

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 1 - Pass

Guide standard exemplification materials

v1.1: Specimen assessment materials
September 2021
603/6901/2

Internal reference: DSS-GSEM-18

T Level Technical Qualification in Digital Support Services Occupational specialism assessment

Guide standard exemplification materials

Digital Support

Assignment 1

Contents

Introduction	3
Assignment 1:	4
Task 1: prepare for installation	4
Student evidence	6
Task 2: install and configure a small network	12
Student evidence	14
Examiner commentary	102
Grade descriptors.....	103
Document information	105
Change History Record.....	105

Introduction

The material within this document relates to the Digital Support occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

In assignment 1, the student must first plan a network installation, then install and configure a small network, before producing installation notes to inform the client of the work they have carried out.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

Assignment 1:

Scenario

You are a digital support specialist who has been contracted to work for a new small food manufacturing company (the client) based in the North of England.

The client requires your digital expertise in planning to support a future network. There are currently no business control techniques in place as the company is only just starting out, and they are unaware of any measures on how to operate their data systems effectively, appropriately, and securely.

The client also requires your immediate support with preparing and installing a smaller network of computers and a mobile device for the employees within the company.

Task 1: prepare for installation

Time limit

8 hours

Task 1(a) must be completed prior to starting task 1(b).

Task 1(a) is allocated 3 hours 30 minutes.

Task 1(b) is allocated 4 hours 30 minutes.

You can use the time how you want but each task must be completed within the time limit.

(20 marks)

Student instructions

Based on the scenario, you are required to complete the relevant preparation that will enable you to set-up 100 computers, a switch, server and 5 colour printers including identifying the relevant software for the client in the future. The network would be required to be set-up within a 2 week window, to ensure all employees are up and running as quickly as possible.

You are required to:

1(a) Create a report to explain the security considerations required for the installation, configuration, and support of end-user services to ensure confidentiality, integrity and availability including:

- suitable recommendations on implementing business control techniques within the workplace (physical/administrative)
- explanations on how the client should operate the new data systems effectively, appropriately, and securely, considering GDPR/ DPA 2018 and its principles

(8 marks)

1(b) Plan and complete the relevant network planning documentation:

- health and safety risk assessment for the work to be undertaken
- network planning, including:
 - timescales
 - network design, including IP addressing scheme
 - inventory
 - security risk assessment for the work to be undertaken, according to ISO 27001 principles

(12 marks)

You will have access to the following equipment:

- a computer with office software pre-installed

Evidence required for submission to NCFE

The following evidence should be submitted:

- summary of all business controls documentation required (word processing document)
- summary of how to secure data systems effectively (word processing document)
- health and safety risk assessment (worksheet in appendix 1)
- network planning documentation including timescales and network design (word processing document)
- inventory log (worksheet in appendix 1)
- security risk assessment (worksheet in appendix 1)

Student evidence

Task 1(a)

Security recommendations for the implementation of business controls in the workplace

Introduction

As a business we have a responsibility to put in place controls to protect our networks and data from loss (accidental or deliberate), theft or damage. To be effective in this we need to ensure that adequate controls are put in place and best practice is that we should use a range of controls of different categories.

Categories of controls include:

- physical - any control which involves a physical action taking place or object in use (for example, locked doors, ID badges, air gapping).
- administrative - any control that involves a procedure or process that may control behaviour to improve security (for example, operating procedures, password policies or mandatory training)

We can also categorise controls based on how they operate:

- preventative – such as installing a keycard reader on the server room door to restrict access to the room.
- detective – such as CCTV cameras to identify who tries to gain access to the server room
- corrective – such as using logs to identify who has had access to areas
- deterrent – such as signs indicating that security measures are in place, such as the keycard or CCTV
- directive – such as the creation of policies around access and security
- compensating – such as having various backup policies in place to protect data rather than offsite duplicate servers
- recovery – such as failover servers off site in case of emergency onsite, whilst expensive this allows for quick restoration

It is possible for controls to fit across multiple categories (for example, a CCTV camera would be an example of a physical control that is both detective and deterrent).

A good security posture will include a mix of both physical and administrative controls and will also include preventative, detective, corrective, deterrent, directive, compensating and recovery controls.

Recommendations

For our network it is recommended that we implement the following controls:

- locked server room
- CCTV cameras
- checking logs
- no entry signage in secure areas
- server rooms should be air conditioned
- password policy with password training
- server backups

Operating the data systems

As well putting these security controls in place it is important that data is handled correctly and securely. This is particularly the case with customer data and information as failure to do so could include a breach of the Data Protection Act (DPA) 2018 which incorporates the General Data Protection Regulation (GDPR) into British law.

The DPA 2018 includes the following principles:

- lawfulness, fairness, and transparency:
 - all data collected must be done in a legal manner
- purpose limitation:
 - we can only use data how we have told the customer we will
- data minimisation:
 - we can only collect data we need
- accuracy:
 - where we hold data on a customer, we need to make sure it is up to date
- storage limitation:
 - we can only keep data for as long as we need it
- integrity and confidentiality (security):
 - all data needs to be kept secure
- accountability:
 - we need to keep records of the data we are keeping

Summary

To ensure that we meet our obligations under the DPA 2018 and to ensure that we protect our networks and data (including company confidential data) adequately we need to implement a range of controls (administrative and physical) across our network. The recommendation above will give a range of preventative, detective, corrective, deterrent, directive, compensating and recovery controls that will maximise the protection our network has from a wide range of potential attacks.

Task 1(b)

Network design

Client specification

Network should include:

- 1 server
- 100 client PCs
- 5 colour printers
- switch

To meet this requirement, I am recommending that we install:

- server:
 - 1 server running Windows Server 2016
 - for security the server should also include antivirus software
- client PCs:
 - all client PCs should be installed with Windows 10 and joined to the server
 - all client PCs should be installed with the following software:
 - Office 365 (Word, Excel, PowerPoint and Outlook)
 - Adobe Acrobat
 - antivirus software
- switches:
 - we will need a managed switch to connect all devices to the network
- IP addressing:
 - it is recommended that the network is configured using the following IP addressing scheme:
 - network IP addressing:
 - network: 192.168.0.0/24
 - IP addresses:
 - 192.168.0.1 server
 - 192.168.0.10 to 14 printers
 - Windows computers:
 - 192.168.0.100 to 199

Full details of network configuration can be seen by consulting the network configuration diagram at the foot of this document.

Network installation plan

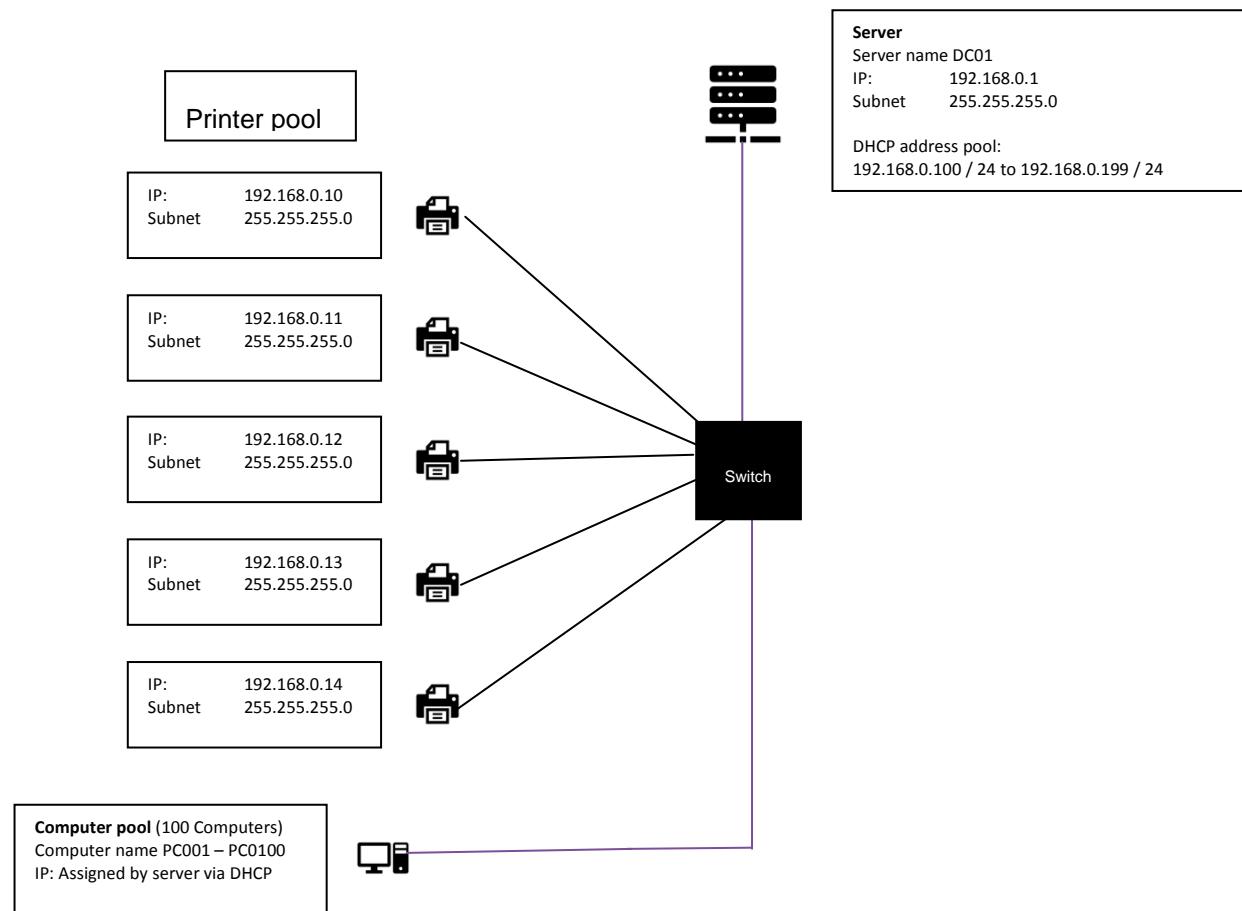
The network installation should be completed with the following steps:

- **stage 1: physical infrastructure set-up:**
 - physical installation of switches and router firewall
 - physical installation of cabling
- **stage 2: server installation:**
 - installation of server 2016 software
 - configuration of server settings
 - installation of Active Directory
 - installation of security software
- **stage 3: set-up and configuration of client PCs:**
 - installation of Windows 10 on reference client PC
 - installation of key software (office, Adobe Acrobat)
 - preparing system ready for imaging
 - imaging of PC
 - adding image to installation server
 - physical installation of client PCs (physical set up)
 - PCs connected to installation server
 - remote installation of client PCs

Project completed.

		Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10	Day 11	Day 12	Day 13	Day 14
Stage 1: Physical Infrastructure Setup	Physical installation of Switches and Router Firewall														
	Physical installation of Cabling														
Stage 2: Server Installation	Installation of Server 2016 Software														
	Configuration of Server Settings														
	Installation of Active Directory														
	Installation of Security Software														
Stage 3: Setup and Configuration of Client PCs	Installation of Windows 10 on reference Client PC														
	Installation of key software (Office, Adobe Acrobat)														
	Sysprep of system ready for imaging														
	Imaging of reference PC														
	Answer file created including configuration of Domain Join														
	Adding Sysprepped image to Installation server														
	Physical installation of client PCs (physical setup)														
	PCs connected to Installation server via PXE boot														
	Remote installation of client PCs.														
	Project Completed.														

Network diagram



Task 2: install and configure a small network

Time limit

11 hours

You can use this time how you want but all parts of task 2 must be completed within the time limit.

(56 marks)

Student instructions

The client has asked you to install a new small network, against a set of requirements. These devices can be either virtual, physical or emulator.

All employees will use the computers centrally within head office, and any off-site employees will use a mobile device (laptop, tablet or phone) to be able to work remotely via the approved remote working solution.

The computers need to be set up allowing the employees to email, write letters to suppliers, update financial spreadsheets and create weekly presentations.

The computers will also need to access the internet and have instant messaging/video conferencing software such as Skype, GoToMeeting or Teams on Microsoft office 365 installed. Employees will require access to project management software in order to help them plan upcoming projects.

The client wants to ensure there is suitable software installed to mitigate any vulnerabilities to the system, including suitable back up security controls in place.

The client has also asked you to create installation notes for the software installations that took place, in order to support their staff responsible for IT. Your final task is therefore to create a useable document that briefs these individuals on the set-up of your system.

You will have access to the following equipment:

- 3 computers with full administrator rights, or virtual/emulator machine and software
- internet
- operating system
- word processing, presentation and spreadsheet software
- email software
- instant messaging software
- project management software
- mobile device or emulator
- IP address allocations for task 2 in line with provider's own network IP addressing schema
- digital camera

2(a) You must install, configure and support a small-scale network which includes 3 workstations and one mobile device via WiFi and evidence (you should reference the IP addressing schema allocated to you by your provider):

- implementing physical network and network security measures to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data (CIA and IAAA)
- install Windows Server and create Active Directory
- software licence management (software install log within appendix 1)

Note: you will need to provide annotated screenshots for the processes you follow and the implementations you make along with any key explanations for all decisions. As you carry out the various tasks, you will log all network security measures that have been implemented along with any software installations that are planned and how software licenses will be managed in the provided installation and configuration log (security risk assessment and software install log worksheets in appendix 1).

(18 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- annotated screenshots (if using virtual machines) or photographs (if using physical machines/devices) showing the setup and successful implementation of the network and server/Active Directory install

2(b) Provide evidence of the following for the client:

- installing and setting up an operating system and antivirus software
- join computer to Active Directory domain
- installing and configuring application software suitable for the client
- implementing back up security controls
- install/update device drivers

Whilst waiting for the installation to take place, set-up and configure a WiFi mobile device for network connectivity:

- configure a mobile device to include device lock security measures, mobile locator application and back up
- carry out all necessary mobile device updates including anti-virus

Note: You will need to provide annotated screenshots/photographs for the processes you follow and any implementations you make. This will include completing the software installation log (worksheet in appendix 1) and explaining your justifications for your decisions. You will also need to show evidence of any drivers which require installing, alongside taking screenshots of device manager. When updating any software/OS updates, you must evidence that there are no further updates required on the system. The installation may take some time to complete and therefore you should continue with task 2(c).

(22 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- screenshots (if using virtual machines) or photographs (if using physical machines/devices) showing the setup and successful implementation of software, device driver status and mobile device

2(c) Review the installation and configuration notes and log (started in task 1) that report the following information to the client, making sure it is up-to-date and correct:

- record of all operating system/software application installations and utilities, upgrades, uninstalls and any major configuration changes
- identify and explain any vulnerabilities detected in the current system set-up/network
- recommend actions to mitigate any vulnerabilities found

Note: You will have been filling in the installation and configuration log as you have been completing the task. You will need to review what you have done, ensure that all information contained is correct and also identify the vulnerabilities and mitigations required.

Apply your communication skills appropriately, using standard English. Use accurate spelling, punctuation and grammar. Consider your target audience.

(16 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- annotated screenshots and/or photographs for the set-up and successful implementation of the network and server/active directory install
- screenshots and/or photographs for the set-up and successful implementation of software, device driver status and mobile device
- completed installation and configuration log (appendix 1)

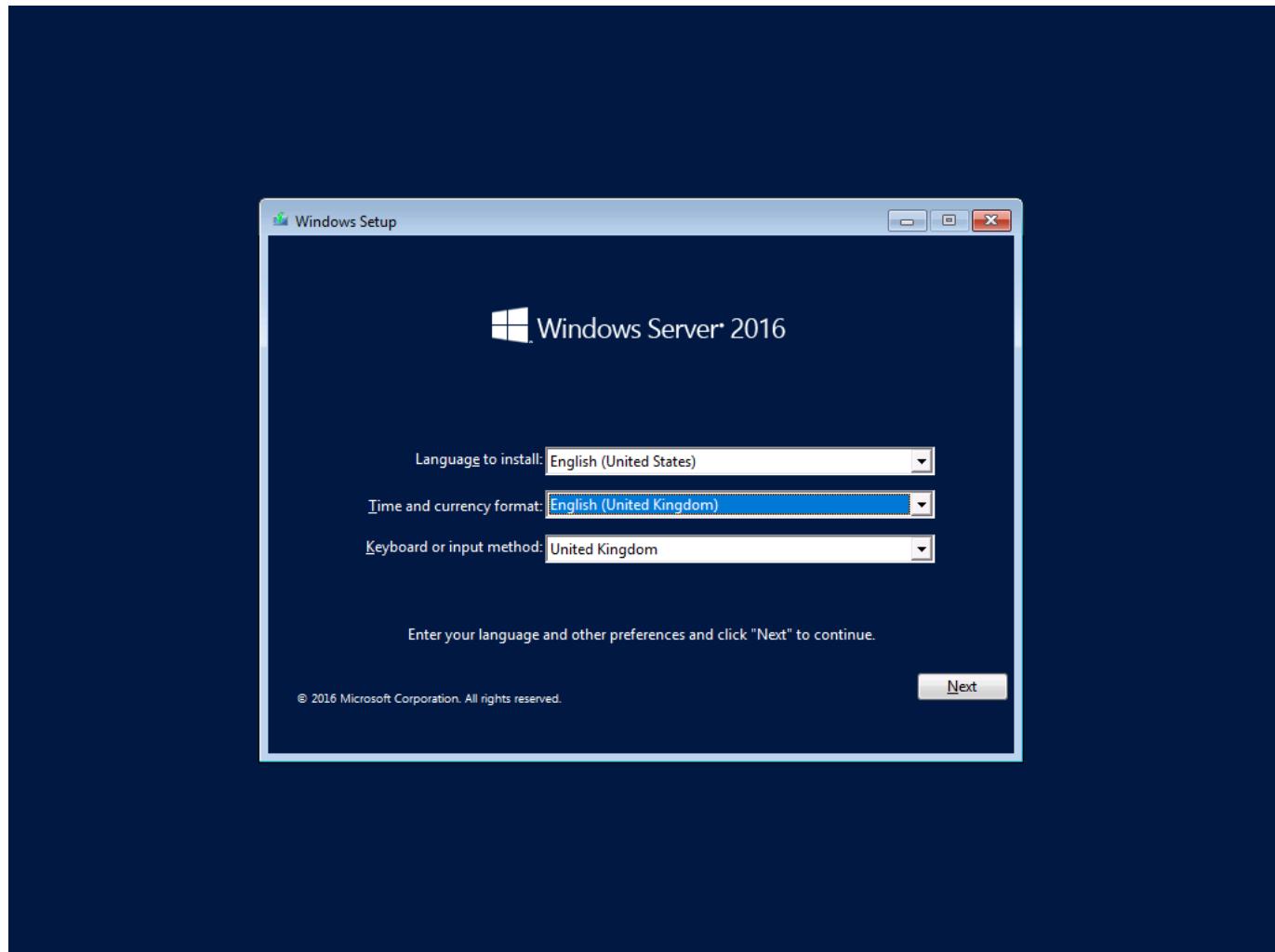
Student evidence

Task 2(a)

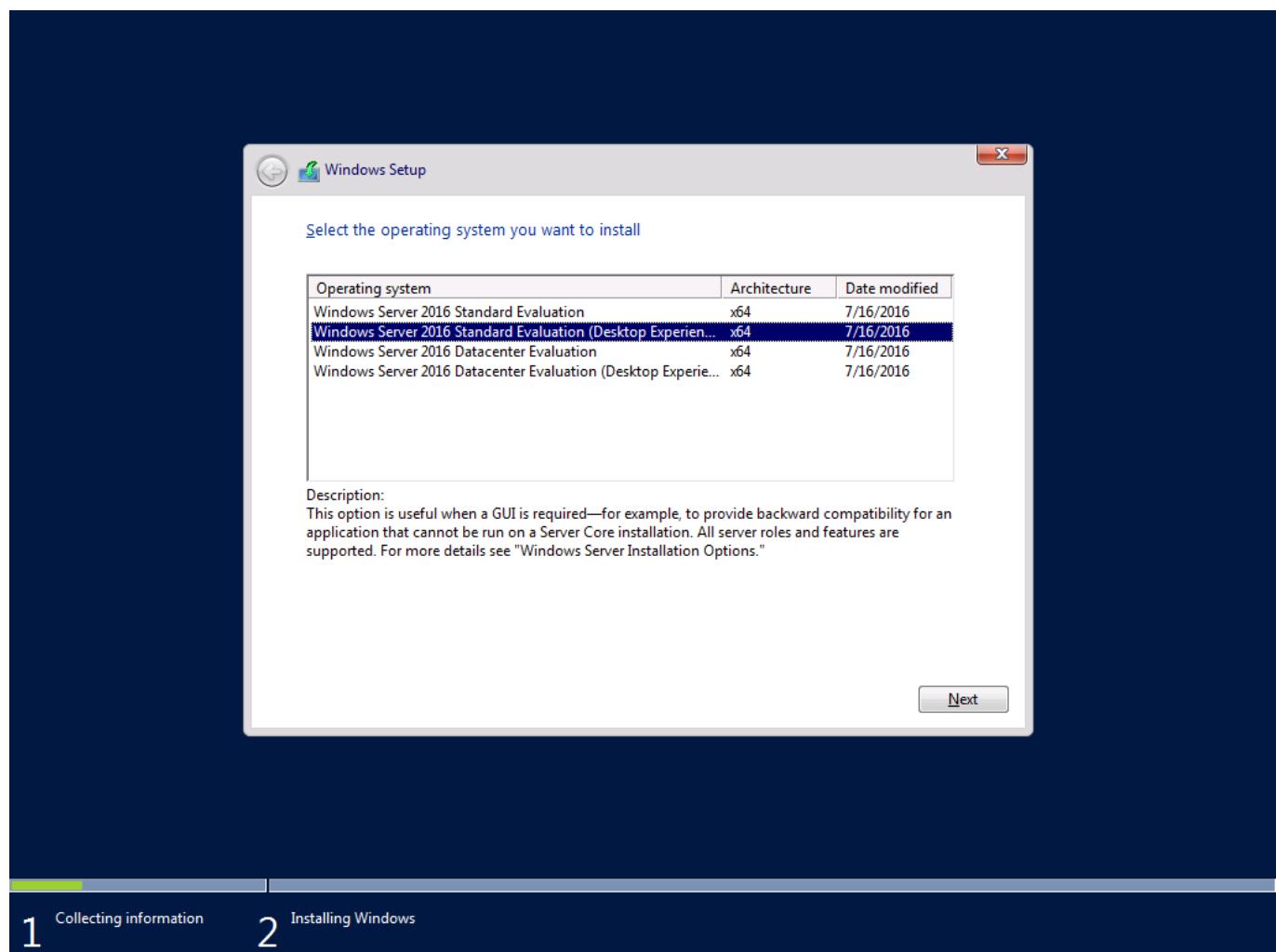
Evidence for this task will include a series of either screenshots or photographs documenting the installation process to show what I done. I have provided a descriptor for each key screenshot I would anticipate along with the appropriate commentary. It is likely that these screenshots will have been taken of an installation of server software such as Windows Server 2016.

Installing Windows Server 2016

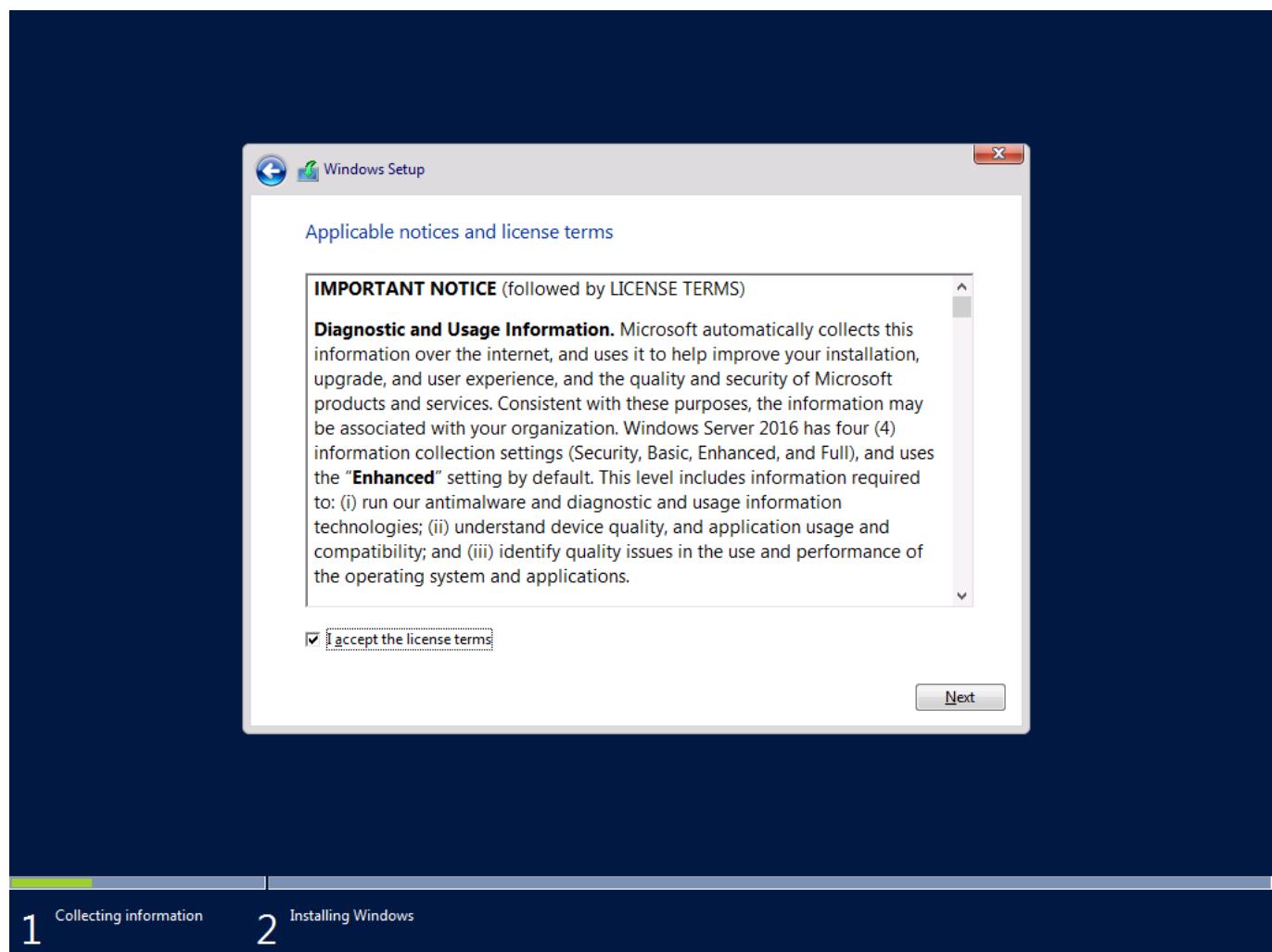
Screenshot:



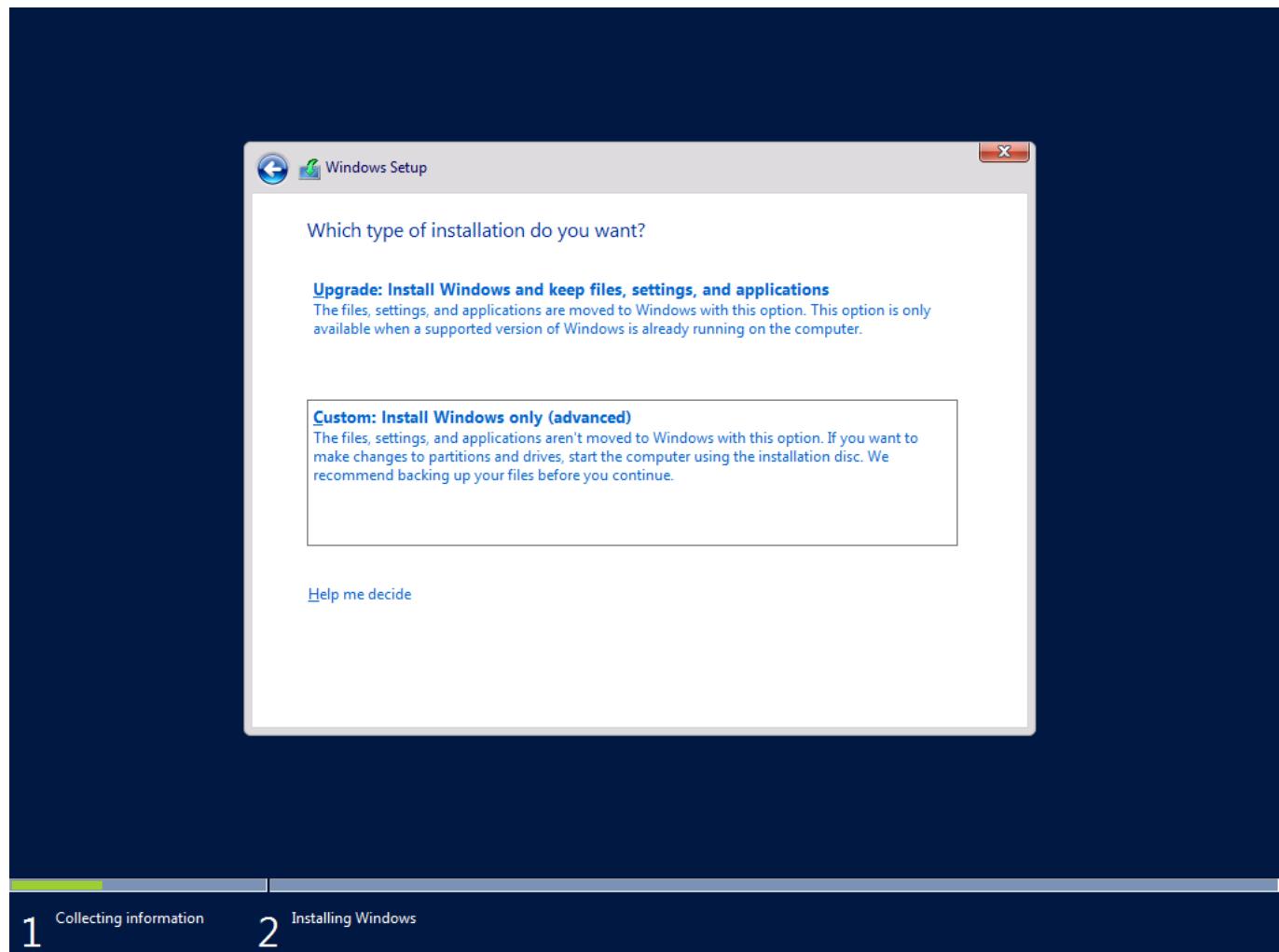
- I select the correct language to install (UK) after booting Windows.



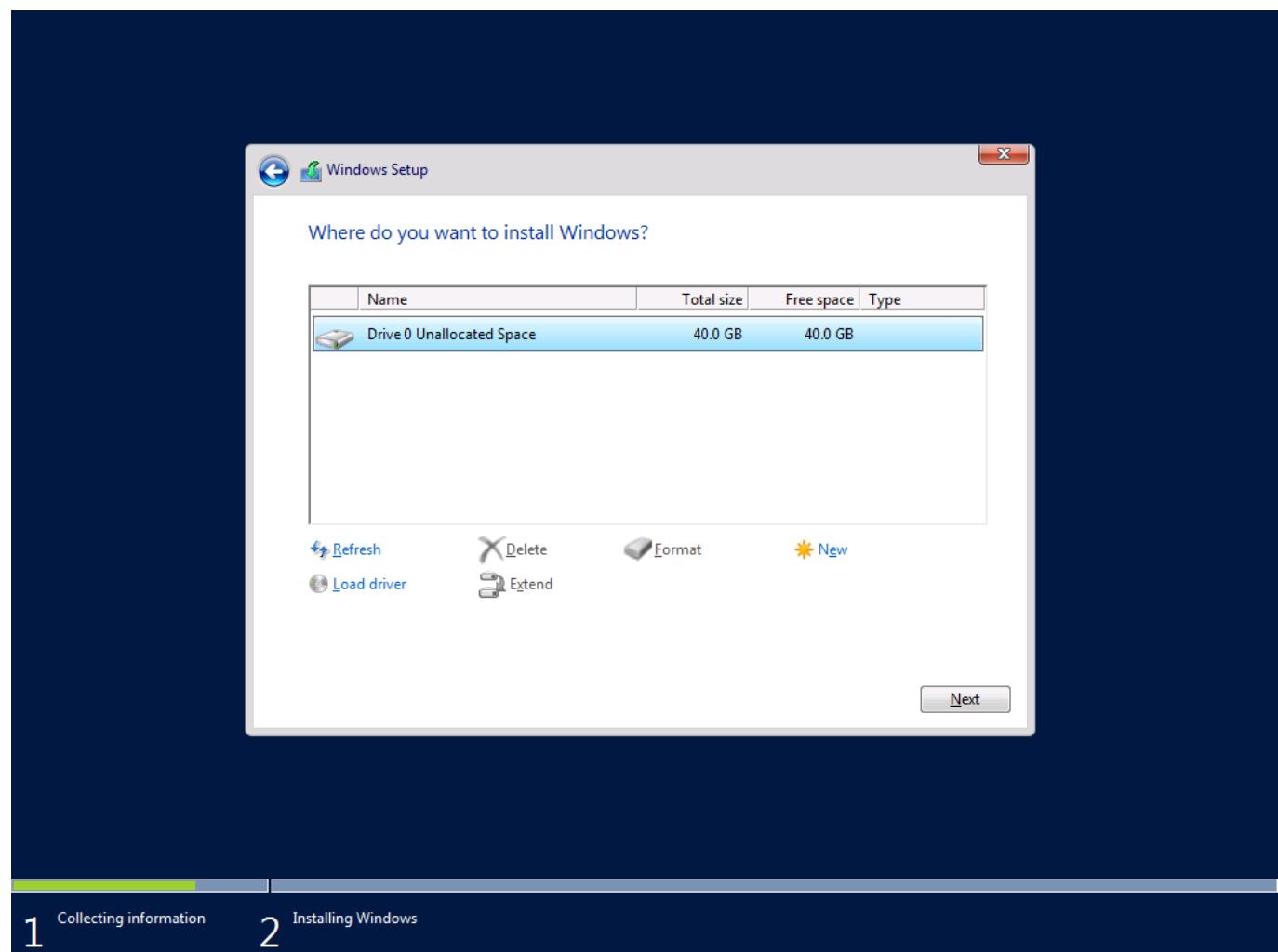
- I choose the correct version of Windows. I also select the desktop experience. Otherwise, it will be command line only



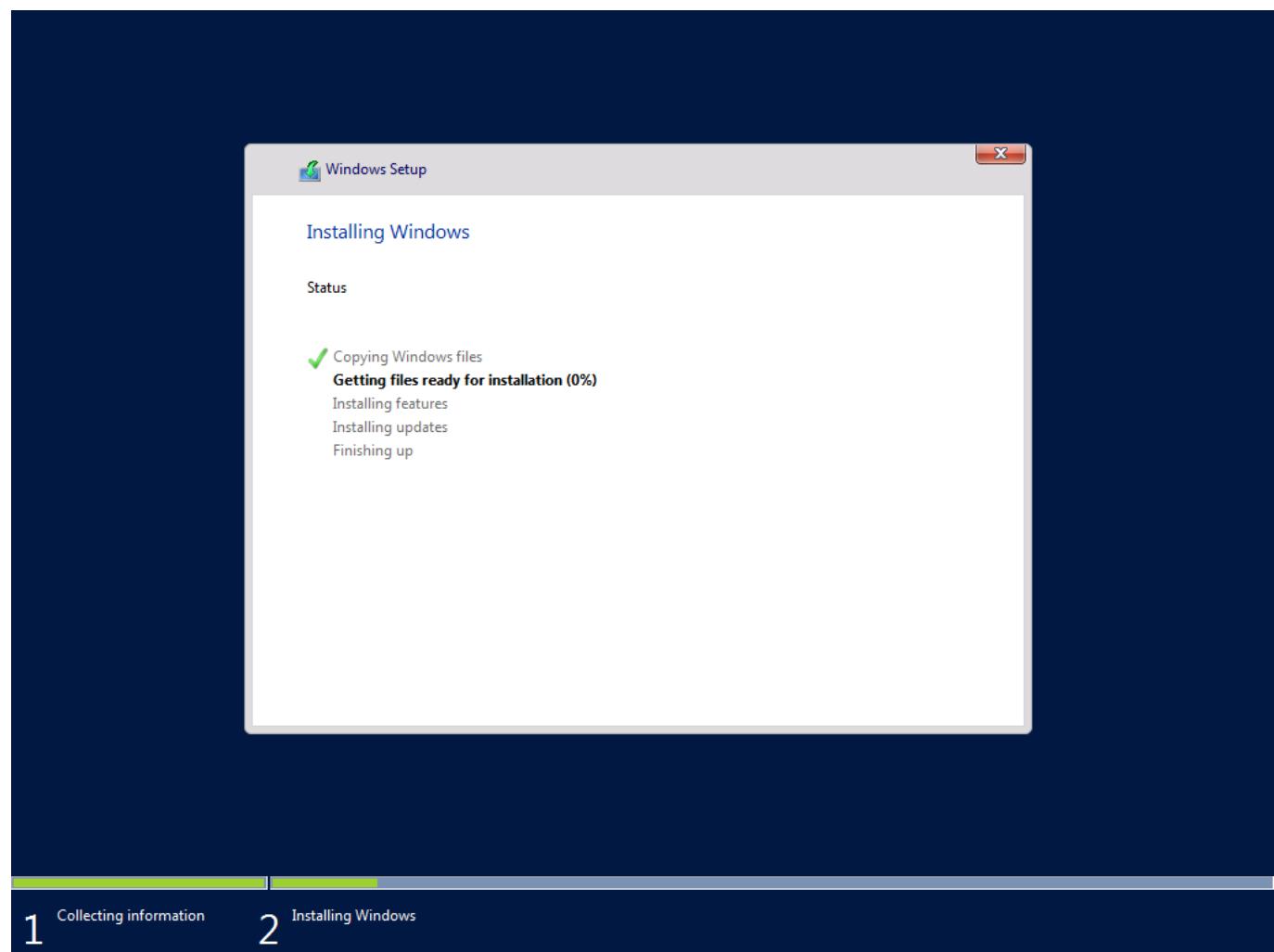
- I agree to the licence as this is mandatory



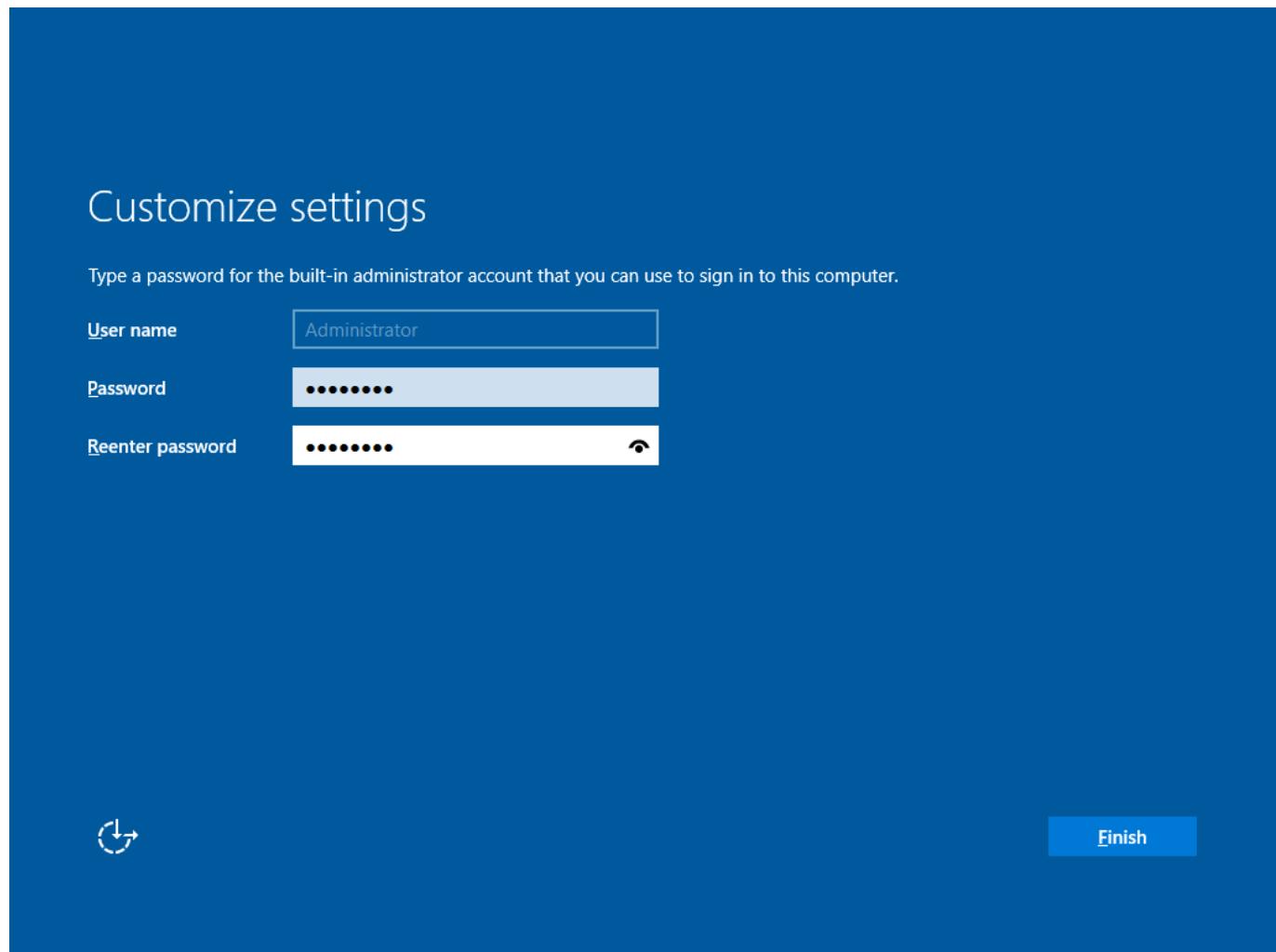
- I select custom so that I can choose the location to install to (below)



