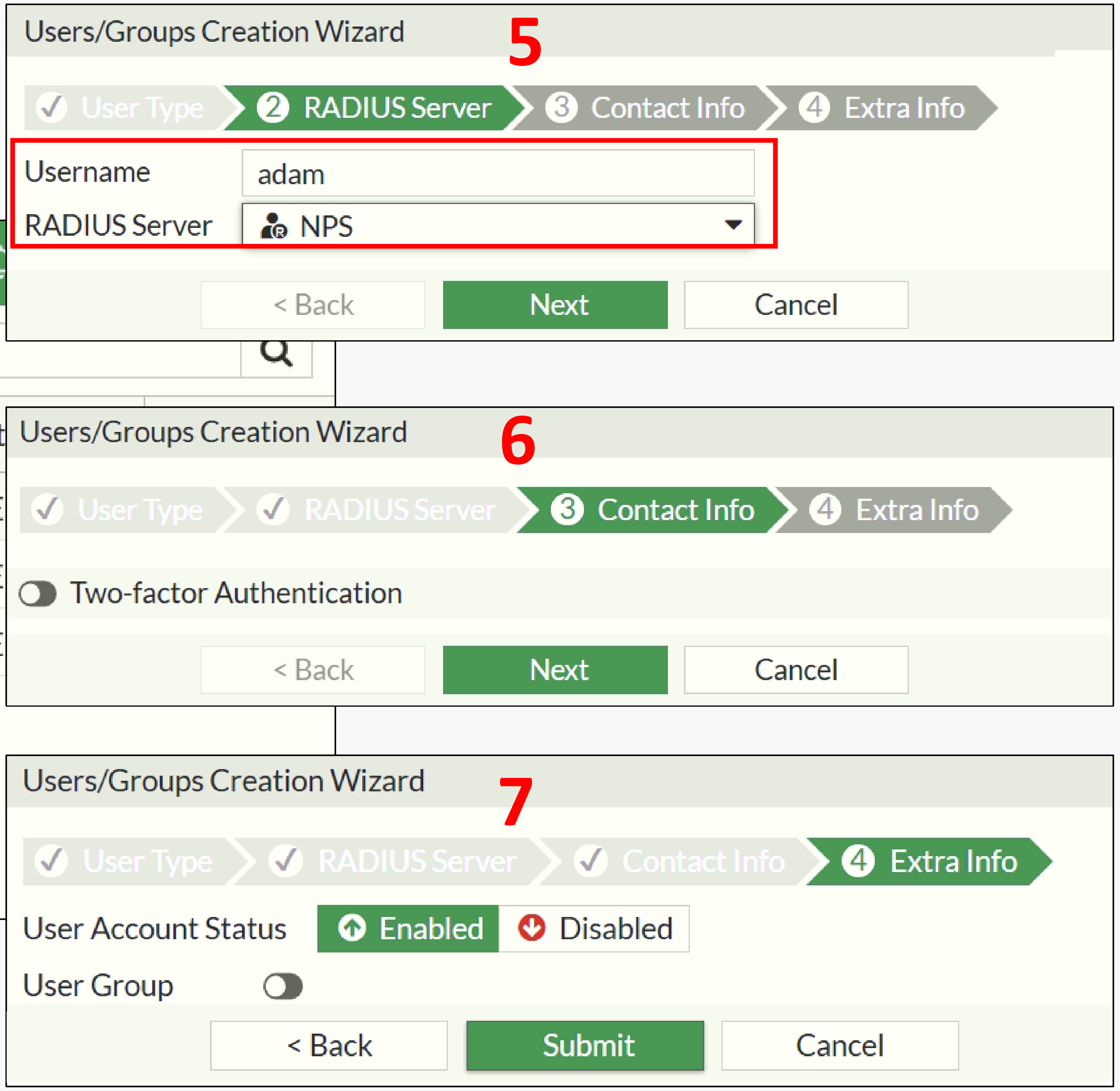
Name	Type	Two-factor Authentication	Groups	Stat
guest	LOCAL	✗	Guest-group	✓ E
miaar				E
zaina				E

Users/Groups Creation Wizard

1 User Type > 2 RADIUS Server > 3 Contact Info > 4 Extra Info

- Local User
- Remote RADIUS User
- Remote TACACS+ User
- Remote LDAP User
- FSSO
- FortiNAC User

