bts >>
cloud computing

# Lab 8 Windows Services: VPN + DirectAccess


**Course / Module:** OSYCL-Windows
**School:** Lycée Guillaume Kroll
**Class:** BCLC25
**Team Members:**

- Moshe Sarkis Marios
- Donovan Glodt

**Teacher:** SPAGNUOLO Maurizio
**Consultant Company**: DON&SAR IT
**Client Company :** Flowdesk

Lycée Guillaume Kroll

Table of Contents

1. Project overview ..... 3
1.1 Client background ..... 3
1.2 Business need ..... 3
1.3 Project objective ..... 4
Virtual Private Network (VPN) ..... 4
Direct Access ..... 4
1.4 High-level scope ..... 5
1.5 Success criteria ..... 6
2. Implemented Solution Overview and Functionality ..... 7
2.1 Overview of the implemented infrastructure ..... 7
2.2 Active Directory Domain Services (AD DS) ..... 7
Function: ..... 7
2.3 File Server and Shared Resources ..... 8
Implemented shares include: ..... 8
Function: ..... 8
2.4 Roaming Profiles (Employees) ..... 8
How it works: ..... 8
Purpose: ..... 8
2.5 DirectAccess (Internal Employees) ..... 9
Key characteristics: ..... 9
How it works: ..... 9
Purpose: ..... 9
2.6 VPN Access for External Clients ..... 10
Key characteristics: ..... 10
Purpose: ..... 10
2.7 Network Policy Server (NPS) ..... 10
How it works: ..... 10
Purpose: ..... 10
2.8 Security and Access Control ..... 11
2. 9 Conclusion ..... 11

3. Installation ..... 12
3.1 Initial Setup ..... 12
Server: ..... 12
VPN_Client: ..... 12
DA_Client: ..... 12
3.2 Configuring the network of the server ..... 13
3.3 Adding the Active Directory Domain Services role ..... 14
3.4 The AD DS Configuration ..... 15
3.5 Setting up the AD UC hierarchy ..... 16
3.6 Installing the Remote Access Role ..... 17
3.7 Setting up DirectAccess ..... 19
3.8 Setting up the DirectAccess Client ..... 21
3.9 Setting up VPN ..... 25
3.10 Setting up the VPN Client ..... 30

# 1.Project overview

## 1.1 Client background

**Flowdesk** is a small **startup company focused on business services and project management**, with **5 employees**. The company uses IT systems mainly to support daily operations such as document management, collaboration with clients, and internal administration. While the company relies heavily on technology, **they do not have dedicated in-house IT specialists** capable of designing and securing a Windows Server–based infrastructure.

To support their growing business and remote working needs, Flowdesk decided to outsource the design and implementation of their Windows Server environment to **DON&SAR IT**, an external IT consulting company specialized in Microsoft Windows infrastructures and secure remote access solutions.

## 1.2 Business need

**Flowdesk** has **two distinct remote-access audiences**:

1. **Employees (internal users)**
   Employees need a secure, "always available" connection from home so they can work as if they were in the office. Flowdesk also wants user settings and data to follow the employee across sessions using **roaming profiles**. For security and control, the company requires that **only company-approved, domain-joined laptops** can access the corporate network remotely.
2. **External clients (non-employees)**
   Flowdesk collaborates with external clients who need access to **specific shared files only**. These clients connect securely via **VPN authenticated by a local NPS**, which ensures that only approved non-employee users can access the restricted resources.

## 1.3 Project objective

Our group will design and implement a remote access solution that provides:

- **DirectAccess** for employee laptops (approved devices only) with access to internal resources and **roaming profiles**.
- **VPN access** for external clients limited to predefined shares, enforced through local **NPS authentication** and **Active Directory** group-based access control,

### Virtual Private Network (VPN)

A **Virtual Private Network (VPN)** is a remote access technology that establishes a **secure, encrypted tunnel** between a user device and the organization's internal network over the public internet. Once authenticated, the remote user can access authorized internal resources (for example, file shares or specific servers) as if they were connected from within the office. VPN access is typically **user-initiated** (the user manually connects using credentials) and can be tightly controlled through authentication policies and group-based permissions, making it well suited for **external partners or clients** who require limited access to specific services.

### Direct Access

**Direct Access** is a Microsoft remote access solution that provides **automatic, always-on connectivity** for **domain-joined, organization-managed computers**. Unlike traditional VPNs, DirectAccess does not require the user to manually start a connection; when an approved device has internet access, it automatically establishes a secure connection to the corporate network. This enables employees to access internal services (such as file servers and domain resources) seamlessly and supports centralized management scenarios, including **Group Policy** application and profile access while working remotely. DirectAccess is therefore best suited for **employees using company-approved laptops**, where the organization needs consistent security and device control.

## 1.4 High-level scope

This table gives a clear summary of the project limits and deliverables. It separates what is included in the work from what is not included, so both the client and DON&SAR IT have the same expectations about what will be delivered.

| In scope | Out of scope |
|---|---|
| Active Directory groups and policies to separate employee's vs external clients | High availability / redundancy |
| Direct Access configuration for approved employee laptops | Multi-site deployments/servers |
| VPN configuration for external clients with restricted access | Advanced PKI infrastructure beyond what's needed for the lab |
| File shares and NTFS permissions (internal vs client-only areas) | Mandatory profiles for the externals |
| Roaming profiles (employees) and mandatory profiles (external clients) | / |
| Basic validation tests and documentation for handover | / |

## 1.5 Success criteria

- Approved employee laptops automatically and securely reach internal file resources from home via **DirectAccess**.
- Employee **roaming profiles** load correctly when working remotely.
- External clients can connect via **VPN** and access **only** the permitted client share(s).
- Access is blocked for non-approved devices/users.

# 2.Implemented Solution Overview and Functionality

## 2.1 Overview of the implemented infrastructure

To meet the requirements of the client, DON&SAR IT designed and implemented a **Windows Server–based remote access infrastructure** that allows secure internal and external access to company resources. The solution is based on a **centralized on-premise Windows Server environment** using Active Directory, file services, profile management, and secure remote access technologies.

The implemented solution separates **internal employees** and **external clients** to ensure security, control, and ease of management.

## 2.2 Active Directory Domain Services (AD DS)

A Windows Server was configured as a **Domain Controller**, providing **Active Directory Domain Services (AD DS)** and **DNS**. This allows centralized management of:

- User accounts
- Computer accounts
- Security groups
- Authentication and authorization

Users and computers are organized into **Organizational Units (OUs)**, and security groups are used to control access to resources and remote access methods (DirectAccess or VPN).

### Function:

AD DS ensures that all authentication is centralized and secure, and that access rights are consistently applied across the environment.

## 2.3 File Server and Shared Resources

A dedicated **File Server** was implemented to store and share company data. Shared folders are protected using **NTFS permissions** and **security groups**.

### Implemented shares include:

- Internal company data (employees only)
- Restricted client delivery folders (external clients only)
- Profile storage locations

### Function:

This ensures that users only access the data they are authorized to see, following the **principle of least privilege**.

## 2.4 Roaming Profiles (Employees)

For internal employees working remotely, **roaming profiles** were implemented. Profile data is stored centrally on the file server and loaded automatically when the user logs in.

### How it works:

- The user's profile is stored on the server
- When logging in (locally or remotely), the profile is downloaded
- When logging off, changes are synchronized back to the server

### Purpose:

This allows employees to keep the same desktop settings, documents, and configuration regardless of location.

## 2.5 DirectAccess (Internal Employees)

DirectAccess was implemented to allow employees to securely access internal resources from home without manually starting a VPN connection.

### Key characteristics:

- Always-on connection
- Only **company-approved, domain-joined laptops** are allowed
- Uses Active Directory group membership to control access

### How it works:

When an approved laptop connects to the internet, it automatically establishes a secure tunnel to the company network. From the user's perspective, internal resources such as file shares are available as if they were in the office.

### Purpose:

DirectAccess provides a seamless and secure remote working experience for employees.

## 2.6 VPN Access for External Clients

A **VPN solution** was configured for external clients who need limited access to specific company files.

### Key characteristics:

- Manual VPN connection
- Access restricted to specific shared folders
- Controlled through Active Directory security groups

### Purpose:

The VPN ensures encrypted communication between external clients and the company server while limiting access strictly to required resources.

## 2.7 Network Policy Server (NPS)

A **local Network Policy Server (NPS)** was implemented to manage authentication and authorization for external VPN connections.

### How it works:

- VPN connection requests are forwarded to NPS
- NPS checks user credentials and group membership
- Only users in the approved external client group are allowed access
- Connection attempts are logged for auditing

### Purpose:

NPS centralizes access control, improves security, and simplifies management of external connections.