- I select the install location. In this case, it's the only disk

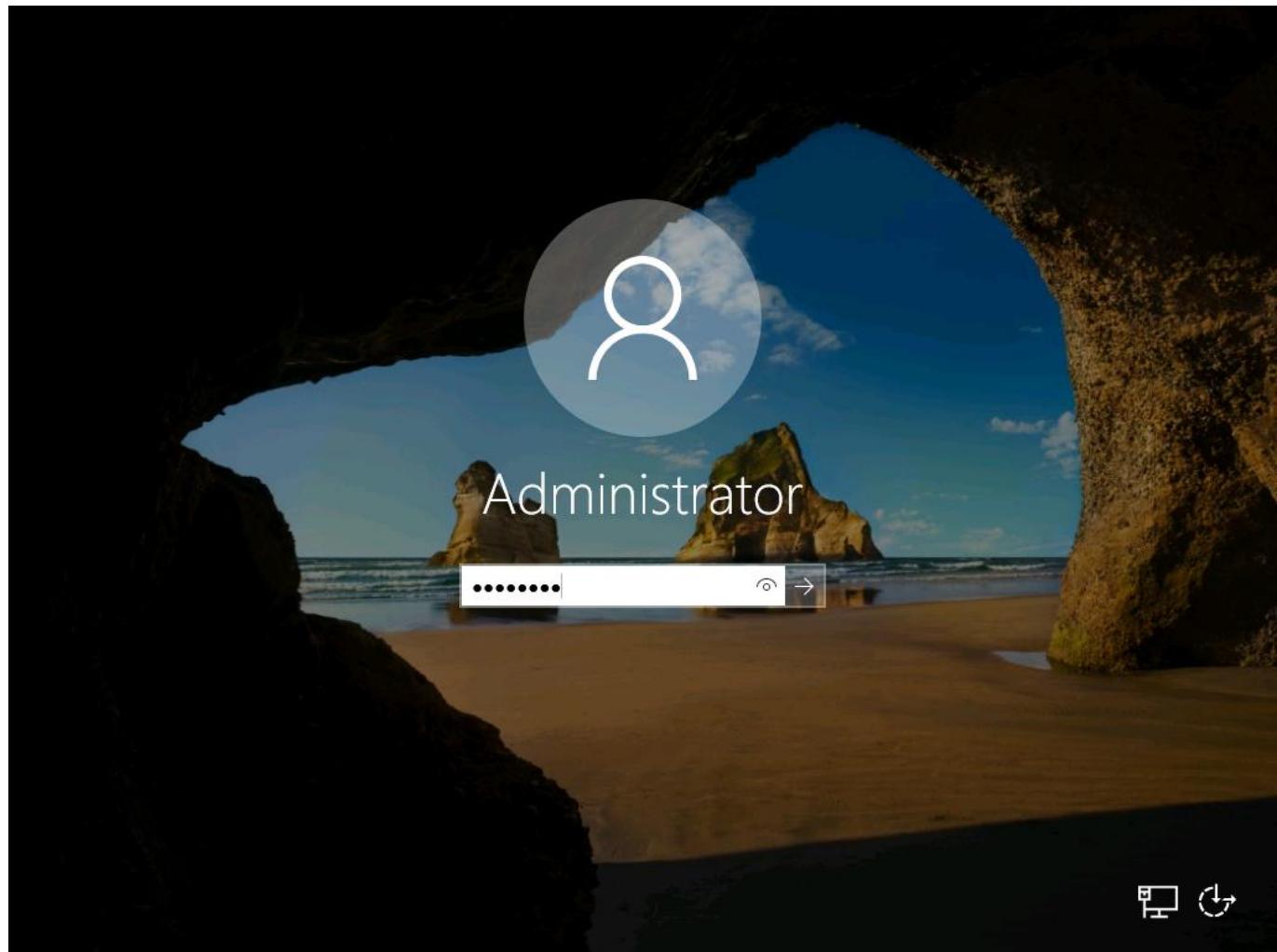


- Windows is now installing

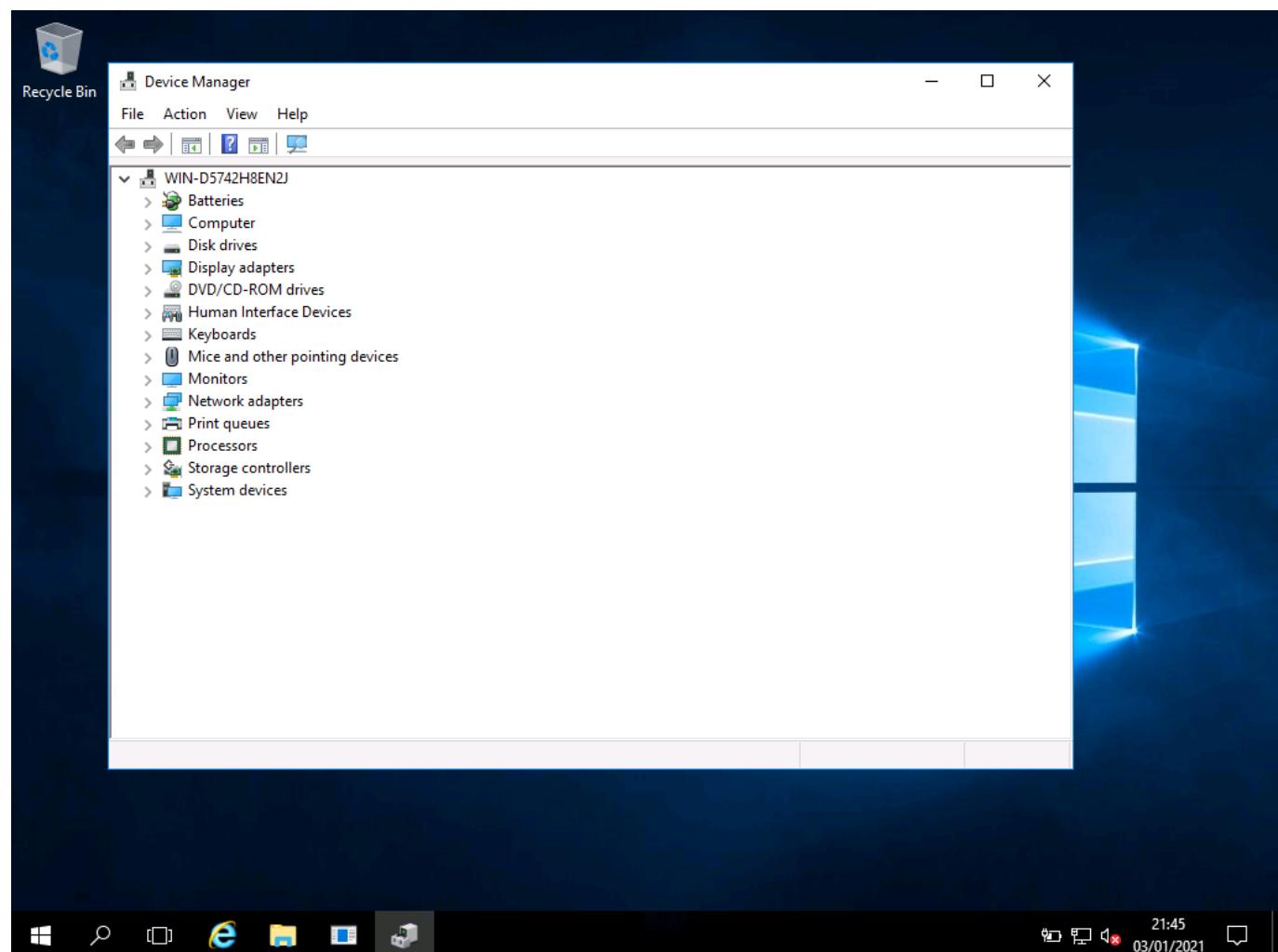


- I create an admin password for security
- These screenshots show me installing the server. Windows is now installed; I am prompted to set a password for the main local administrator account for the server

Screenshot:



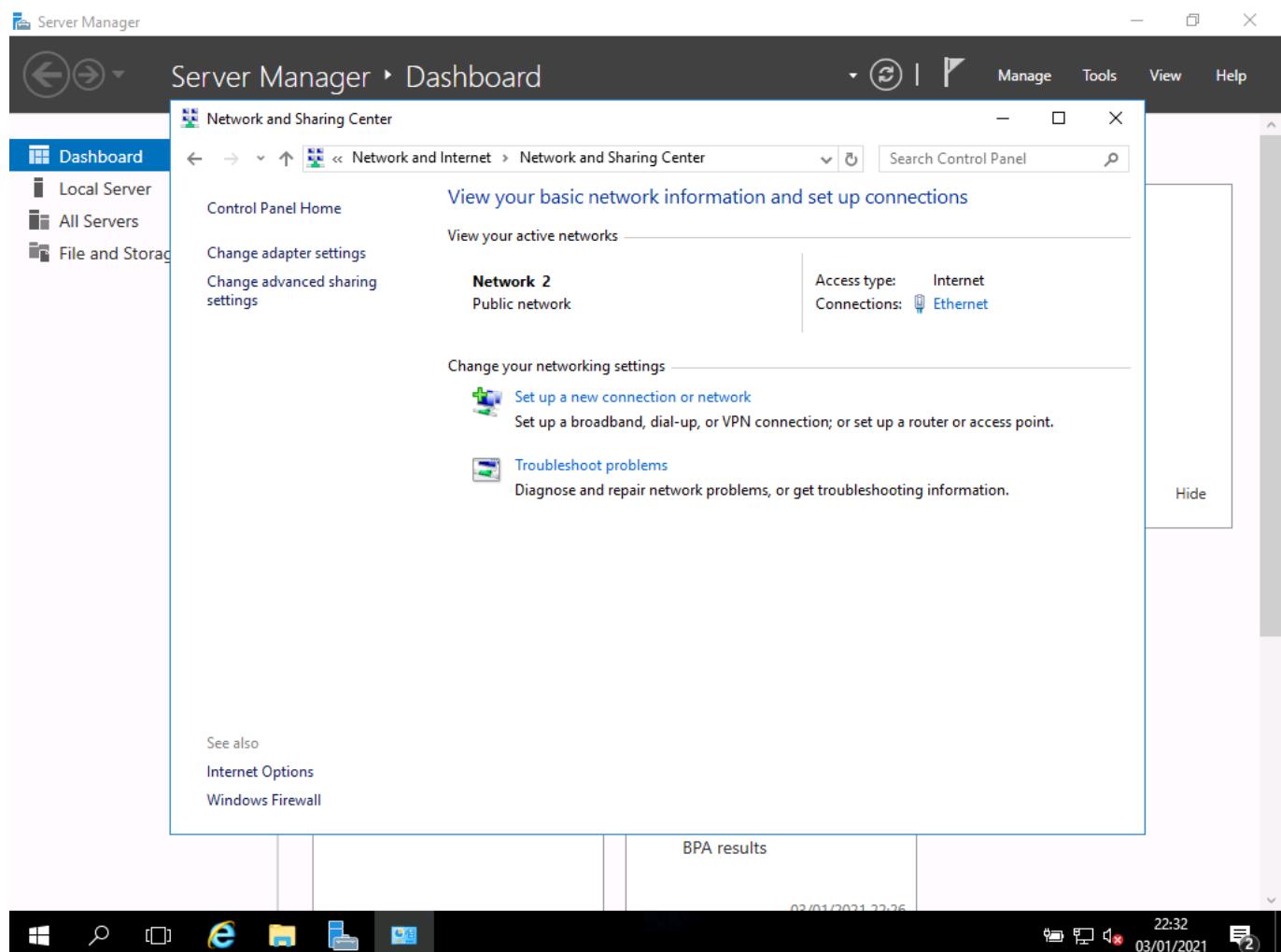
- I log in as administrator using the login and password previously set-up



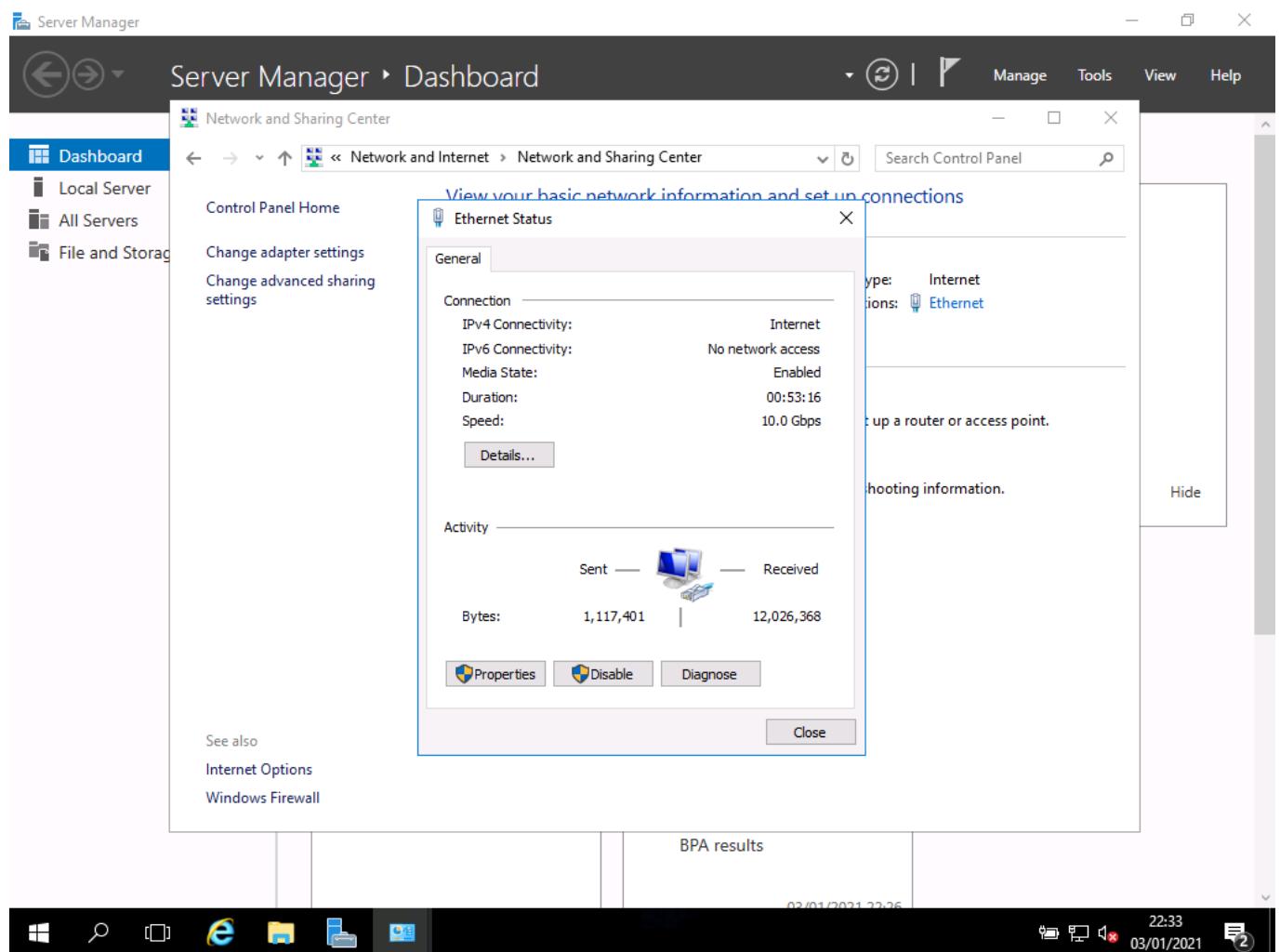
- I have checked device manager. All drivers for this server have been detected and installed

Setting up network settings

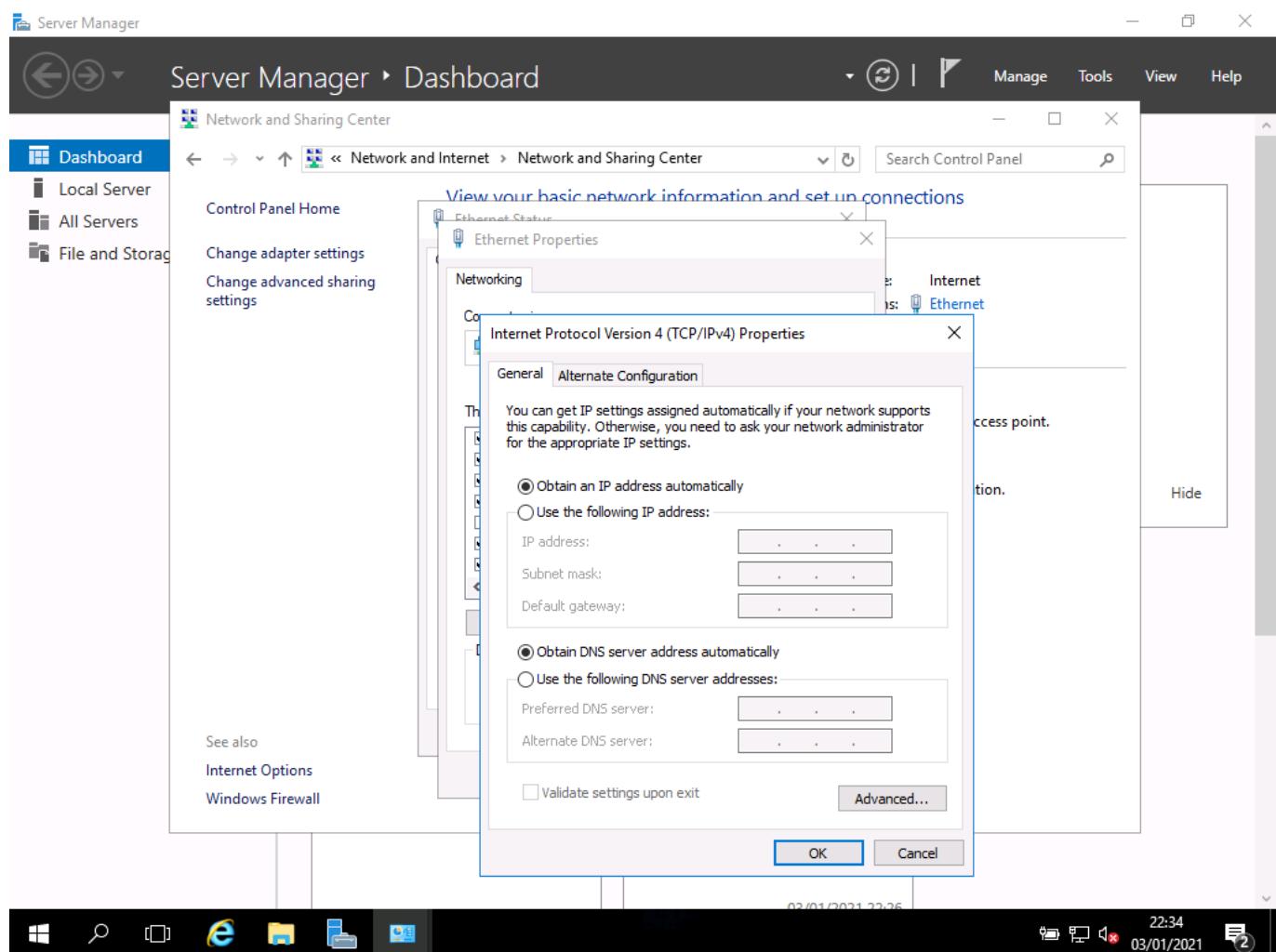
Screenshots:



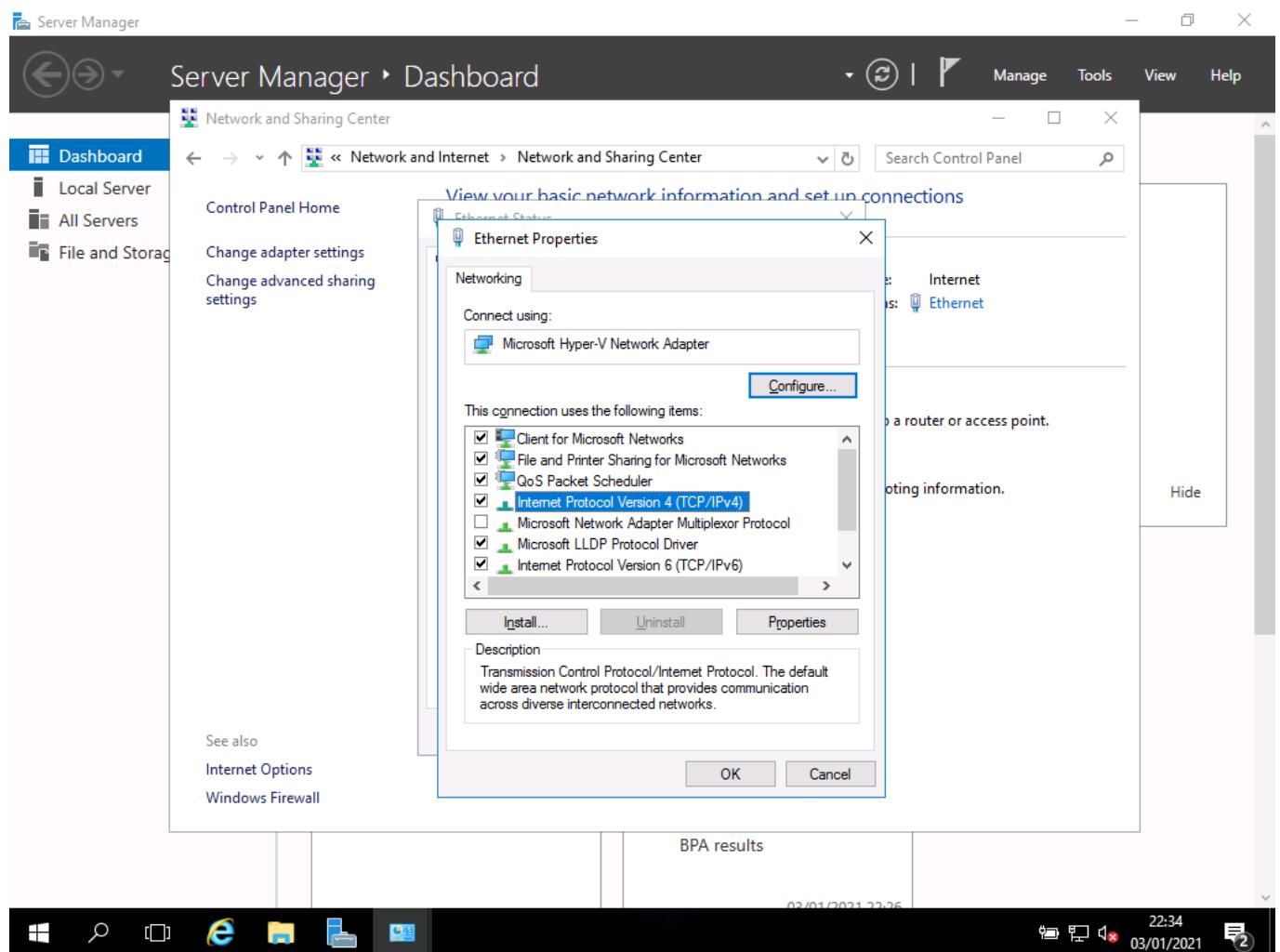
- I open the network settings



- I can see the selected network properties, and there is no connection

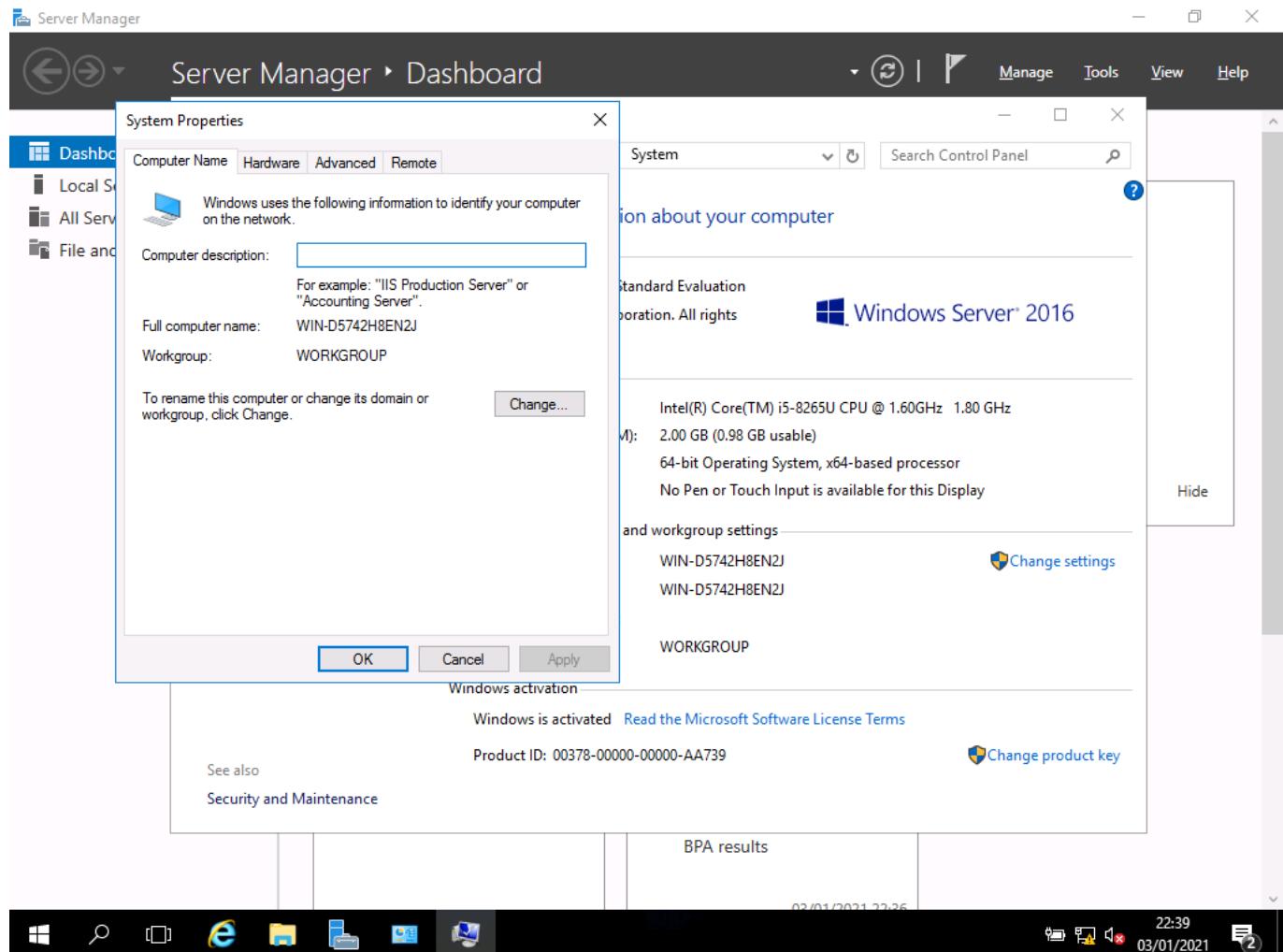


- I have located the properties for the network adapter

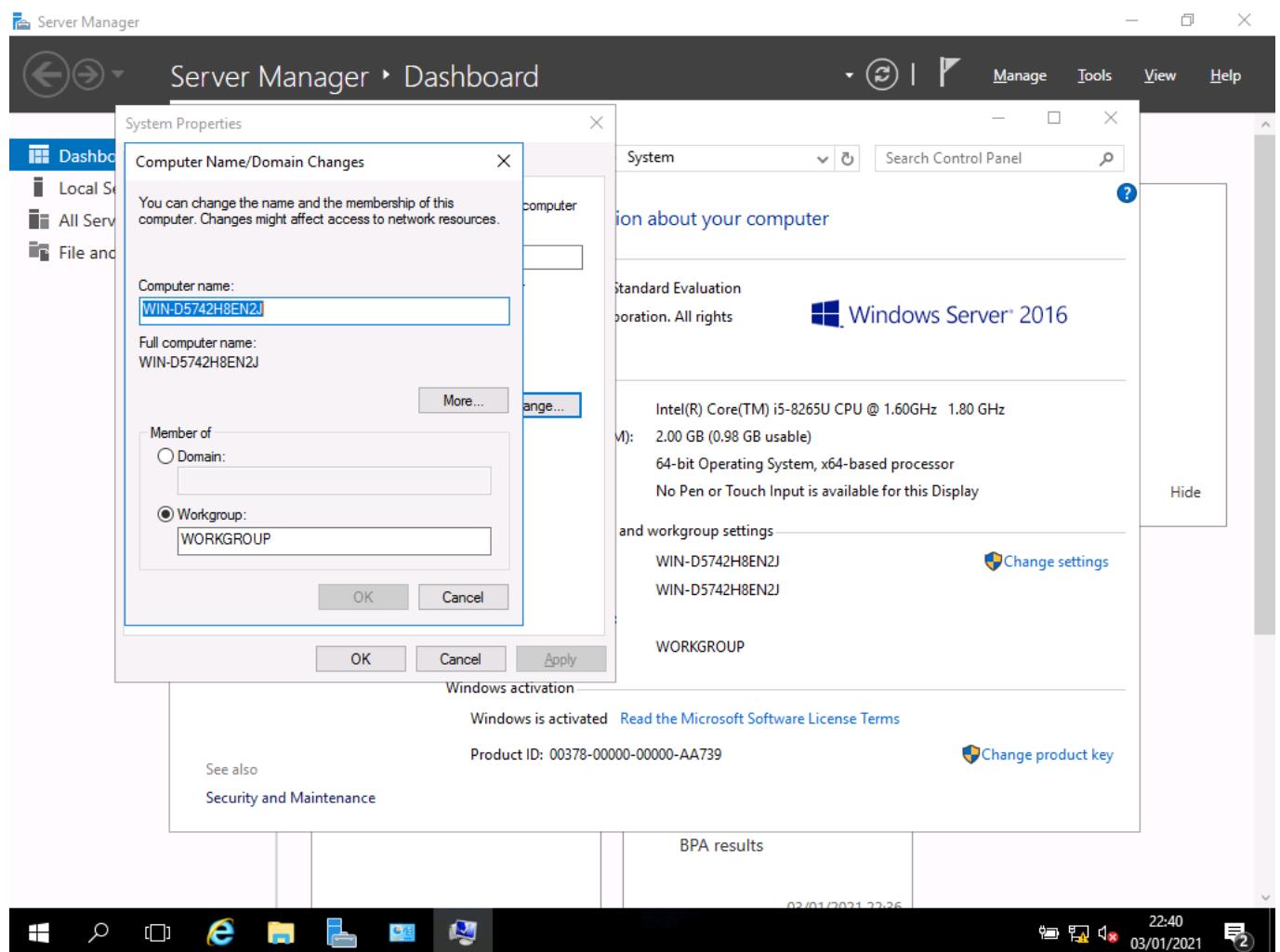


- These screenshots show me opening the properties for my network card and setting the IP address

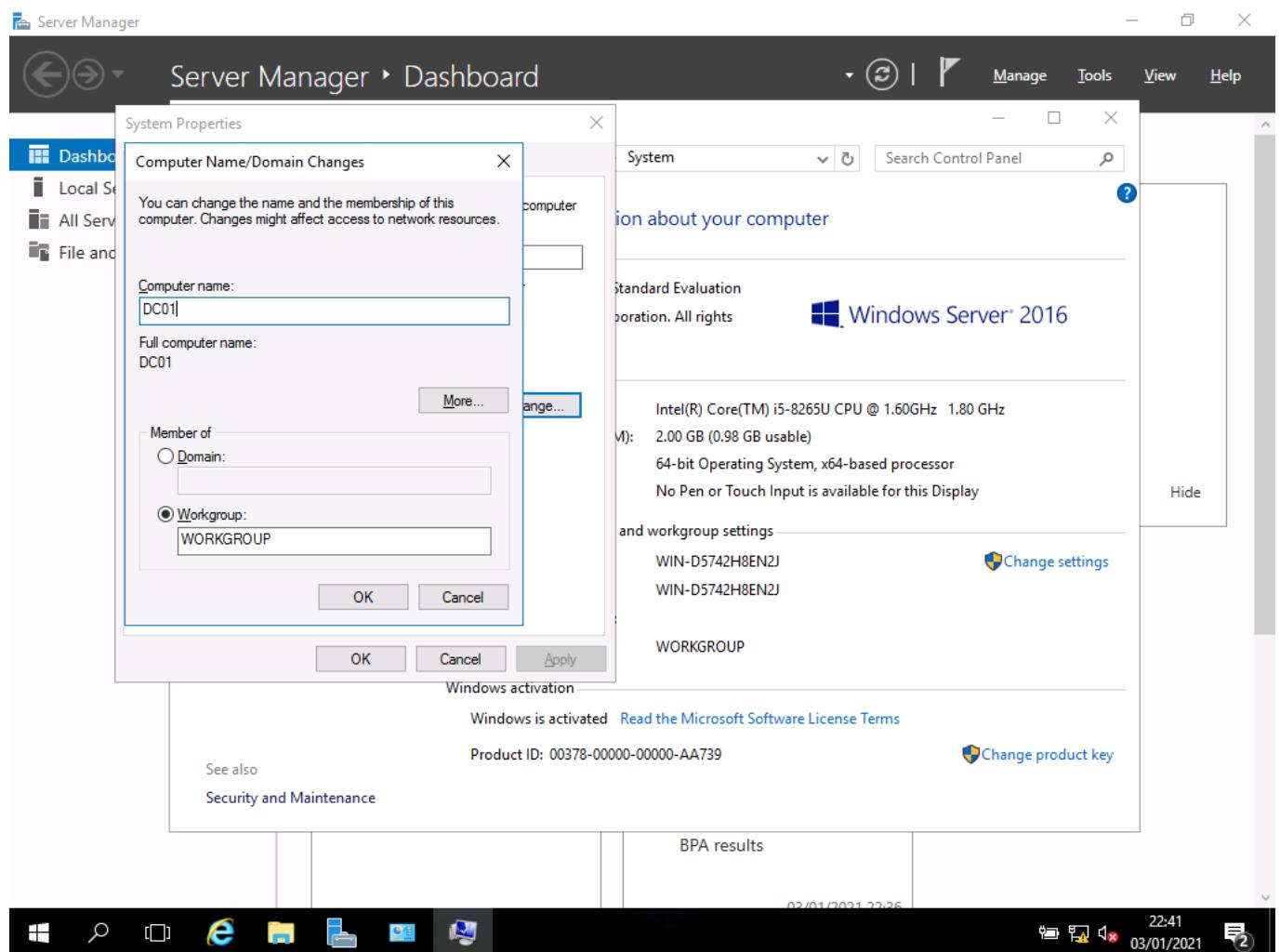
Screenshots



- I can now rename the PC so that it is can easily be known



- I give it a new name

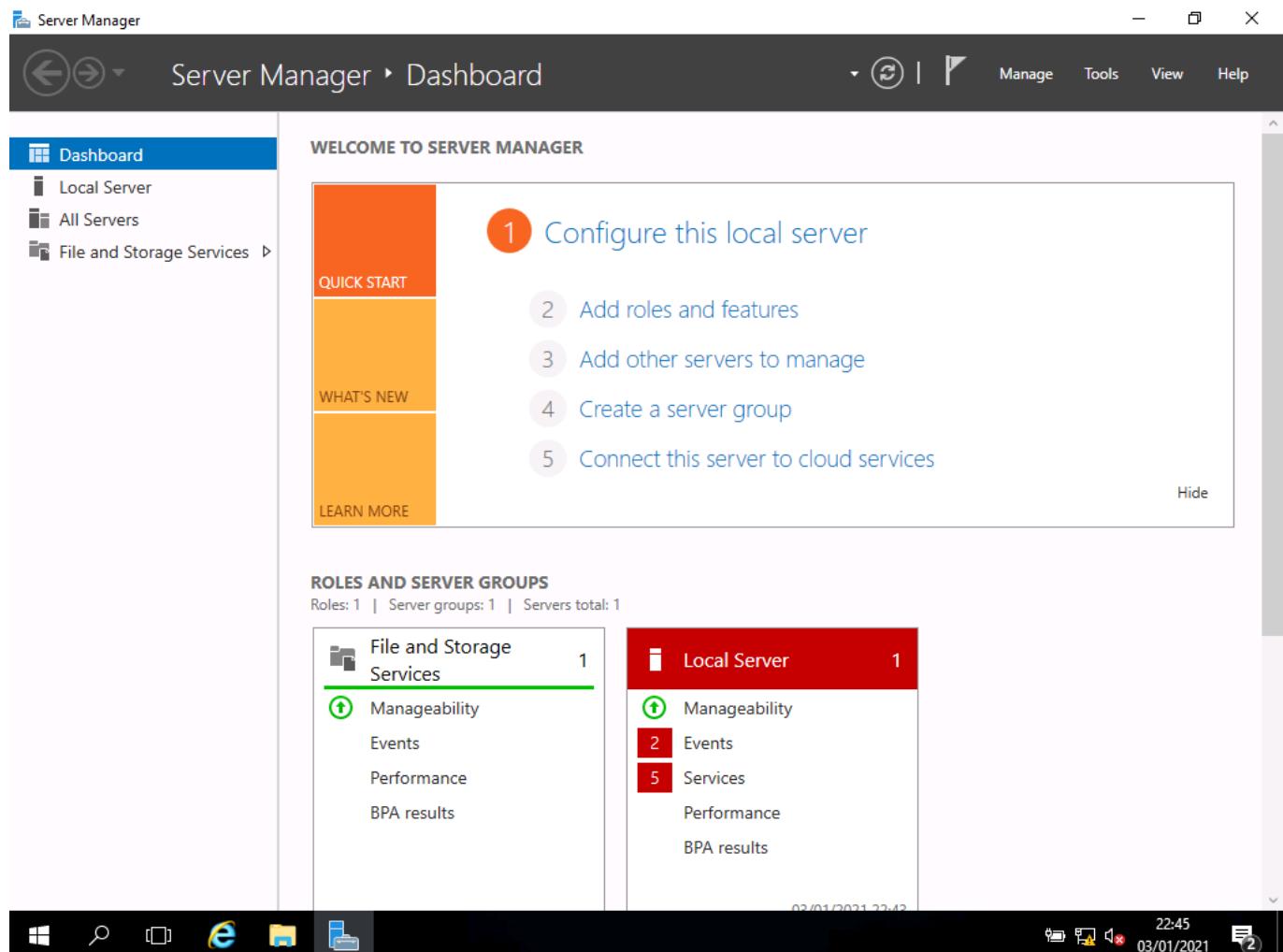


Adding name

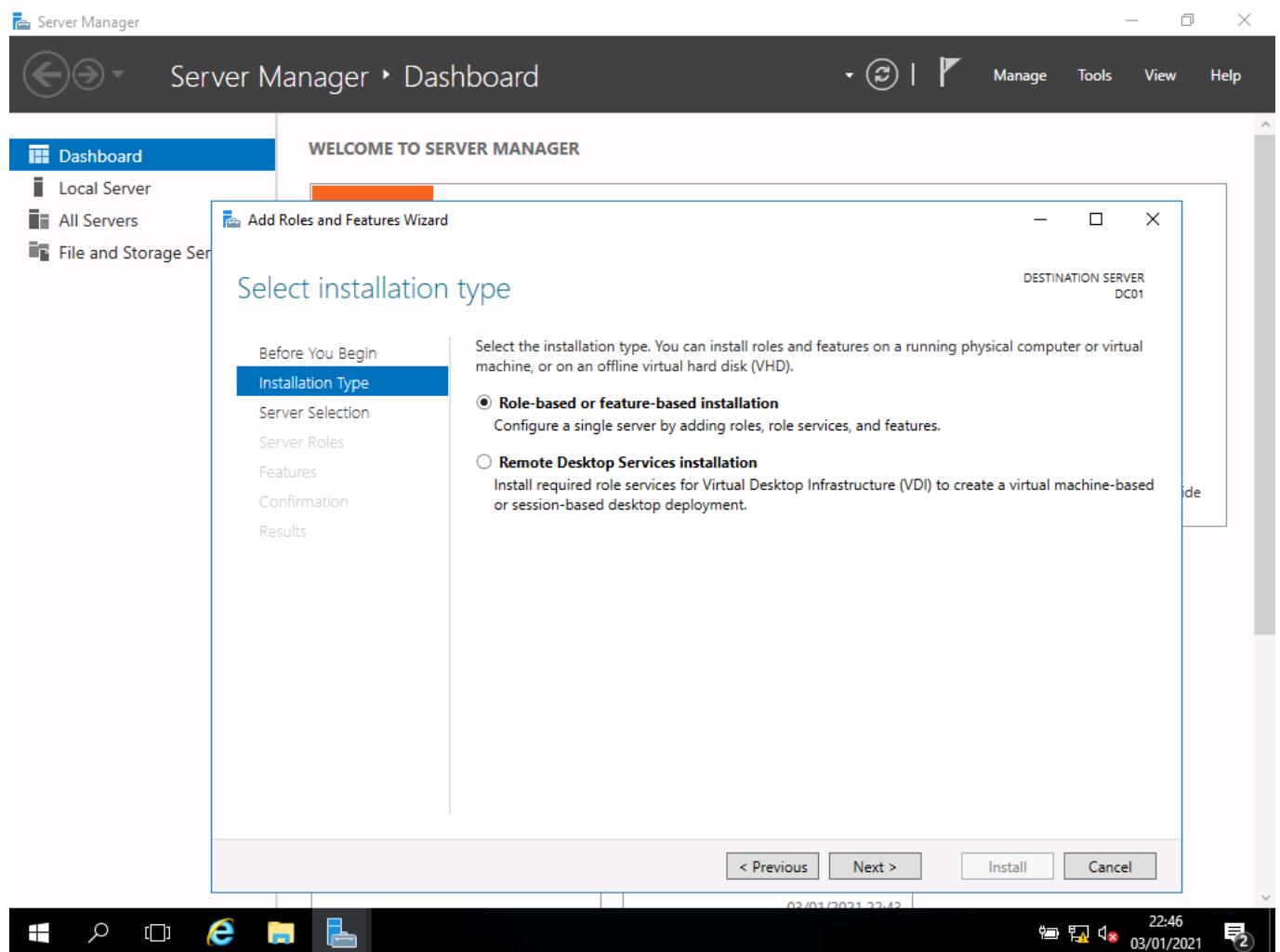
- The above 3 images show me opening the computer name settings and changing the computer name DC01