< Back | Next | Cancel



Users/Groups Creation Wizard

✓ User Type > 2 RADIUS Server > 3 Contact Info > 4 Extra Info

Username: adam

RADIUS Server: NPS

< Back | Next | Cancel

Users/Groups Creation Wizard

✓ User Type > ✓ RADIUS Server > 3 Contact Info > 4 Extra Info

○ Two-factor Authentication

< Back | Next | Cancel

Users/Groups Creation Wizard

✓ User Type > ✓ RADIUS Server > ✓ Contact Info > 4 Extra Info

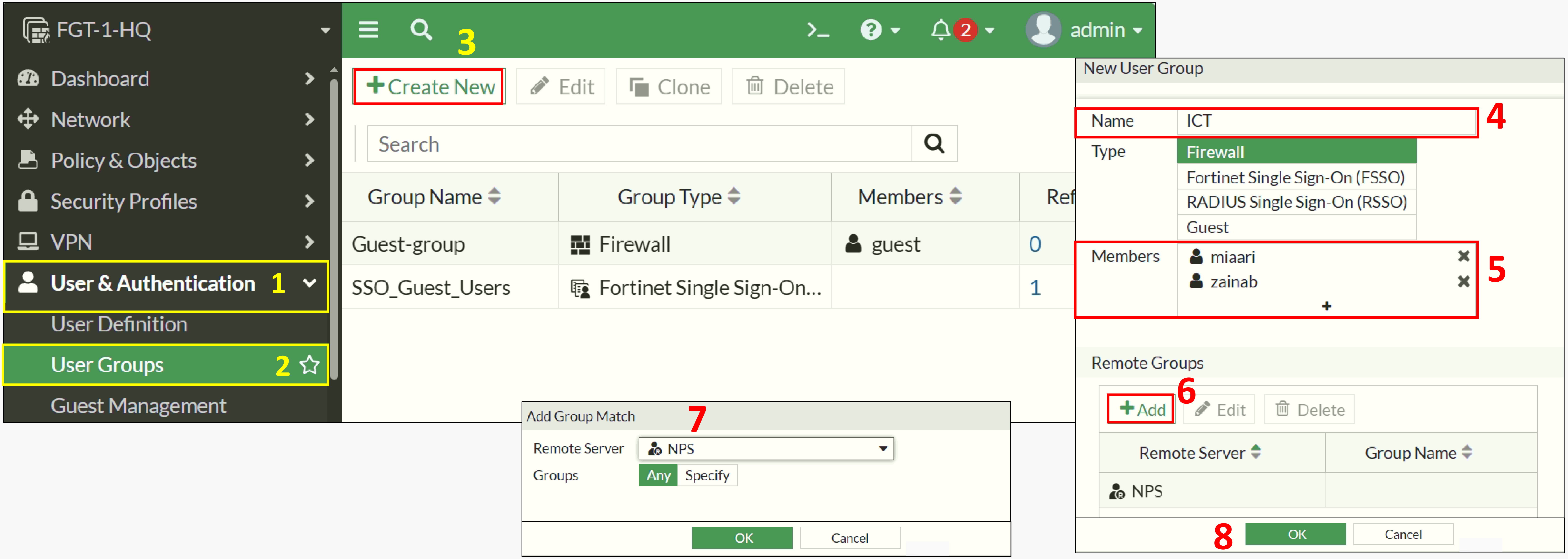
User Account Status: [✓ Enabled] Disabled

User Group ○

< Back | Submit | Cancel

Creating User Group (ICT) in FortiGate for RADIUS Users

1. Navigate to **User & Authentication** from the FortiGate menu.
2. Click on **User Groups**.
3. Click **Create New** to add a new user group.
4. Enter the Group Name (e.g., **ICT**) and select Firewall as the Group Type.
5. Add existing RADIUS users (e.g., **miaari and zainab**) as Members.
6. Under Remote Groups, click **Add** to configure the RADIUS Server group mapping.
7. Choose the configured Remote Server (e.g., **NPS**) and select Any or Specify to match specific groups.
8. Click **OK** to save and create the User Group.



Group Name	Group Type	Members	Ref
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On...		1

New User Group

Name: ICT

Type: Firewall (selected) / Fortinet Single Sign-On (FSSO) / RADIUS Single Sign-On (RSSO) / Guest

