T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 1 - Distinction

Guide standard exemplification materials

v2.0: Specimen assessment materials
19 June 2023
603/6901/2

Internal reference: DSS-GSEM-15

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment

Guide standard exemplification materials

Digital Support

Assignment 1

Contents

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 - something that physically stops an attacker or breach (for example, a locked door will prevent access to the server)
- detective - something that can be used to identify how a security breach happened or who was responsible (for example, log files, CCTV cameras or intrusion detection system (IDS) software)
- corrective - a control designed to fix or stop a security breach in progress (for example, fire suppression systems to put out a fire or intrusion prevention system (IPS) software)
- deterrent - anything that makes an attacker think twice (security guard, signage, acceptable use policies (AUP))
- directive - anything control that requires someone to behave in a certain manner (security policies, signage)
- compensating - controls that compensate for something that could otherwise cause harm (for example, air conditioning)
- recovery - controls to allow the business to get up and running again after a breach (for example, daily backups or business continuity plans)

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 in nature, or a company's AUP would be directive in nature as it specifies usage and behaviour, but also is a deterrent as it could potentially influence someone to avoid malicious or harmful behaviour).

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 (physical, preventative) - prevents unauthorised access to company servers
- separation of duties (administrative, preventative) - prevents one person checking their own work meaning that they cannot hide fraudulent activity, for example, someone responsible for creating user accounts would not audit user accounts and vice versa
- CCTV cameras in critical areas and corridors (physical, detective and deterrent) - allows identification of an intruder as well as the presence of visible cameras discouraging the intruder in the first place
- daily audit log checks (administrative, detective) - allows identification of security breaches that have triggered entries on logs such as the event log
- no entry signage in secure areas - (physical, directive and deterrent) - provides clear instruction on what access is allowed as well as a deterrent for an intruder
- server rooms should be air conditioned (physical, compensating) ensures servers are maintained at a constant temperature reducing risk of system failure from overheating
- password policy with password training (administrative, directive and compensating) policy will prevent the use of inadequate passwords with training to ensure staff know how to choose a good password, and also not make common password mistakes such as writing them down where an attacker could see or find them
- server backups to cloud (physical, recovery) ensure all business critical data is backed up off site to a cloud provider on a daily basis

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 meaning the customer must know their data is being collected and have given consent to do so. We need to tell the customer how we are going to use the data at the point of collection (transparency) and needs to only use it for the reasons we have told them (fairness). This should all be included in a data notice at point of collection
- purpose limitation:
    - this puts the idea of fairness into practice. We need to inform clients of what we will do with their data and be explicit and specific about this. Once we have the customer data, we should only ever use it for the purposes we said we would use it for
- data minimisation:
    - we can only collect data we need. This means that we should know what data we need from the customer and only ever ask for this. Under GDPR rules we have to justify in our policy the amount of data we wish to collect and why
- accuracy:

    - where we hold data on a customer, we need to make sure it is up to date. When a customer informs us of an update or change to their data or information, we should update this immediately. Old or outdated data should not be kept and should be removed
- storage limitation:
    - we can only keep data for as long as we need it. We have a responsibility to keep data in a form which permits identification of data subjects for no longer than necessary. A data retention policy will specify what data we keep, for what reasons and how long
- integrity and confidentiality (security):
    - all data needs to be kept secure. This means we need to implement adequate security (for example, encryption of customer data in transit, policies preventing customer data being kept on mobile devices, or anonymising data to protect customer identity. ISO 27001 accreditation will help achieve this)
- accountability:
    - adequate documentation should be maintained to allow any auditor to see that you are compliant with the DPA 2018. All data management needs to be planned and you must be able to demonstrate that you are compliant with all 7 principles

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 with the following roles:
        - domain controller (Active Directory)
        - file and print server
        - DHCP server
        - DNS server

- Windows server update service (WSUS) server (to manage operating system updates)
- for security the server should also include antivirus/endpoint protection software capable of maintaining antivirus/endpoint protection clients on all client PCs (Sophos Endpoint Protection)
- client PCs
    - all client PCs should be installed with Windows 10 Enterprise and joined to the domain
    - all client PCs should be installed with the following software:
        - productivity software:
            - Office 365 (Word, Excel, PowerPoint and Outlook)
            - allows working with common working documents and email management
    - Adobe Acrobat
        - allows opening and working with PDF format files
    - endpoint protection software:
        - Sophos Endpoint Protection - maintains protection from viruses, malware, spam, external threats
- switches:
    - based on the client specification, the network will require connectivity for a minimum of 106 devices (100 PCs, 1 server, 5 printers). I have also allowed for connectivity to a gateway firewall/router as well to provide internet access
    - to allow for this level of connectivity we are recommending installation of 4 managed switches:
        - switch 1 - connectivity of core hardware (server, gateway firewall/router, printers, other switches (10 devices in total)):
            - specified as one 12 port switch allowing 2 spare ports for future growth
        - switch 2 to 4 - connectivity of client PCs:
            - specified as three 40 port switches with 1/3 of client PCs connected to each, allowing spare ports on each switch for future expansion
- gateway router/firewall:
    - although not listed in the specification brief, a gateway router/firewall has been included to allow secure internet connectivity
- 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
    - reserved IP addresses:
        - 192.168.0.1 reserved for server
        - 192.168.0.10-19 reserved for printers

        - 192.168.0.220-229 reserved for switches
        - 192.168.0.254 reserved for gateway router
    - DHCP server scope:
        - 192.168.0.100 to 209

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

Network installation plan

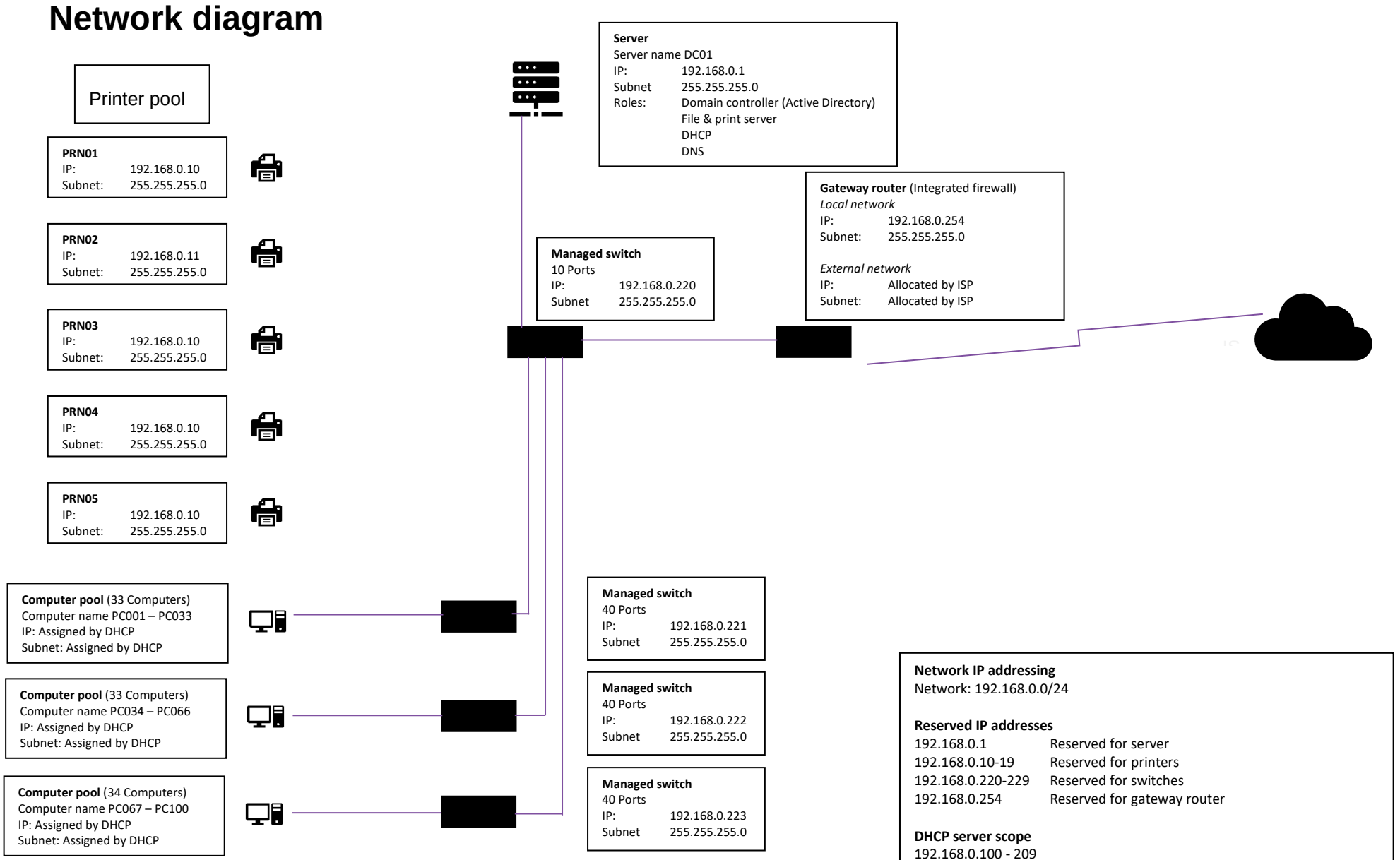
The network installation should be completed with the following steps:

- **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)
    - 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 set-up)
    - PCs connected to installation server via PXE boot
    - 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



Network IP addressing
Network: 192.168.0.0/24

Reserved IP addresses

192.168.0.1	Reserved for server
192.168.0.10-19	Reserved for printers
192.168.0.220-229	Reserved for switches
192.168.0.254	Reserved for gateway router

DHCP server scope
192.168.0.100 - 209

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)

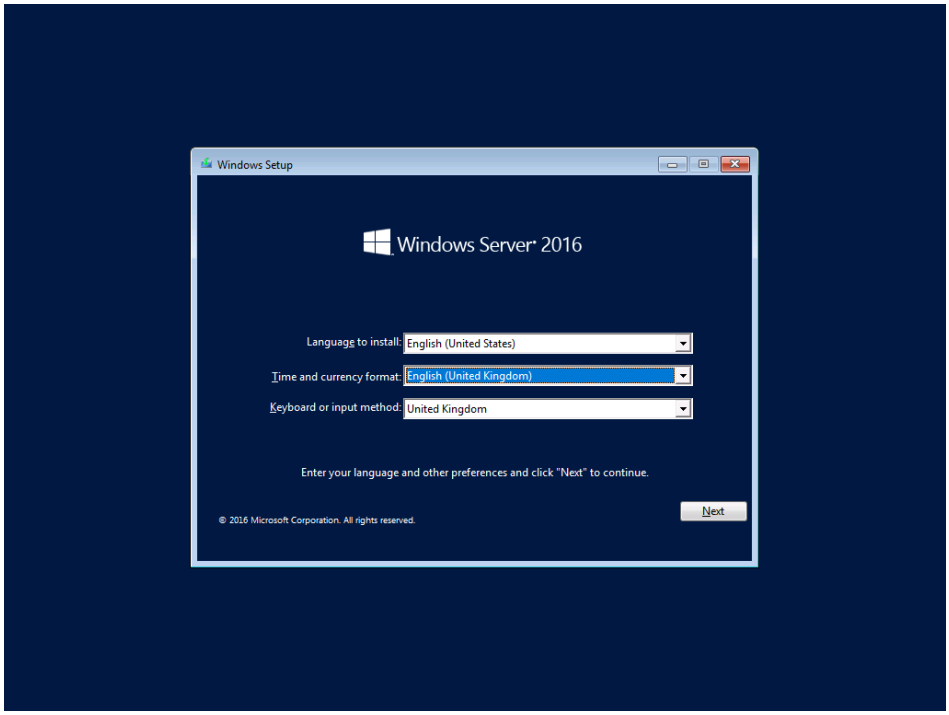
Student evidence

Task 2(a)

Evidence for this task will include a series of either screenshots or photographs documenting the installation process to show what the student has 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.

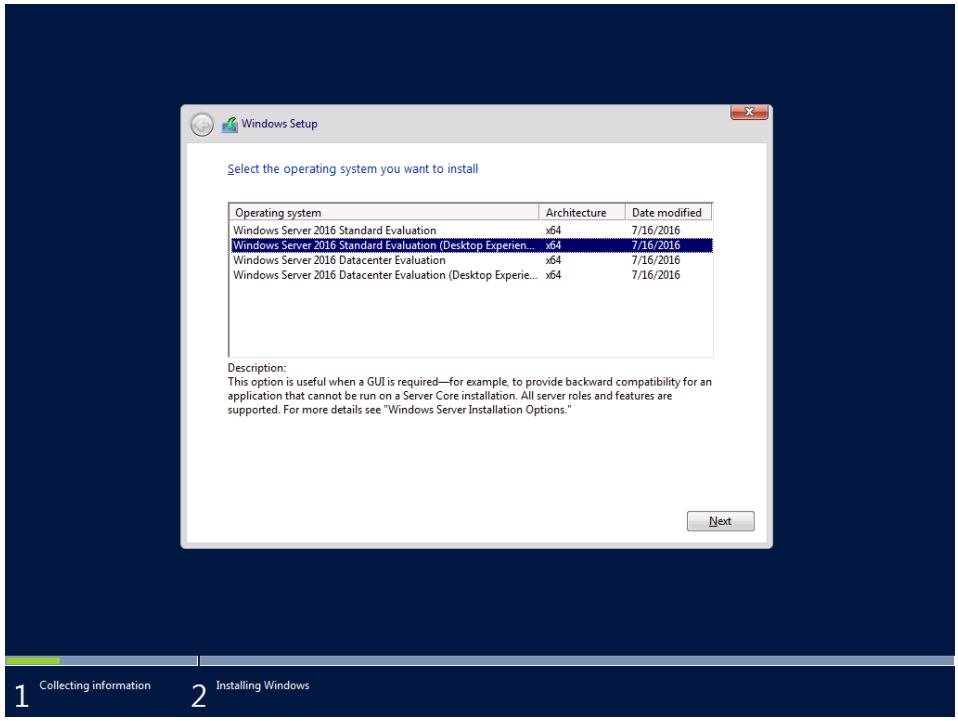
Installing Windows Server 2016

Screenshot:



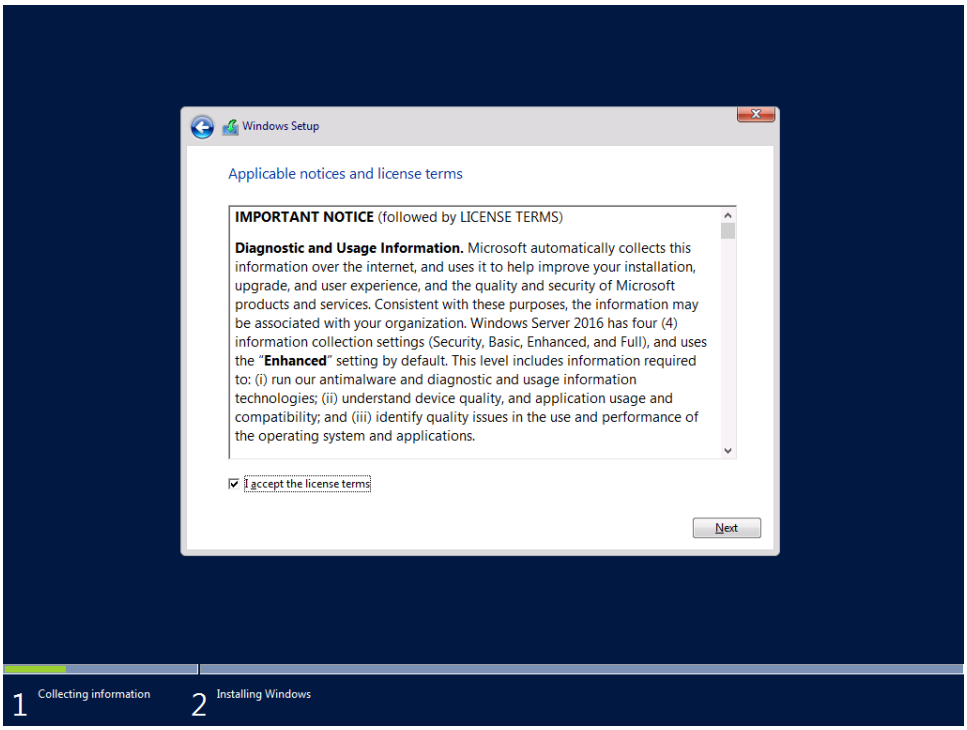
- screenshot shows server being booted from Windows server installation media

Screenshot:



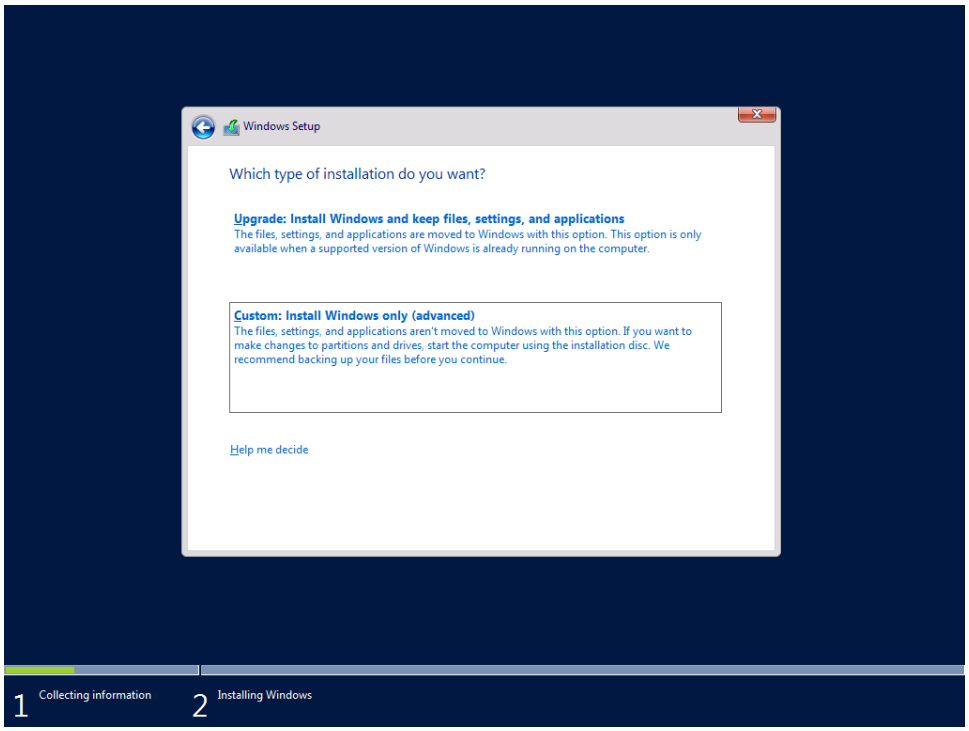
- screenshot shows selection of Windows Server 2016 (desktop experience) - this provides a full Windows desktop to make it easier to manage the Windows environment on our network

Screenshot:



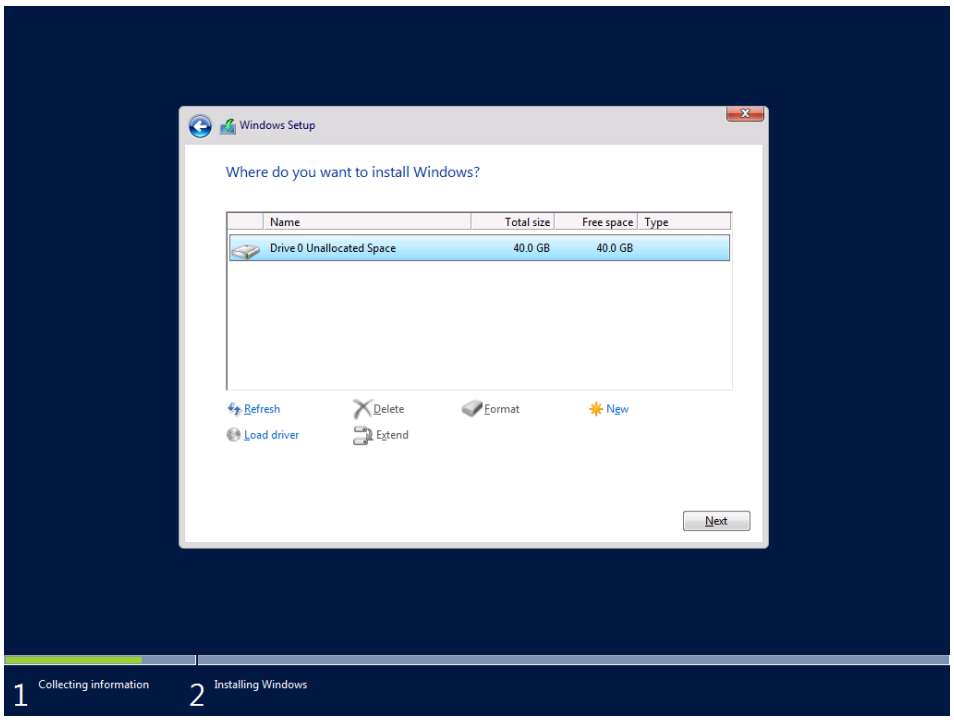
- screenshot shows me selecting to agree to the licence agreement as required by Microsoft to use the software

Screenshot:



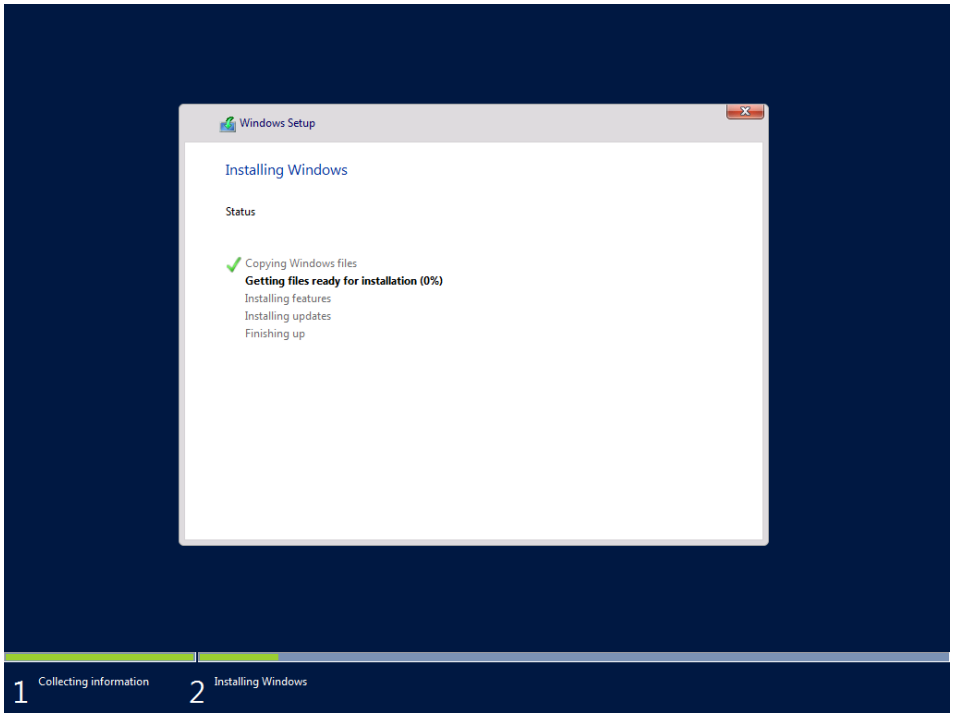
- screenshot shows me selecting a custom install - this option allows me to do a full installation of the Windows software

Screenshot:



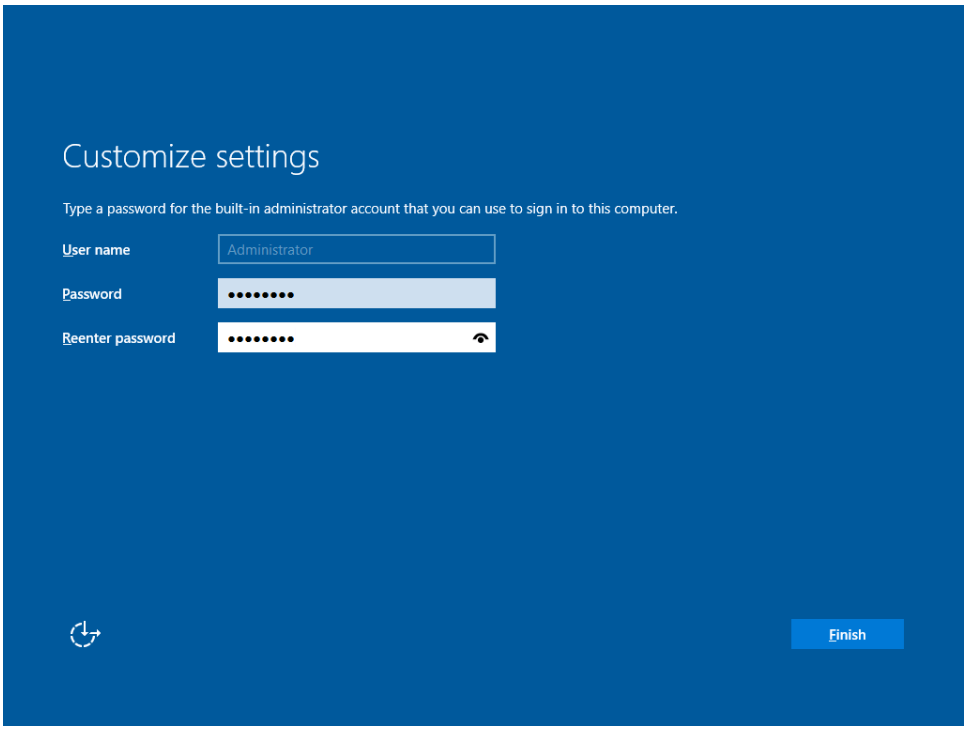
- screenshot shows me selecting the hard drive that I want to install Windows onto

Screenshot:



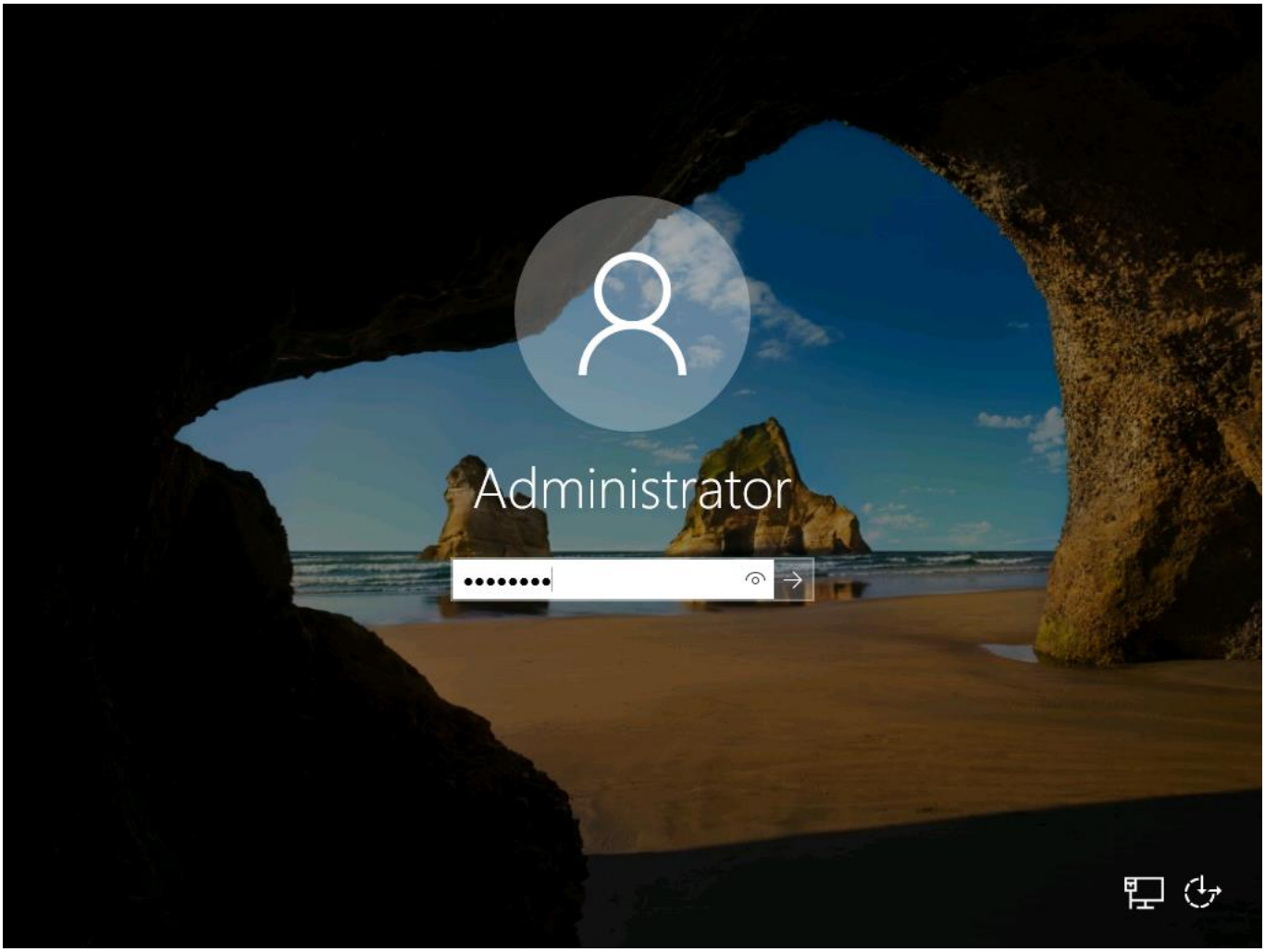
- Windows Server 2016 is now installing on the server; this will take some time

Screenshot:



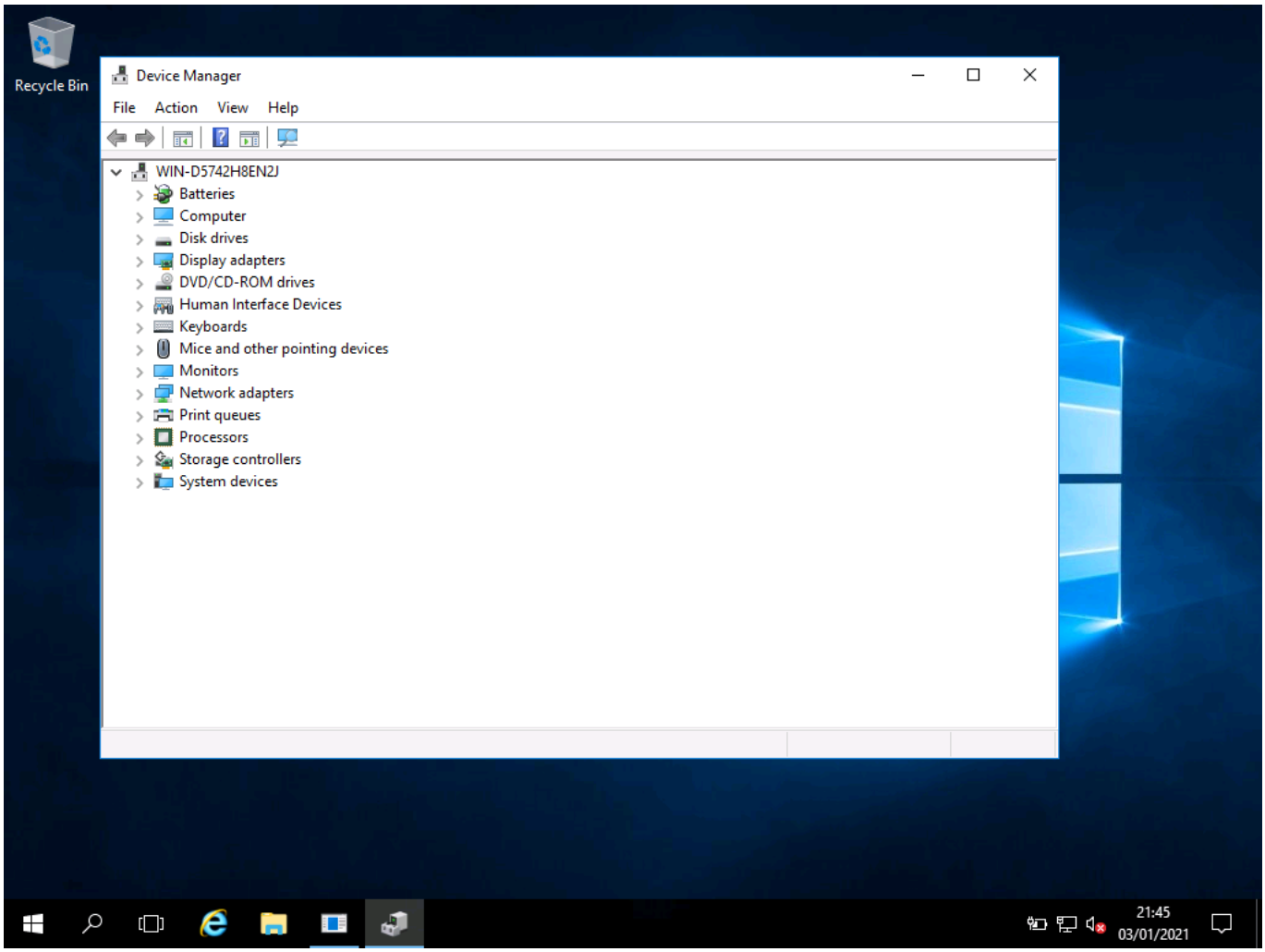
- Windows is now installed; I am prompted to set a password for the main local administrator account for the server
- for security reasons, this password must be complex (for example, at least 8 characters, including upper/lowercase and a symbol) to minimise the risk of the password being compromised

Screenshot:



- I am now prompted to log into Windows for the first time with the administrative details set in the previous step

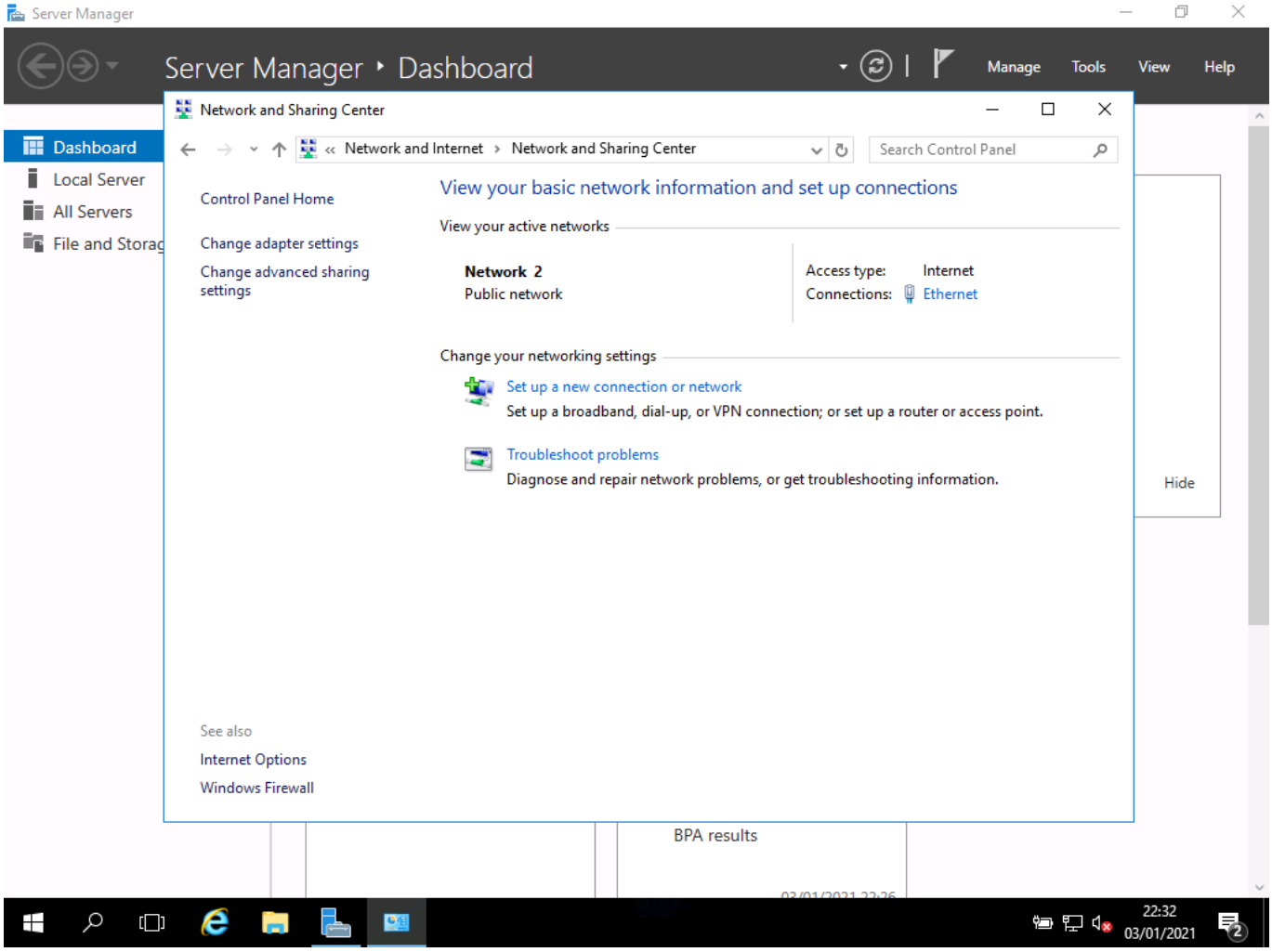
Screenshot:



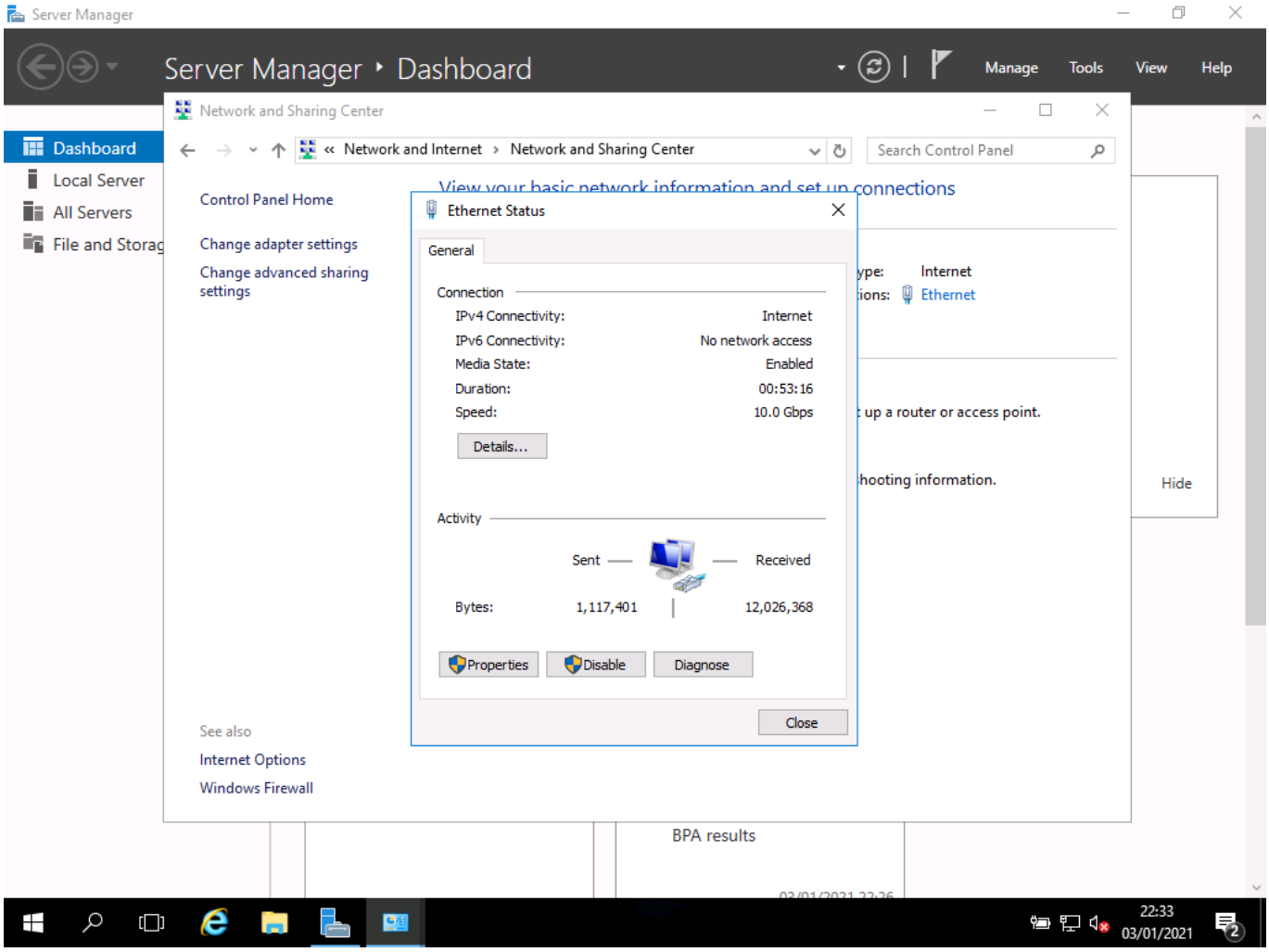
- I have checked device manager; all drivers for this server have been detected and installed automatically

Setting up network settings

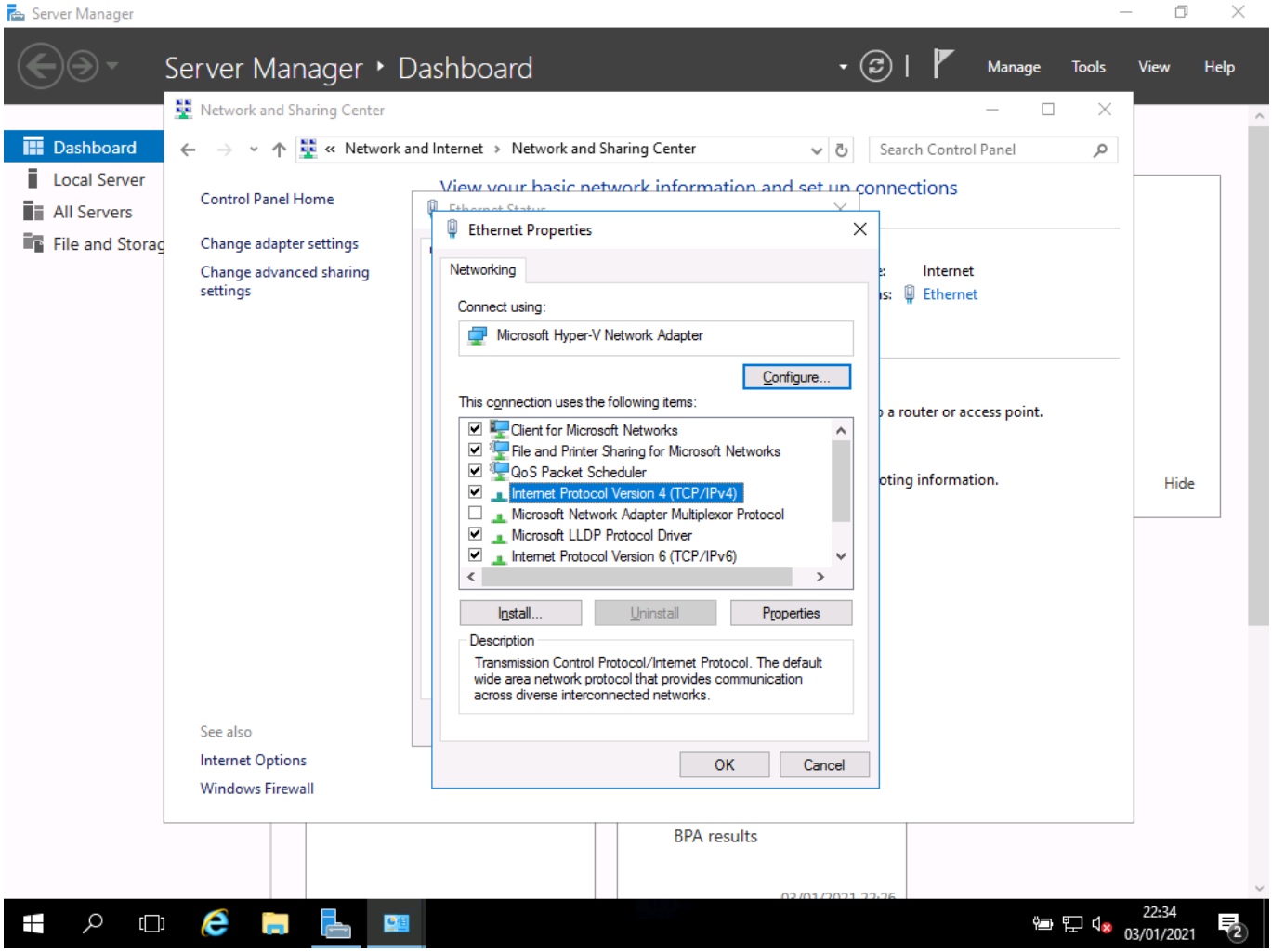
Screenshots:



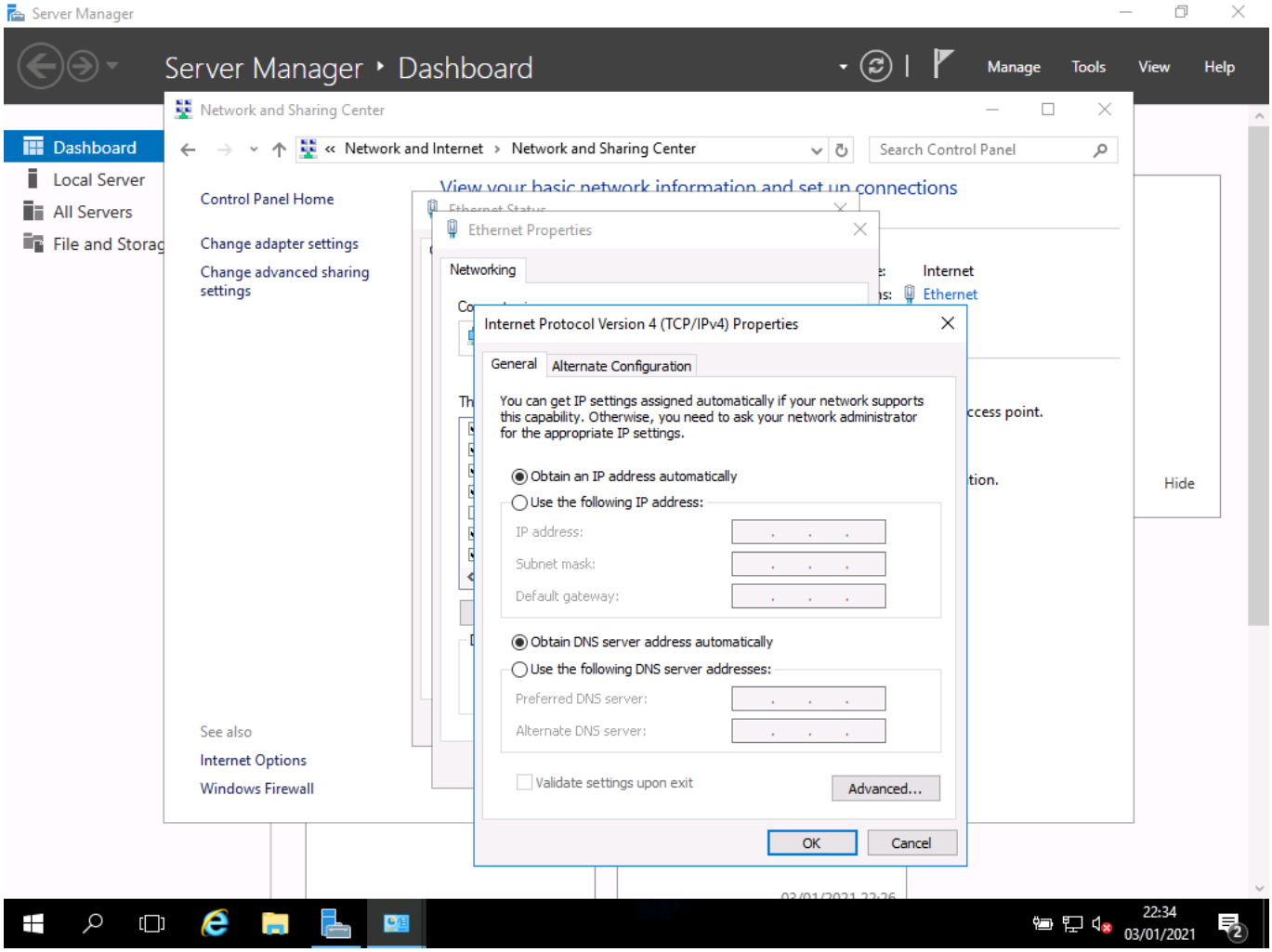
- using server manager, I access the network settings in order to set up connection to the network