Allocating server roles

Screenshot

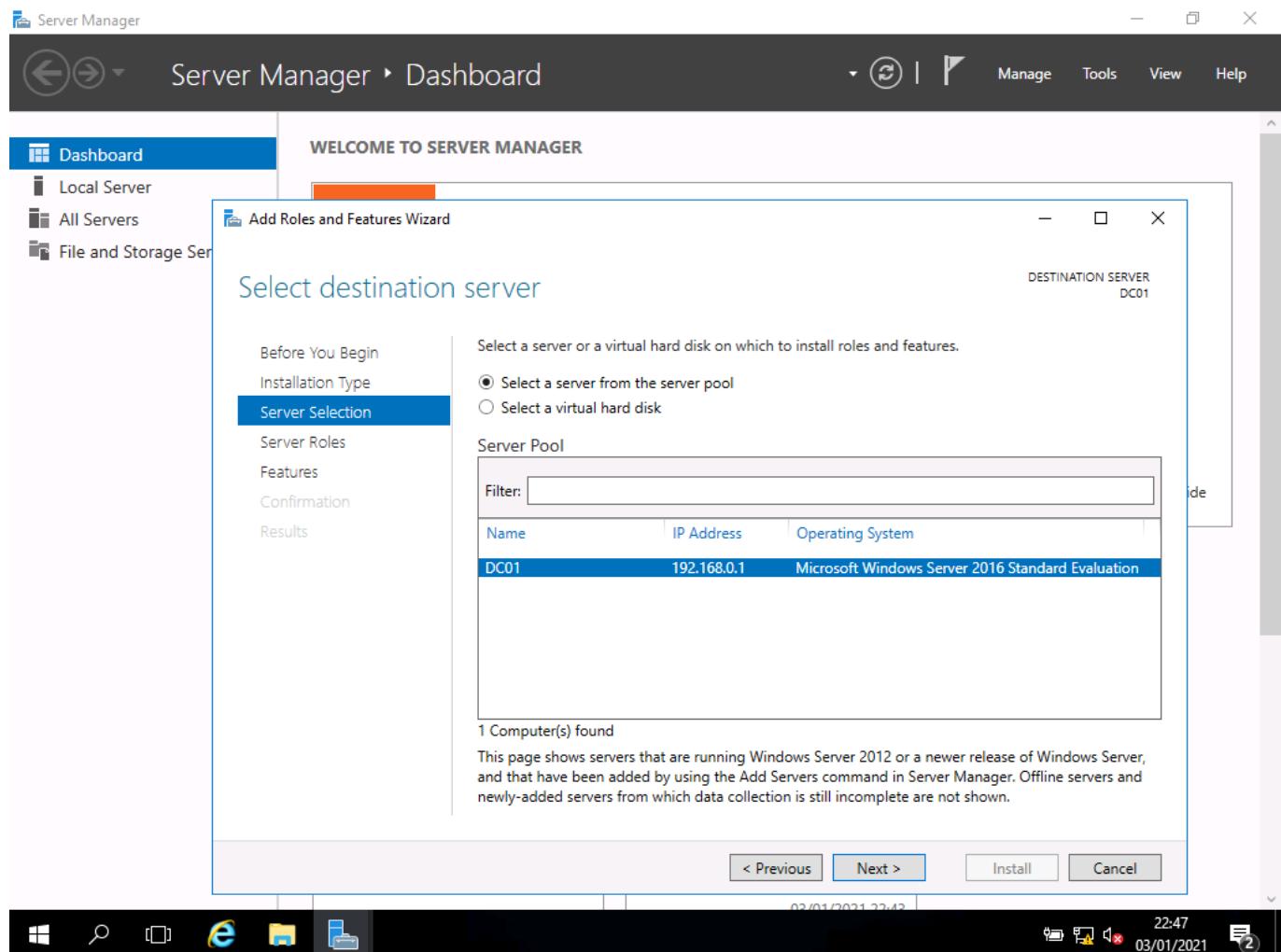


- I now open Server Manager



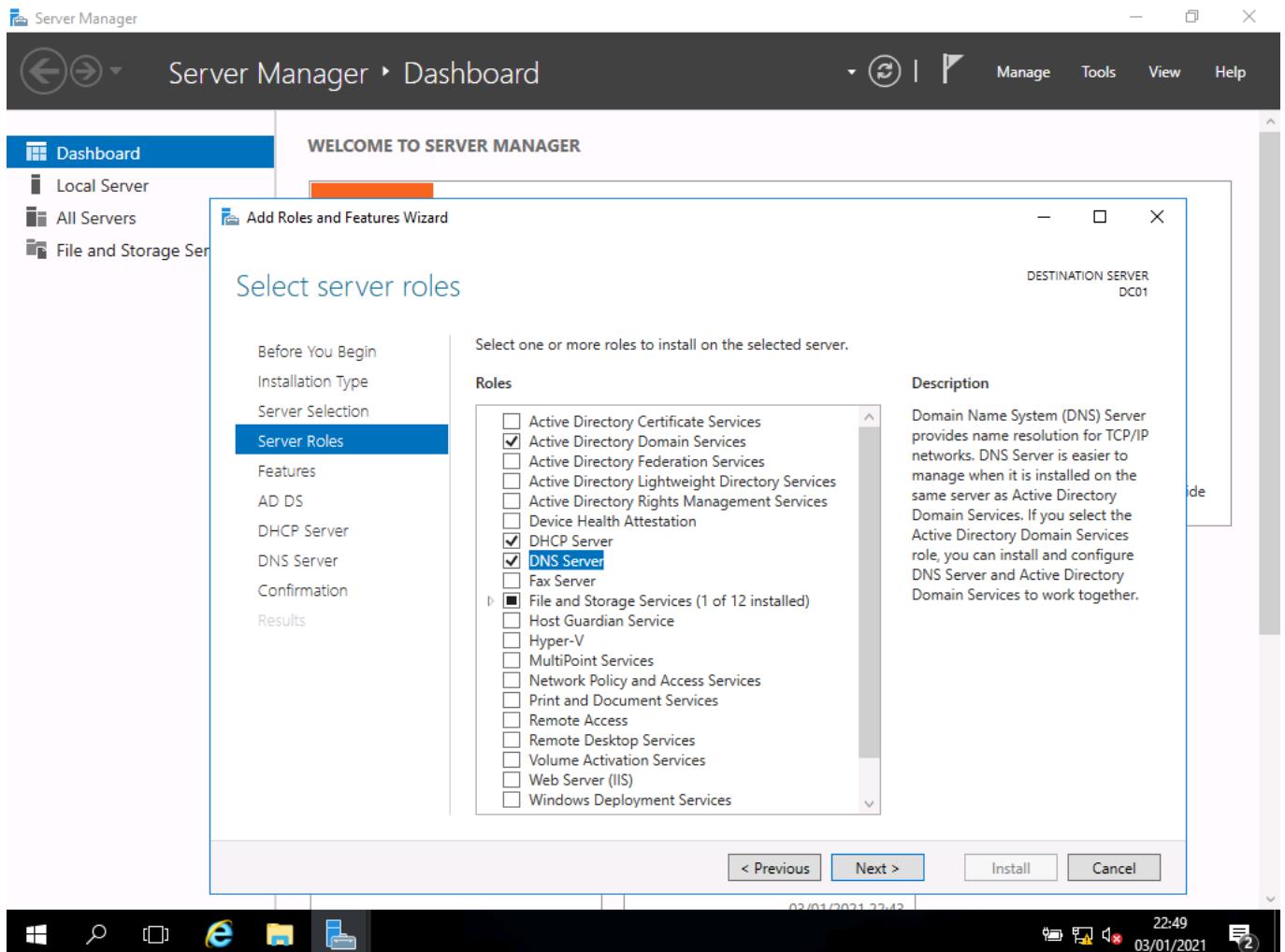
- I choose role-based installation to add the new roles as this is the easiest to use
- I can now set the roles for the server

Screenshot:

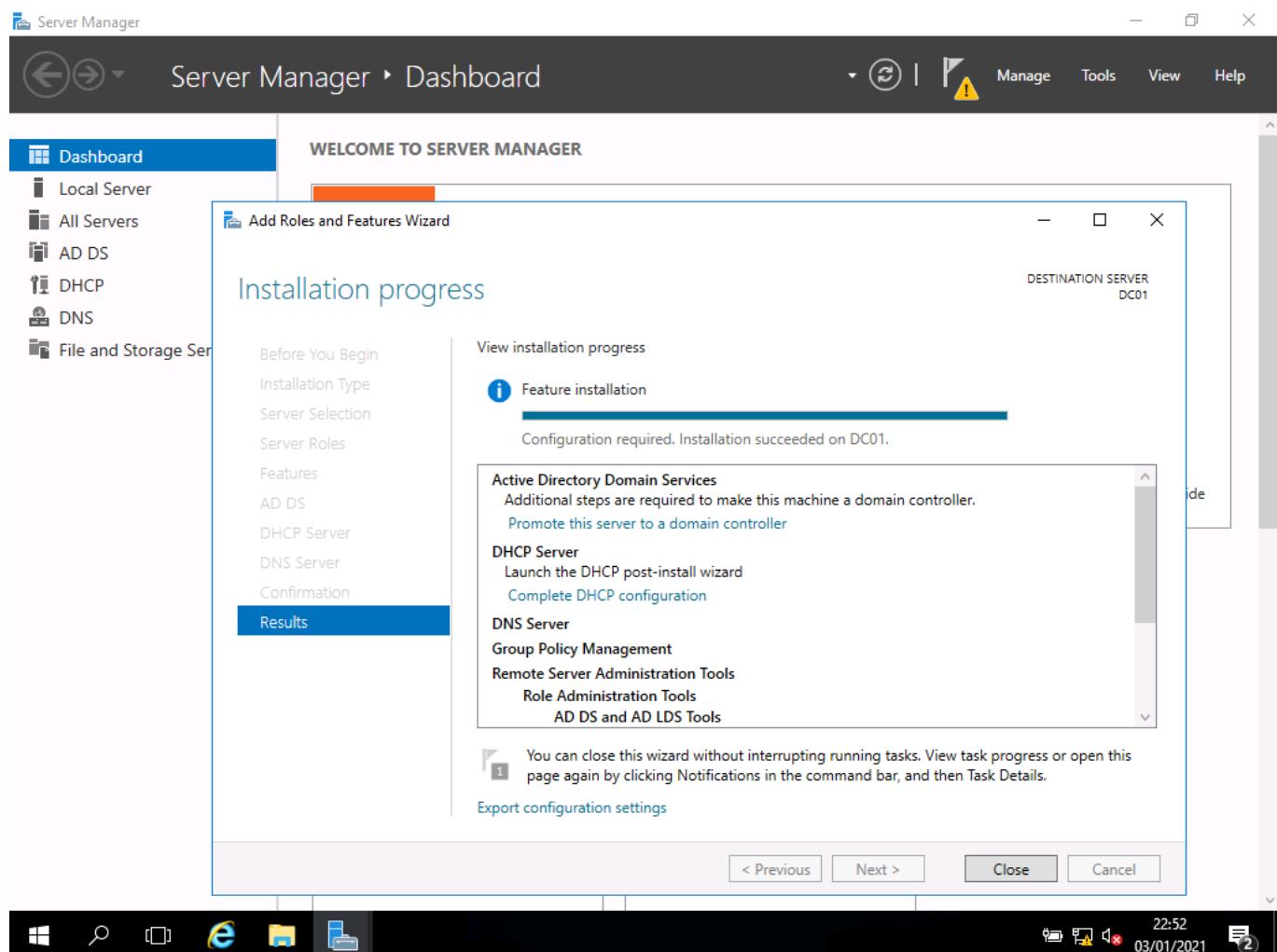


- I choose this server as it is the only one in the list

Screenshot:

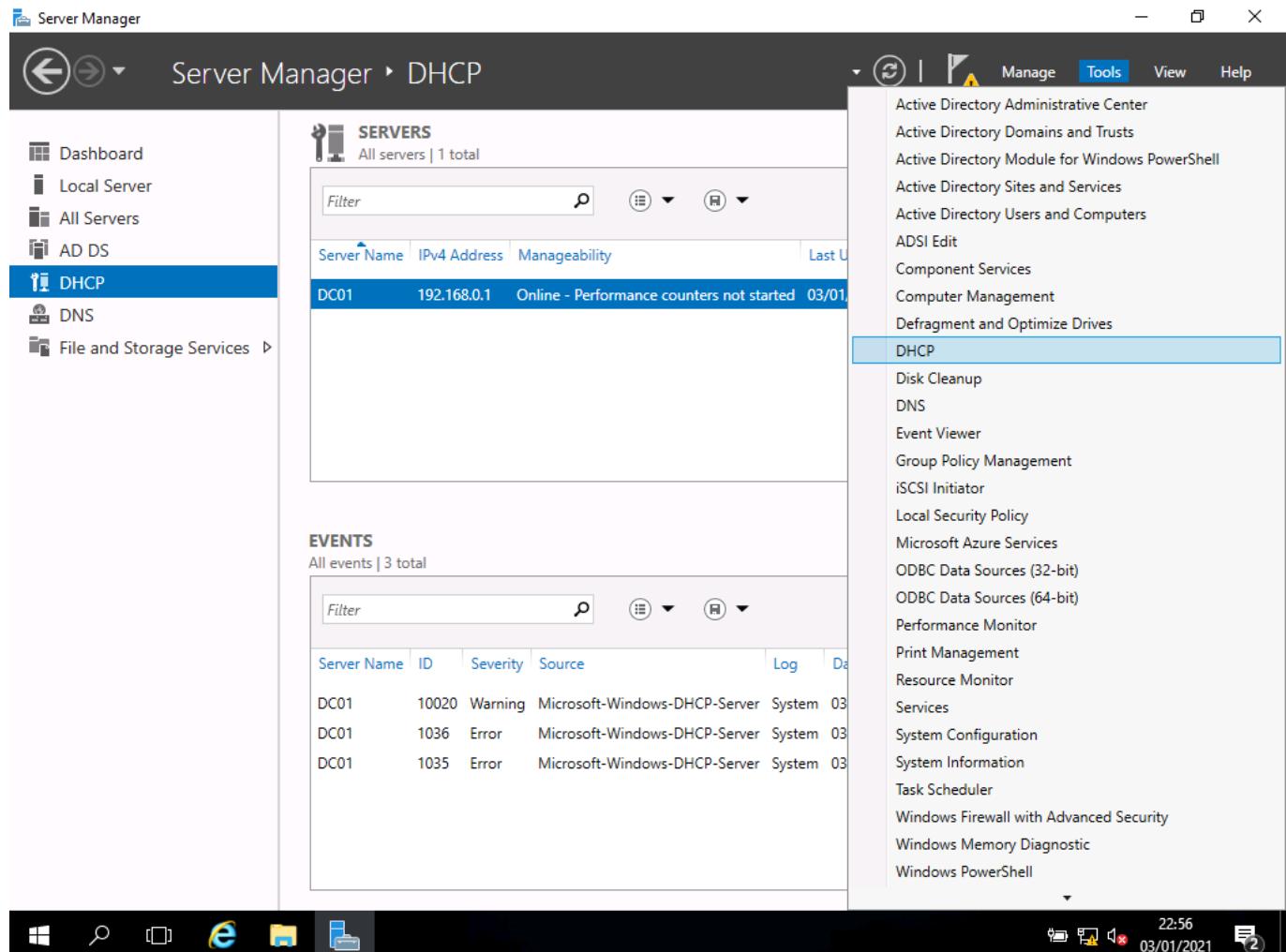


- I add the required features that I need to add, for example: Active Directory Domain Services, DHCP Server, DNS Server

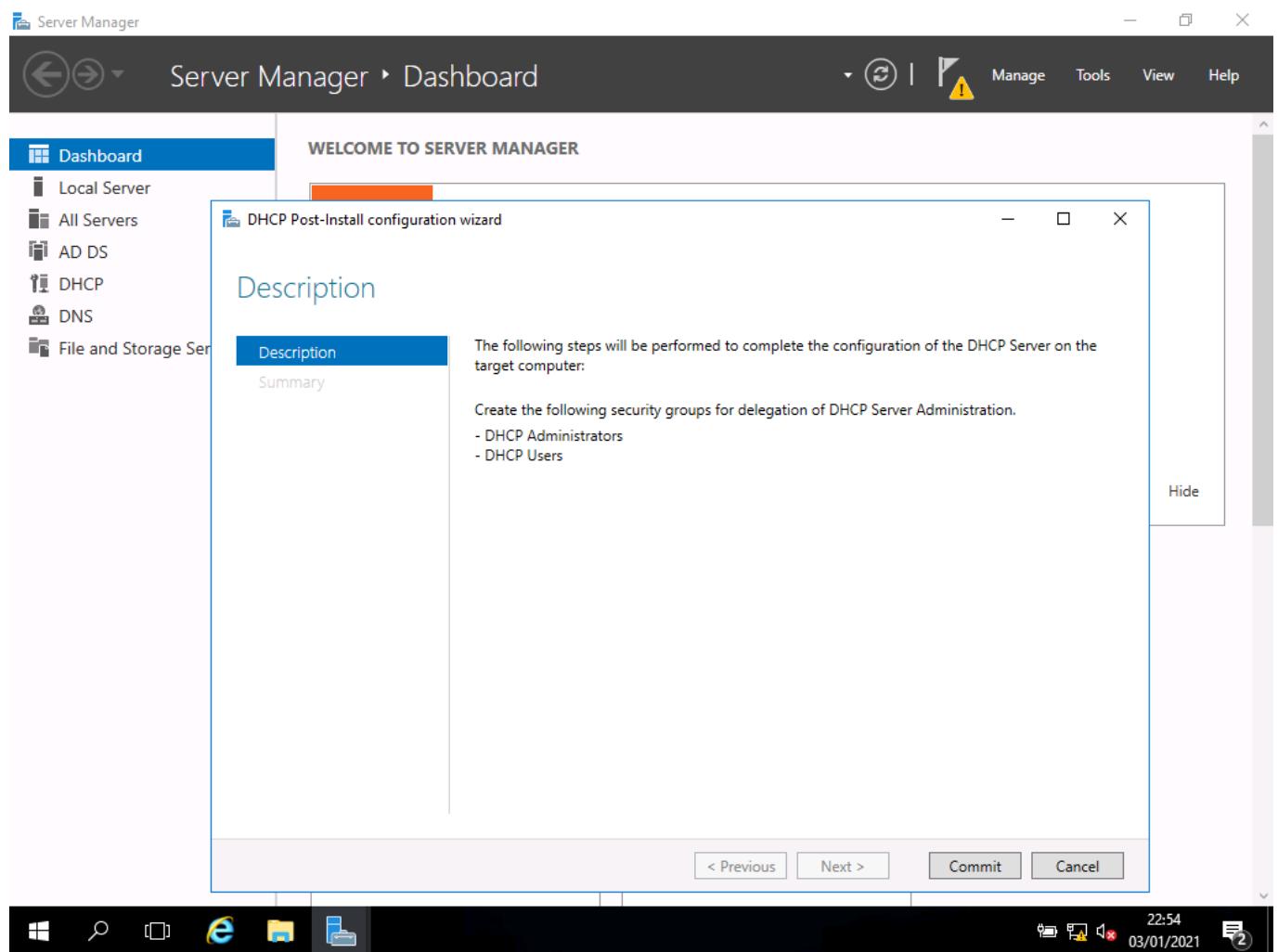


- These screenshots show the server roles of Active Directory, DNS, and DHCP
- Once the server has added the new roles and rebooted I can set-up the DHCP

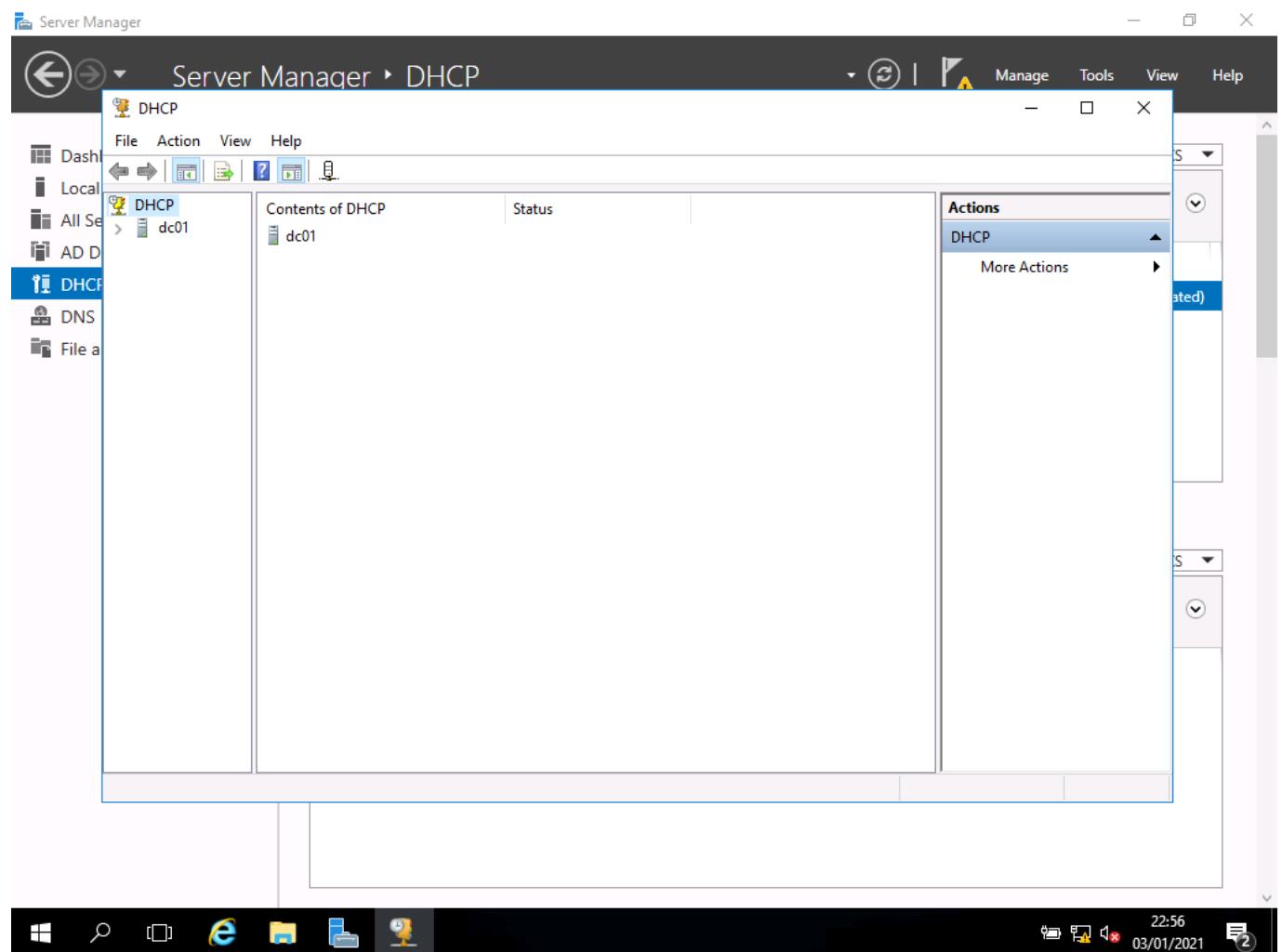
Setting up DHCP



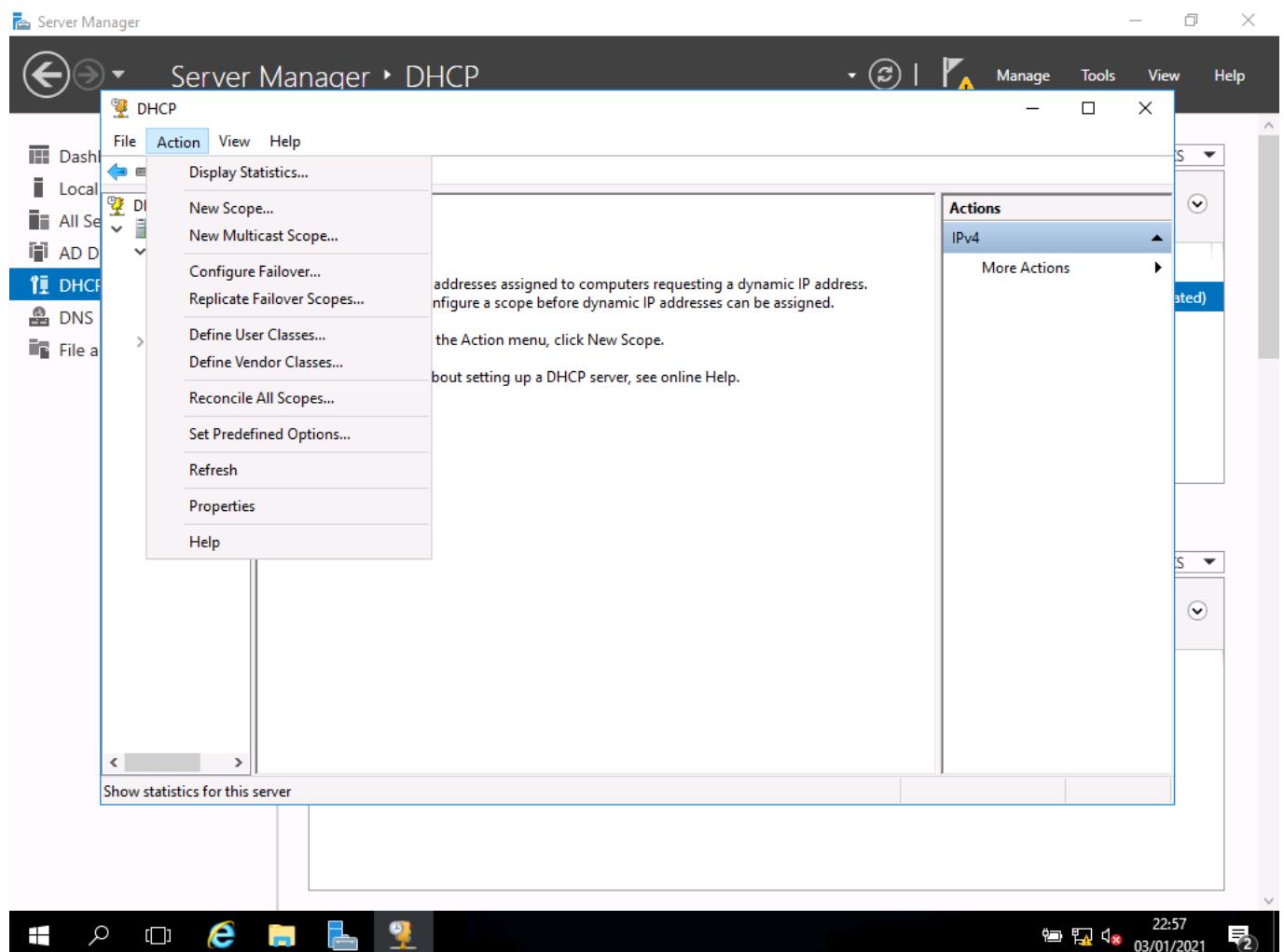
- From tools, I choose DHCP



- I click continue to go to the next step

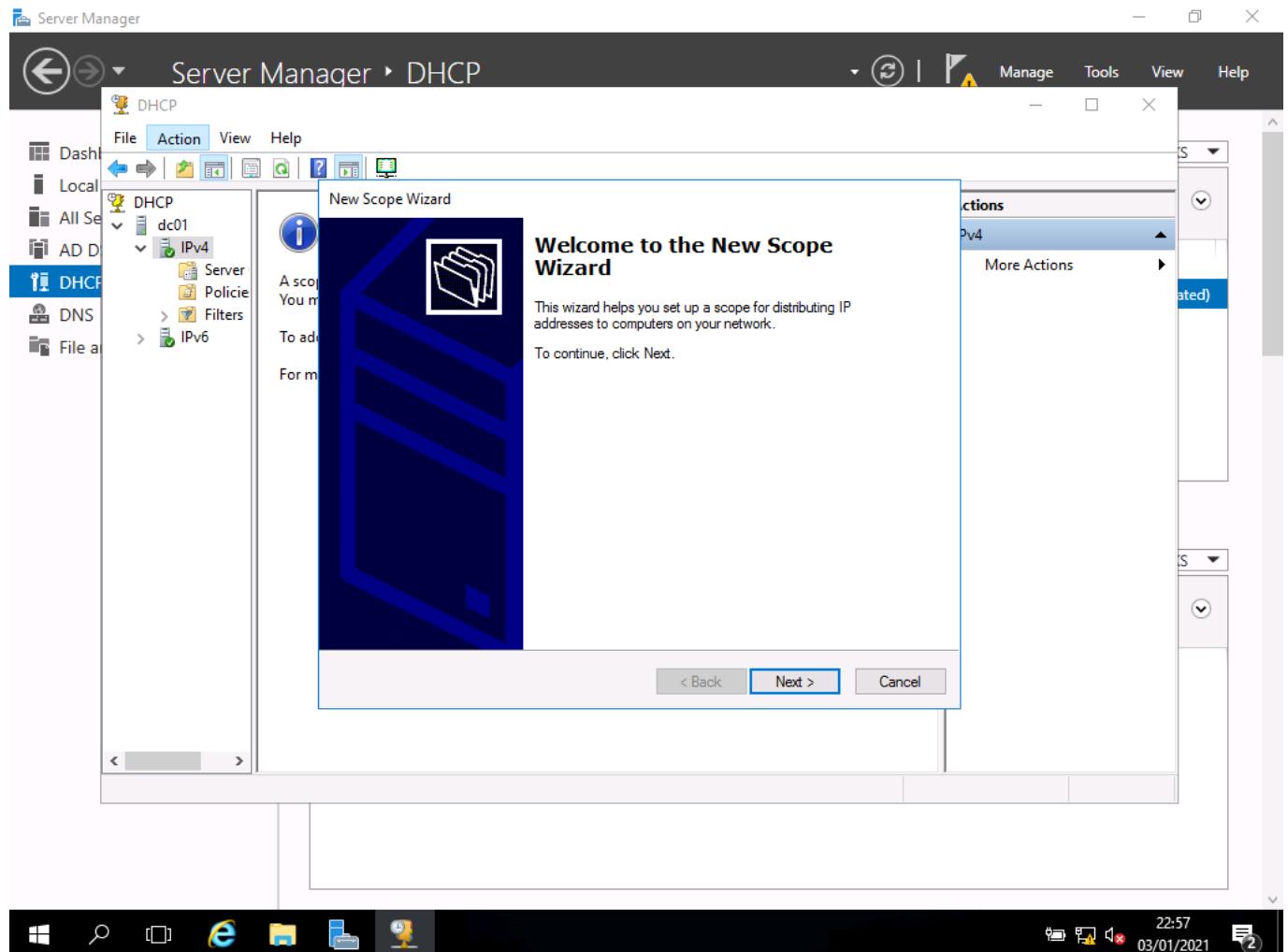


- I have now added DHCP

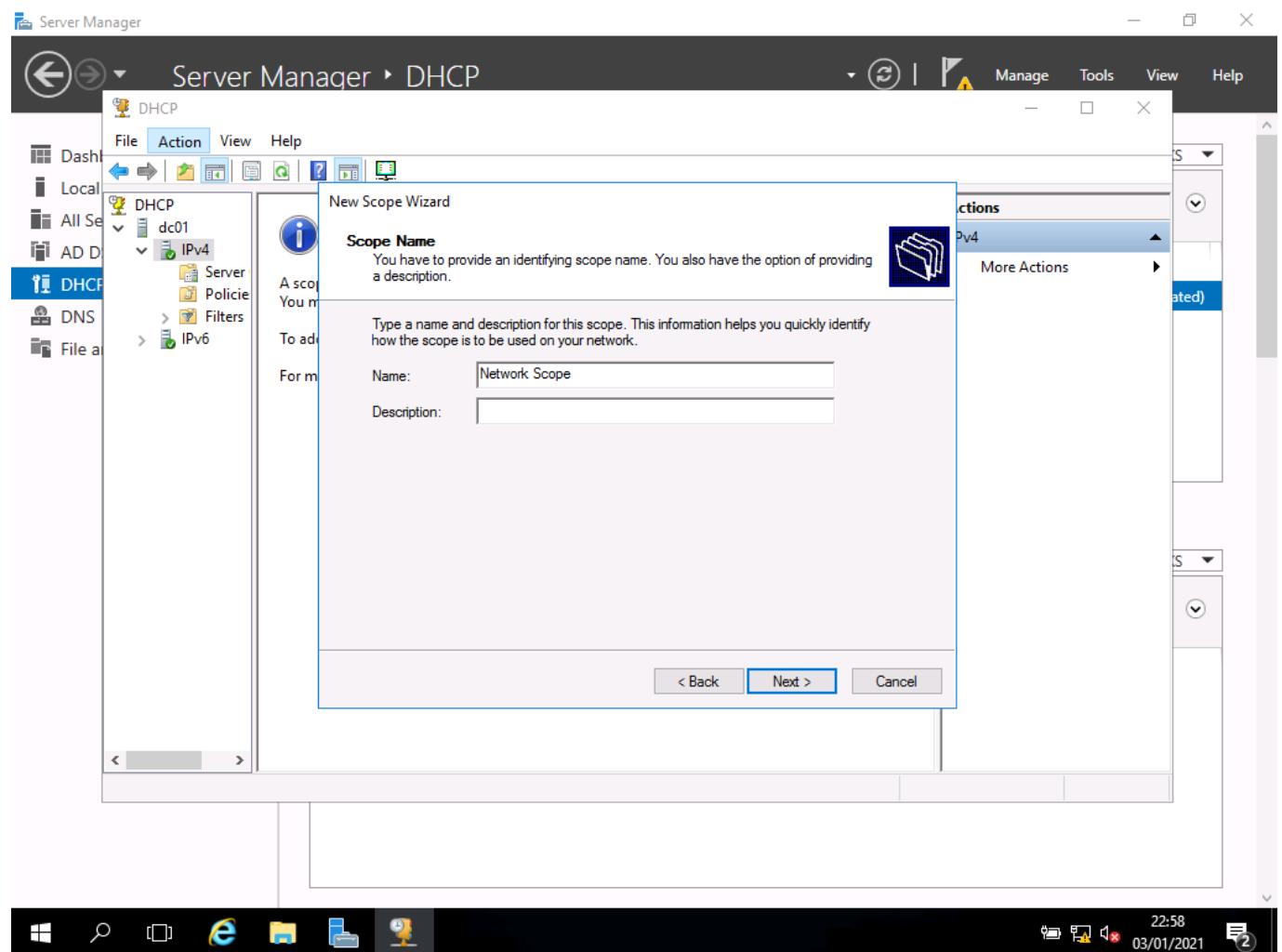


- I now add a new scope to give out the addresses

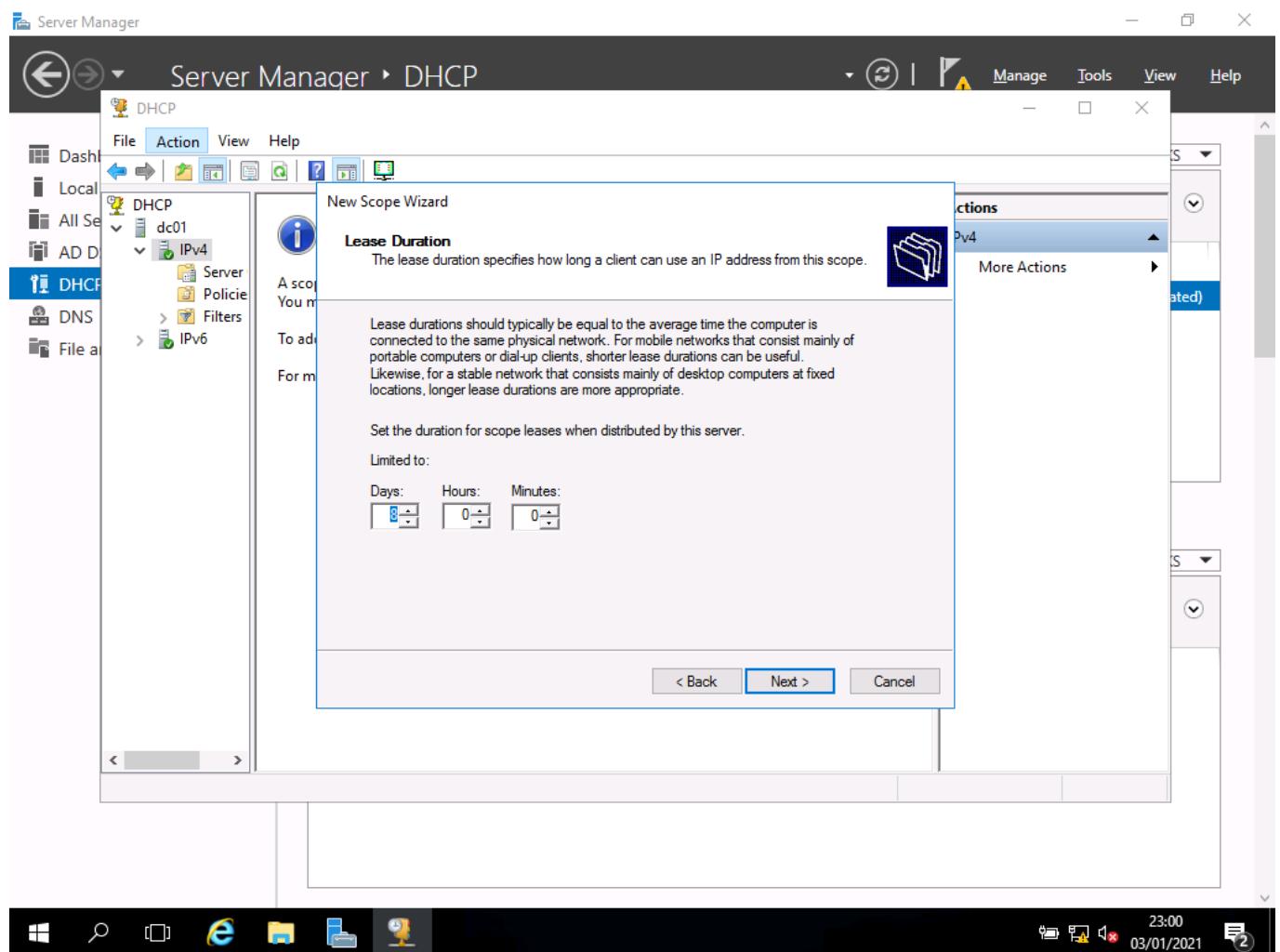
Selecting new scope



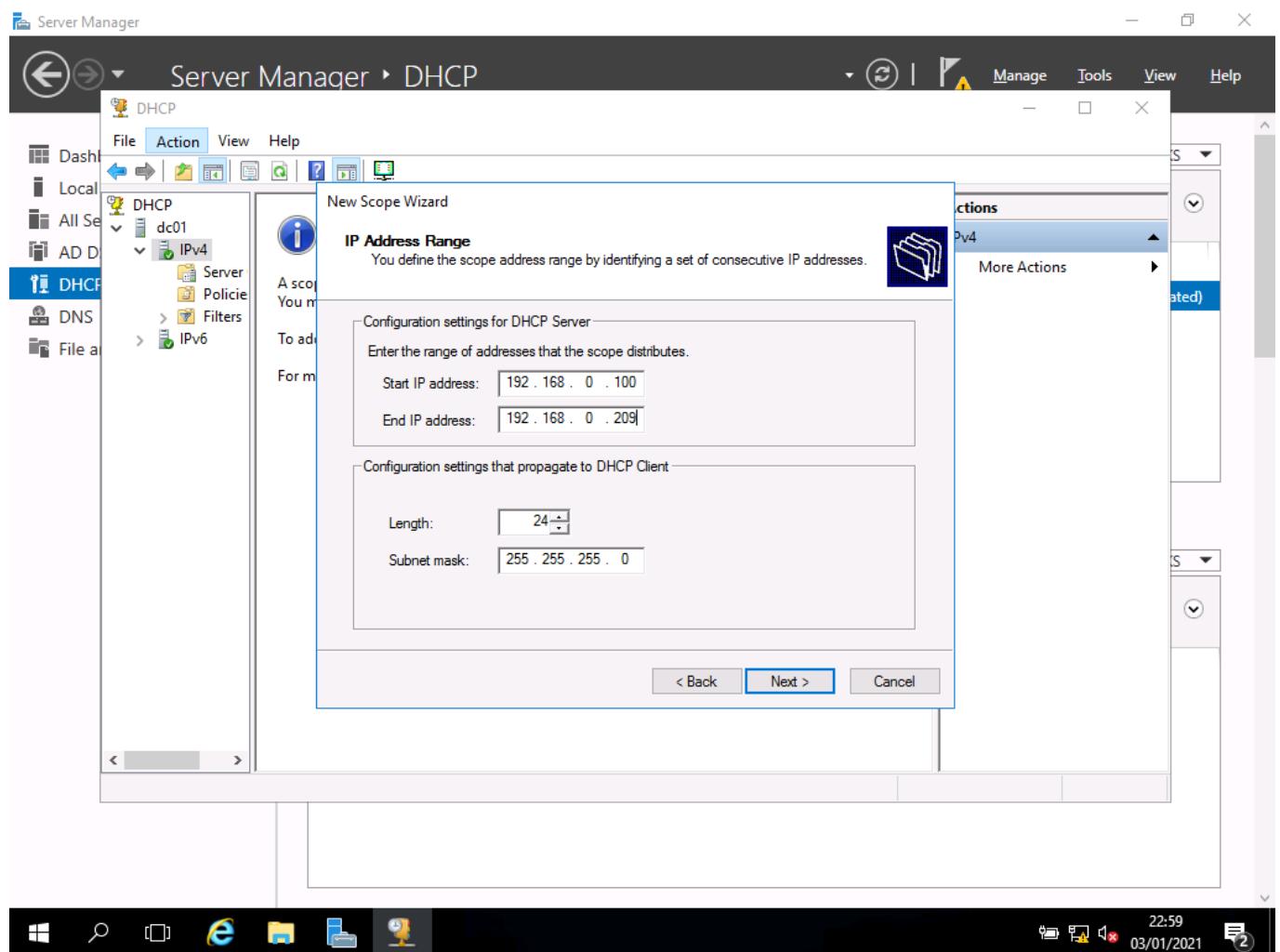
- I run the New Scope Wizard



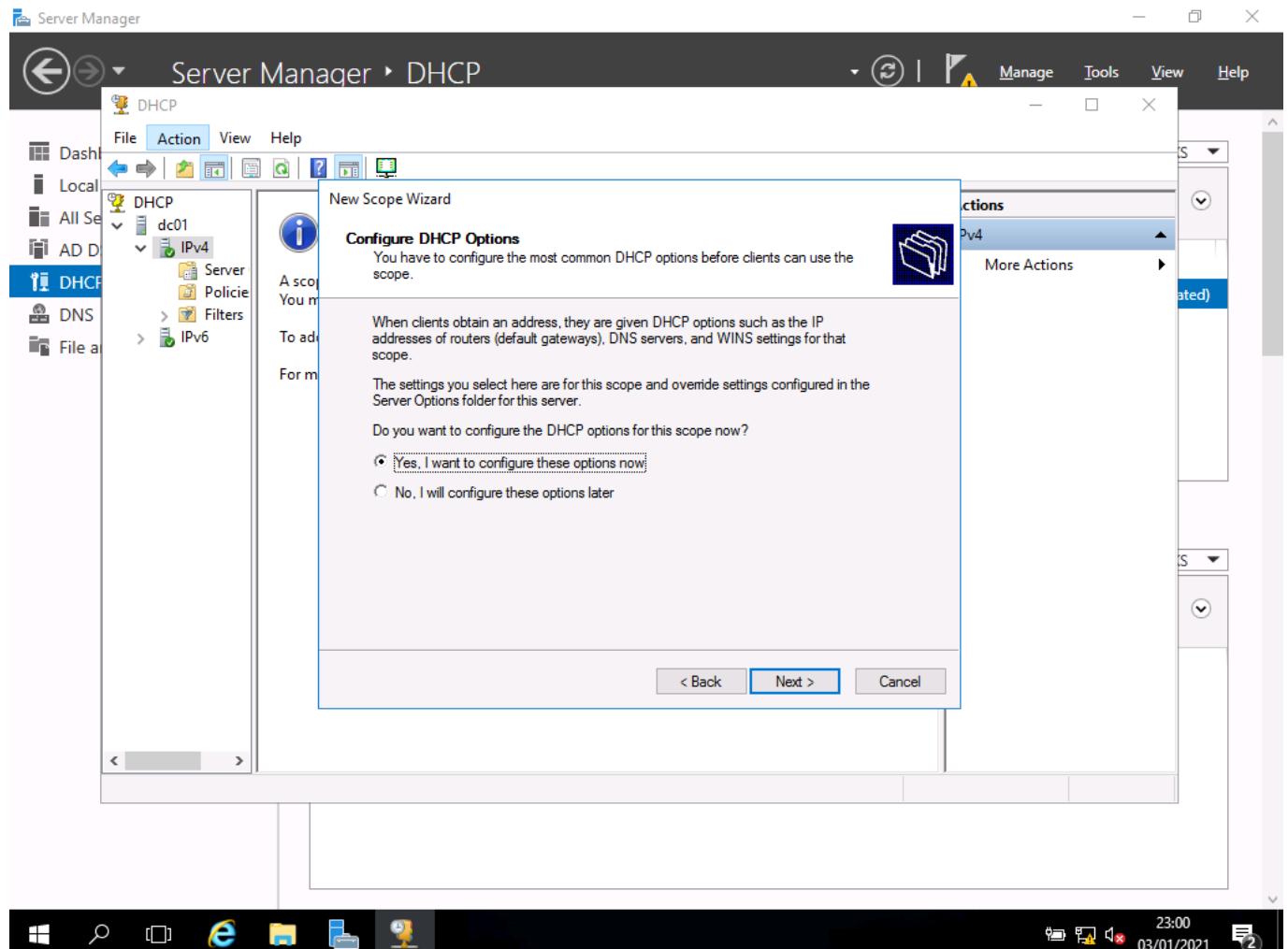
- I leave the default settings as these are OK to use