Members: miaari, zainab

Remote Groups

Remote Server	Group Name
NPS	

Add Group Match

Remote Server: NPS

Groups: Any (selected) / Specify

Creating User Group (HR) in FortiGate for RADIUS Users

1. Navigate to **User & Authentication** from the FortiGate menu.

2. Click on **User Groups**.

3. Click **Create New** to add a new user group.

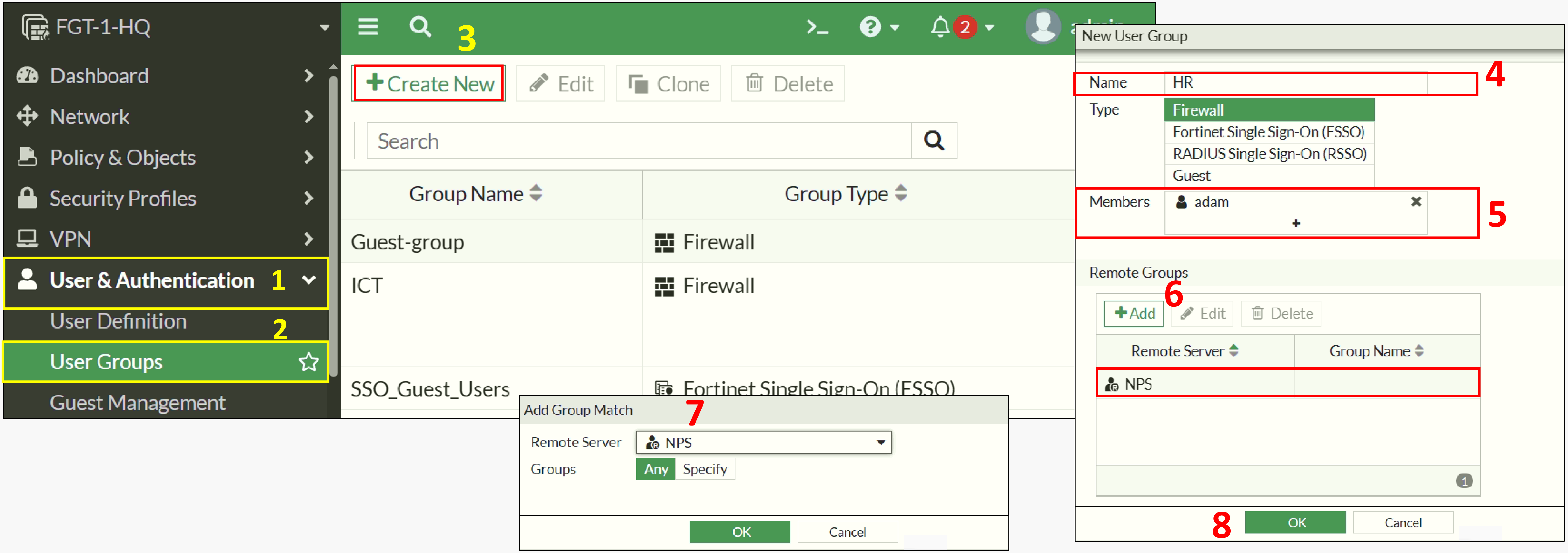
4. Enter the Group Name (e.g., **HR**) and select Firewall as the Group Type.

5. Add existing RADIUS users (e.g., **adam**) as Members.

6. Under Remote Groups, click **Add** to configure the RADIUS Server group mapping.

7. Choose the configured Remote Server (e.g., **NPS**) and select Any or Specify to match specific groups.

8. Click **OK** to save and create the User Group.



Group Name	Group Type
Guest-group	Firewall
ICT	Firewall
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)