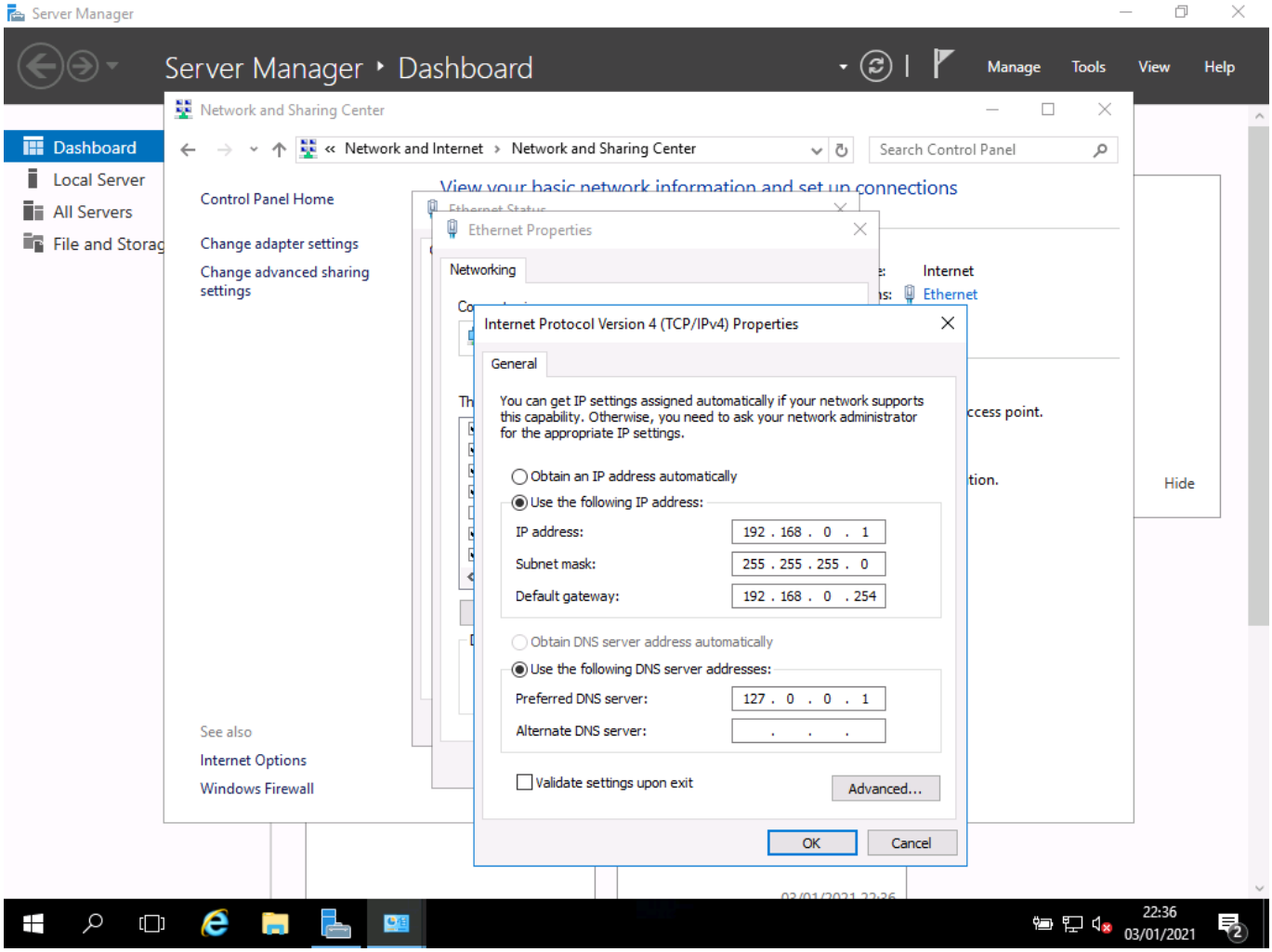
- I can now see the details for the network card in use



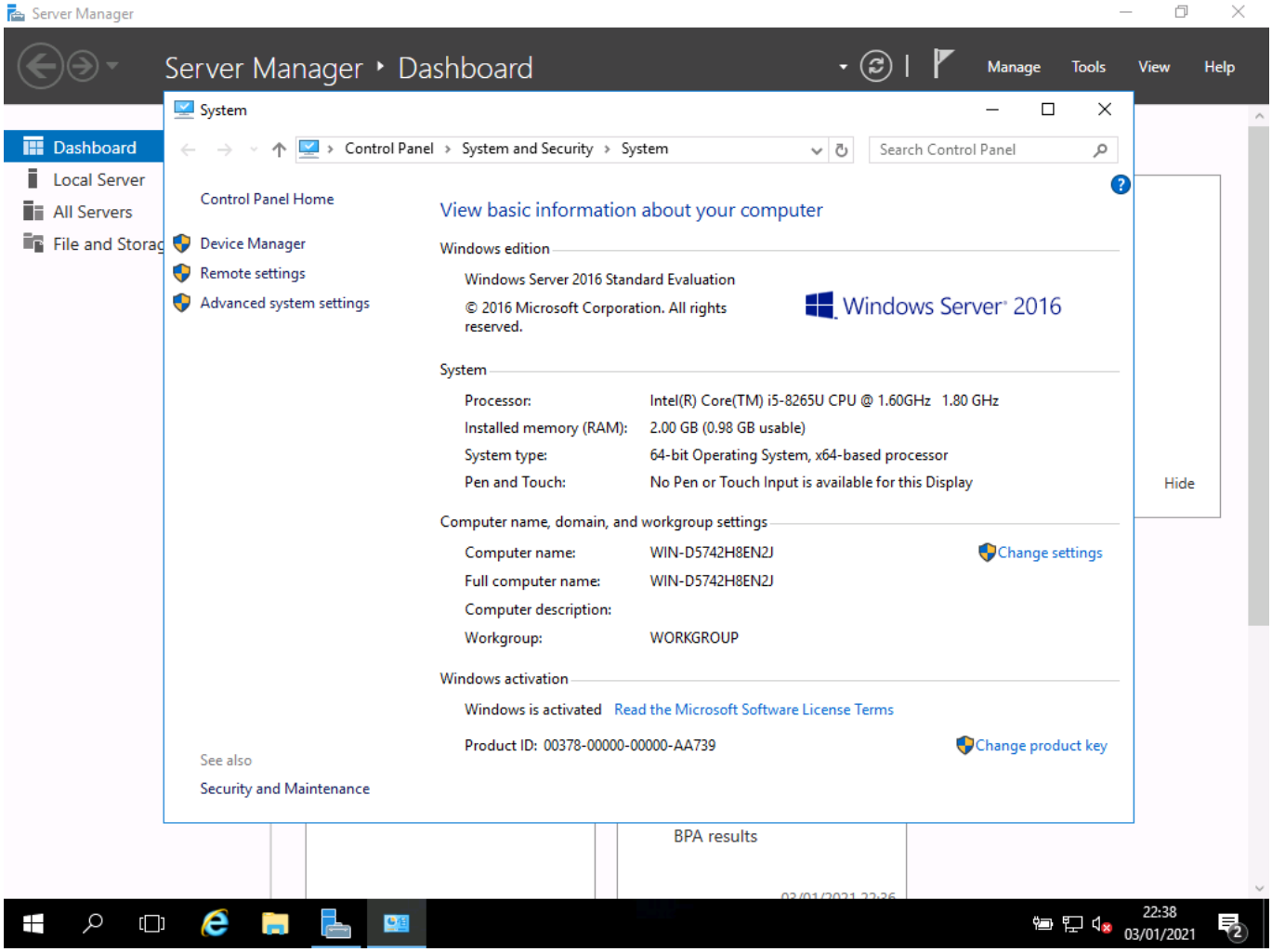
- I open the settings and select IP settings because I need to change the settings to a static (fixed) address



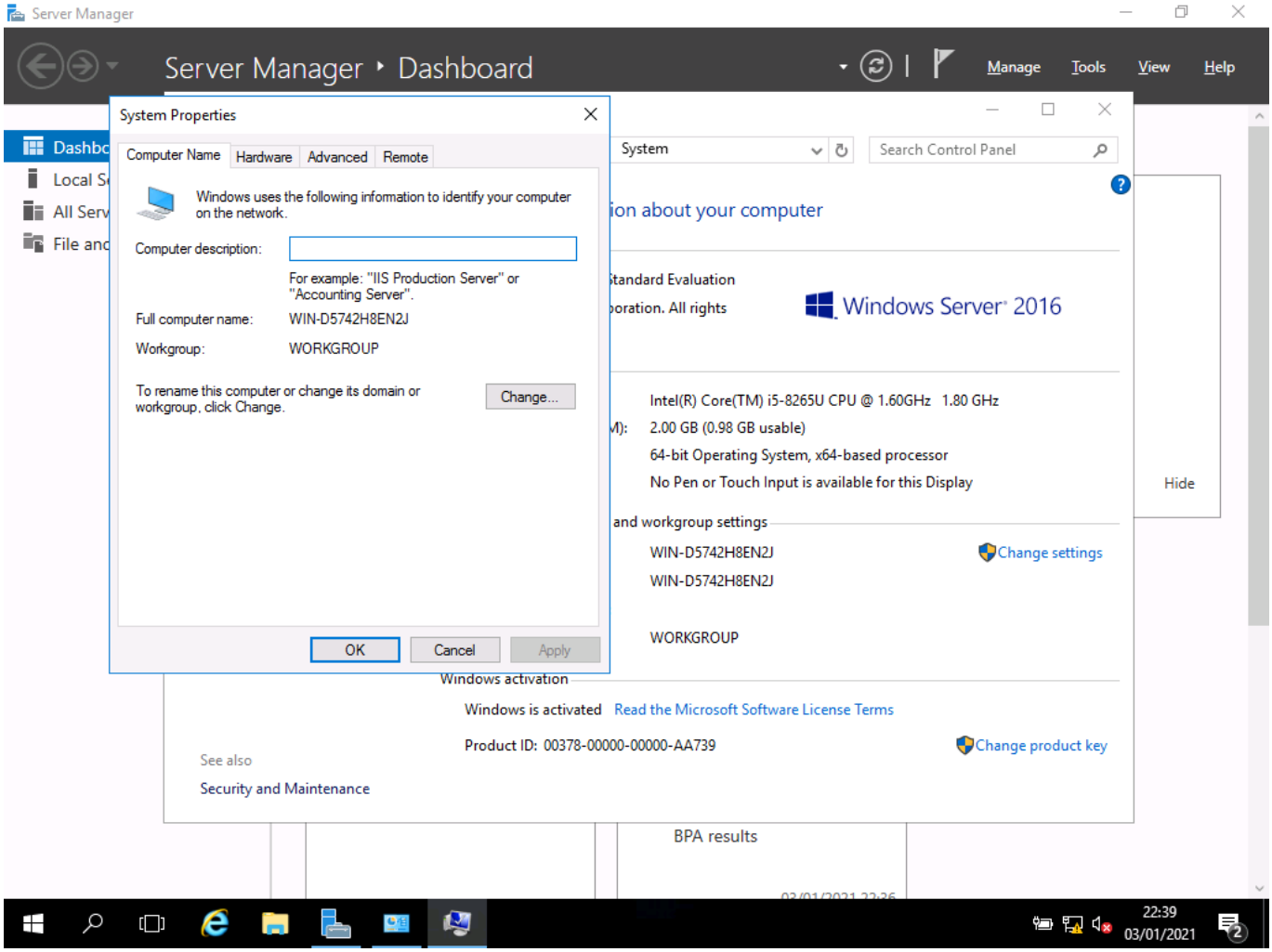
- it is currently set to use DHCP



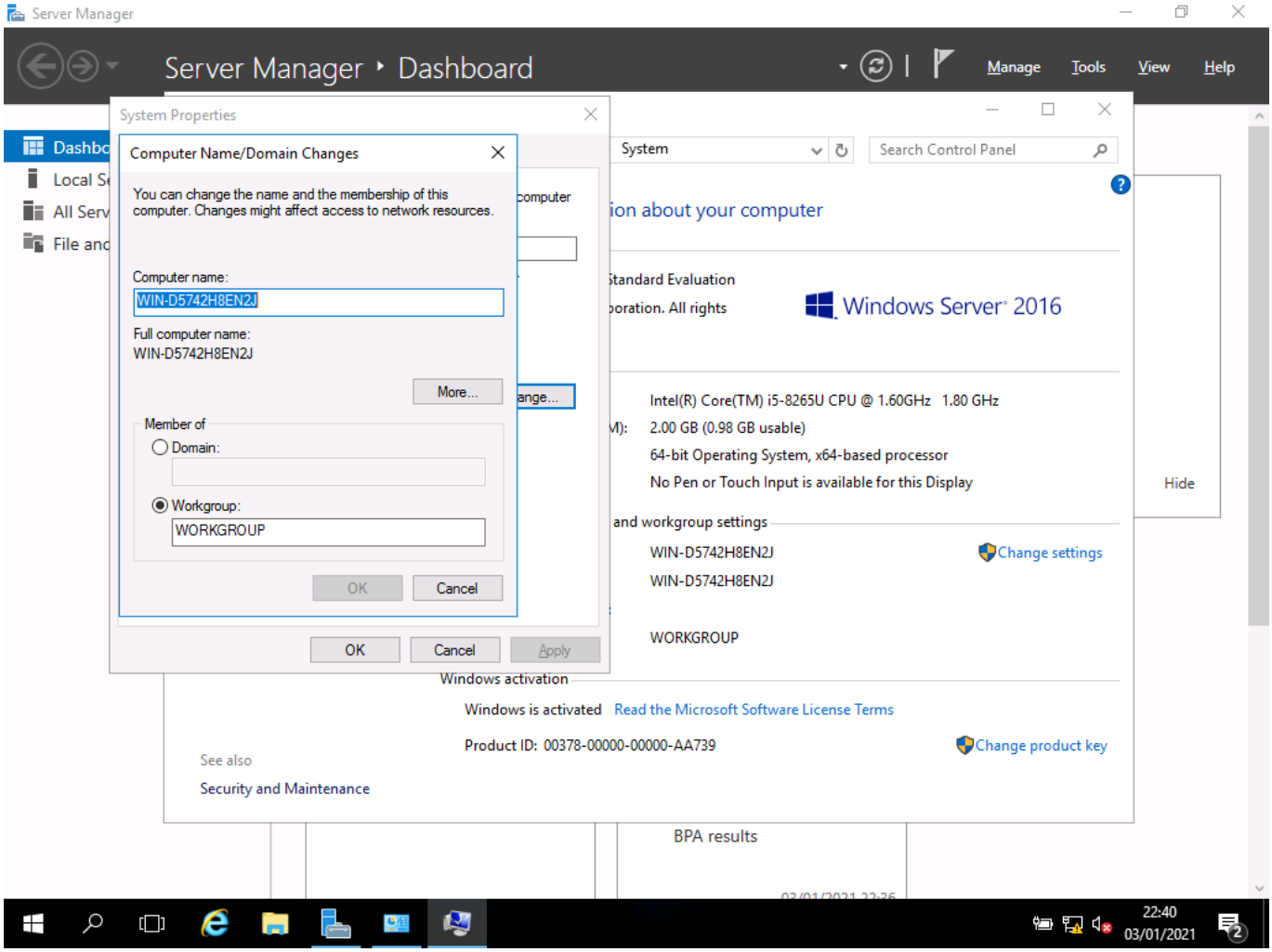
- I set to static and add the address details I wish to use
- I set the server with the IP address 192.168.0.1/Subnet Mask 255.255.255.0 in line with my network configuration plan



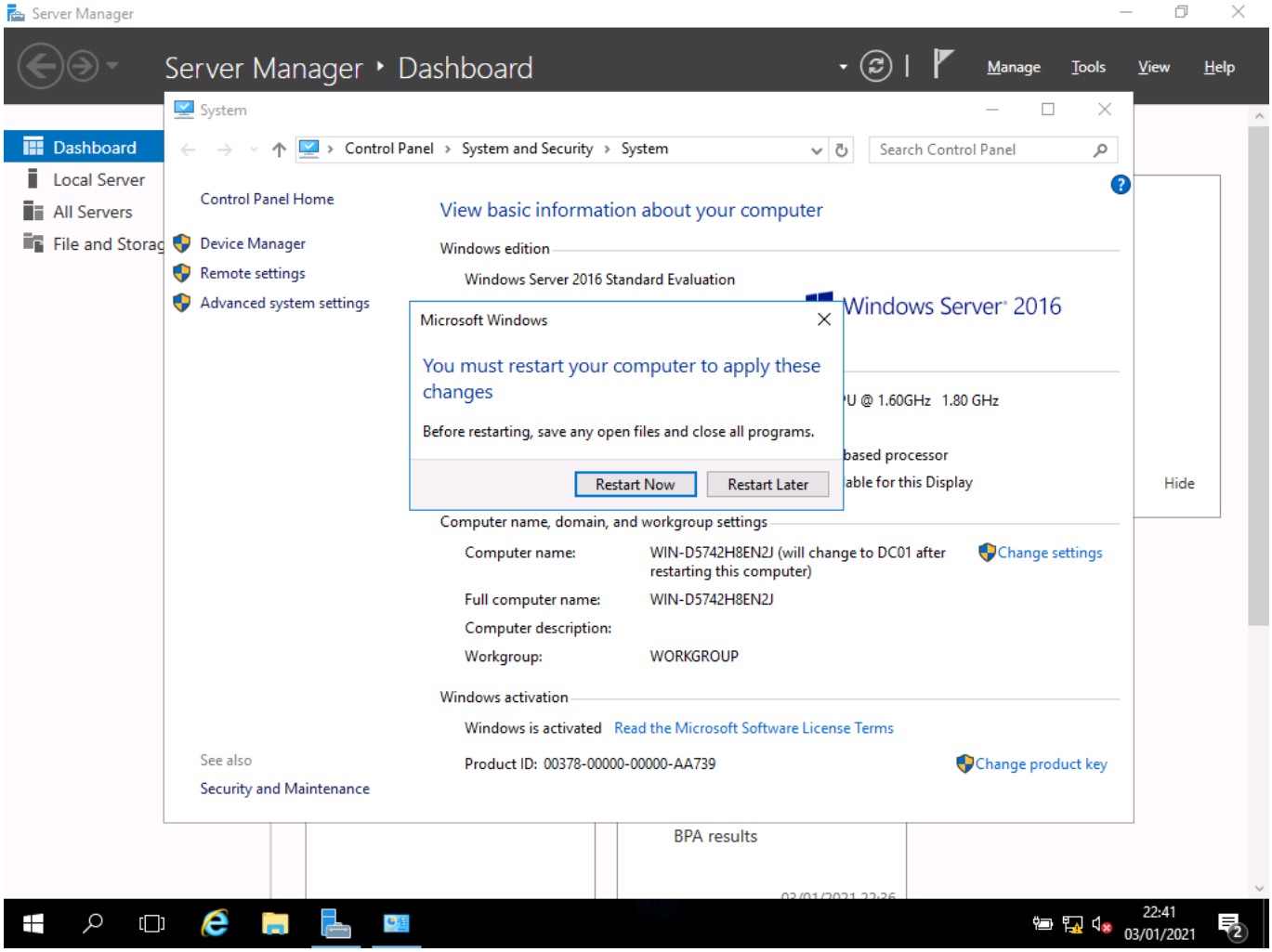
- having set the network, I open the server information window to see settings



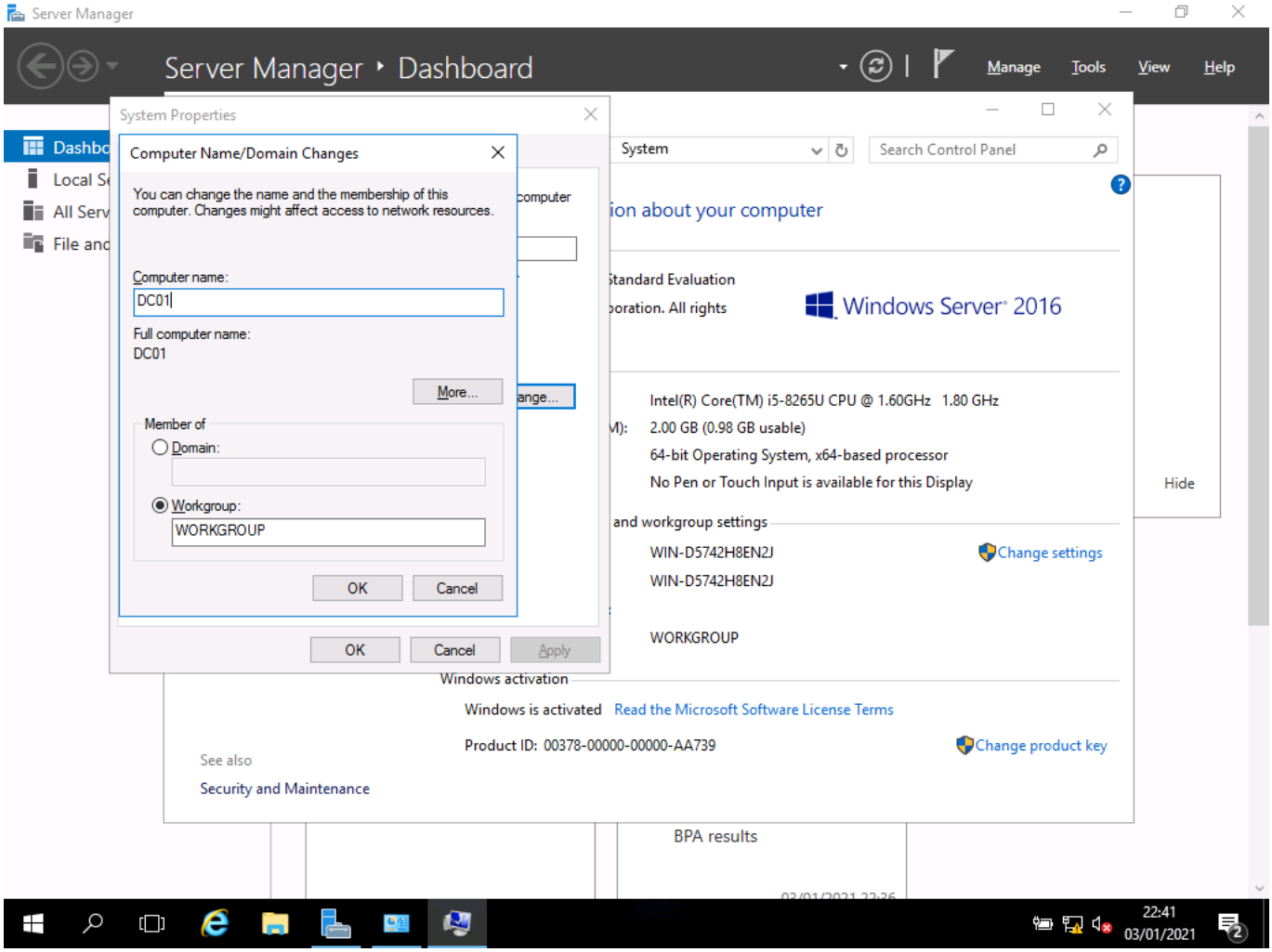
- I can now set the name of the machine so that it is easily recognised



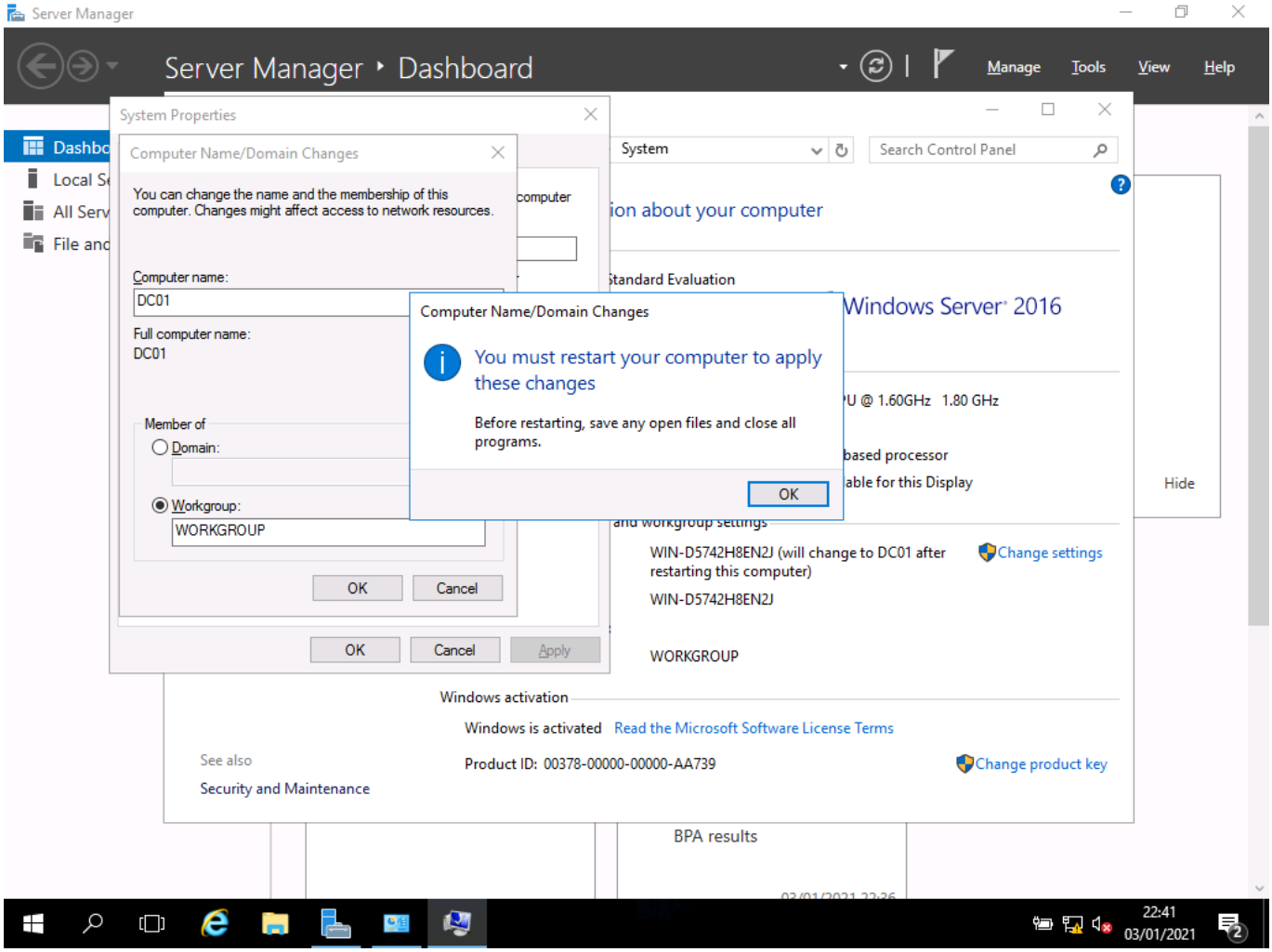
- here I add the name to use, WORKGROUP, so that it is easily recognised



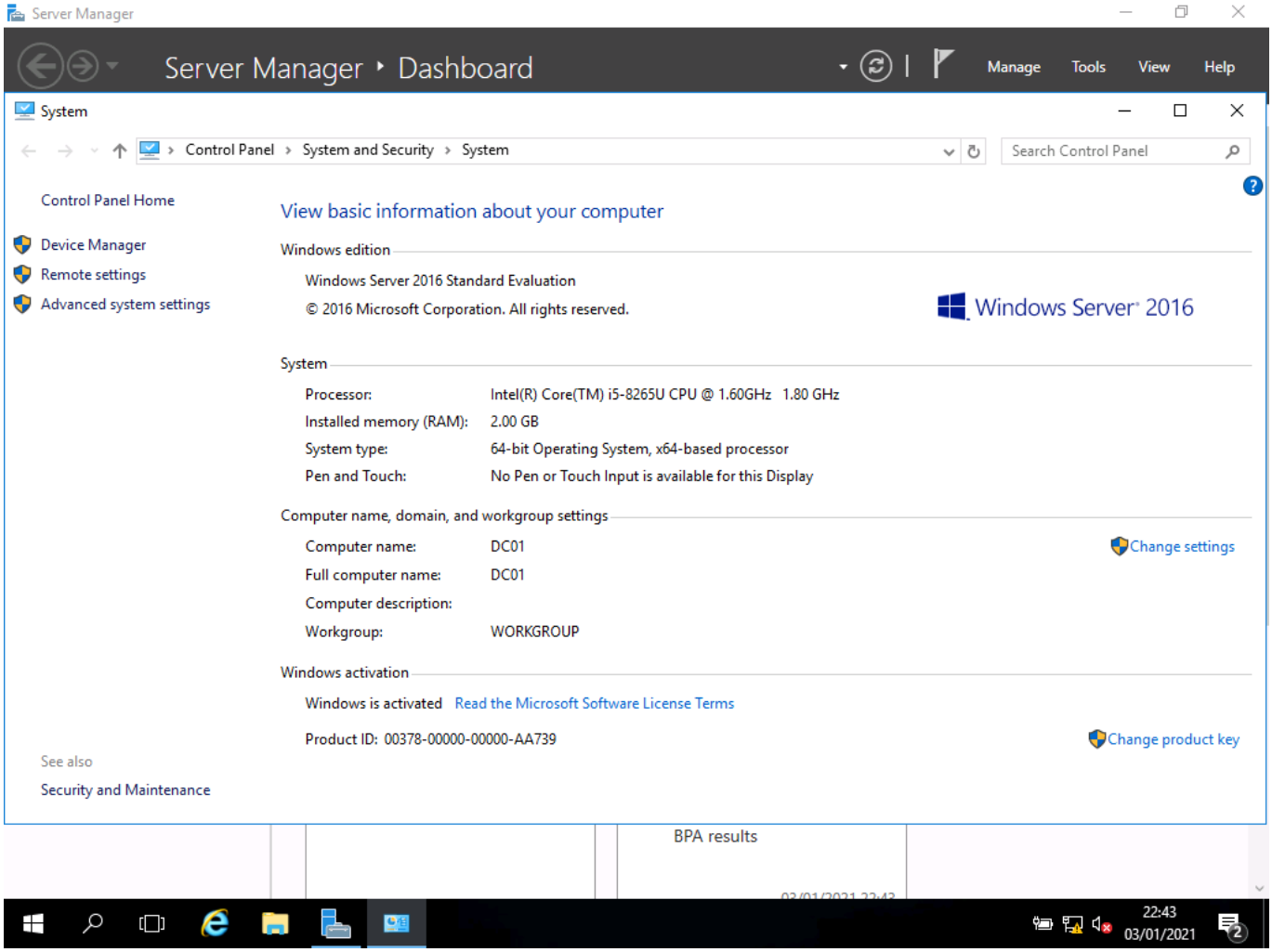
- the PC will need to restart to apply the name change



- once restarted, I return to the settings and now I set the domain



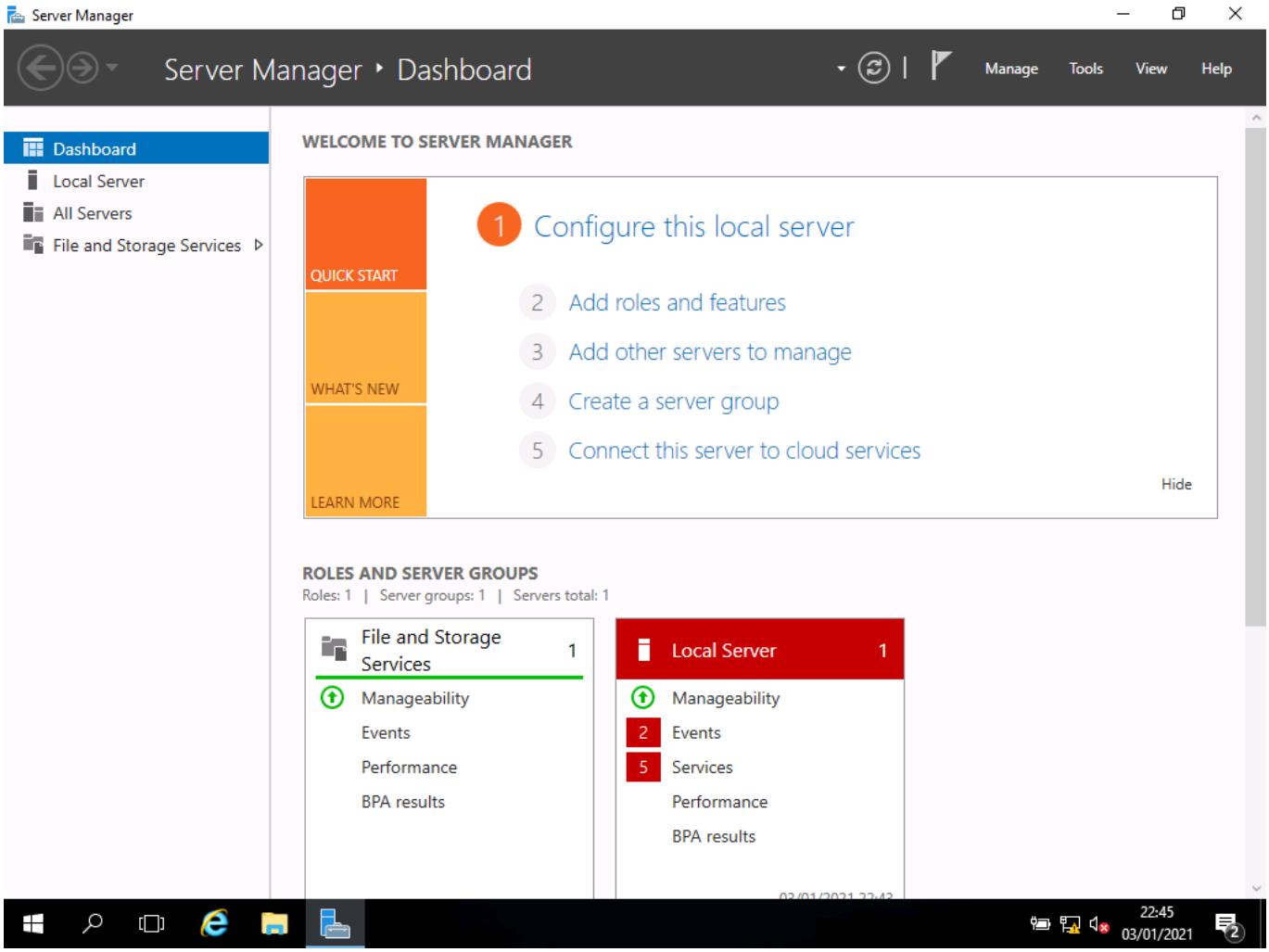
- again, a restart is required to complete this change



- after that restart, I can confirm the name and domain are now set

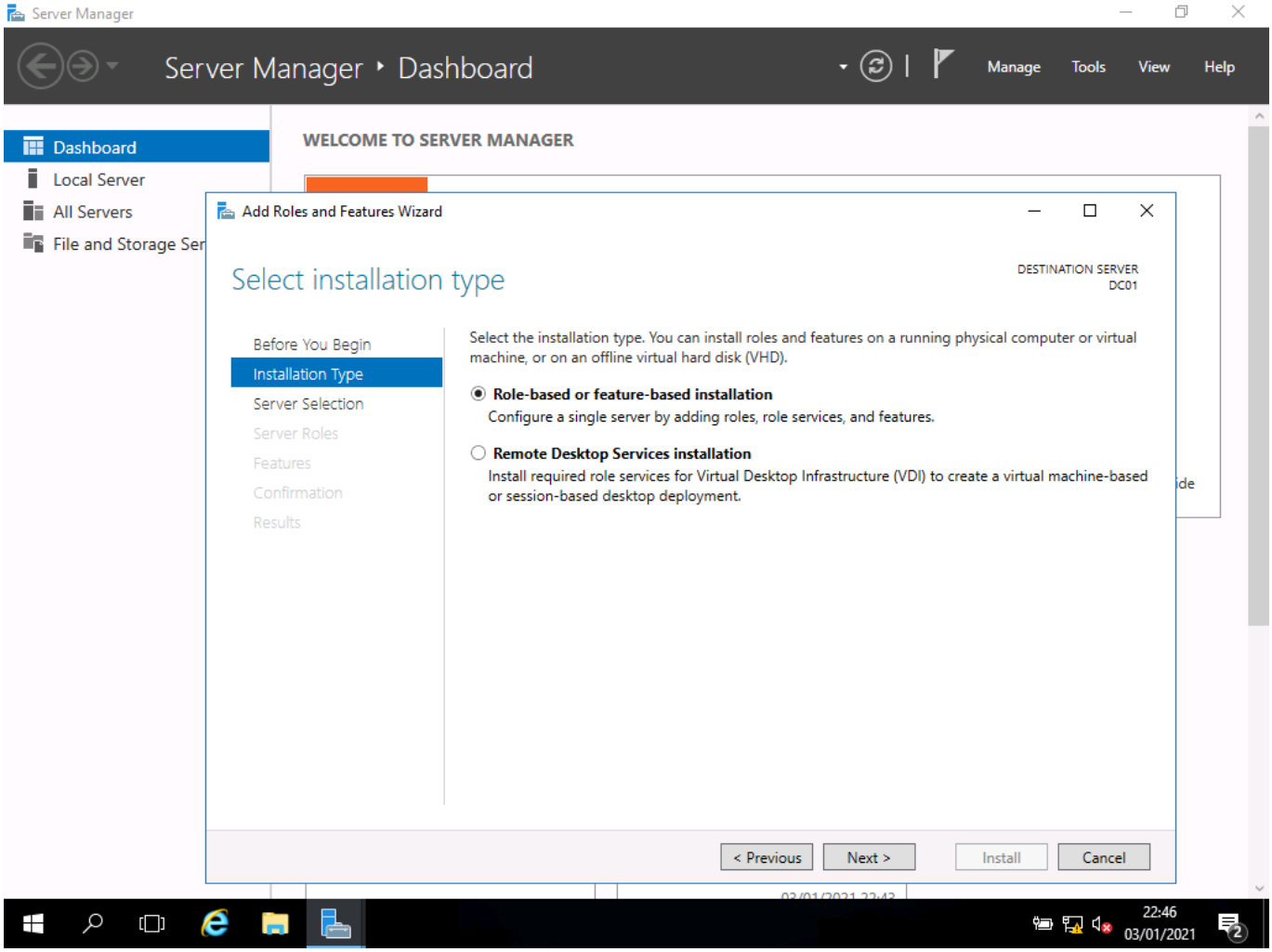
Allocating server roles

Screenshot:



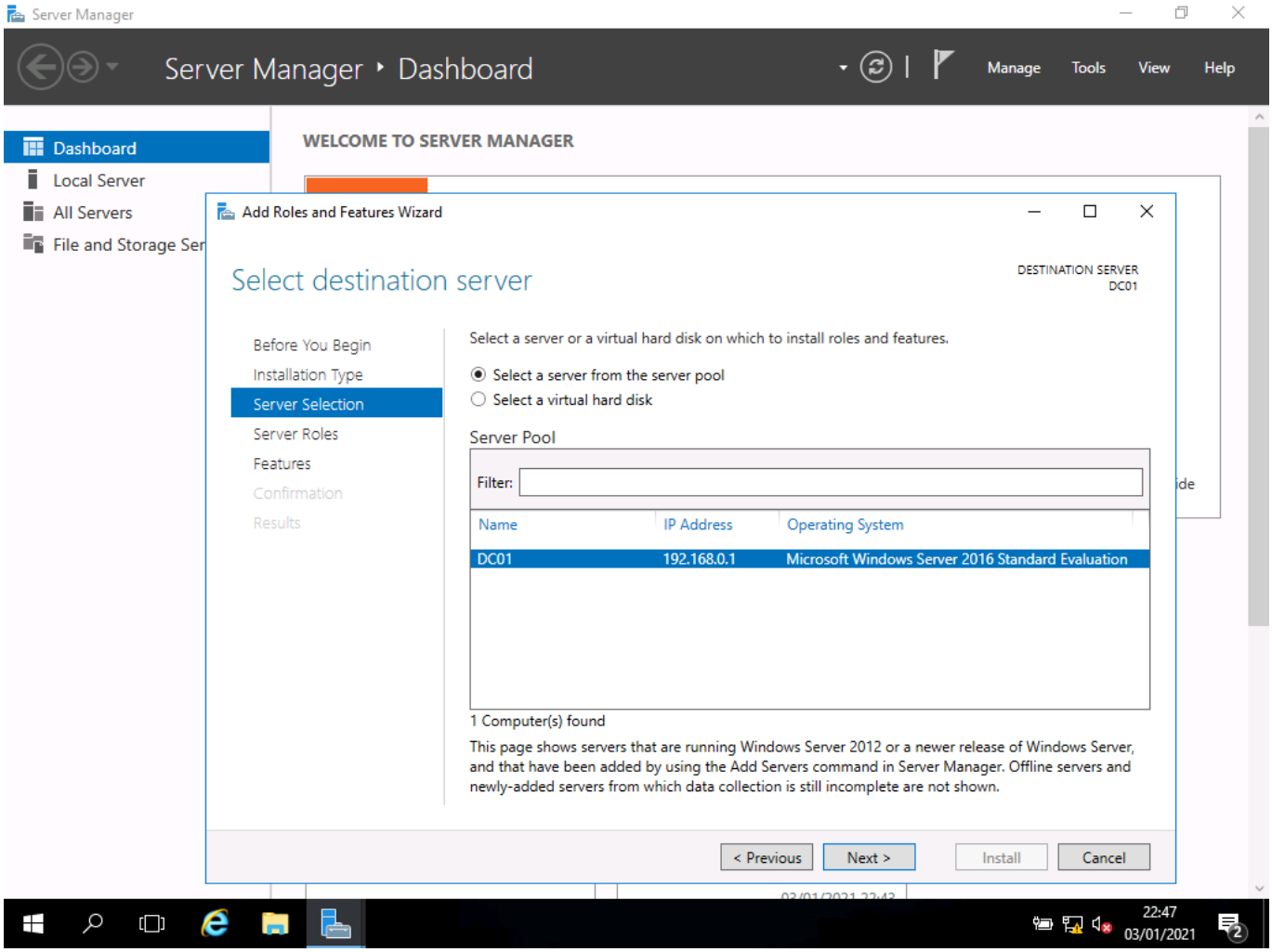
- here I have opened the server dashboard so I can start the process of allocating server roles and installing active directory - on this screen, I will select roles and features

Screenshot:



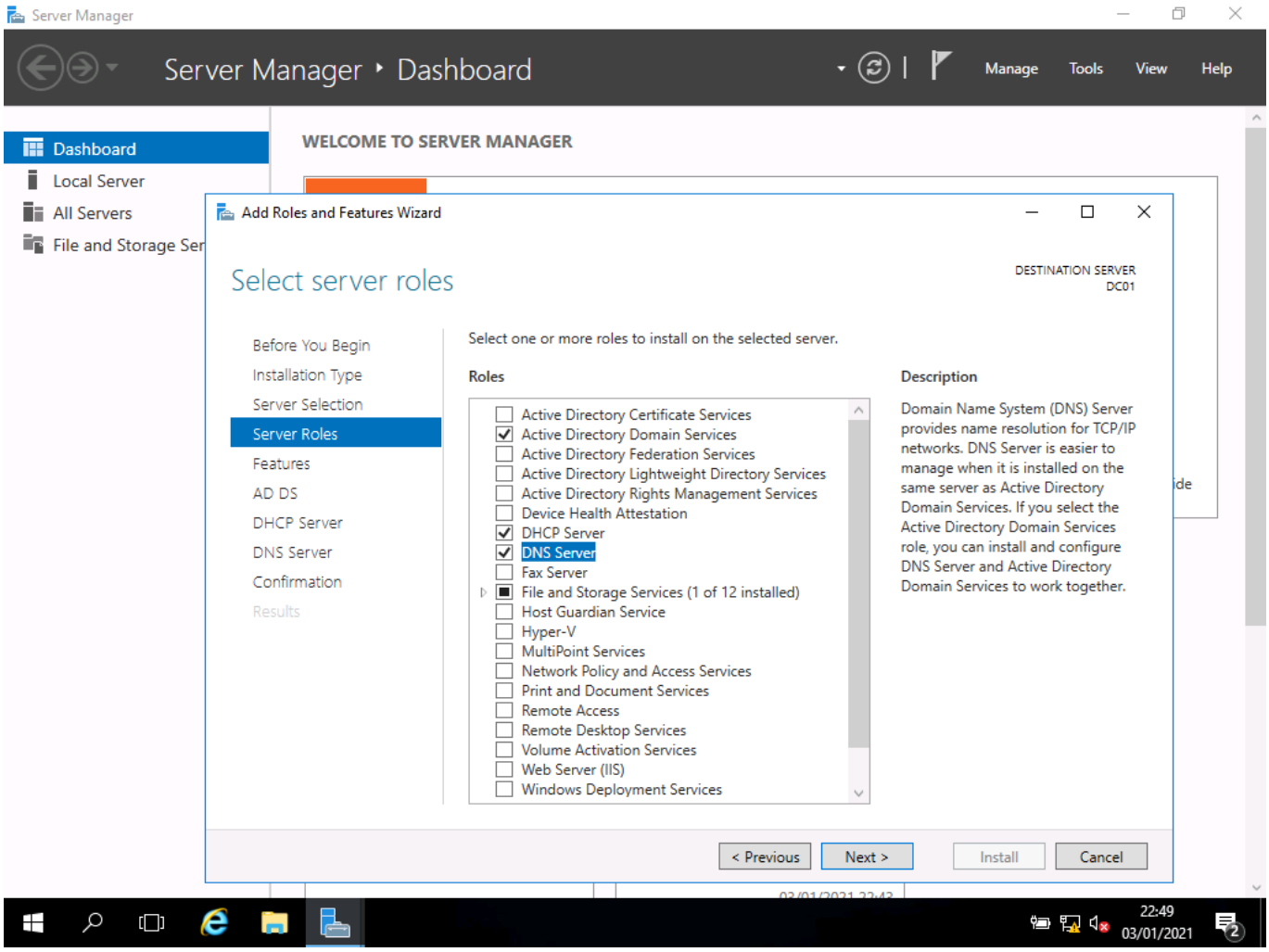
- I am selecting role-based installation as this is the simplest way to install the features as it uses a wizard

Screenshot:

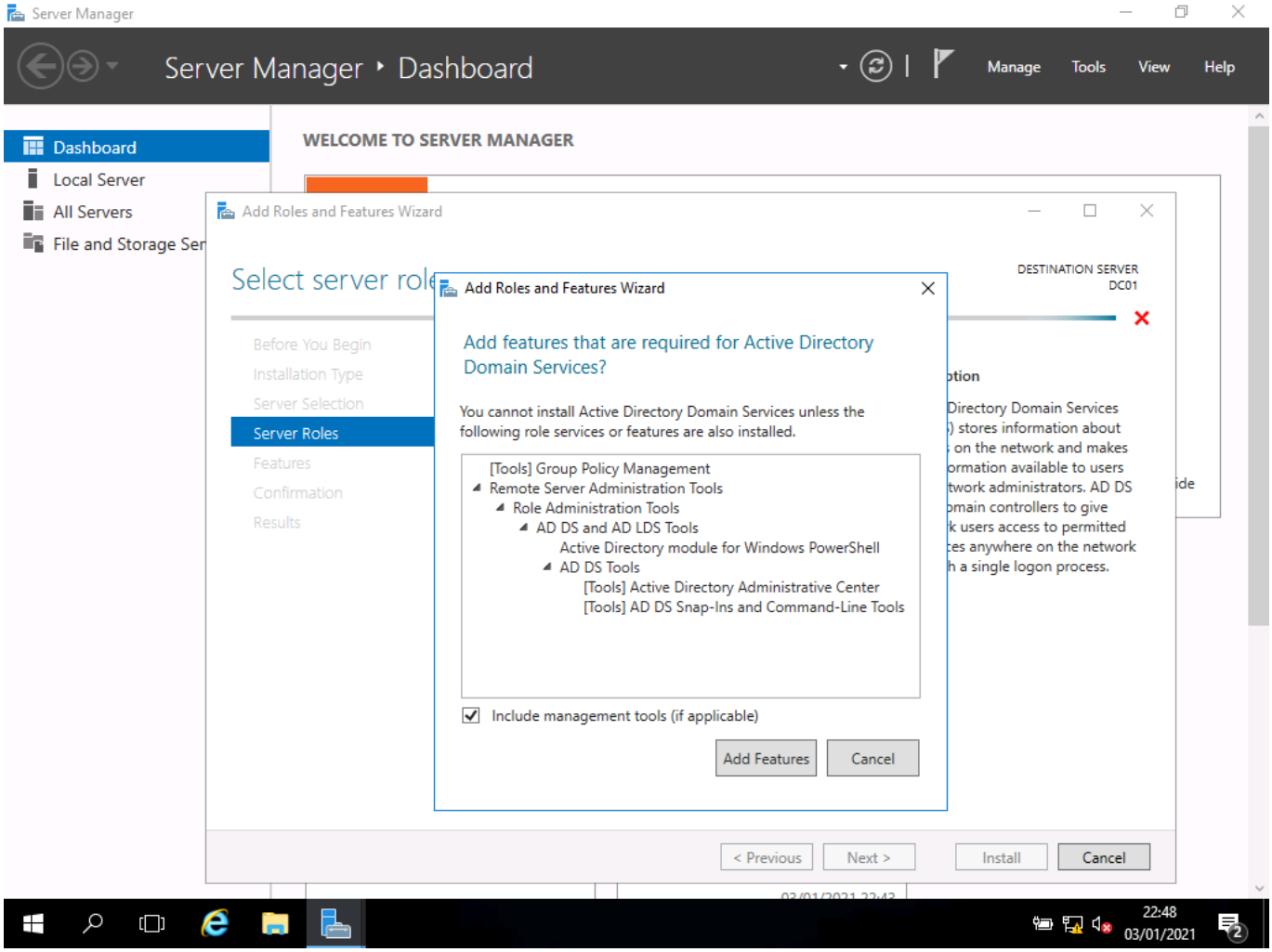


- I am selecting my server here (DC01); server manager allows 1 PC to control several servers if it is set up to do so

