



PHASE 12: Setup the NPS Server (RADIUS)

 Server: DC01 (Windows Server 2022 – Active Directory Domain Controller)

 Purpose: Enable RADIUS-based certificate authentication (802.1X) for enterprise Wi-Fi

 Real-World Note:

In production, NPS should ideally be hosted on a separate dedicated server for load balancing and security reasons. But in this lab, we'll proceed on DC01 due to resource constraints.

I. Install NPS (Network Policy Server) Role on DC01

Actions Completed:

Step 1: Open Server Manager

- Log into DC01 as a Domain Admin
- Click Start → Search for “Server Manager” → Open it

Step 2: Add Roles and Features

- In Server Manager → Click Manage (top-right) → Add Roles and Features
- Click Next on the “Before you begin” screen

Step 3: Select Installation Type

- Select: "Role-based or feature-based installation" → Click Next

Step 4: Select Destination Server

- Choose: “DC01.dipeshcorp.local” → Click Next

Step 5: Select Server Roles

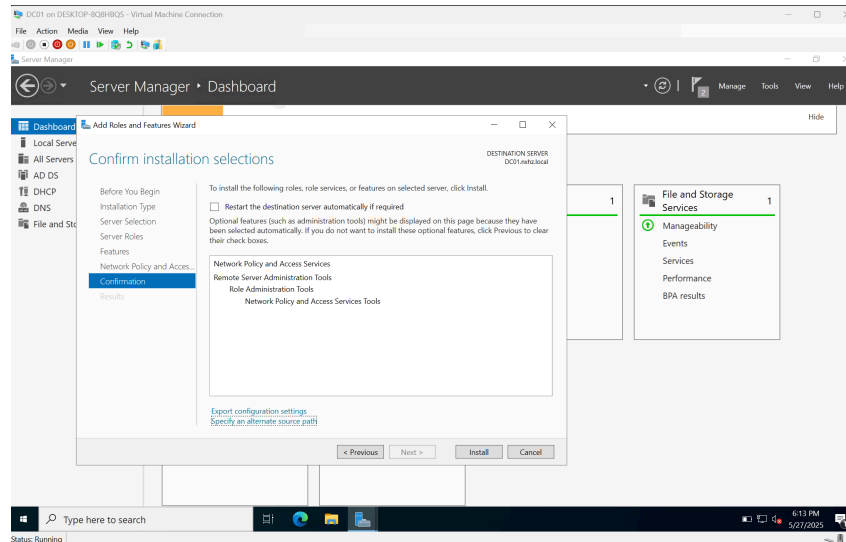
- Scroll down and check:
 - Network Policy and Access Services
 - A popup will appear → Click “Add Features”
- Click Next

Step 6: Skip Features Page > Click Next (no changes on “Features” page)

Step 7: Confirm Role Services

- On "Role Services" screen, ensure: Network Policy Server (checked by default)
- Click Next → Confirm → Click Install

⚠ Note: Do NOT reboot yet, continue after install completes.



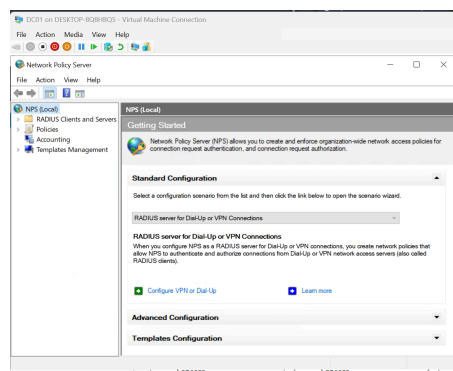
Step 8: Verify NPS Installation

Once the installation is complete:

- Go to Start → Search: nps.msc → Open “Network Policy Server” console

Or: Start → Administrative Tools → Network Policy Server

If it opens without error, the installation succeeded.