New User Group

Name: HR

Type: Firewall

Members: adam

Remote Groups

Remote Server	Group Name
NPS	

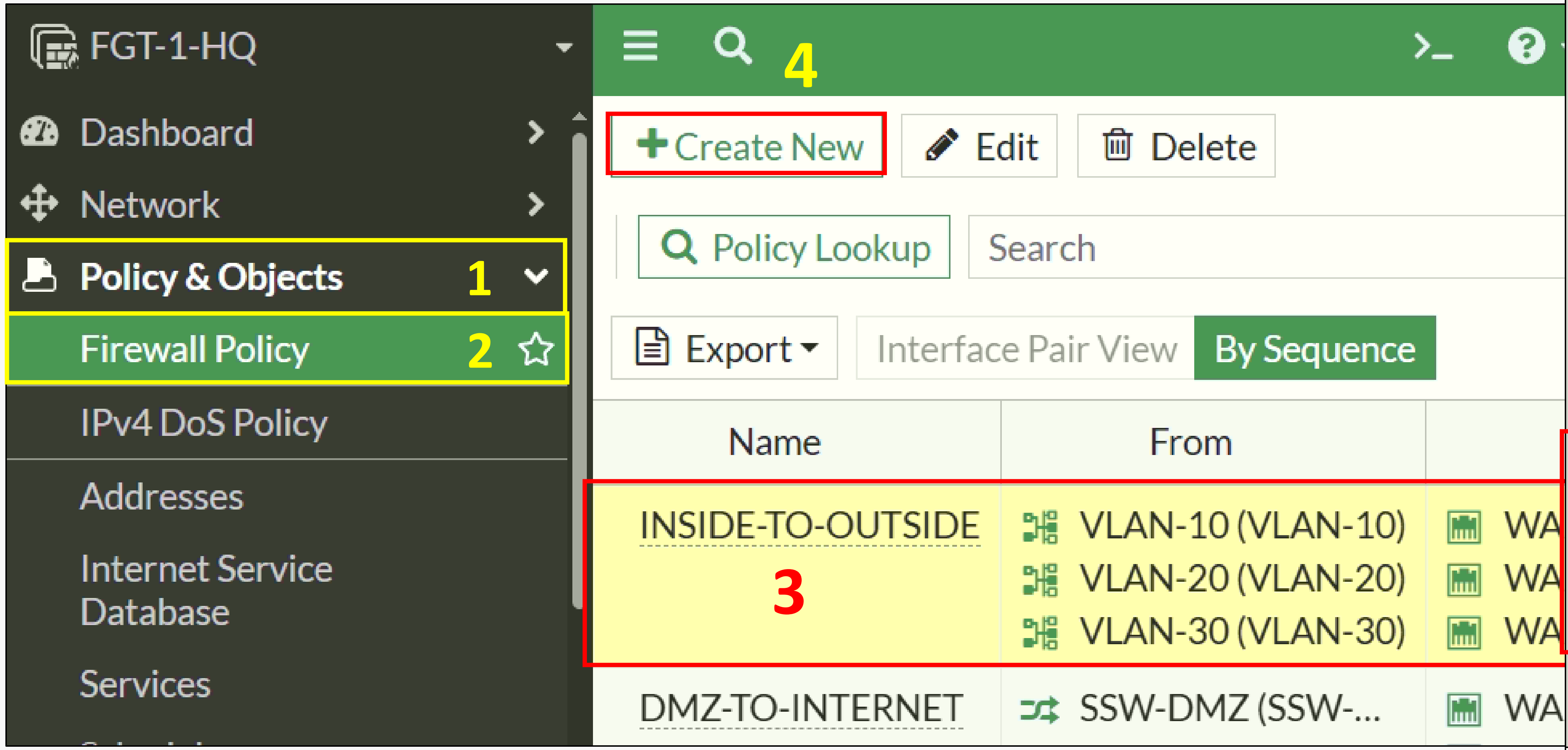
Add Group Match

Remote Server: NPS

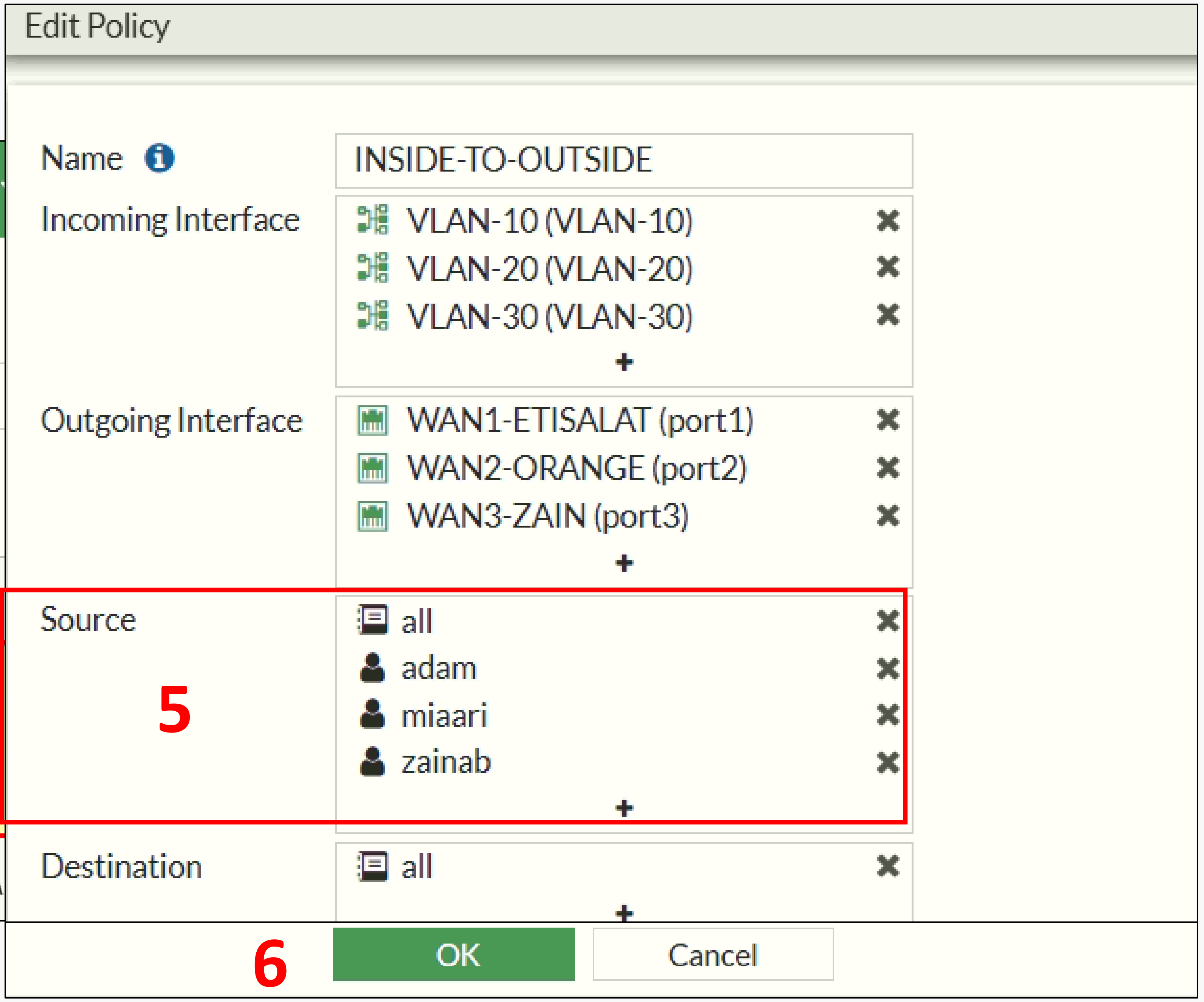
Groups: Any

Modify Firewall Policy INSIDE-TO-OUTSIDE in FortiGate for RADIUS Users

1. Navigate to `Policy & Objects` in the FortiGate menu.
2. Click on `Firewall Policy` from the submenu.
3. Select the existing policy `INSIDE-TO-OUTSIDE` (or create a new one).
4. Click `Create New` to create a new policy or edit the existing one.
5. In the Source field, add the RADIUS Users (e.g., `adam, miaari, zainab`) and select `all` for the Destination.
6. Click `OK` to save the policy configuration.