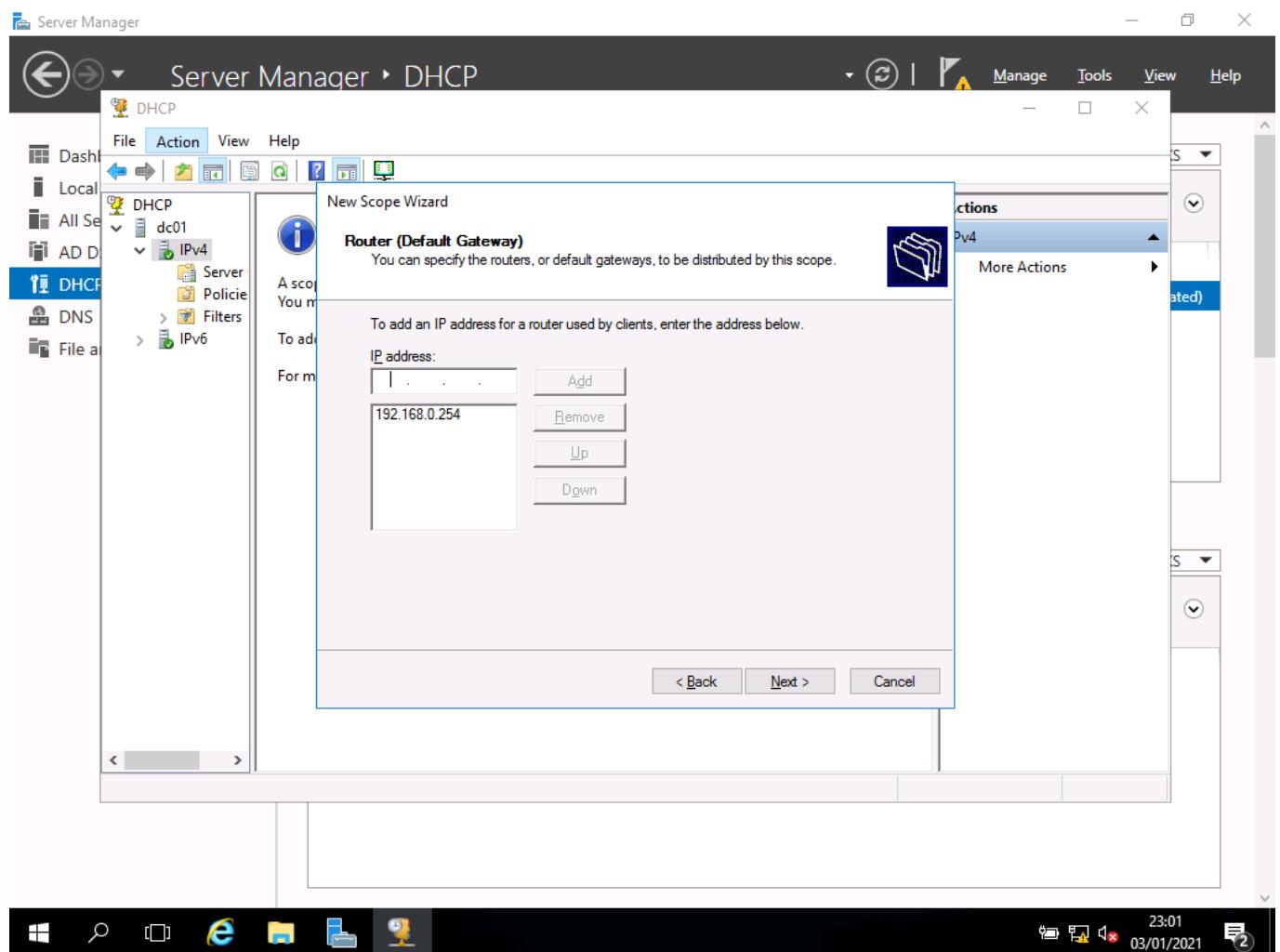
- I add a lease time of 8 days, which is the normal length of time set



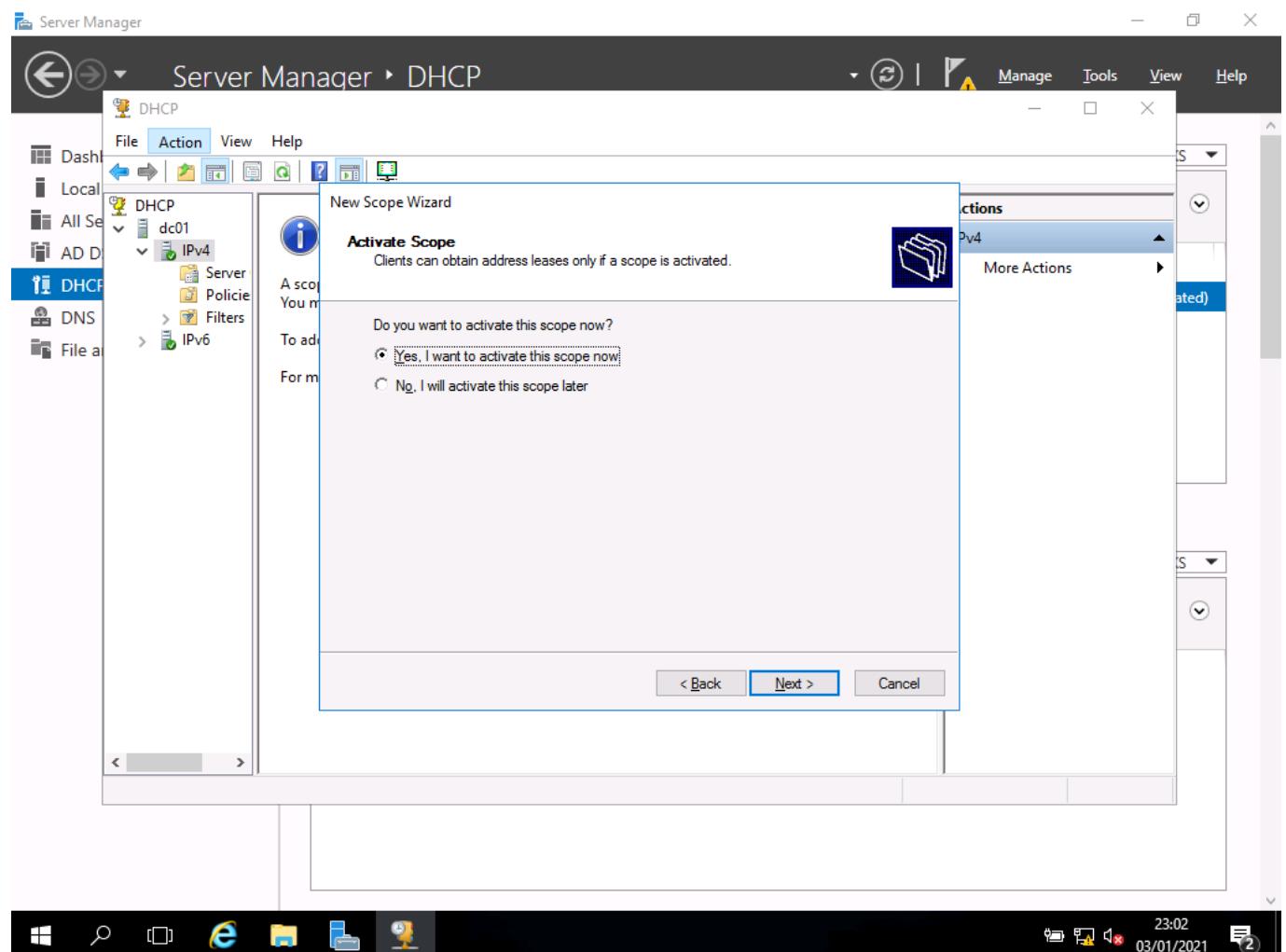
- I add a DHCP range for the addresses to give out.
- I add a range of addresses to use



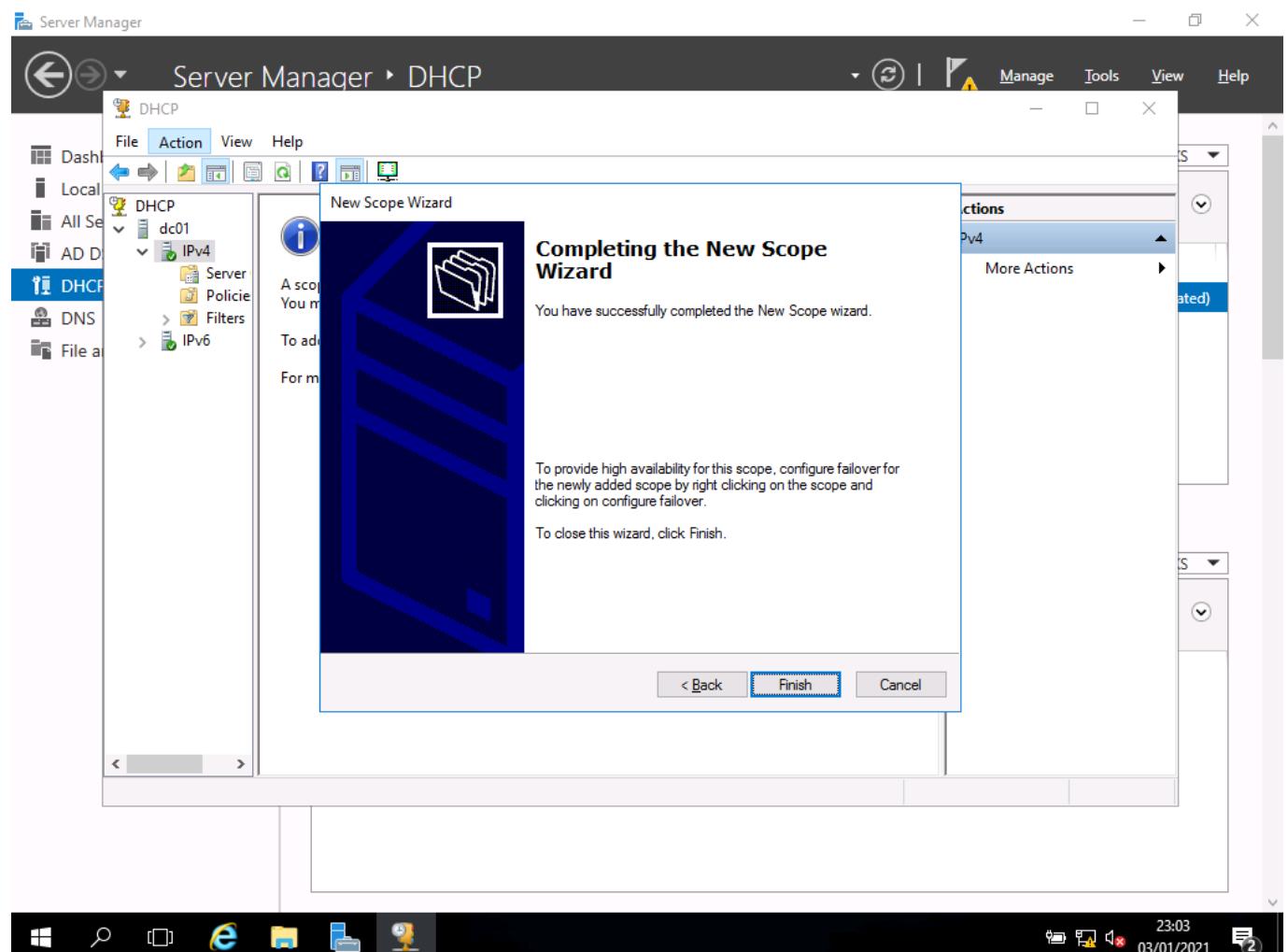
- I add options



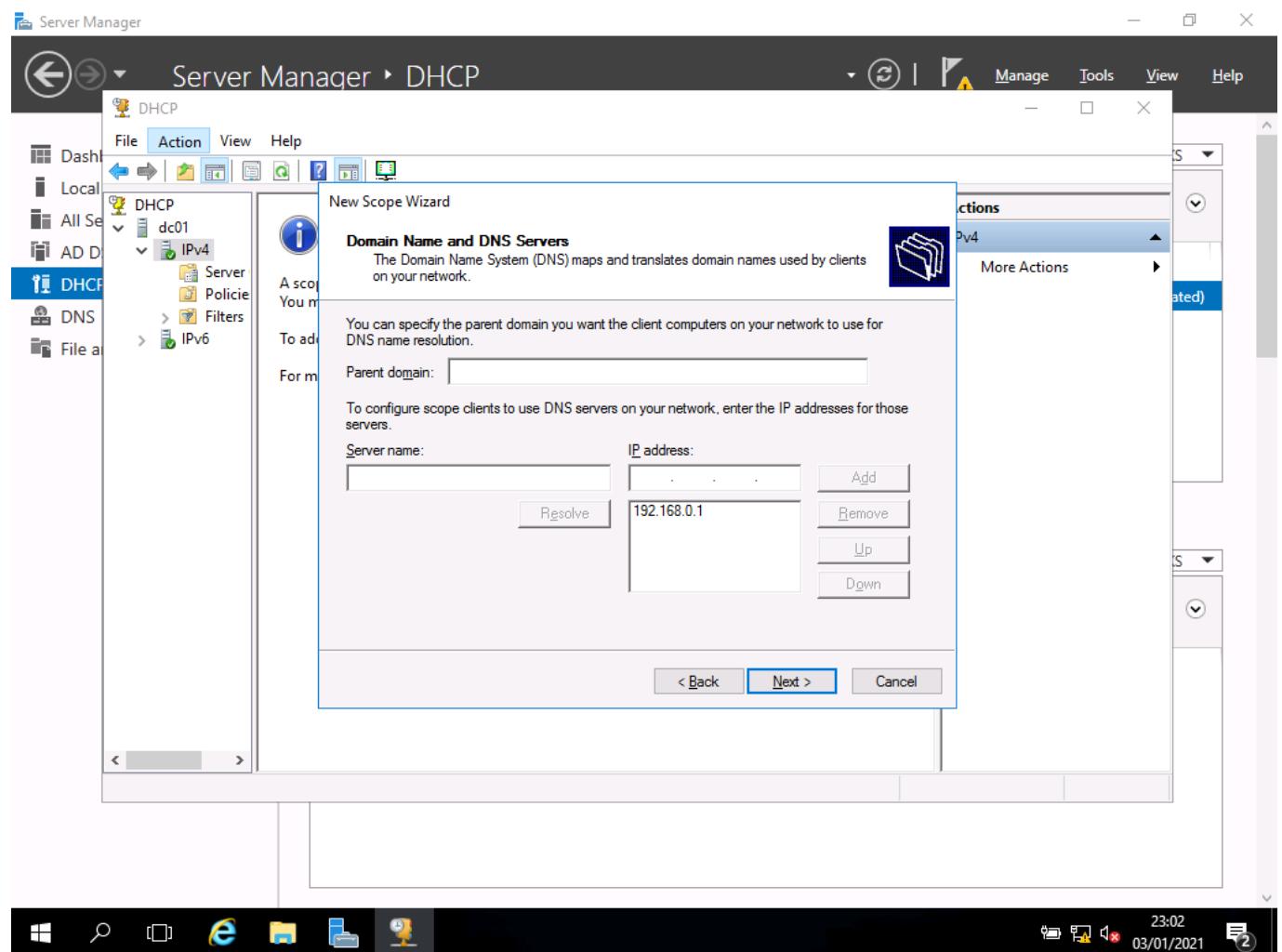
- I set the Gateway address. This is the router for connecting to the internet



Once the scope is made, I need to activate it so that it will give out address



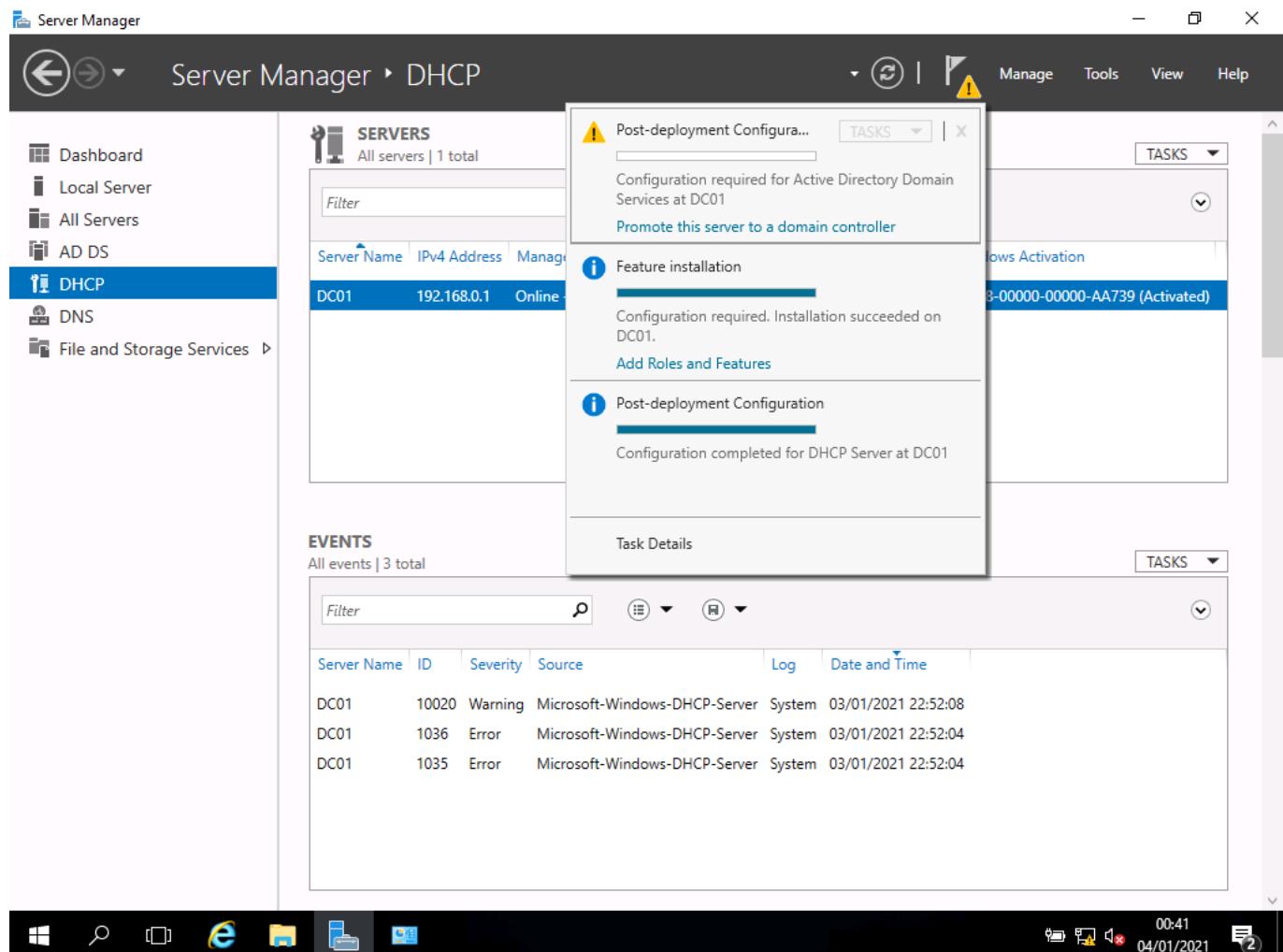
I click finish to complete installation



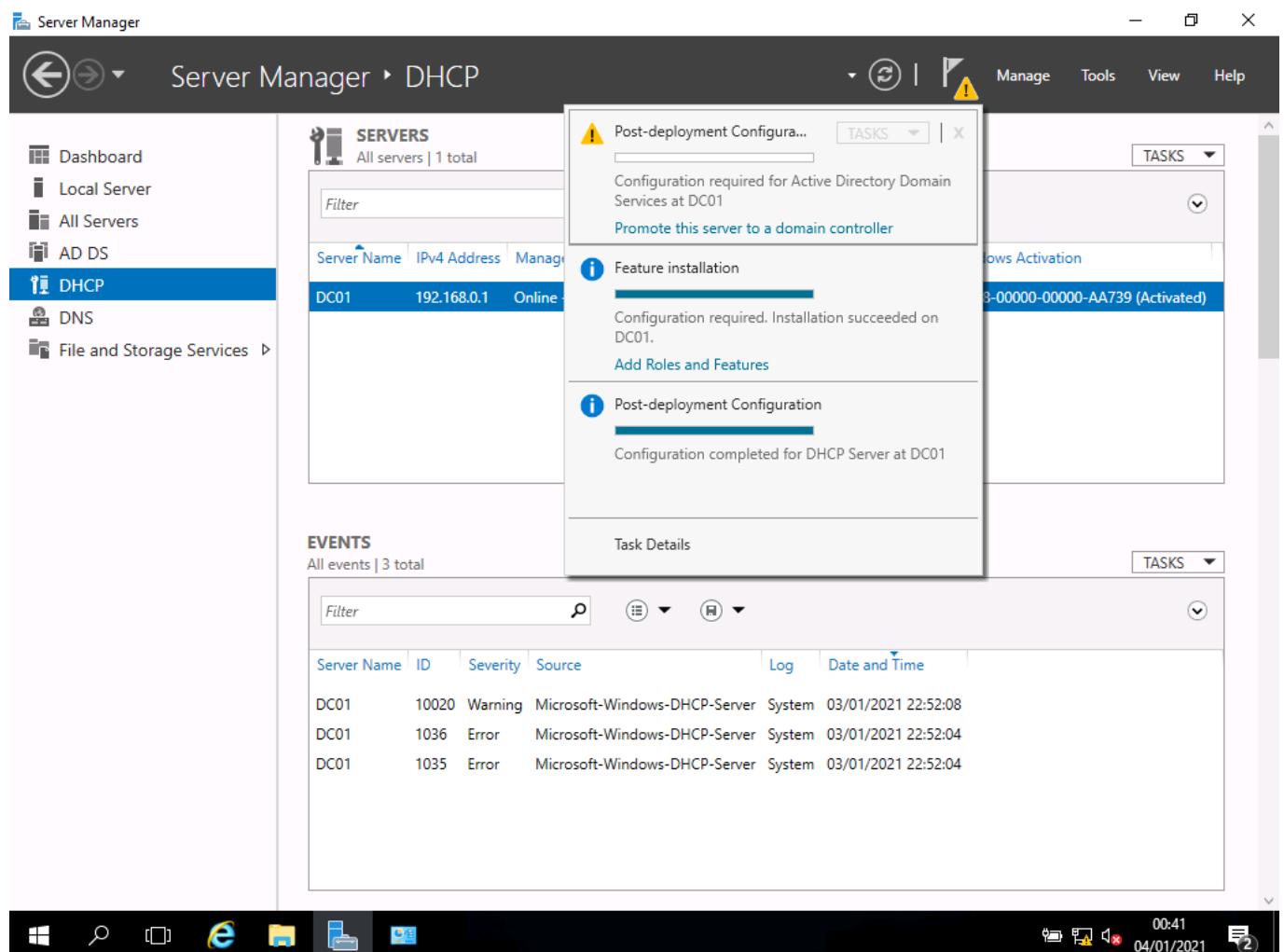
- I have set-up DHCP and activated it

Setting up Active Directory

Screenshot:



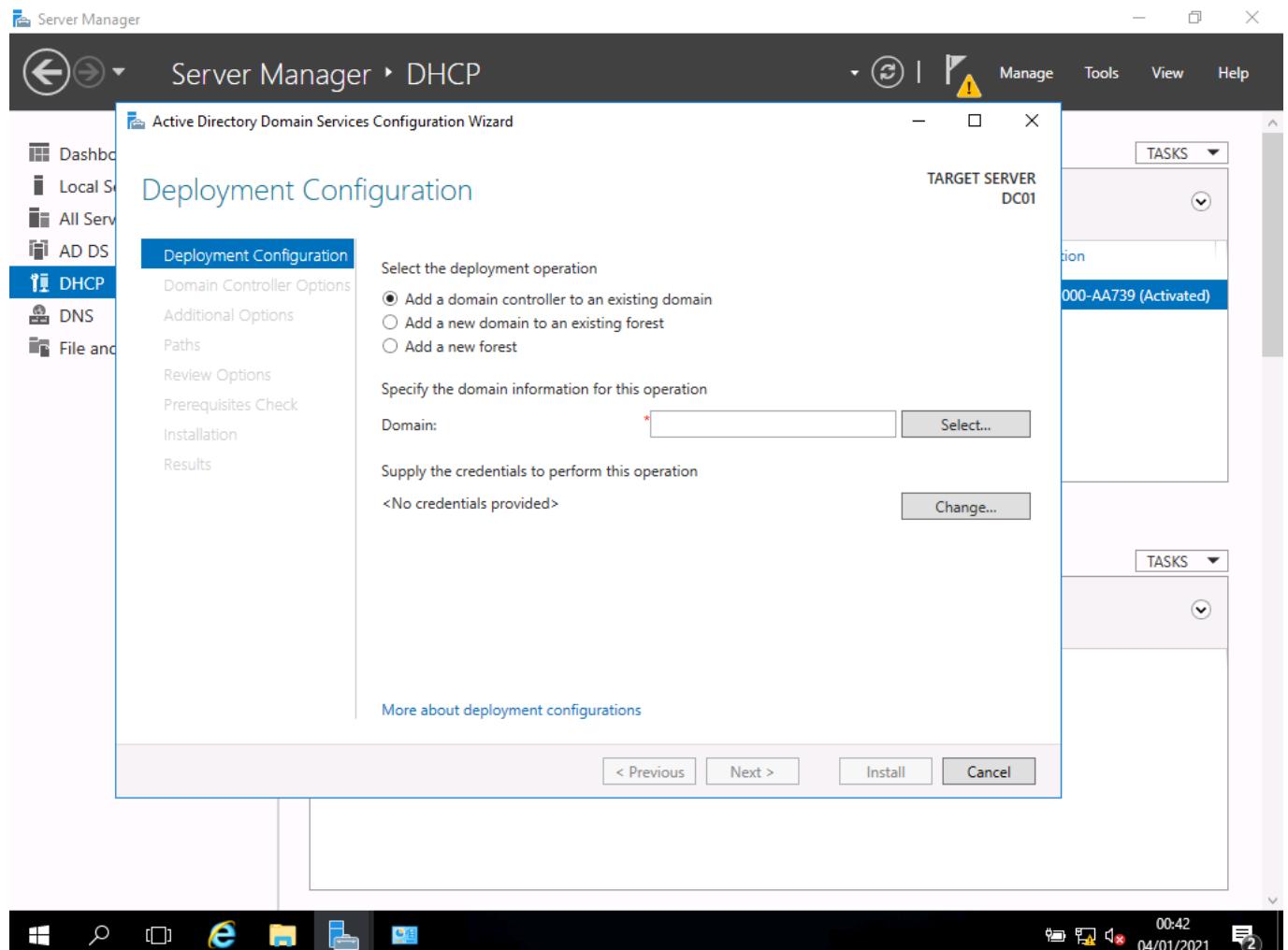
- I clicked on the yellow warning in server manager and selected promote this server to a domain controller



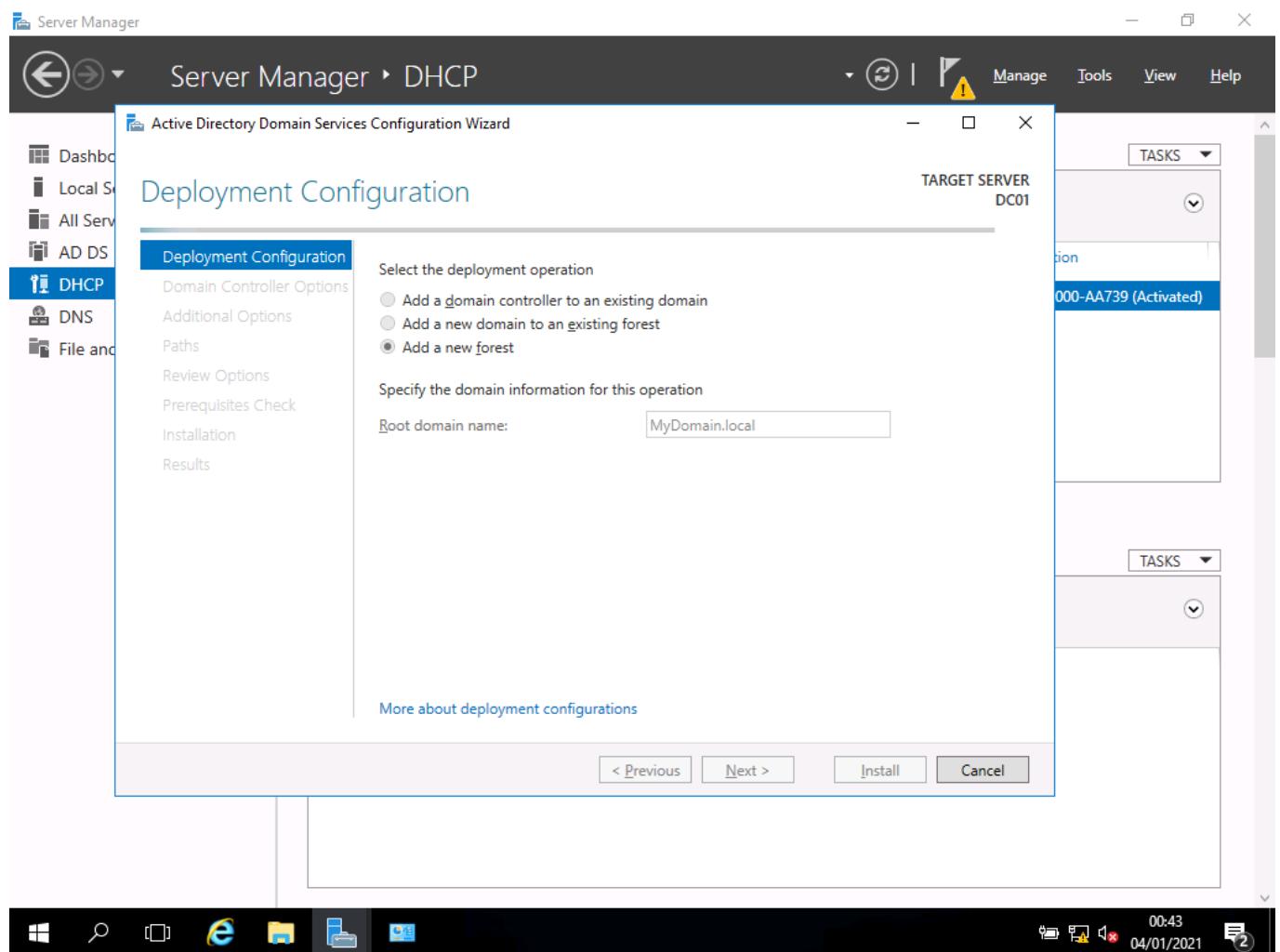
Here we can see the progress of the new features we are installing on the server

Screenshots:

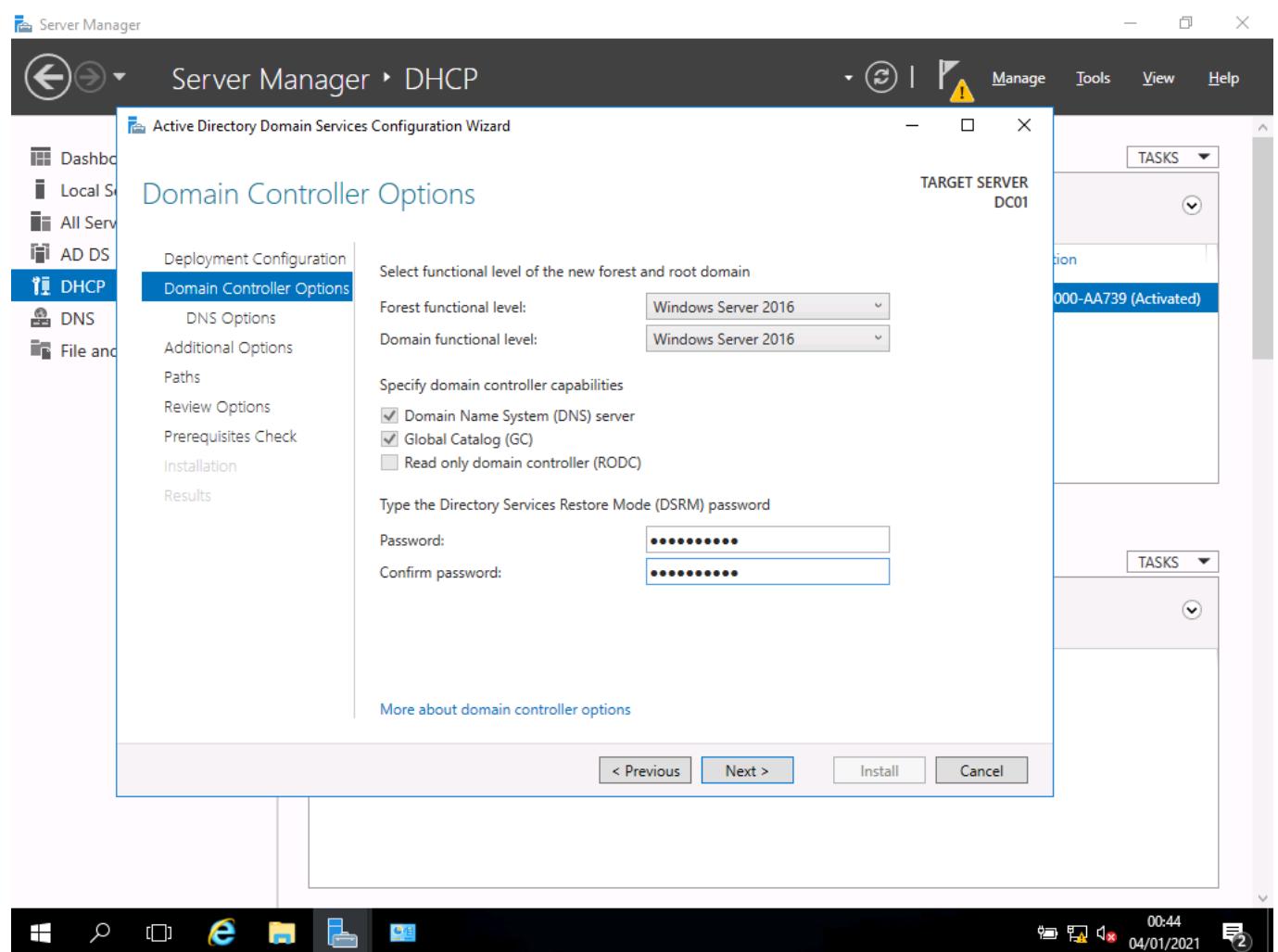
Set domain options



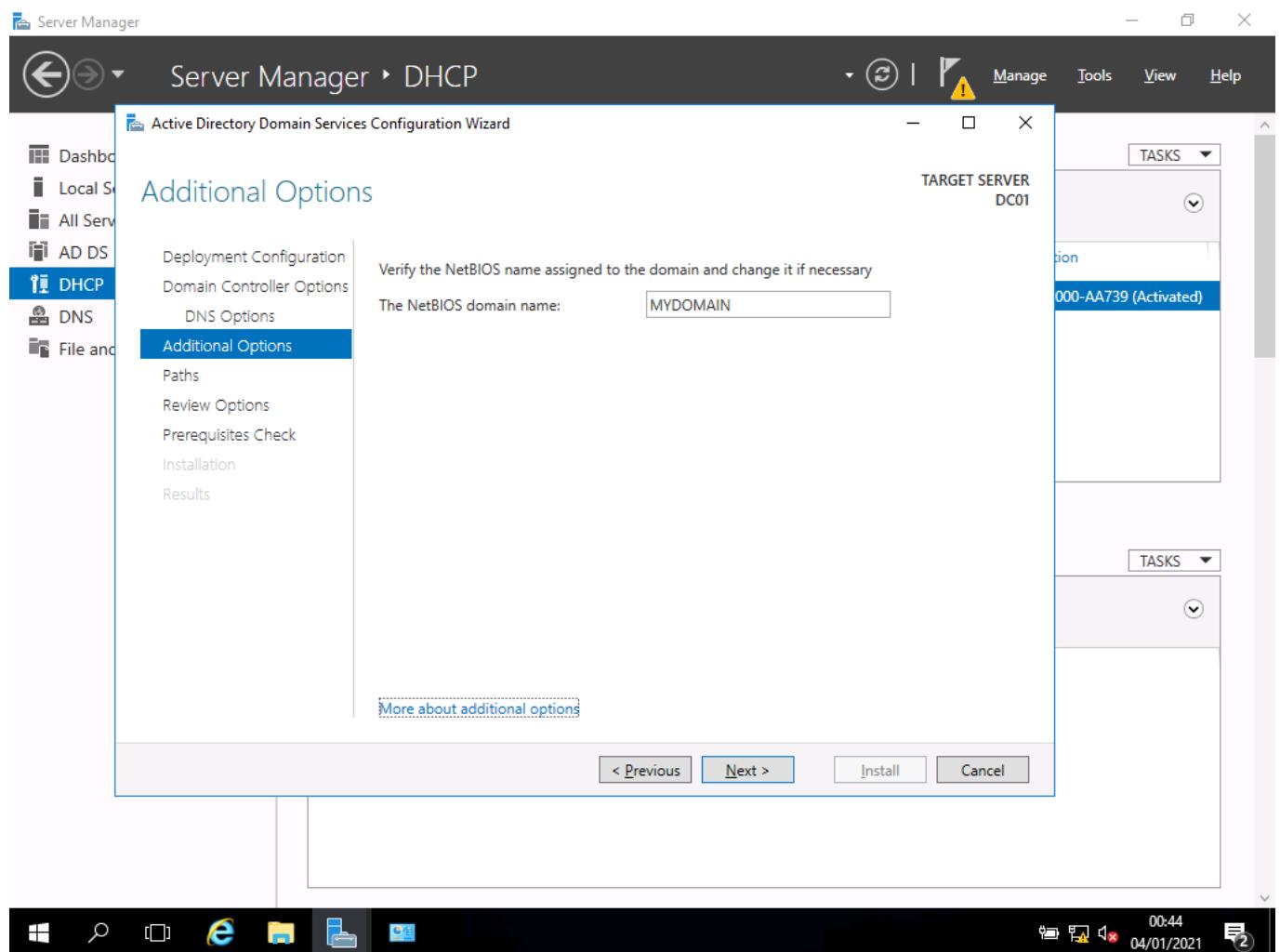
- I add a Deployment Configuration to this PC



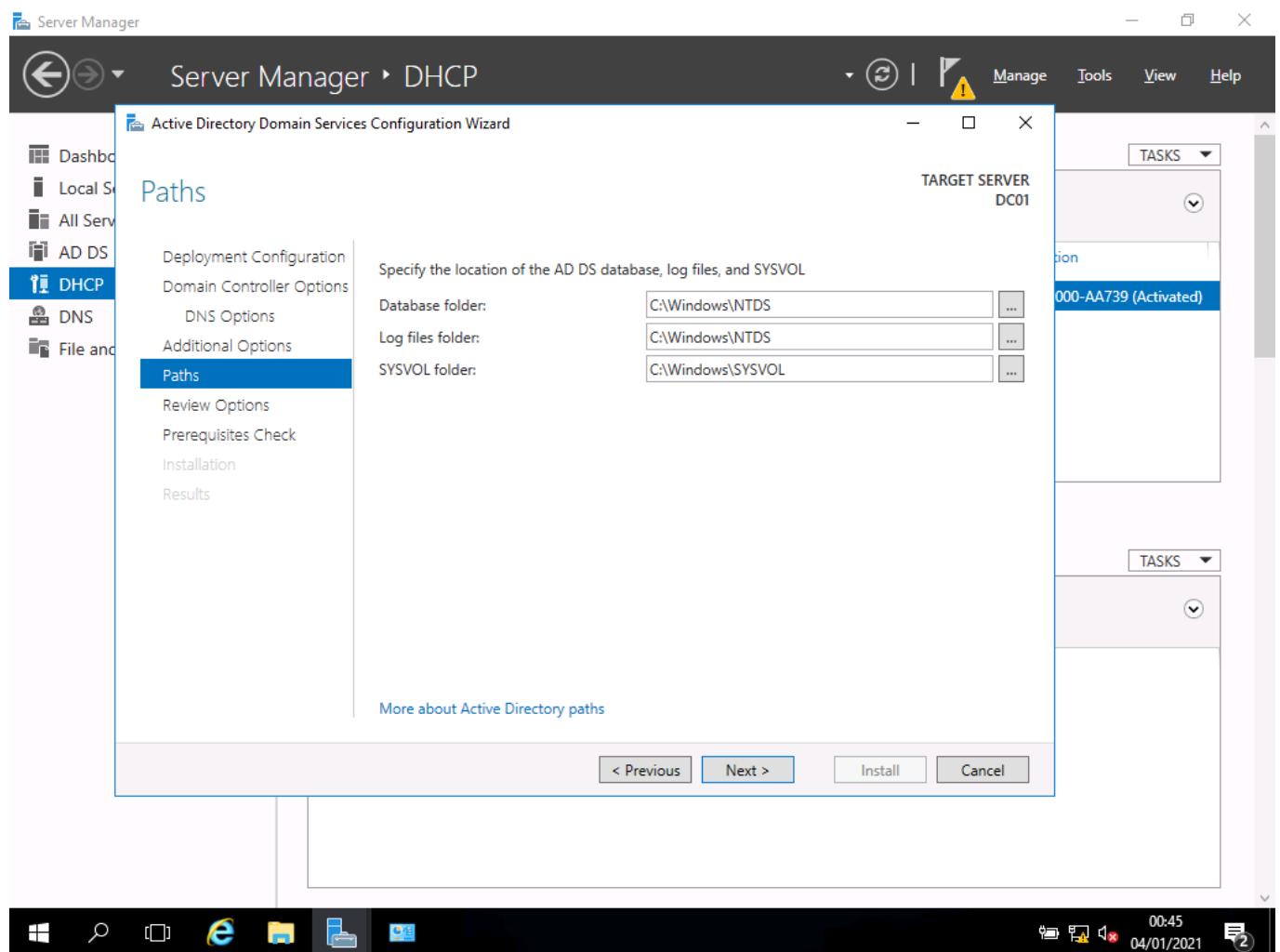
- I keep the default settings. This will make a new forest that you need when this is the first server