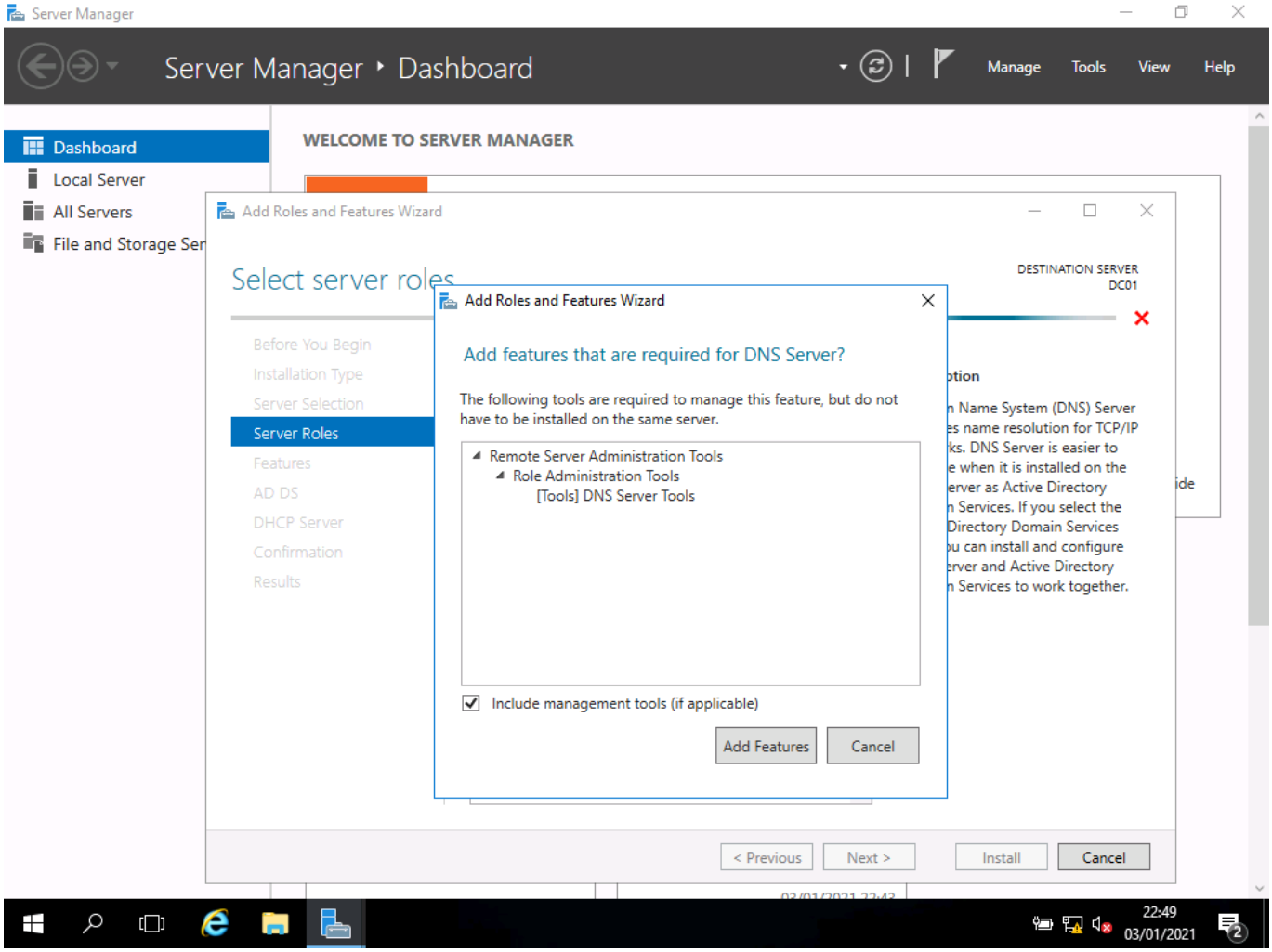
Screenshot:



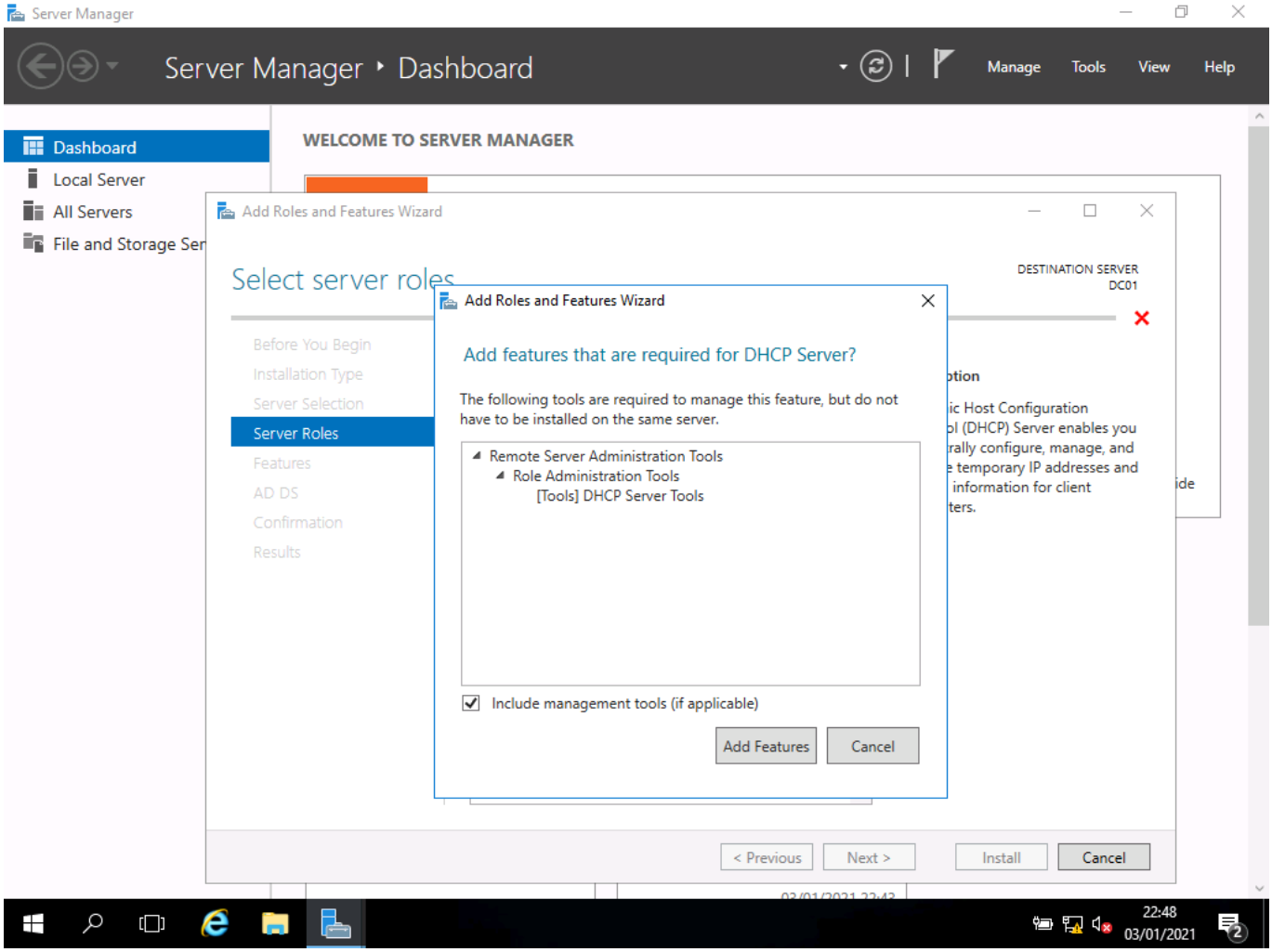
- I select the roles I want to add: AD, DHCP and DNS



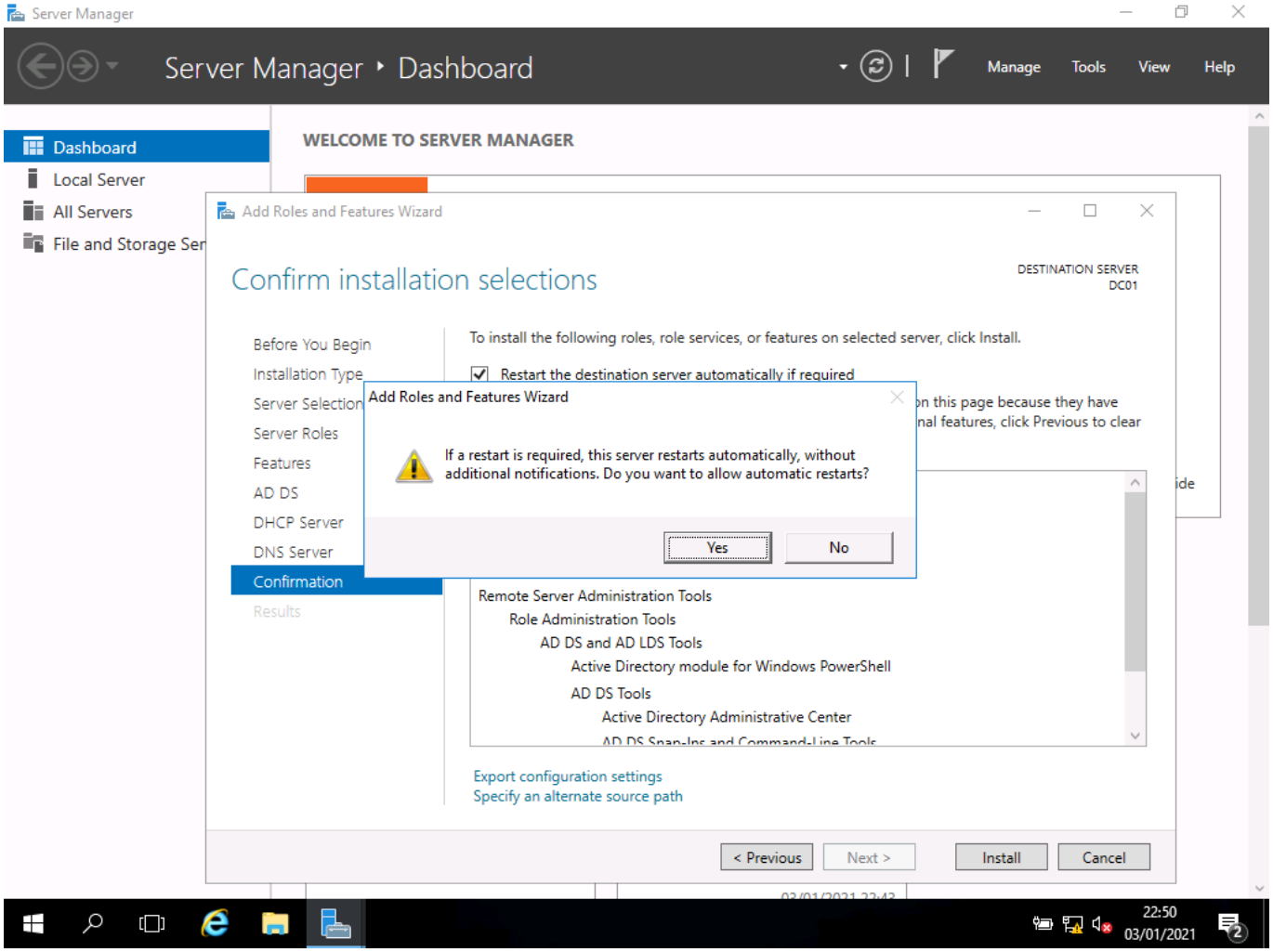
- I add the additional features needed for AD



- I add the additional features needed for DNS; these are selected automatically when you use this wizard

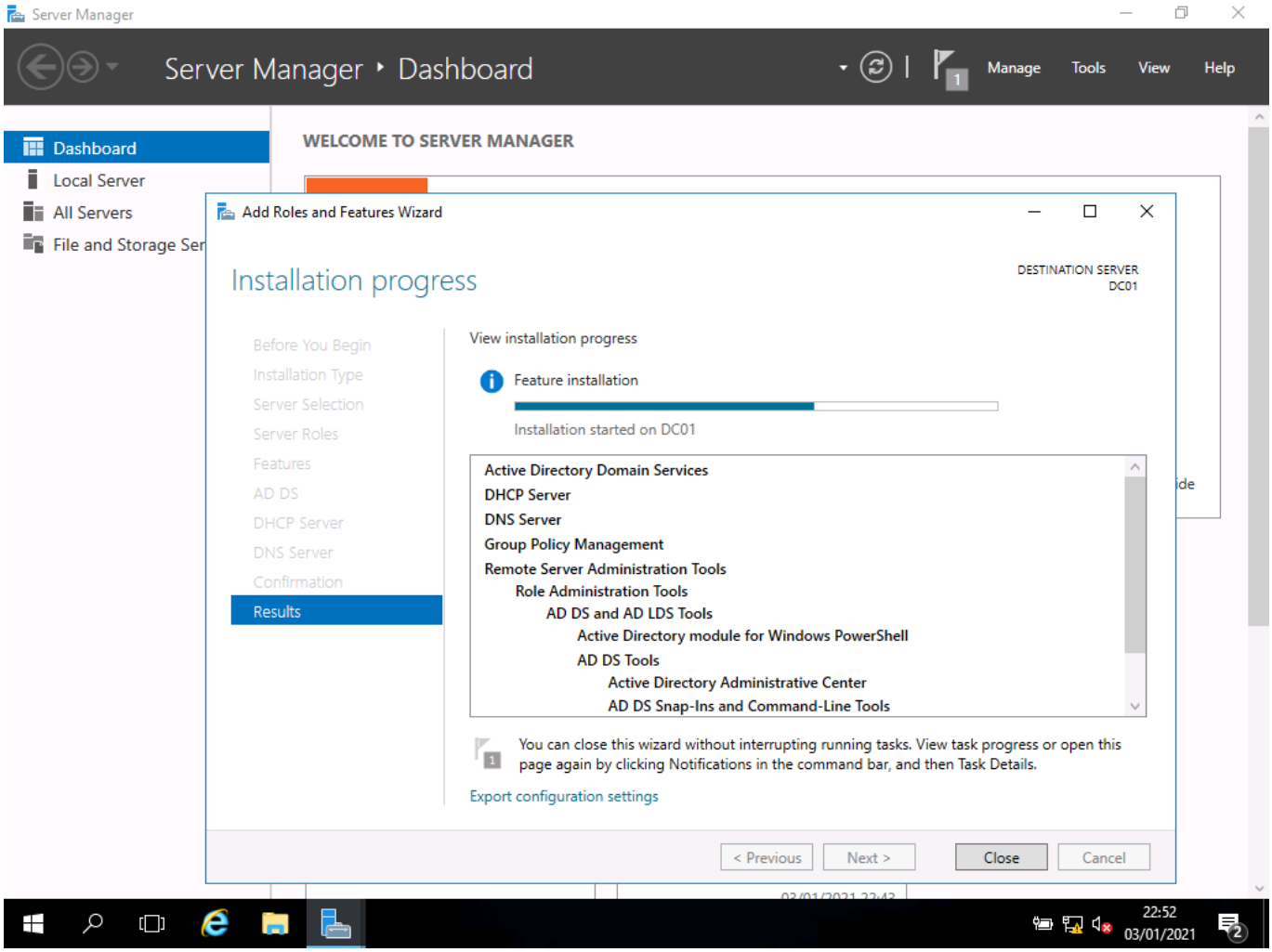


- I add the additional features needed for DHCP

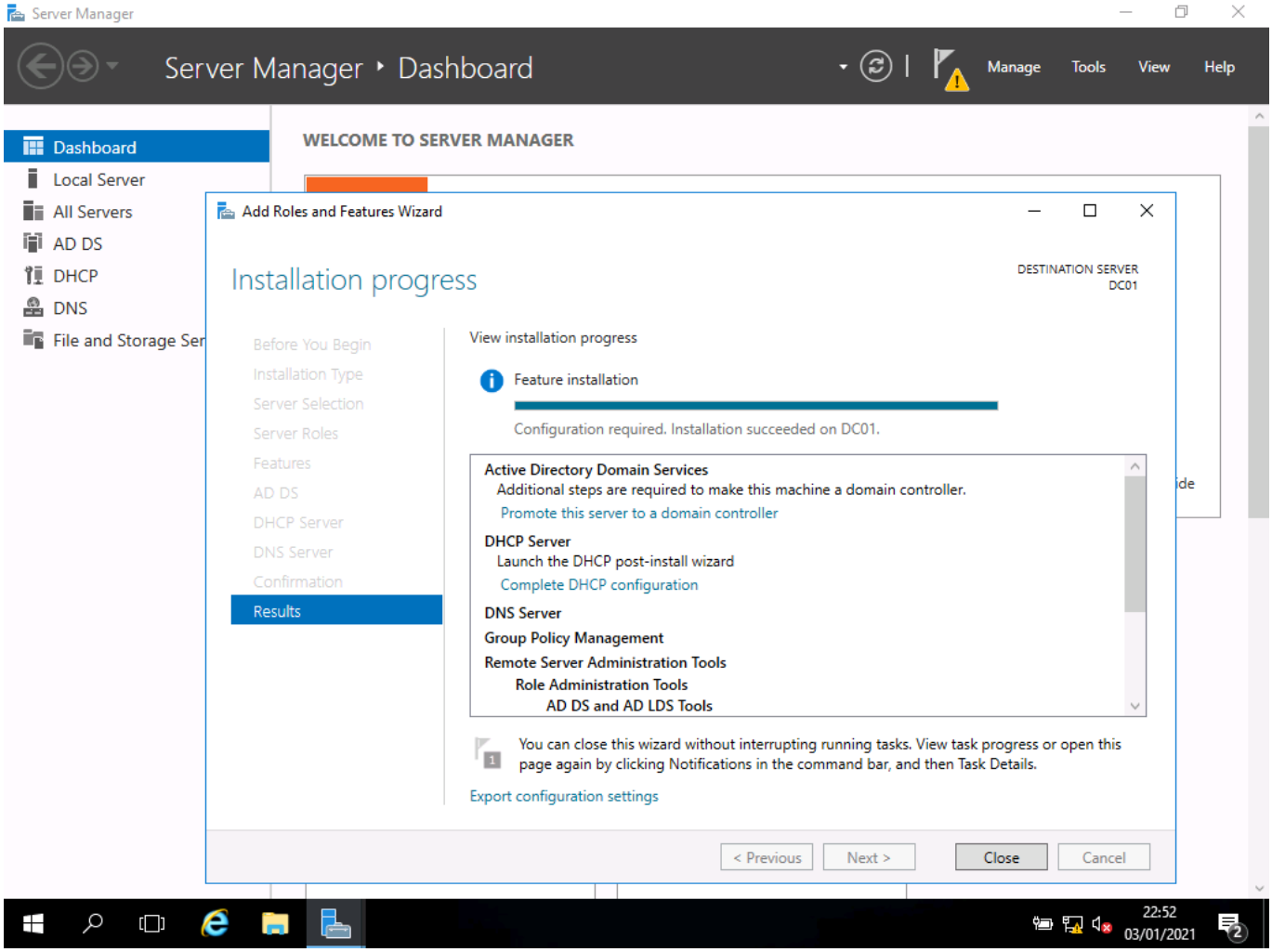


- I accept the automatic restarts; this speeds up the process

Screenshot:



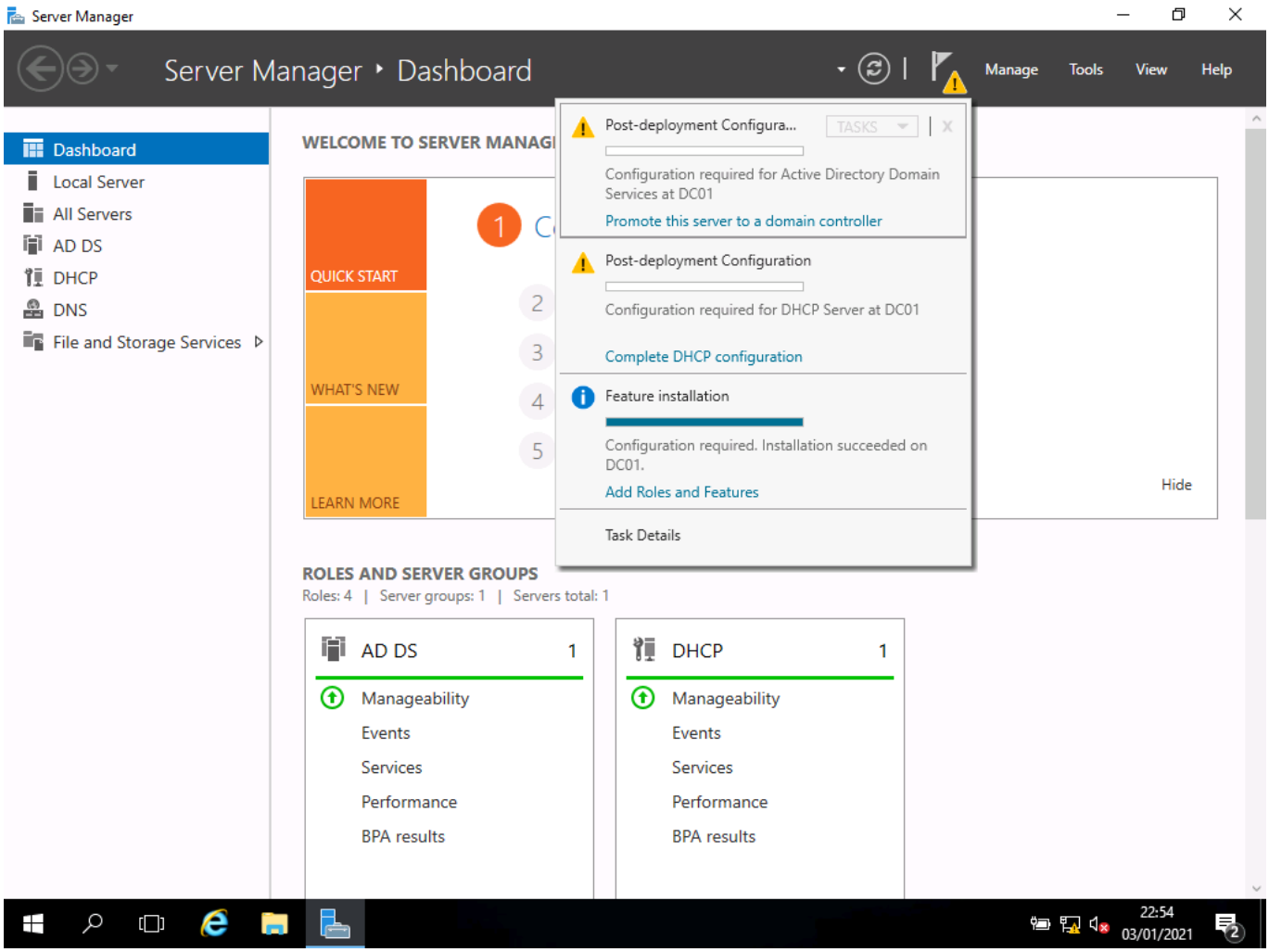
- the features install and the server restarts as needed



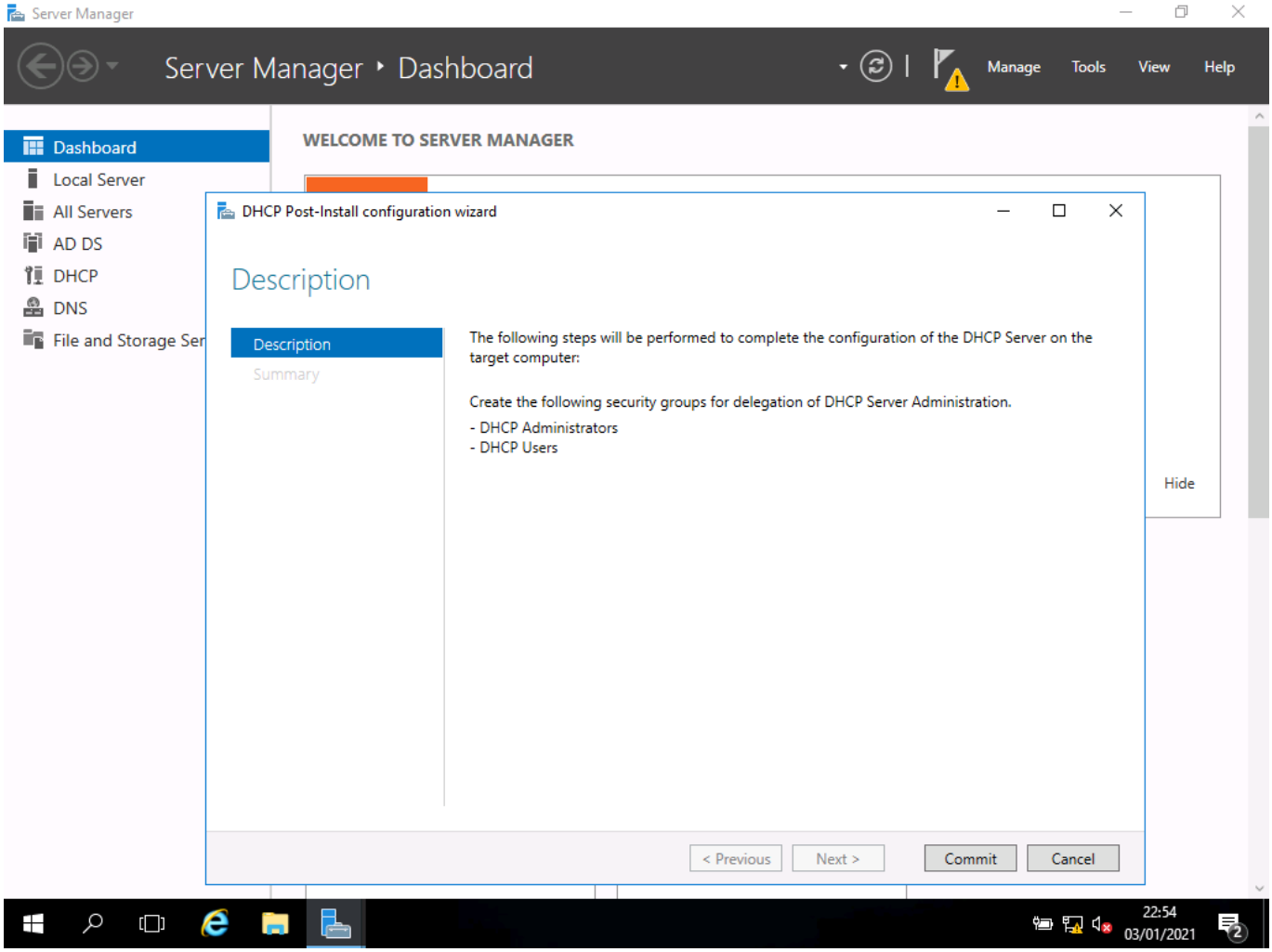
- this screenshot shows the server roles installing without error

Setting up DHCP

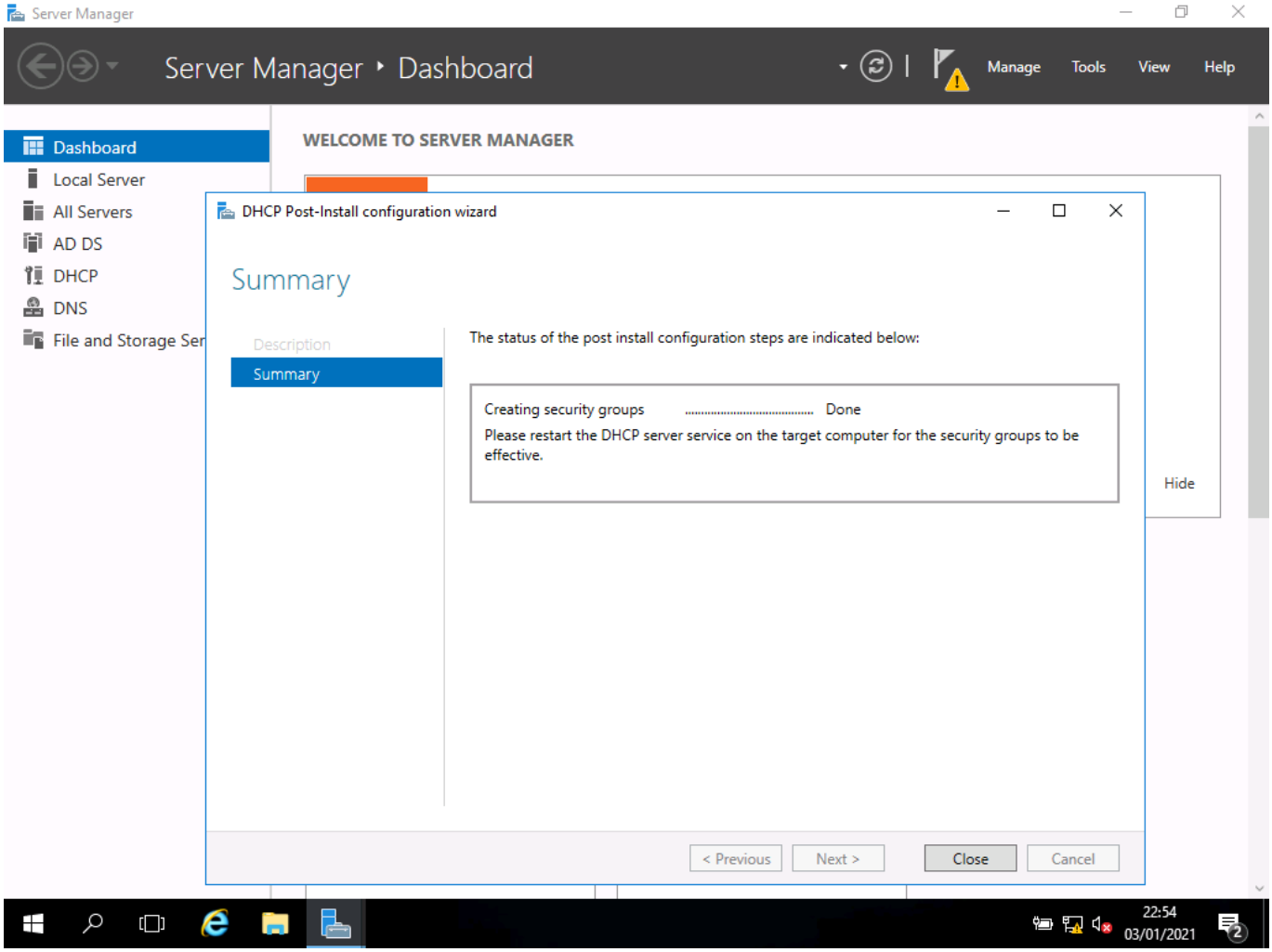
Screenshot:



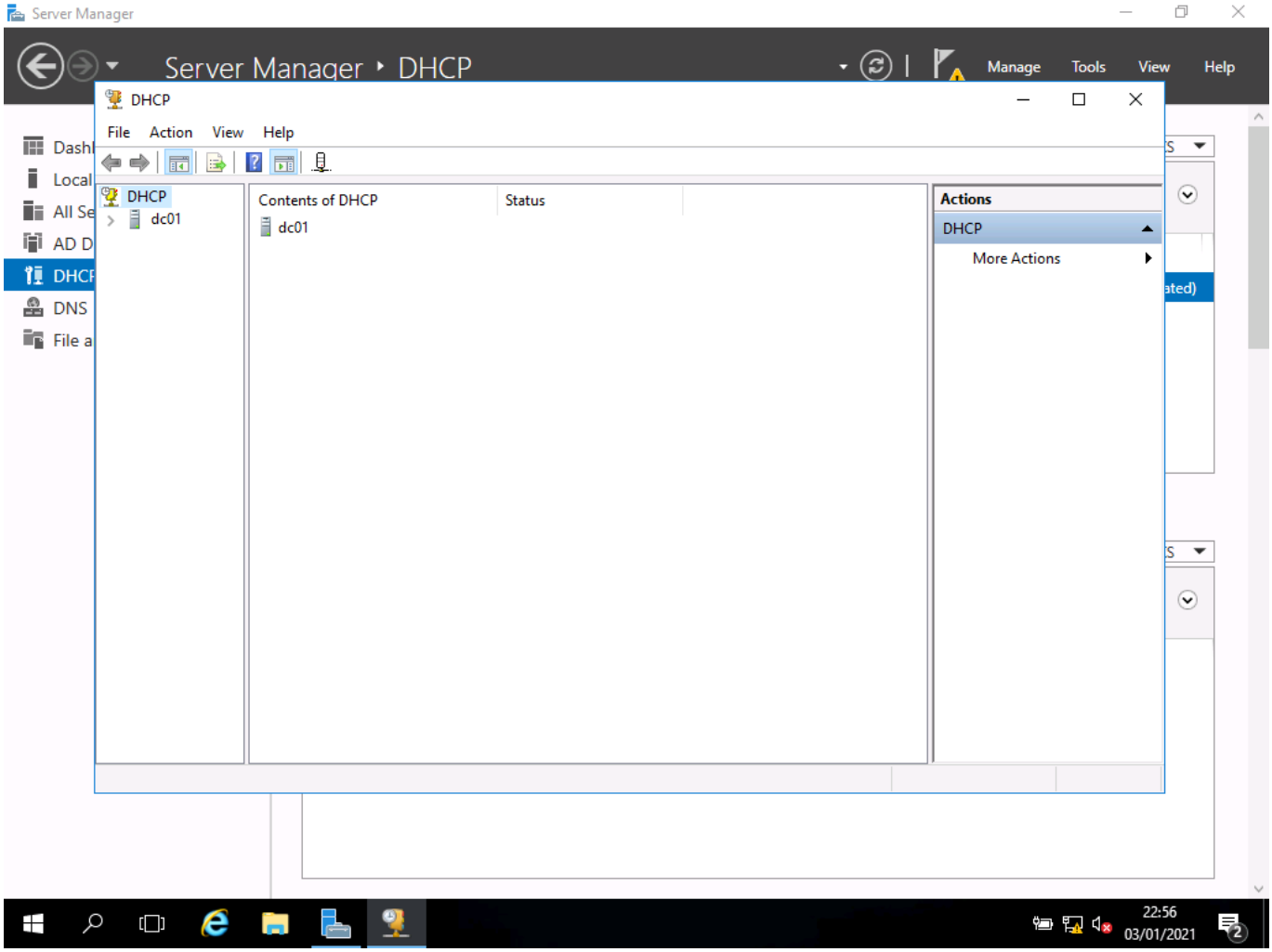
- now we can see there is configuration needed for DHCP and DNS
- at the top of the server manager window, I click on the yellow symbol and select complete DHCP configuration and then complete the wizard using the default settings as they are the ones I want to use



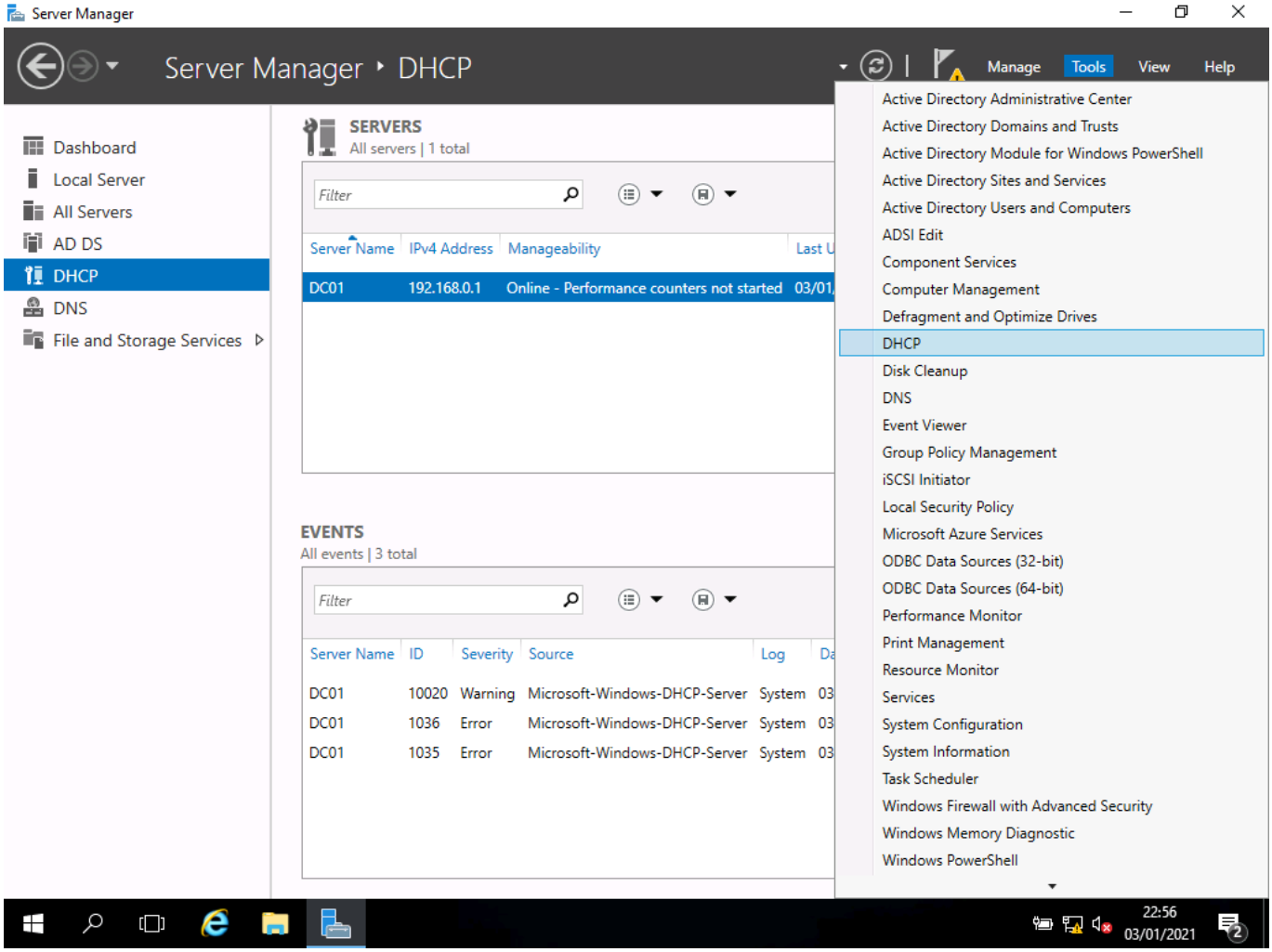
- I follow the wizard



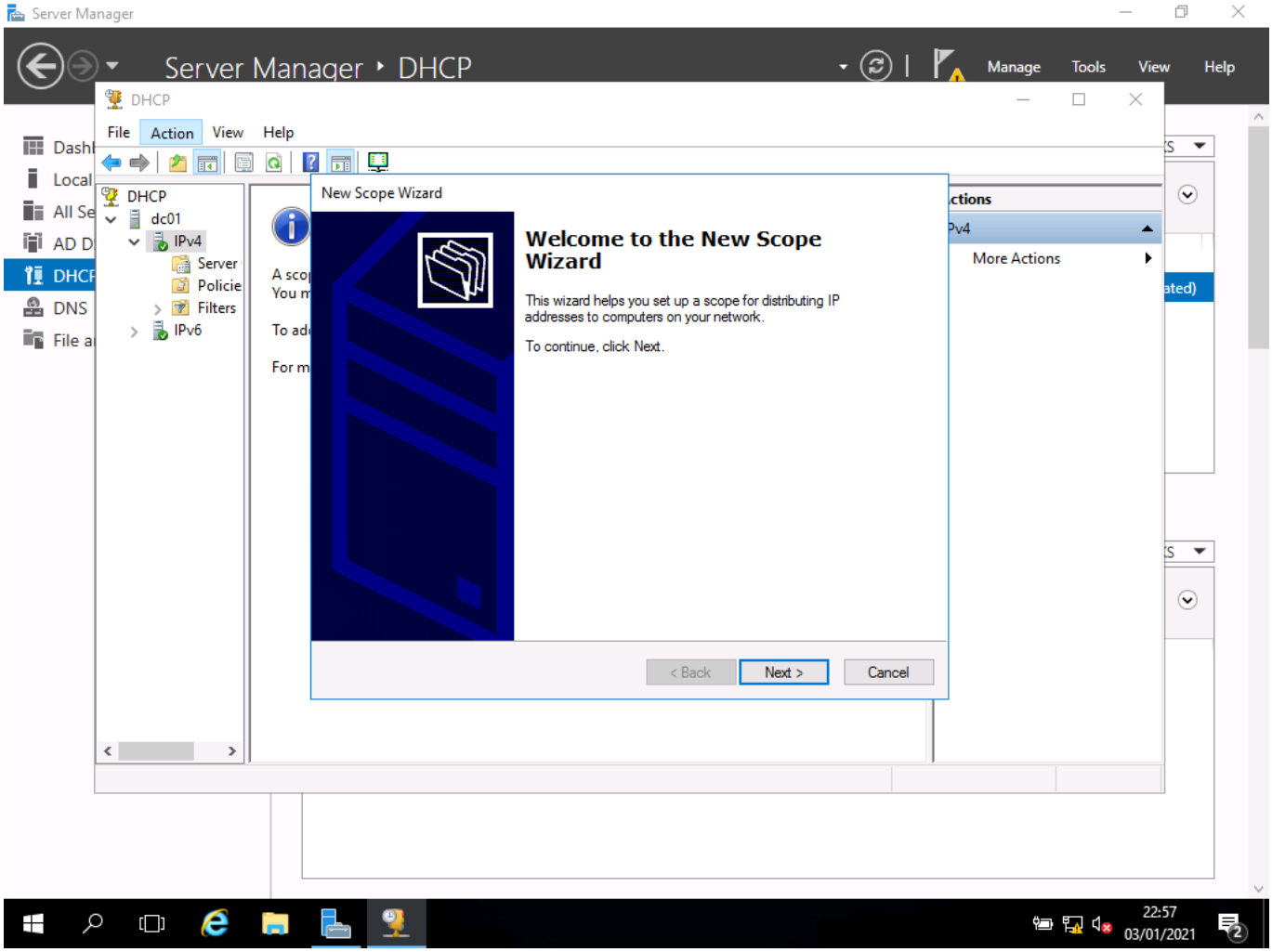
- once configured, the DHCP needs to be restarted so that the scope can be configured



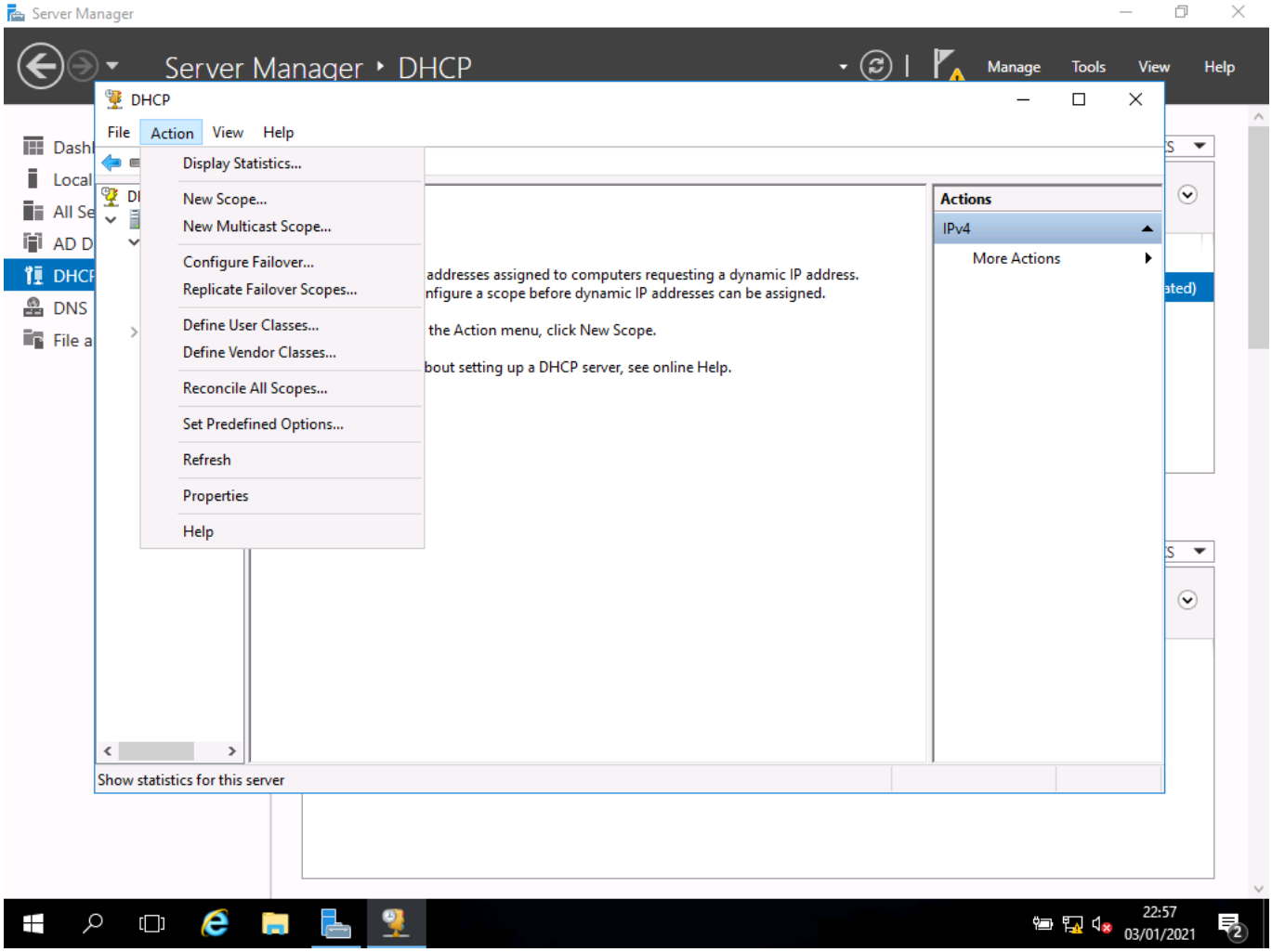
- here you can see that the server dc01 is shown in the DHCP table, this is because it is the DHCP server



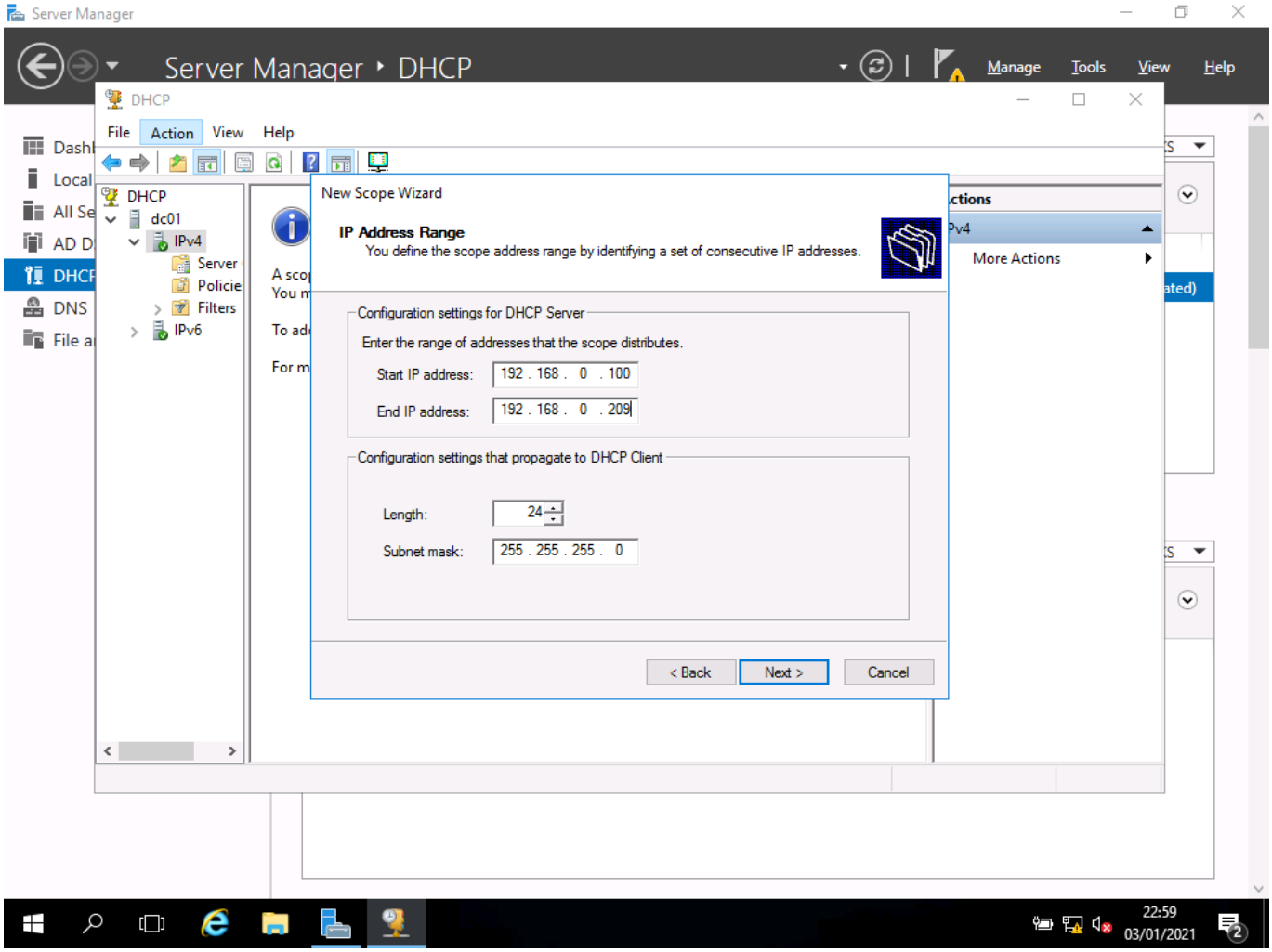
- from tools, I select DHCP to open the next wizard