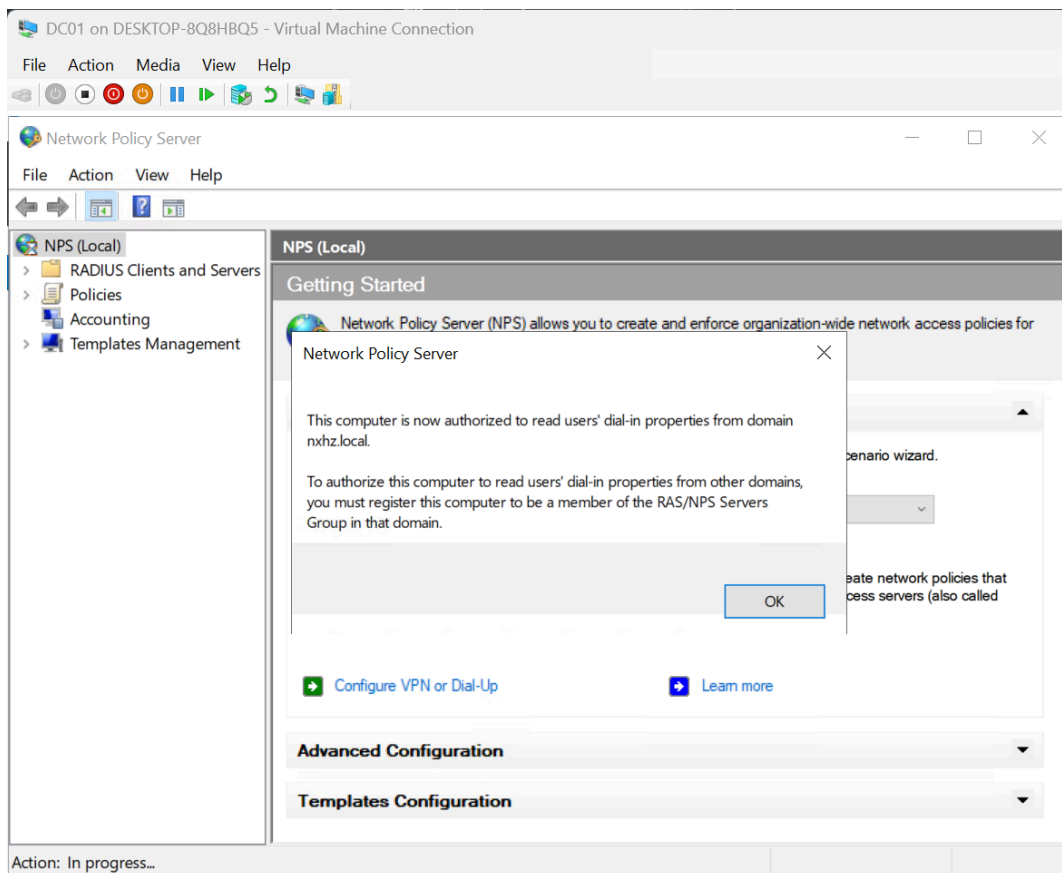


II. Register NPS Server in Active Directory

This is required so NPS can query user/group info from AD.

Actions Completed:

1. Open the NPS Management Console: Start → Run → nps.msc
2. In the left pane, right-click on "NPS (Local)" → Select: Register server in Active Directory
3. A prompt appears → Click "OK" to confirm registration.
4. Message should read:
"The server was successfully registered in Active Directory."



🔗 This step allows NPS to authenticate credentials against the domain (dipeshcorp.local).

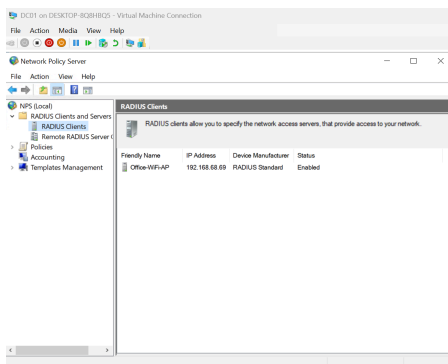
III. Configure RADIUS Clients (Access Points)

This defines which network devices (e.g., Wi-Fi routers) are allowed to send RADIUS authentication requests to your NPS server.

Actions Completed:

1. In the NPS console:
 - Expand: “RADIUS Clients and Servers” → Right-click “RADIUS Clients” → Select “New”
2. Fill in the following:

Field	Value
Friendly Name	Office-WiFi-AP
Address (IP/Name)	192.168.68.69 (Your AP's IP)
Shared Secret	Set a strong password (e.g., R@dius123!)
Confirm Secret	Same as above
3. Click OK.



⚠ Note:

- You'll enter the same Shared Secret into your Wi-Fi AP's RADIUS settings.
- For added security, you can restrict which APs are allowed using IP filtering on the firewall.

IV. Create a Connection Request Policy

This policy determines how incoming RADIUS requests are processed.

Actions Completed:

1. In NPS Console: Expand “Policies” → Right-click “Connection Request Policies” → Click “New”

2. Policy Name: WiFi Connection Policy

3. Conditions:

Click “Add” → Select: NAS Port Type → Wireless - IEEE 802.11

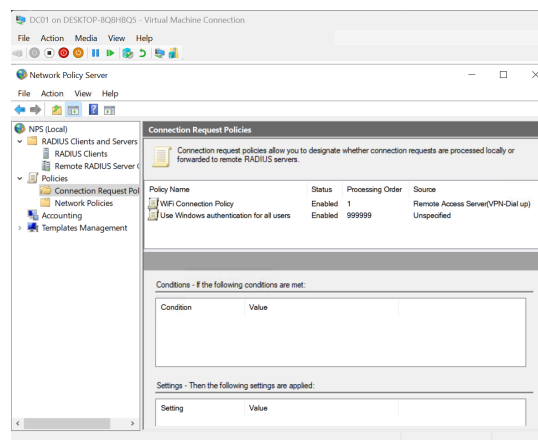
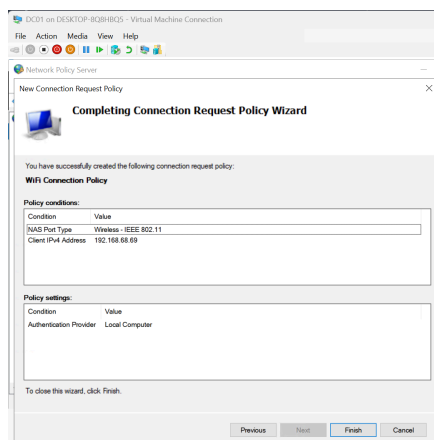
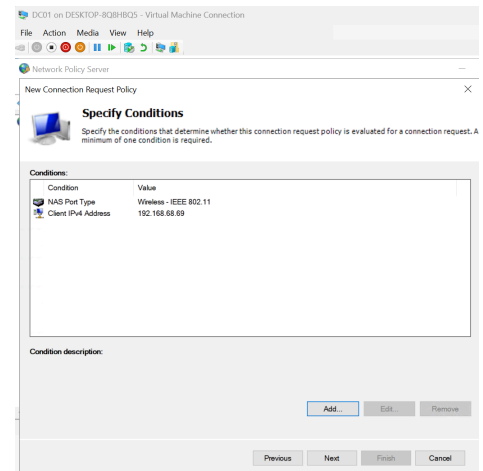
Click “Add” again → Select: Client IPv4 Address → 192.168.1.10

- (This limits requests to only your AP.)

4. Settings:

- Leave default → Make sure “Authentication handled locally > Authenticate requests on this server” is selected

- Click “Next” until the Finish page → Click “Finish”



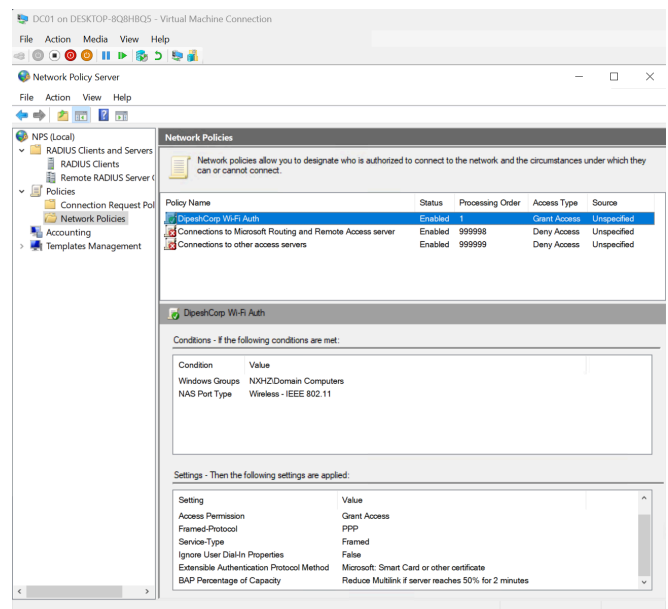
🎯 This ensures only Wi-Fi RADIUS requests from your AP get processed by this server.

V. Create a Network Policy (Main Authentication Logic)

This is the core policy that determines who can connect and under what conditions.

Actions Completed:

1. Go to “Policies” → Right-click “Network Policies” → Click “New”
2. Policy Name: DipeshCorp Wi-Fi Auth
3. Conditions: Click “Add” → Choose: Windows Group → Domain Computers
→ Add: dipeshcorp\Domain Computers (or a custom security group for Wi-Fi devices)
 - Click “Add” → Select:NAS Port Type → Wireless - IEEE 802.11
4. Constraints: Go to “Authentication Methods”:
 - Click “Add” → Choose: Microsoft: Smart Card or other certificate
 - Uncheck other options (PAP, MS-CHAPv2, etc.)
5. Settings:
 - “Access granted”
 - “Ignore user dial-in settings”
6. Click “Next” → “Finish”



Security Tip:

- If you want different behavior for user-authenticated Wi-Fi, create a second policy targeting “Domain Users”.
-

V. Completion Outcome:

Successfully installed the Network Policy and Access Services role on the DC01 server, specifically enabling the Network Policy Server (NPS) and RADIUS Server for 802.1X features. The installation was completed using Server Manager with default selections, followed by a system verification ensuring all required services and dependencies were active. This step lays the groundwork for implementing RADIUS-based enterprise Wi-Fi authentication through centralized access control.