## 2.8 Security and Access Control

The overall solution enforces security by:

- Separating internal employees and external clients
- Restricting access through AD groups
- Using encrypted connections (DirectAccess and VPN)
- Applying profile management to control user environments

## 2. 9 Conclusion

The implemented infrastructure provides a **secure, manageable, and scalable remote access solution** tailored to a small business environment. By combining Active Directory, file services, profile management, DirectAccess, VPN, and NPS, DON&SAR IT delivered a solution that meets the client's operational needs while maintaining strong security and simplicity.

# 3.Installation

## 3.1 Initial Setup

For VirtualBox, we created a **NAT Network** to simulate a **WAN/Internet connection** that the server and clients can communicate over.

For this lab setup, we used **one Windows Server** to host **Active Directory**, **VPN**, and **DirectAccess**, along with **two client machines**: one client connects to the network using **VPN**, and the other connects using **DirectAccess**.

### Server:

- Windows 2022 Server
- Name: STBServer
- 2 Network cards
    - One connected to LAN
    - The other connected to a NAT Network (WAN)¨

### VPN_Client:

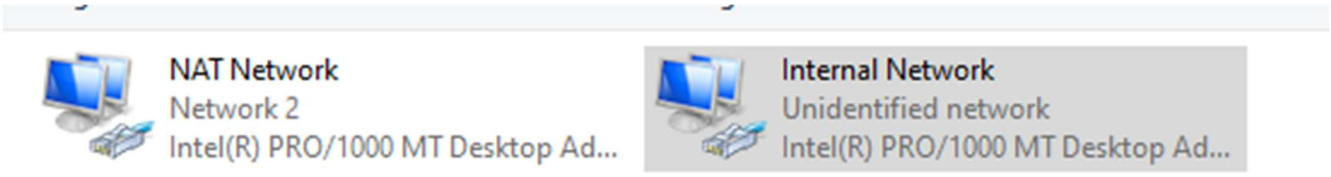
- Windows 10 Enterprise Client
- PC Name: VPNClient
- Connected to the WAN

### DA_Client:

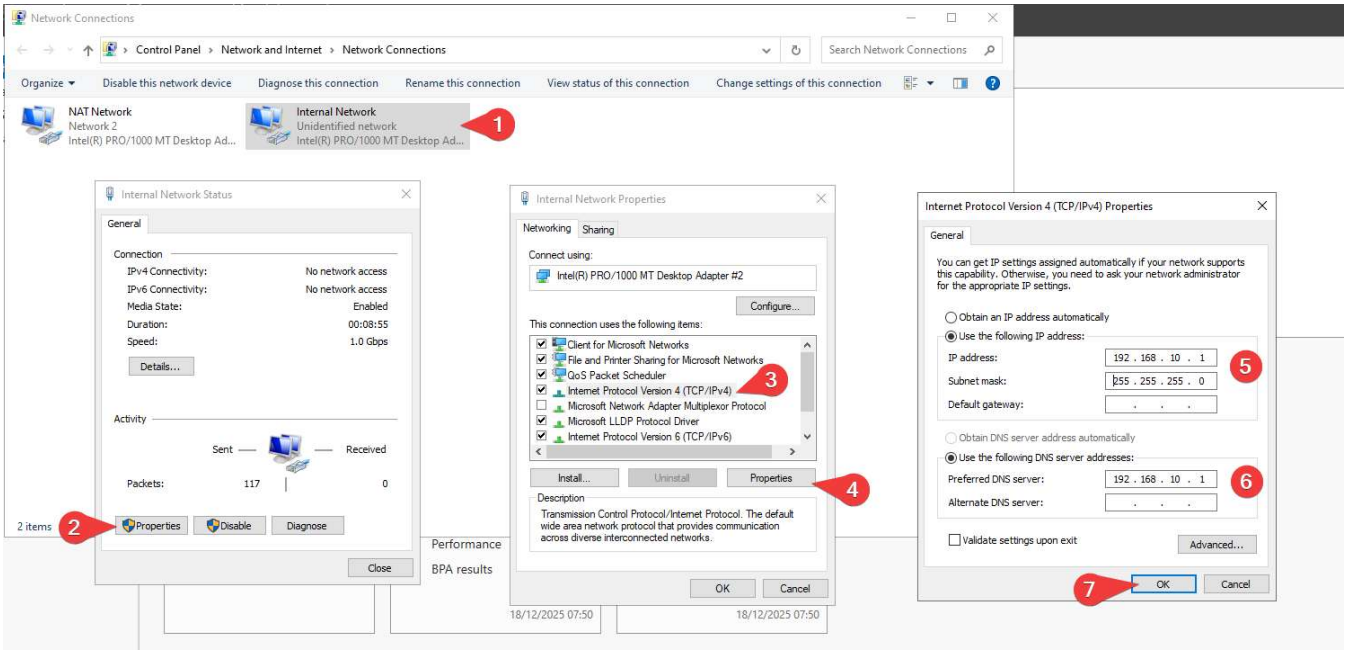
- Windows 10 Enterprise Client
- PC Name: DAClient
- First connected to the LAN for joining to the domain
    - After connected to the WAN

## 3.2 Configuring the network of the server

We first configure the network adapters to the correct names.



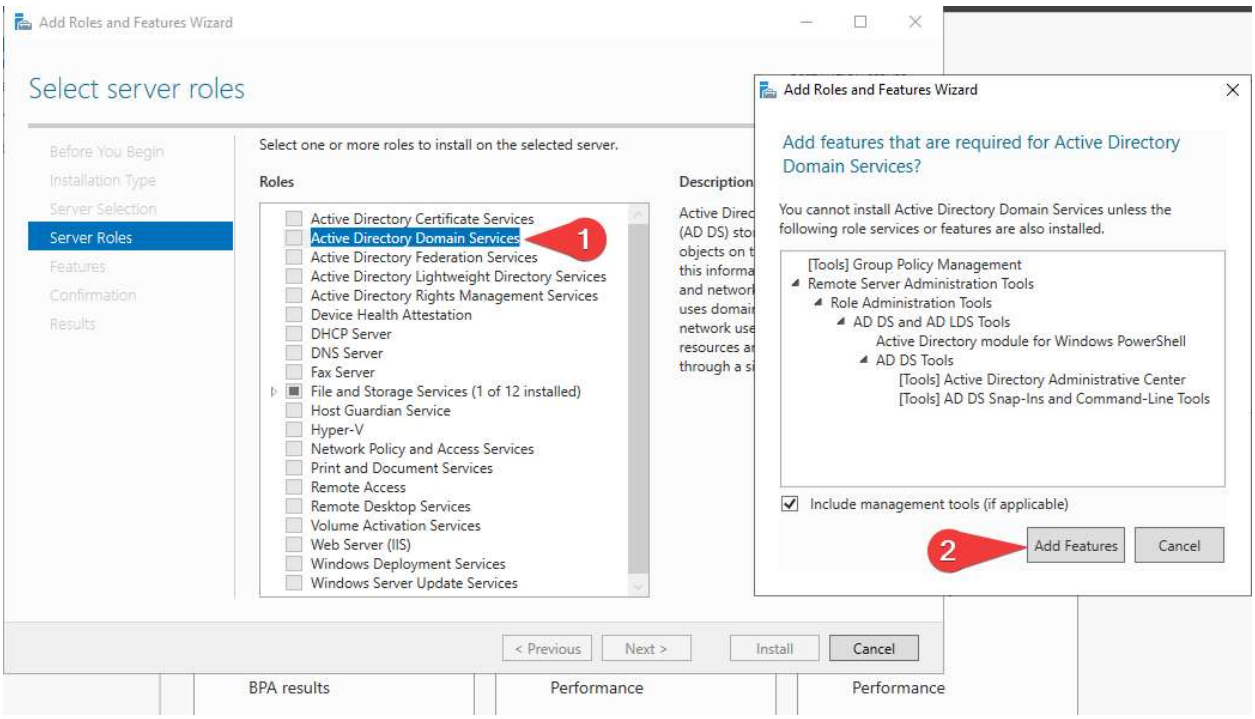

Then we configure the IP address of the Internal Network to a static IP address.



## 3.3 Adding the Active Directory Domain Services role

Manage → Add Roles and Features

Then click next, since we only have 1 server we don't need to select a specific server.