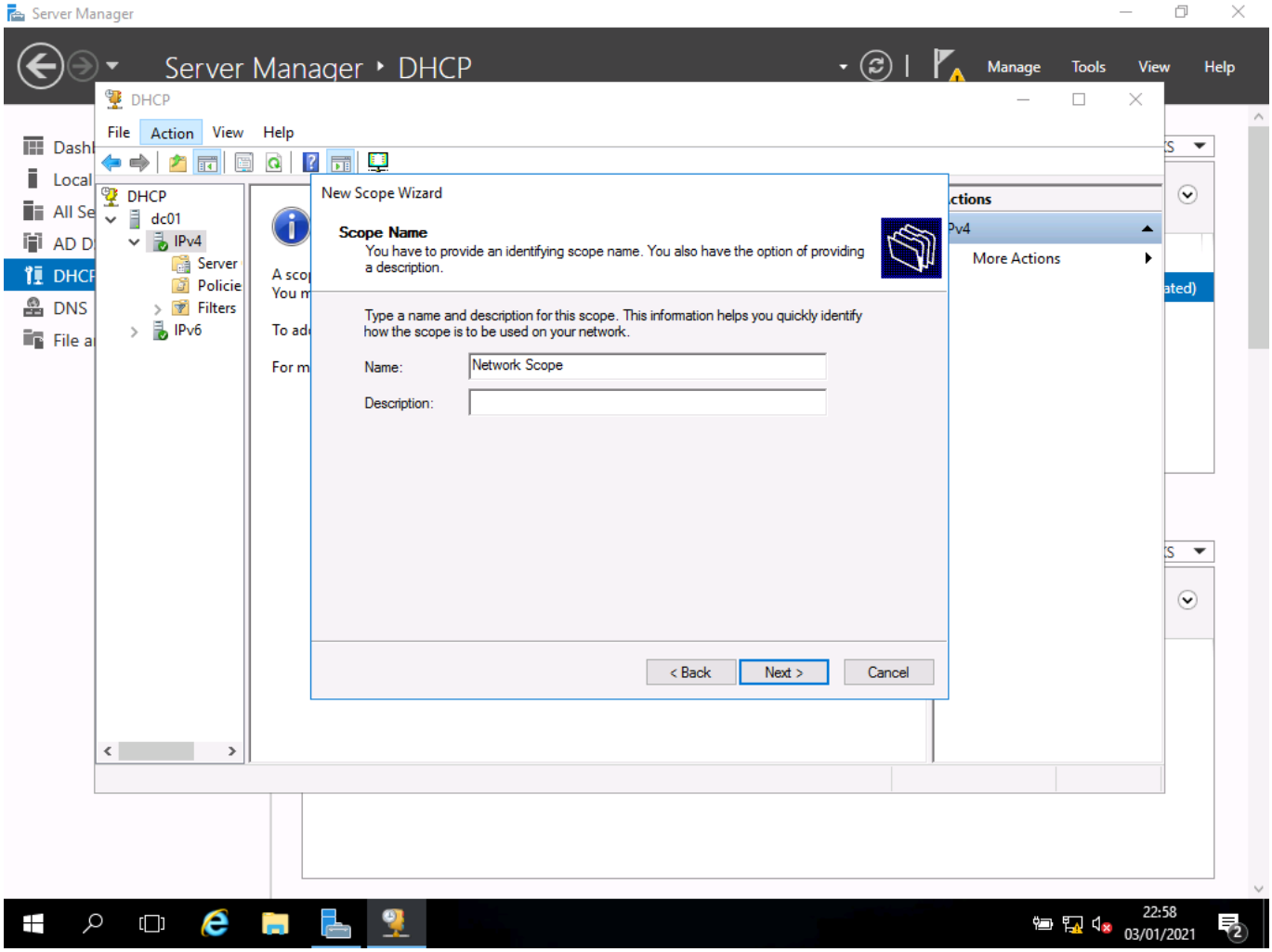
- when the new scope wizard opens I click next to begin



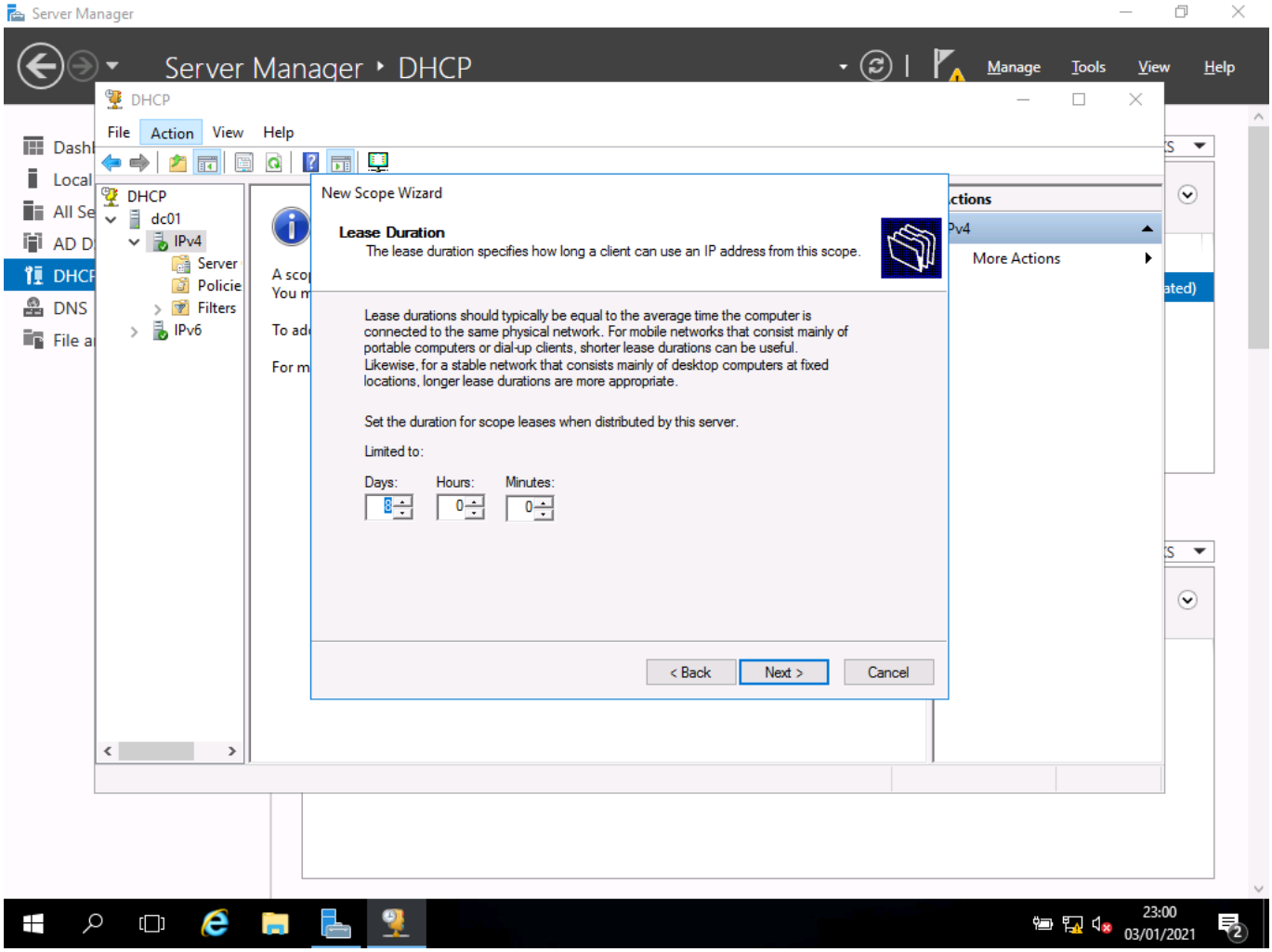
- I start the wizard



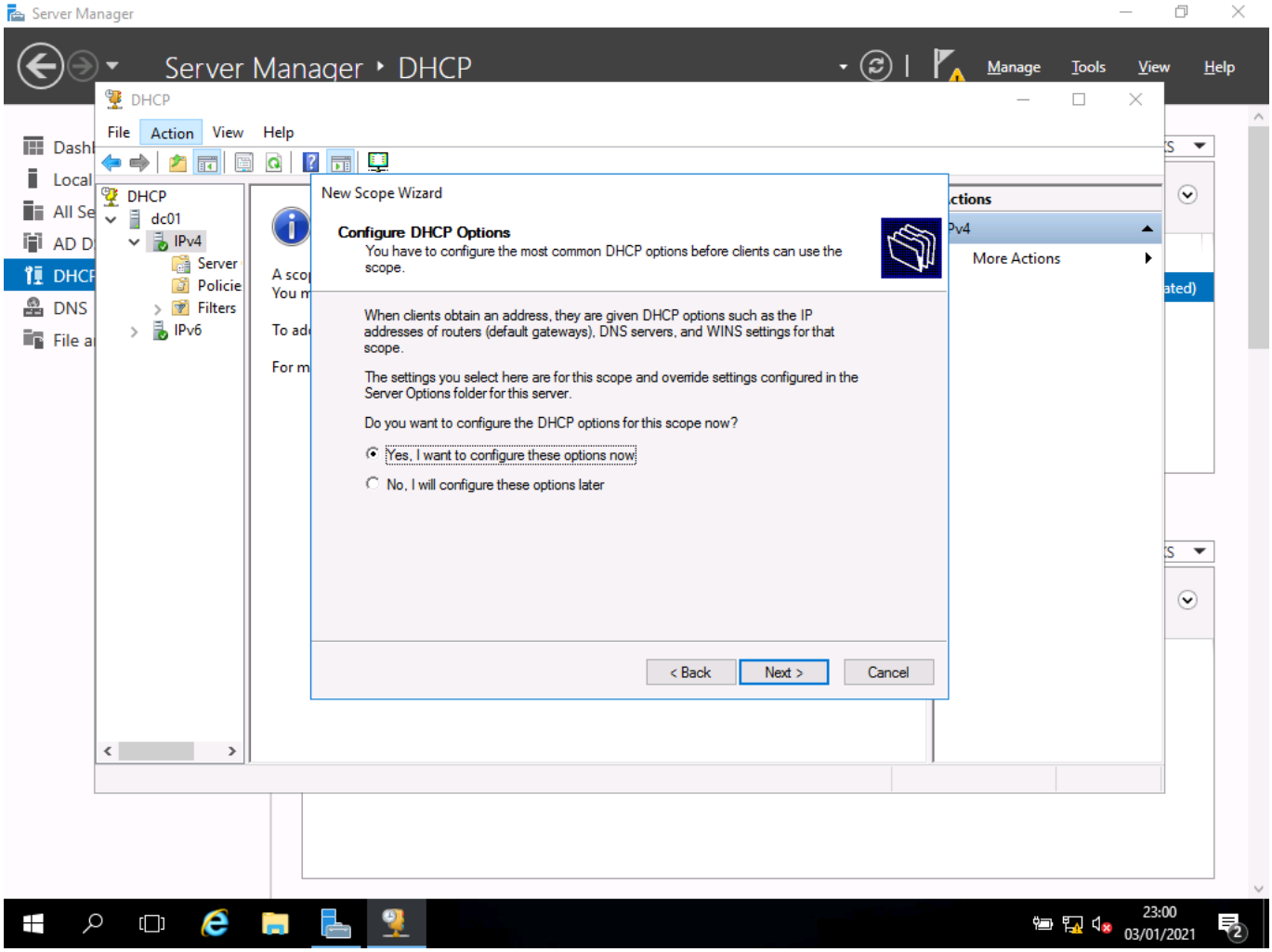
- I input the first and last address I want to use in the pool and select the length of the subnet which is default at /24 for a 192 address range



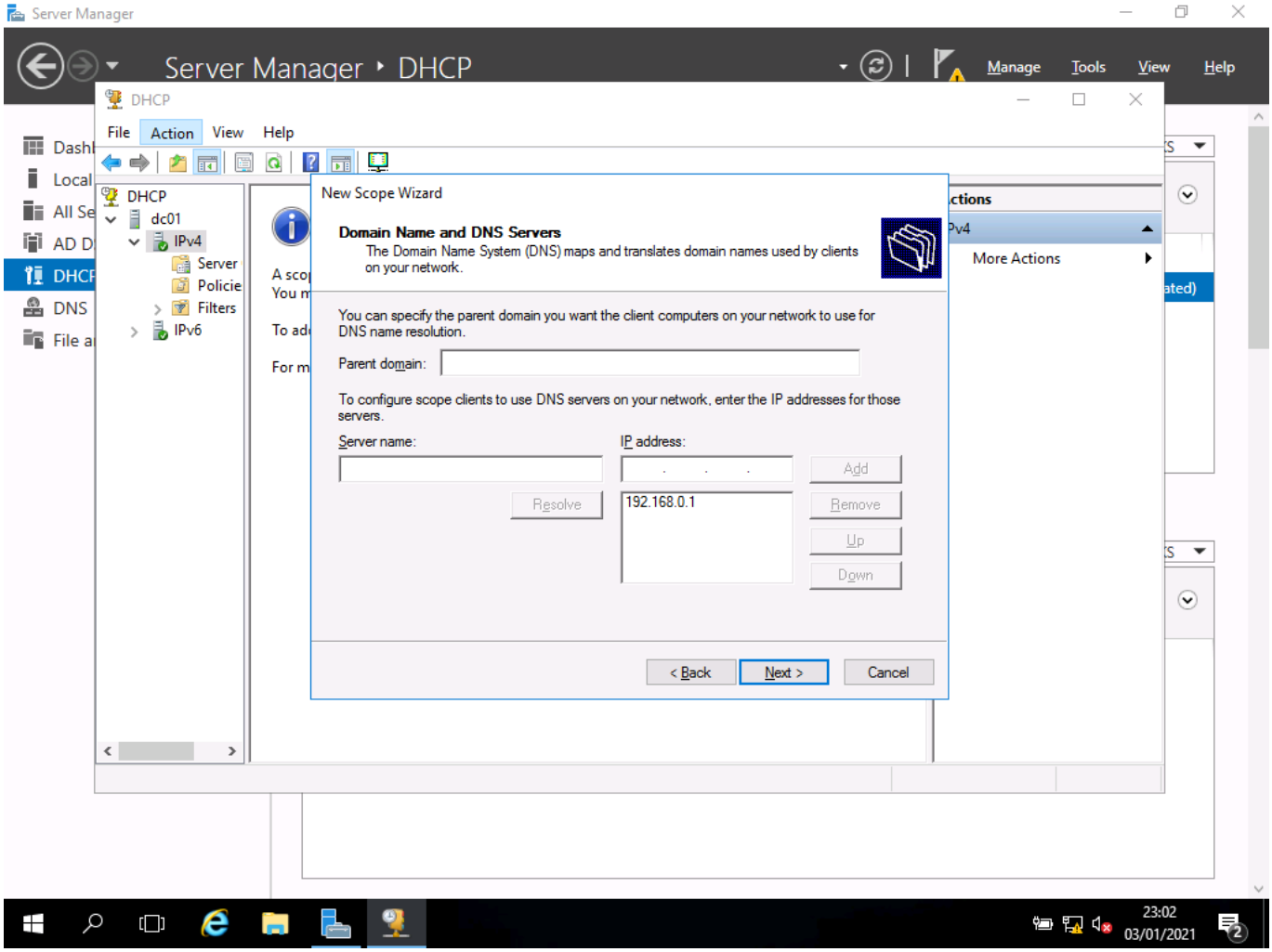
- I add the range of IP addresses that I want to use (details below)



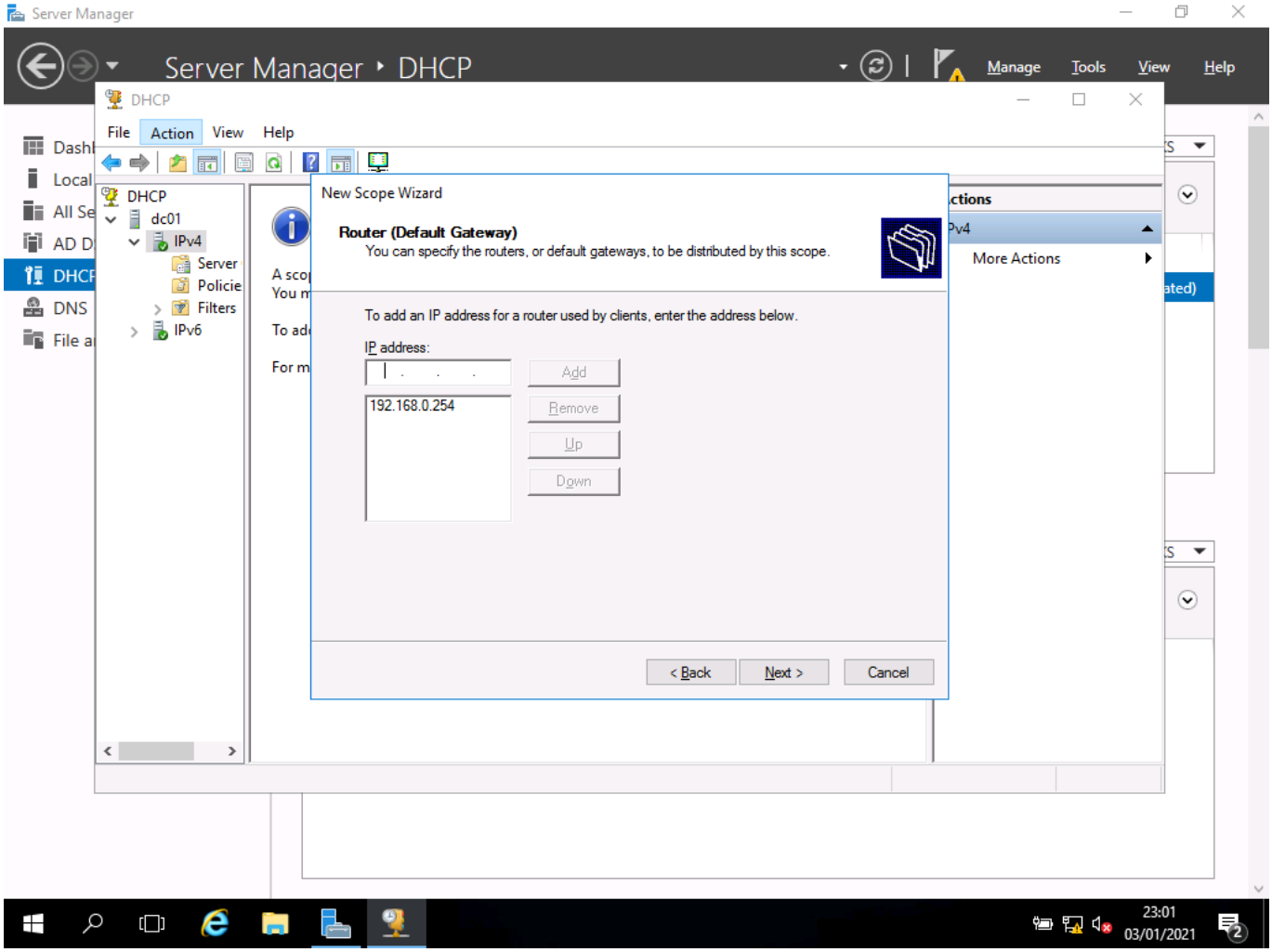
- I now set the lease time, this is how long that address will be held for a particular machine, the default is 8 days



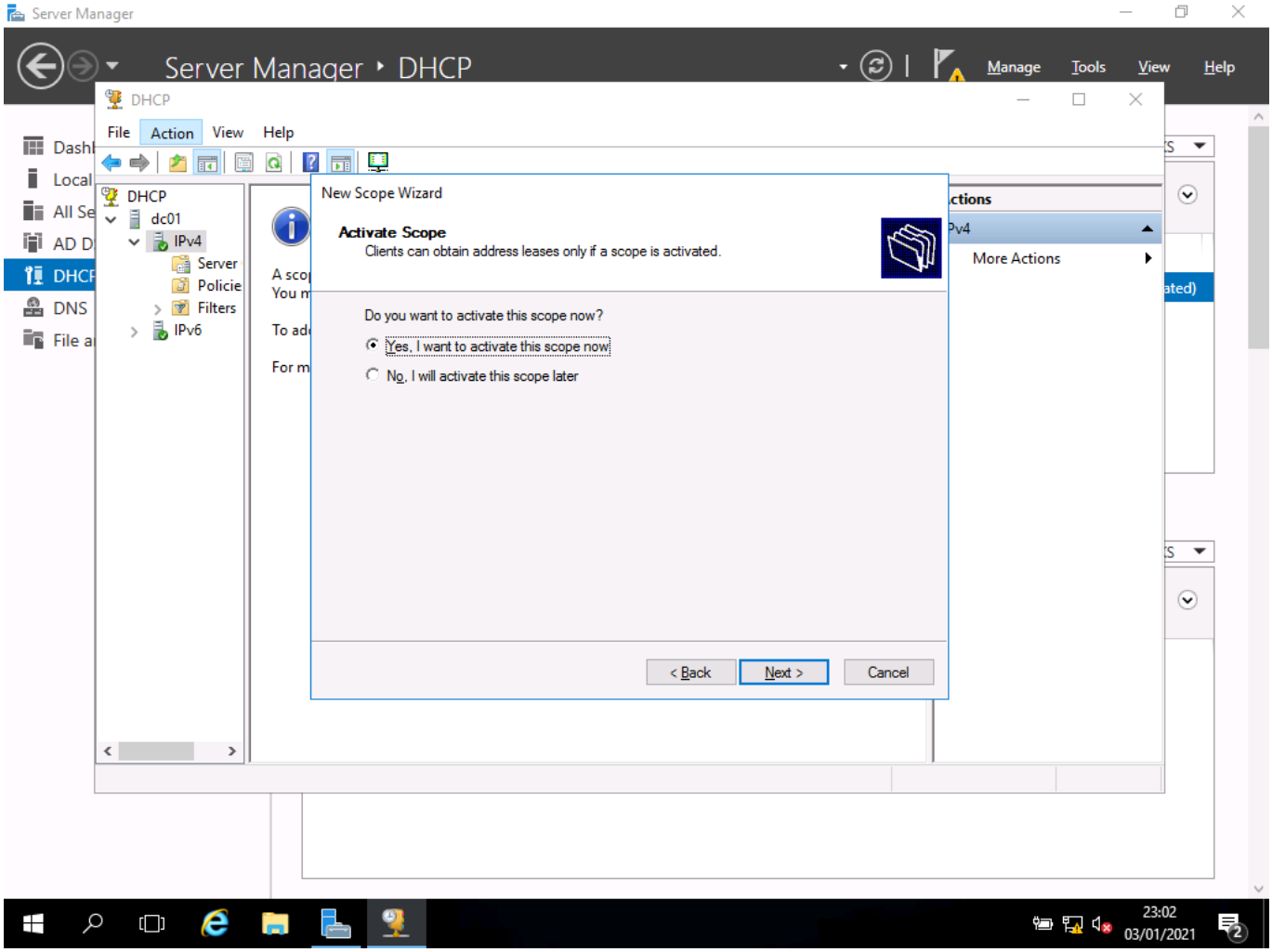
- I agree to the next option



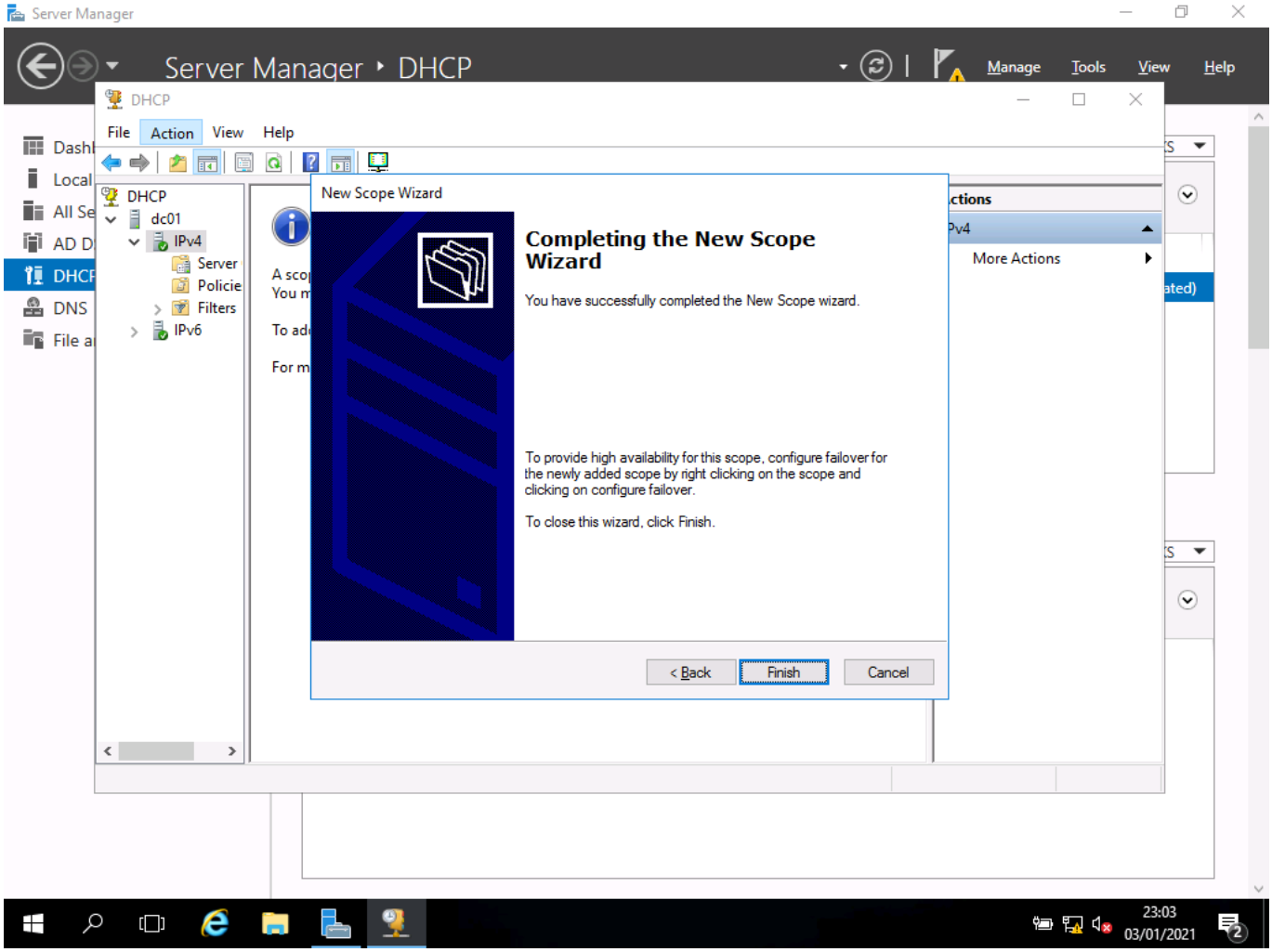
- I add in the details for the DNS server so that they will be given out by the DHCP server along with the host address



- and again, I use the default option



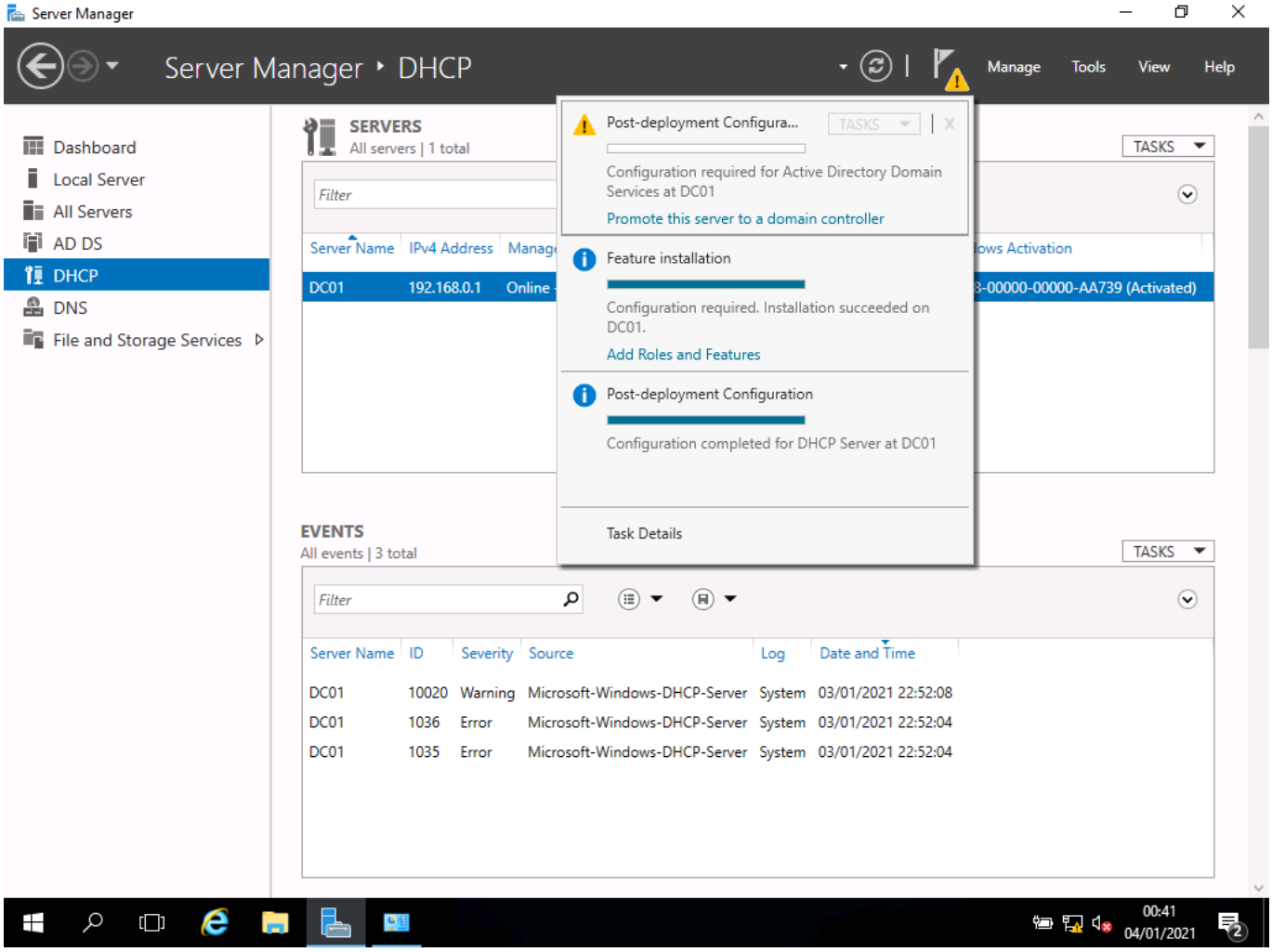
- once created the DHCP tool needs to be activated in order for it to give out host addresses, this allows you to create pools in advance of being needed



- now I click finish
- I used the following settings in the wizard:
  - scope name: network IP addresses
  - IP address range: 192.168.0.100 to 192.168.0.209
  - length: 24/Subnet Mask: 255.255.255.0
  - no exclusions were added
  - lease duration: 8 days
- I chose to configure DHCP options:
  - default gateway: 192.168.0.254 (as specified in network plan)
  - DNS IP address: 192.168.0.1
- once complete, I chose to activate the scope

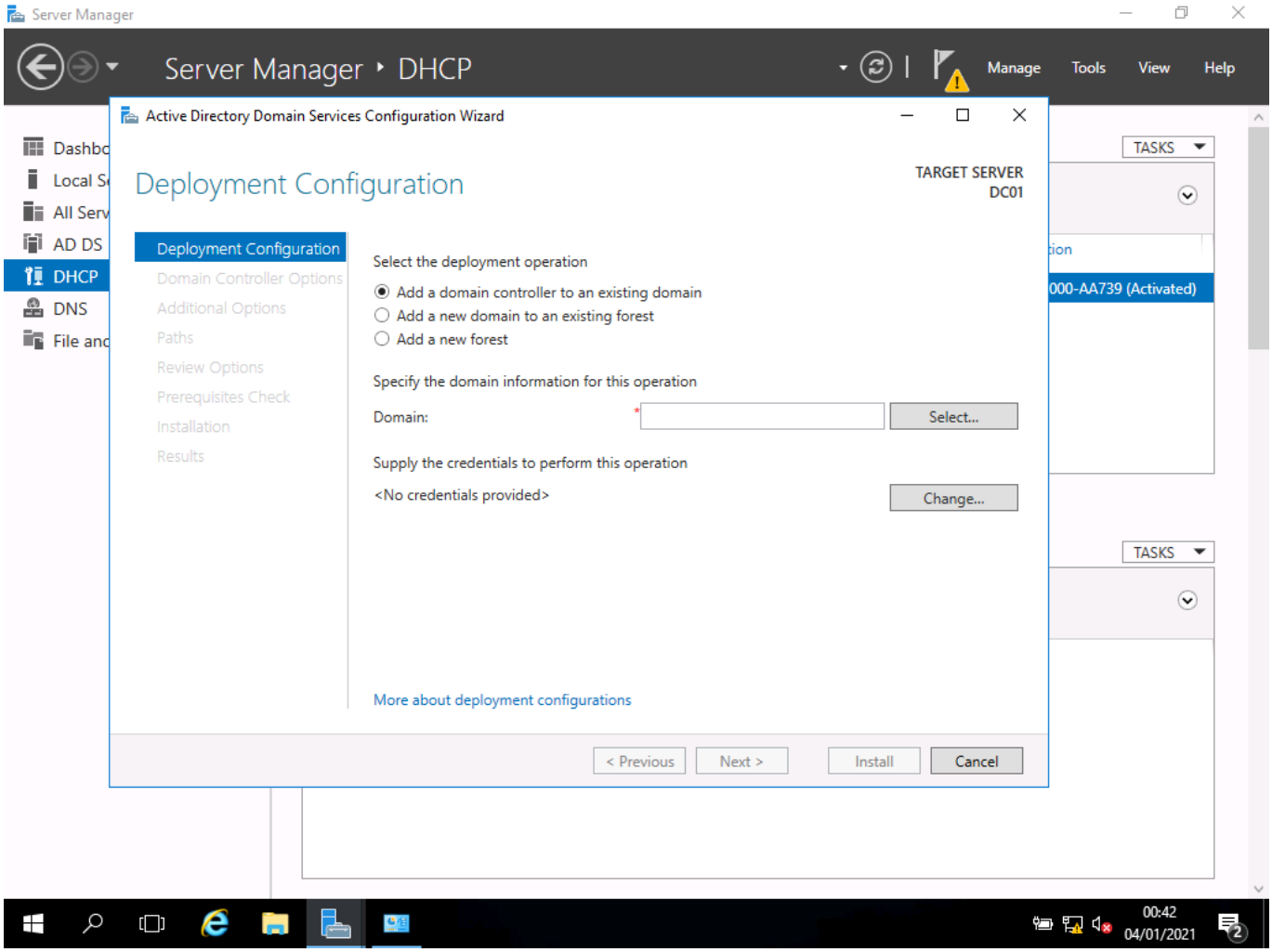
Setting up active directory

Screenshot:

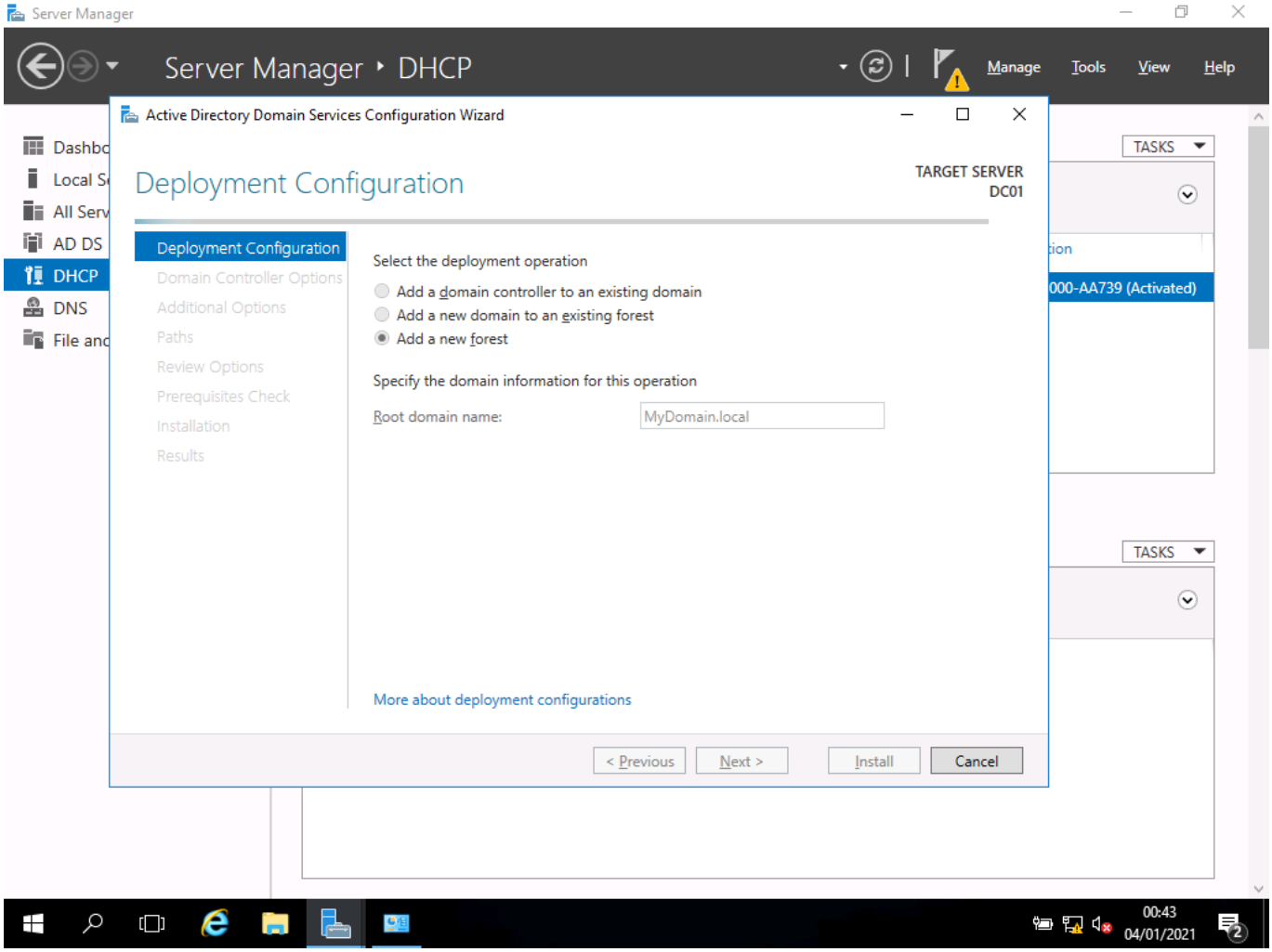


- I click on the yellow warning in server manager and select promote this server to a domain controller

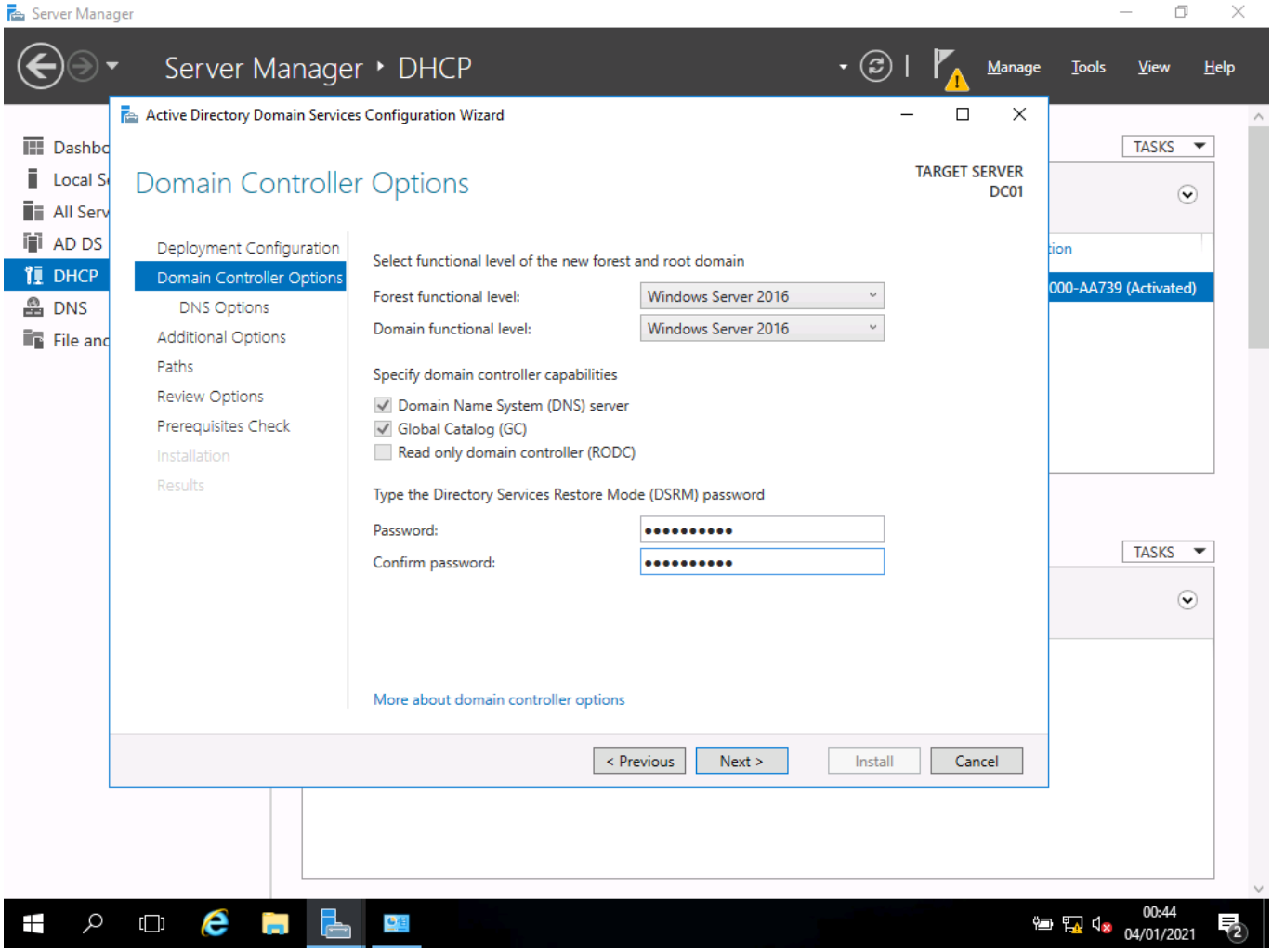
Screenshots:



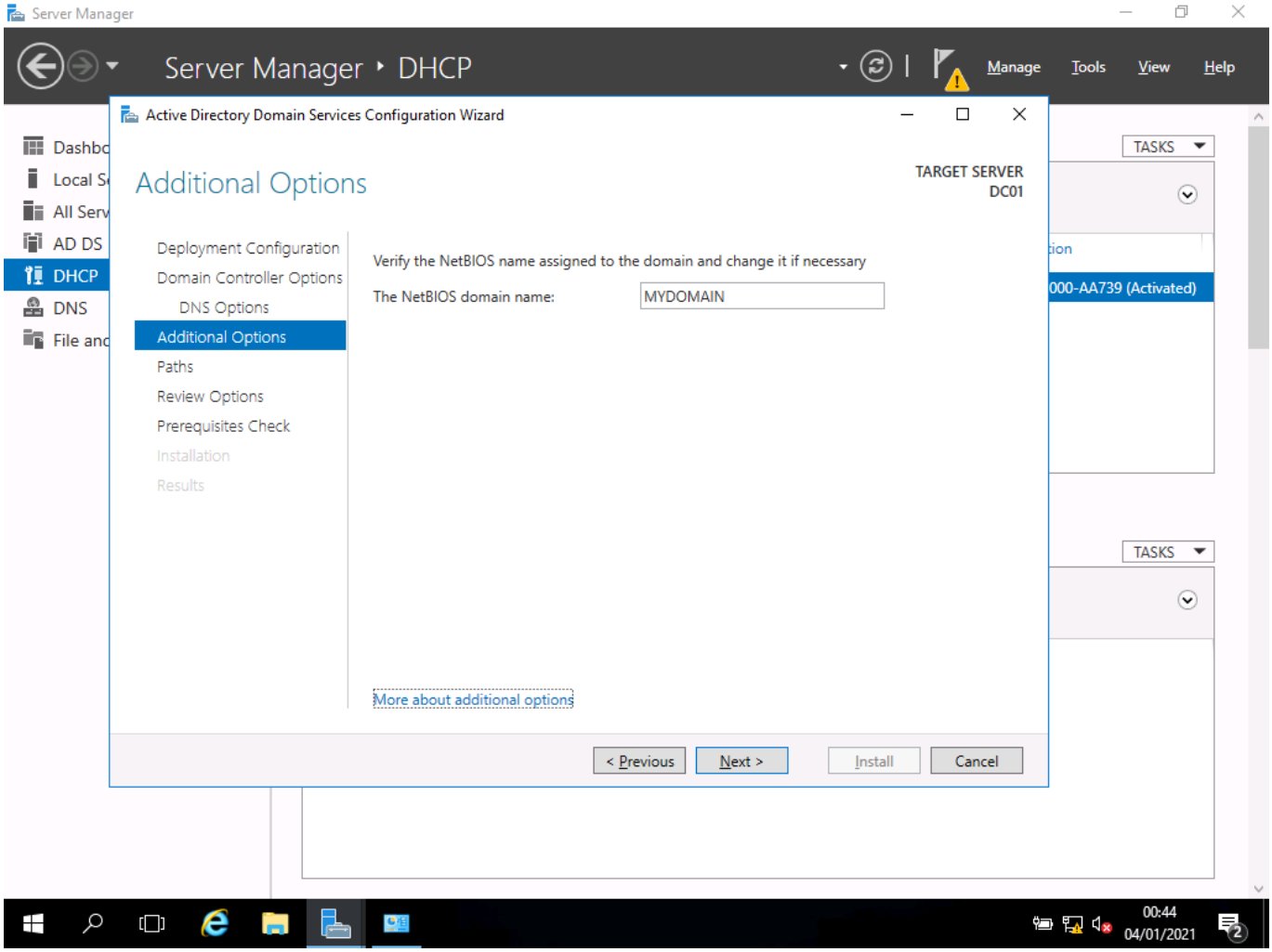
- now I need to add a domain



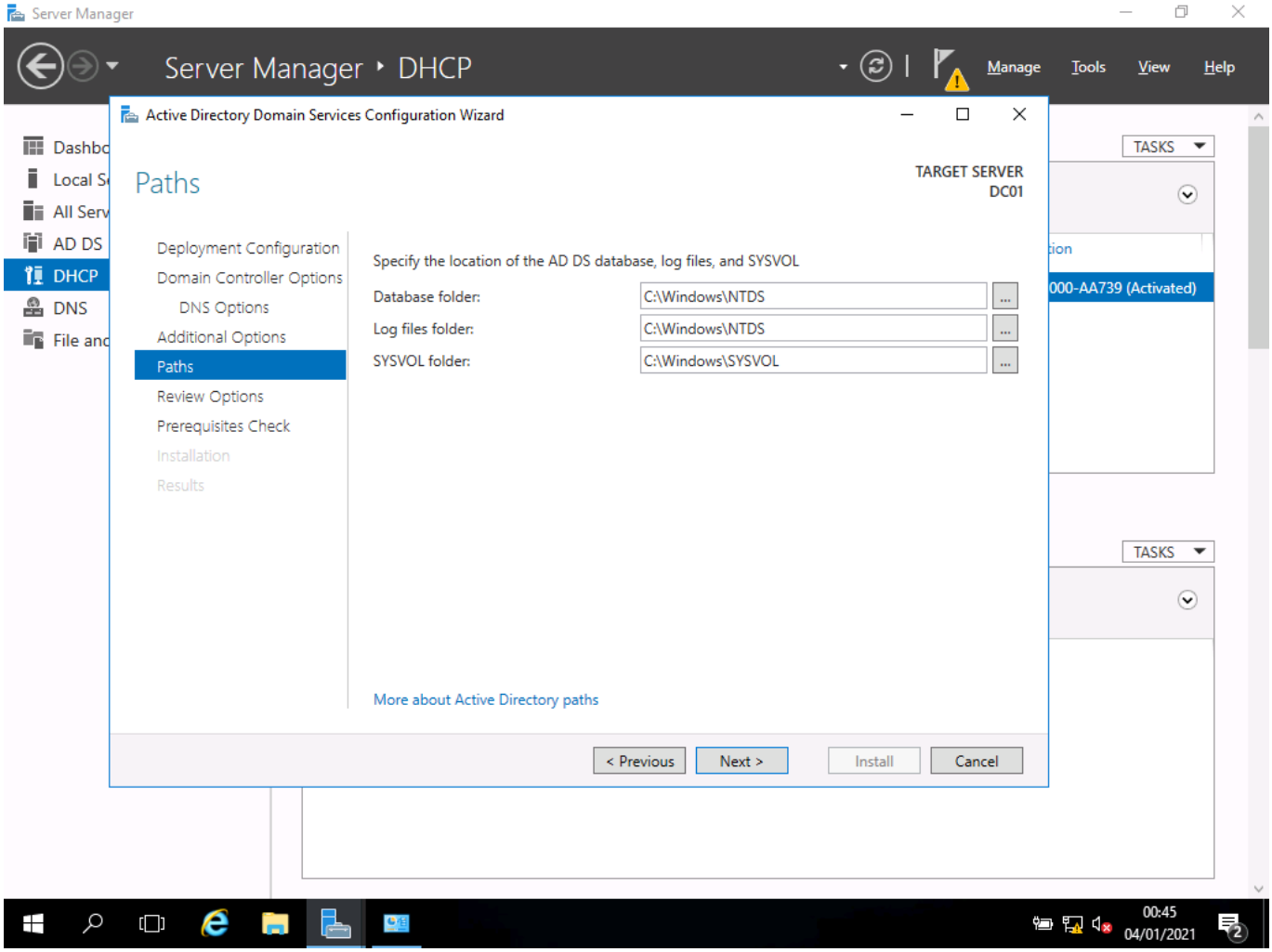
- as the primary deployment configuration, I select new forest