Name	From	
INSIDE-TO-OUTSIDE	VLAN-10 (VLAN-10) VLAN-20 (VLAN-20) VLAN-30 (VLAN-30)	WA WA WA
DMZ-TO-INTERNET	SSW-DMZ (SSW-...	WA


Edit Policy

Name: INSIDE-TO-OUTSIDE

Incoming Interface: VLAN-10 (VLAN-10), VLAN-20 (VLAN-20), VLAN-30 (VLAN-30)

Outgoing Interface: WAN1-ETISALAT (port1), WAN2-ORANGE (port2), WAN3-ZAIN (port3)

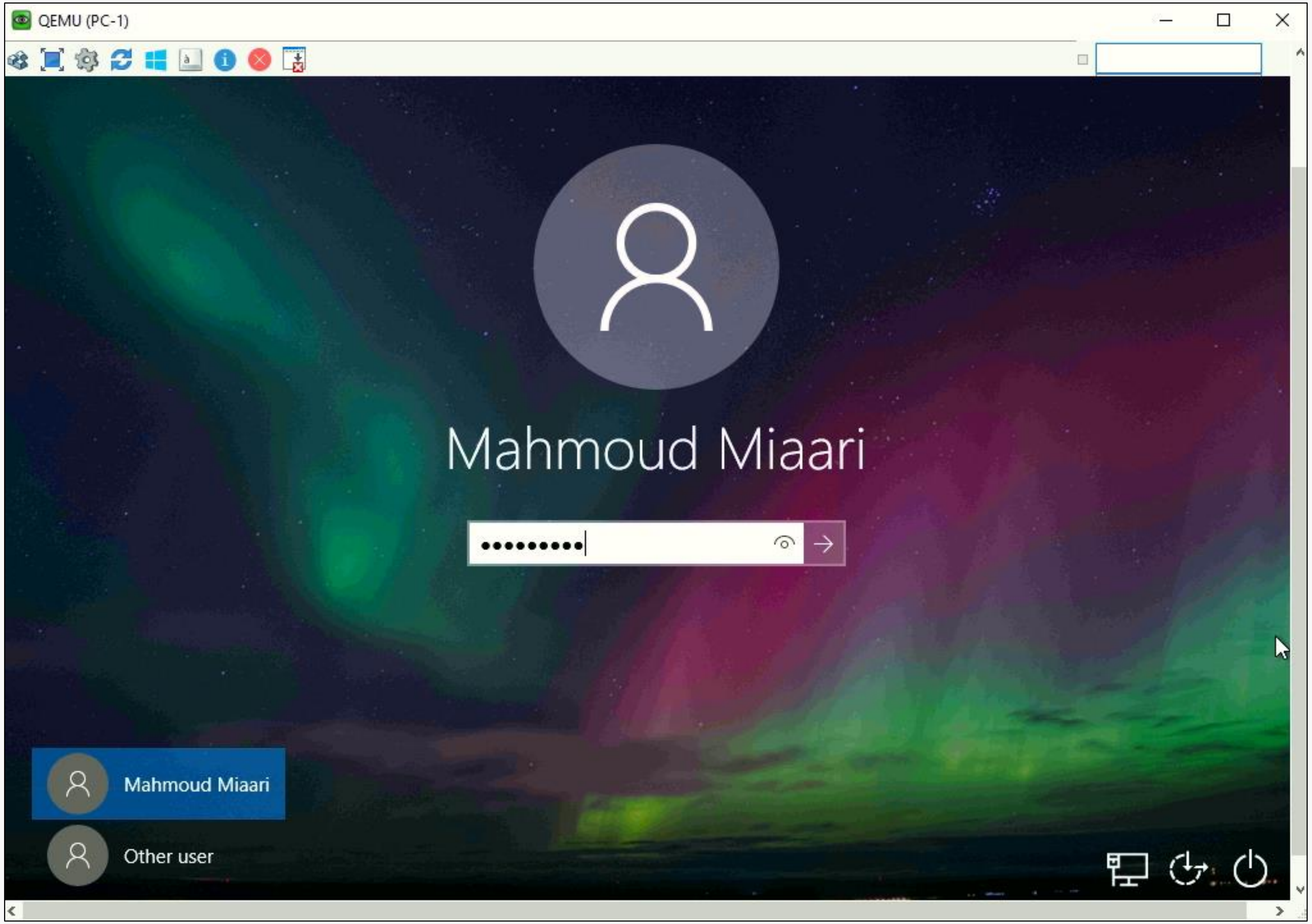
Source: all, adam, miaari, zainab

Destination: all

User Authentication Login Verification via RADIUS Server (NPS)