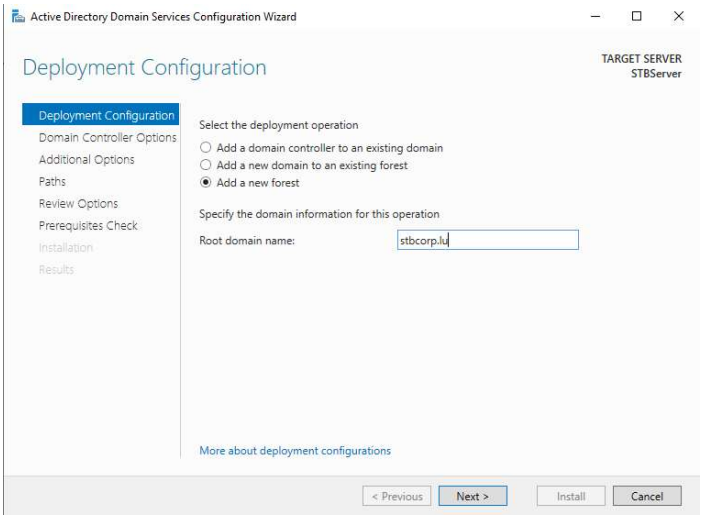


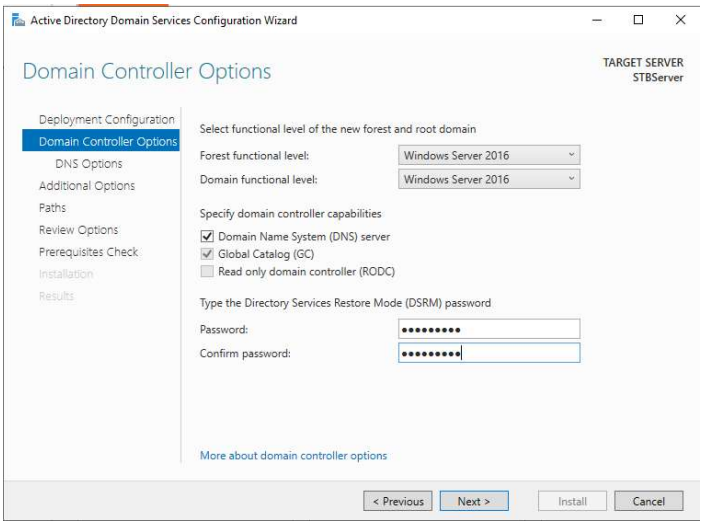

Then we add the Active Directory Domain Services role and add its respective features.

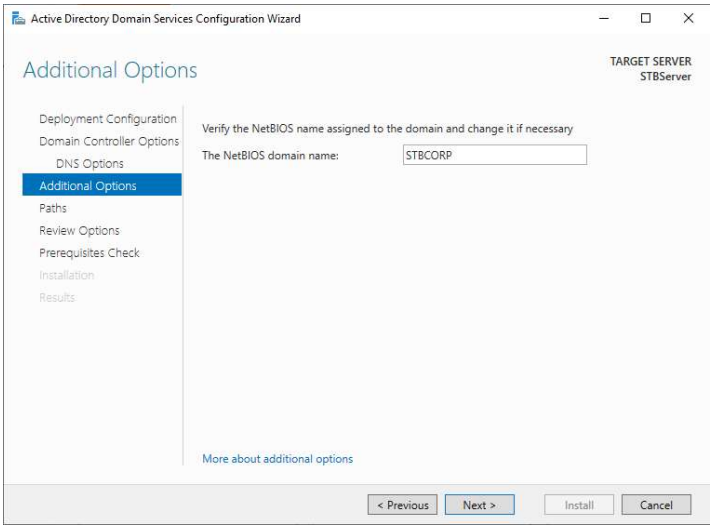
Click next until install.

Click the notifications for the post-deployment

## 3.4 The AD DS Configuration

1. 

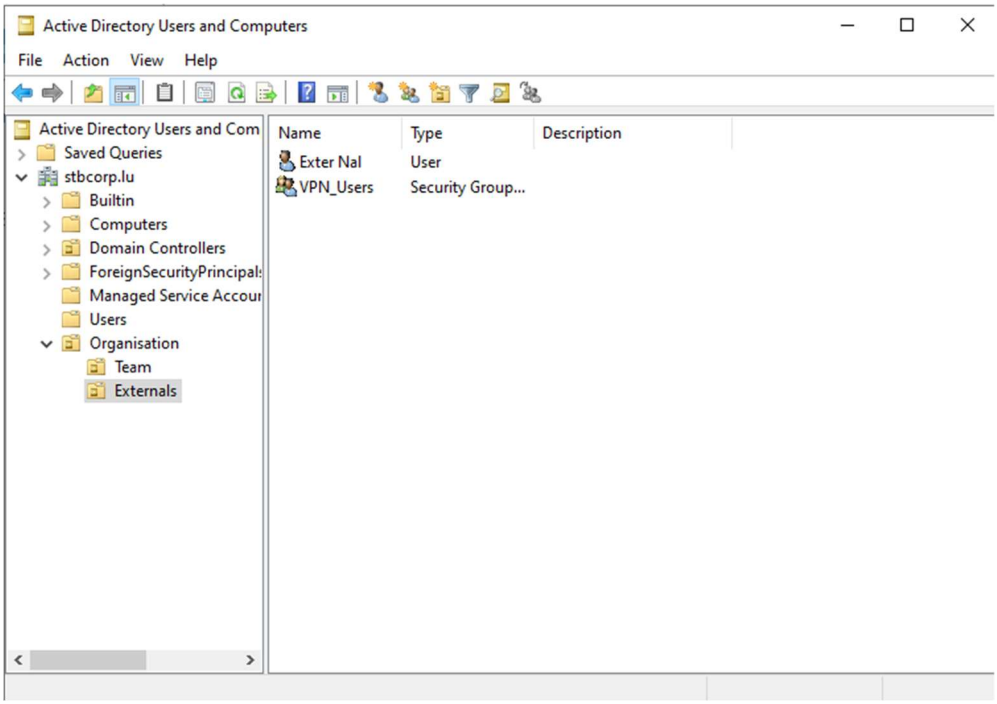

2. 

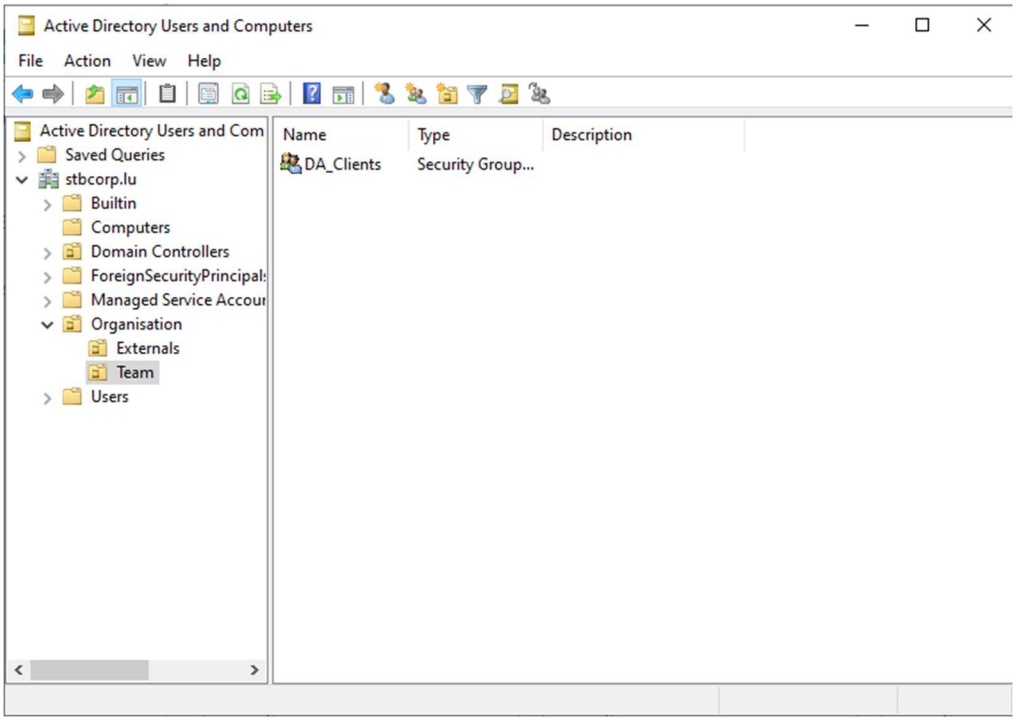

3. 