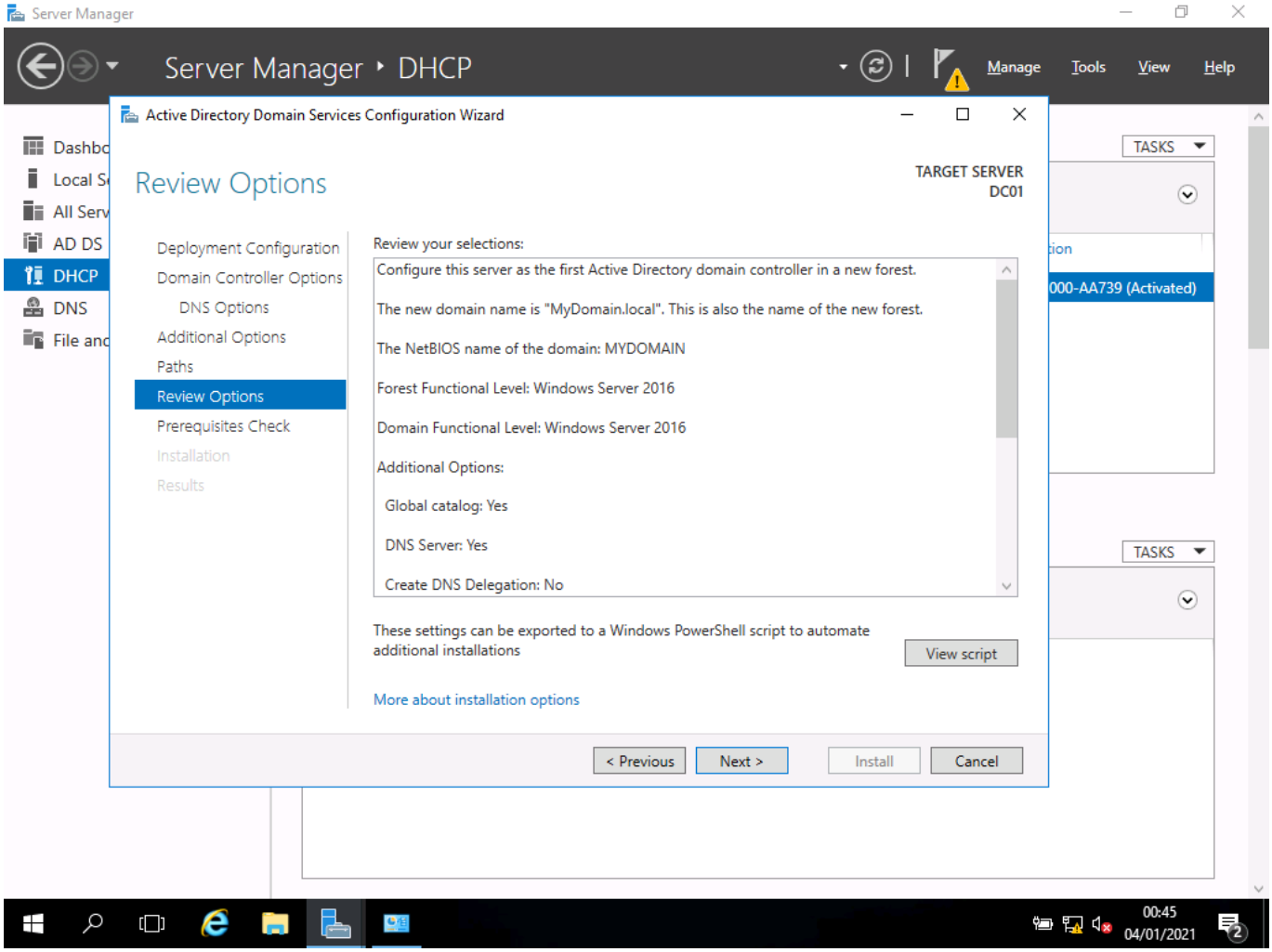
- I add some security information (details below)



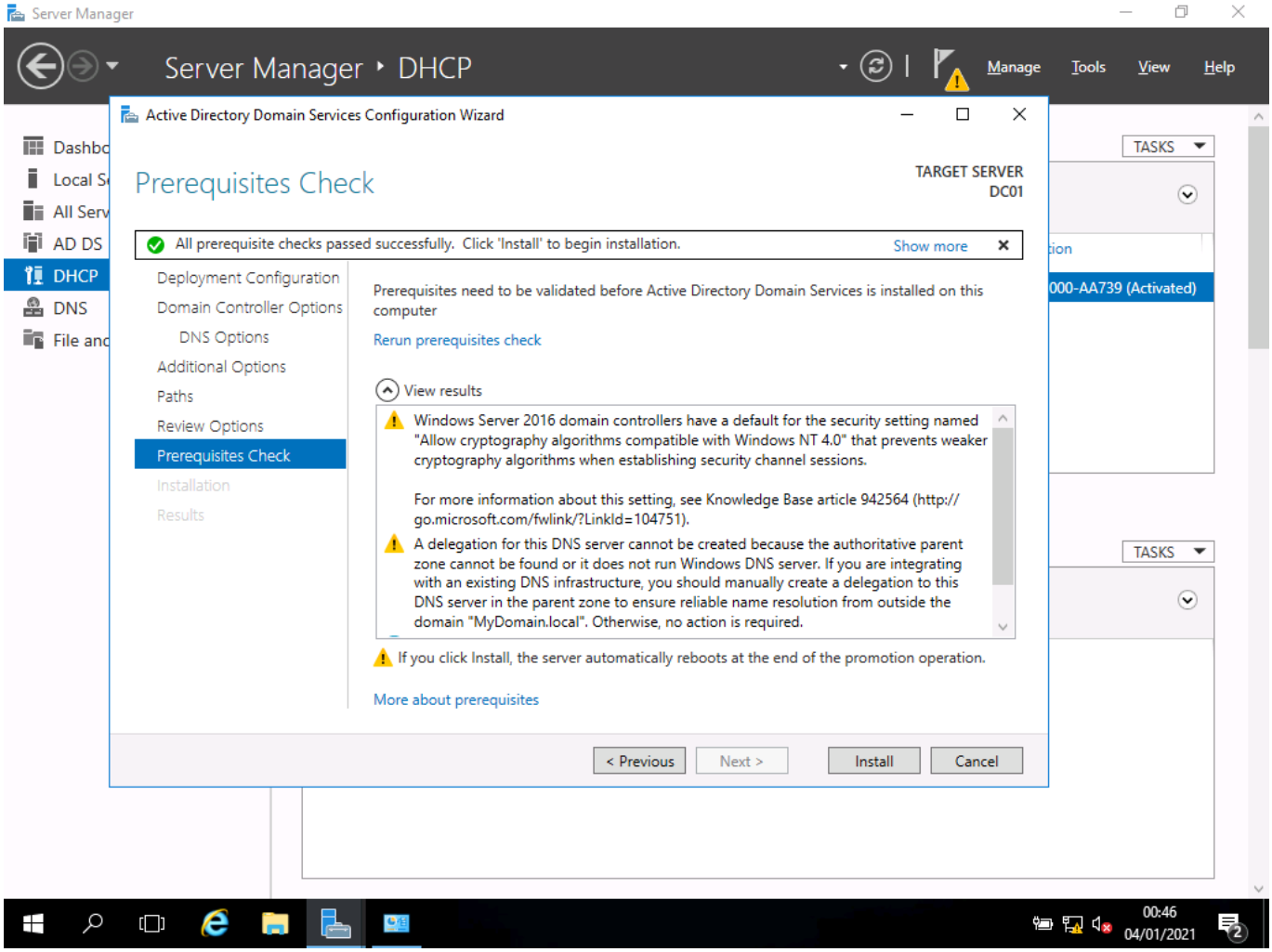
- I give it a name



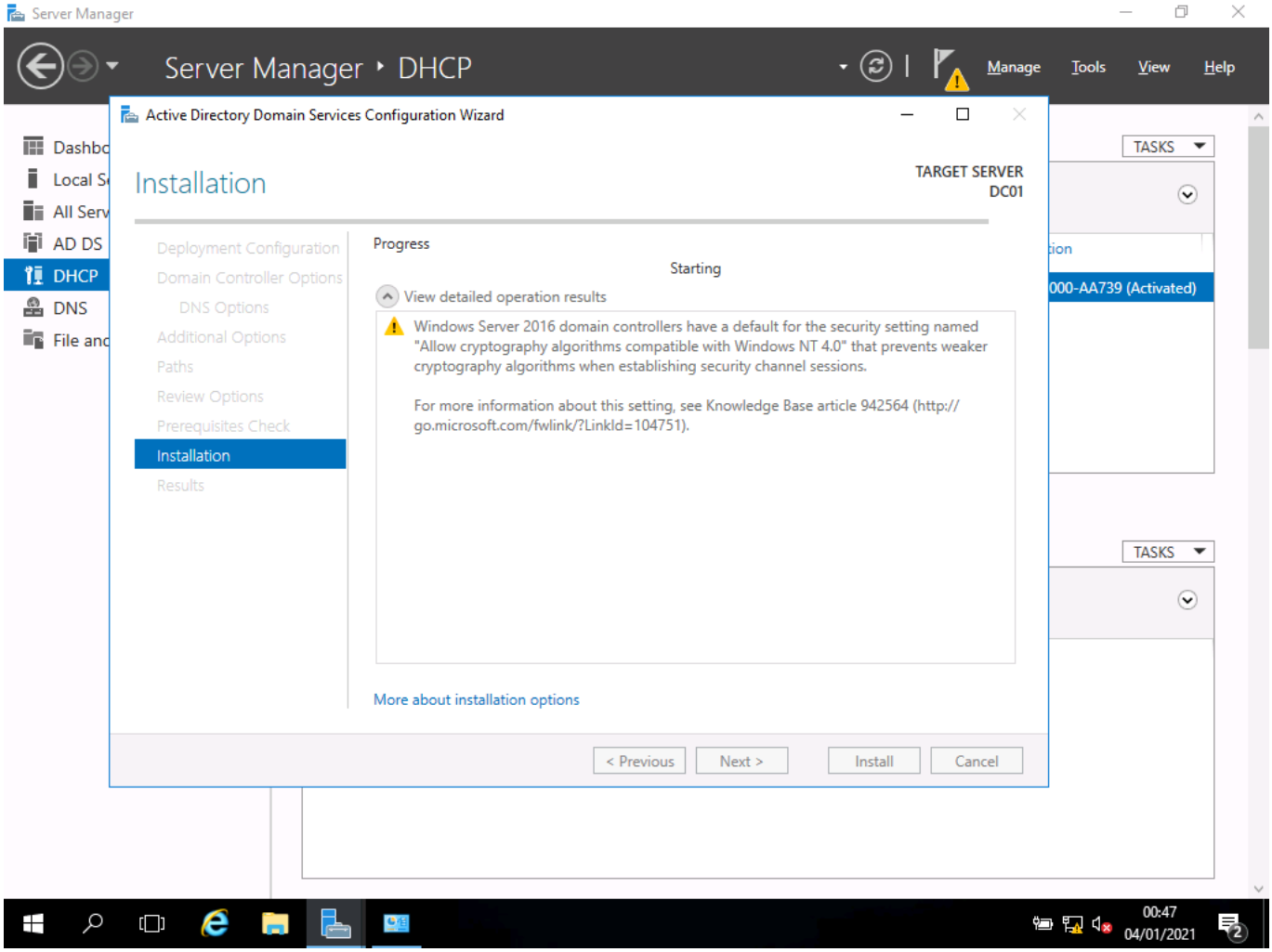
- I select the default options



- and again, I select defaults

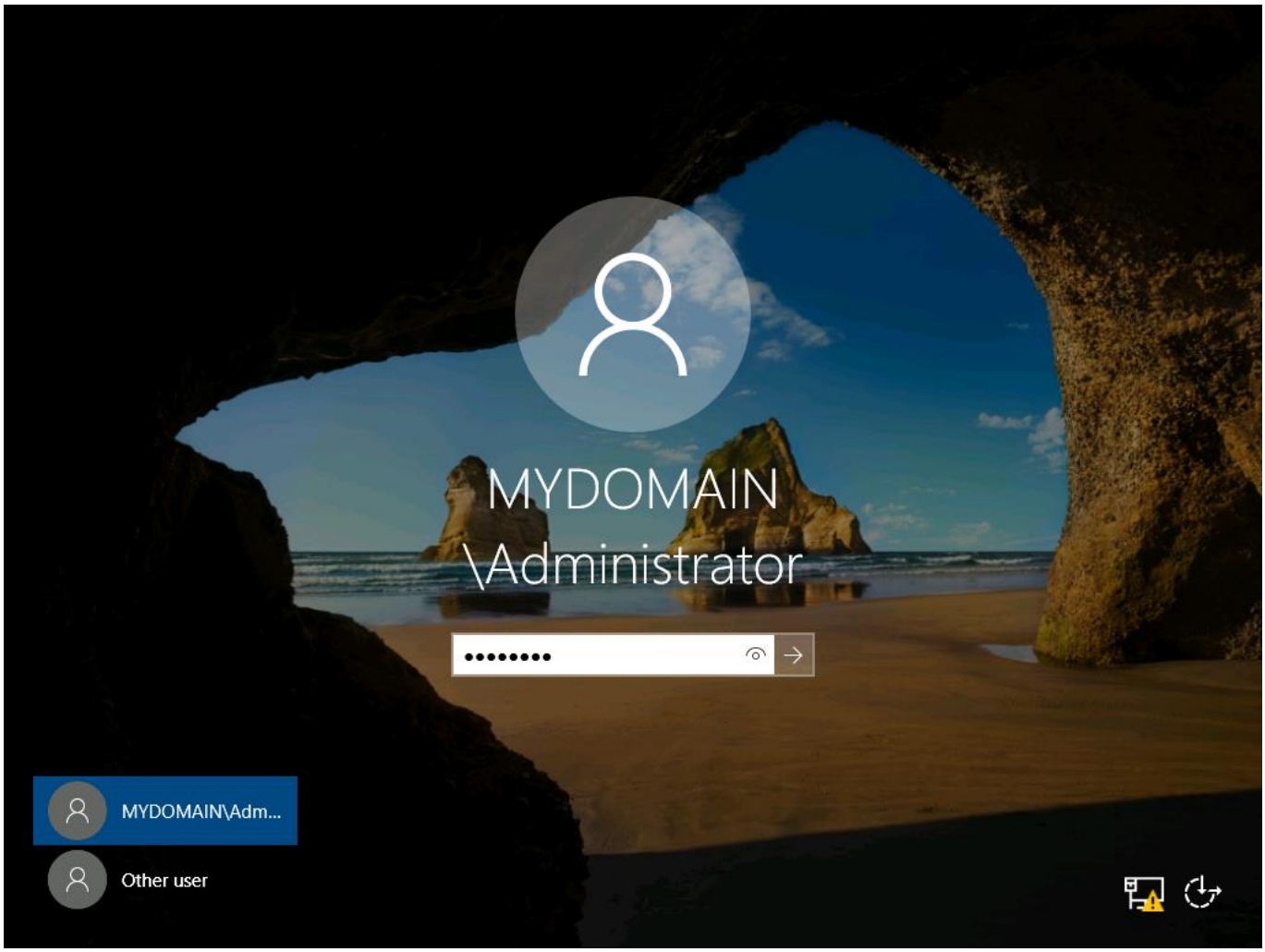


- and I select install, having read the warnings

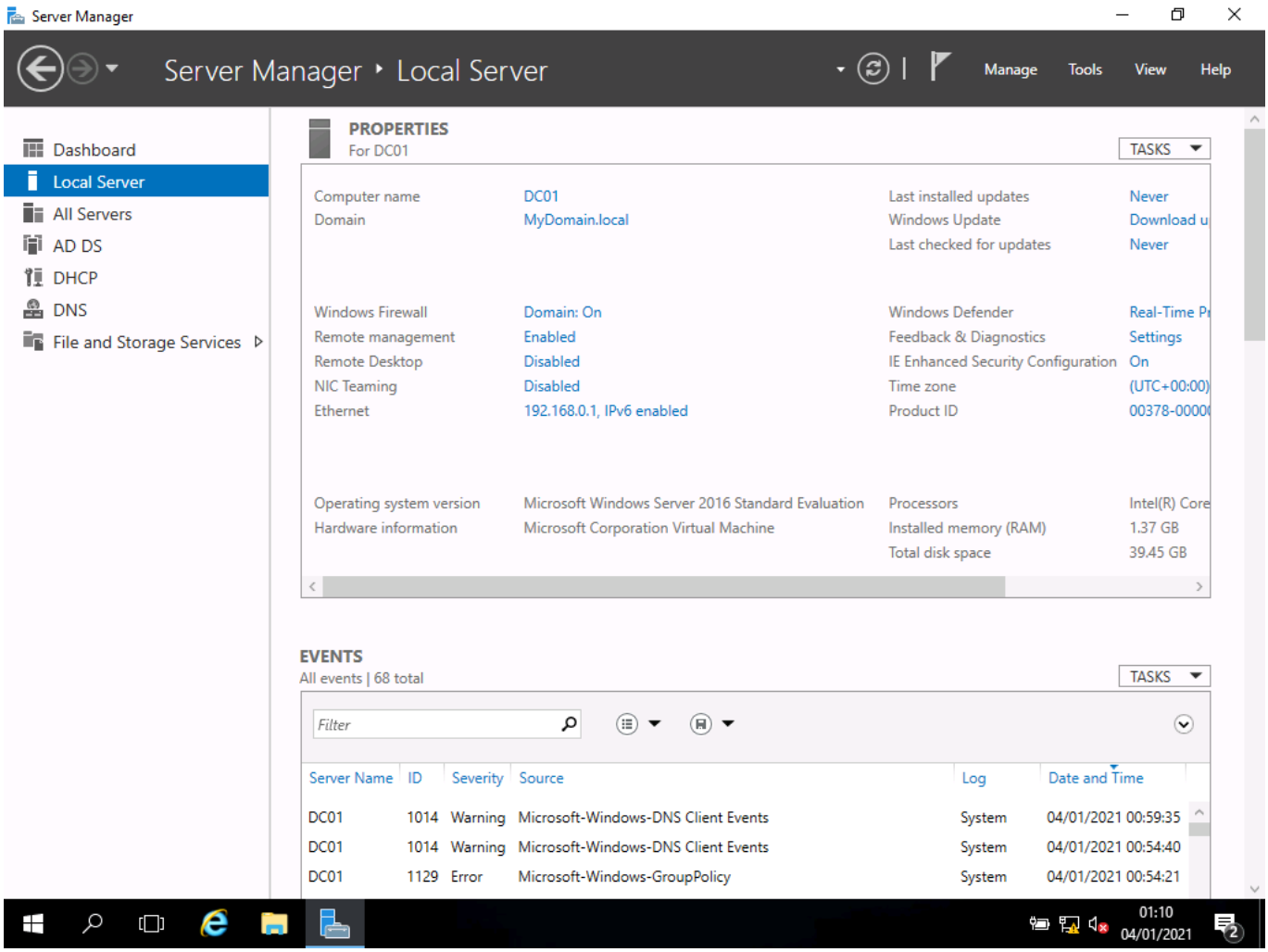


- I use the standard cryptography
- I follow the active directory domain service (ADDS) with the following settings:
  - deployment configuration - add a new forest
  - root domain name - MyDomain.local (I have chosen this domain name for my local network)
  - directory services restore mode password: I have set a secure password of ionsiTyp!1 for this password

Screenshot:

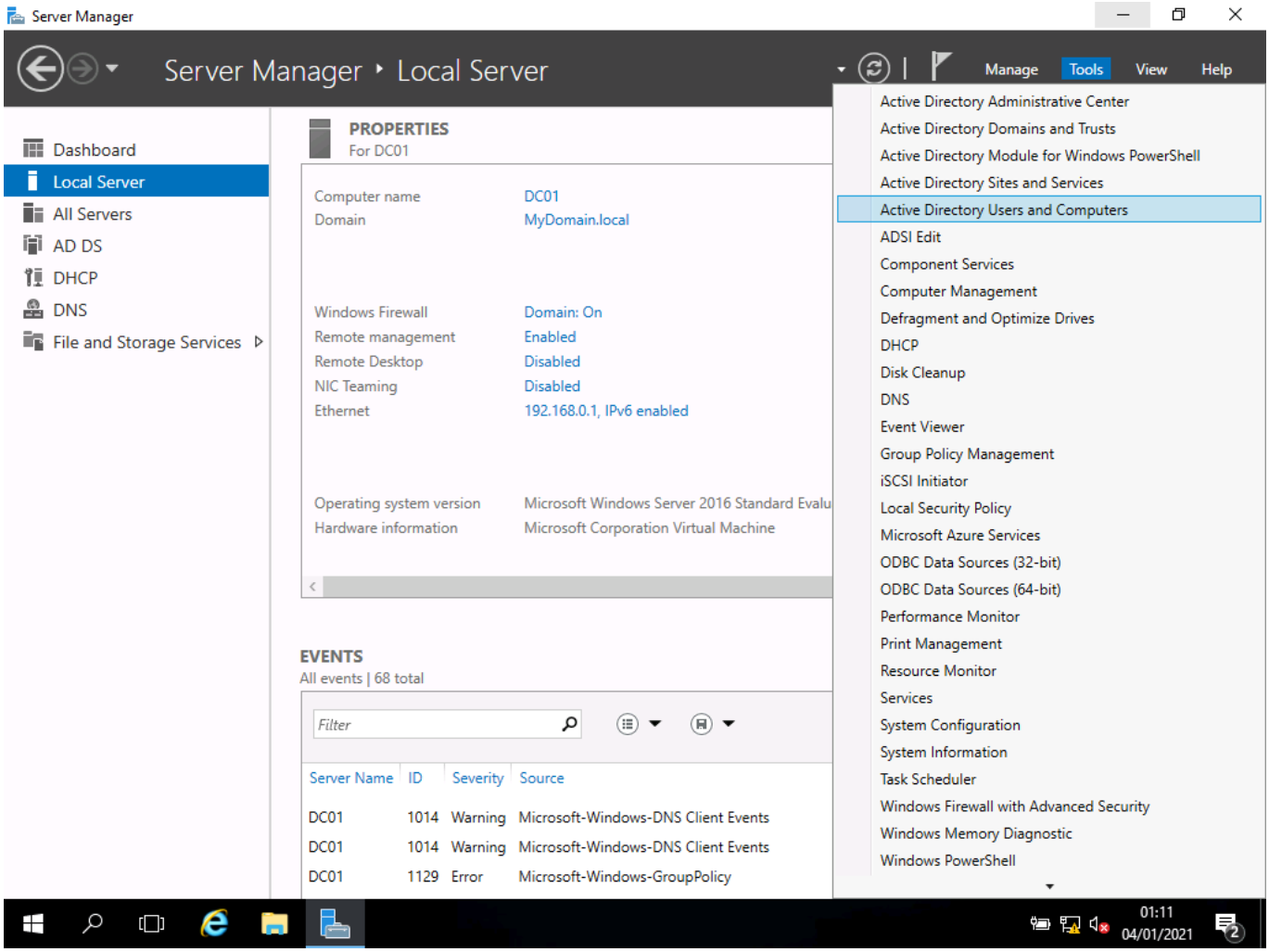


- after a server reboot, I can now log in using the domain admin password I set above

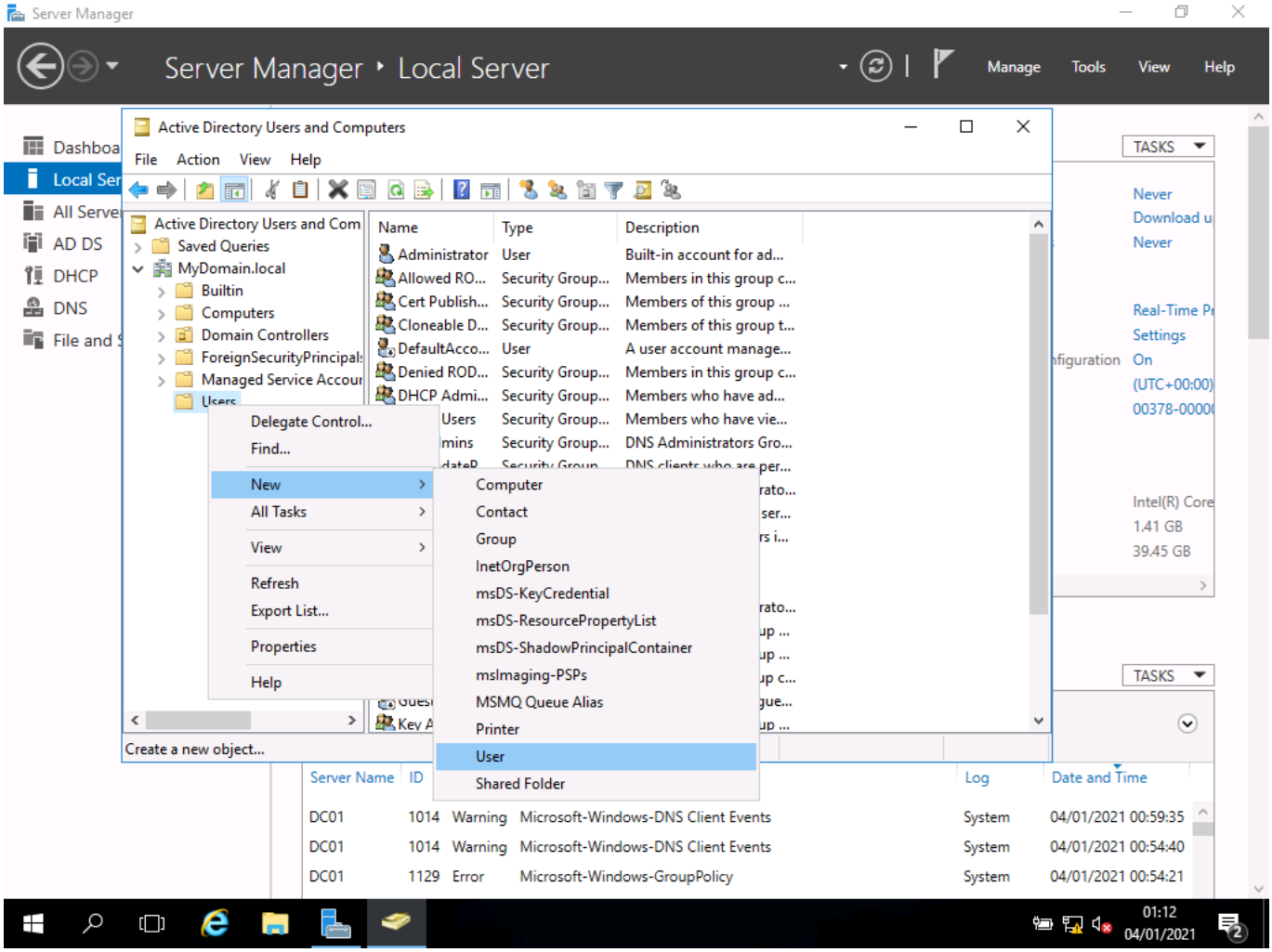


- I can see everything is now complete and there are no warnings
- I can now set up domain administrator accounts and manage the active directory

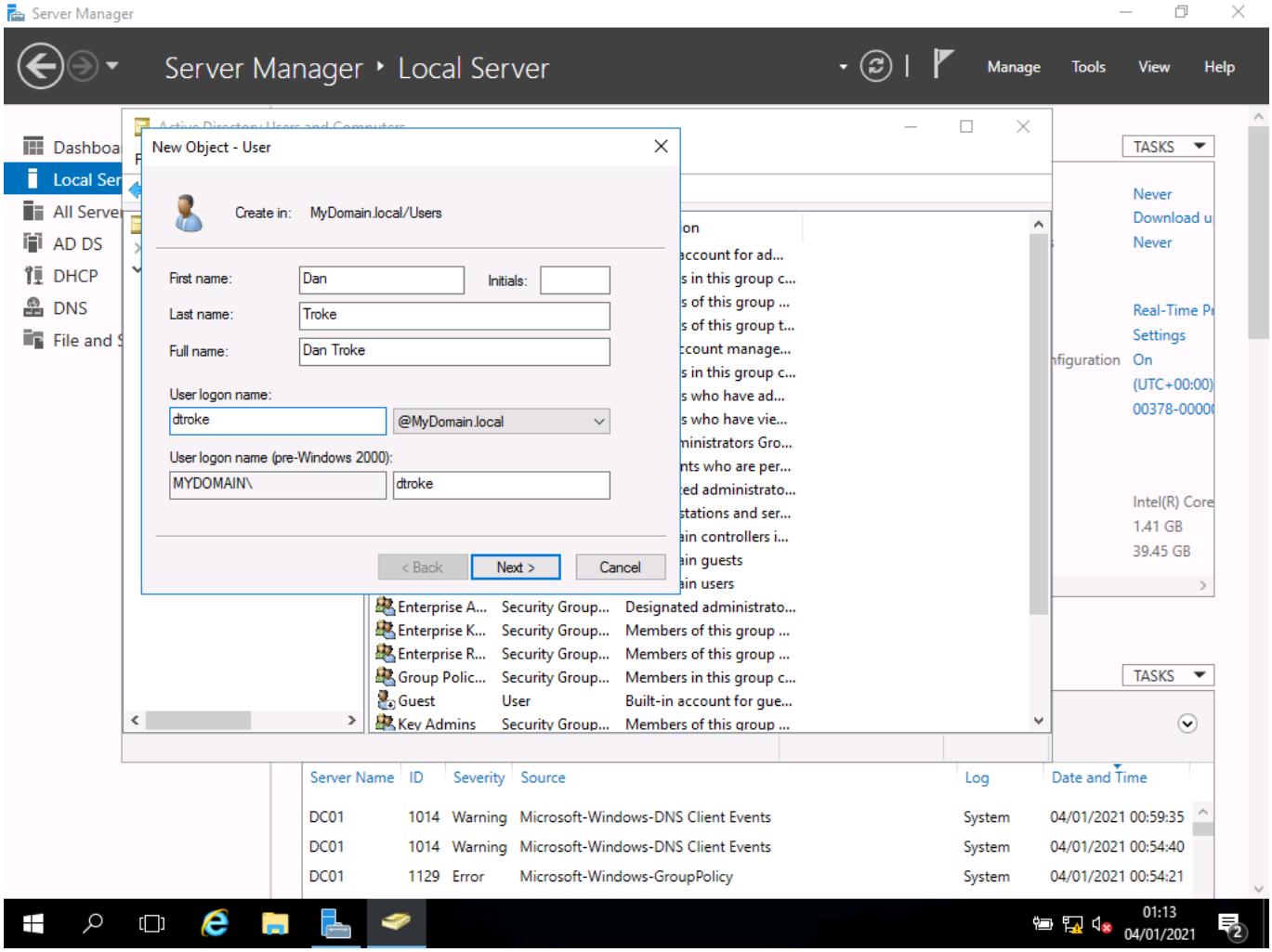
Screenshots:



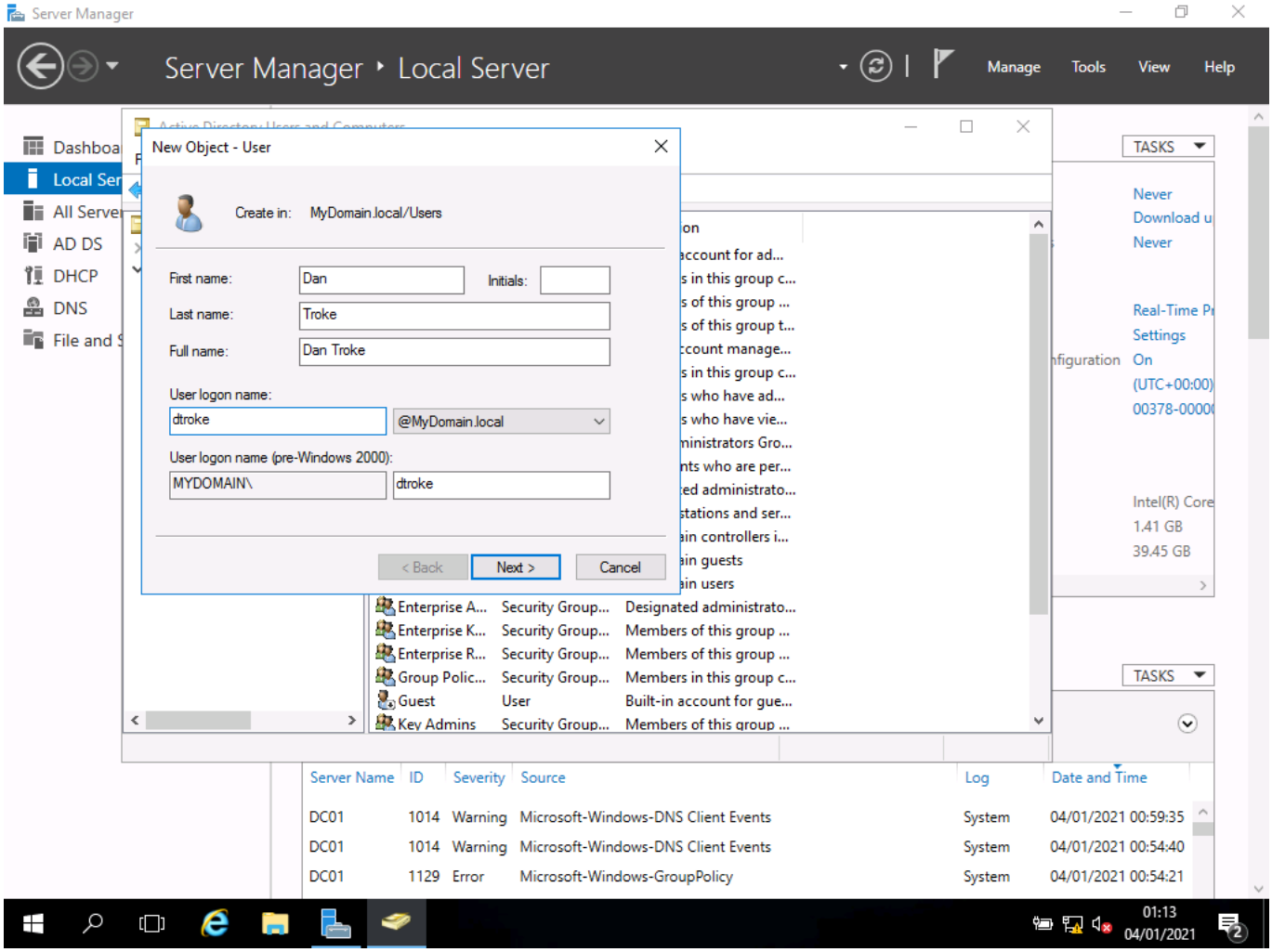
- in server manager, I open tools and the AD wizard



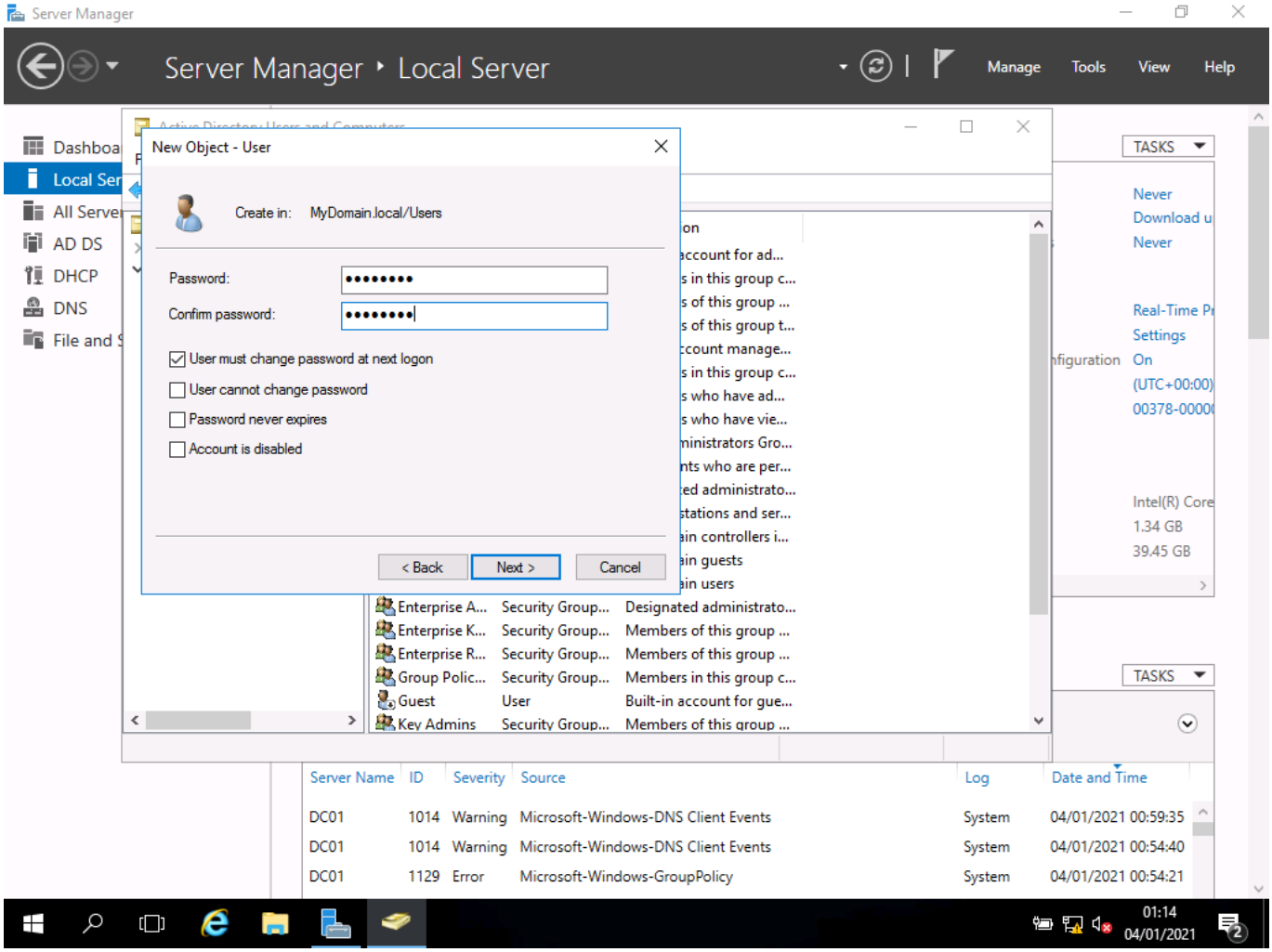
- I start by selecting ‘New’ and then ‘User’



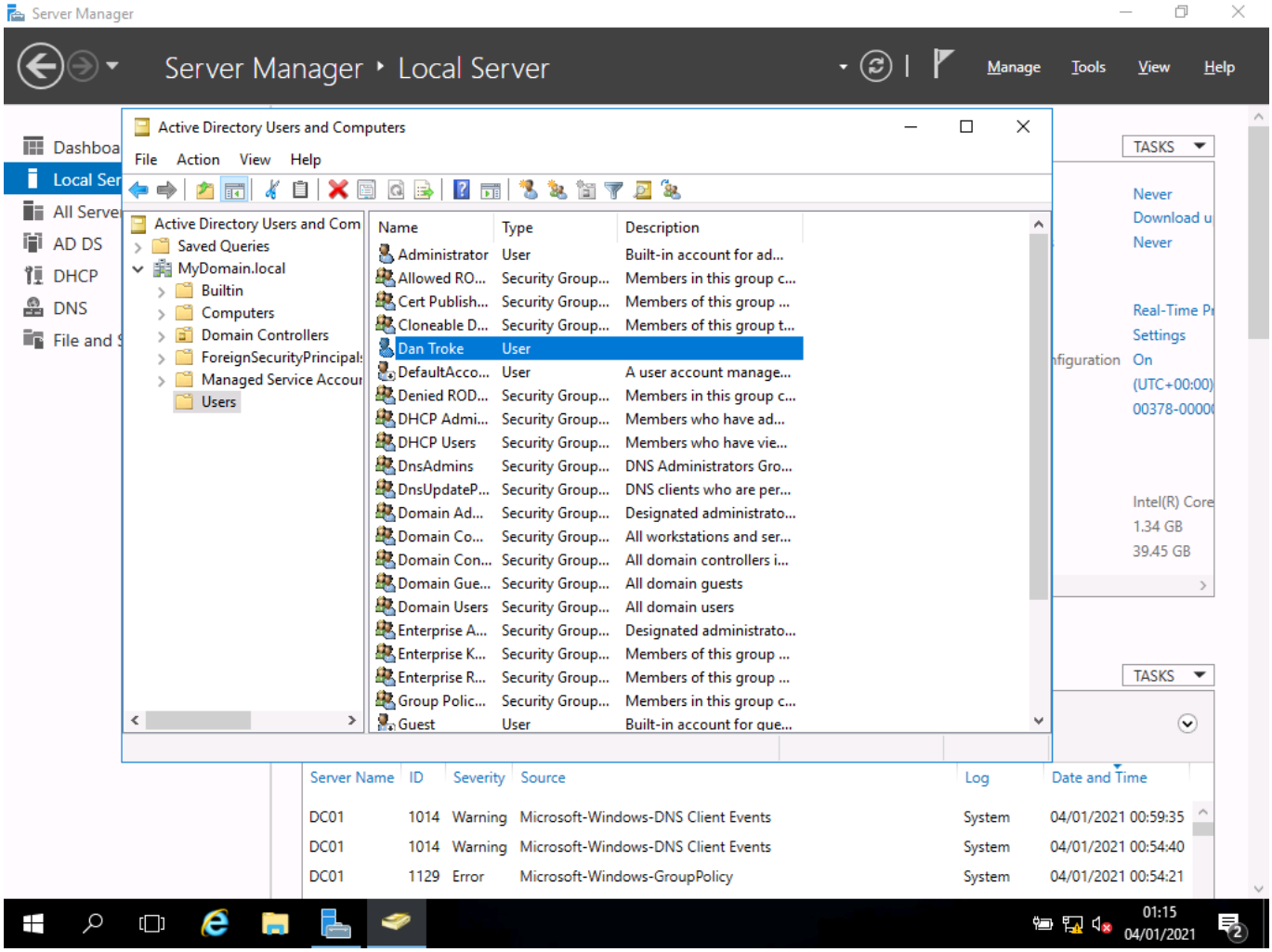
- I add the new user's details



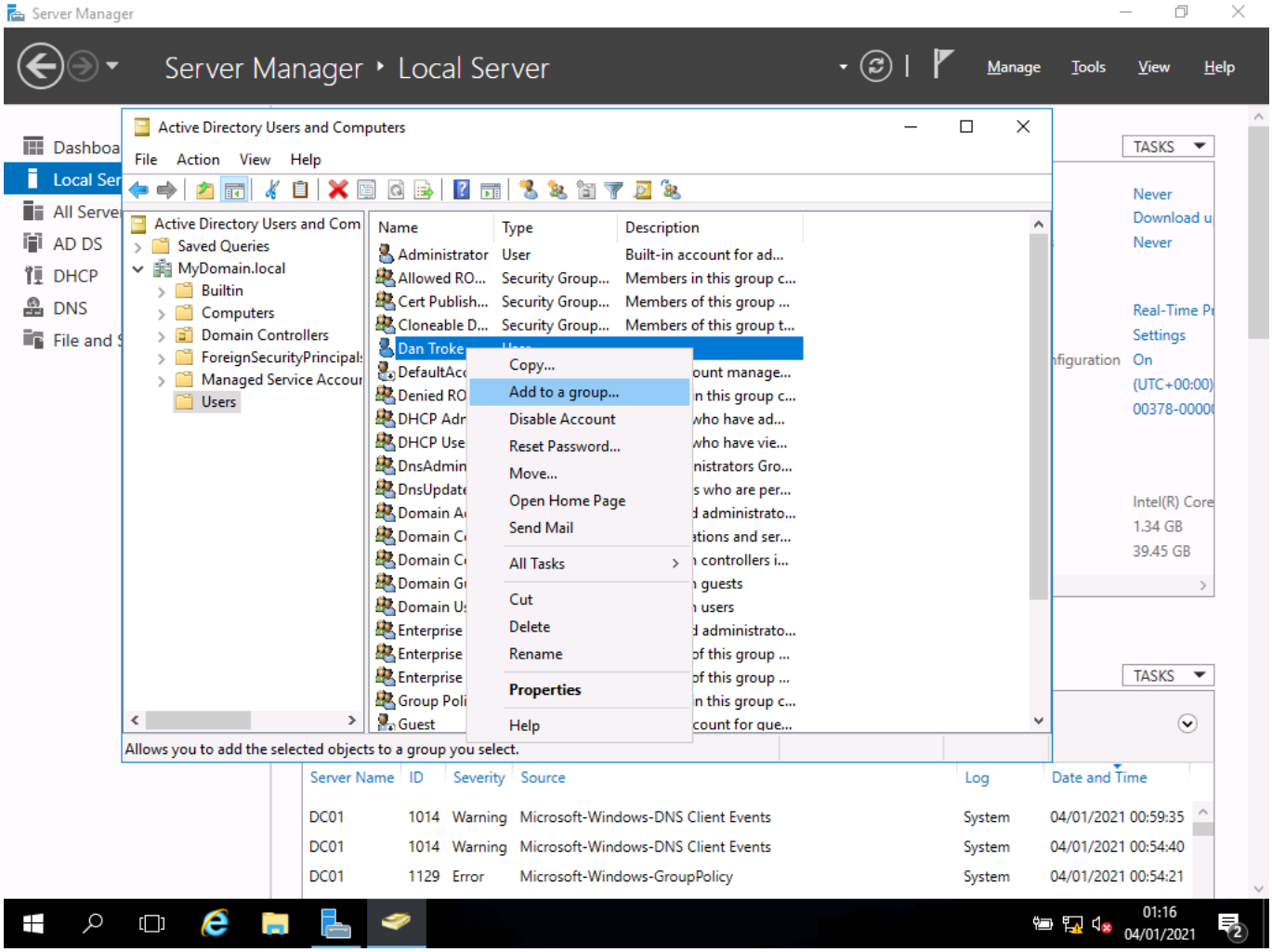
- here I add the details for the new user