User Login to PC

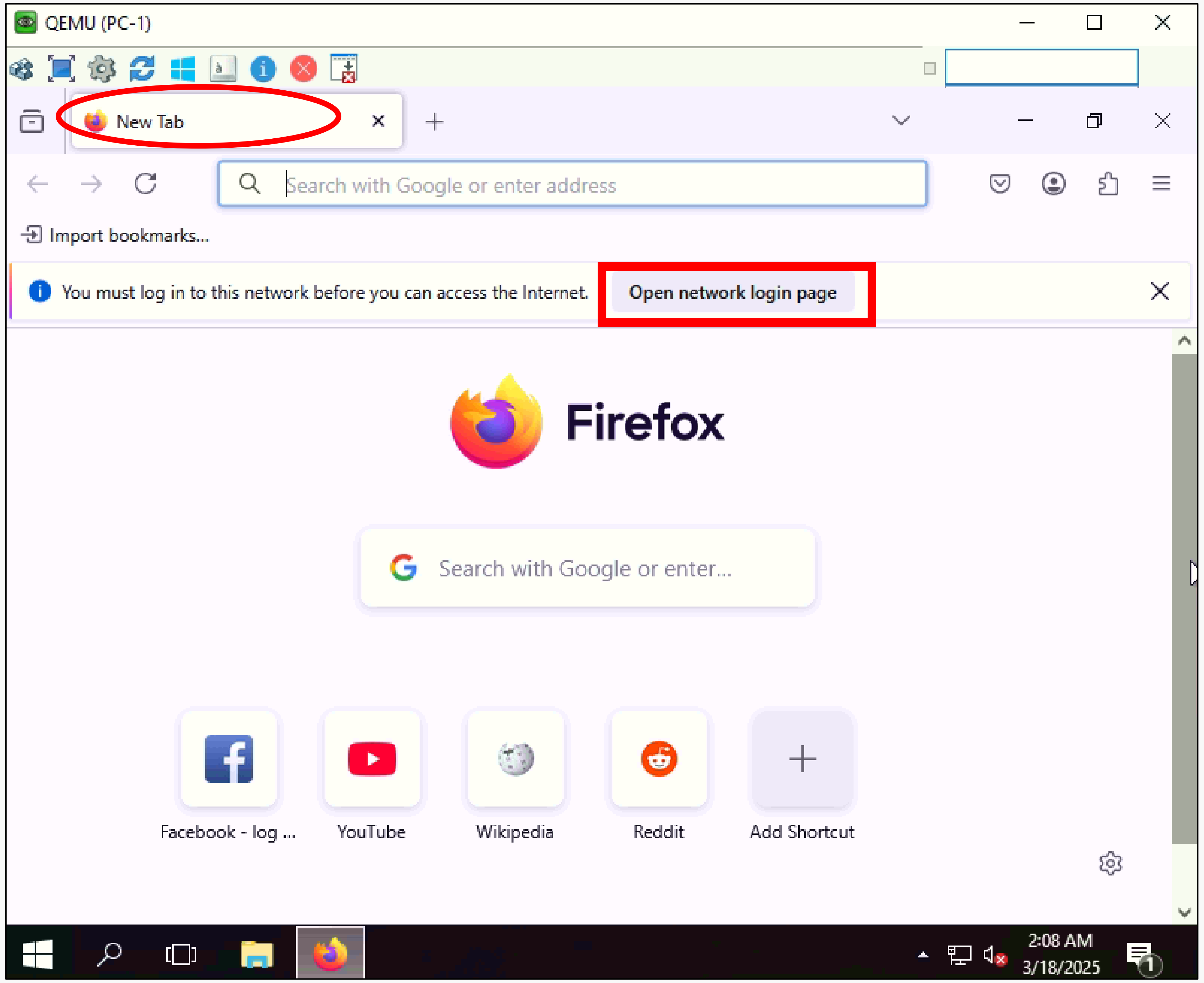
- The user Mahmoud Miaari eht sretne nigol swodniW eht no slatinederc niamod ercsen.
- Login is successful due to RADIUS server (NPS) authentication.



User Authentication Login Verification via RADIUS Server (NPS) Cont..

Open Browser for Internet Access

- Open Firefox browser.
- Notice the message: *"You must log in to this network before you can access the Internet."*
- Click on *"Open network login page"*.