After installing → Reboot

## 3.5 Setting up the AD UC hierarchy

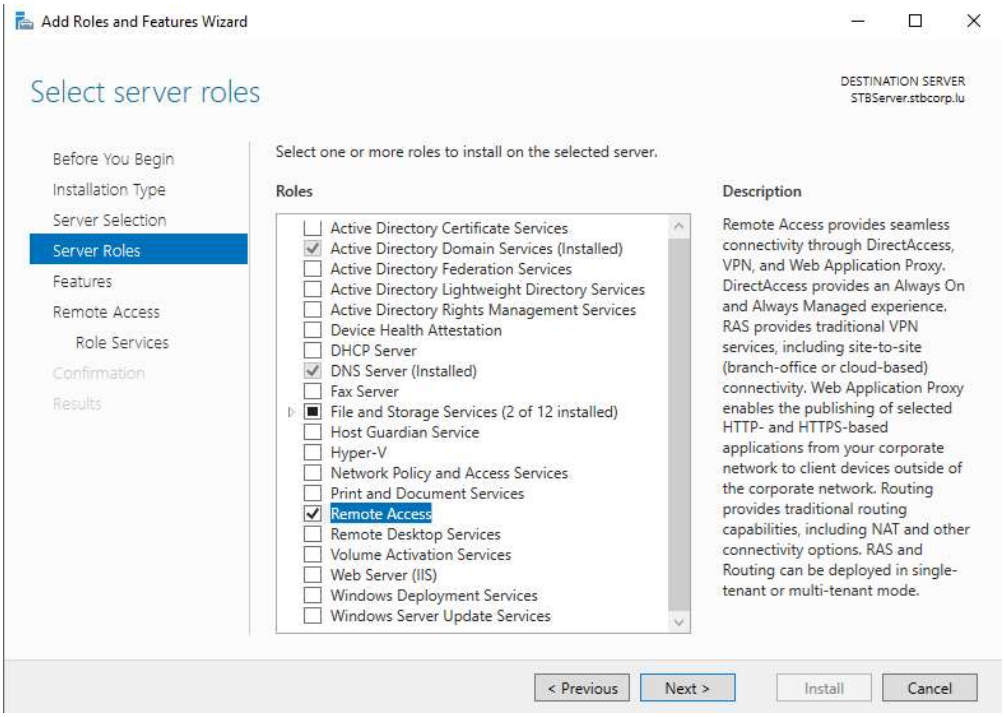
We will have 2 security groups, one for the VPN users and another for the DirectAccess clients, along with one VPN user for now.



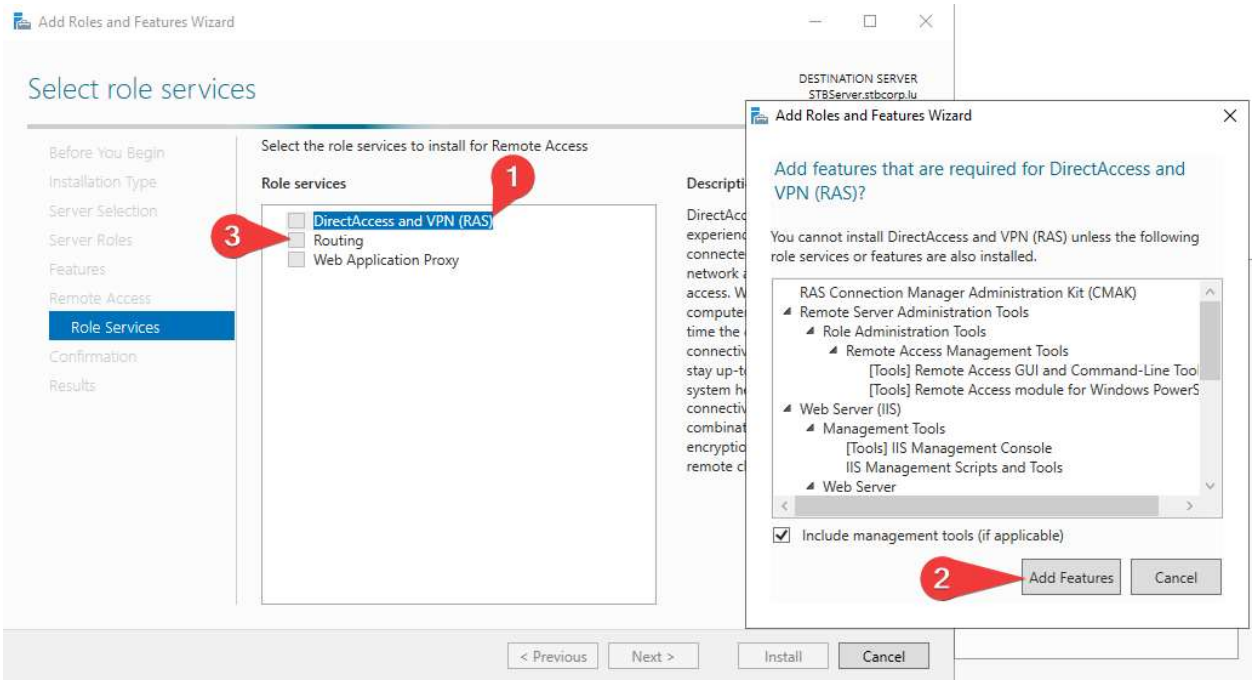



## 3.6 Installing the Remote Access Role

Manage → Add Roles and Features



We want to add the Remote Access role.




At Role Services we want to add in DirectAccess and VPN, add its features.

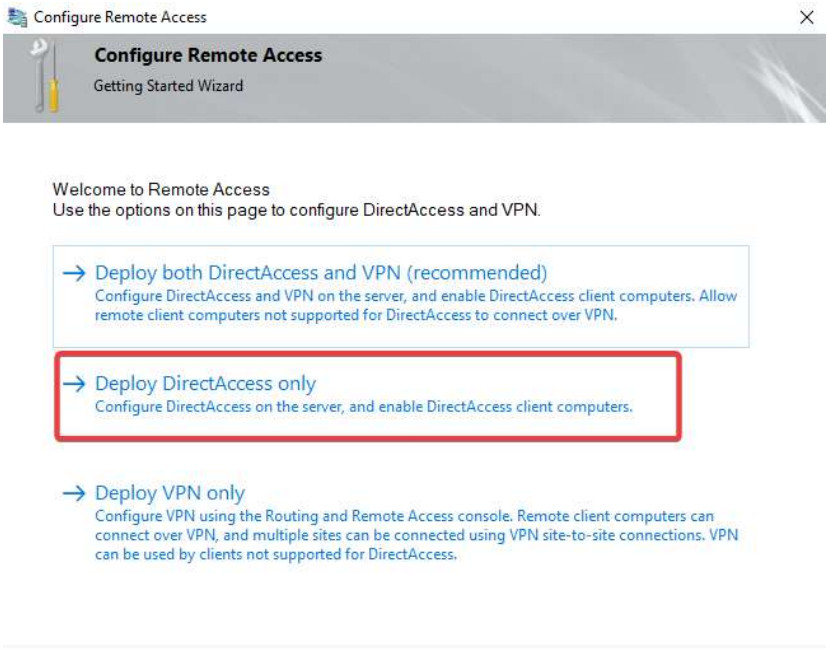
Then add Routing.

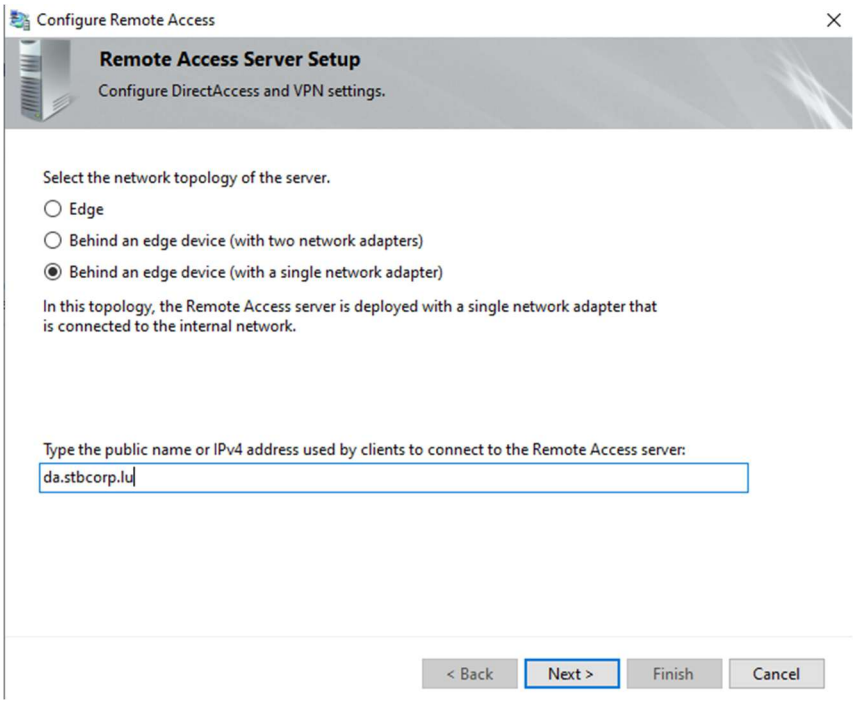
Web Server Roles (ISS) will also be installed along. Click next until install.

Notifications → Post-Deployment Configuration → Open the Getting Started Wizard.