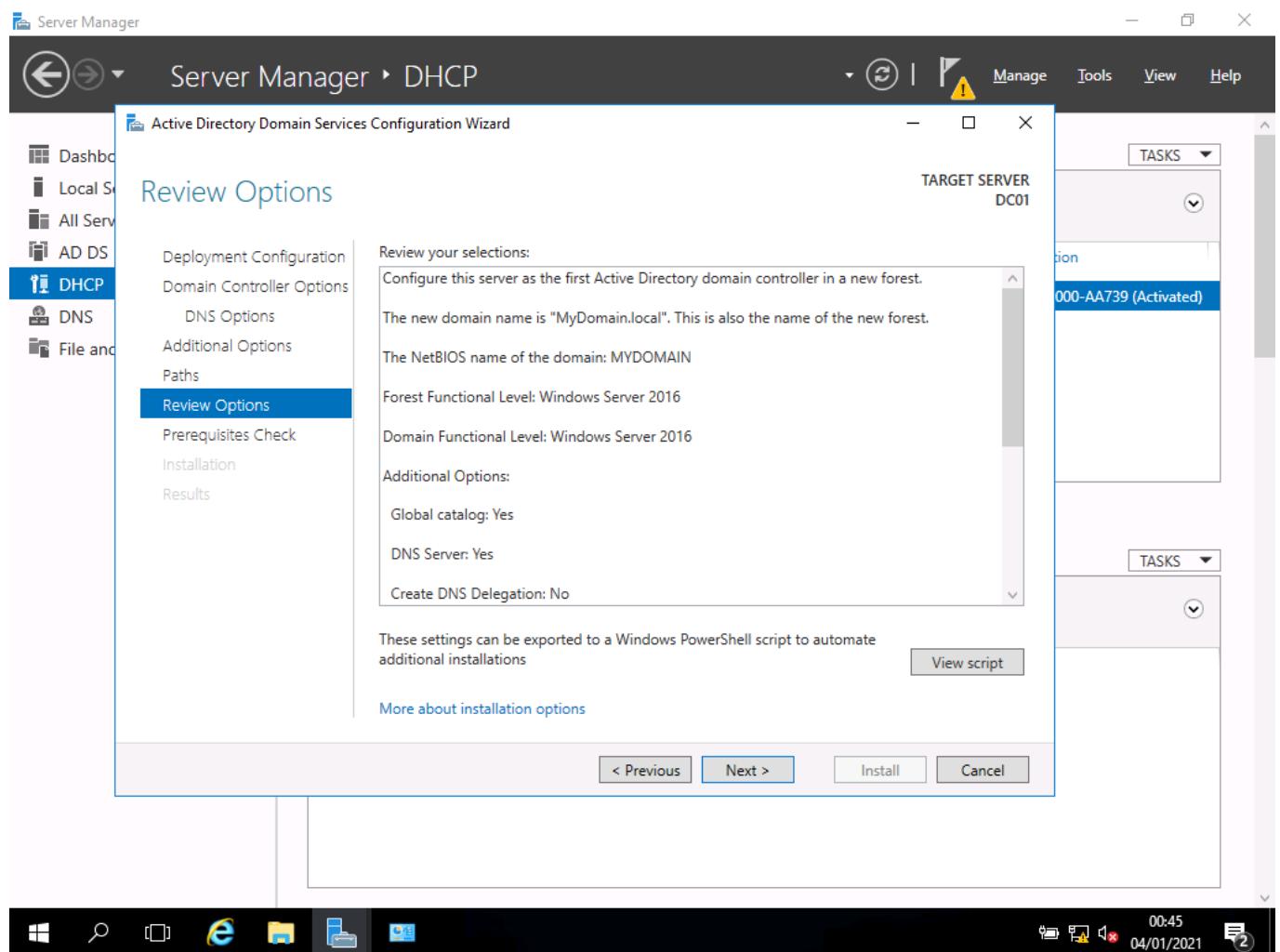
- I create a new domain



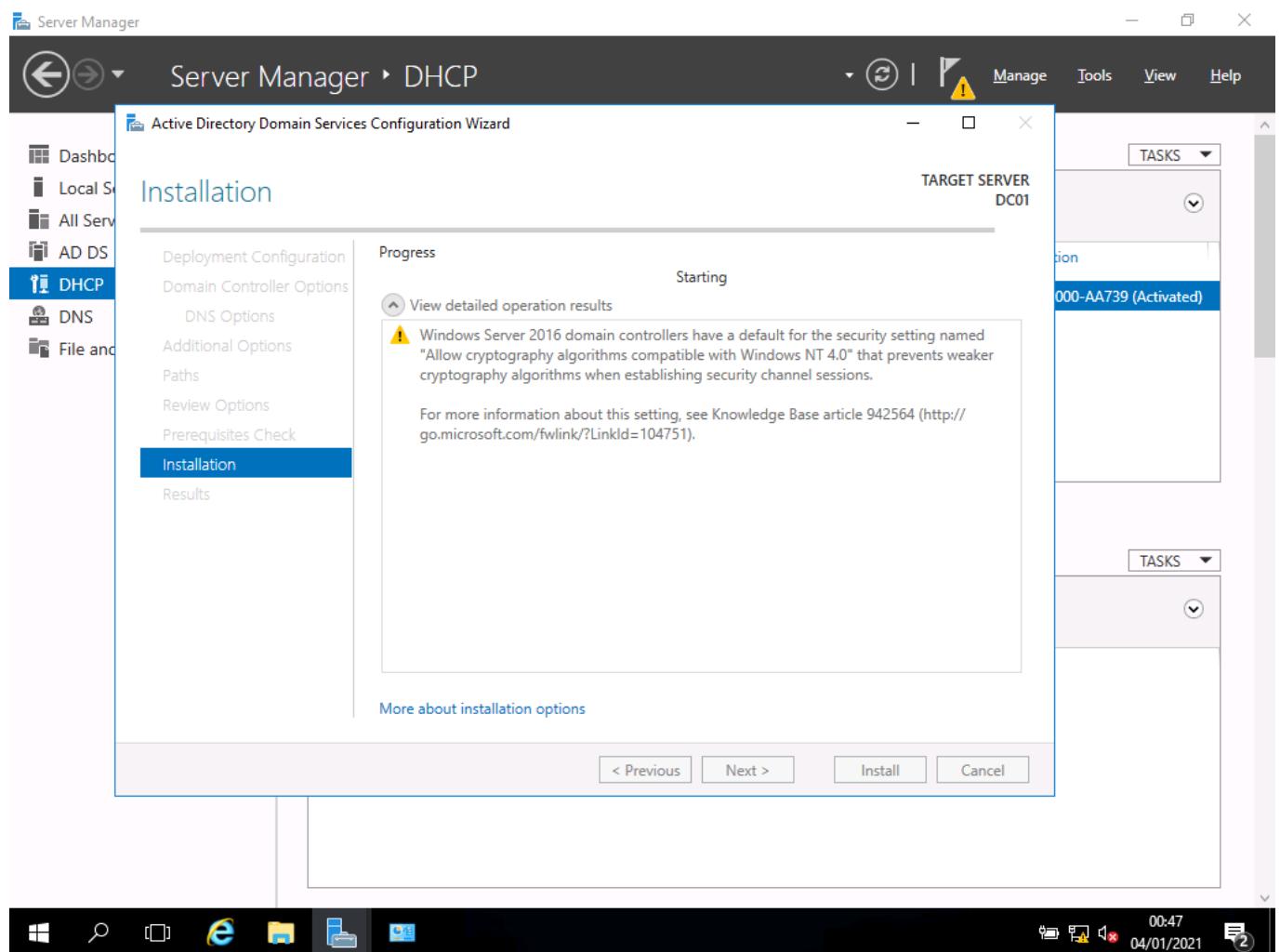
- I set the options for compatibility with other servers



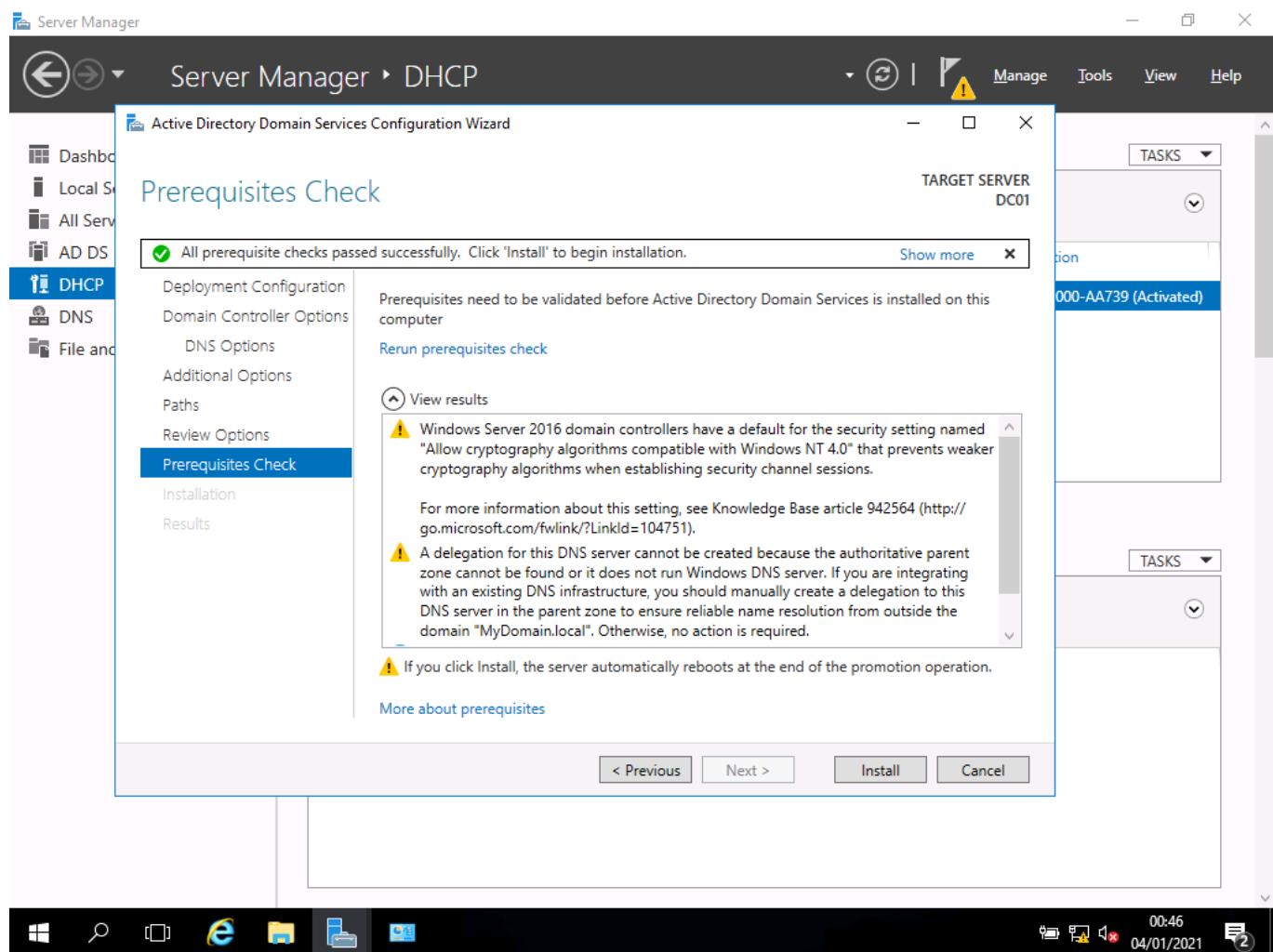
- I add DHCP to my domain



- I set the location of the log files

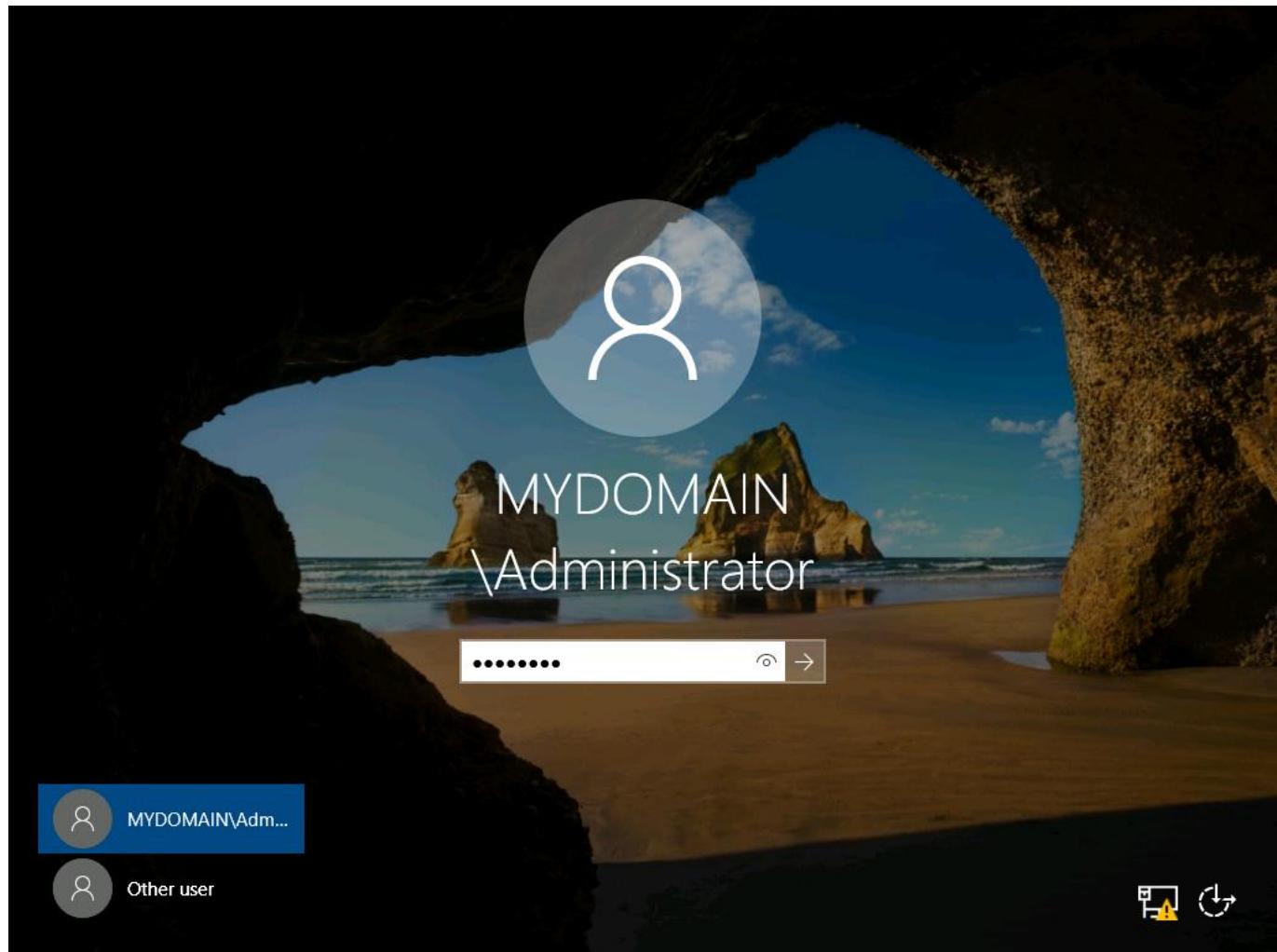


Here we see a warning about the compatibility level and the need to change it if you have older servers in your network.



- I follow the Active Directory domain service (ADDS) configuration wizard calling my network MyDomain.Local

Screenshot:



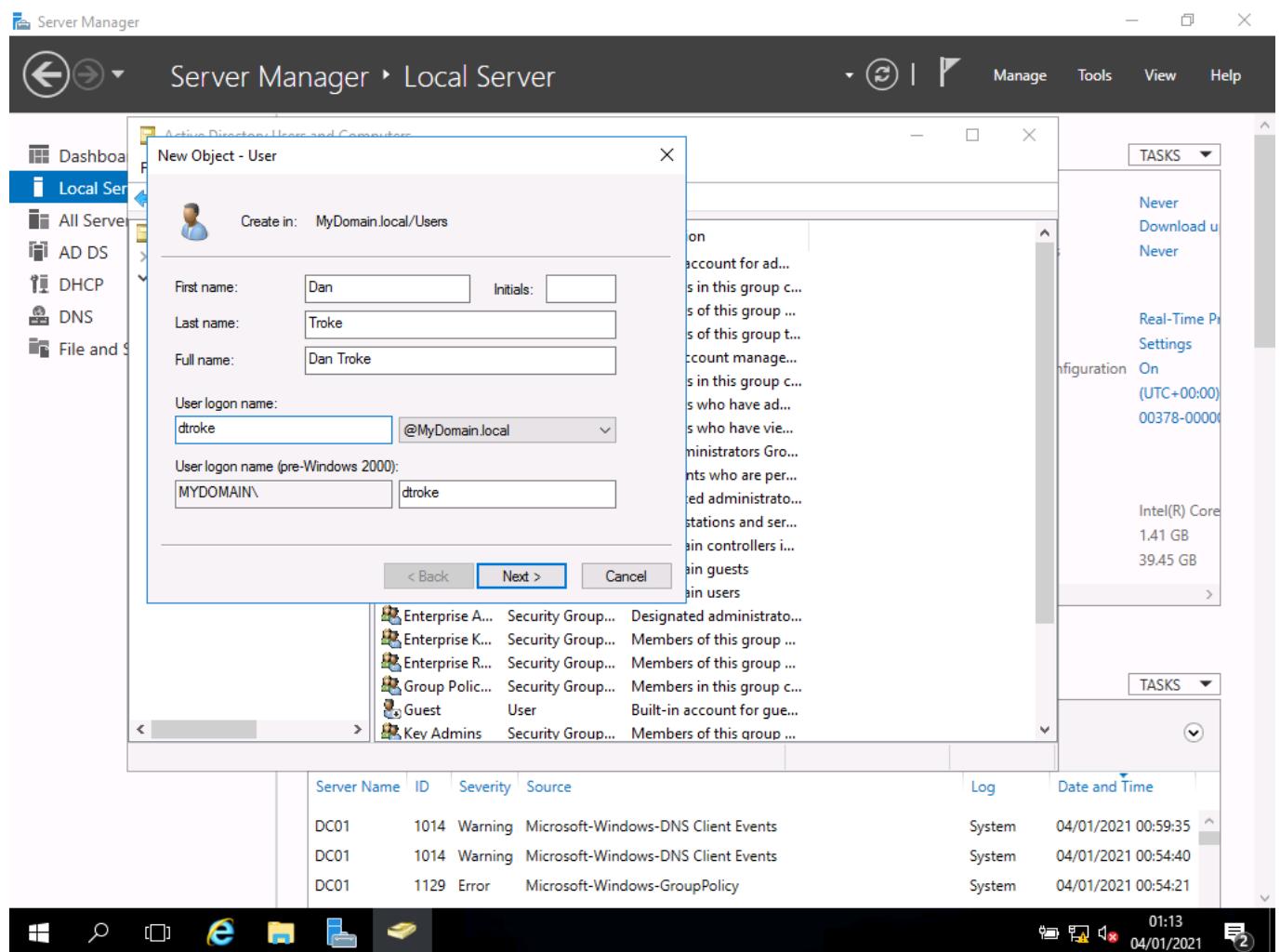
- I now login to the domain as an administrator

Screenshots:

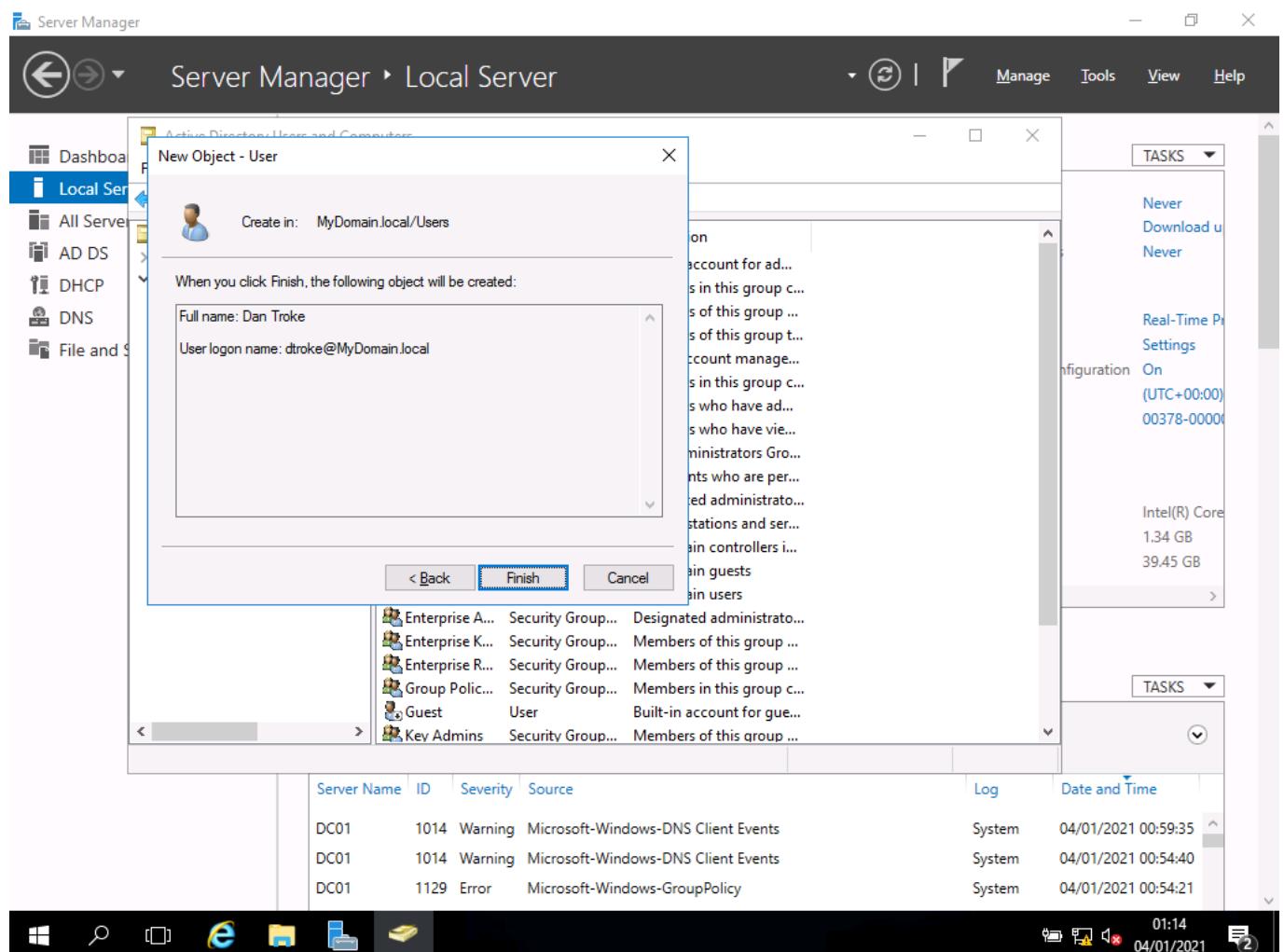
Active Directory is now installed

The screenshot shows the Windows Server Manager interface. The left navigation pane is visible with options like Dashboard, Local Server (selected), All Servers, AD DS, DHCP, DNS, and File and Storage Services. The main content area displays the properties for the local server DC01, including its computer name (DC01) and domain (MyDomain.local). Below this, network settings like Windows Firewall (Domain: On), Remote management (Enabled), and NIC Teaming (Disabled) are listed. The Events section shows a list of 68 total events, with three entries for DC01: two warnings from Microsoft-Windows-DNS Client Events and one error from Microsoft-Windows-GroupPolicy. The right-hand sidebar lists various management tools, with 'Active Directory Users and Computers' currently selected.

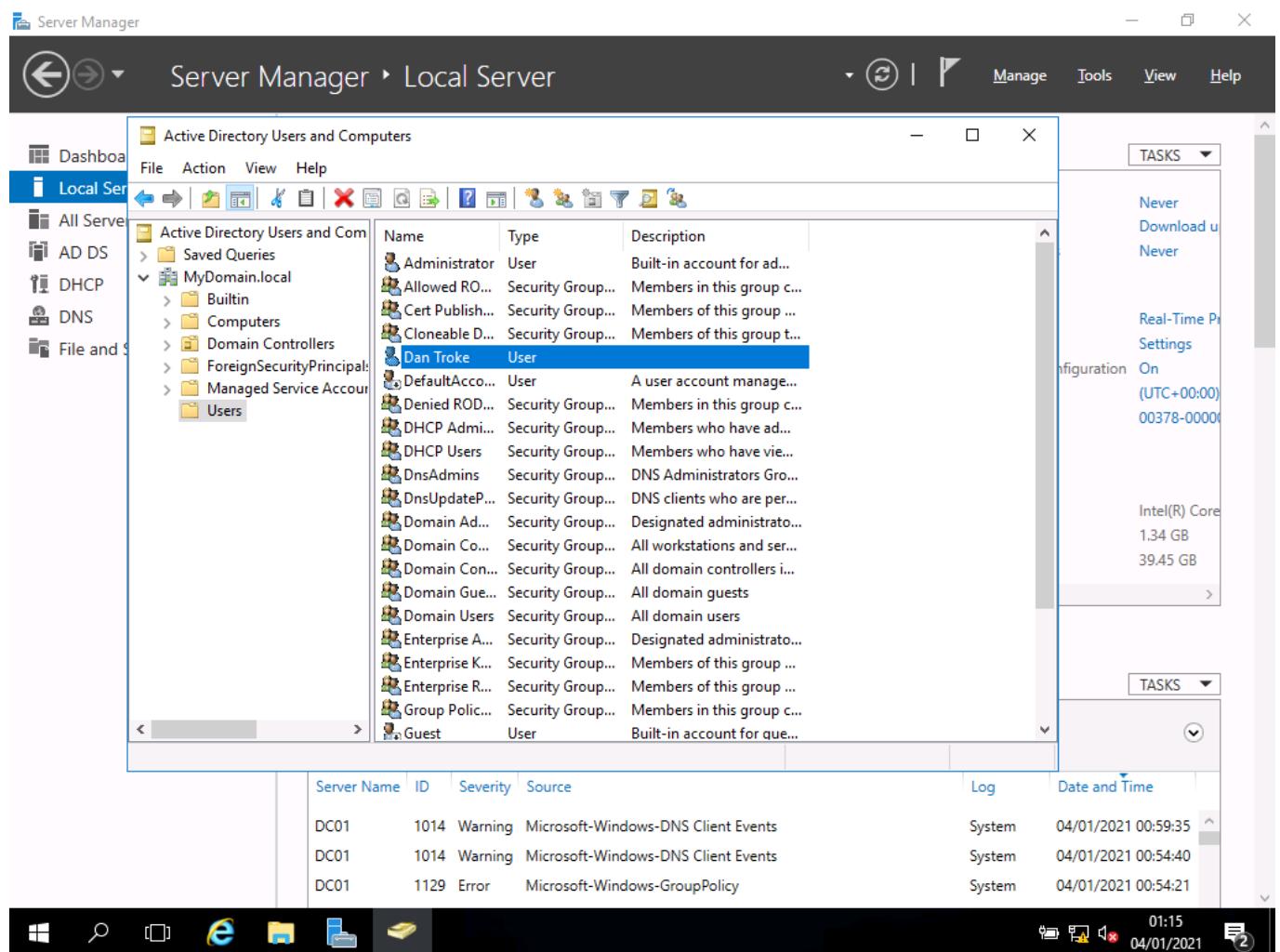
- I can now add a new user



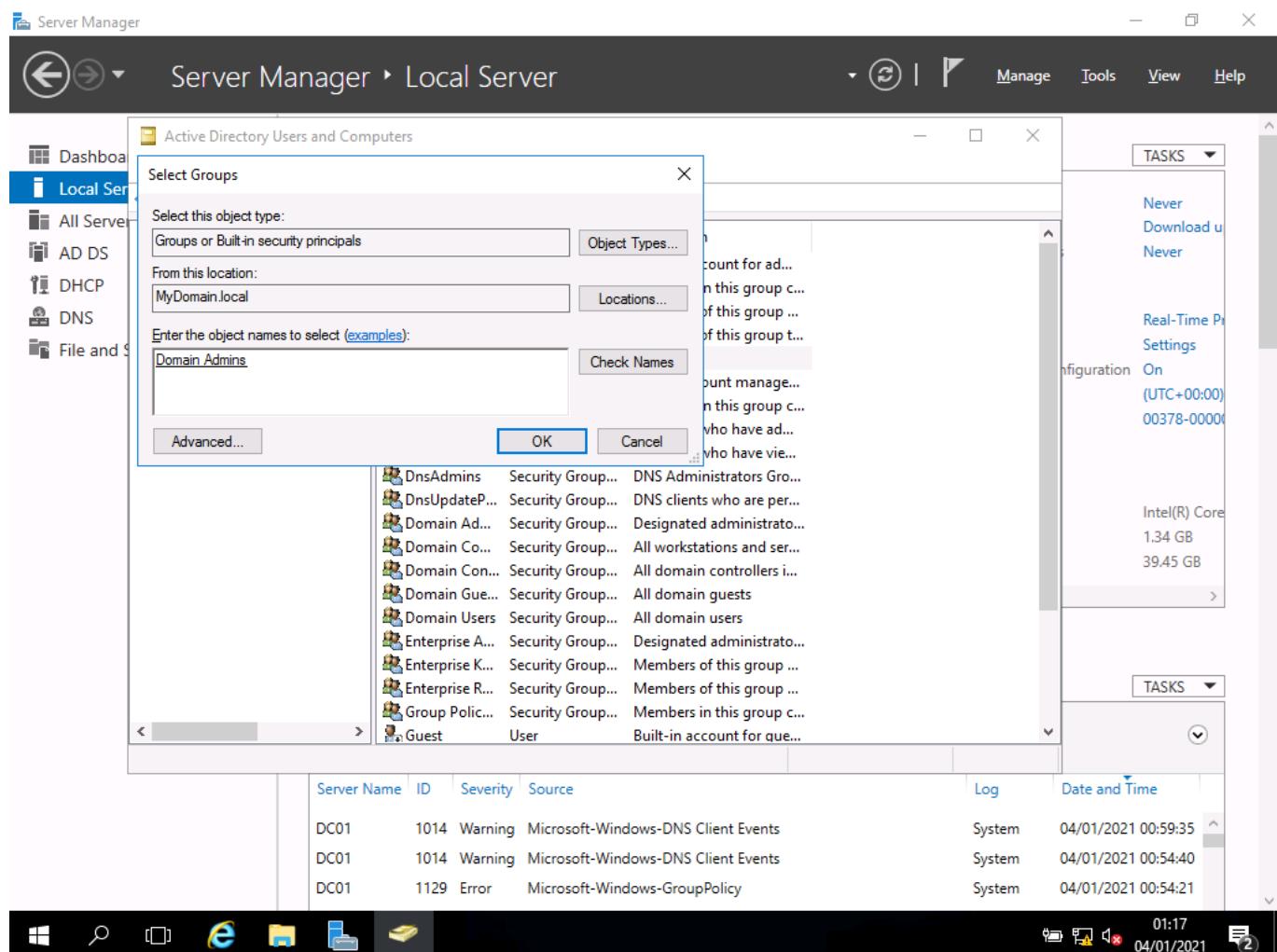
- I can now add new user details



- I click finish to add/create the object



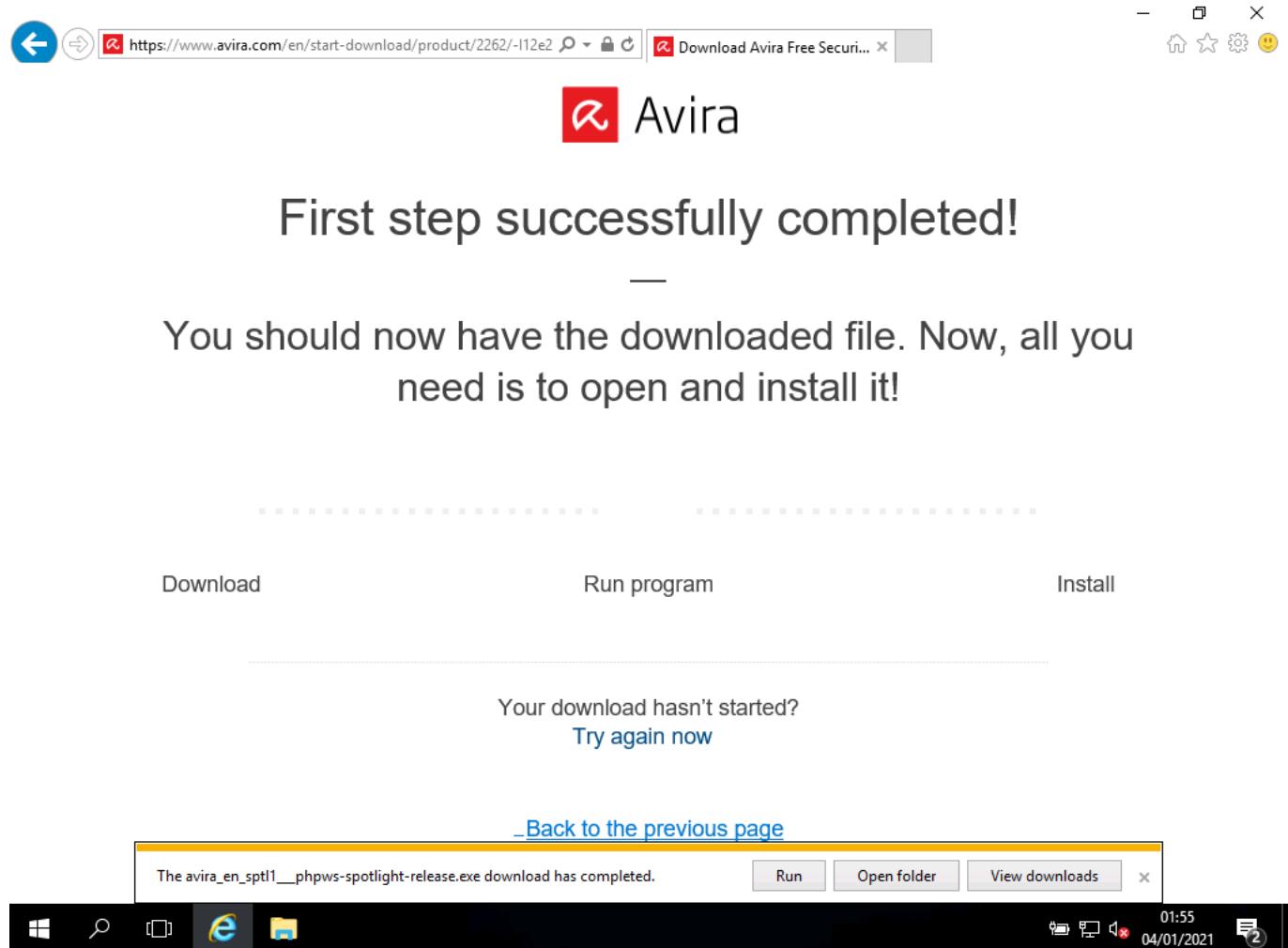
- The new user is now added to the Active Directory of Users and Computers



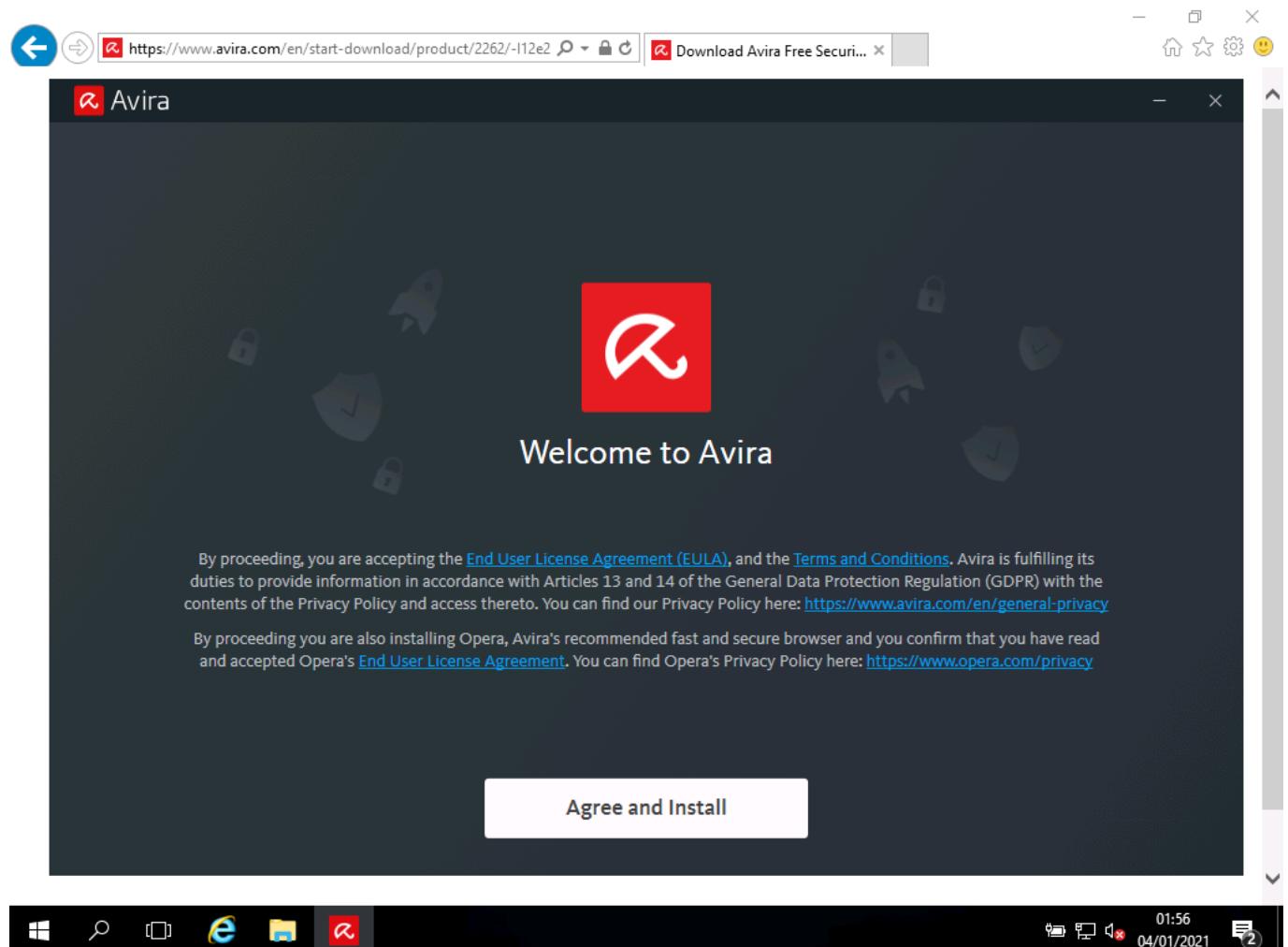
- I can add new user to the group that best suits their job
- The screenshots above show me accessing Active Directory and creating a user account called **dtroke** and making it a domain admin

Installing security software

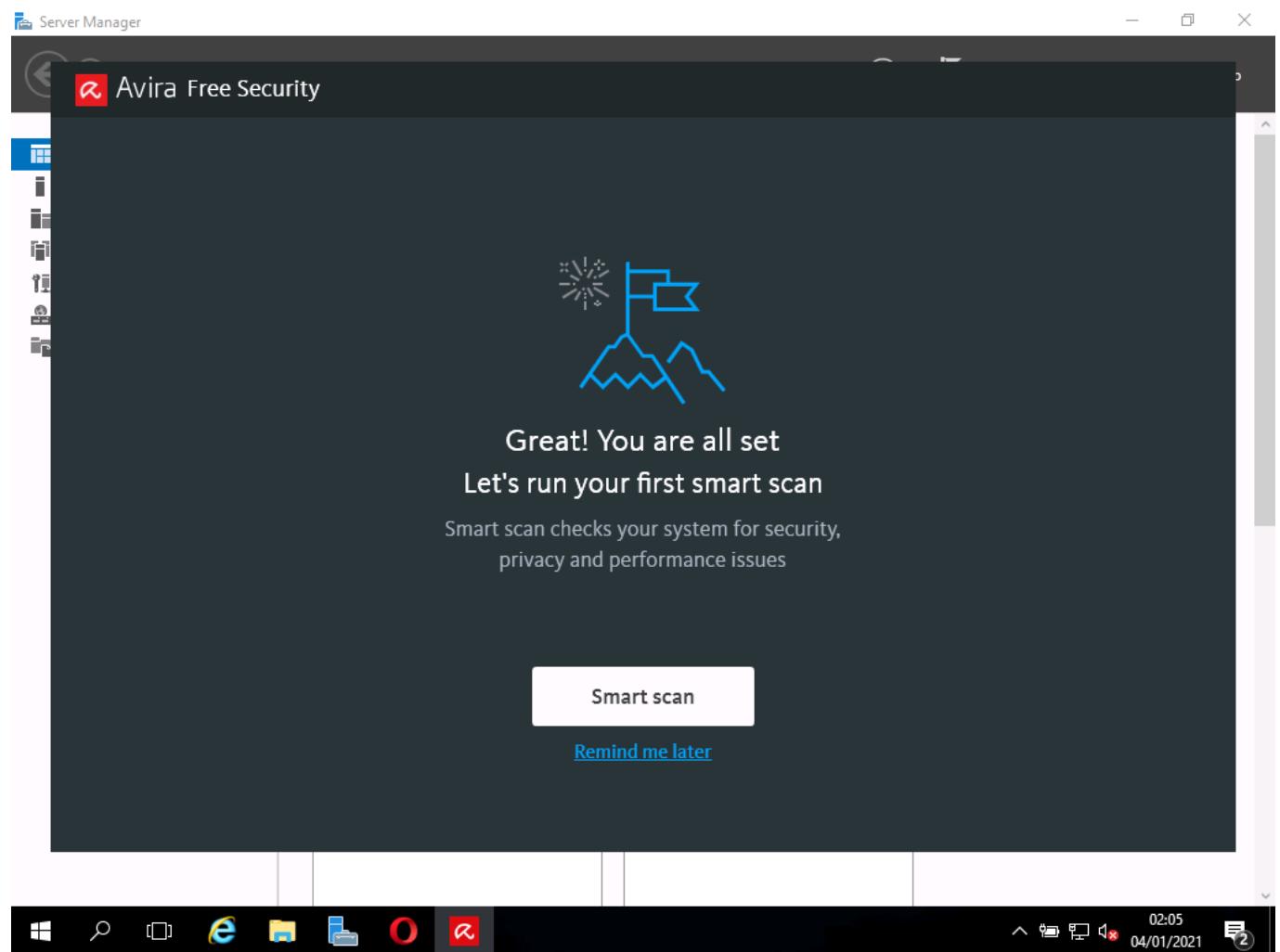
Screenshots:



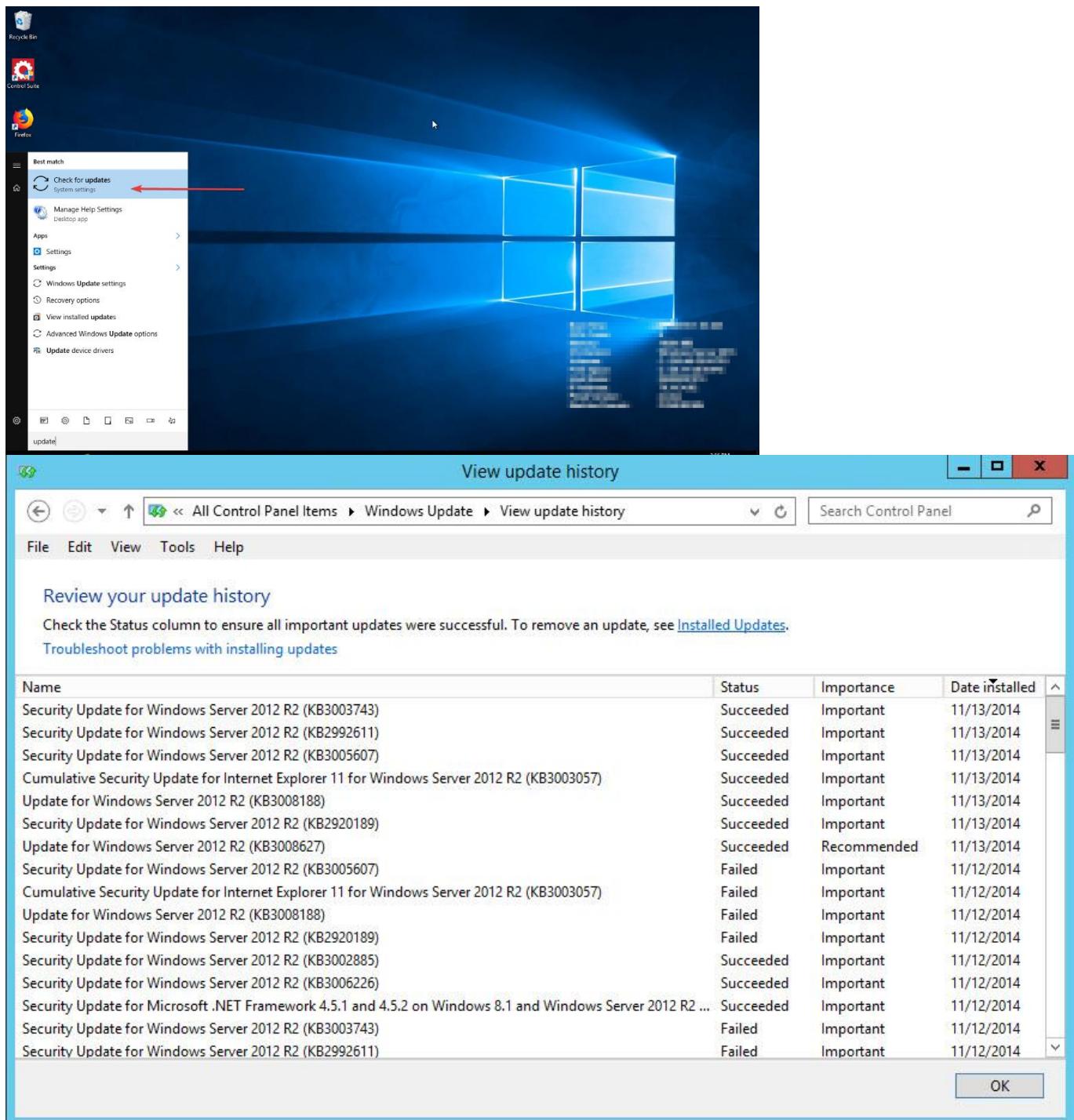
- I browse for the website and choose to use Avira. Here I download the programme



- After the download is complete, I agree to the terms and install it



- Once installed, I can run a Smart scan

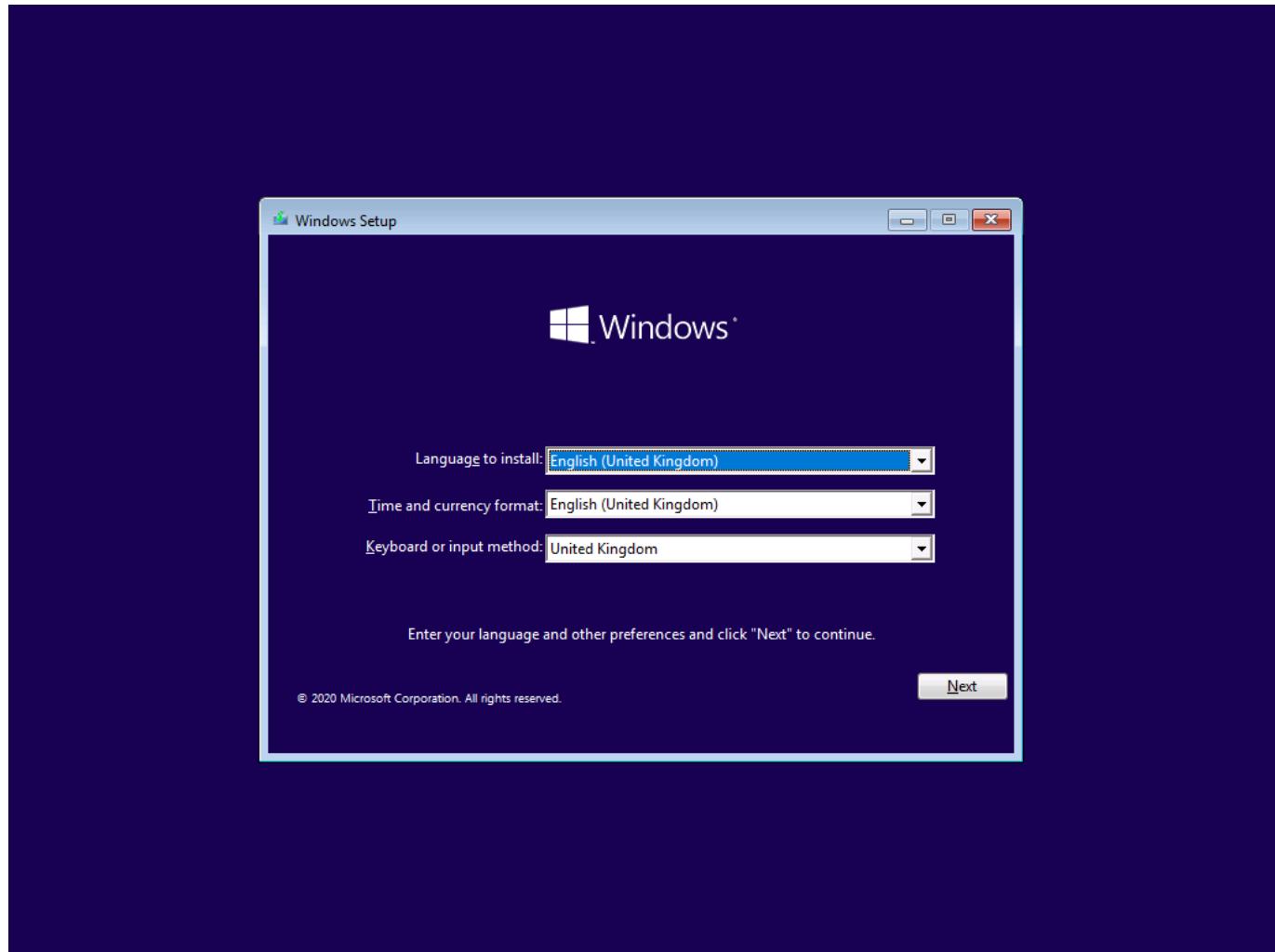


- I now check for Windows updates
- Antivirus is installed and Windows is up to date

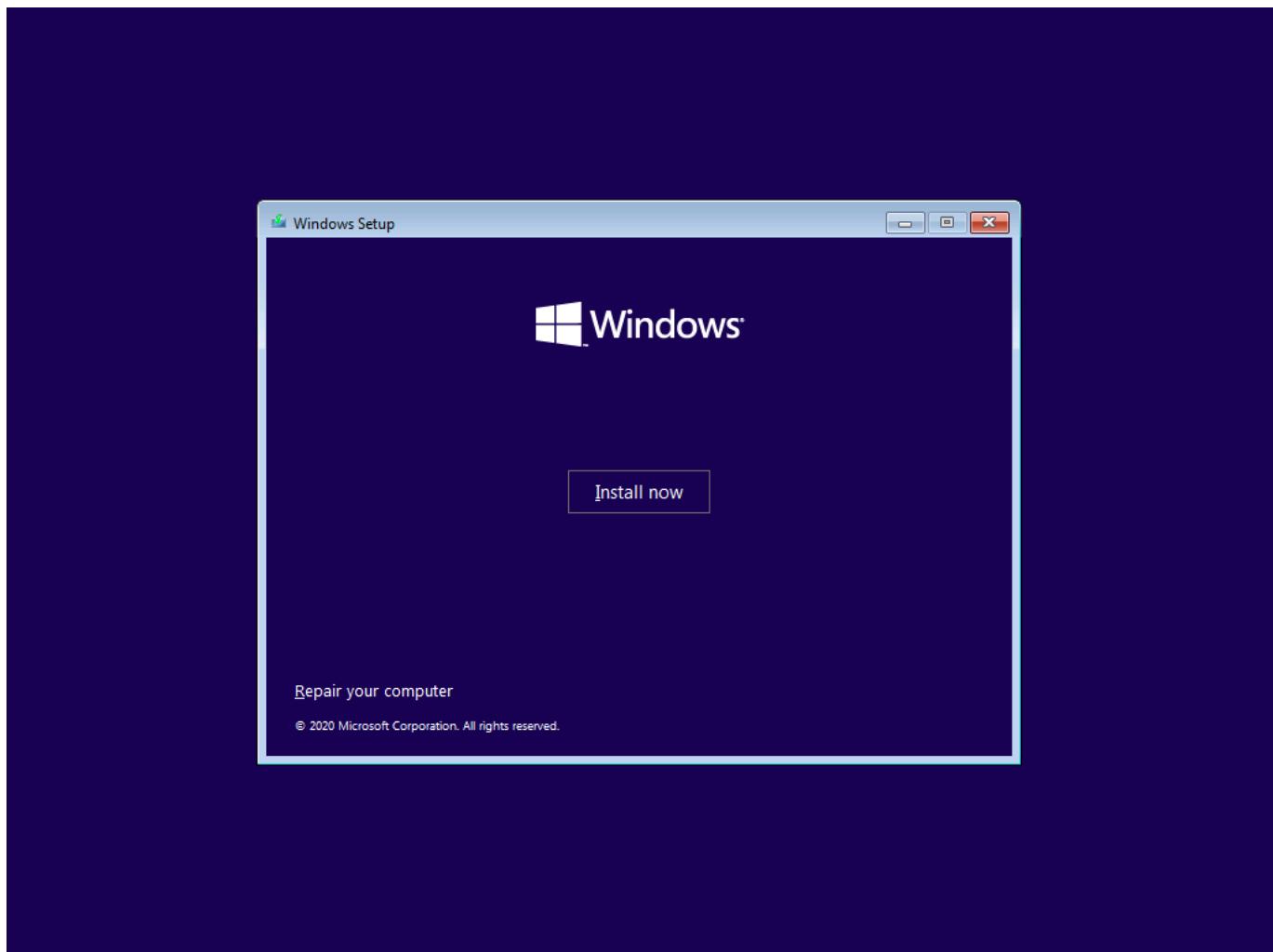
Task 2(b)

Installation of client PC

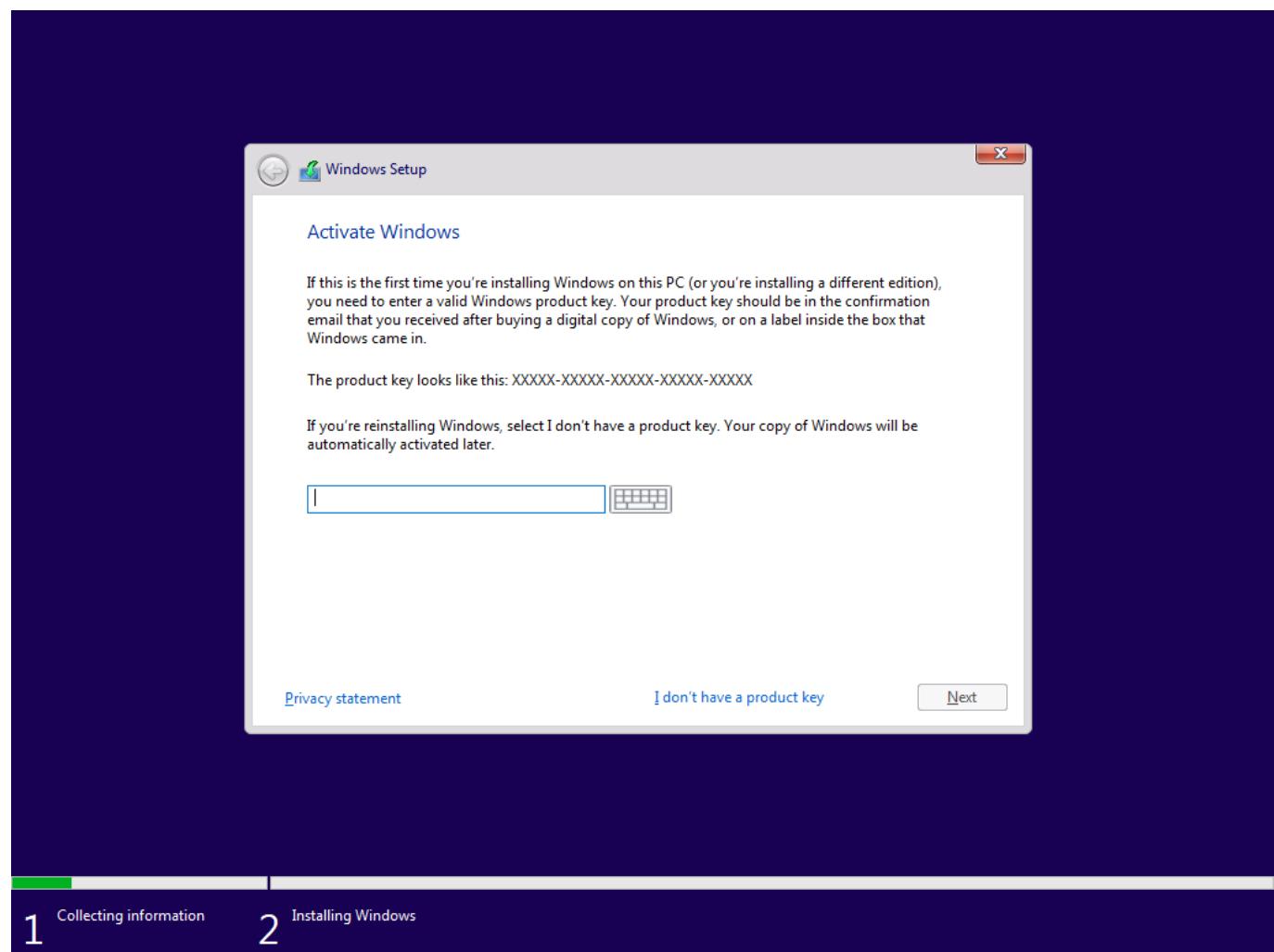
Screenshots:



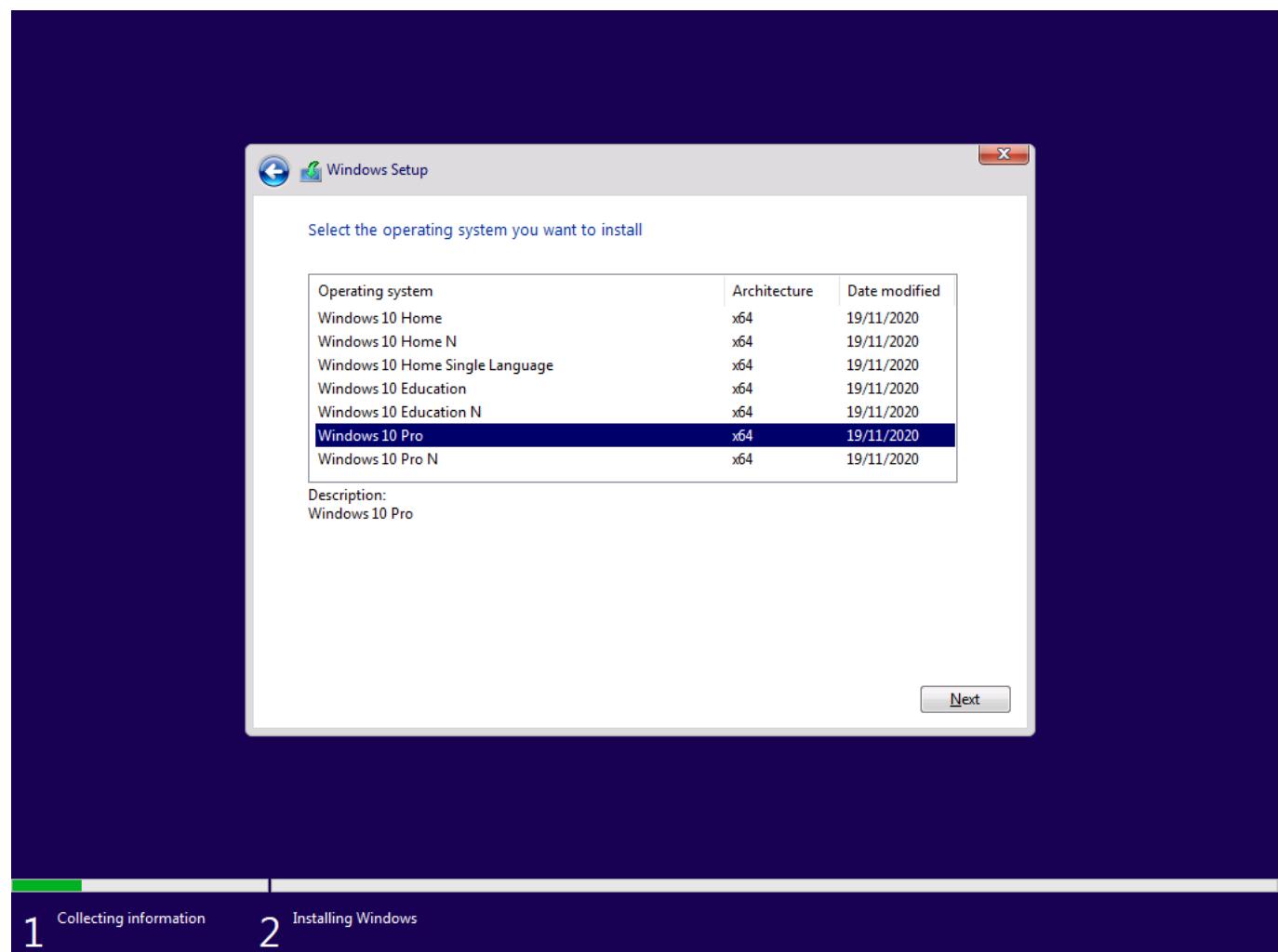
- I select the correct language for the UK



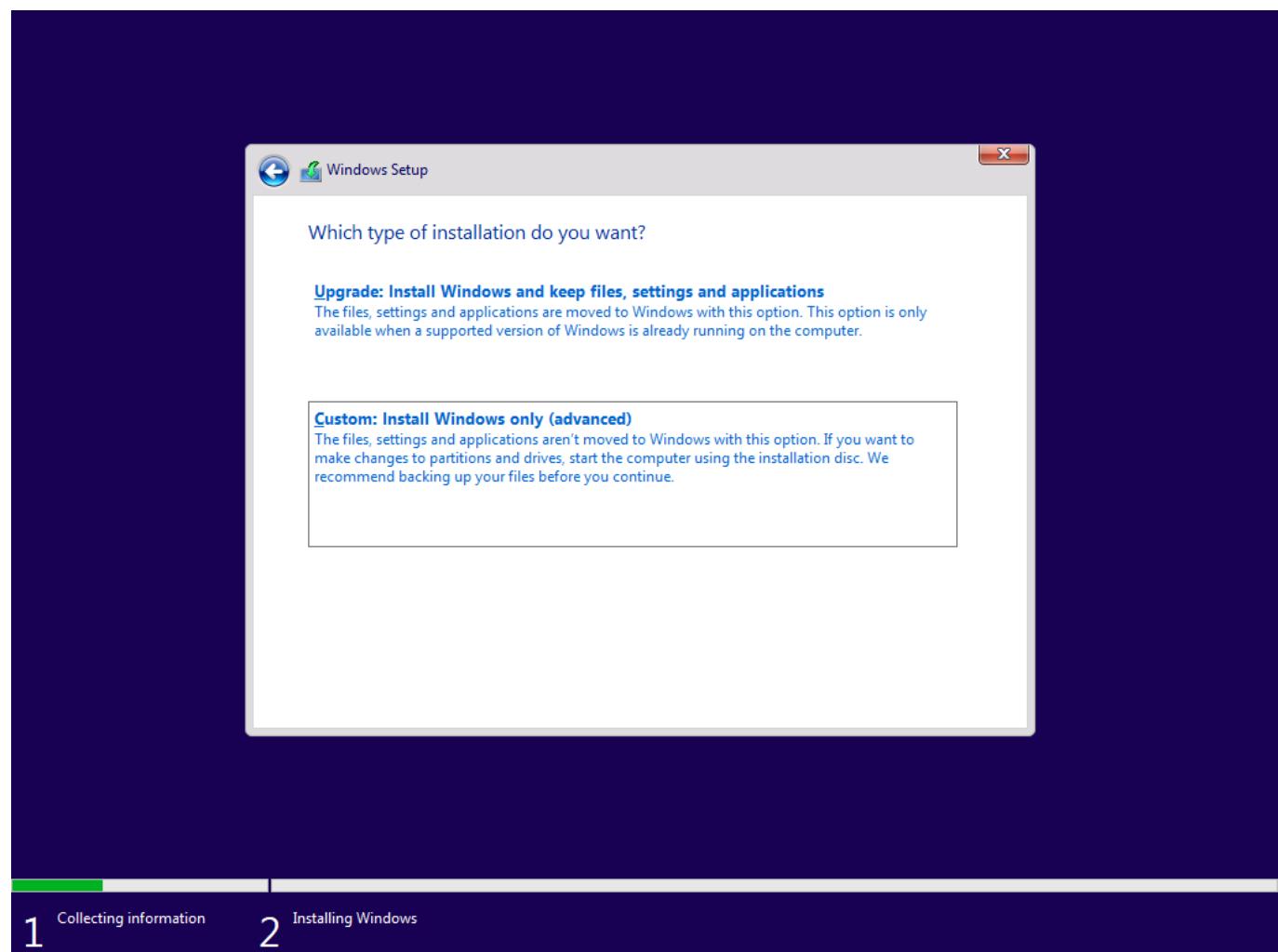
- I click install



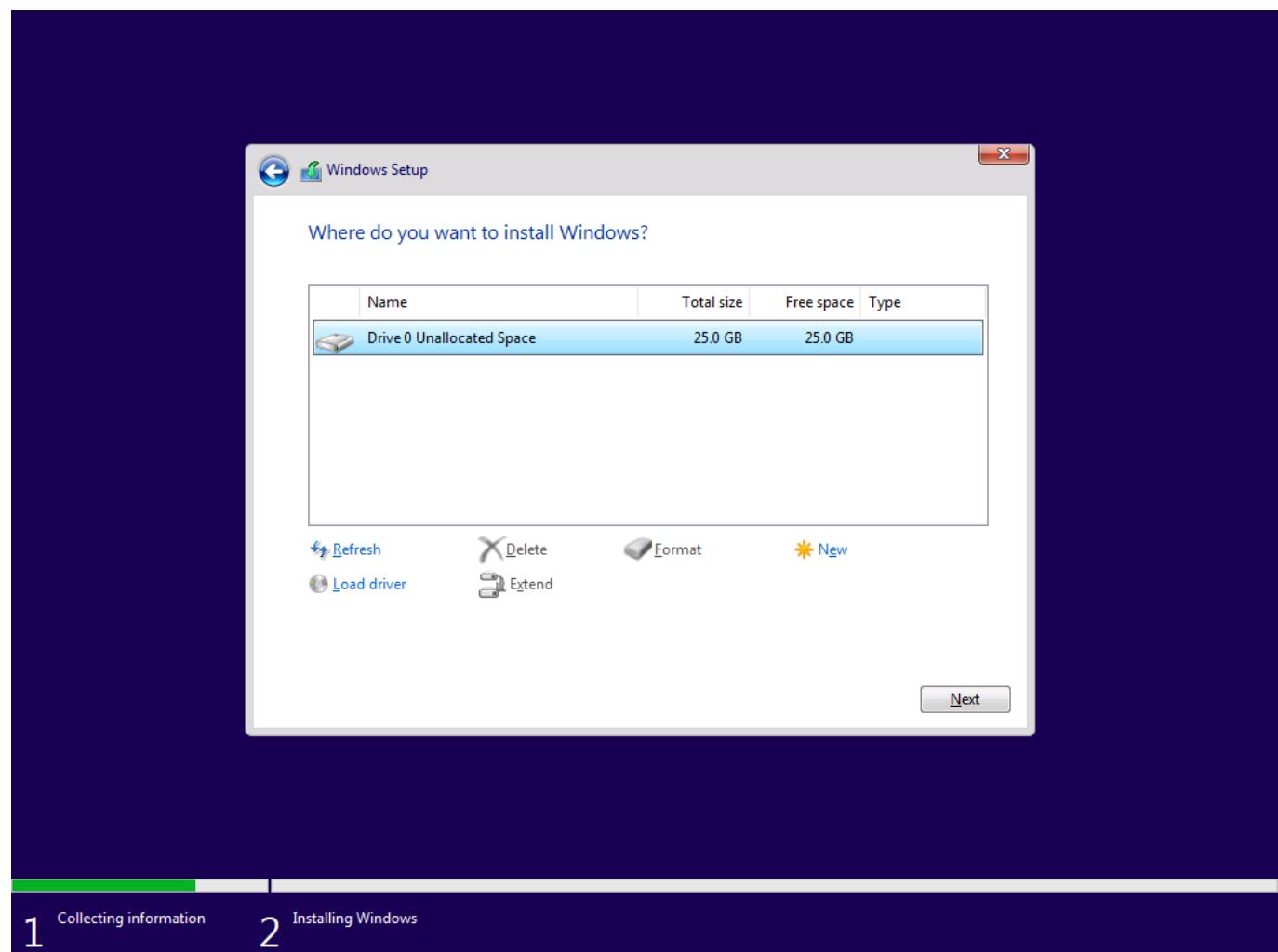
- I add the license number as proof of license



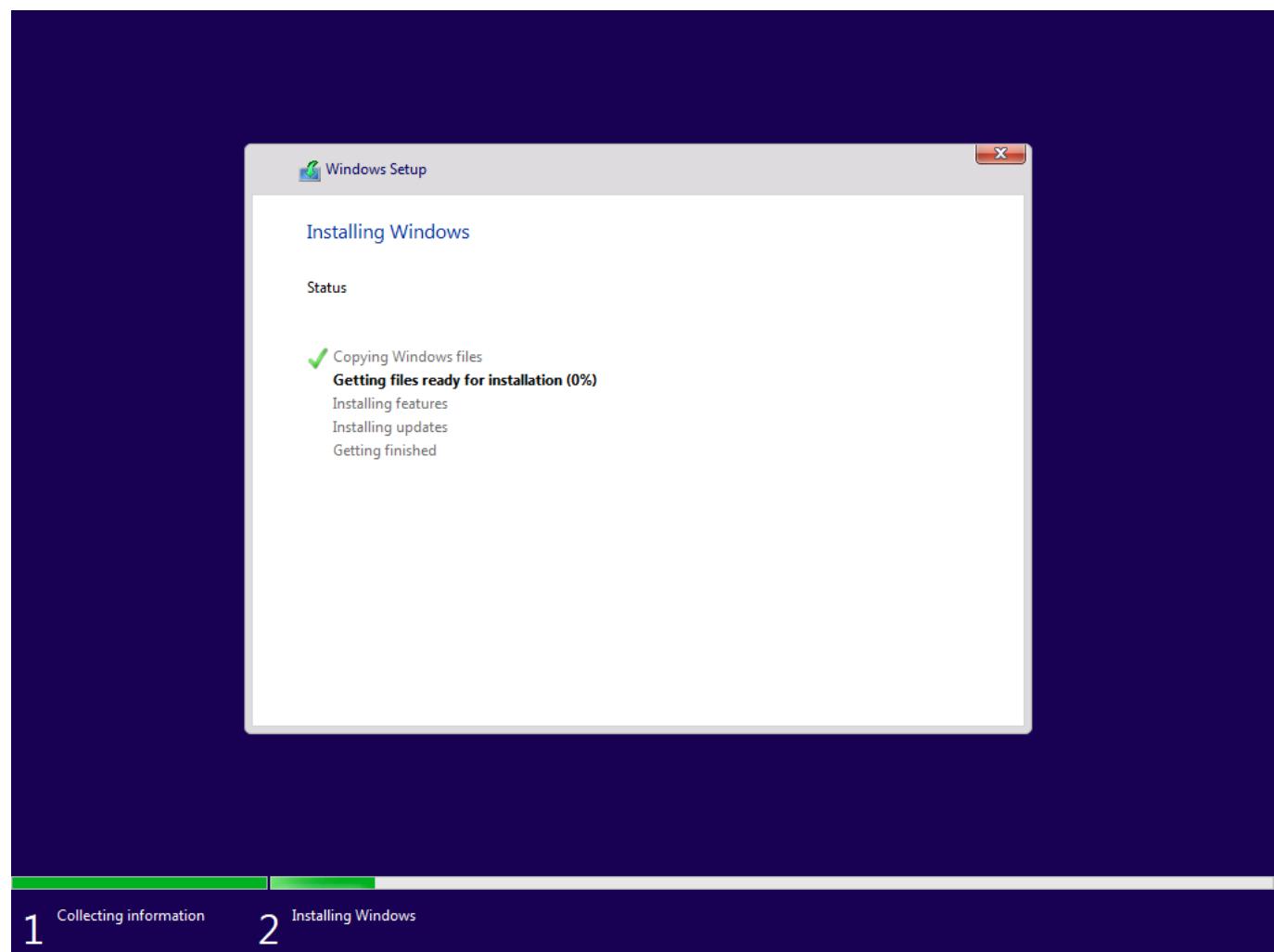
- select the correct version of Windows necessary. I am going to install Pro as this is a corporate machine



- I use a custom install as this will keep the old data if there is any and let me choose more options



- I select the disk I wish to use. As there is only one disk, this is selected by default. I choose it

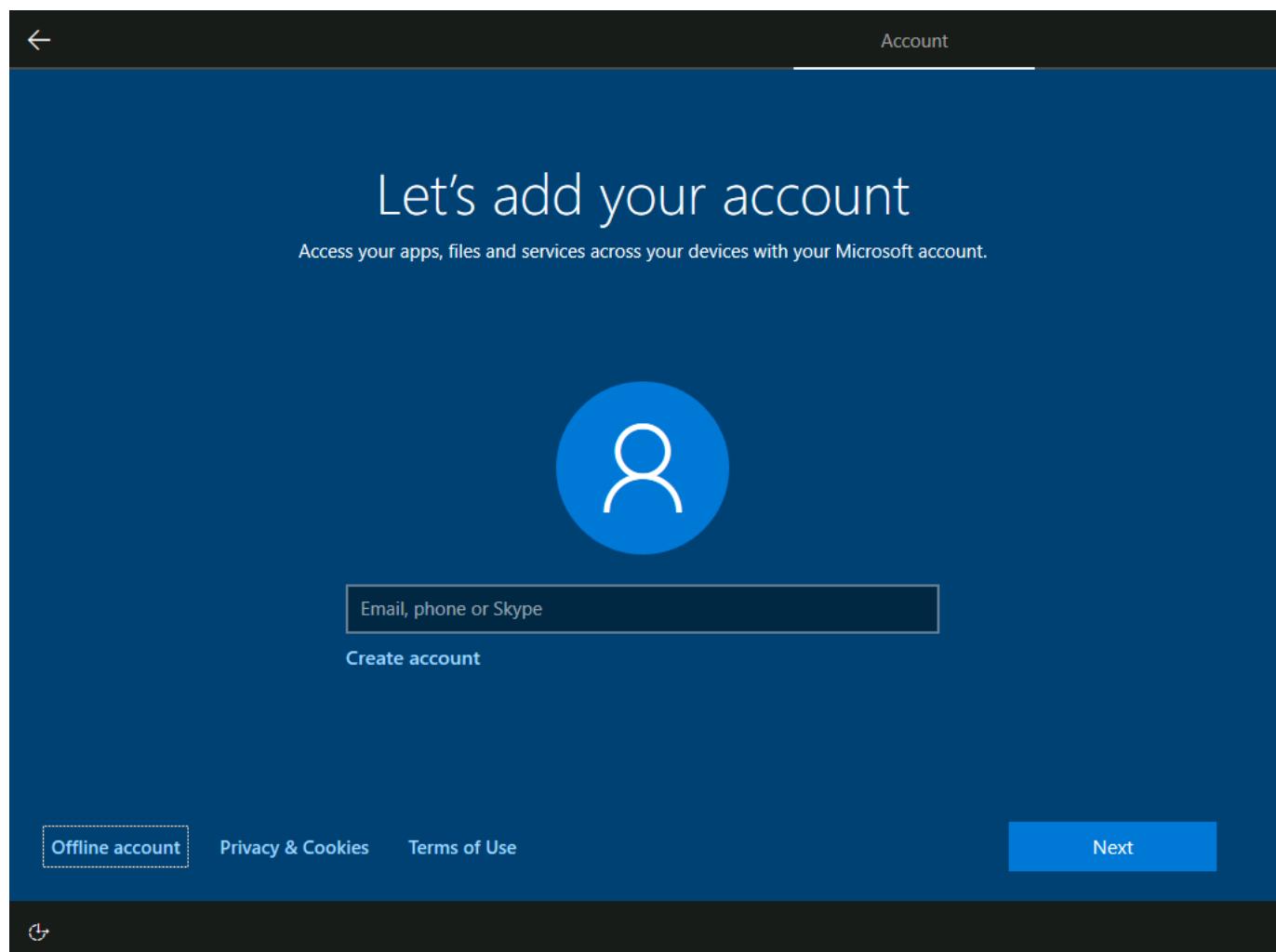


- these screenshots show me installing Windows 10 onto the client computer

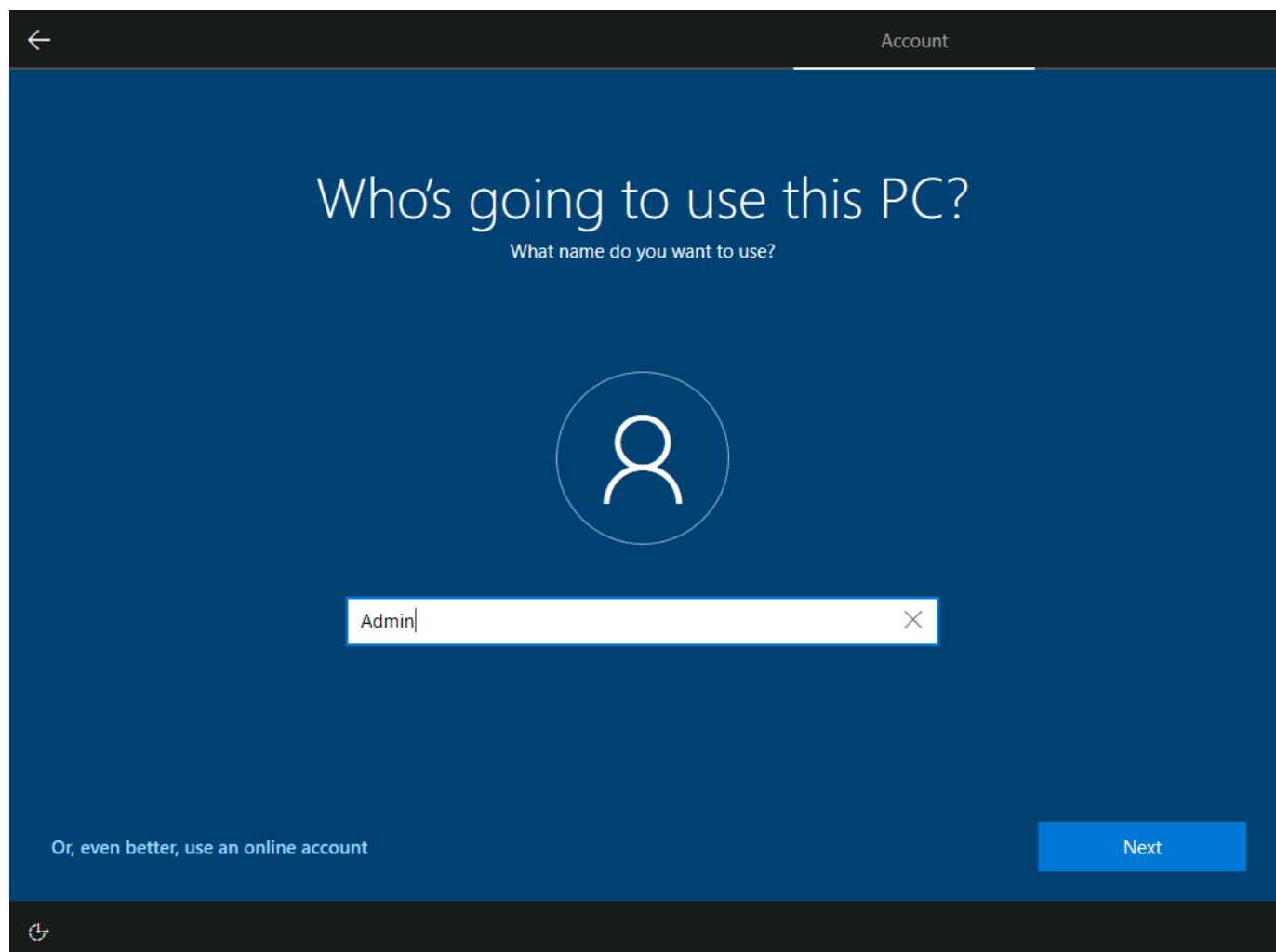
Screenshots:

The screenshot shows a digital interface for a 'Digital Support' assignment. At the top, a dark bar displays the title 'T Level Technical Qualification in Digital Support Services (603/6901/2), OSA' and 'Digital Support, Assignment 1, Pass'. Below this, a sub-header 'Guide standard exemplification materials' is visible. The main content area has a blue background. At the top left, the word 'Basics' is written. In the center, the question 'Is this the right keyboard layout?' is displayed in large white text. Below it, a smaller text says 'If you also use another keyboard layout, you can add that next.' A dropdown menu is open, listing several keyboard layouts. The first item, 'United Kingdom', is highlighted with a blue background and a dashed border. Other items in the list include 'Canadian Multilingual Standard', 'English (India)', 'Irish', 'Scottish Gaelic', 'United States-Dvorak', and 'United States-Dvorak for left hand'. To the right of the dropdown is a vertical scroll bar. At the bottom right of the screen, there is a blue button labeled 'Yes'. On the far left, there is a small circular icon with a white symbol inside.