QEMU (PC-1)

New Tab

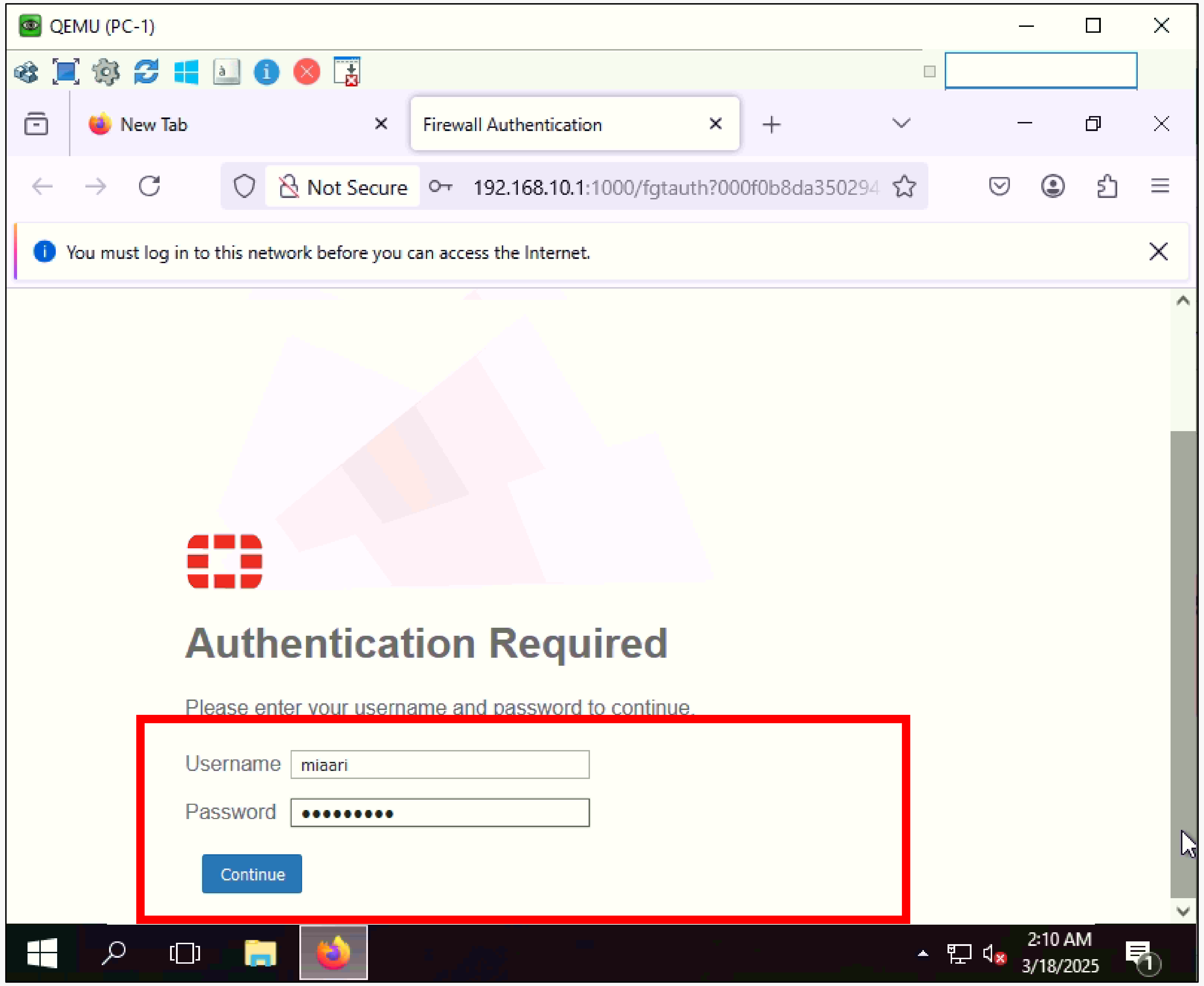
Search with Google or enter address

Import bookmarks...

You must log in to this network before you can access the Internet. Open network login page

RADIUS Authentication Prompt

- The FortiGate firewall redirects to the captive portal authentication page.
- Enter the Username: `miaari` and Password.
- Click *Continue*.



QEMU (PC-1)

New Tab | Firewall Authentication

Not Secure 192.168.10.1:1000/fgtauth?000f0b8da350294

You must log in to this network before you can access the Internet.

Authentication Required

Please enter your username and password to continue.