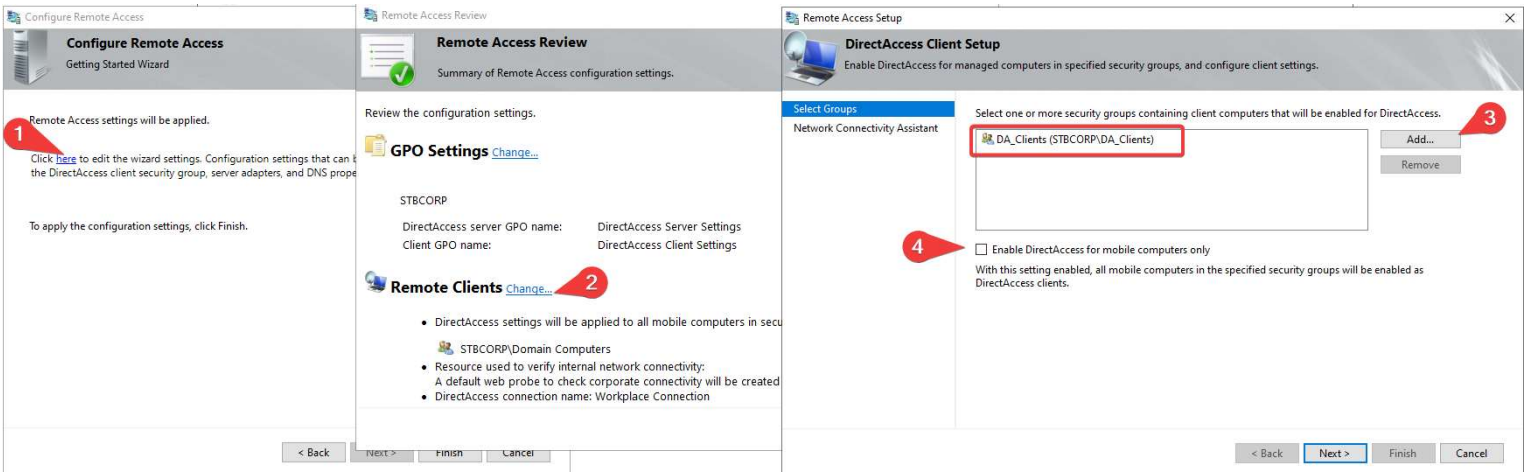
## 3.7 Setting up DirectAccess

For simplicity we will first configure DirectAccess before VPN.



We configure DirectAccess

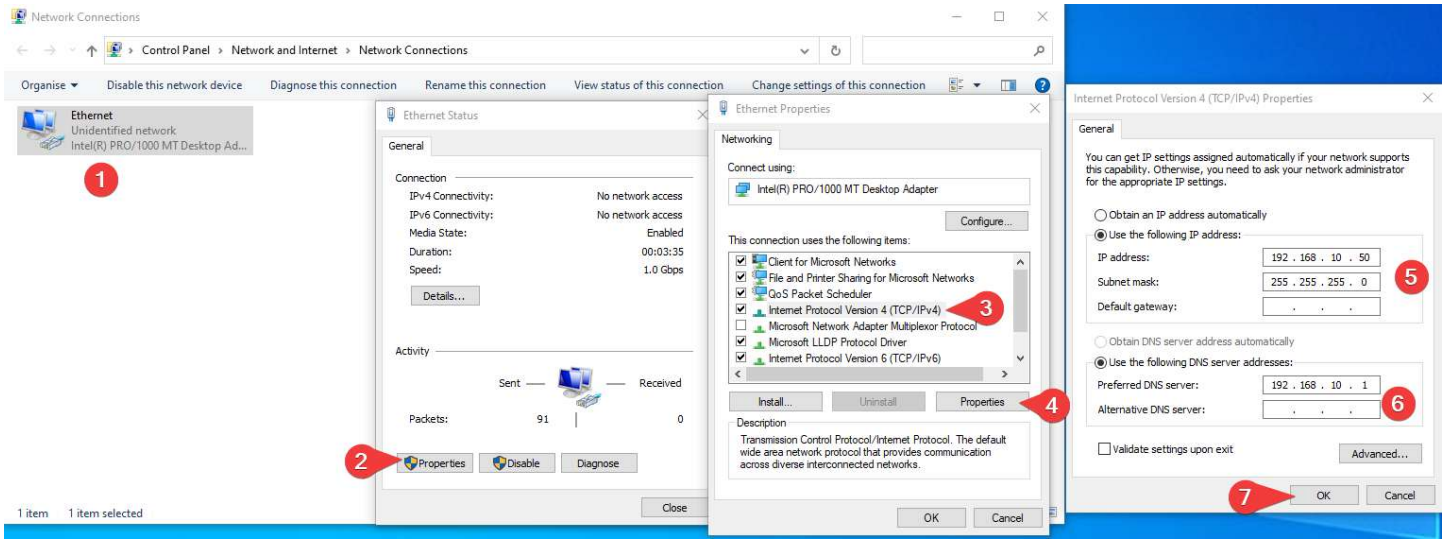



We change the Remote Clients to be our DAClients that we made.

We finish the configuration.

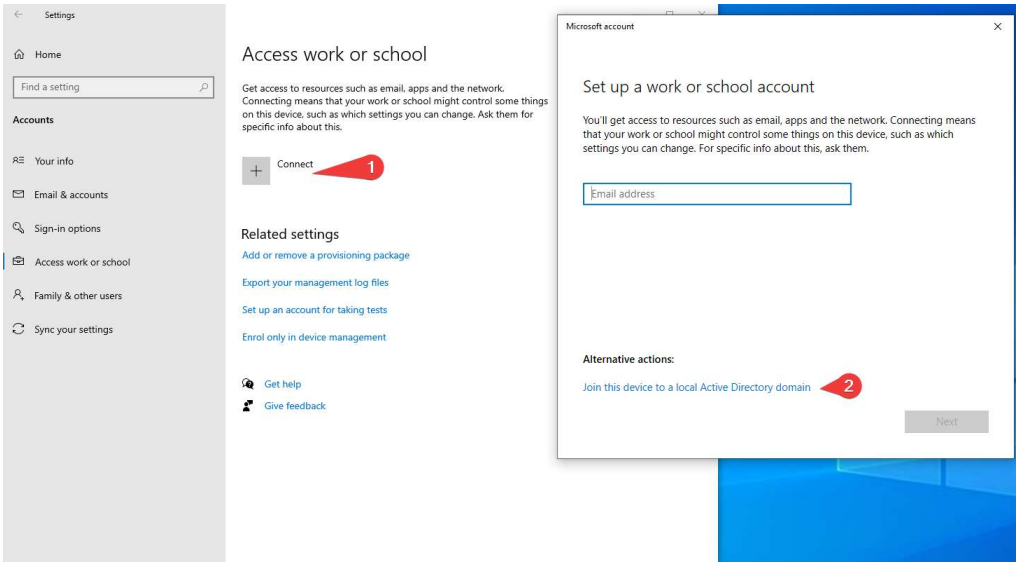
## 3.8 Setting up the DirectAccess Client

We set the Client to be in the same network as the server




Next we join the domain with the client.

In Settings go to Accounts → Access work or school

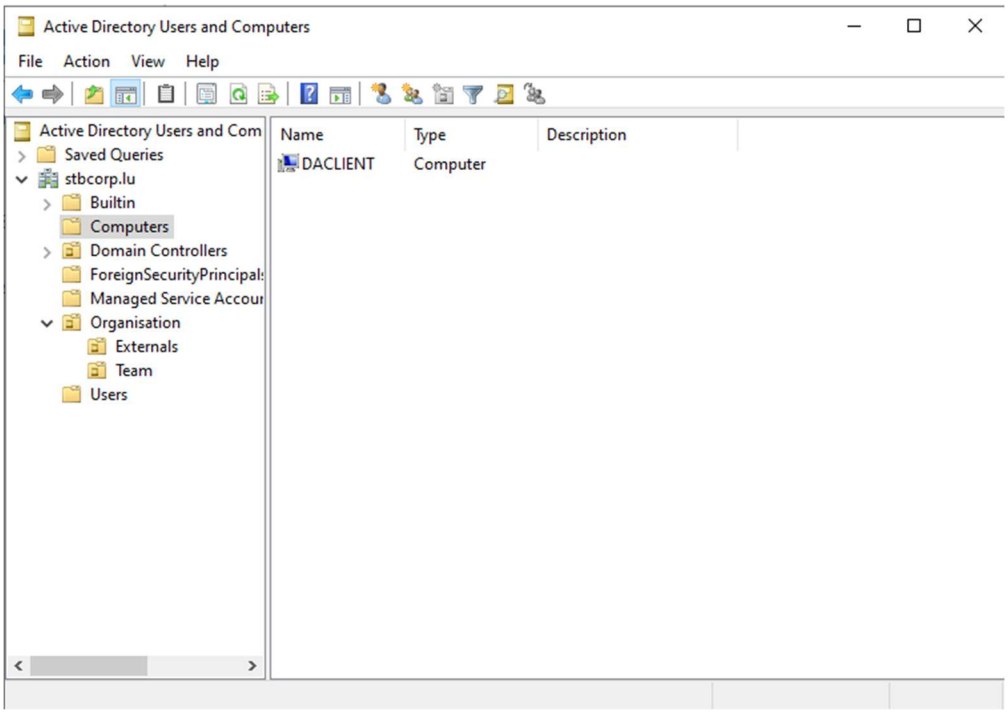



Then log in to your Administrator account from your server.