- I select the correct keyboard for use in the UK

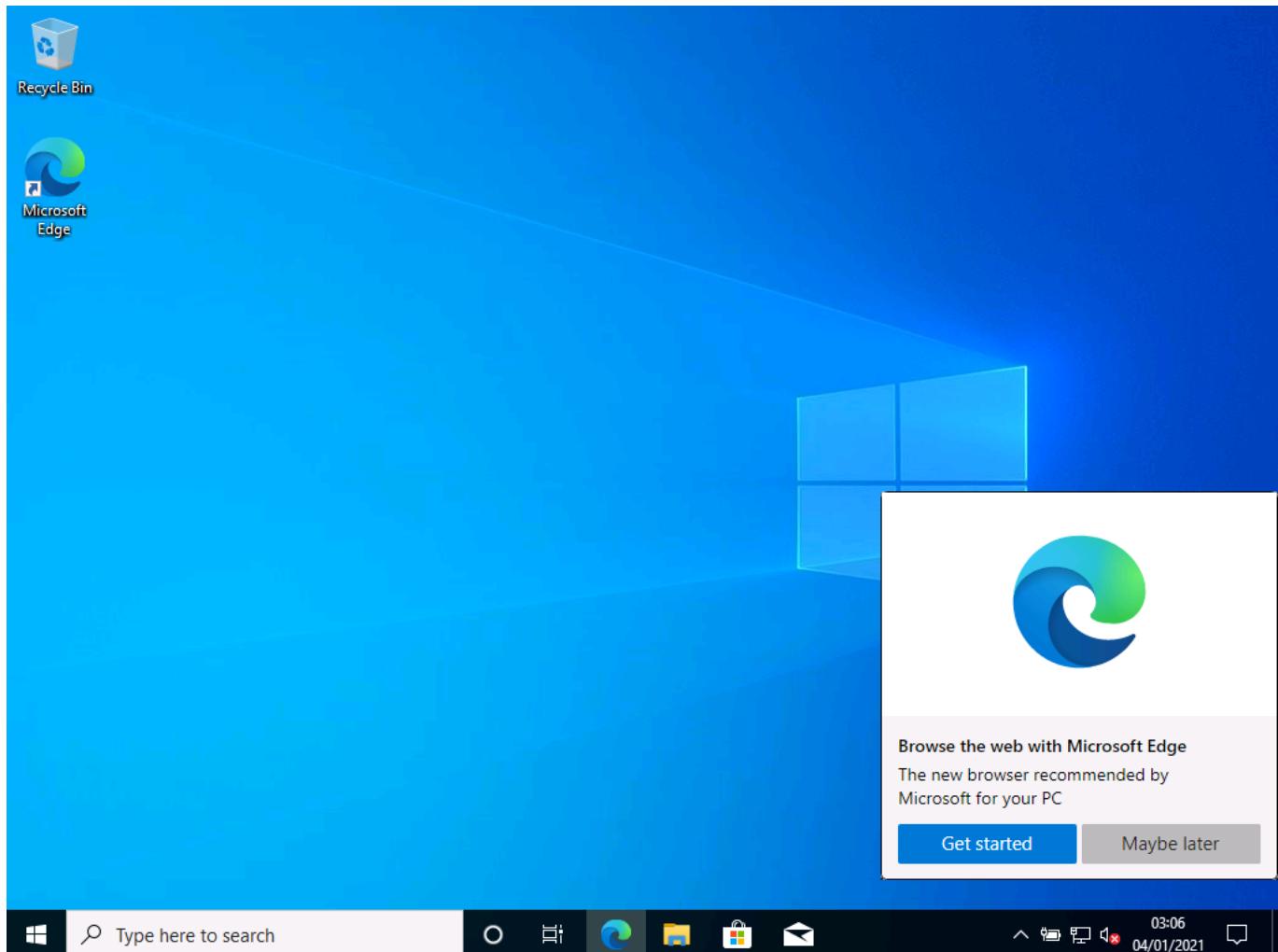


- I add a local account for Microsoft



- These screenshots show me performing the initial set-up for first use of Windows 10

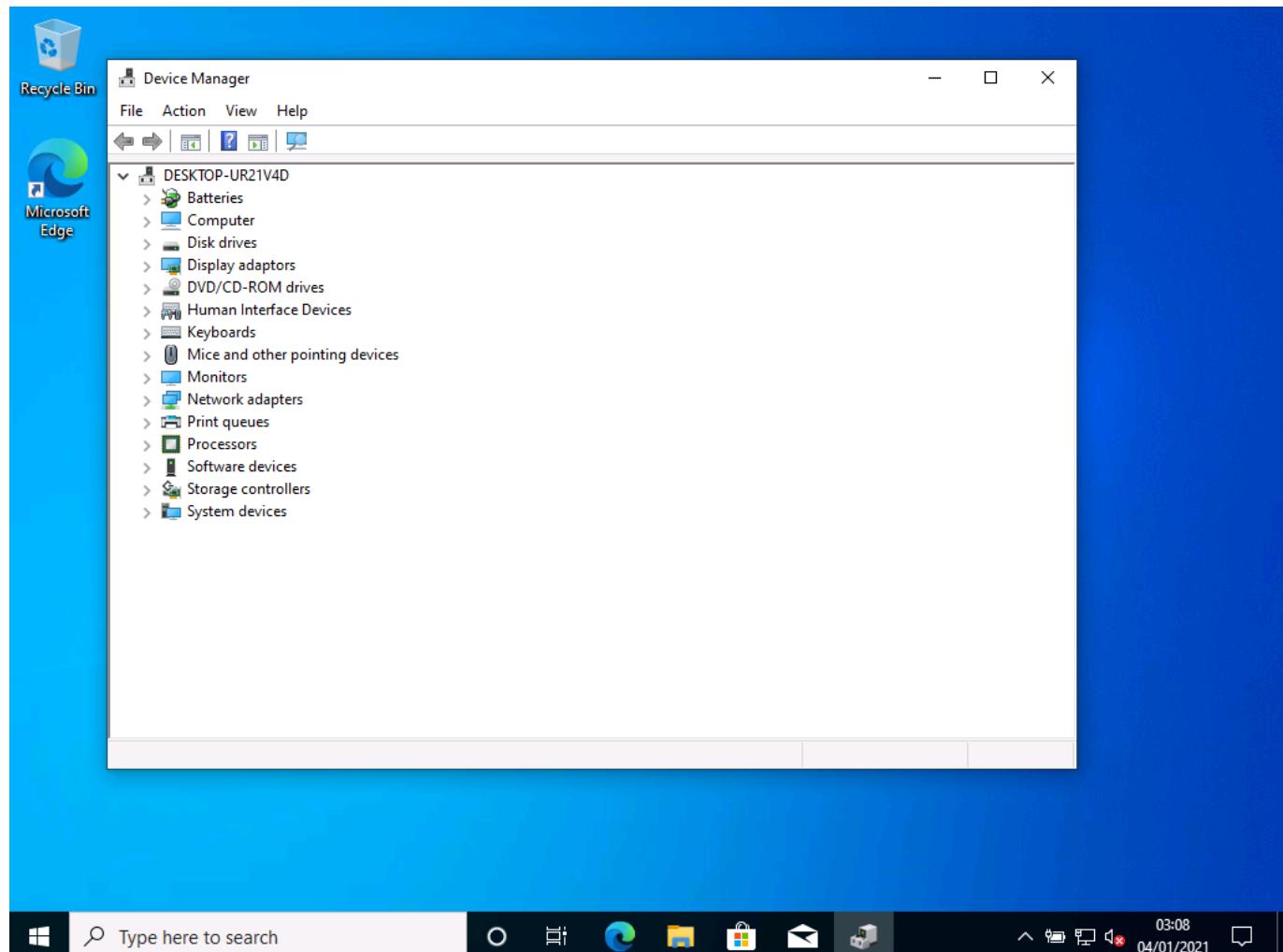
Screenshot:



- I have now logged into Windows 10 for the first time

Checking device drivers

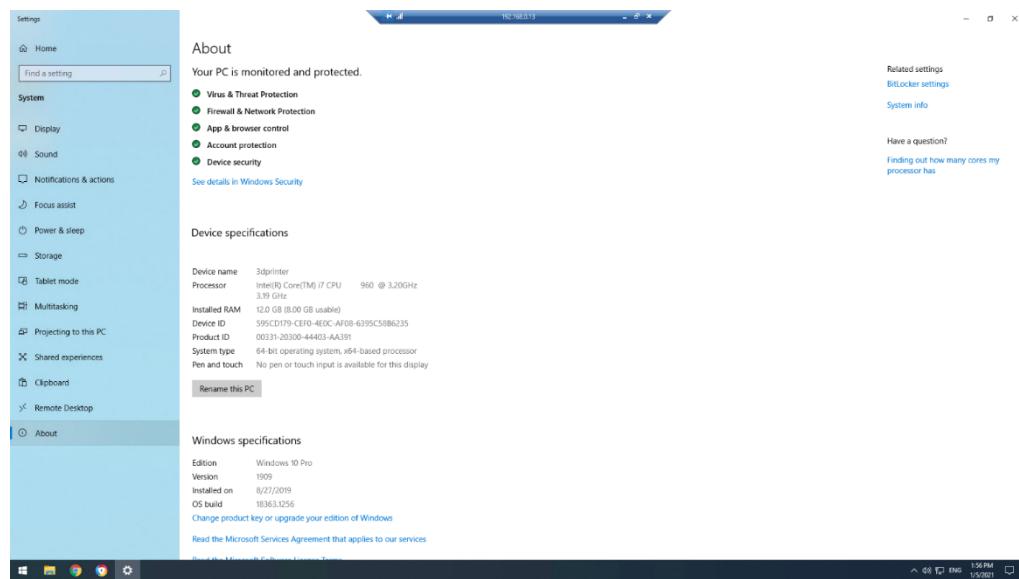
Screenshots:



- I check all drivers are installed

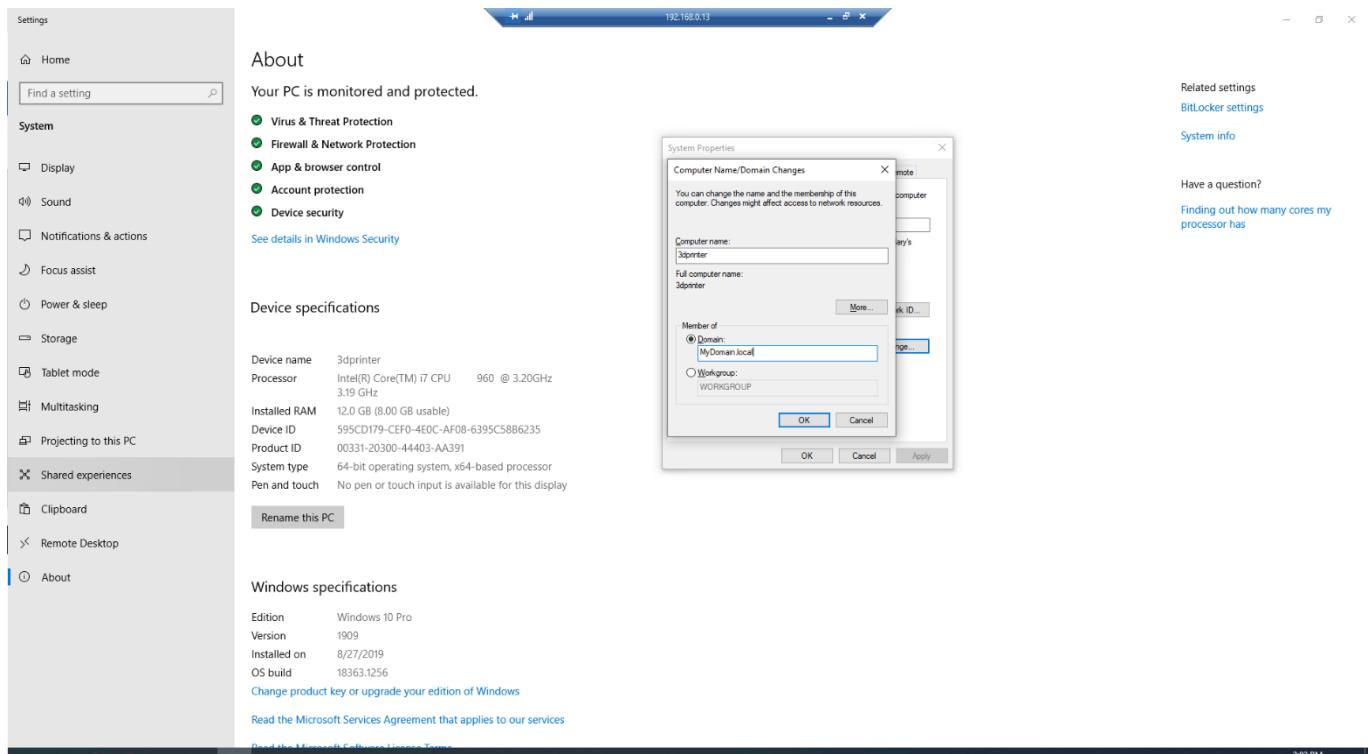
Network configuration/domain joining

Screenshots:



- I open settings

T Level Technical Qualification in Digital Support Services (603/6901/2), OSA
 Digital Support, Assignment 1, Pass
 Guide standard exemplification materials



The screenshot shows the Windows Settings interface under the 'About' tab. It displays system protection status (Virus & Threat Protection, Firewall & Network Protection, App & browser control, Account protection, Device security) and device specifications (Device name: 3dprinter, Processor: Intel(R) Core(TM) i7 CPU 960 @ 3.20GHz, Installed RAM: 12.0 GB (8.00 GB usable), Device ID: 595CD179-CE00-4E0C-AF08-6395C5886235, Product ID: 00331-20300-44403-AA391, System type: 64-bit operating system, x64-based processor). The 'Rename this PC' button is highlighted.

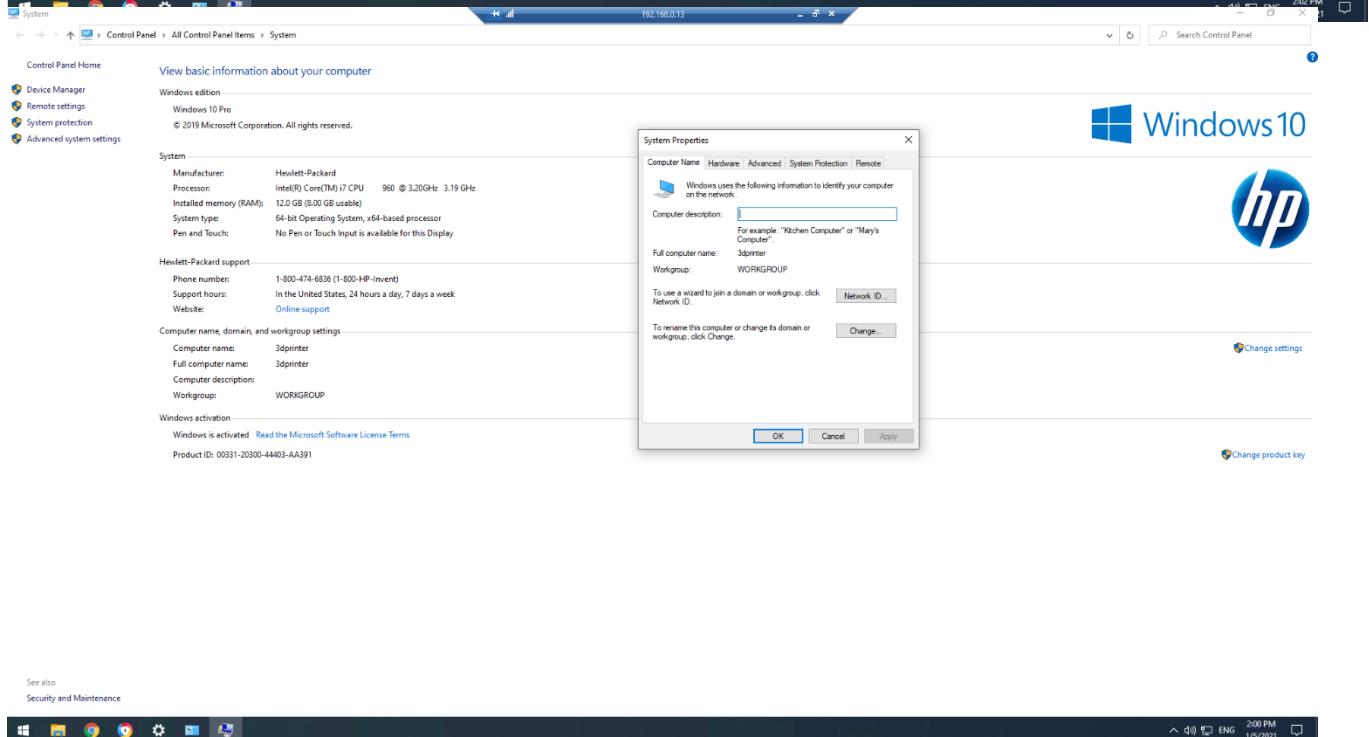
System Properties Dialog:

```

Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: 3dprinter
Full computer name: 3dprinter
Member of:
 Domain: MyDomain.local
 Workgroup: WORKGROUP

OK Cancel Apply
  
```



The screenshot shows the Control Panel under the 'System' category. It displays basic information about the computer (Windows edition: Windows 10 Pro, Version: 1909, Installed on: 8/27/2019, OS build: 18363.1256) and system settings (Manufacturer: Hewlett-Packard, Processor: Intel(R) Core(TM) i7 CPU 960 @ 3.20GHz, Installed memory (RAM): 12.0 GB (8.00 GB usable), System type: 64-bit Operating System, x64-based processor, Pen and Touch: No Pen or Touch Input is available for this Display).

System Properties Dialog:

```

System Properties
Computer Name: 3dprinter
Hardware Advanced System Protection Remote
Computer description: For example: "Kitchen Computer" or "Mary's Computer".
Full computer name: 3dprinter
Workgroup: WORKGROUP
Network ID...
Change...
OK Cancel Apply
  
```

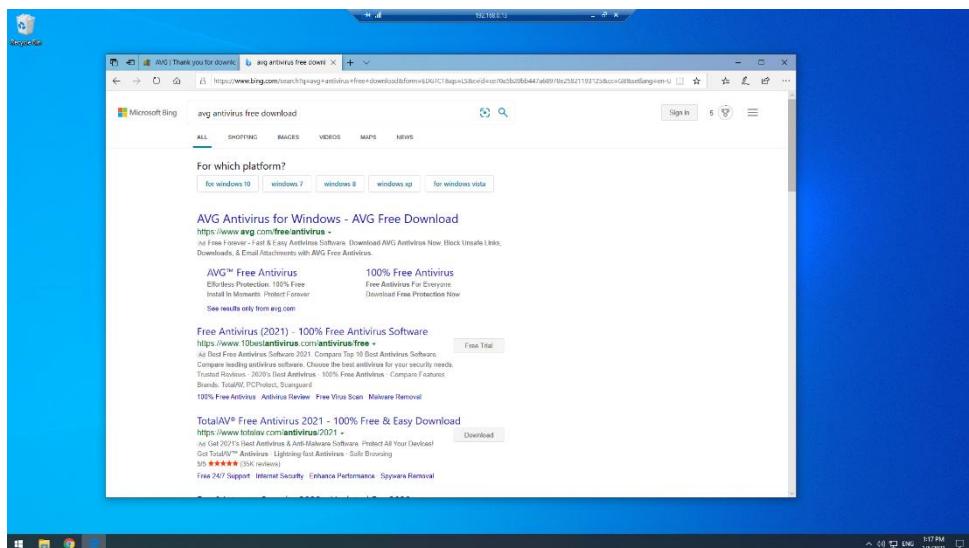
Windows 10 and HP Logos:

Windows 10 logo and HP logo are displayed on the right side of the Control Panel window.

- here I am joining the Domain I created above
- I have joined the **MyDomain.local**, using the domain admin account **dtroke** when prompted
- after joining the domain, the computer has rebooted, and I can now log in with the **dtroke** account

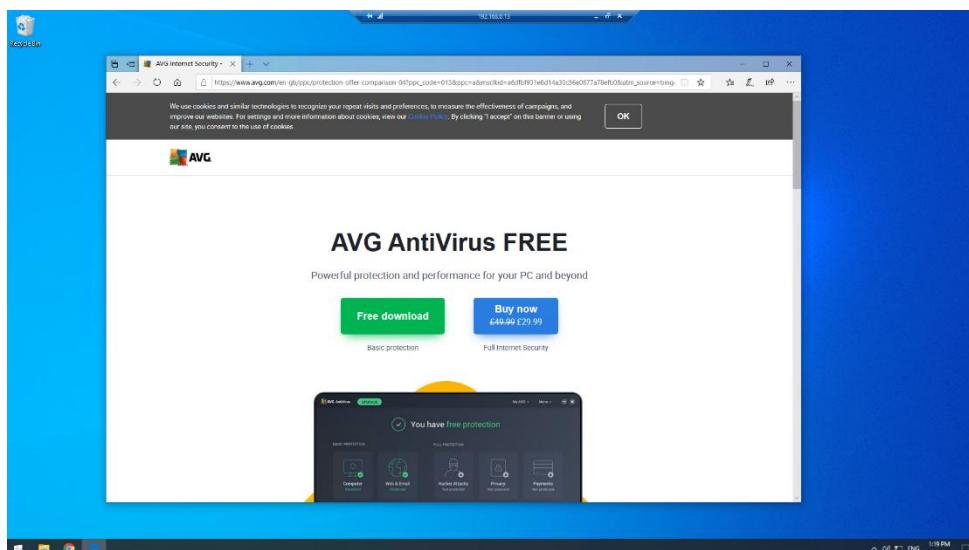
Security and installation of antivirus software

Screenshots:

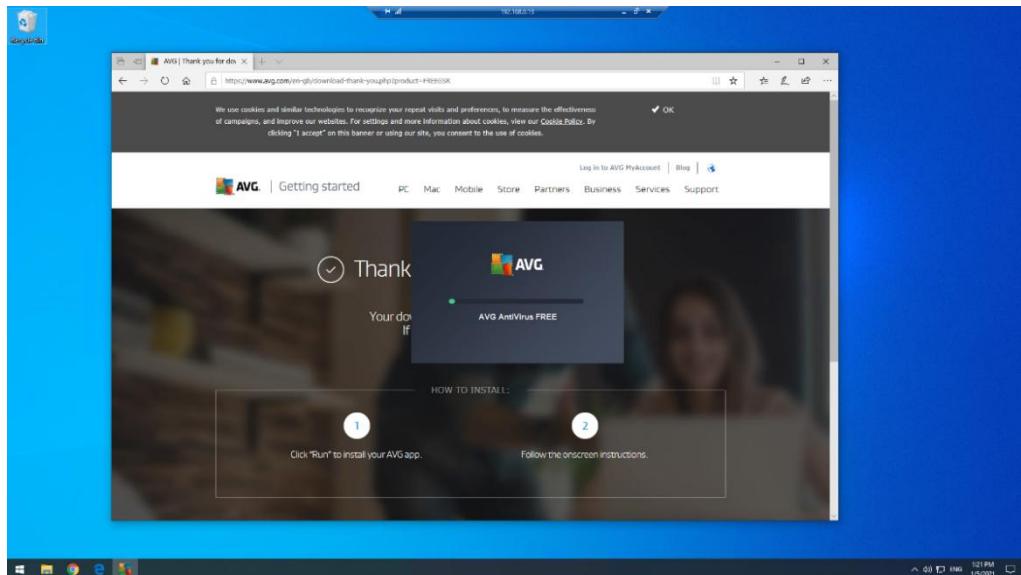


- I browse for antivirus software on the web

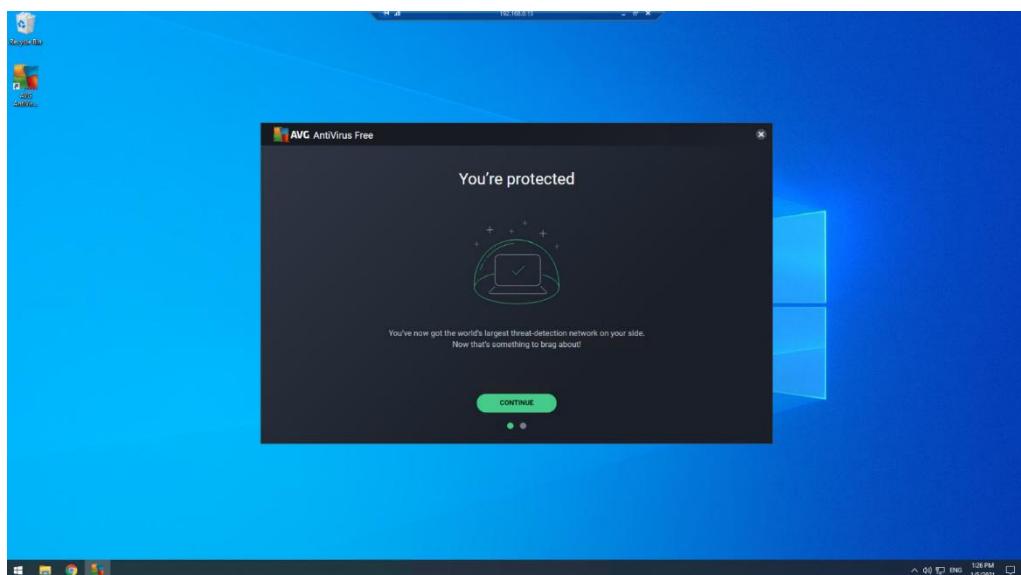
Screenshots:



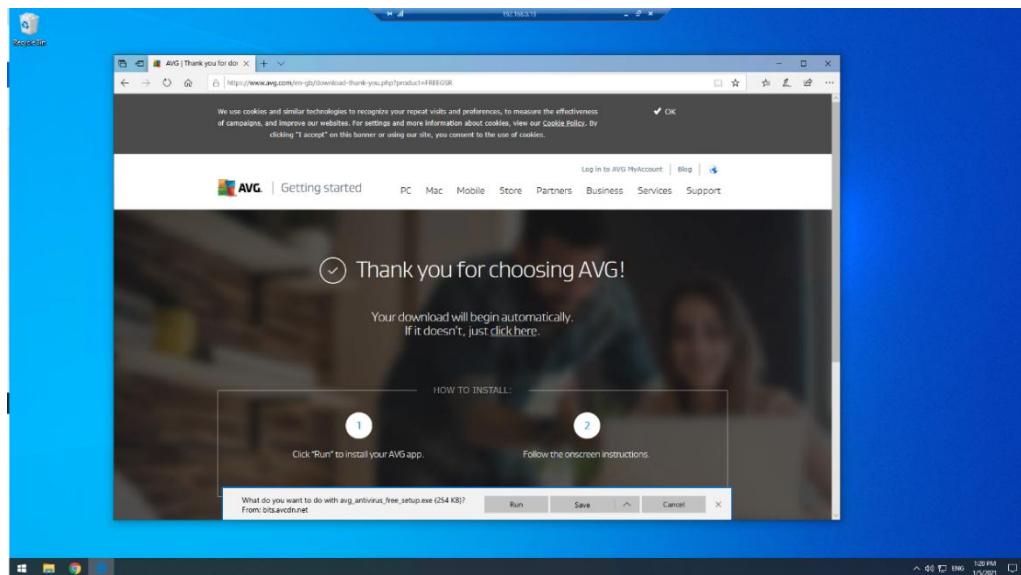
- I select the free download



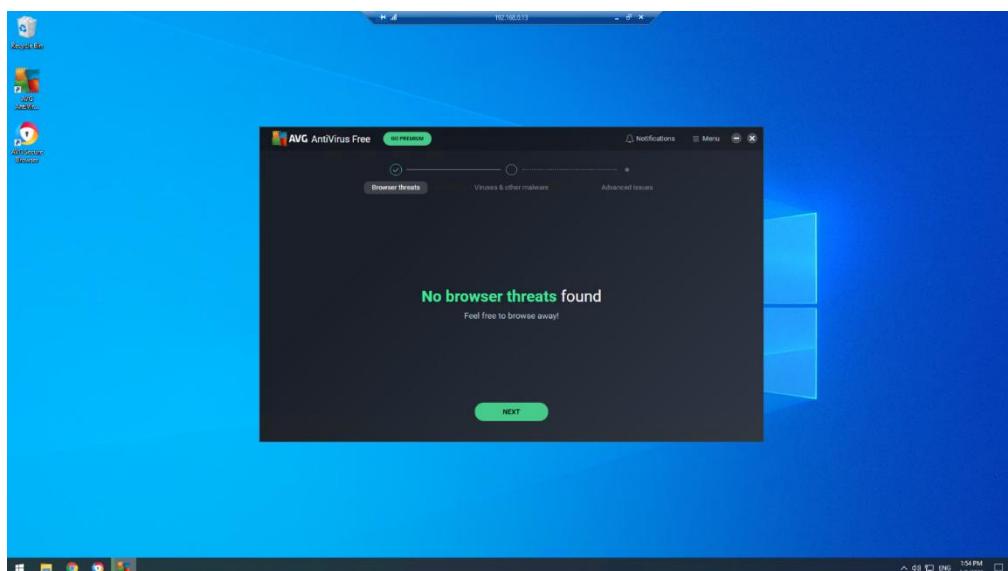
- I download the installer



- Antivirus software is now installed

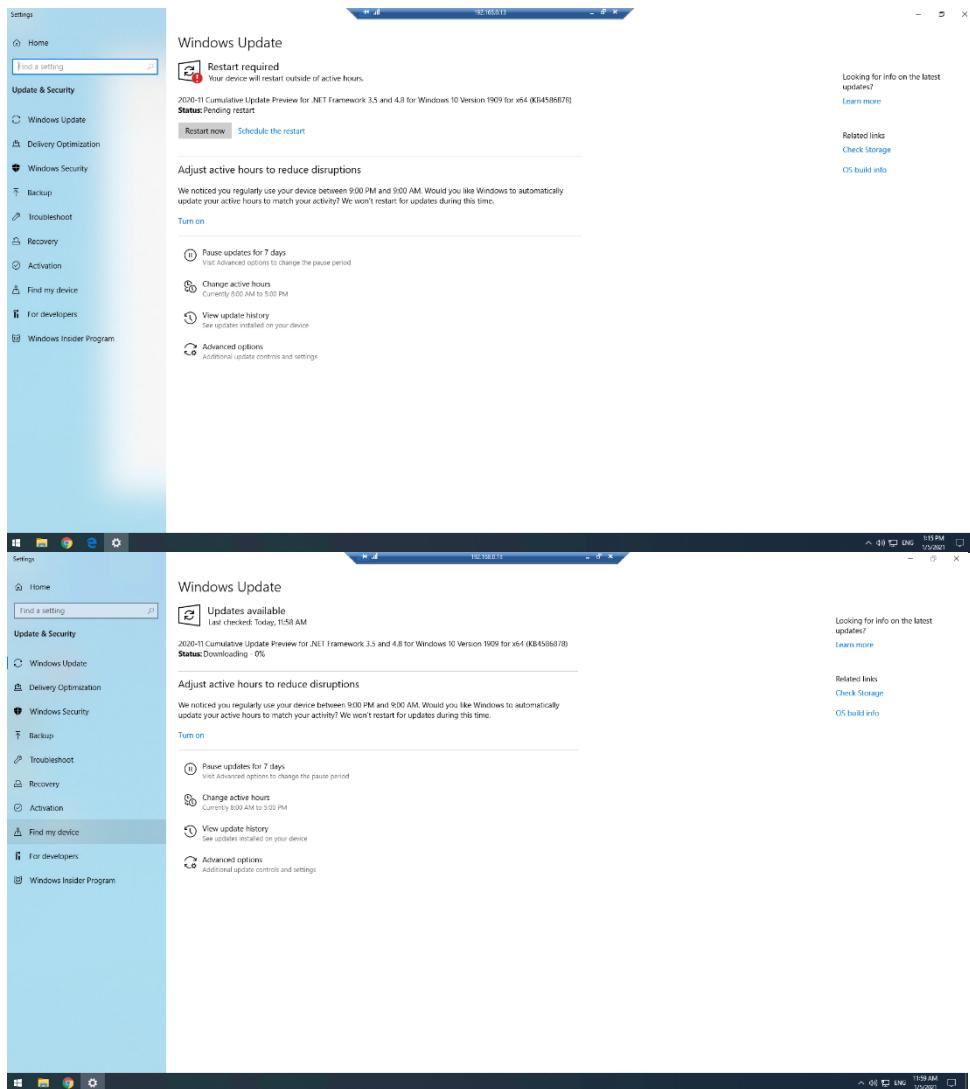


- Antivirus software is now installed 'Thank you' message from AVG



- I run a virus scan to check for viruses

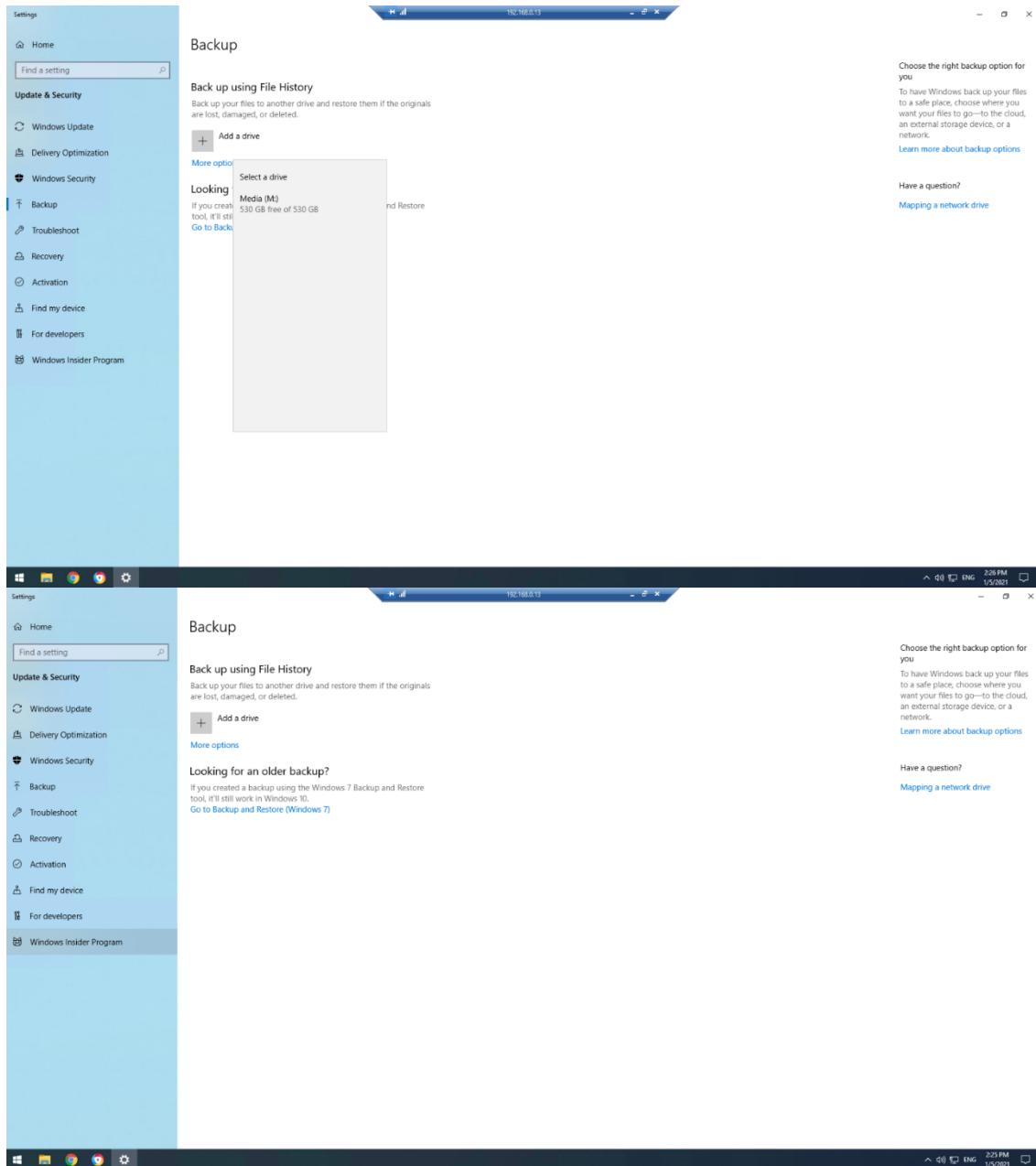
Screenshots:



- I check for Windows updates

Configuring backups

Screenshots:



Client software

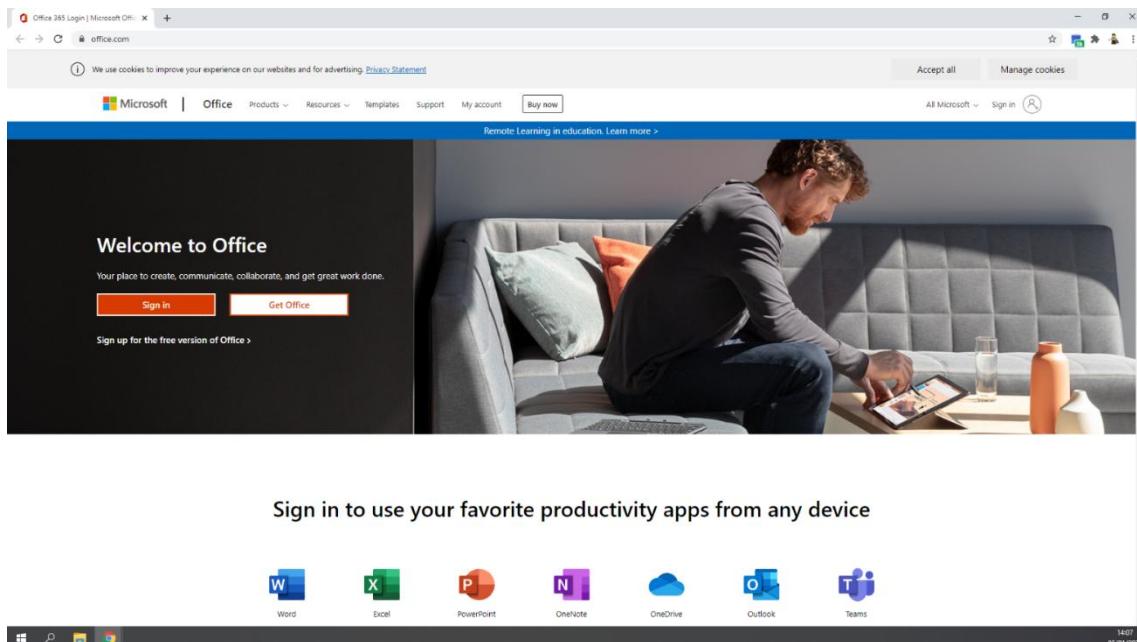
The following software was requested for installation:

- office software
- project management software
- instant messaging client software

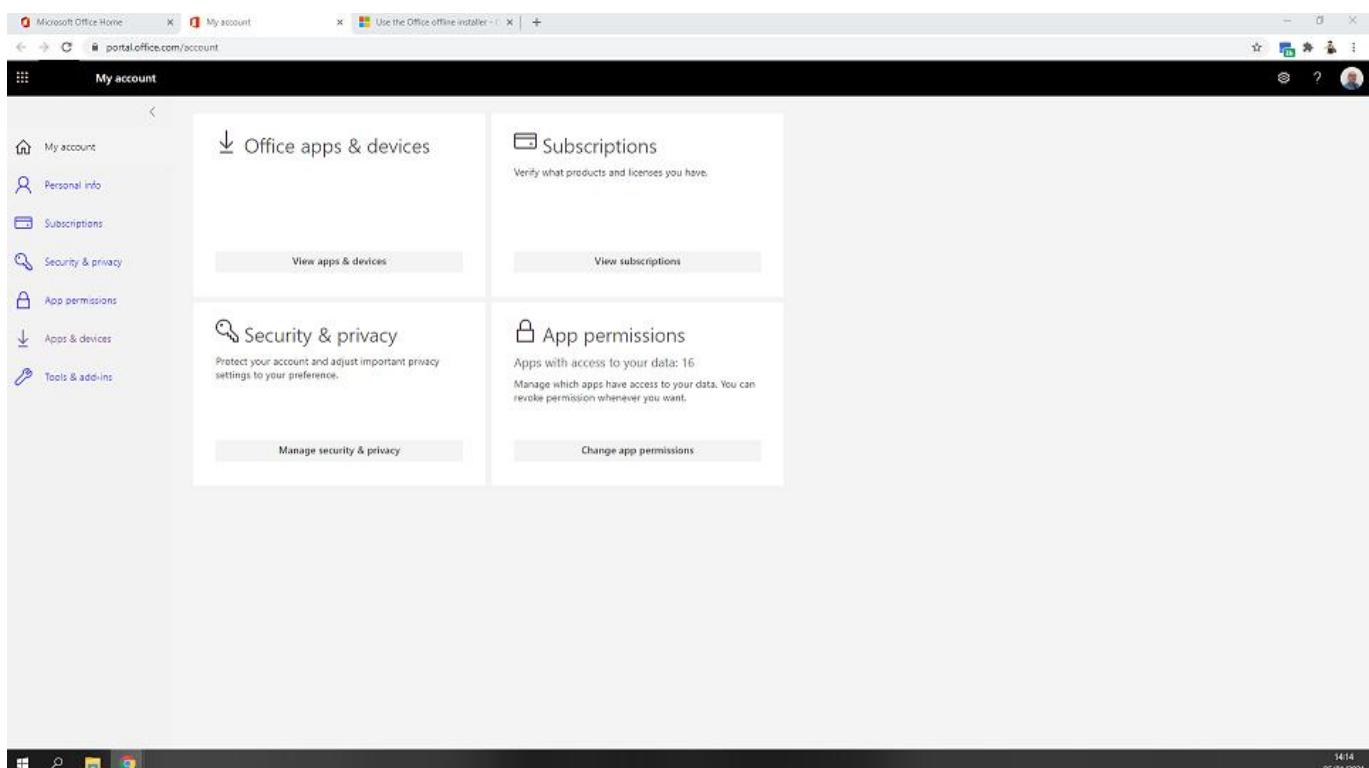
As per the network installation specification, I will install Microsoft Office 2019 which included Microsoft Project and Microsoft Teams.