Username: miaari

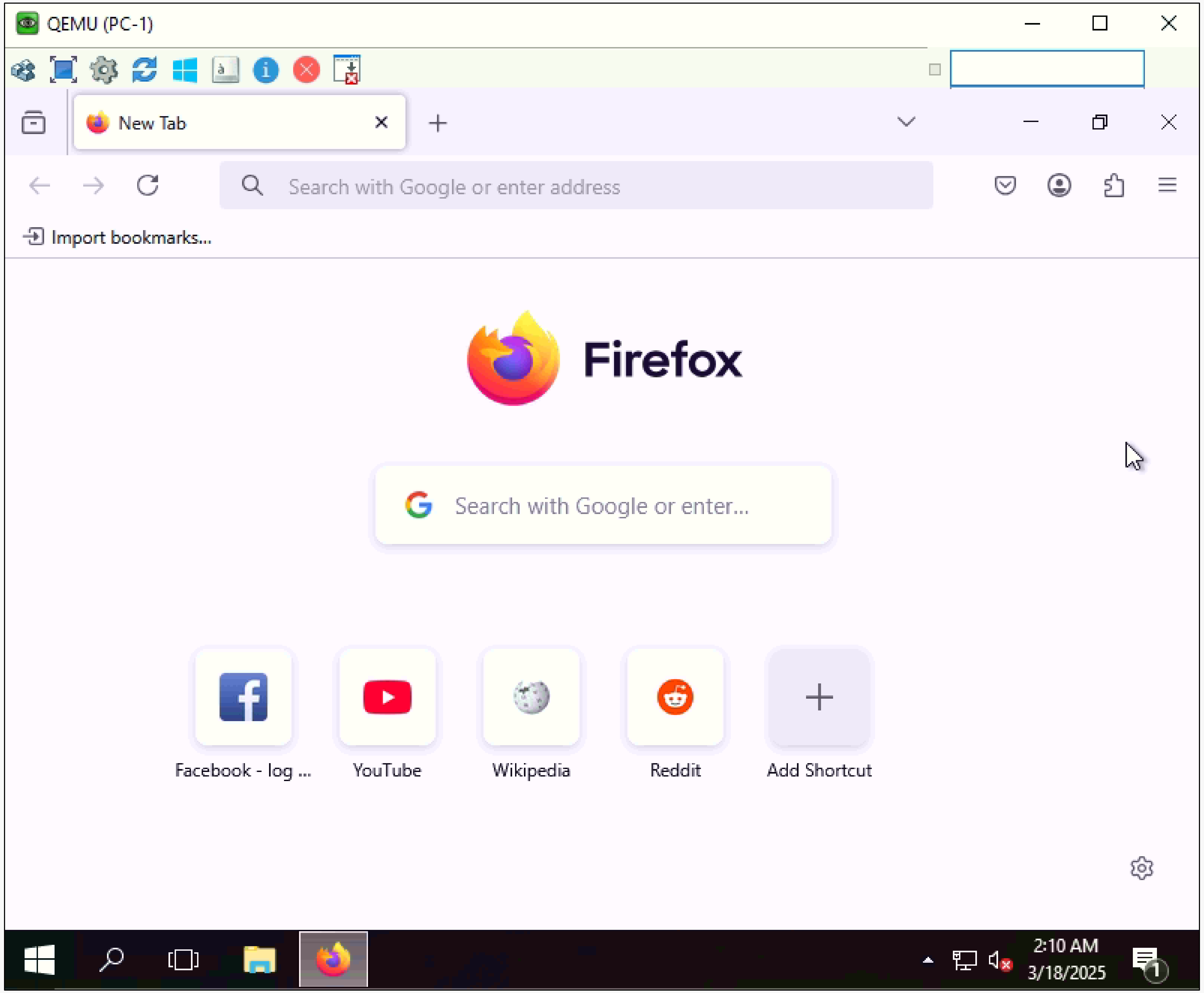
Password: •••••••••

Continue

User Authentication Login Verification via RADIUS Server (NPS) Cont..

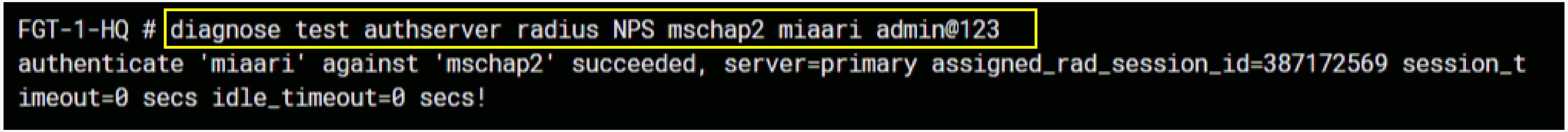
Successful Internet Access

- After successful authentication, the user gains internet access.
- The browser now opens and displays the default homepage without restrictions.



Testing RADIUS Server Authentication Using Diagnose Command in FortiGate

- This command output shows that user miaari was successfully authenticated against the RADIUS server (NPS) using mschap2 protocol.



```
FGT-1-HQ # diagnose test authserver radius NPS mschap2 miaari admin@123
authenticate 'miaari' against 'mschap2' succeeded, server=primary assigned_rad_session_id=387172569 session_t
imeout=0 secs idle_timeout=0 secs!
```

Result:

Authentication succeeded — A session ID was assigned confirming that RADIUS server authentication is working properly for the user credentials provided.

Thank you!

WELCOME TO THE
MIAARI ACADEMY VIP COMMUNITY!
GATEWAY TO NETWORKING, SECURITY, AND CLOUD COMPUTING EXCELLENCE
PREMIUM COURSES
HANDS-ON LABS
LIVE EVENTS
MIAARI ACADE

Linkedin linkedin-MiaariAcademy

miaariacademy.com

miaariacademy@gmail.com

Mahmoud Miaari

Facebook-MiaariAcademy

Miaari Academy Community