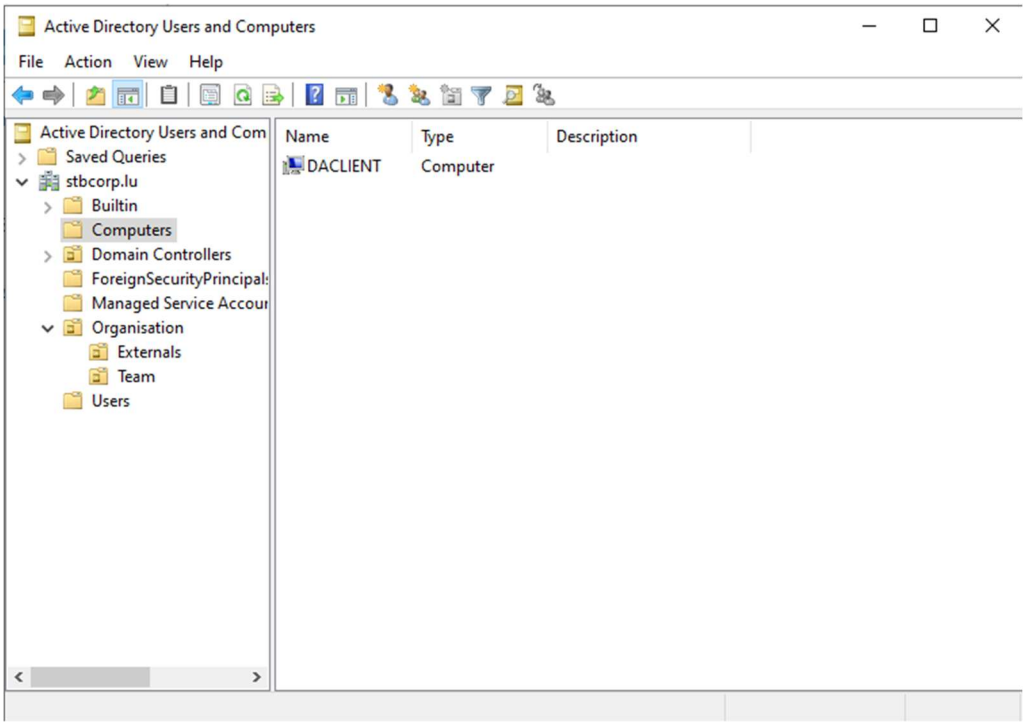
Skip the account creation.

Reboot and your client will be domain joined.

On your server you will find the Client Computer in the AD UC.



Then you want to add this Client to your DA_Clients group.

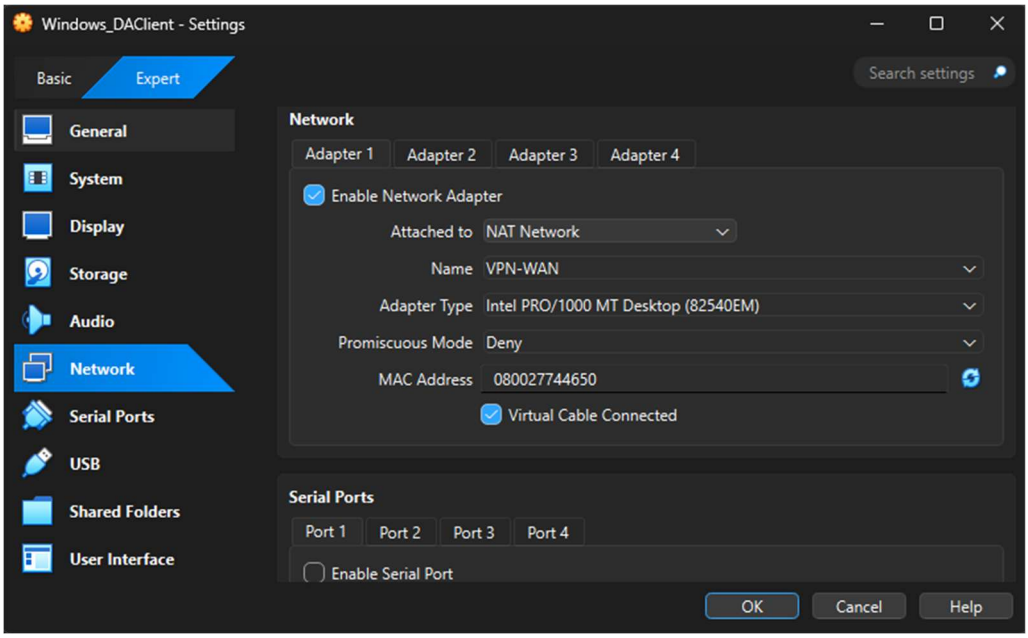



Add a test user for DirectAccess on your Server to log into with your client

On you client run the command: “gpupdate /force” to update the GPO on it

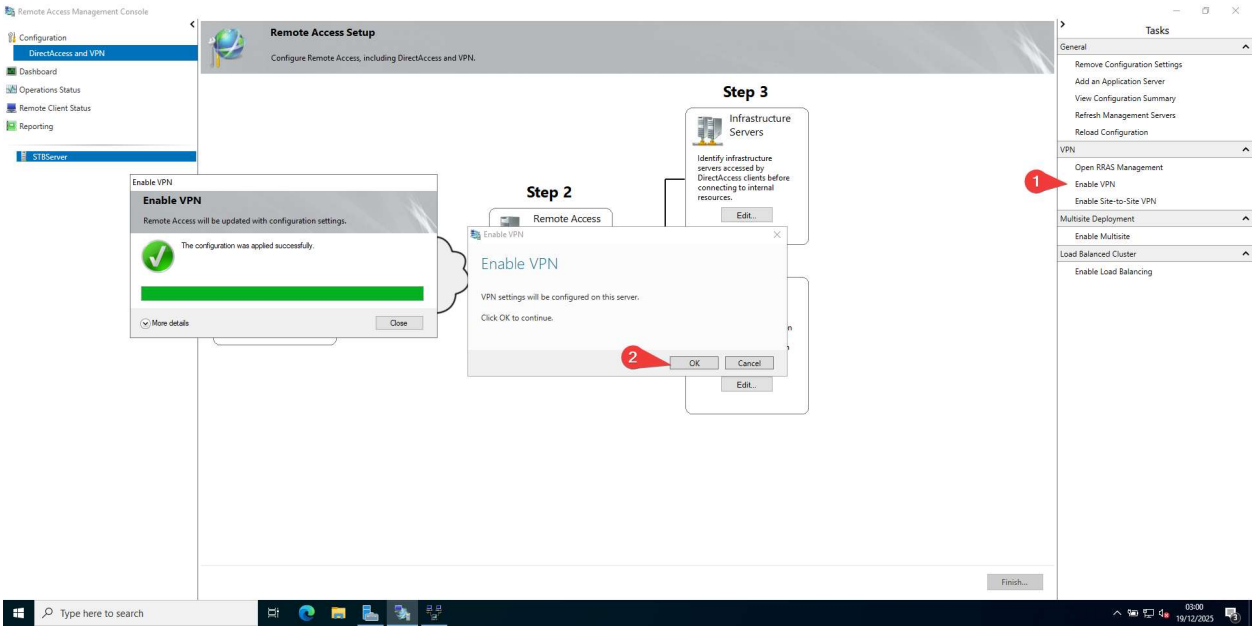
Shut down your DirectAccess client and change it network to the WAN

Now you should be able to connect to the Server with the client.