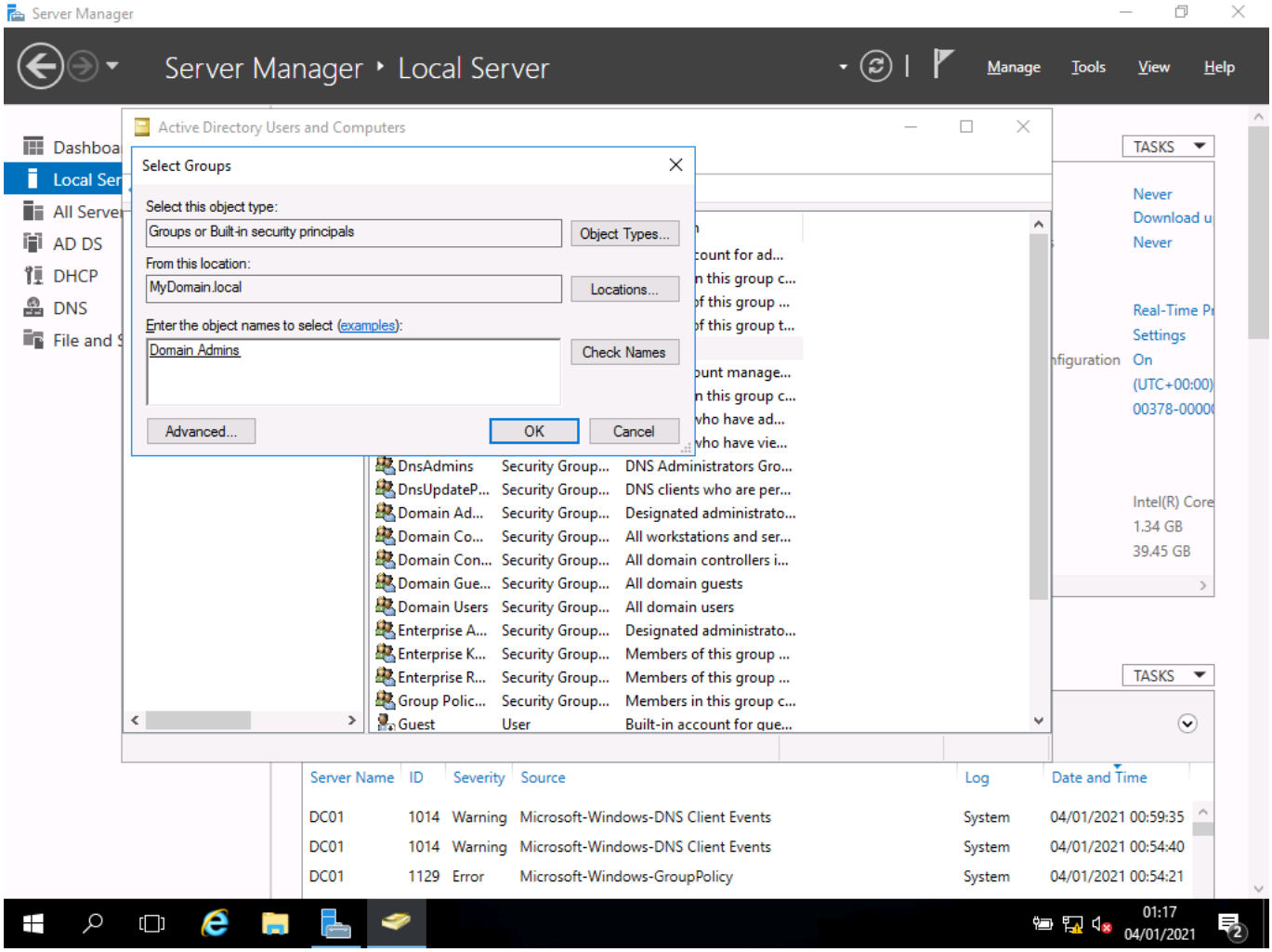
- I add the initial password for the new user; this password will have to change at first log in (see tick box)



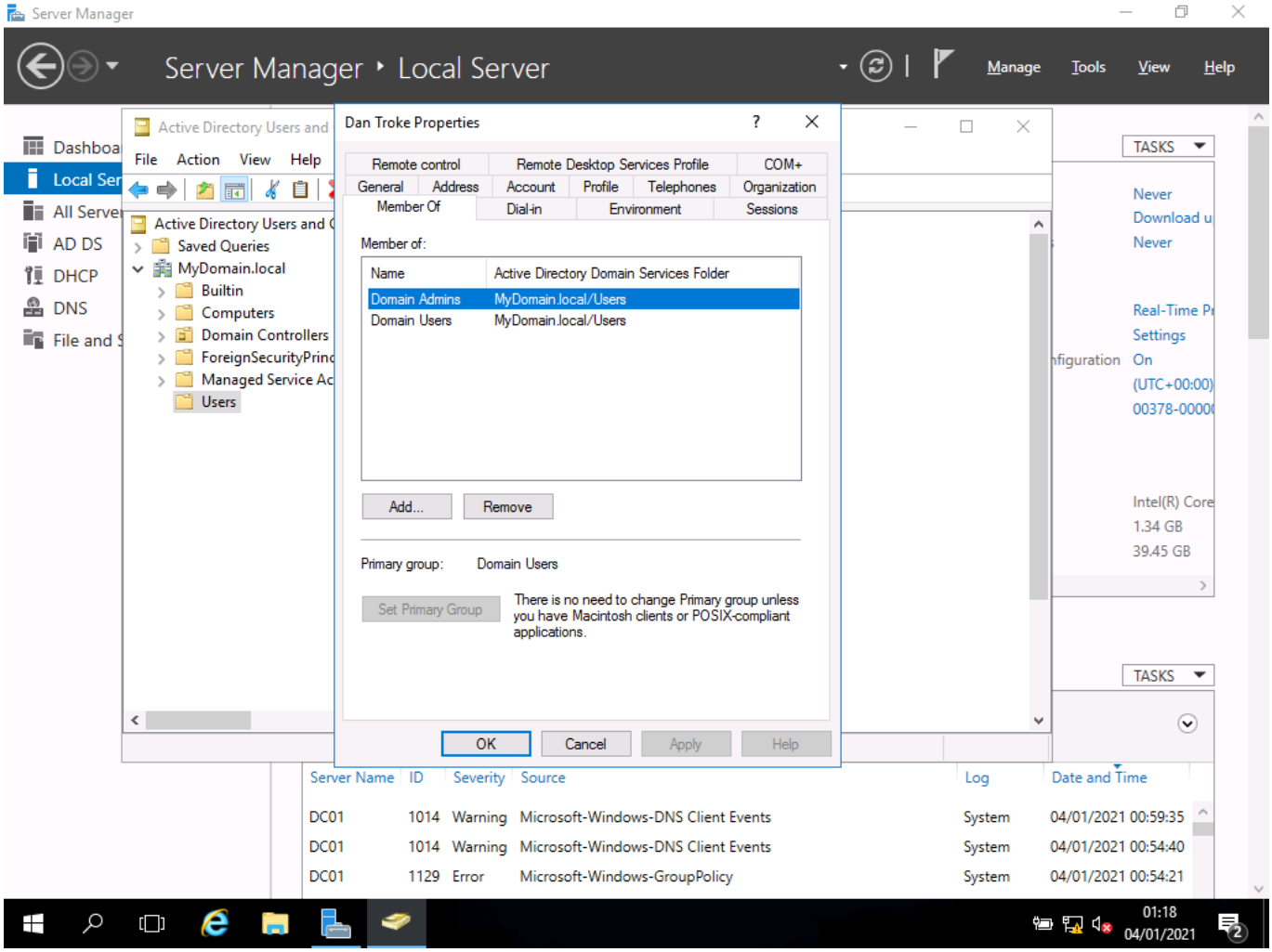
- the new user has been created



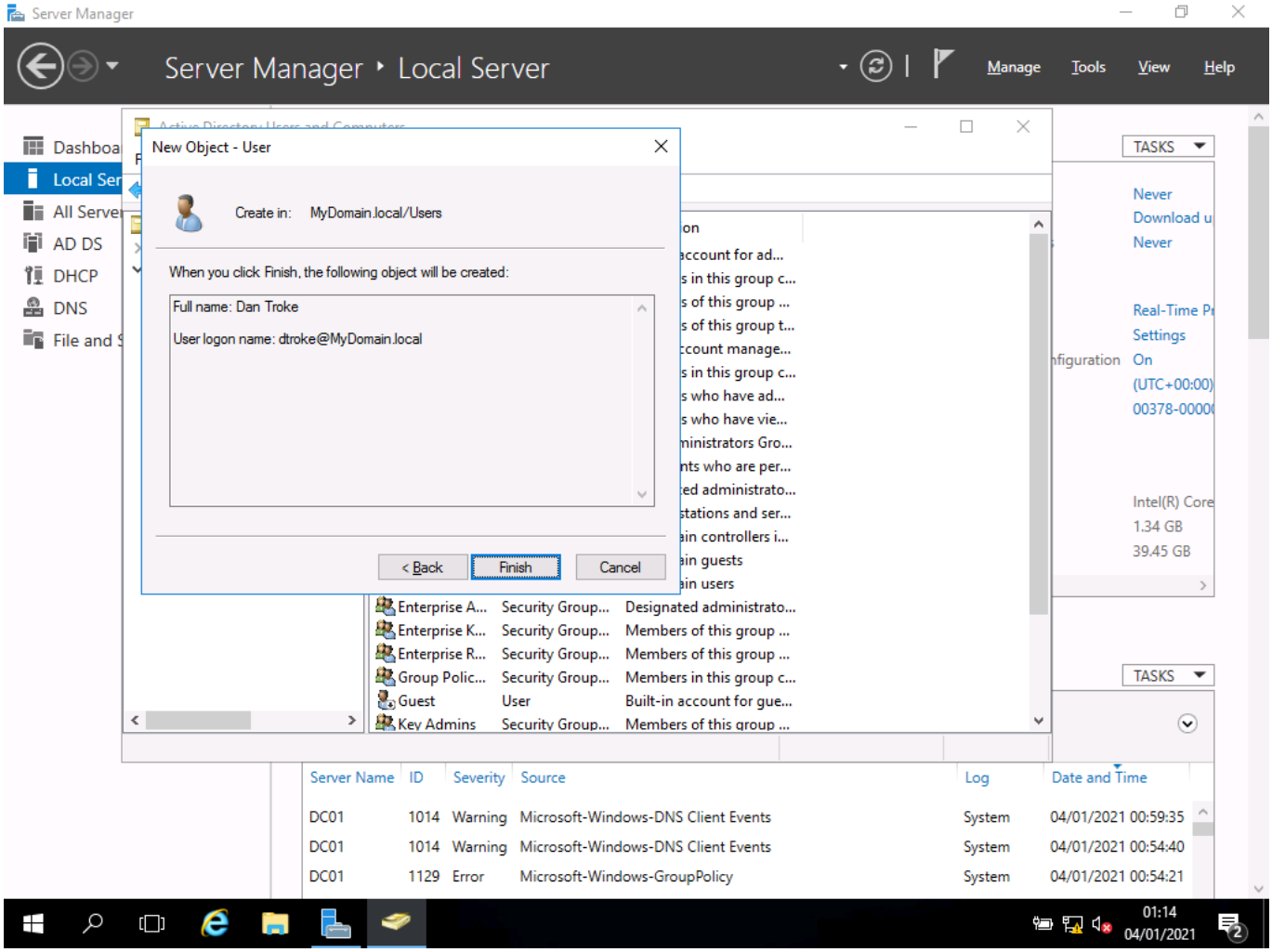
- I now add the new user to a security group



- the new user has been selected



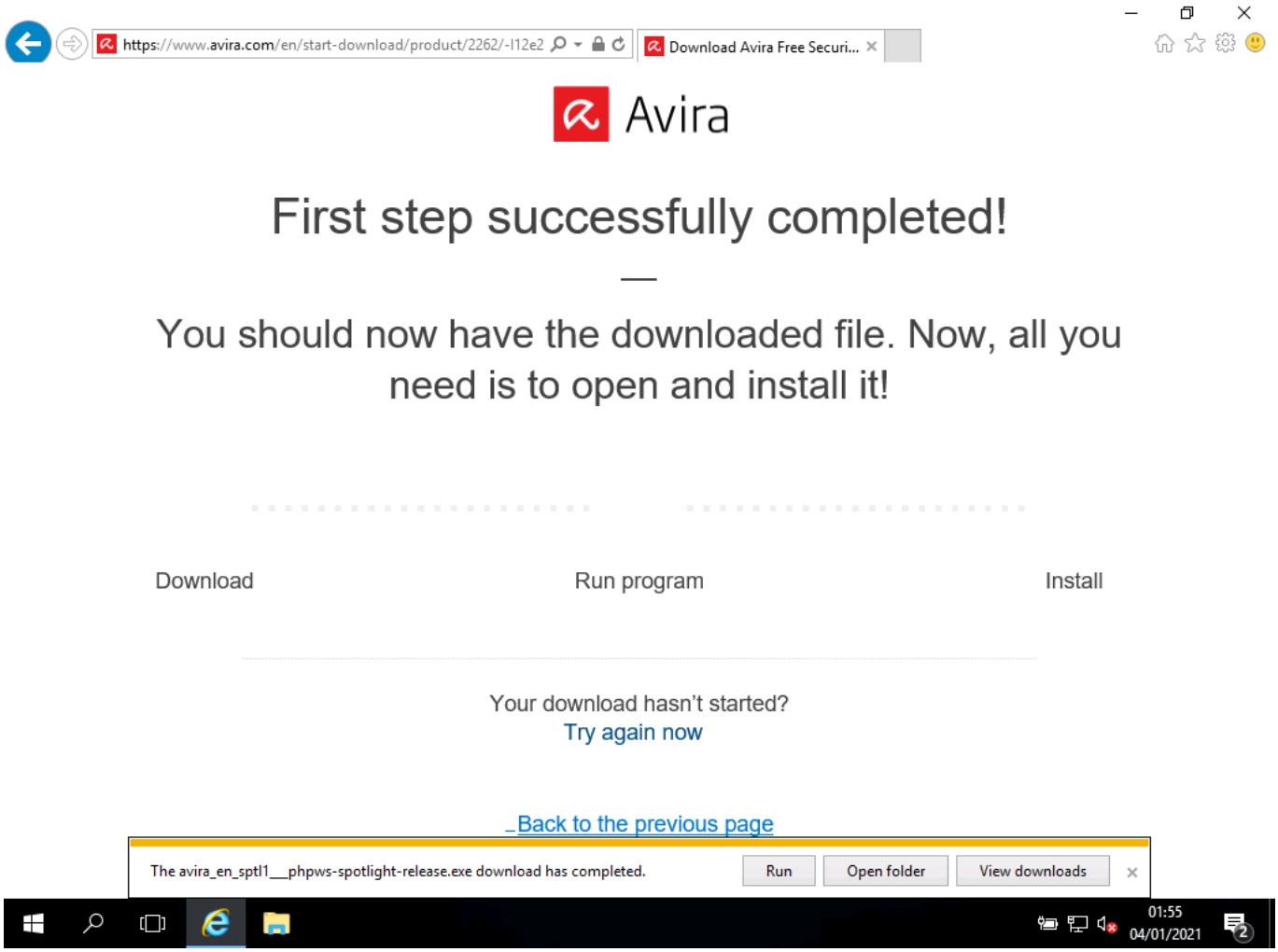
- and here we see the user's properties showing group membership



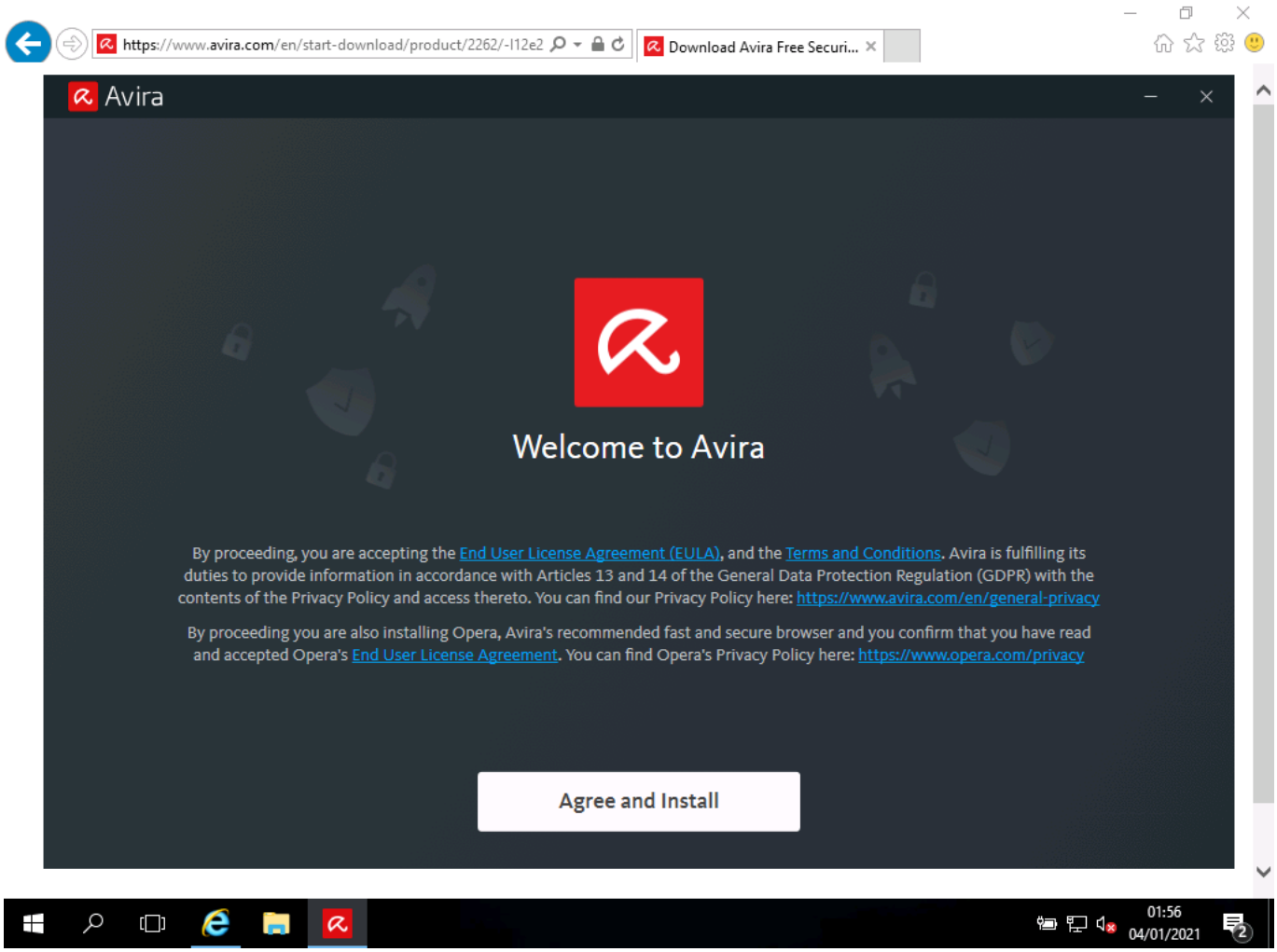
- I click finish to confirm
- I created a user account called dtroke - I have added this account to the domain admin group to allow me to administer computers on the network

Installing security software

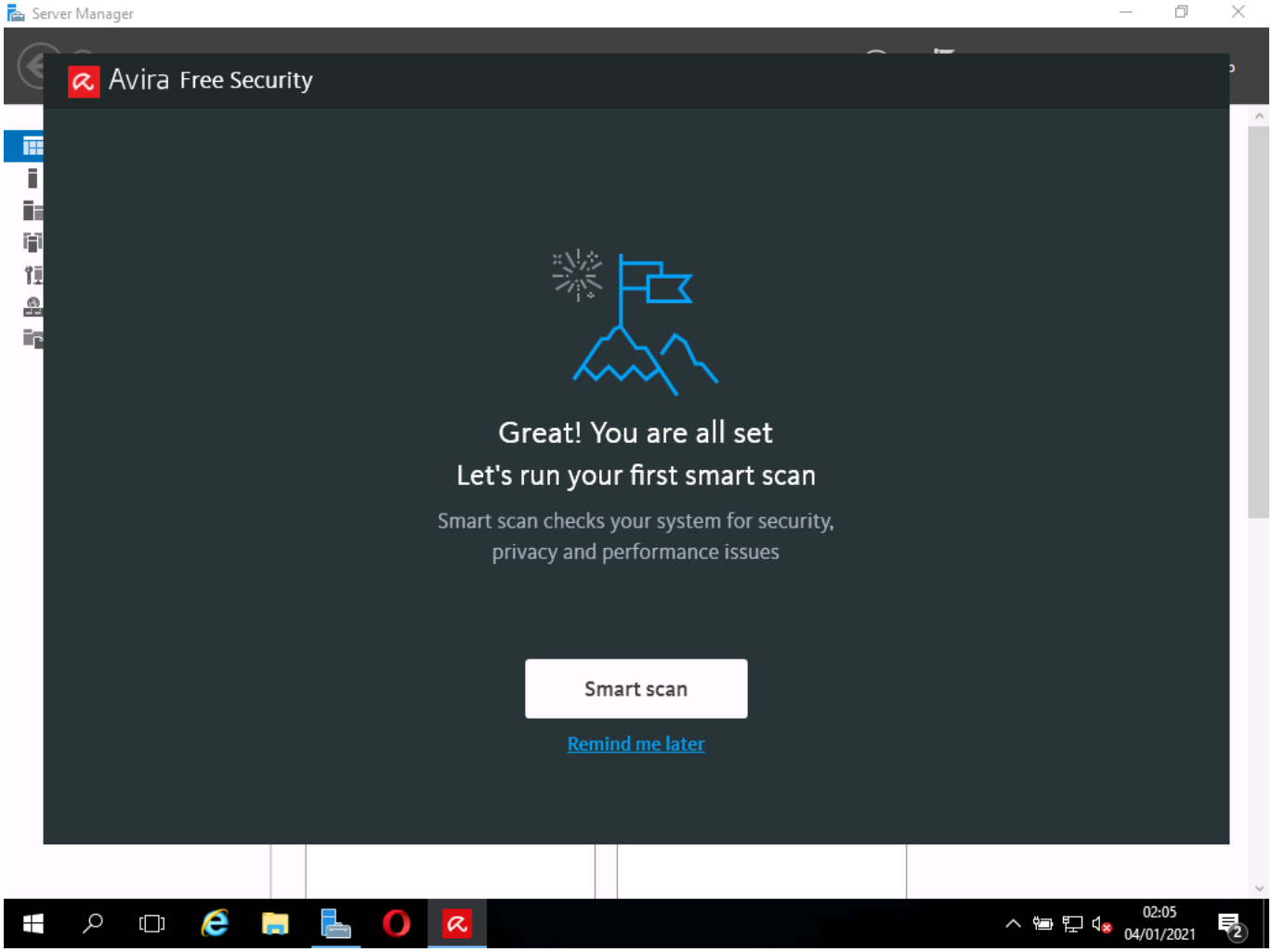
Screenshots:



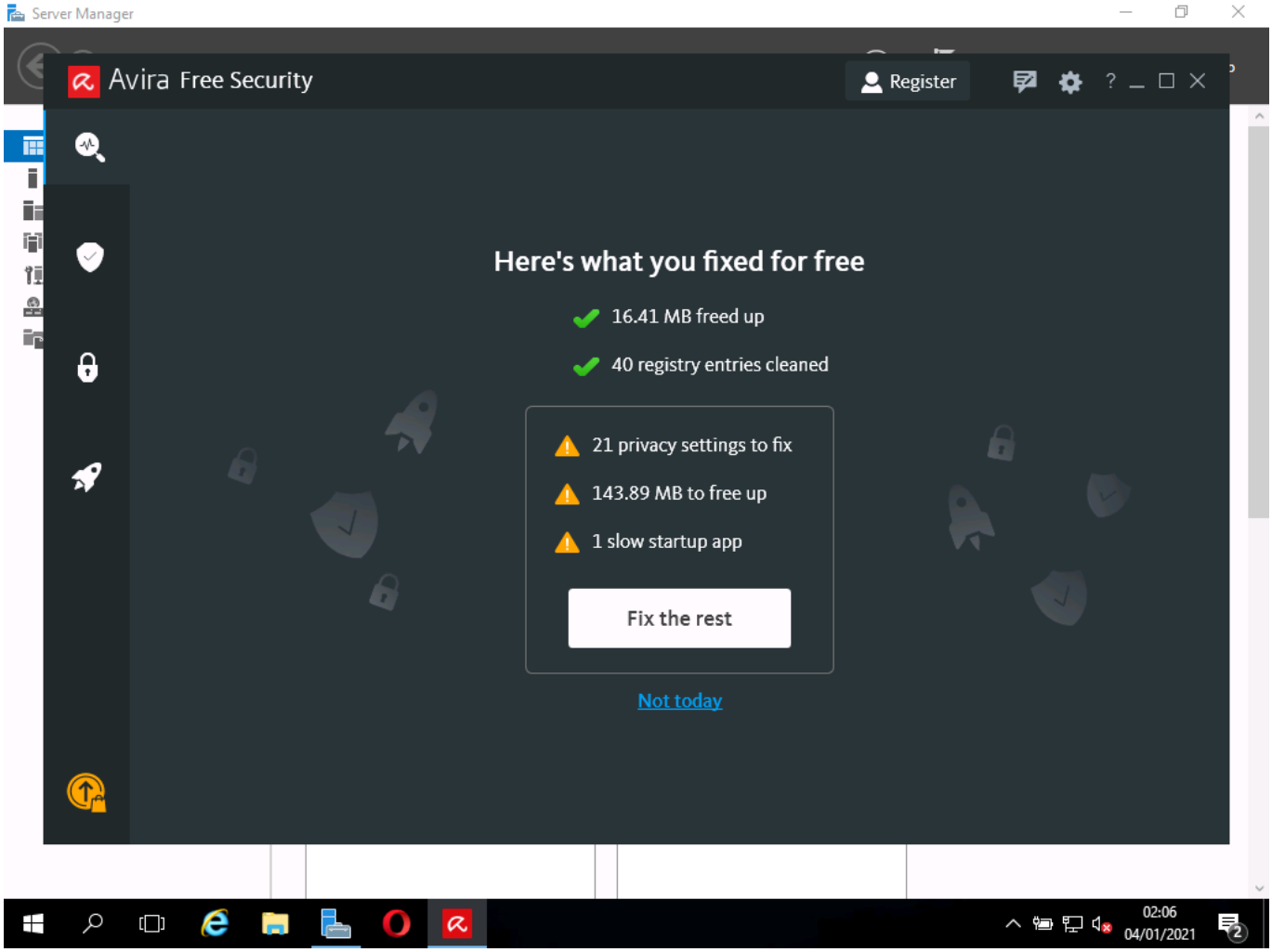
- I navigate to the correct website and download the software I need



- I agree to the licence as required

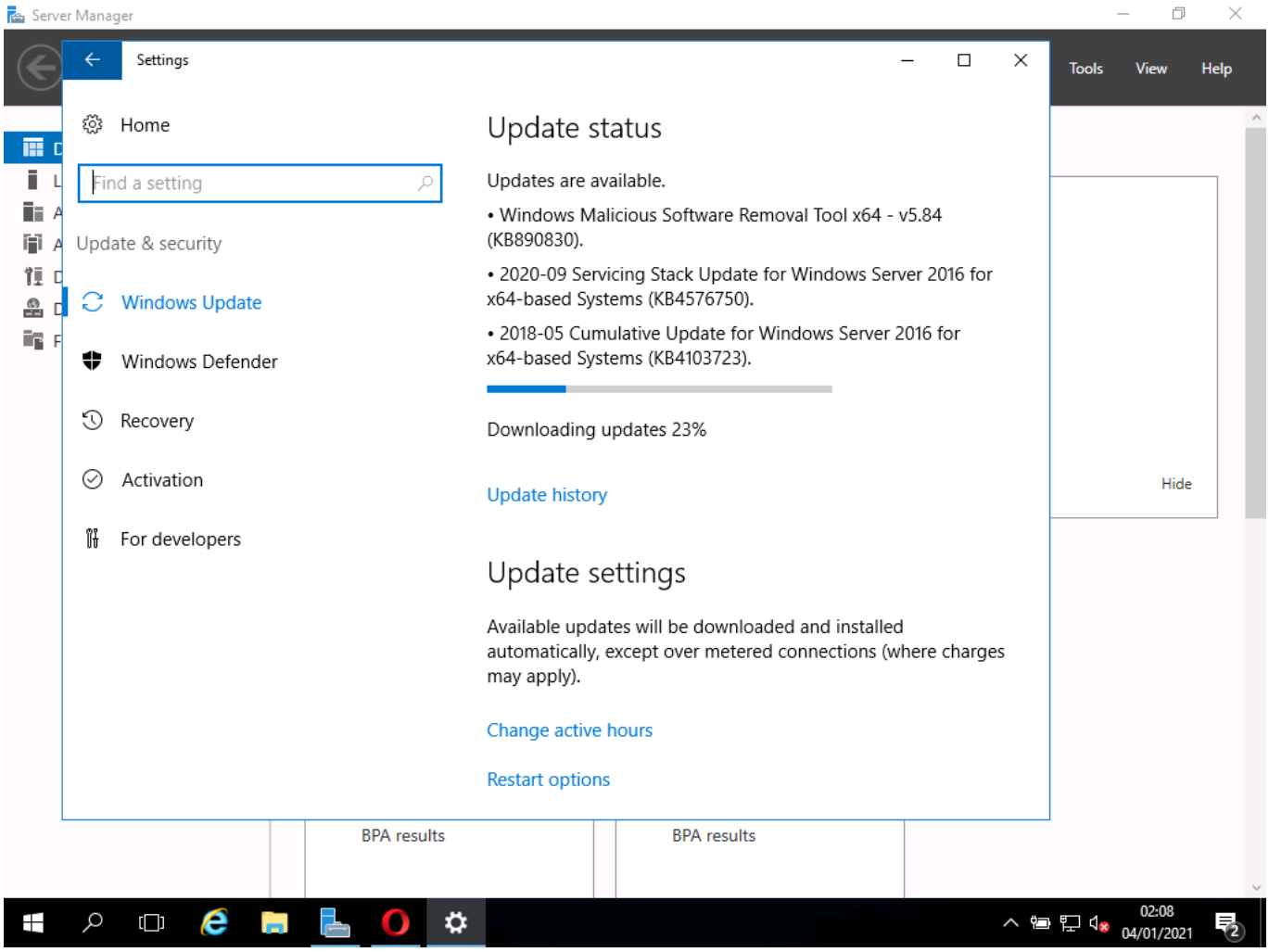


- once installed, I run the first smart scan



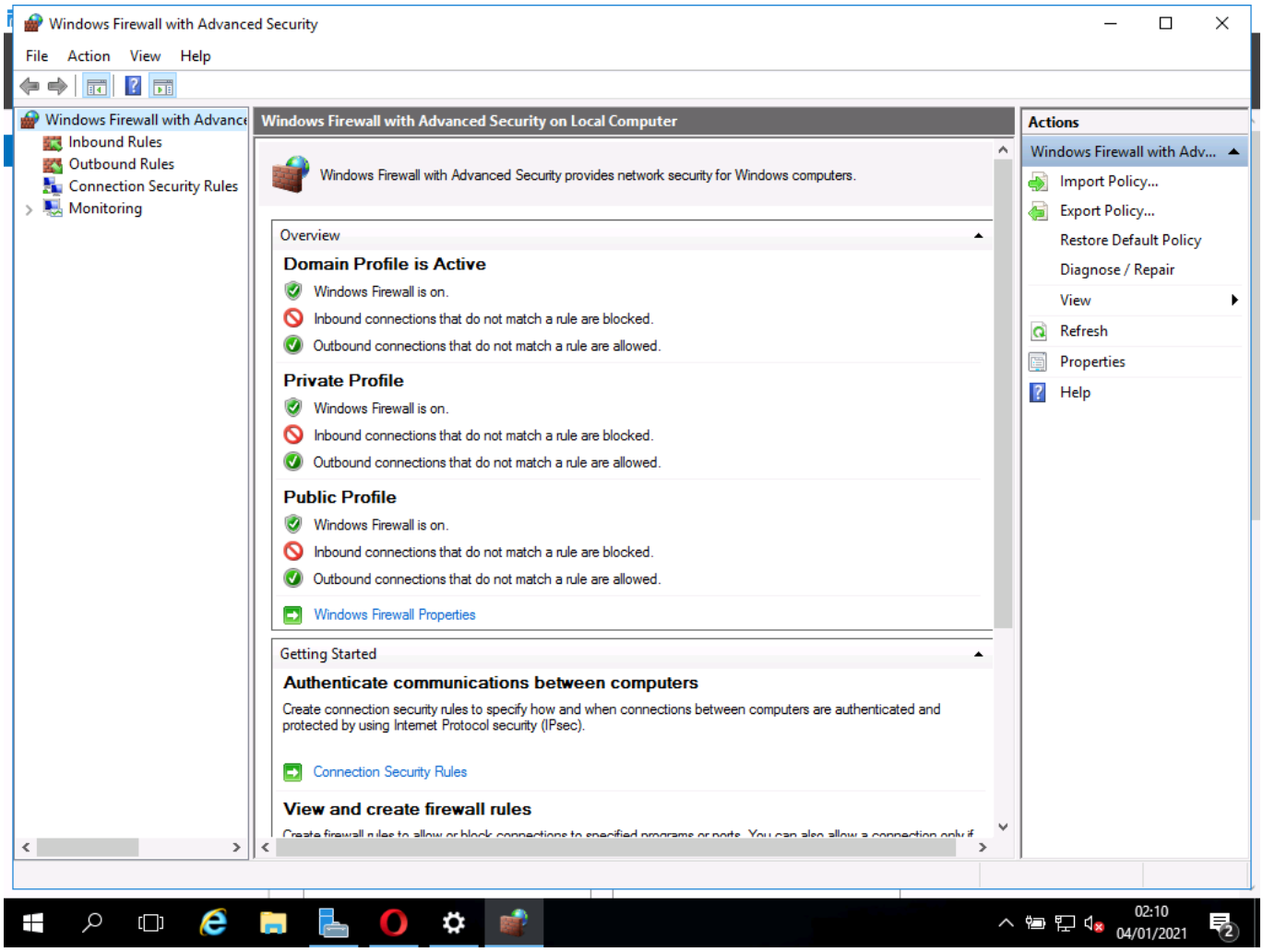
- here are the results for the free software
- to ensure that the server is protected, I have installed antivirus software onto the server and run a scan

Screenshots:



- I have checked and installed any Windows updates to ensure Windows is fully patched to close any vulnerabilities

Screenshots:

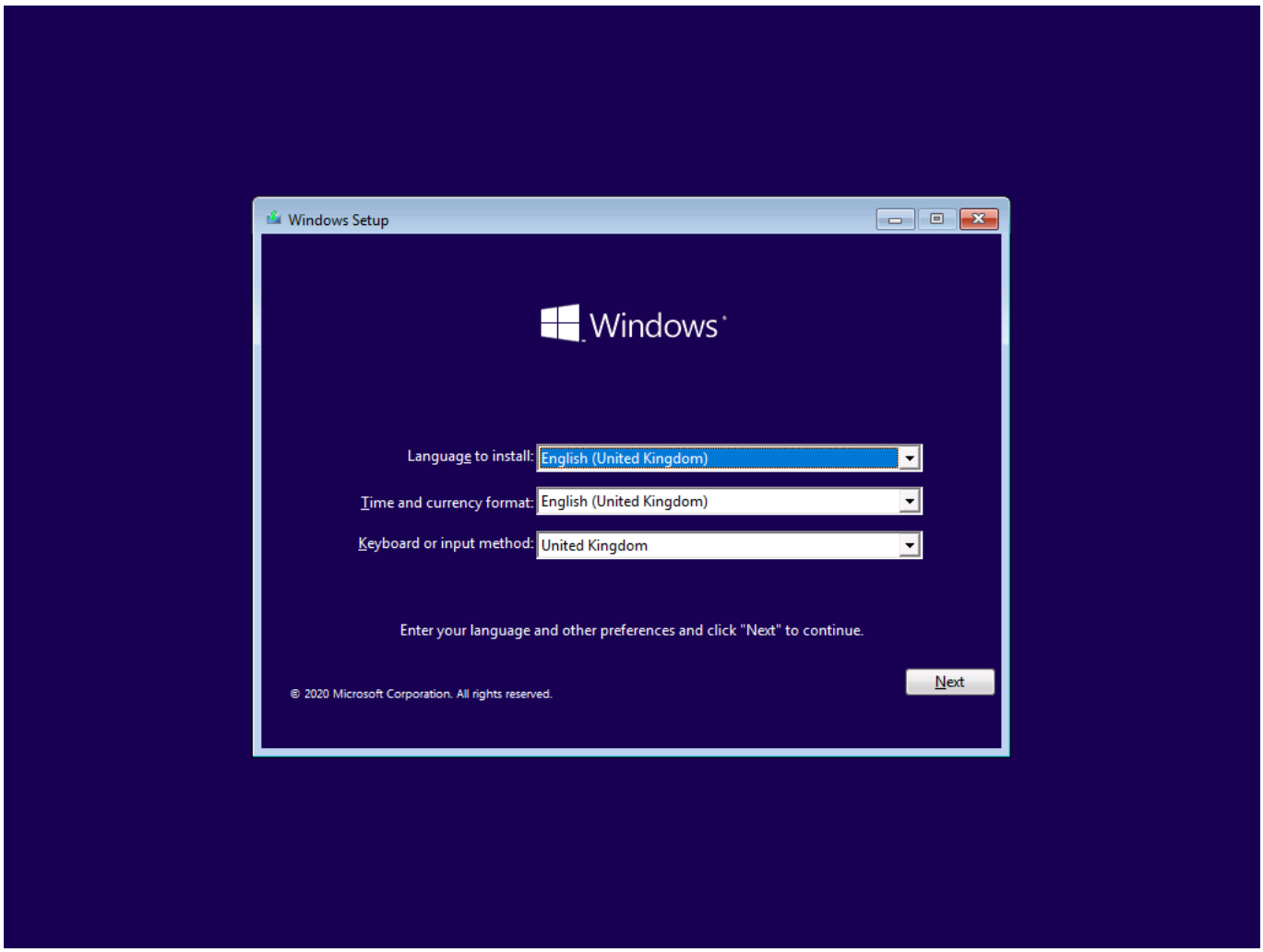


- I have opened Windows firewall to ensure it is enabled and working to protect the server from external attacks

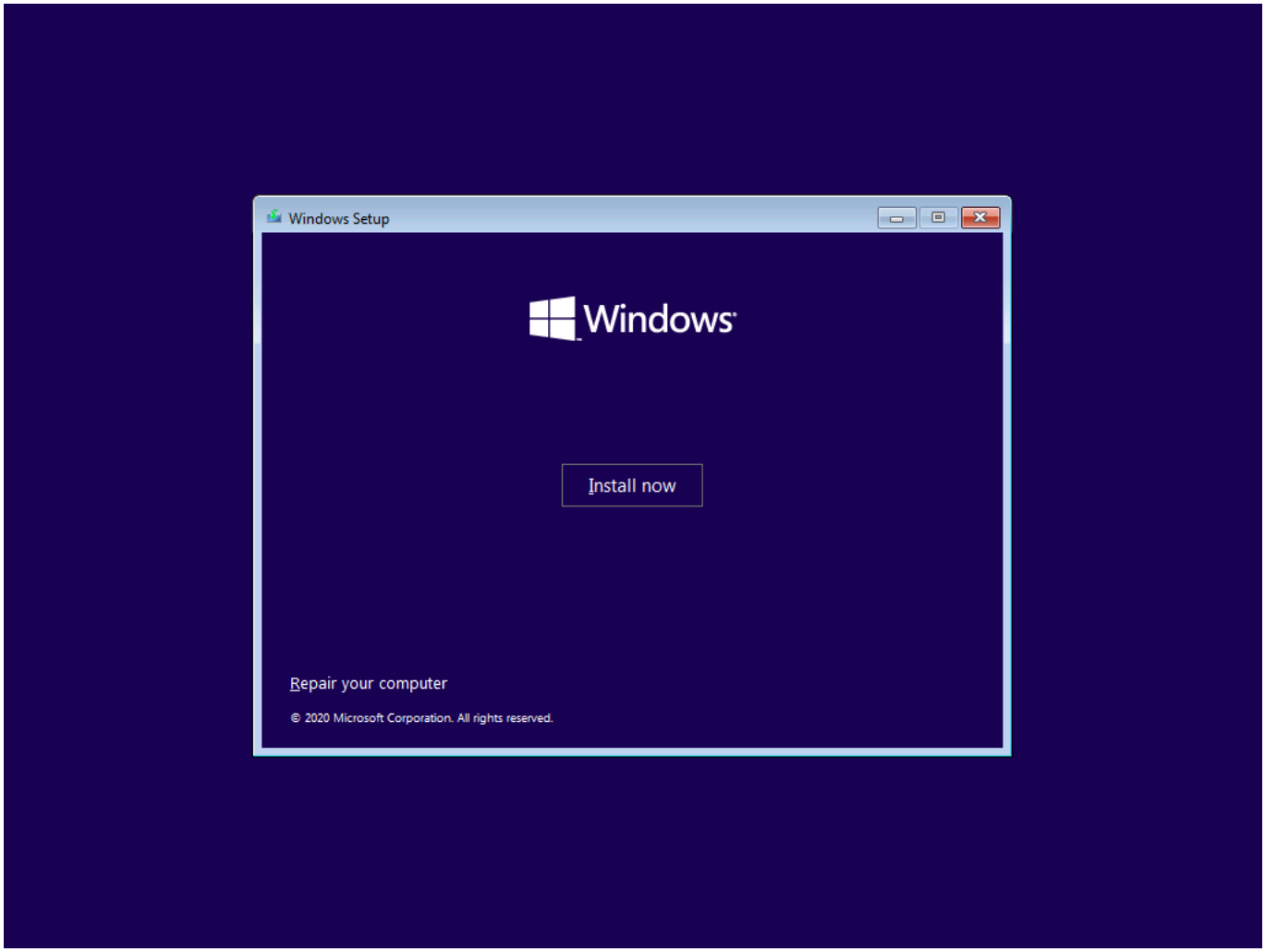
Task 2(b)

Installation of client PC

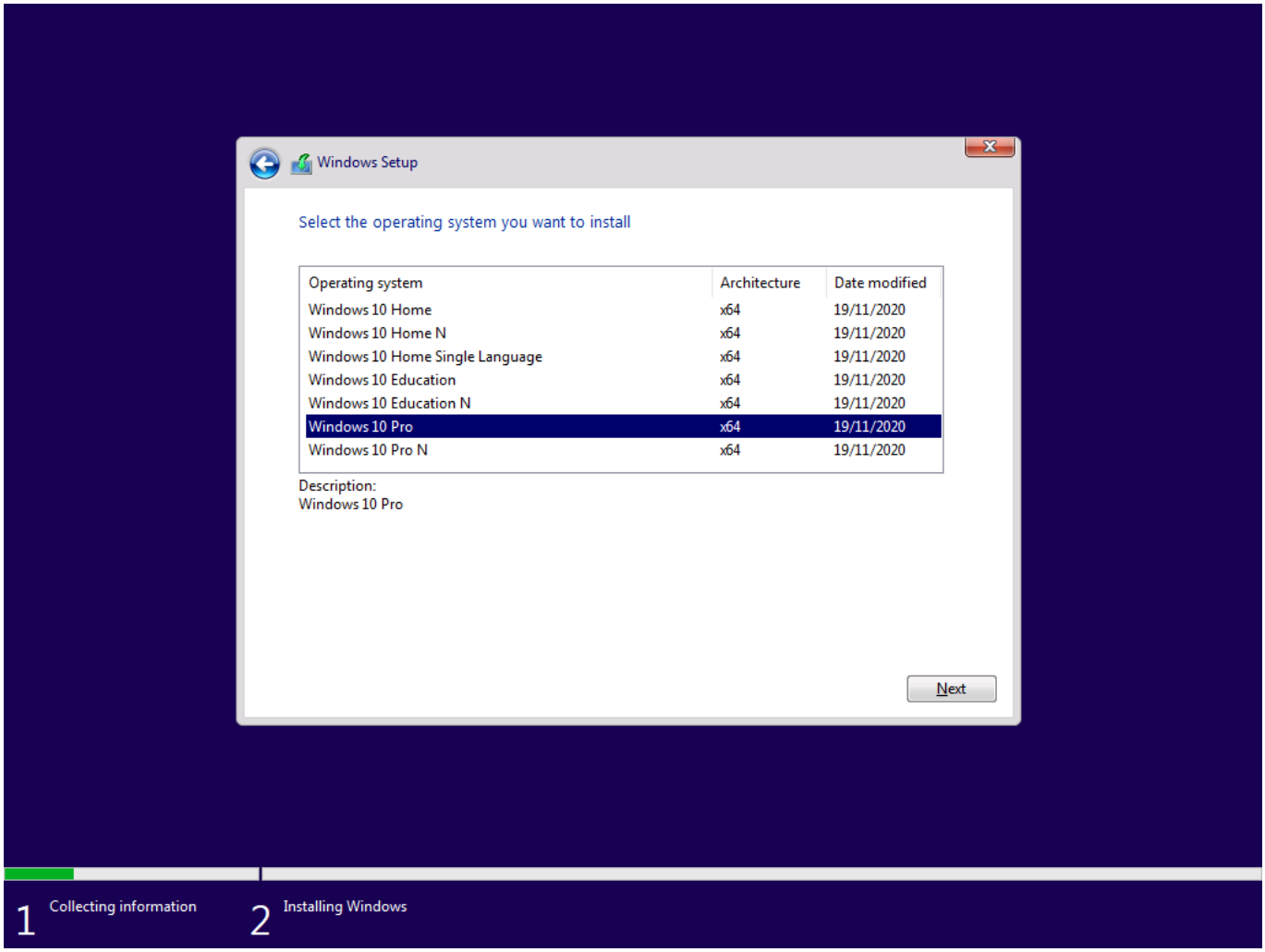
Screenshots:



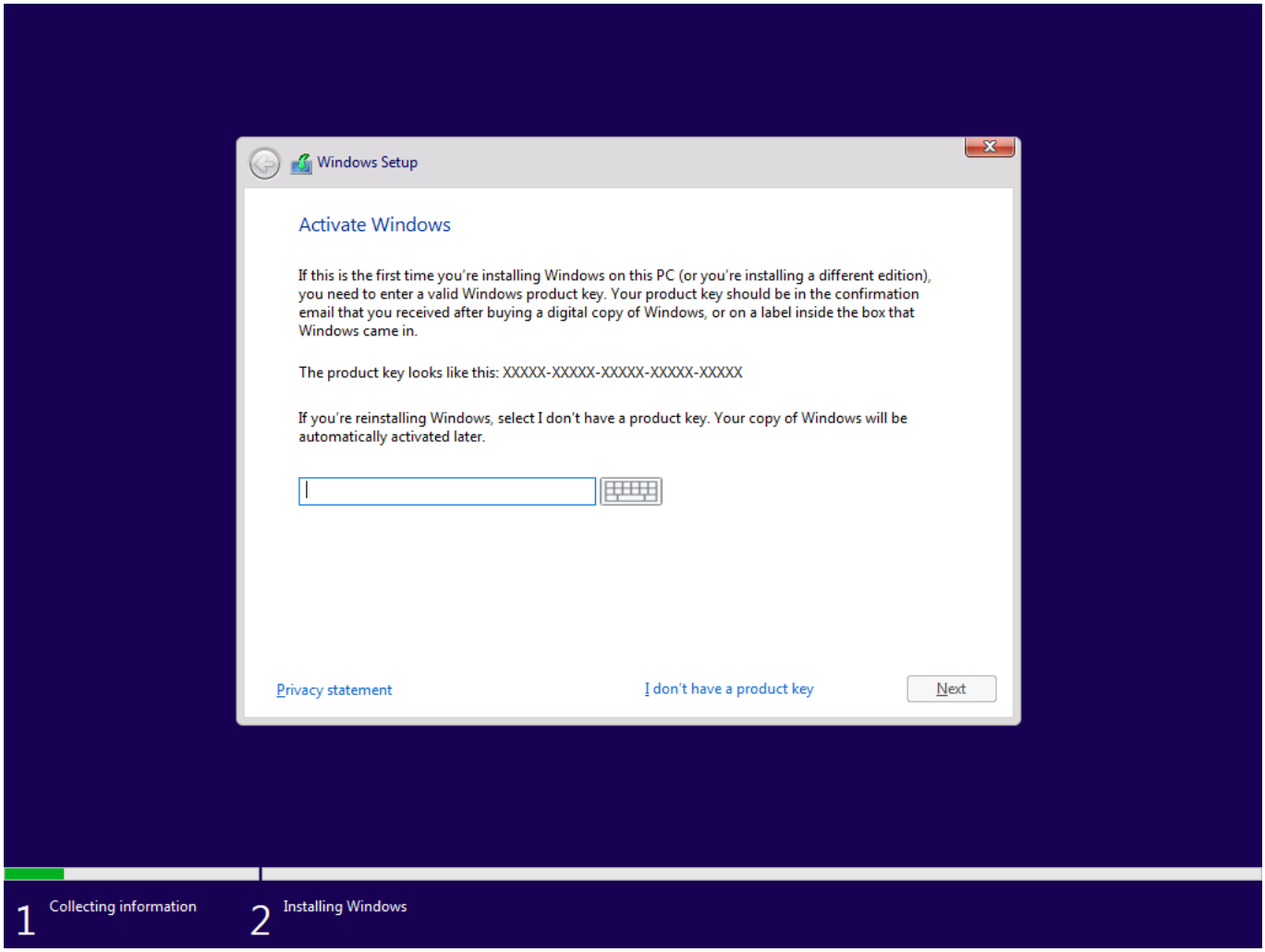
- I first select the installation language, time and currency format and keyboard or input methods to meet the client's needs