Screenshots:

Setting up email

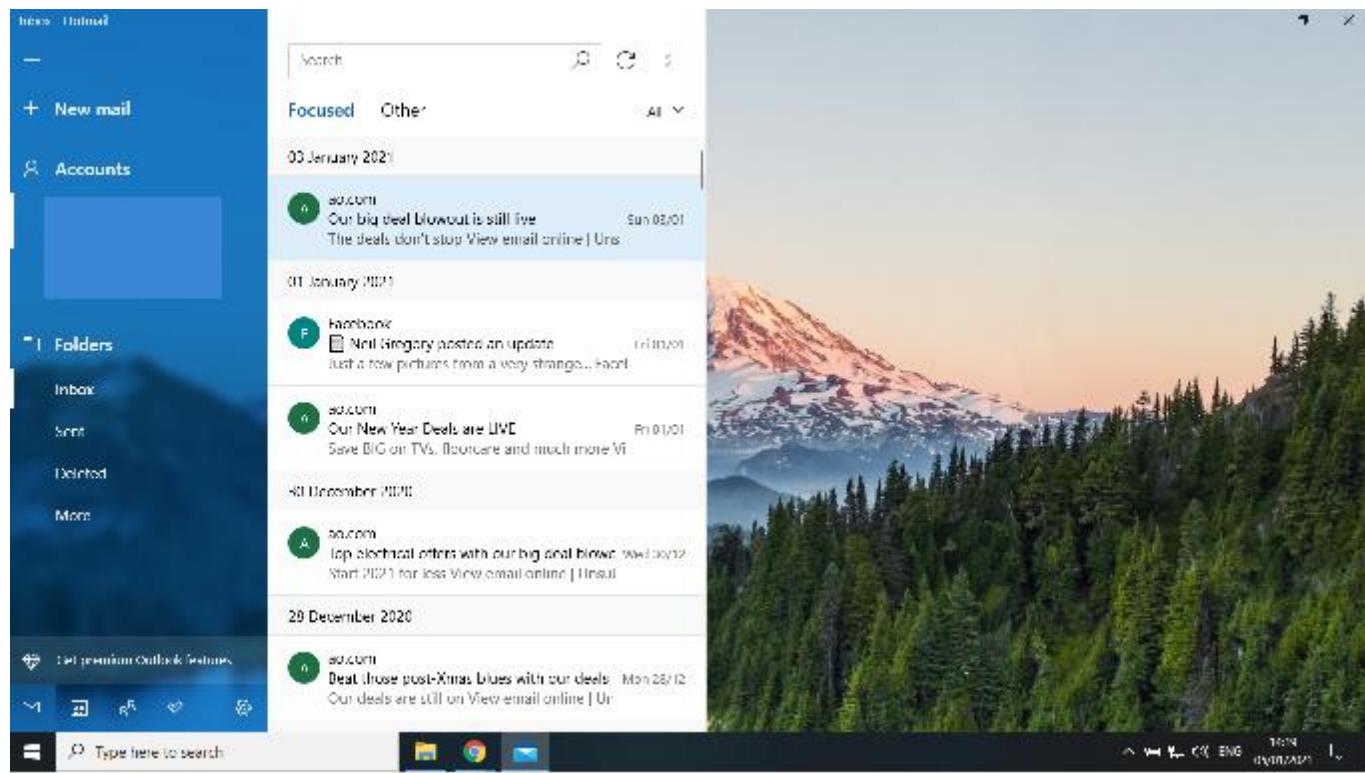


- I go to the Microsoft website



- I search for what I need and set up the email

Screenshots:

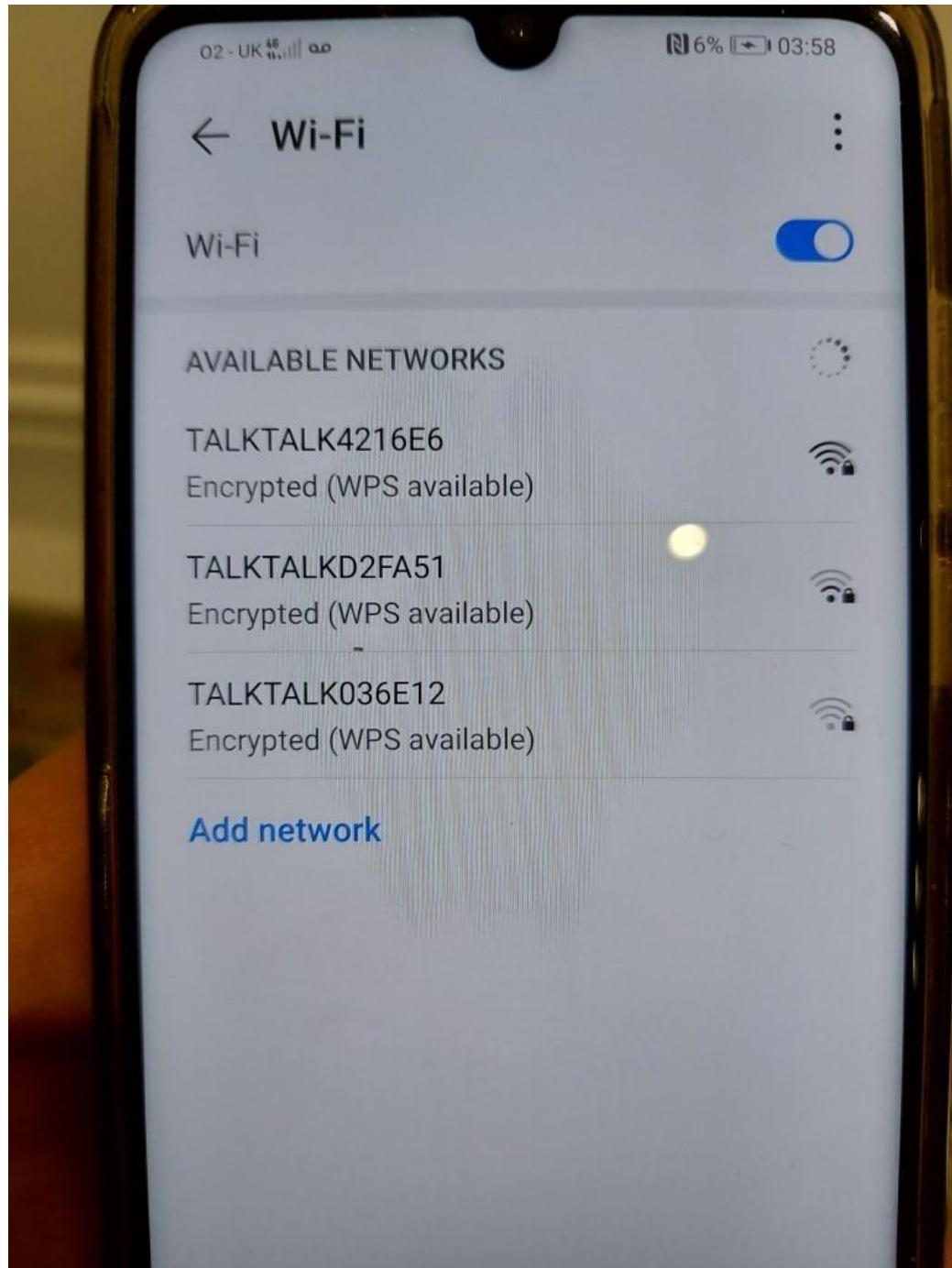


- I have set the customer email up on the client PC using the provided email configuration settings. The screenshots show I can now send and receive email

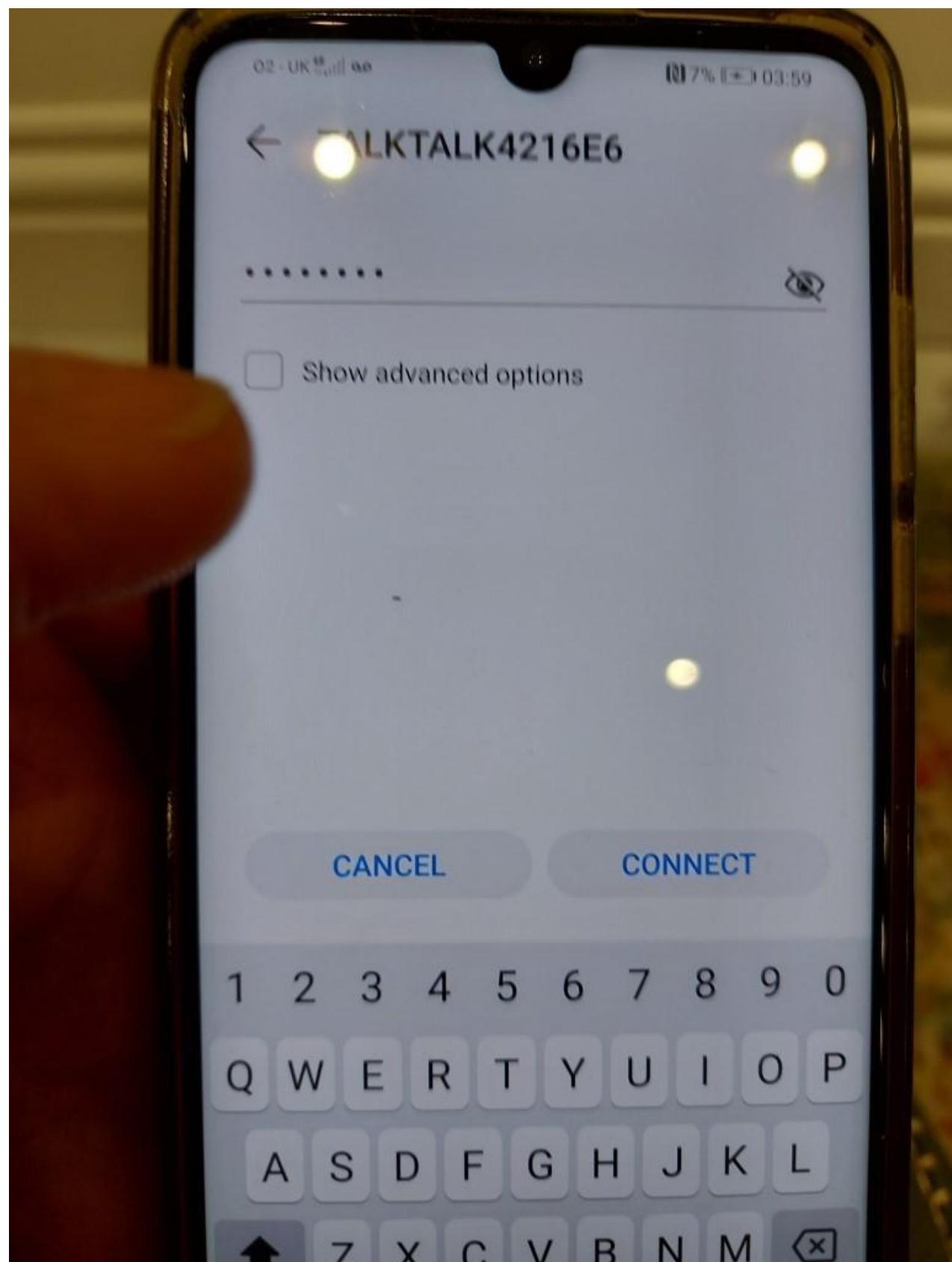
Mobile phone set-up

Connecting to wireless network

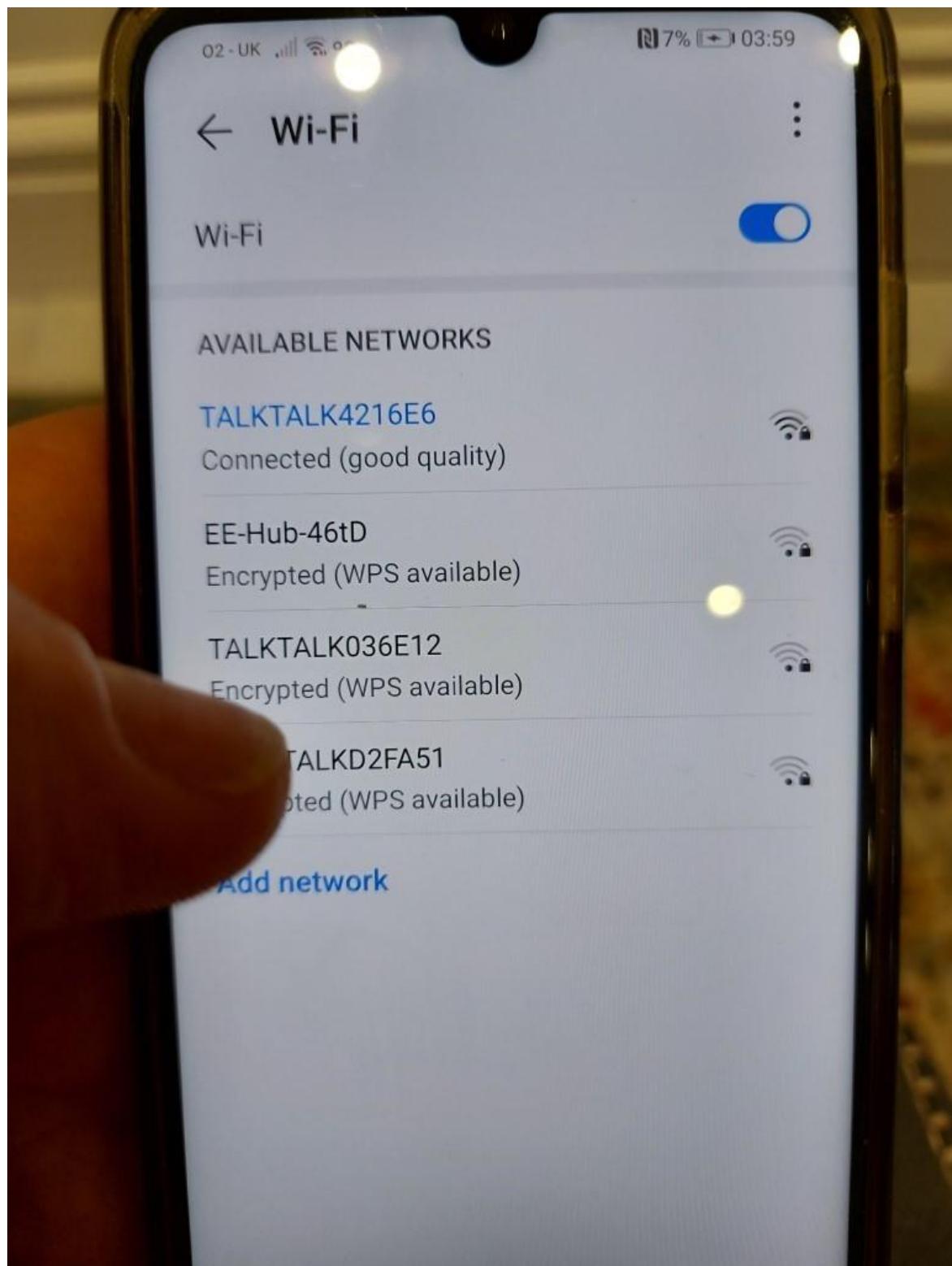
Photos:



- I open settings and scan for the company network I want



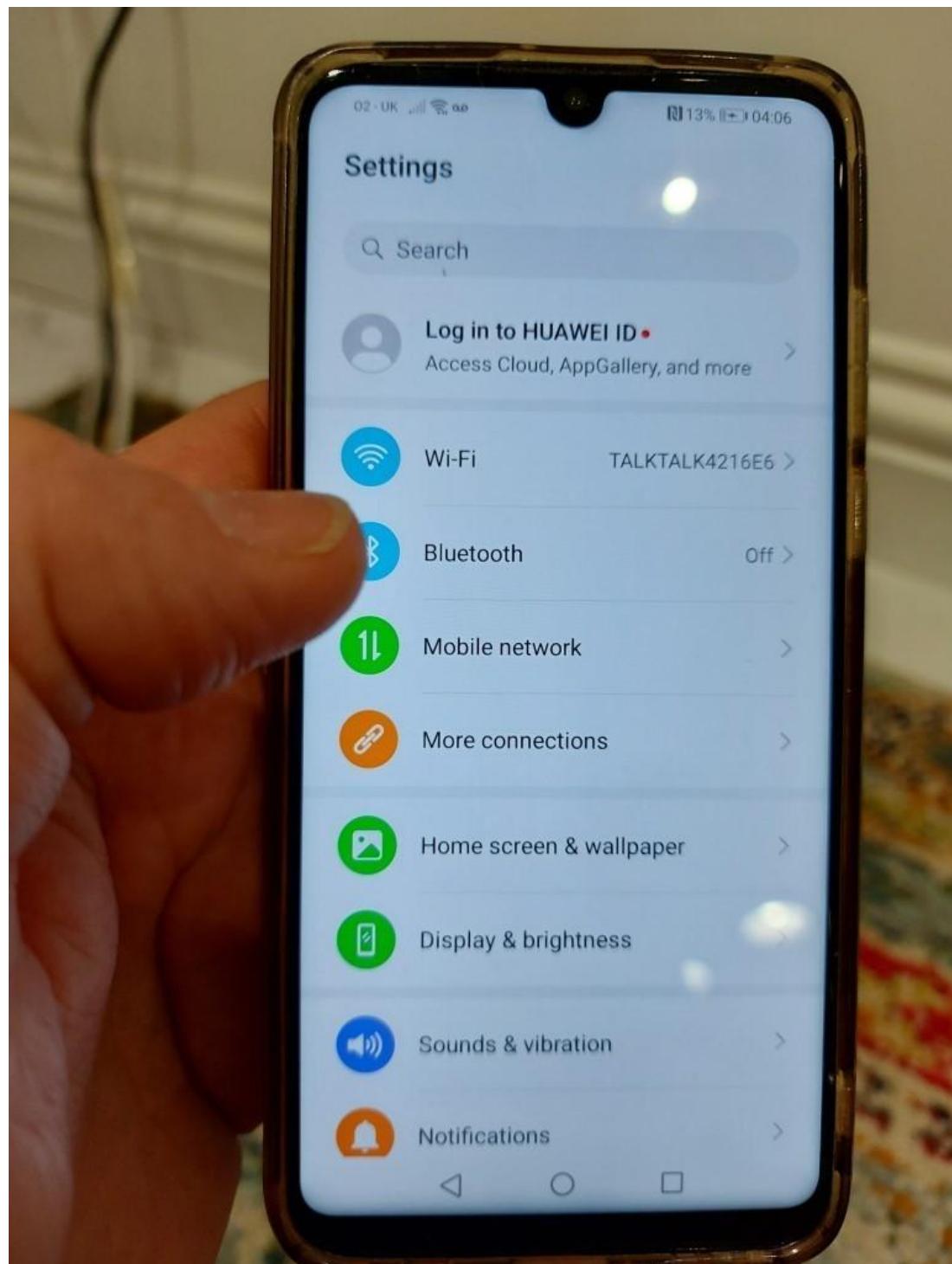
- I select the network and add the password



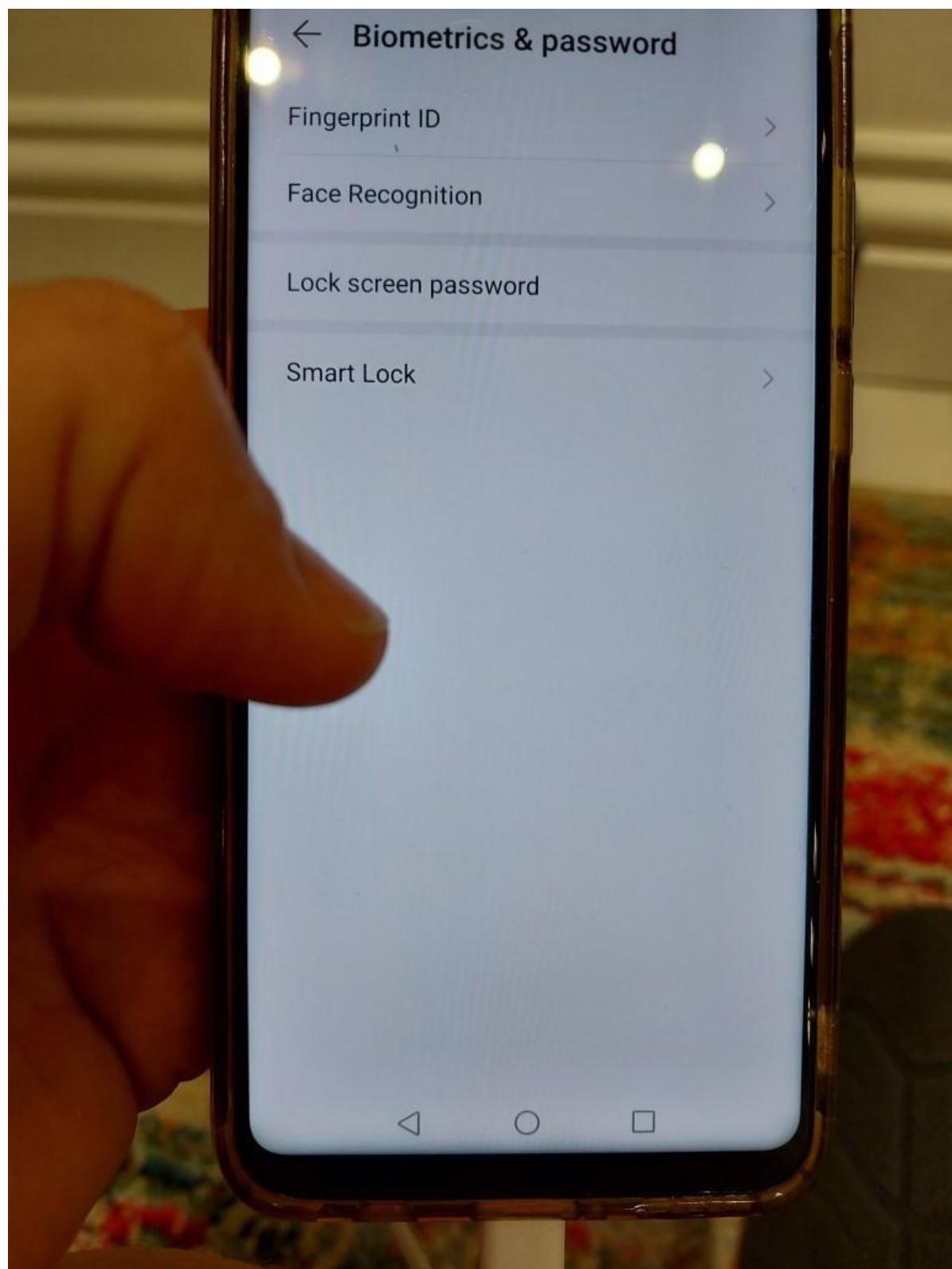
- I join the mobile phone to the office network

Implementing screen lock, fingerprint and Find My Phone

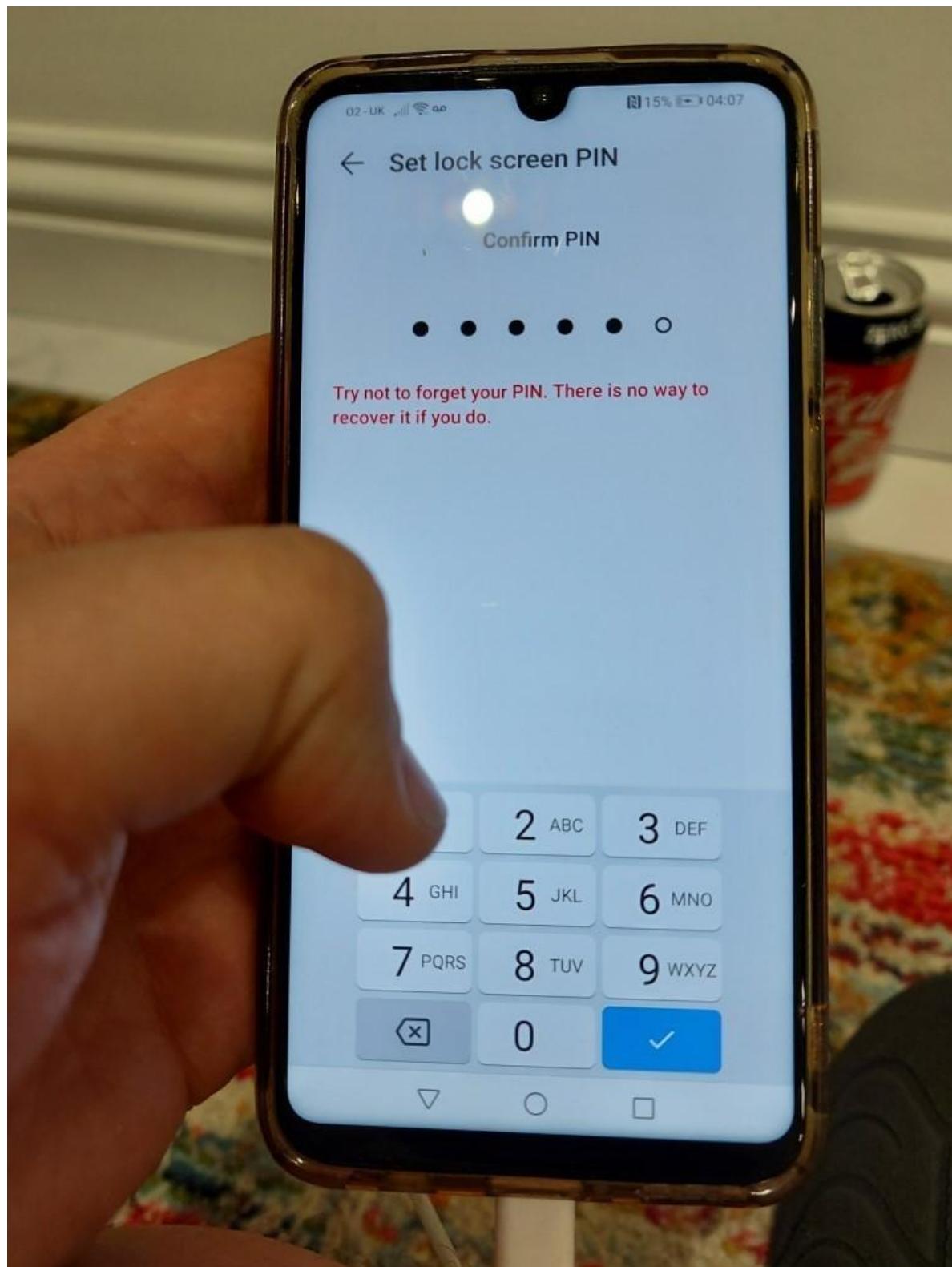
Photos:



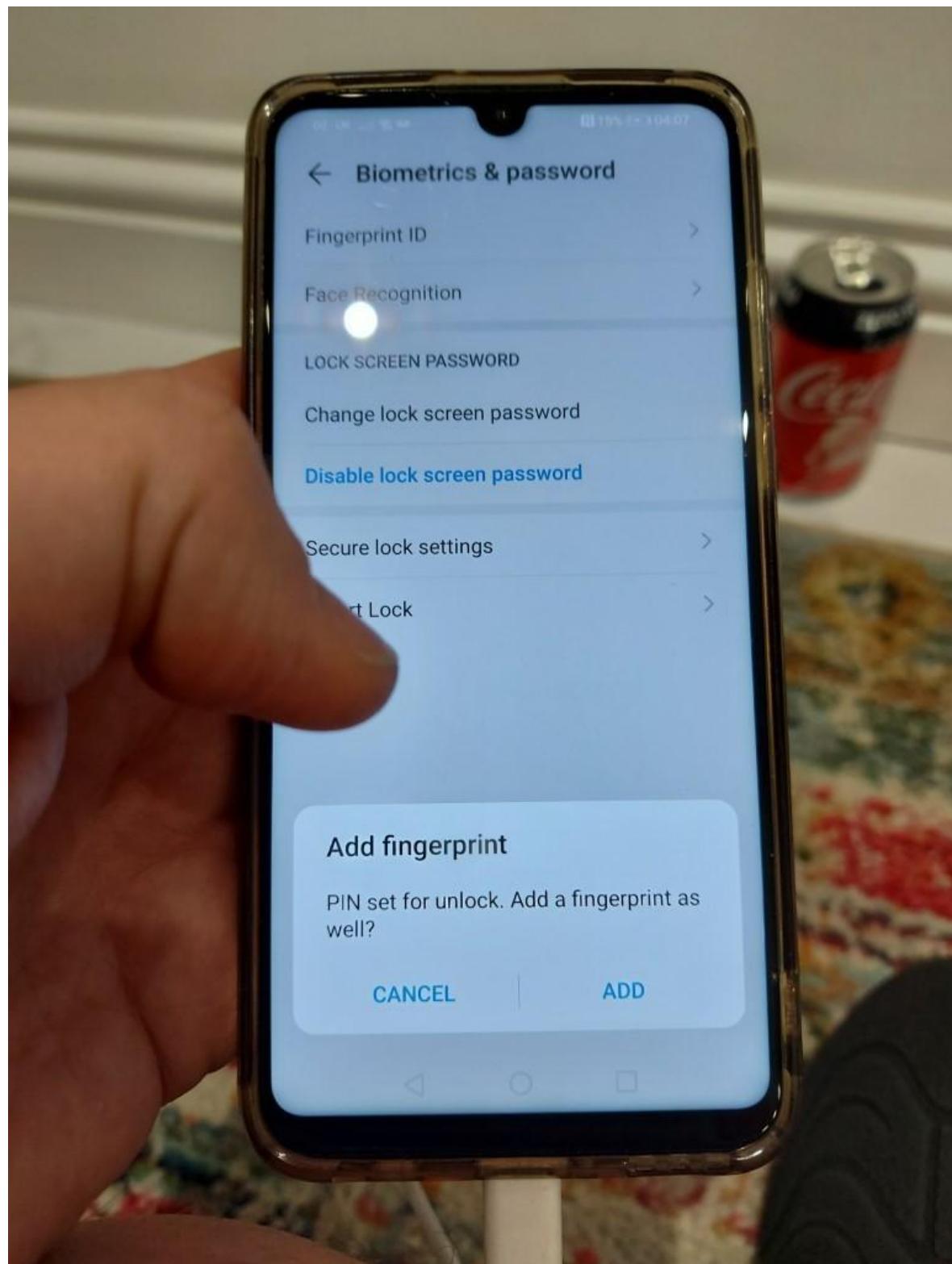
- I open settings and go to security



- I select password for the type of security

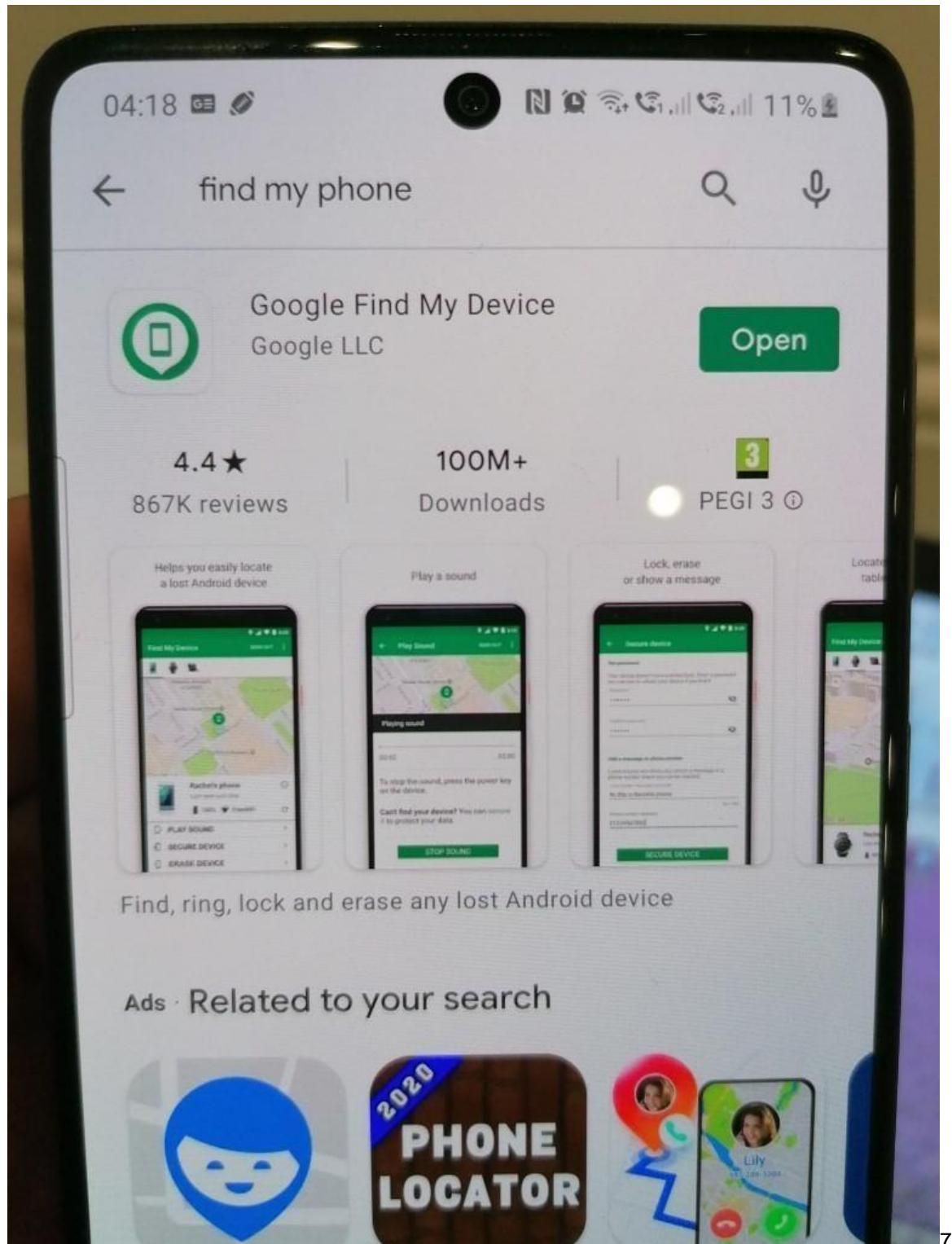


- I create a password/pin number for security

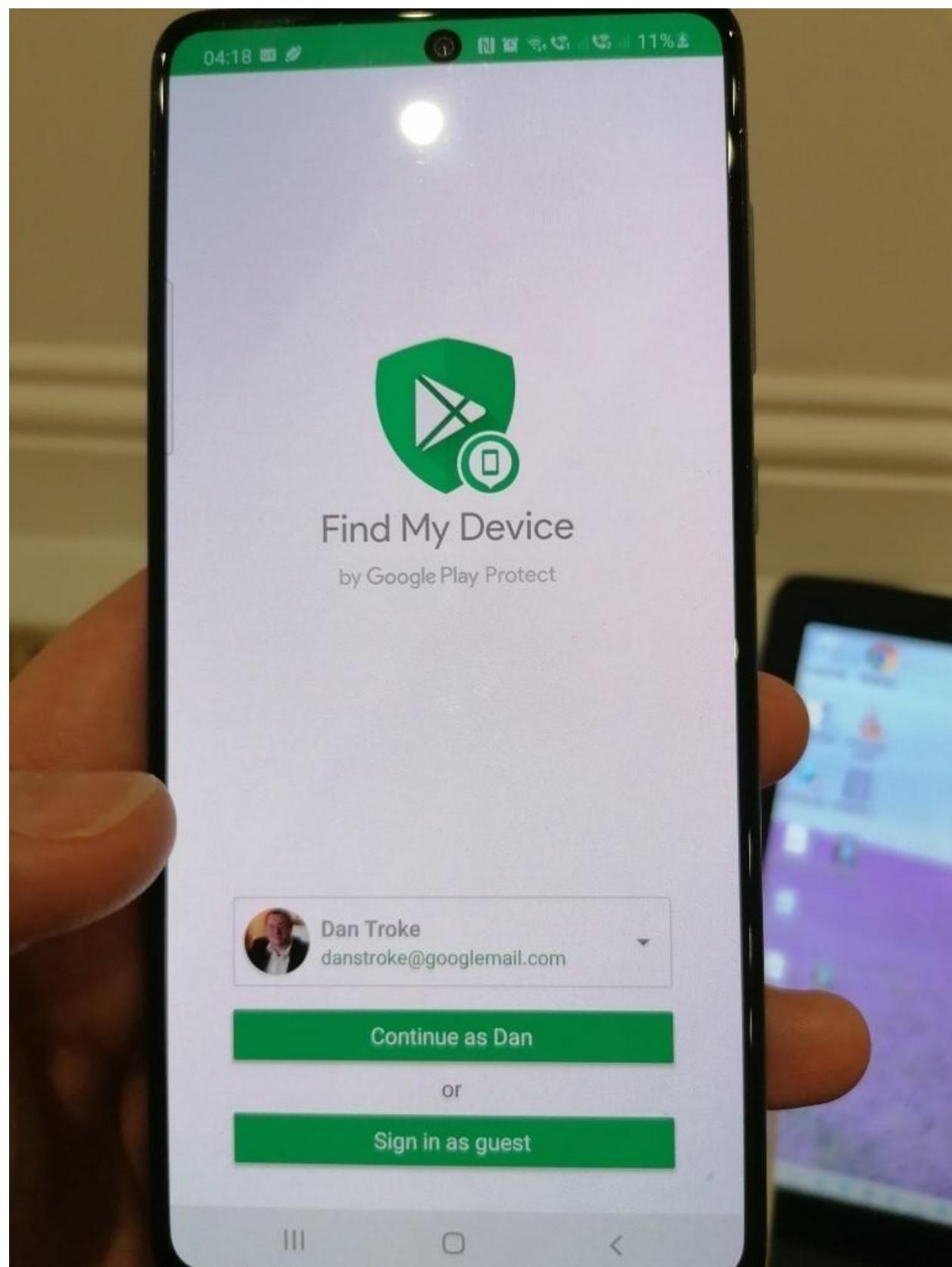


- To improve security of the mobile device I have added a screen lock with a PIN number of 8330

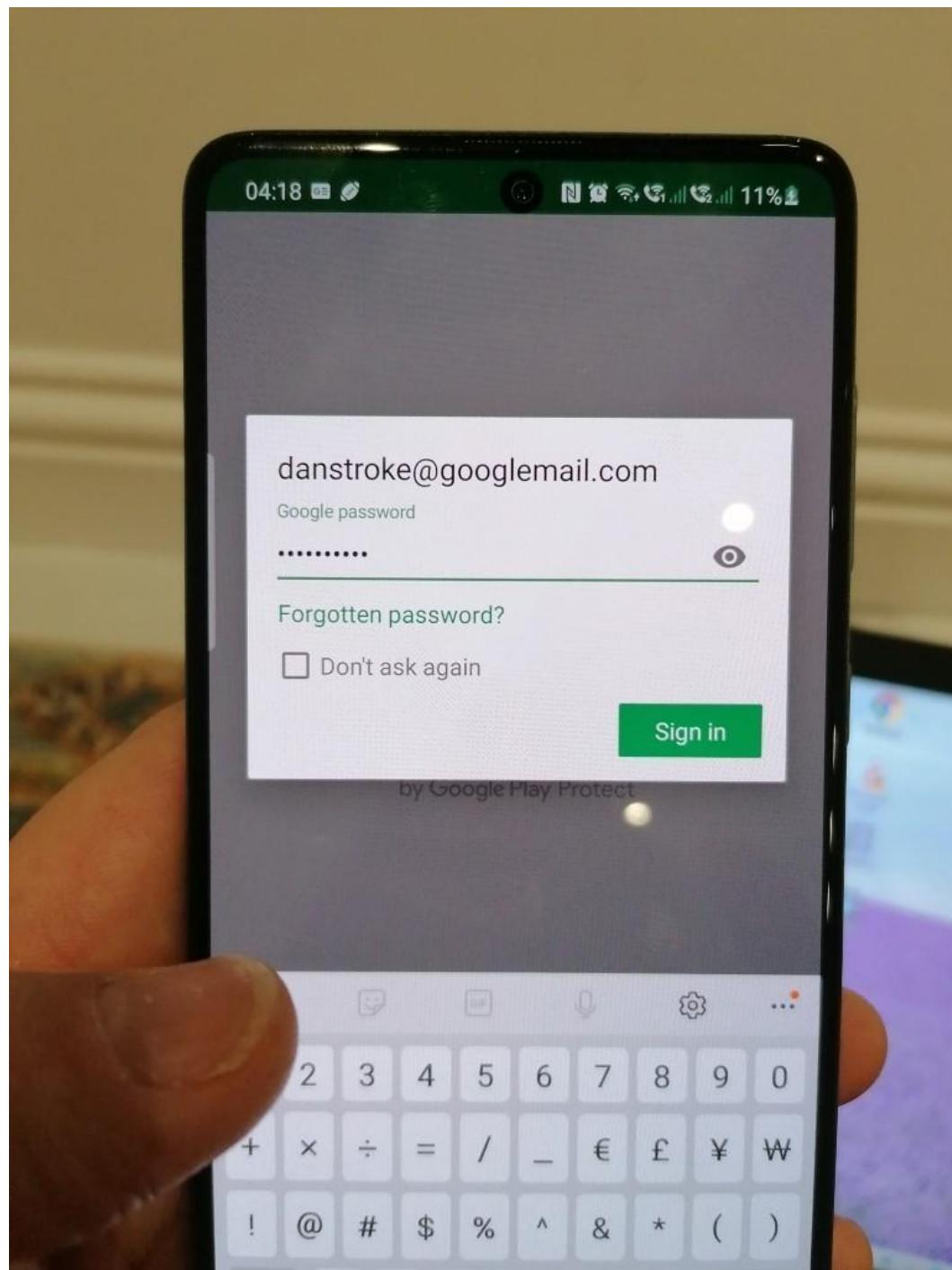
Photos:



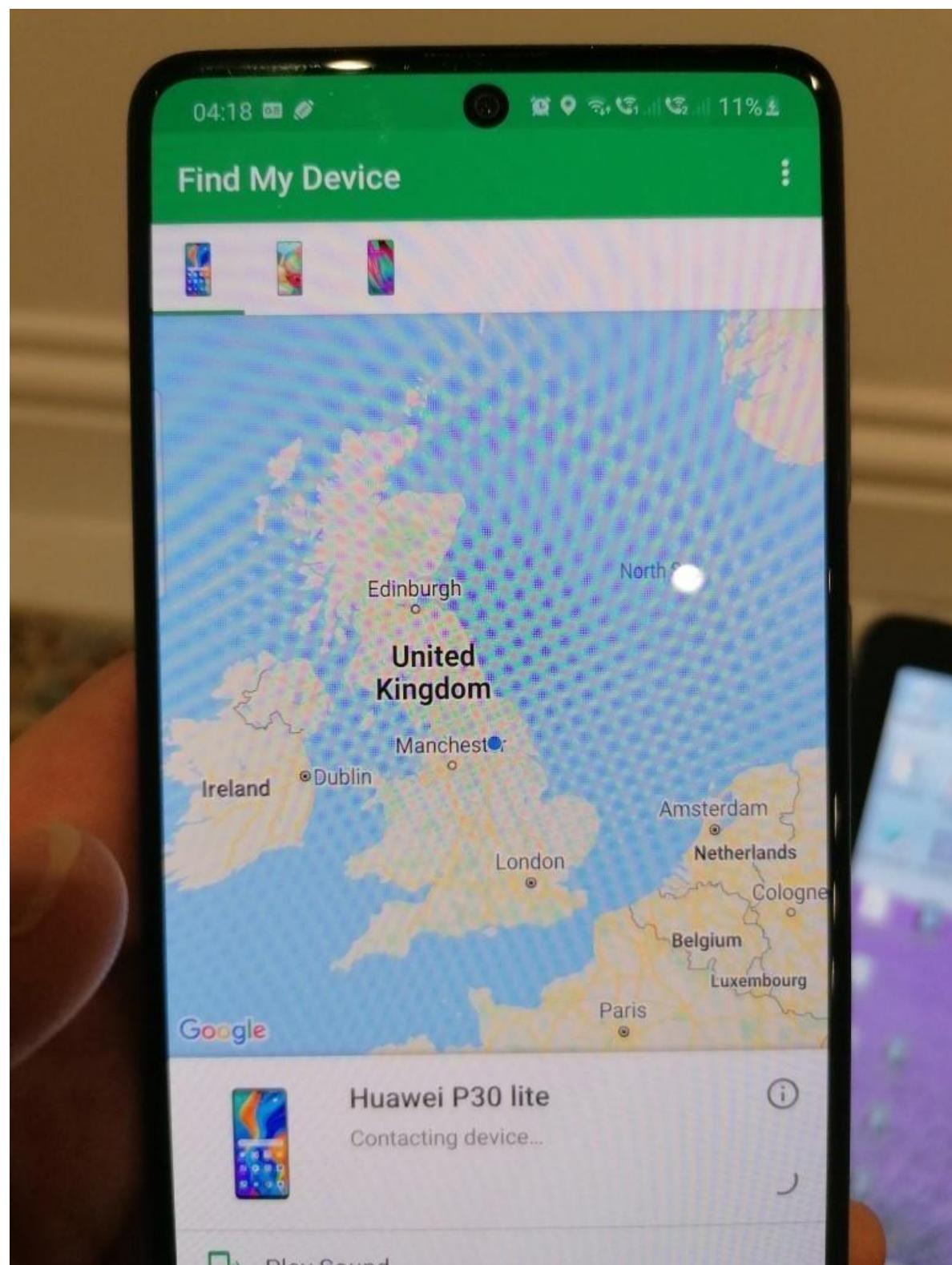
- I search the app store and open Find My Phone



- I install it



- I log in



- I can see my mobile phone's location
- In case of loss or theft of the mobile phone, I have added the Find My Phone app to help

Task 2(c) (see Appendix 1 - Workbook - DSS-007-01 Assignment 1 pass)

Examiner commentary

The student has achieved the required standard for the following reasons:

This project overall meets the requirement of the brief, however, did not fully provide all of the details that could have been included.

- there was a basic business understanding taking into consideration legislation such as GDPR
- the student has taken basic health and safety and security considerations such as signs to prevent access to dangerous areas, but they could have done more to identify risks and mitigate them
- where practical tasks are part of the assignment, they have achieved the required outcomes of the task (installing Windows server, setting up Active Directory, installing Windows 10) but has not looked deeper. This is seen in the document by specifying a 100+ port server and not considering internet access as it is not explicitly requested
- where commentary is given it is generalised and does not use many technical terms. They demonstrate general understanding of concepts but have not shown detailed knowledge of the technical terminology used in the sector
- where technical understanding of concepts is required, some detail is seen (for instance when looking at IP addressing the student has identified appropriate IP addresses but not considered subnet mask)

Grade descriptors

The performance outcomes form the basis of the overall grading descriptors for pass and distinction grades.

These grading descriptors have been developed to reflect the appropriate level of demand for students of other level 3 qualifications, the threshold competence requirements of the role and have been validated with employers within the sector to describe achievement appropriate to the role.

Grade	Demonstration of attainment
Distinction	<p>The evidence is logical and provides an excellent response to the demands of the brief</p> <p>Makes use of relevant knowledge and is well informed by the practices of the sector</p> <p>Demonstrates an understanding of the different perspectives/approaches associated within the sector</p> <p>Makes excellent use of facts/theories/approaches/concepts</p> <p>Demonstrates comprehensive use of breadth and depth of knowledge and understanding</p> <p>Consistently selects appropriate skills/techniques/methods</p> <p>Identifies information from a range of suitable sources and makes use of appropriate information/appraises relevancy of information</p> <p>Combines information to make accurate and appropriate decisions</p> <p>Makes sound judgements/takes appropriate action/seeks clarification and guidance</p> <p>Successfully tackles both routine and non-routine problems that reflect real life situations in the sector</p> <p>Effectively demonstrates skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across a variety of contexts</p> <p>Tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems</p> <p>Analyses data/information in context and applies appropriate analysis in confirming or refuting conclusions and carrying out further work to evaluate conclusions</p> <p>Justifies strategies for solving problems, giving clear explanations for their reasoning</p>
Pass	<p>The evidence is logical and a good response to the demands of the brief</p> <p>Makes use of relevant knowledge and is generally informed by the practices of the sector</p> <p>Demonstrates an understanding of some perspectives or approaches associated within the sector</p>

Makes good use of facts/theories/approaches/concepts
Demonstrates breadth and depth of knowledge and understanding
Generally selects appropriate skills/techniques/methods
Identifies information from appropriate sources
Makes use of appropriate information/appraises relevancy of information
Combines information to make accurate decisions
Makes generally sound judgements/takes appropriate action/seeks clarification and guidance
Able to successfully tackle routine problems and make some progress on solving non-routine problems in real life situations
Demonstrates most skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across different contexts
Able to make some progress on unstructured problems that have not been seen before, using their knowledge to find solutions to problems
Makes some justification for strategies for solving problems, giving explanations for their reasoning

* “Threshold competence” refers to a level of competence that:

- signifies that a student is well placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

U grades

- if a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2021.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021