## 3.9 Setting up VPN

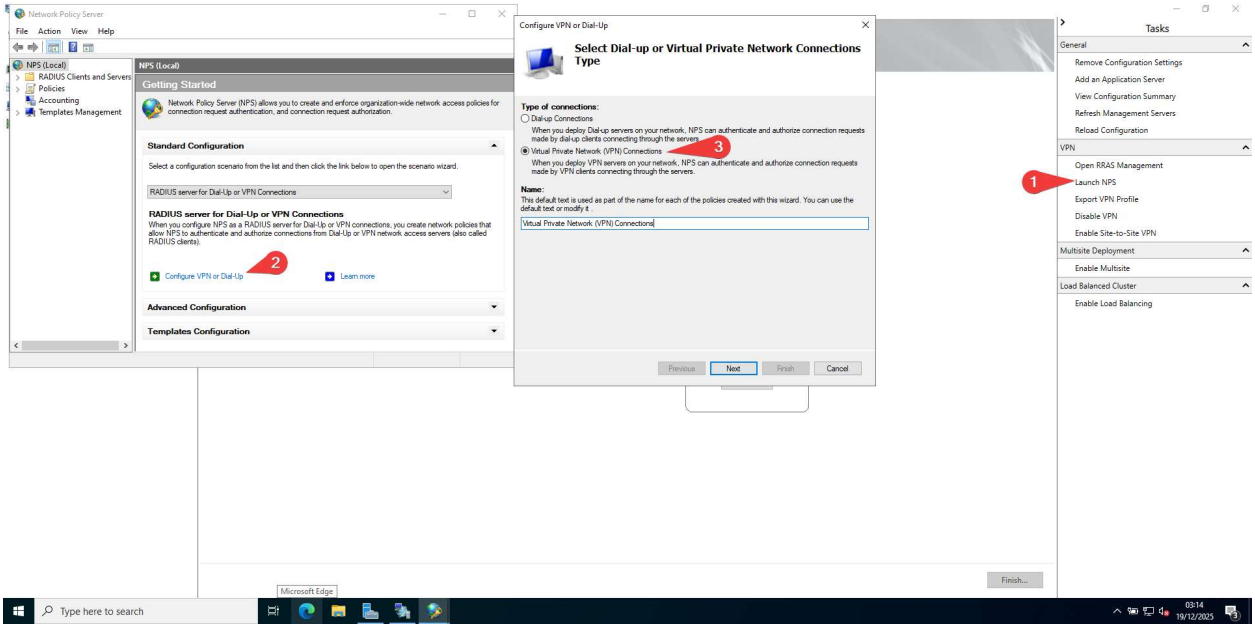
In Manage → Remote Access Management → DirectAccess and VPN




Enable VPN on the server

Next, we configure NPS for the VPN

Click Next until we get to the “Specify User Groups” where we add our VPN Users group

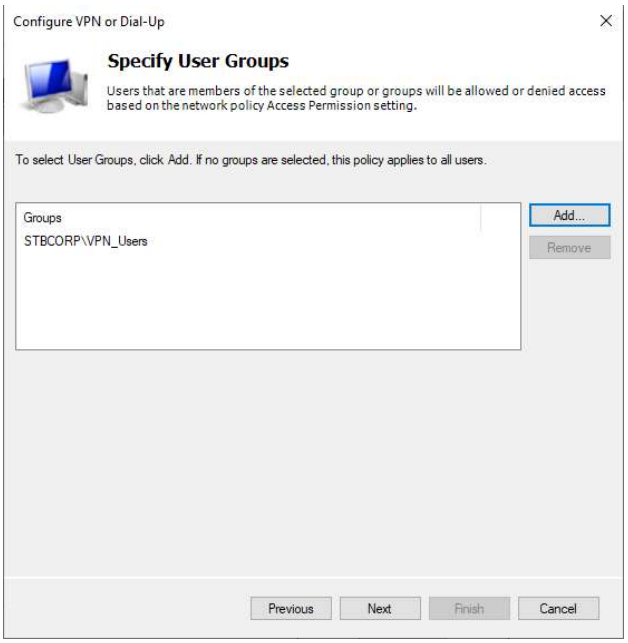


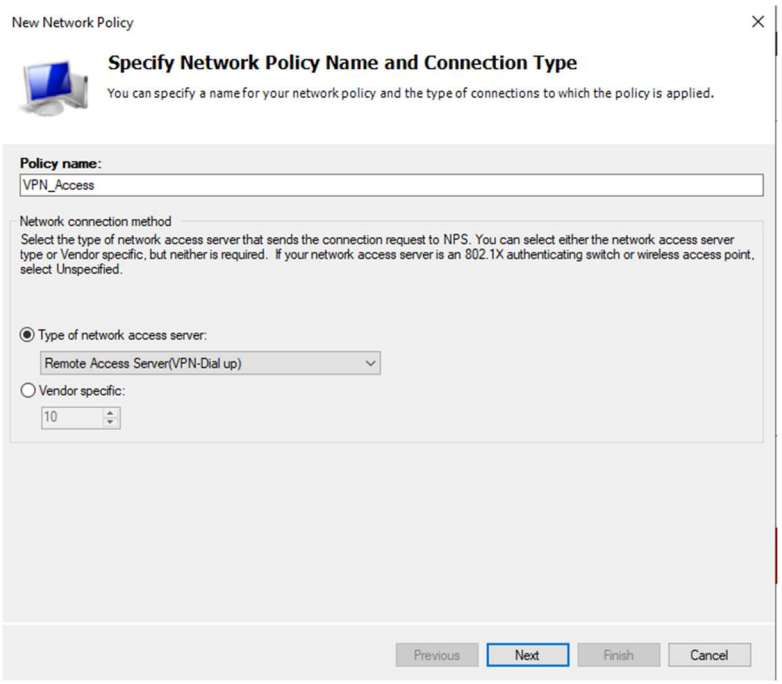

Then finish the NPS setup.

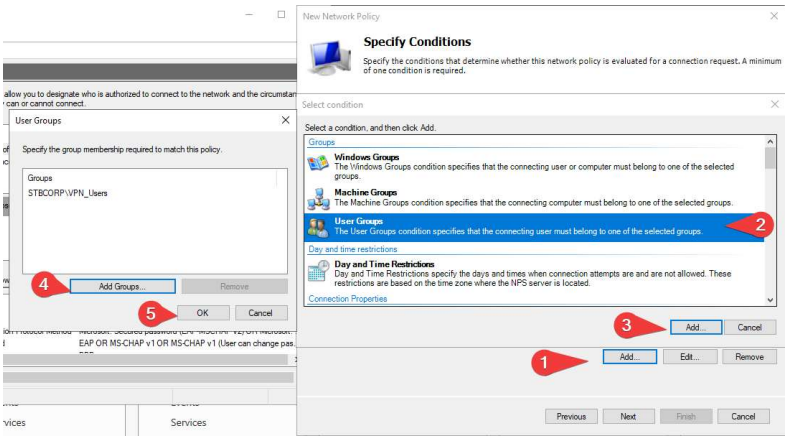
Setting a policy for VPN

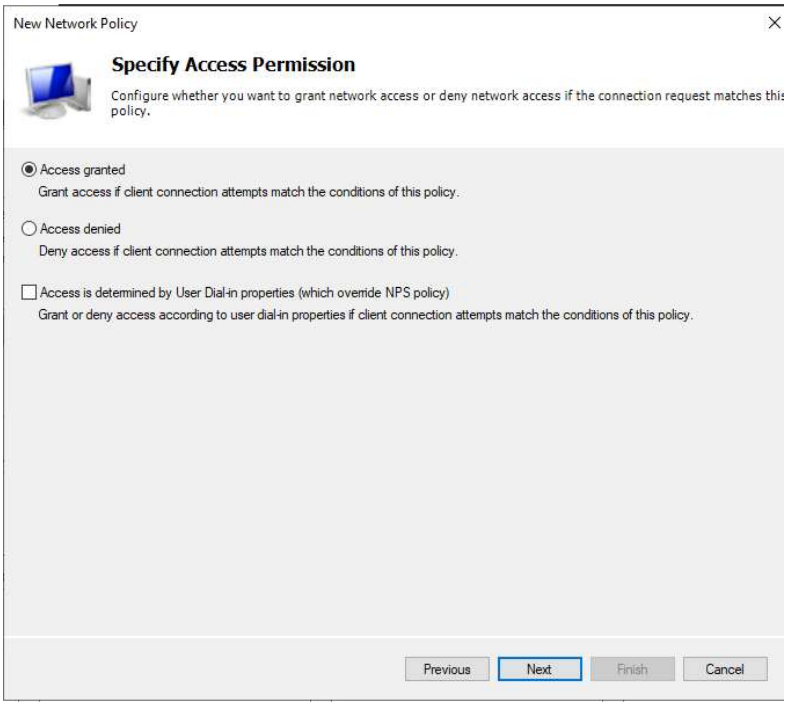
Manage → Network Policy Server → Policies → Network Policies

Create a new policy




New Network Policy
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:
VPN_Access
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:
Remote Access Server(VPN-Dial up)
Vendor specific:
10
Previous
Next
Finish
Cancel