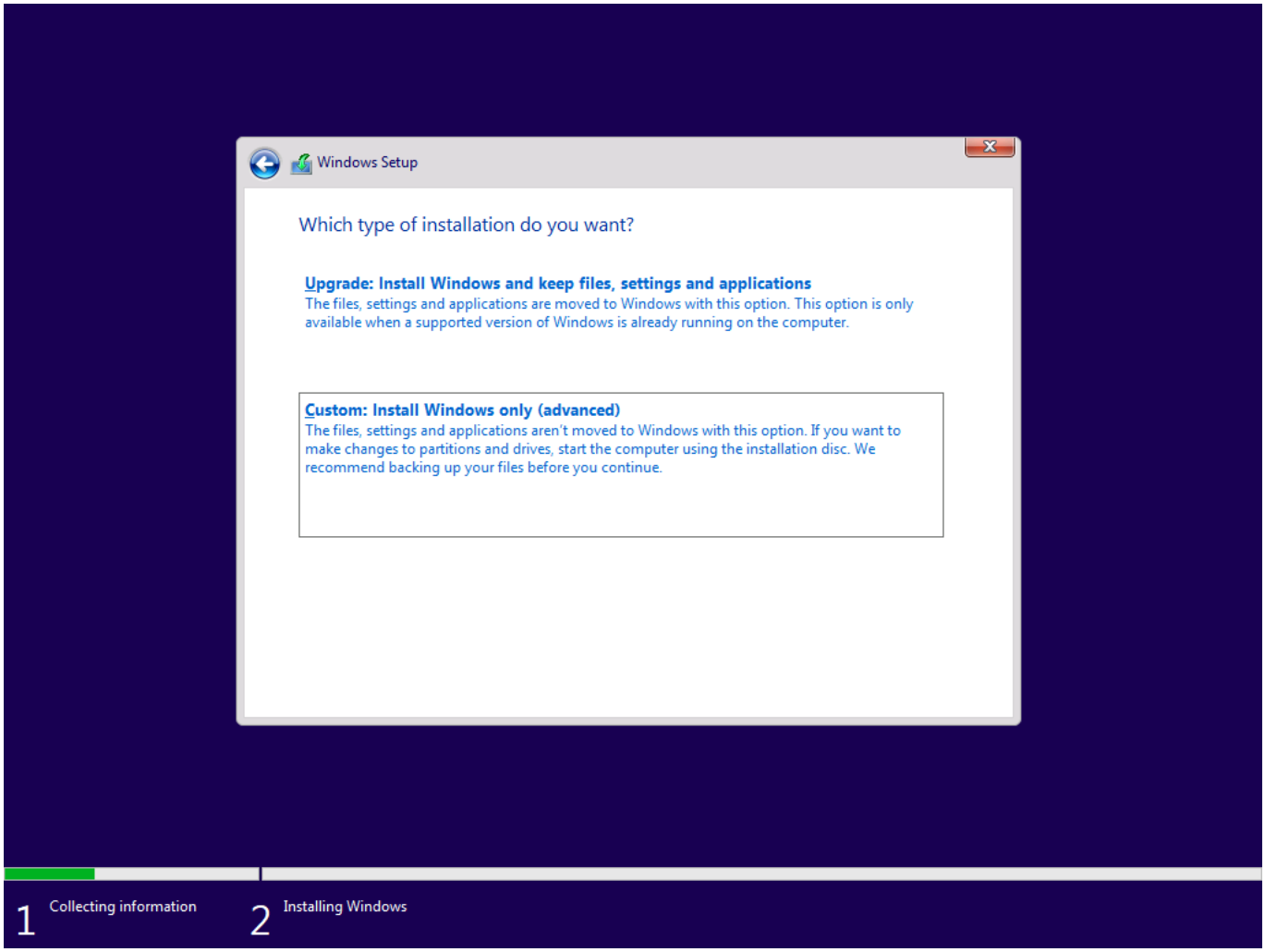
- then I click install



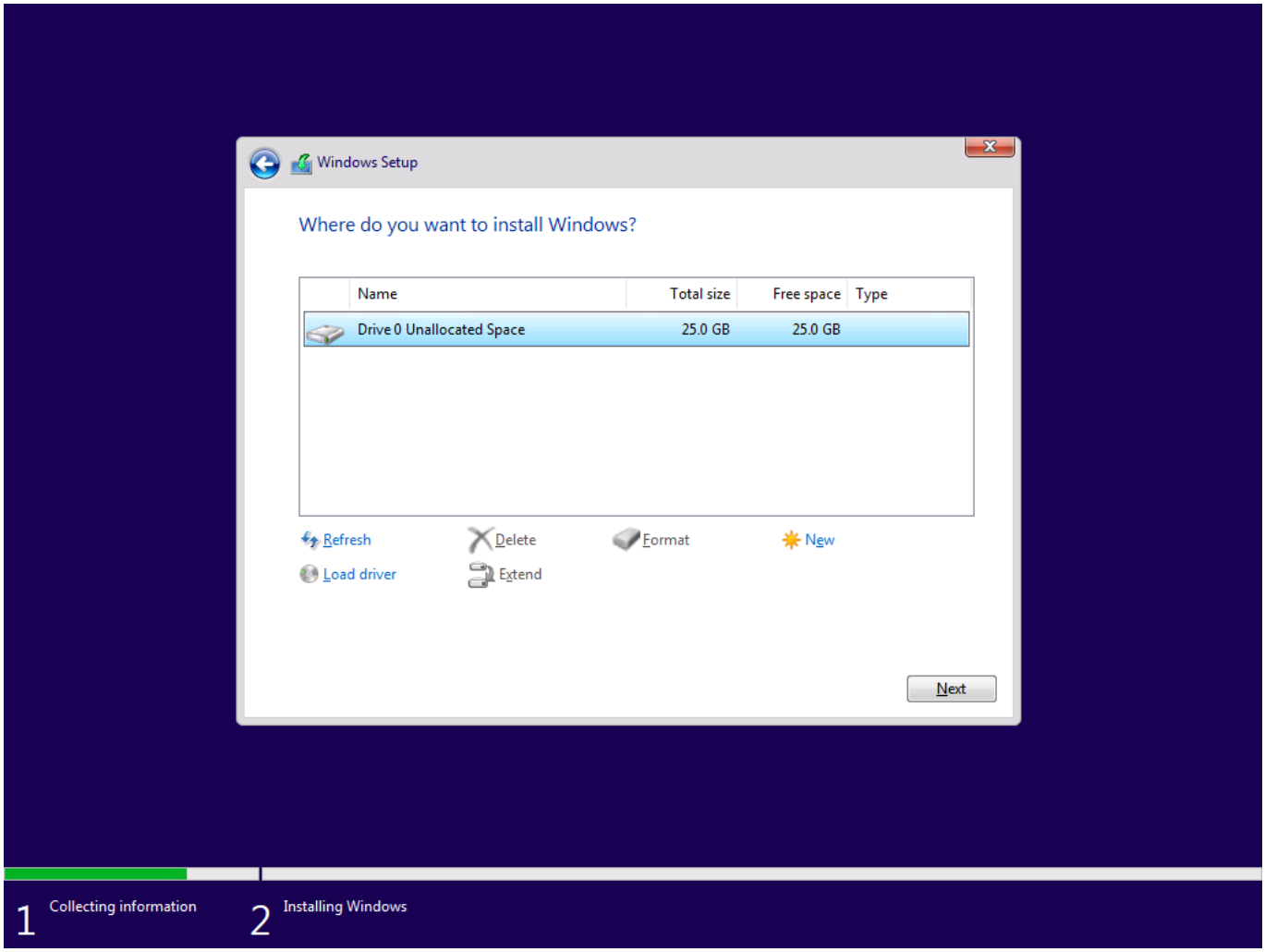
- I select the version of windows I want to install, here I choose Pro as the home versions do not allow connection to a domain



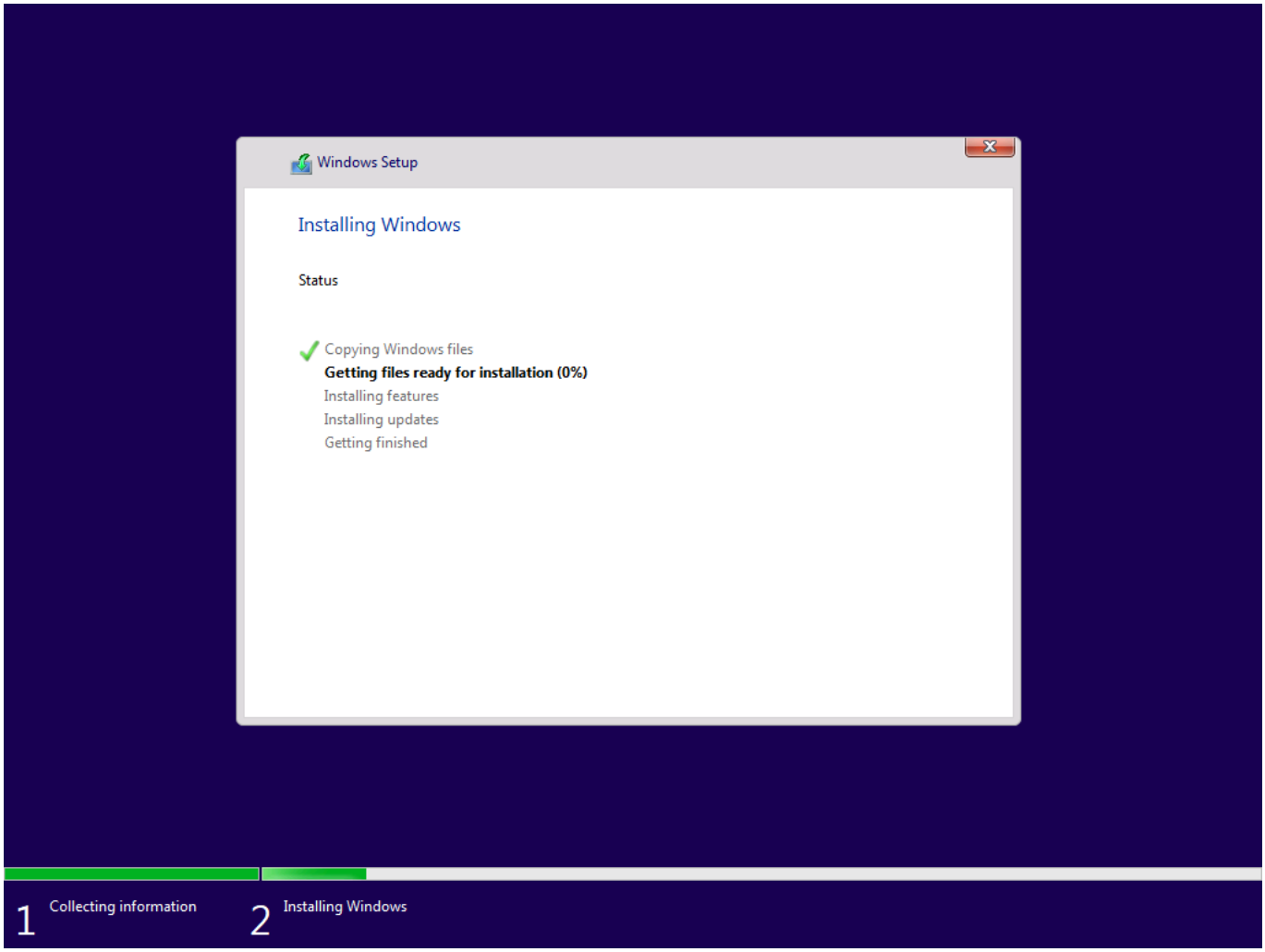
- now I enter the product key



- I choose installation type



- and an installation location

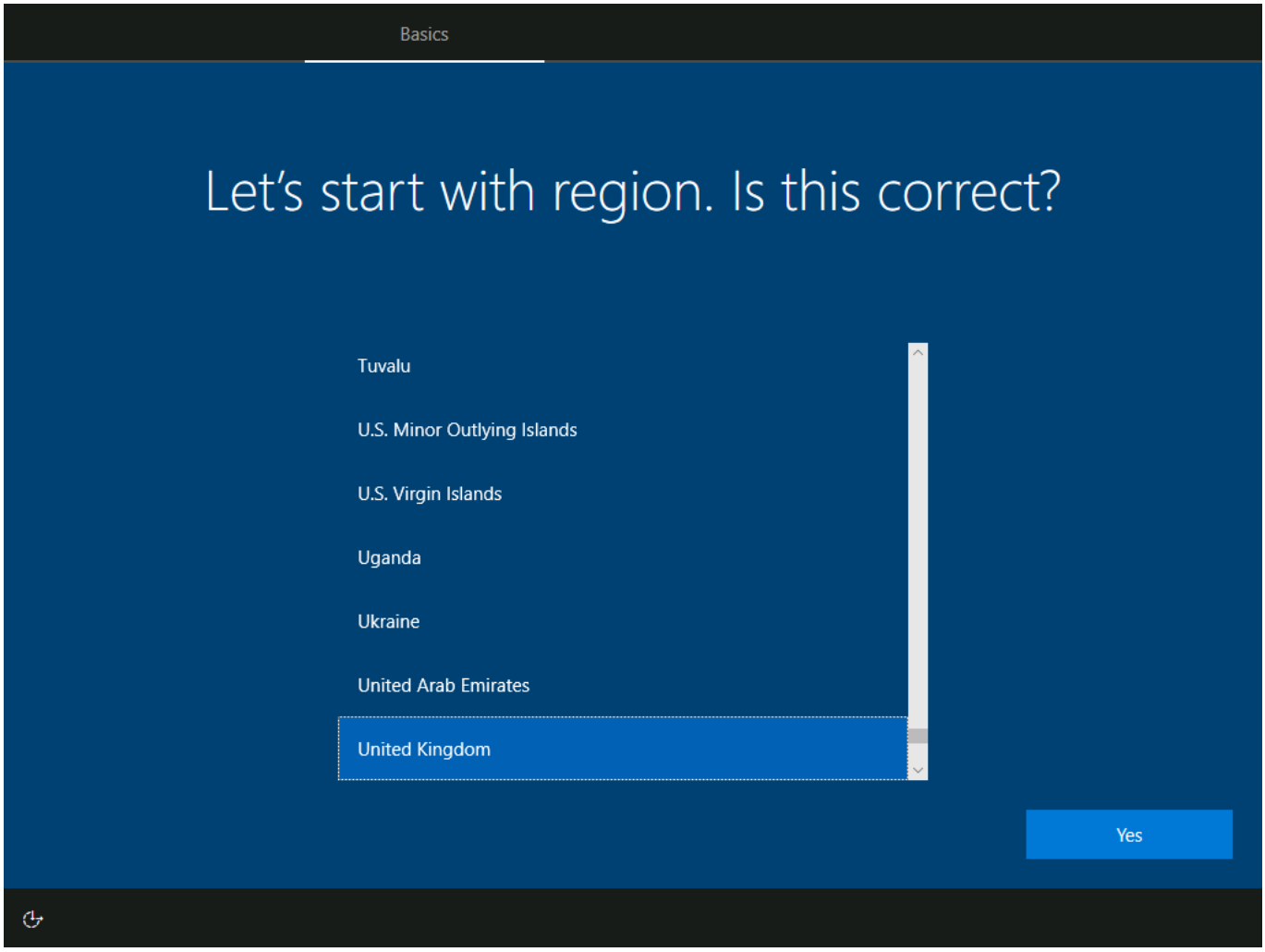


- now Windows installs and I can monitor the progress

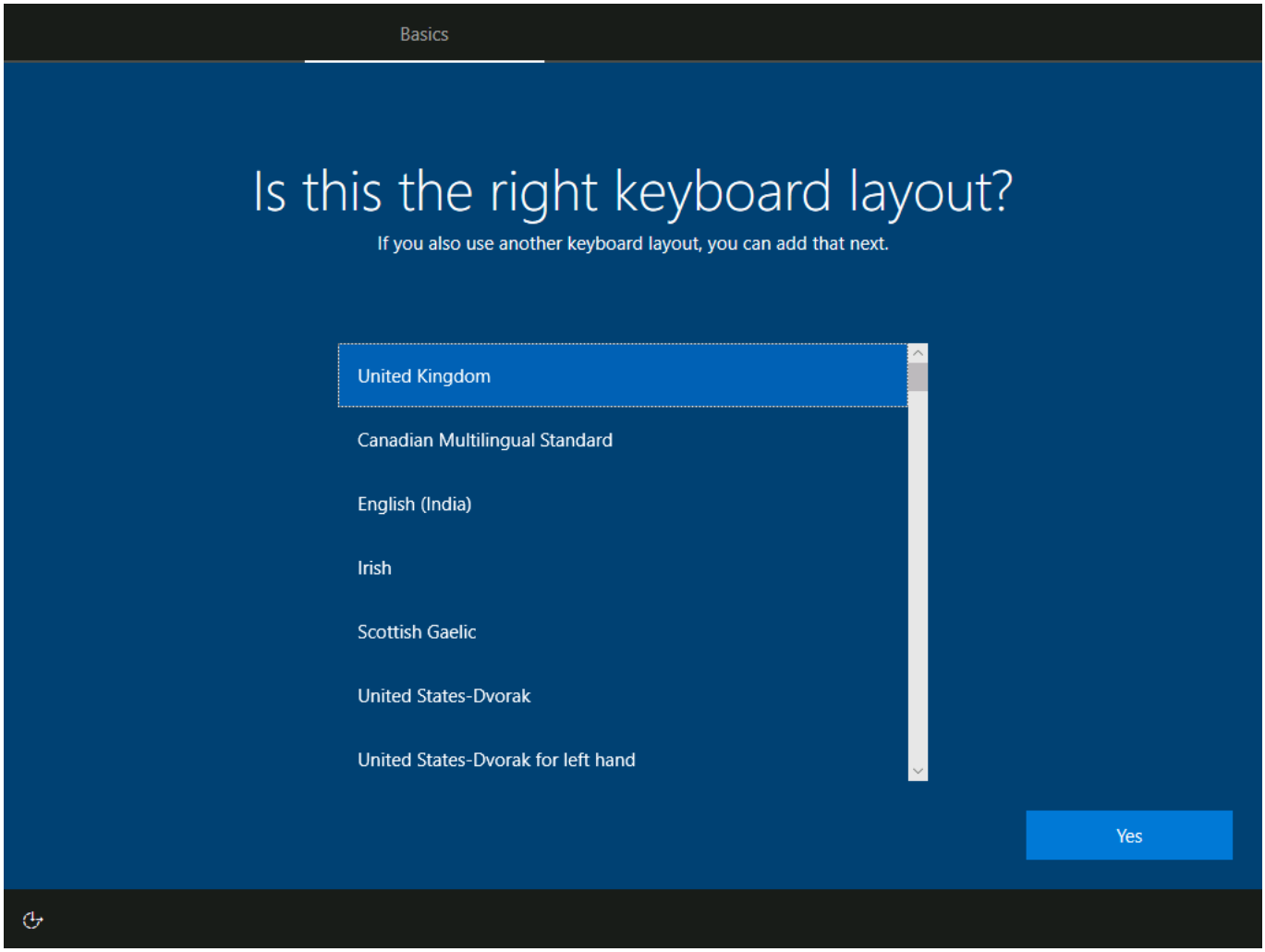
The above screenshots show me installing Windows 10 onto the client computer.

- configuration steps included:
  - selecting UK English as the installation language and keyboard layout
  - inputting Windows 10 product key - I have selected ‘I don’t have a Product Key’ and will input/activate Windows after installation
  - selecting Windows 10 Pro for installation
  - accepting the licence agreement
  - selecting custom installation to perform a clean installation of Windows 10
  - selecting the HDD partition to install Windows into

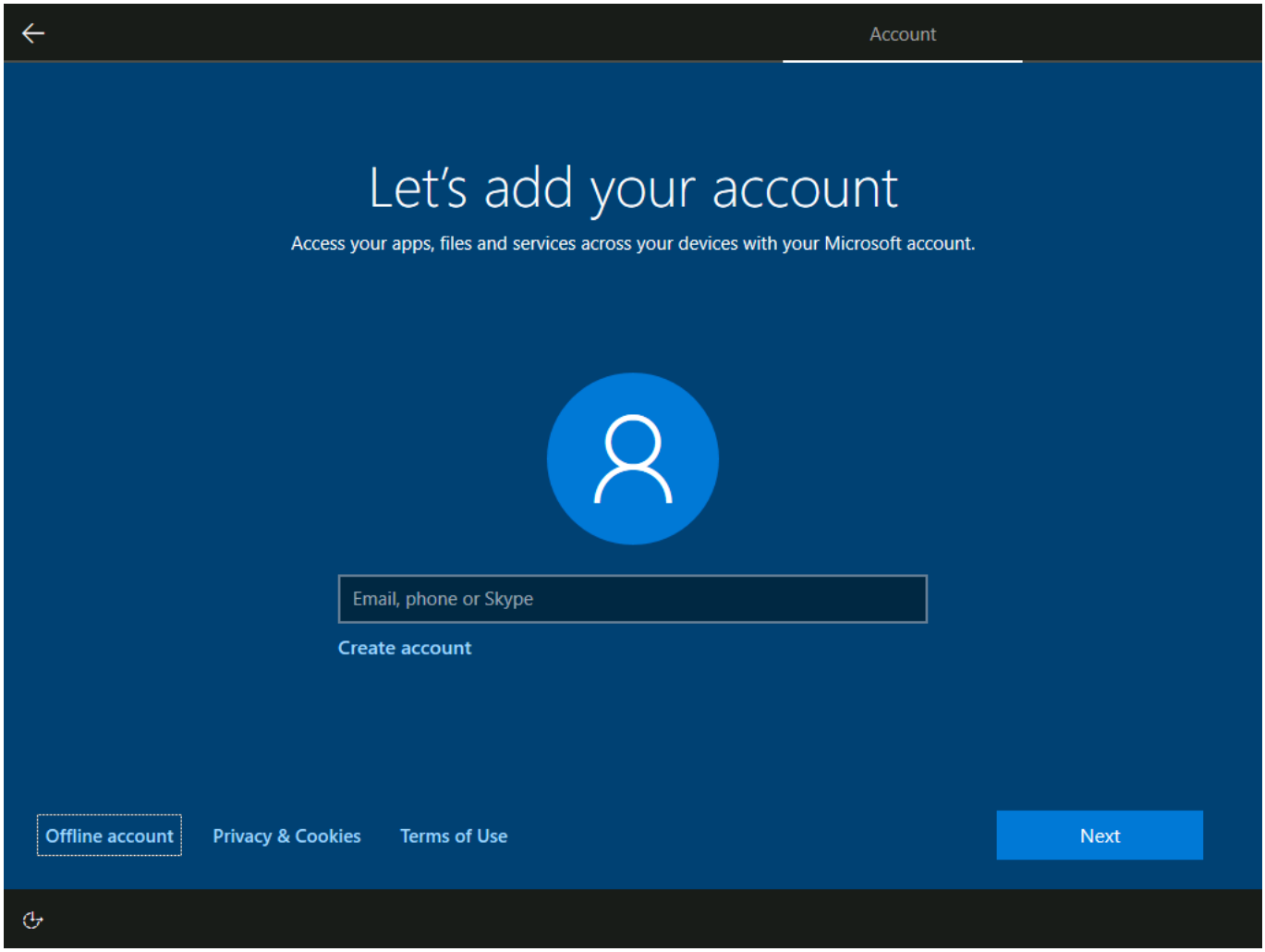
Screenshots:



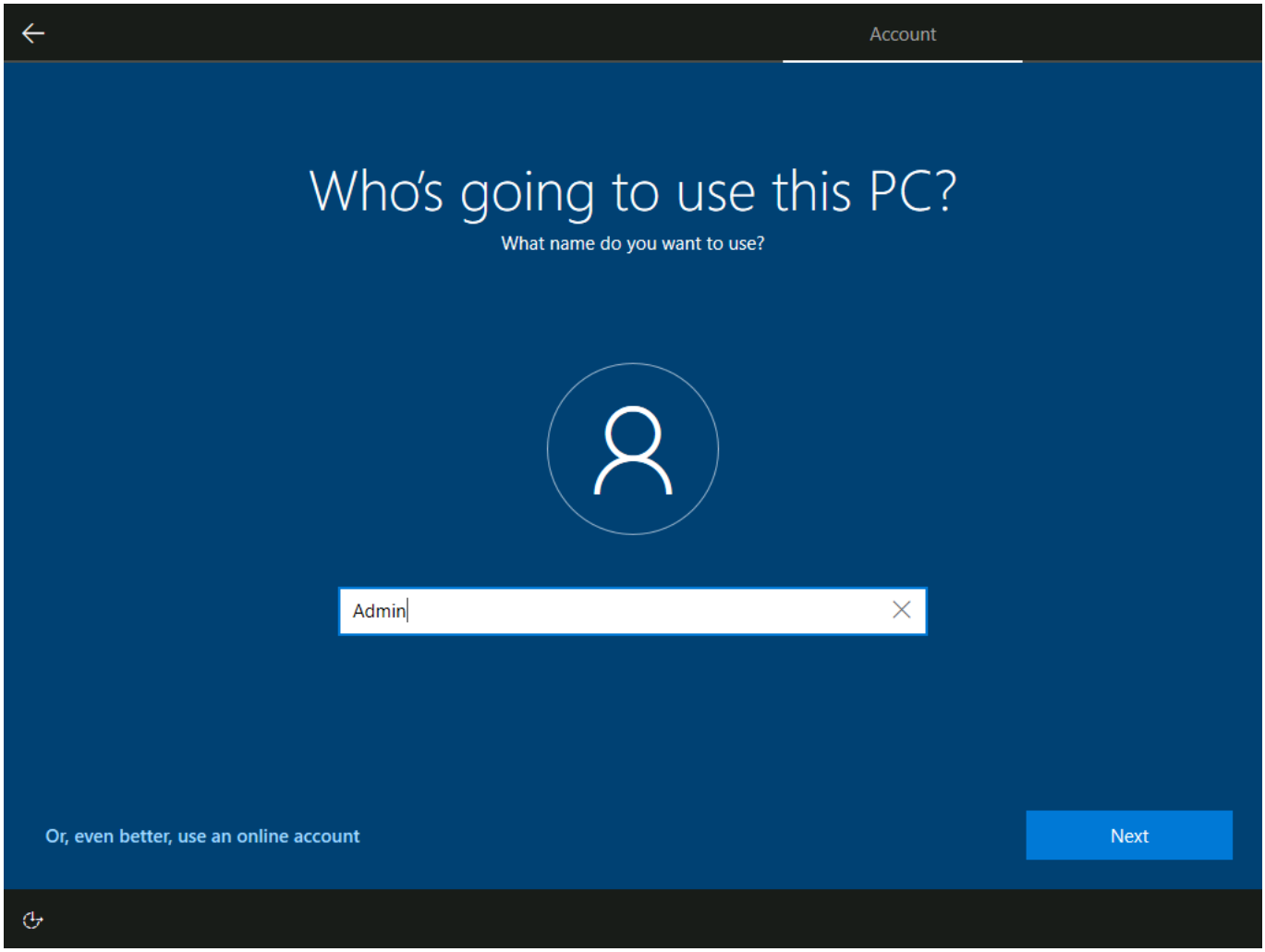
- once installed, I need to select my location



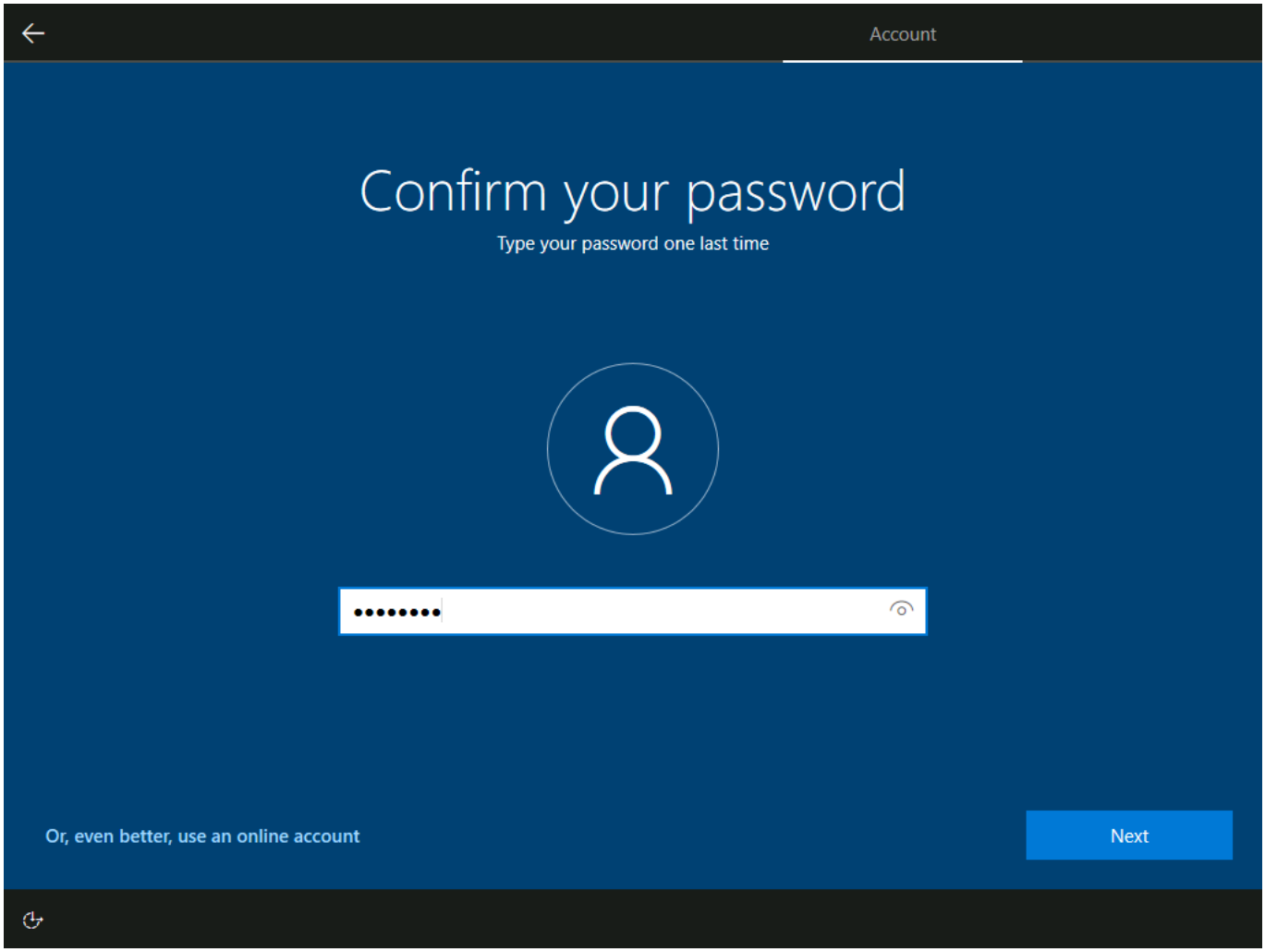
- I select the keyboard layout



- now I can add an initial account



- I enter the initial username as Admin

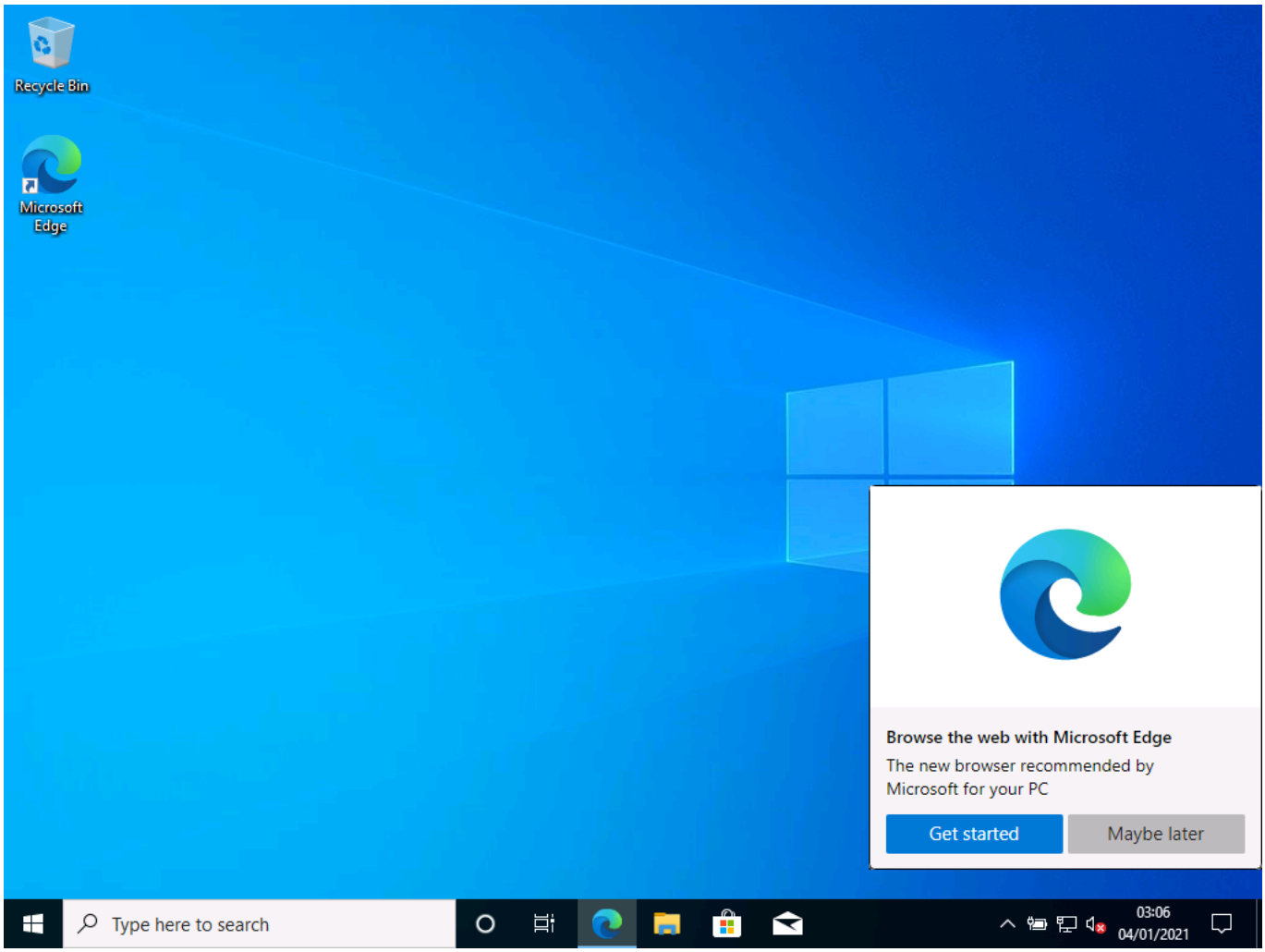


- and I choose a password for security

The above screenshots show me performing the initial configuration for first use of Windows 10.

- configuration steps included:
  - selecting region (UK) and input language (British English)
  - creation of local user account (admin) with a complex password (ionsiTyp!2)

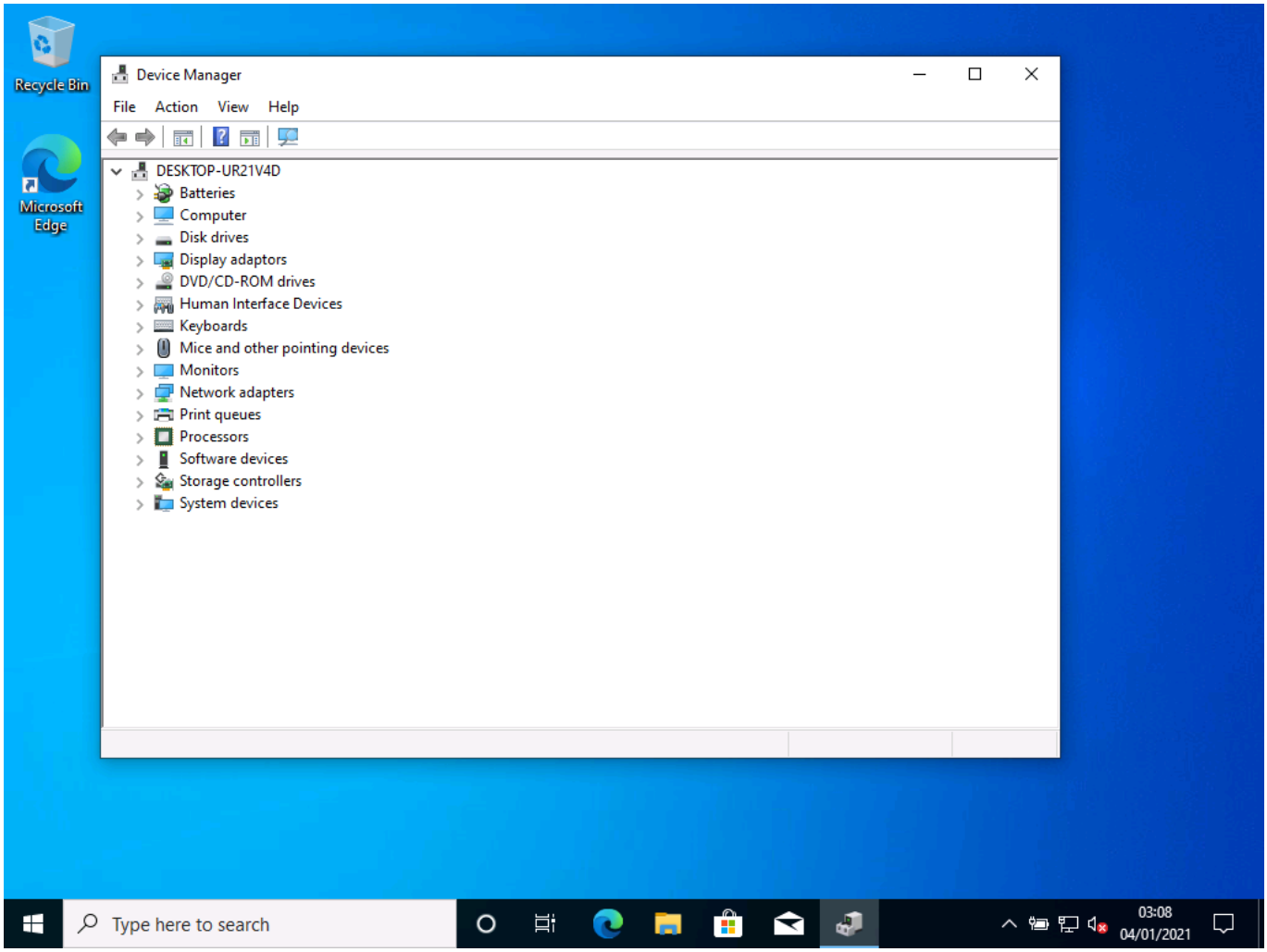
Screenshot:



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

Checking device drivers

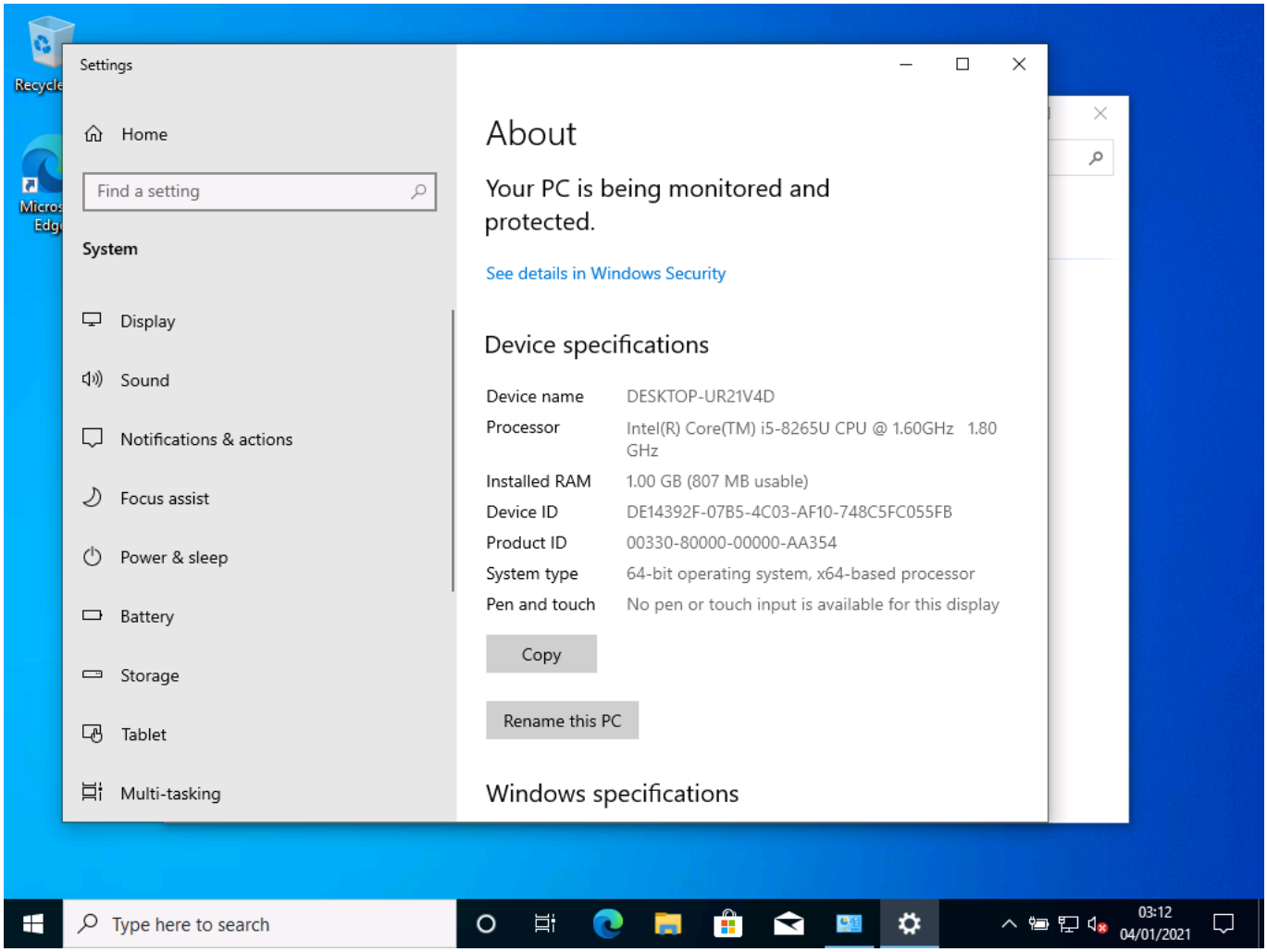
Screenshot:



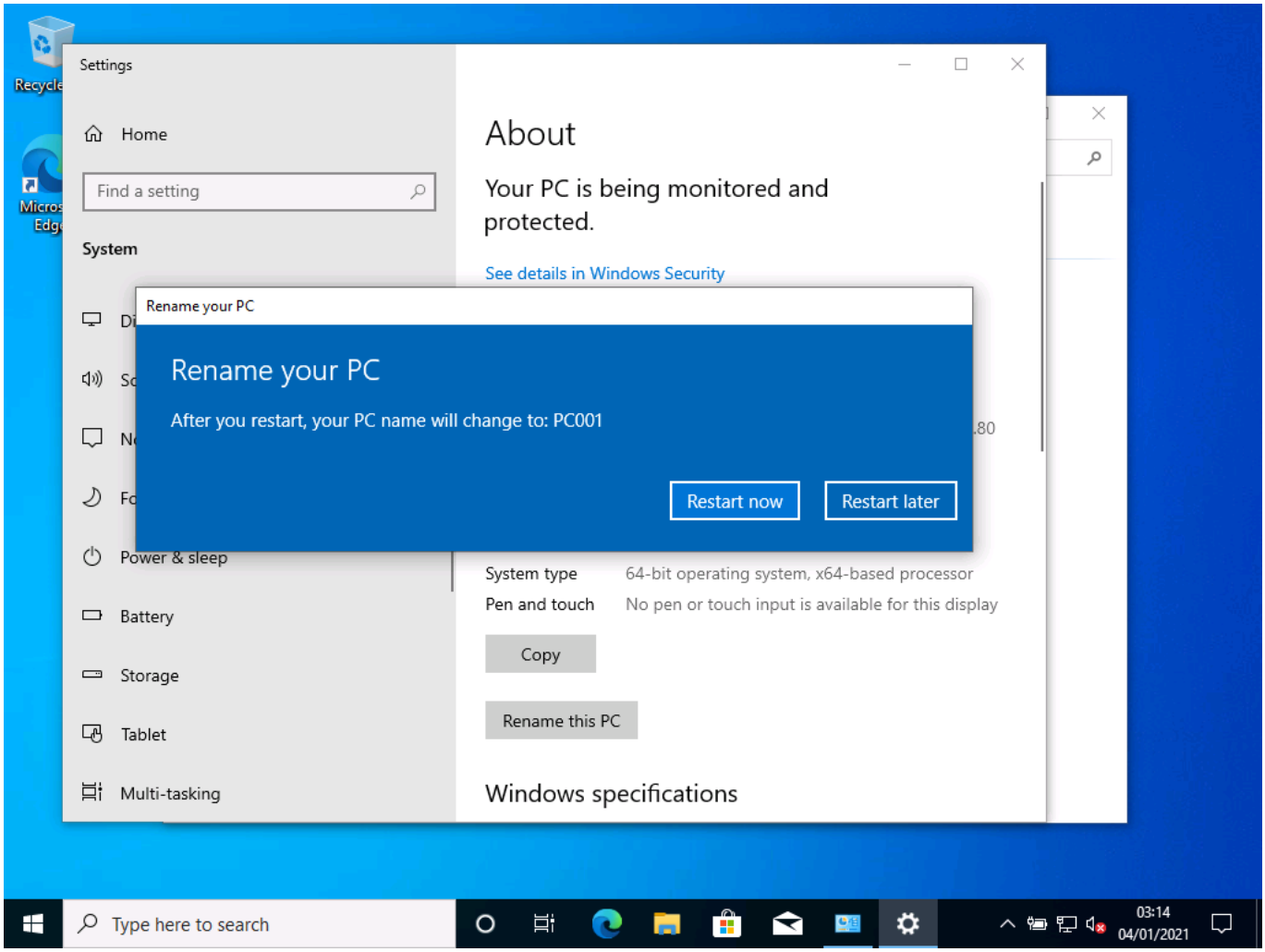
- I have logged into device manager on the computer and identified that all drivers have been installed correctly as part of the Windows installation process