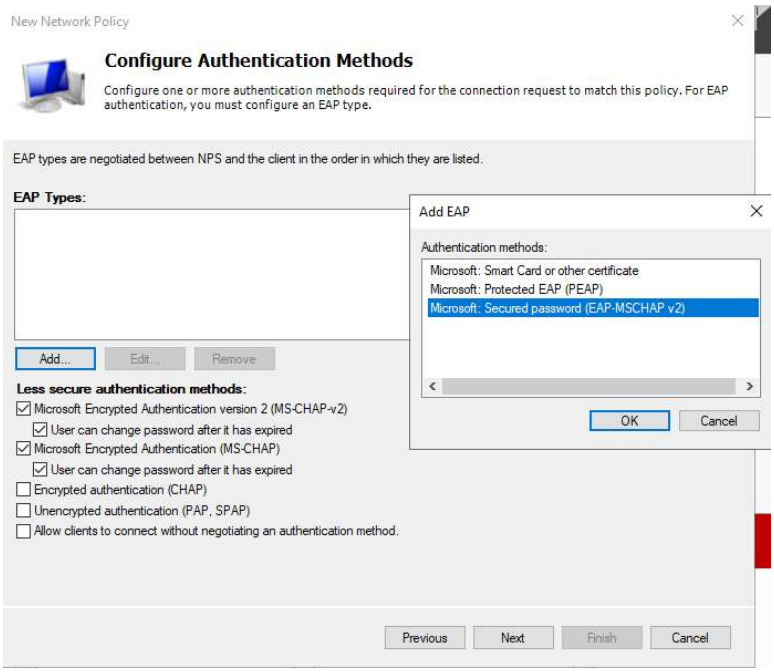

New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected 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. These restrictions are based on the time zone where the NPS server is located.
Connection Properties
Add...
Cancel
Edit...
Remove
Previous
Next
Finish
Cancel
User Groups
Specify the group membership required to match this policy.
STBCORP\VPN_Users
Add Groups...
OK
1
2
3
4
5

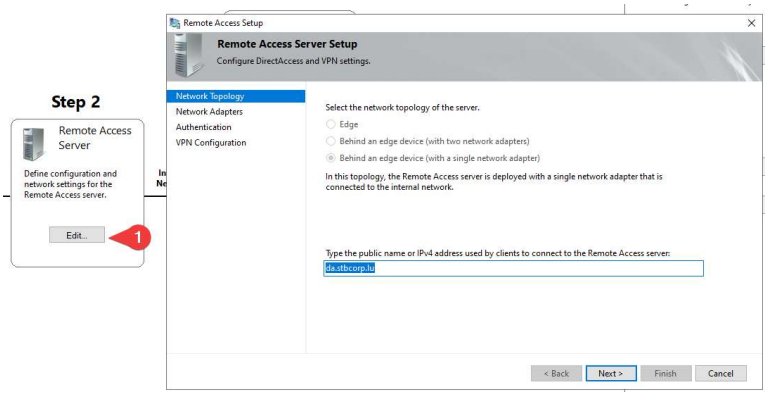

New Network Policy
Specify Access Permission
Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access granted
Grant access if client connection attempts match the conditions of this policy.
Access denied
Deny access if client connection 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

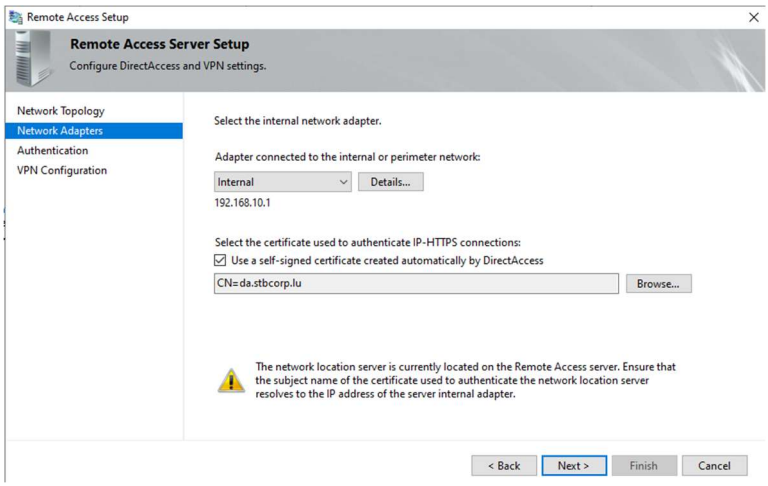
Click Next until finishing the policy

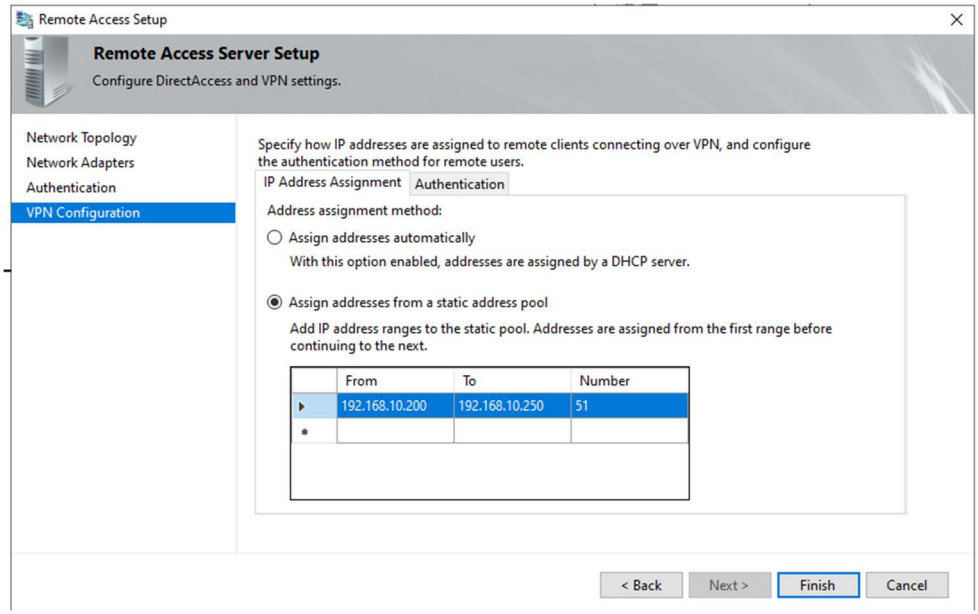
VPN Configuration

Manage → Remote Access Management






Create an IP Range for the VPN server

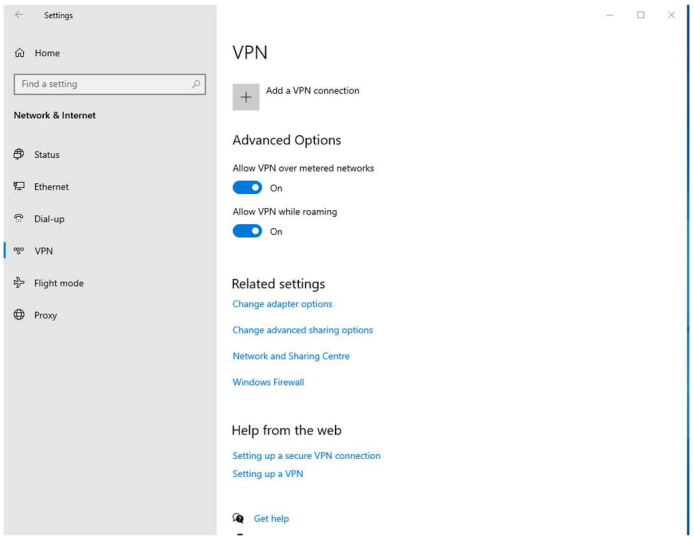
## 3.10 Setting up the VPN Client

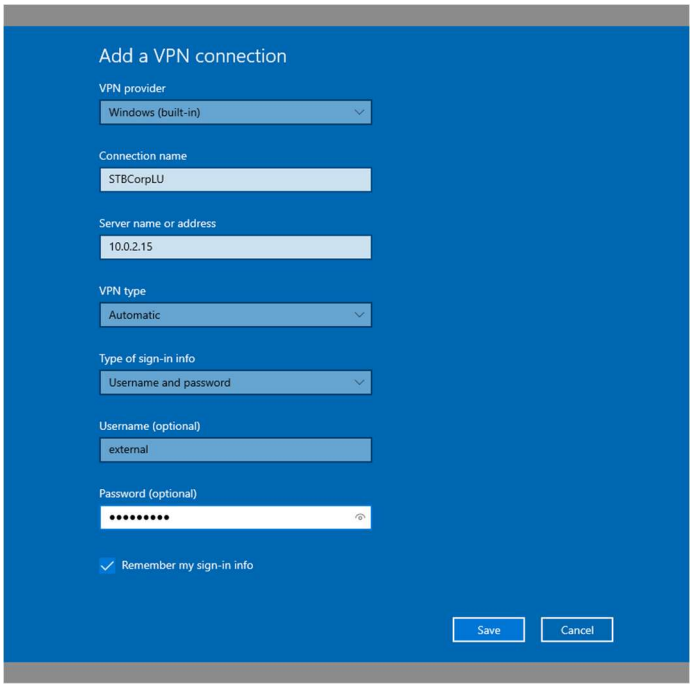
Settings → Network & Internet → VPN

Click on Connect and the Client should now connect to the Server

If it doesn't connect,

- Change VPN Type to IPKeV2
- On the server check if the ports are open and not take by another service



With the configuration and installations completed, the remote access environment is now fully operational. Approved employee laptops can securely access internal resources through **DirectAccess**, while external clients can connect through **VPN** authenticated via **local NPS** and access only the predefined shared folders with a controlled user environment. All access is managed through **Active Directory groups and permissions**, ensuring a secure, structured, and maintainable solution aligned with the client's requirements.