Network configuration/domain joining

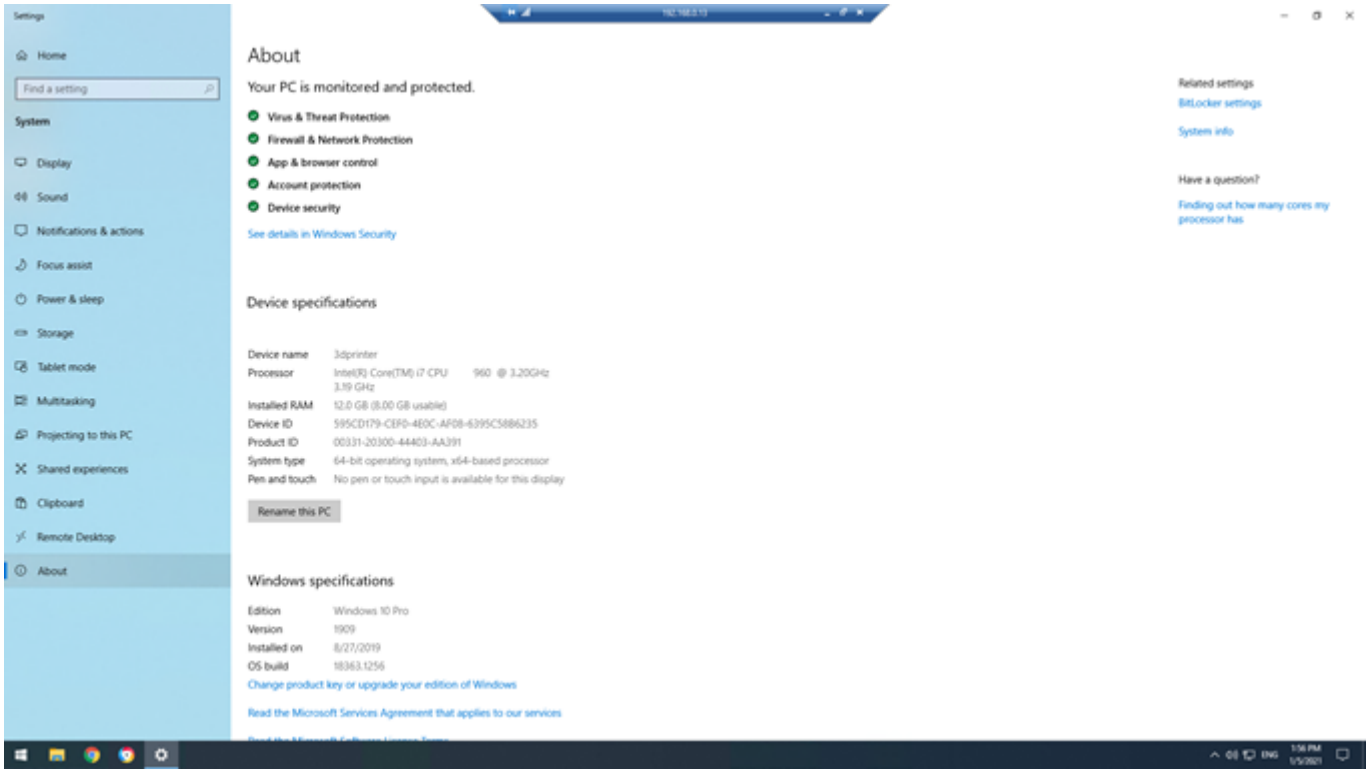
Screenshots:



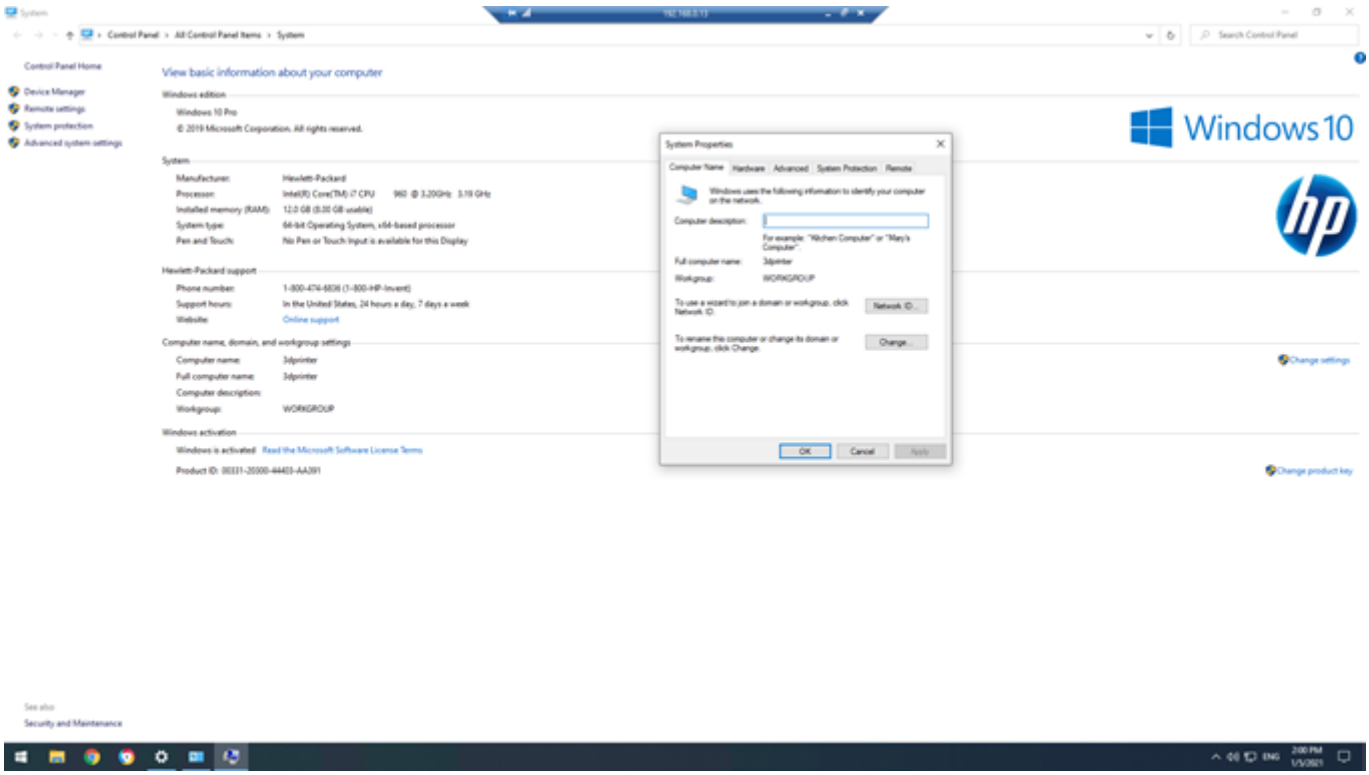
- I select rename PC and give it a name so that it is easy to recognise

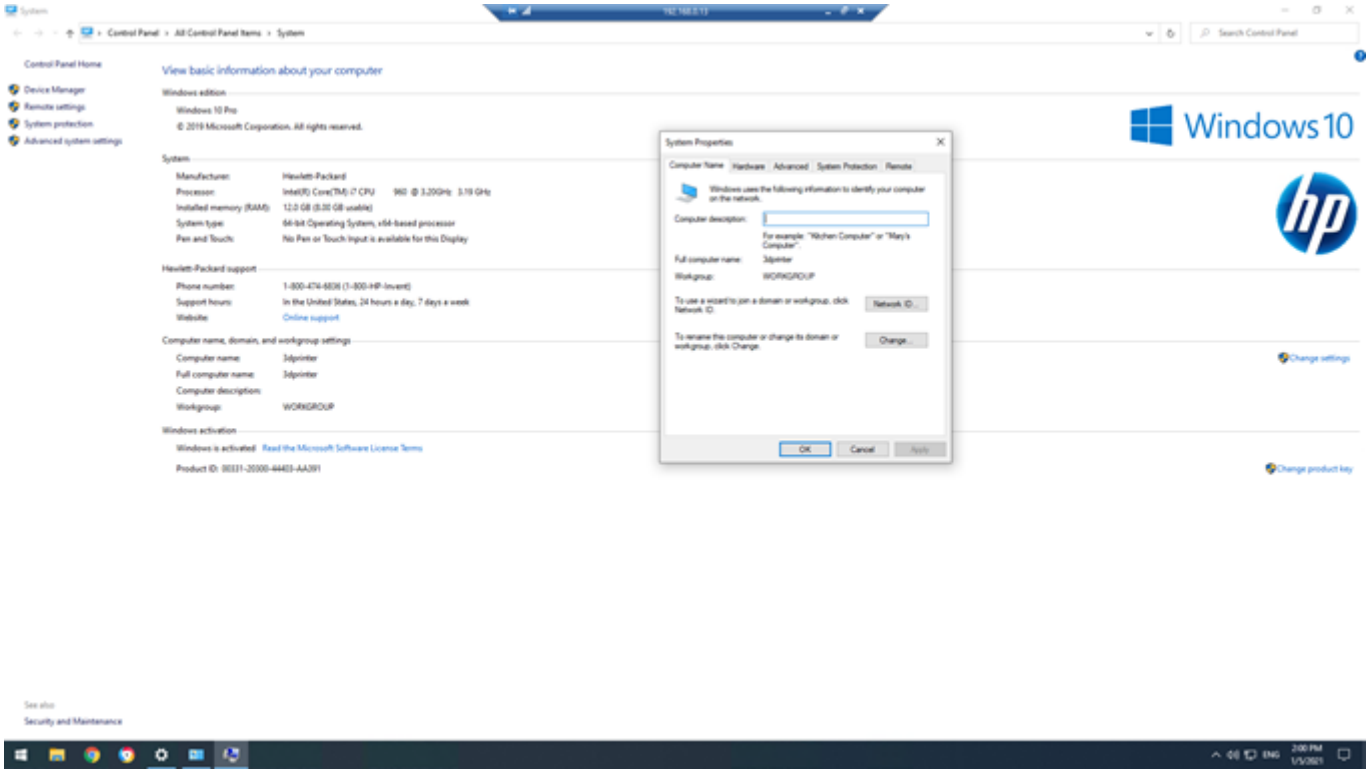


- I then need to restart for the name change to become effective



- once restarted, I can add the PC to the domain I created

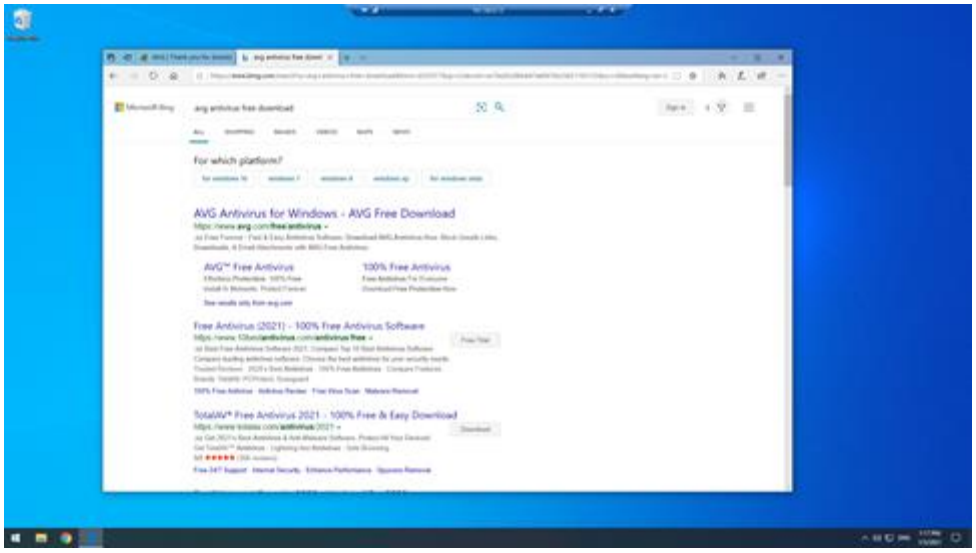




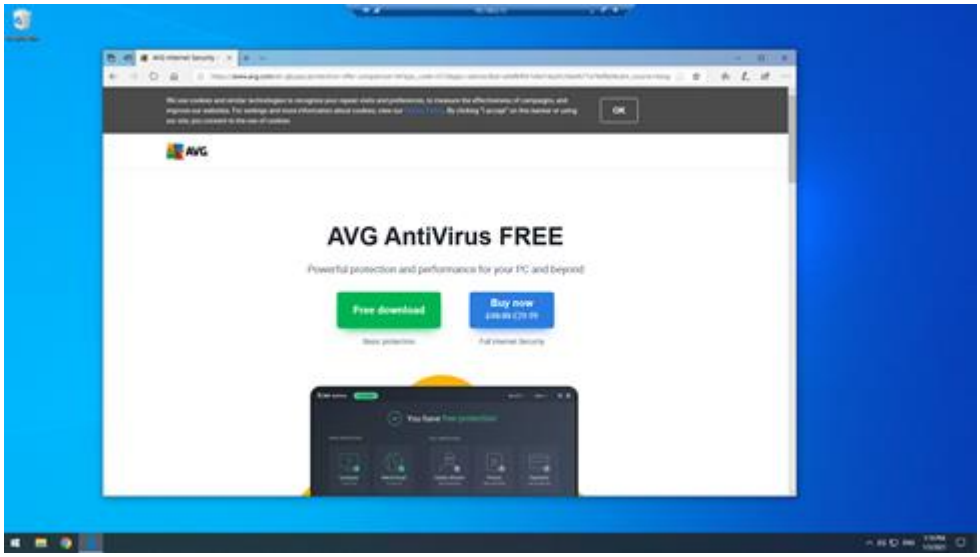
- here I type the name of the domain I want to join
- I have updated the computer name of the client to be PC01 in line with the network installation plan, I have also joined the MyDomain.local, using the domain admin account dtroke when prompted
- after joining the domain, the computer has rebooted and I can now log in with my domain user account - I will log in with the dtroke account as this is a domain admin account and will allow me to install software as well as finish configuring the workstation

Security and installation of antivirus software

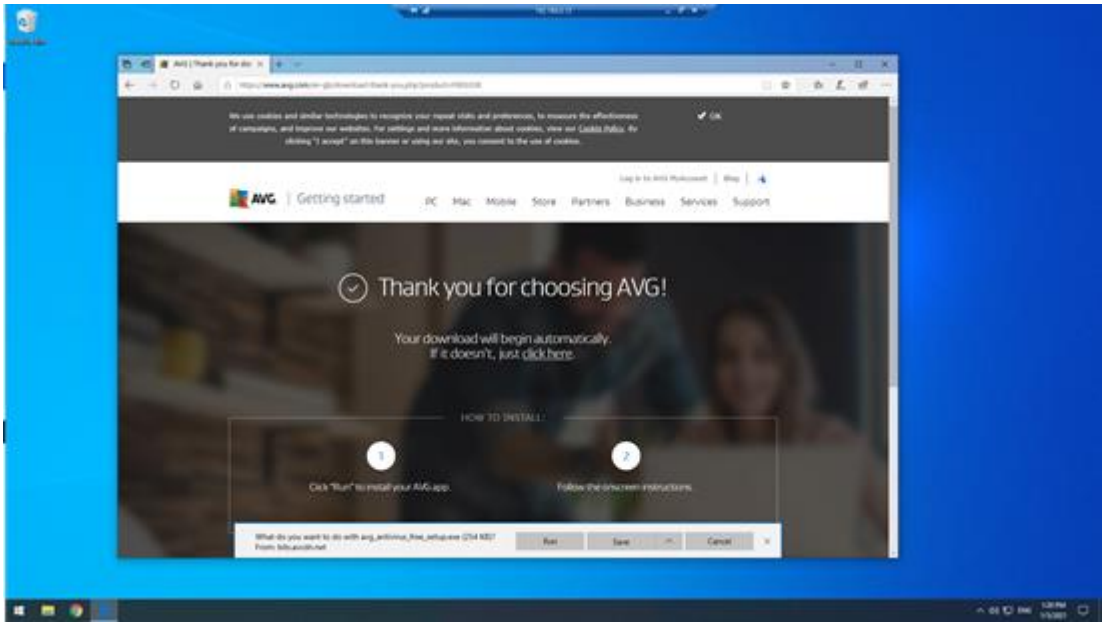
Screenshots:



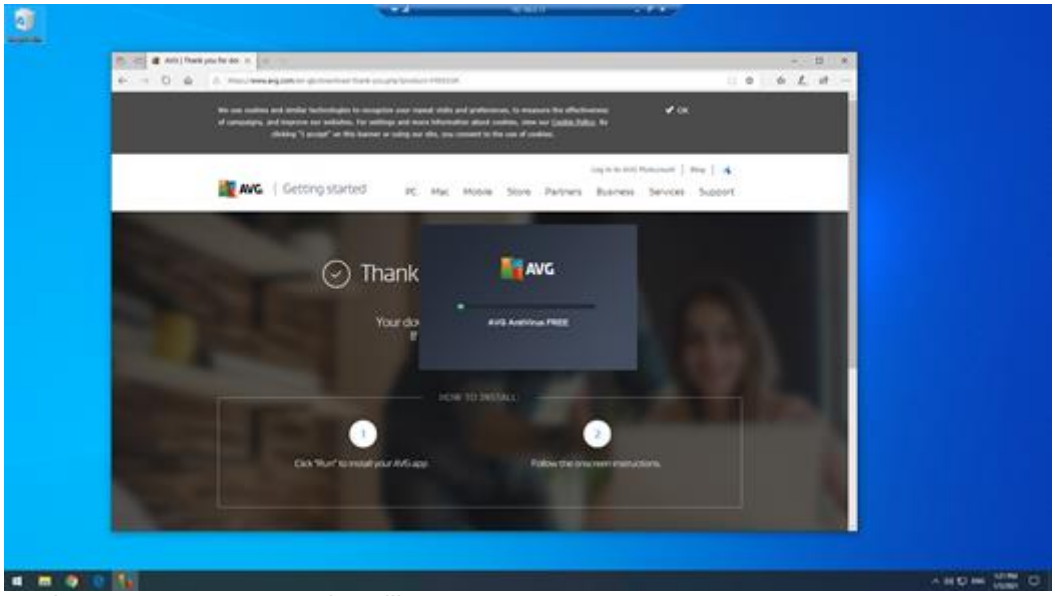
- I now search for an antivirus programme



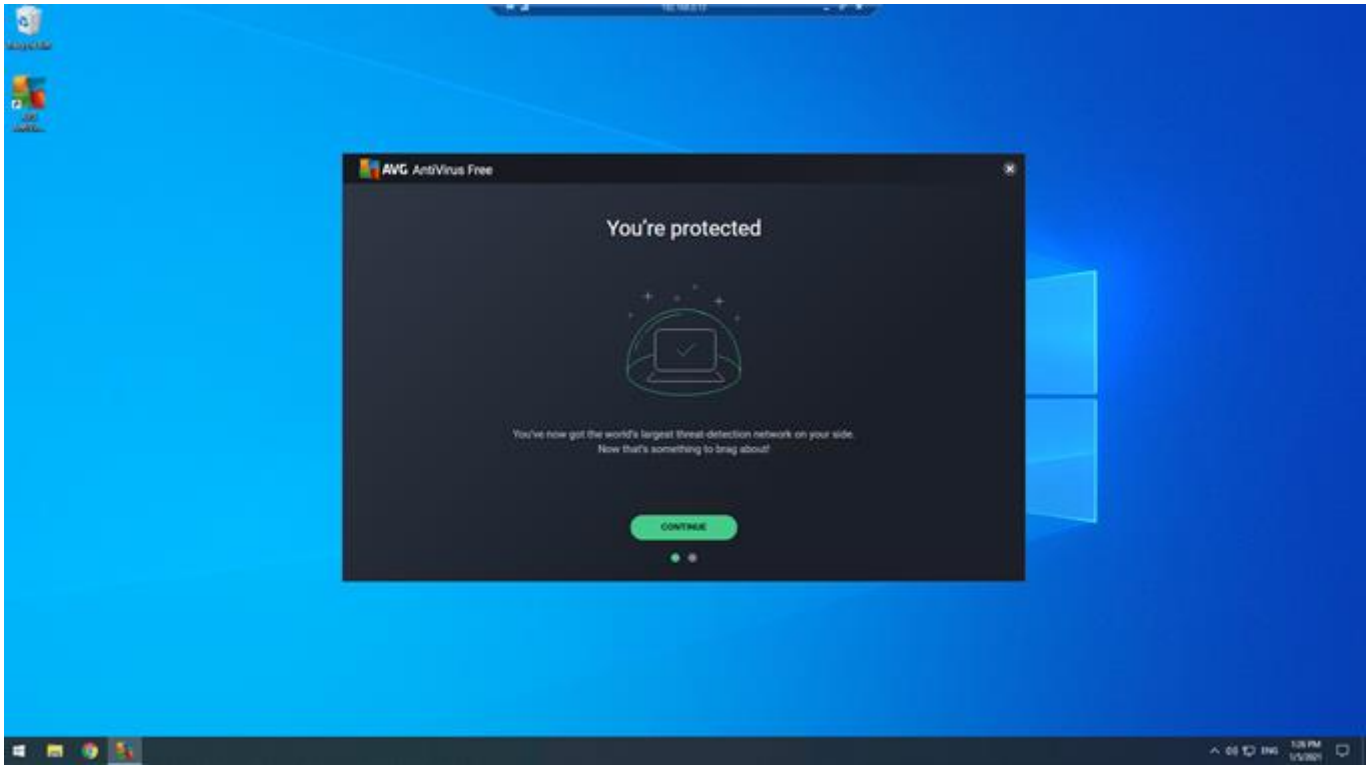
- I choose AVG and select the free download (please note: the company would have the option of purchasing a version of AVG)



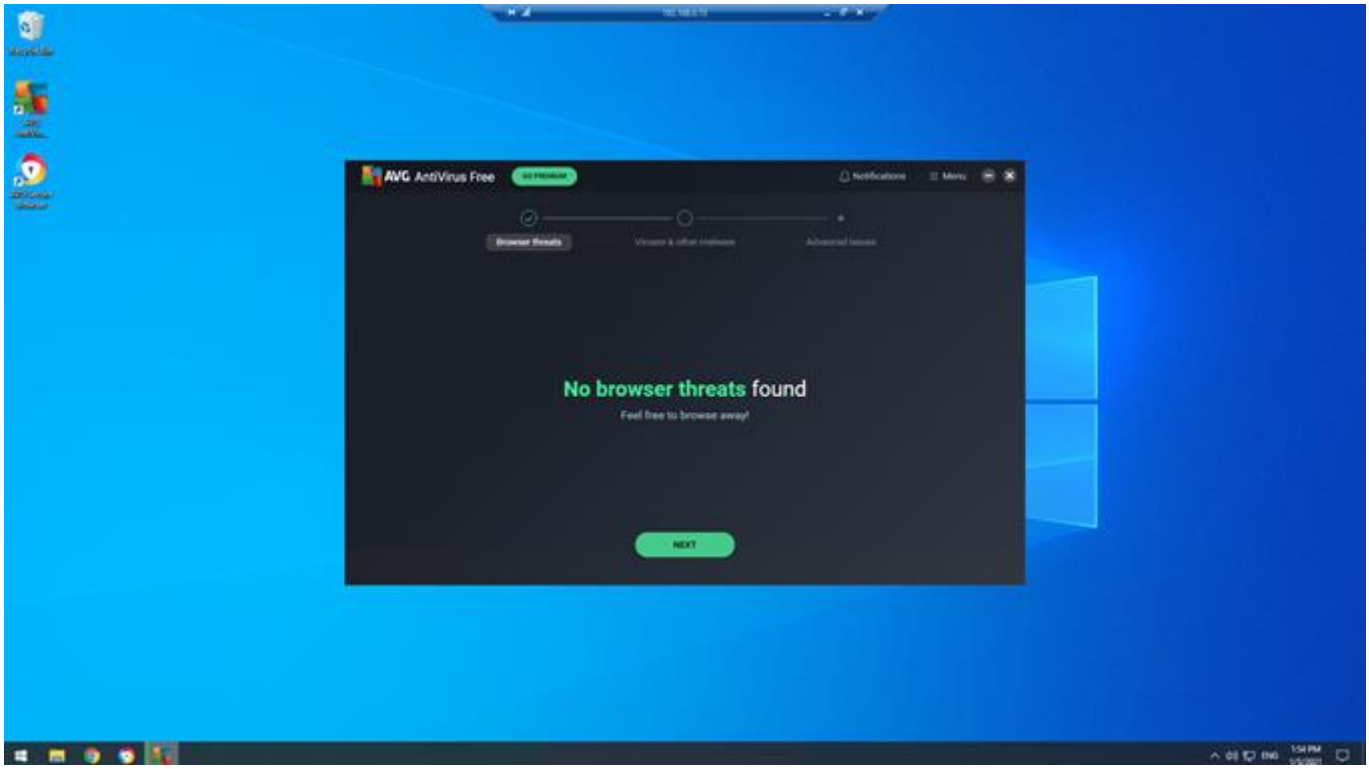
- I run the download



- here you can see AVG installing

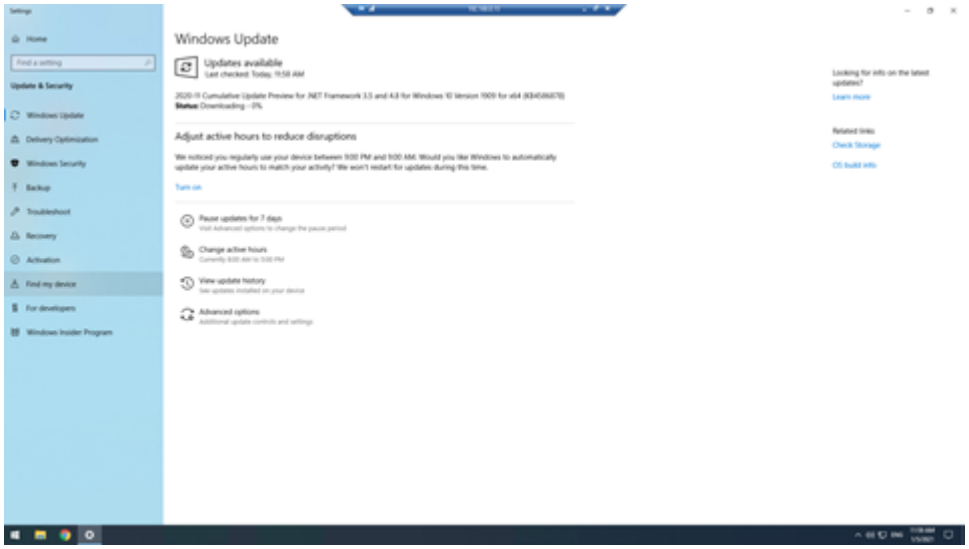


- and now the software is installed, and the computer is protected



- I run a scan and the results are above; there are no browser threats

Screenshots:

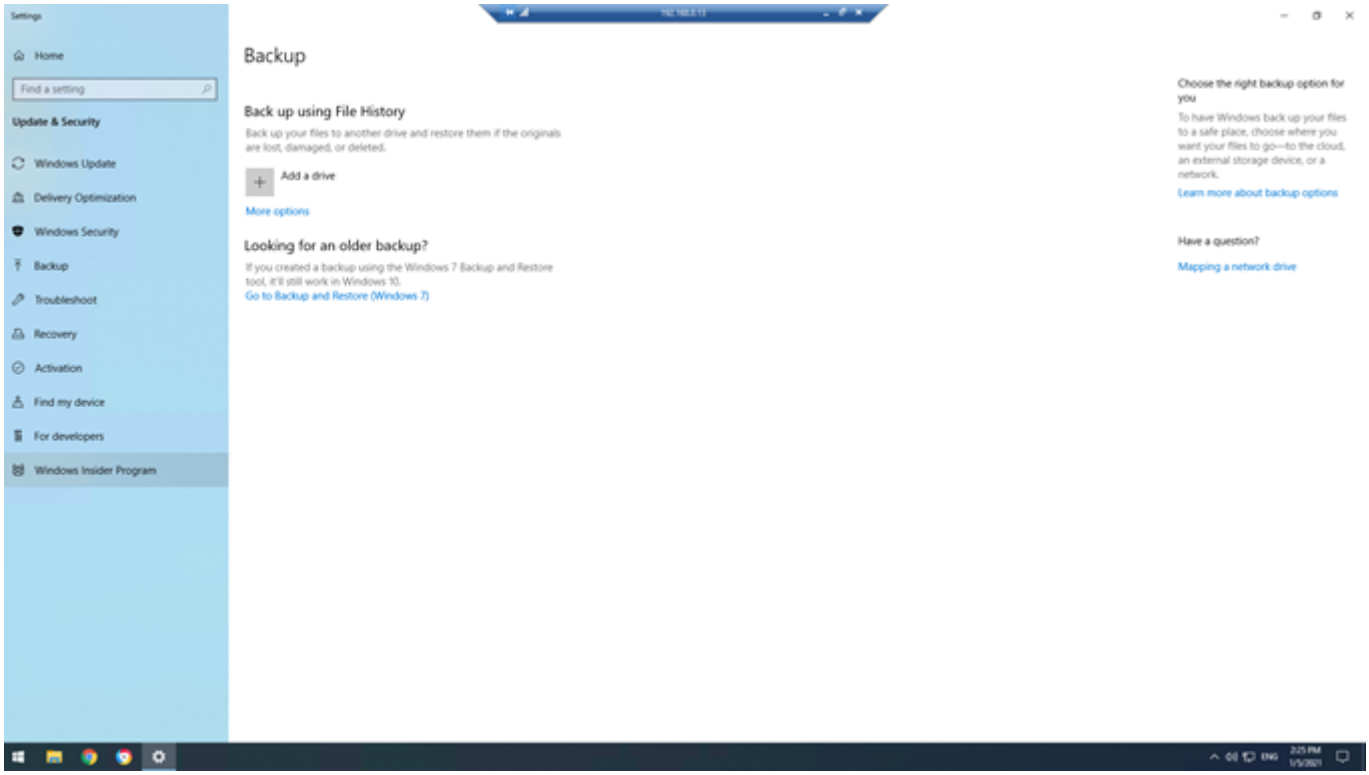


- I now open settings to check for updates to see any that are not currently installed

- after scanning, the computer shows it has missing updates which I can now install

Configuring backups

Screenshots:



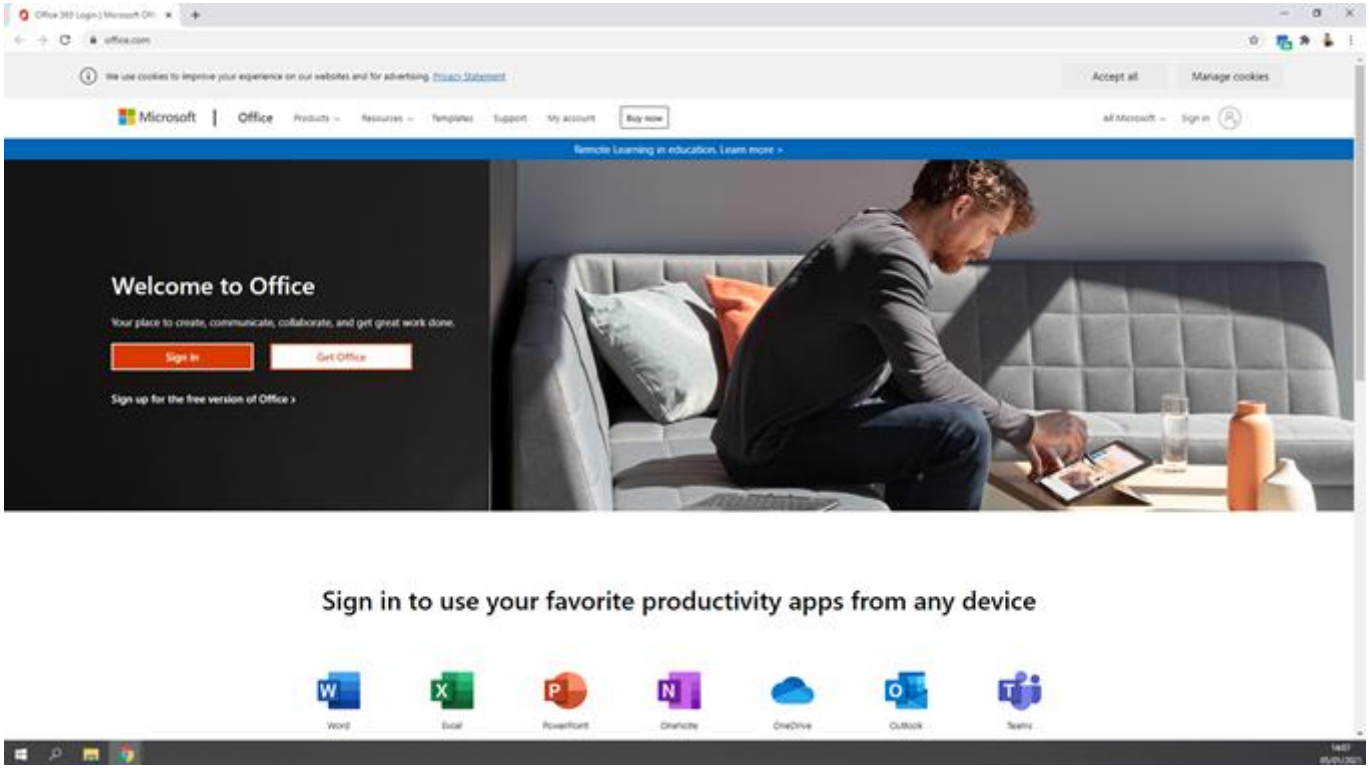
- Windows now shows it is fully up-to-date and so I can now run a backup to protect the data

Client software

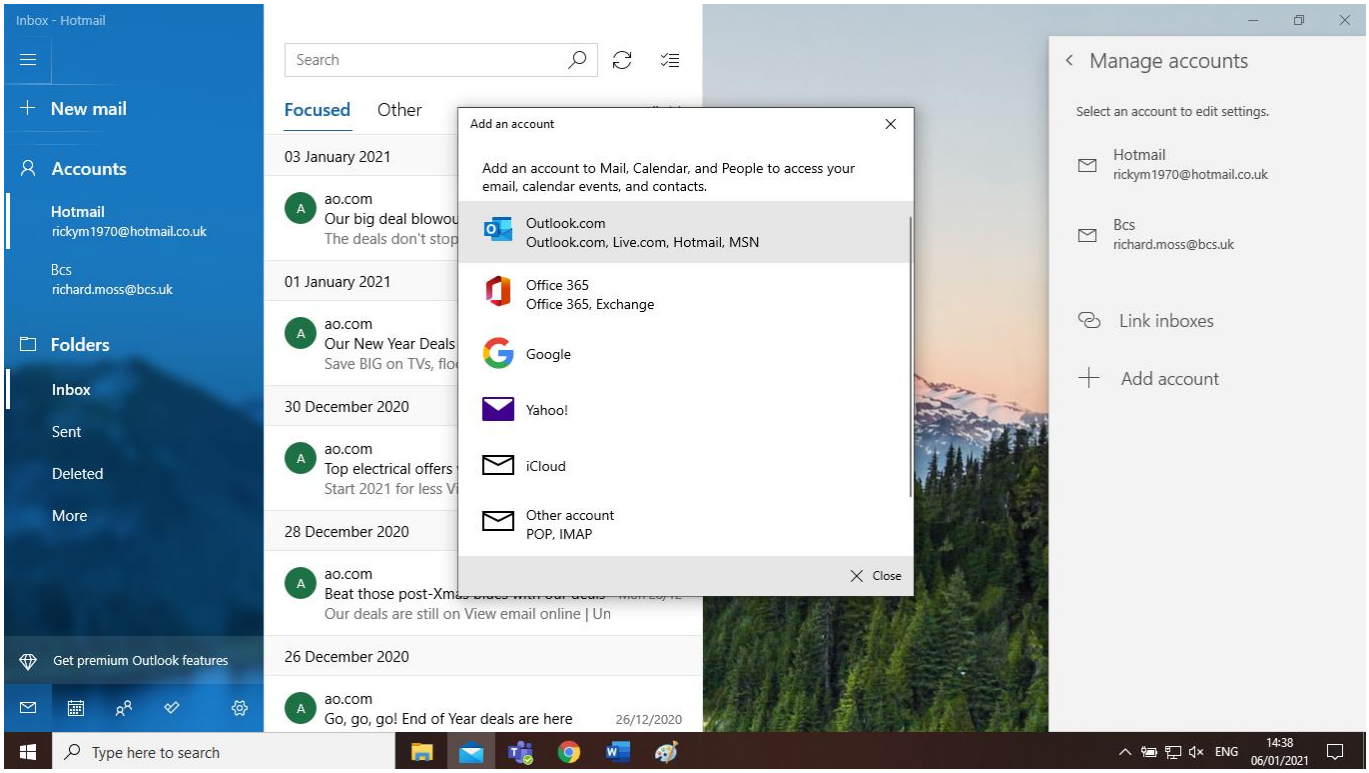
The following software was requested for installation:

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

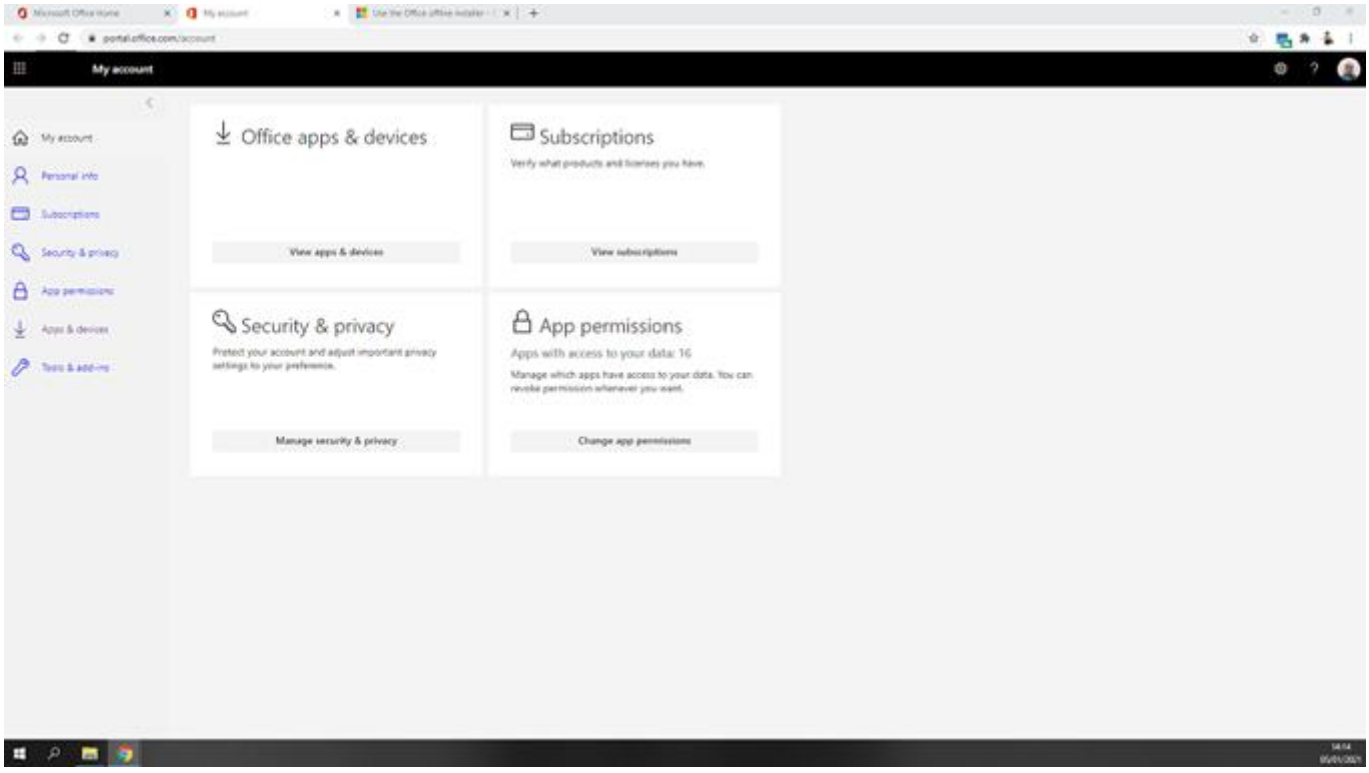
As per the network installation specification, I will install Microsoft Office 2019, Microsoft Project and Microsoft Teams.



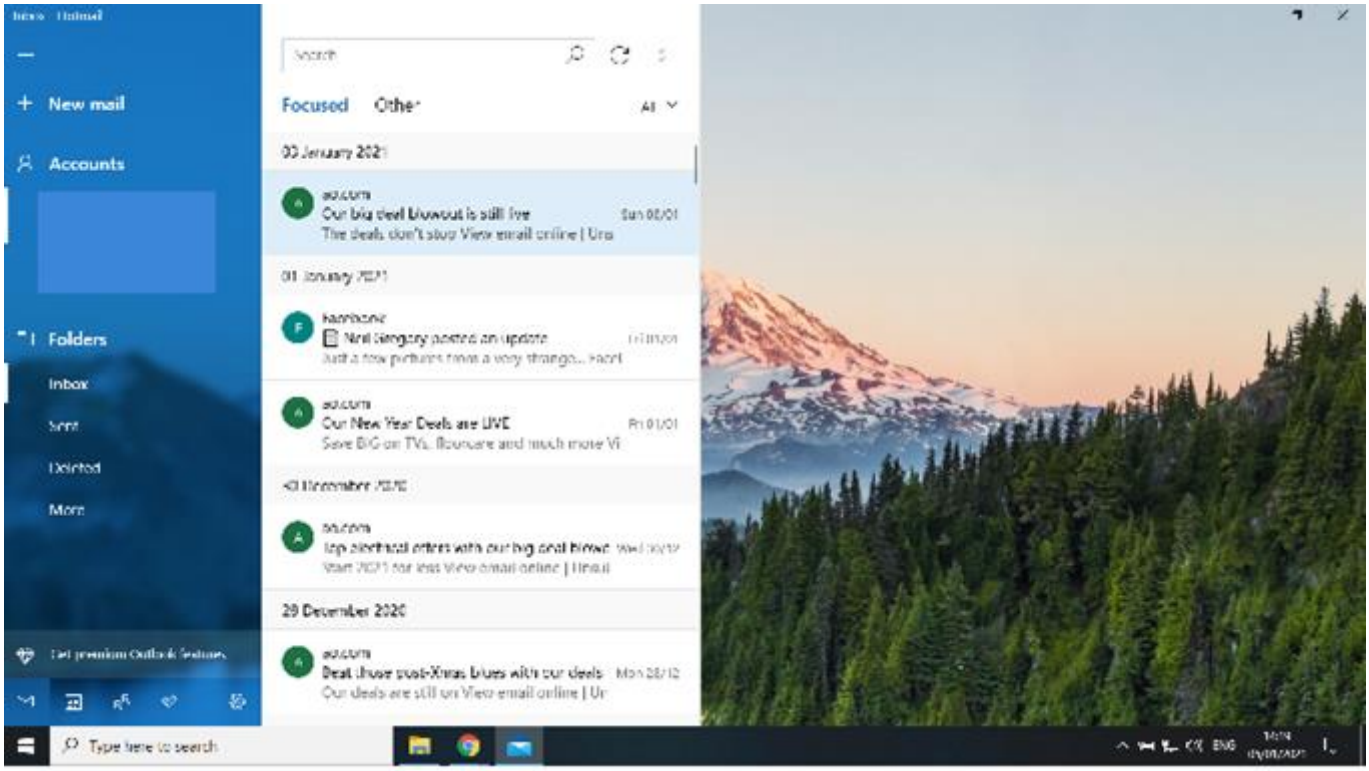
- here I go to the Microsoft website and select the office packages I want to install



- here I have the option to add an additional account



- here I can configure personalisation such as security

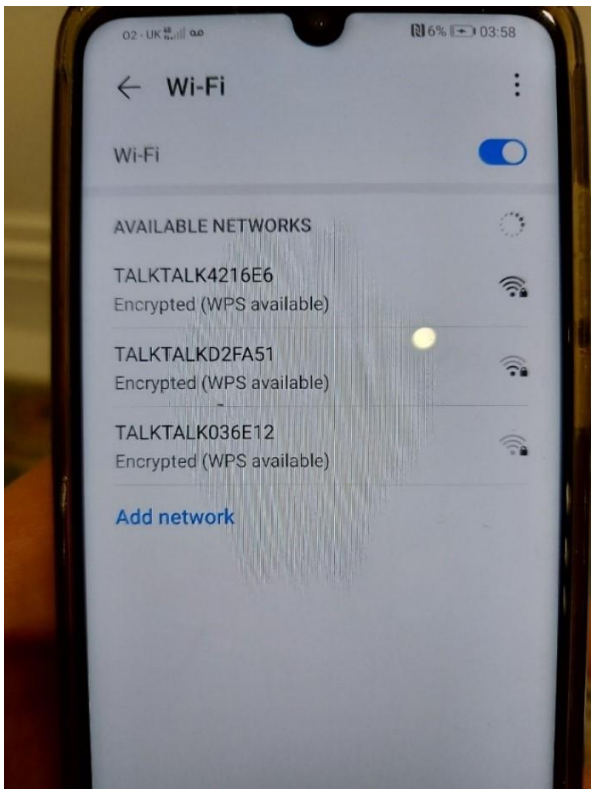


- here we see the configured mail programme

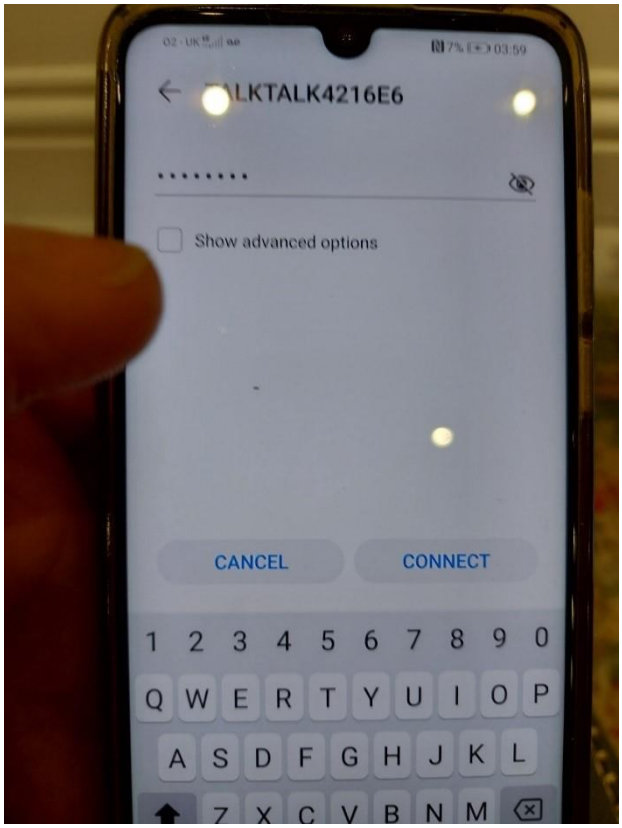
Mobile phone set-up

Connecting to wireless network

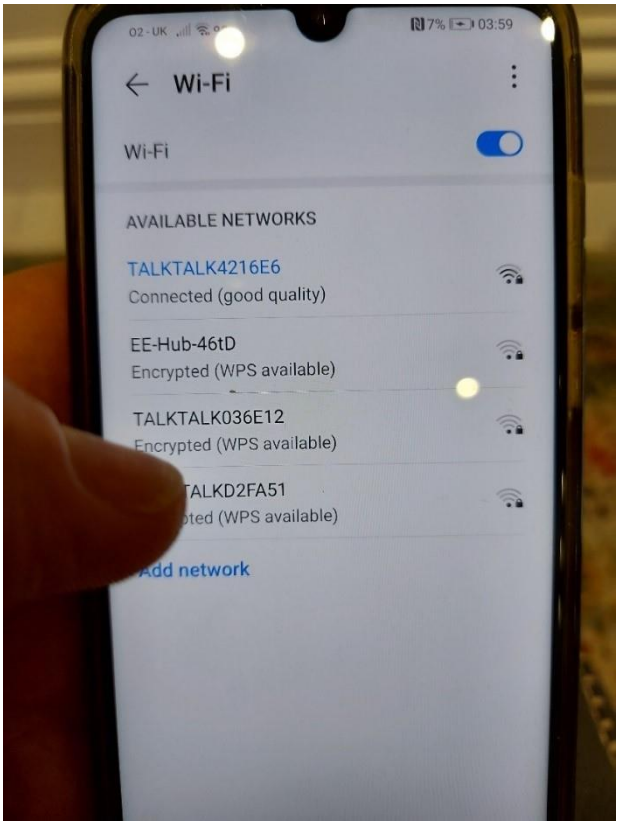
Photos:



- to connect the mobile phone to WiFi, I first open settings and then WiFi options



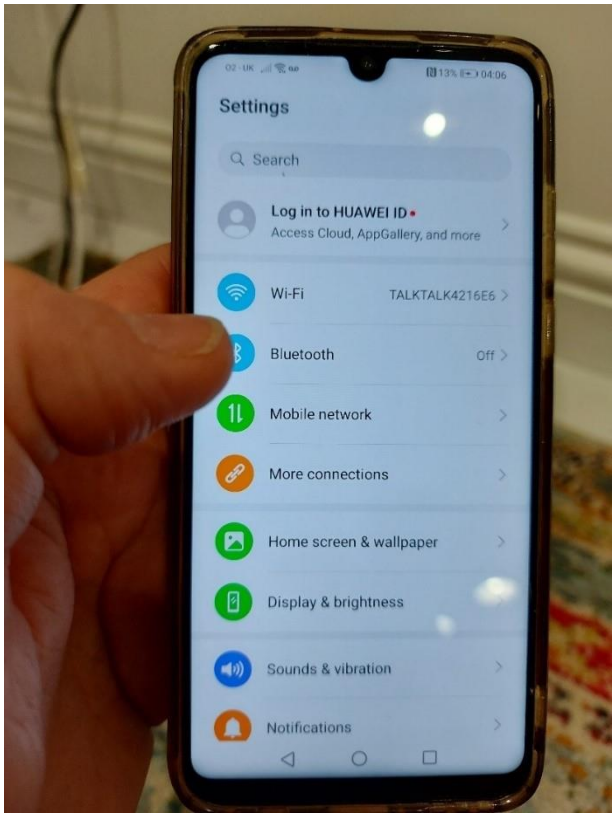
- I select the correct WiFi access point and input the password to gain access



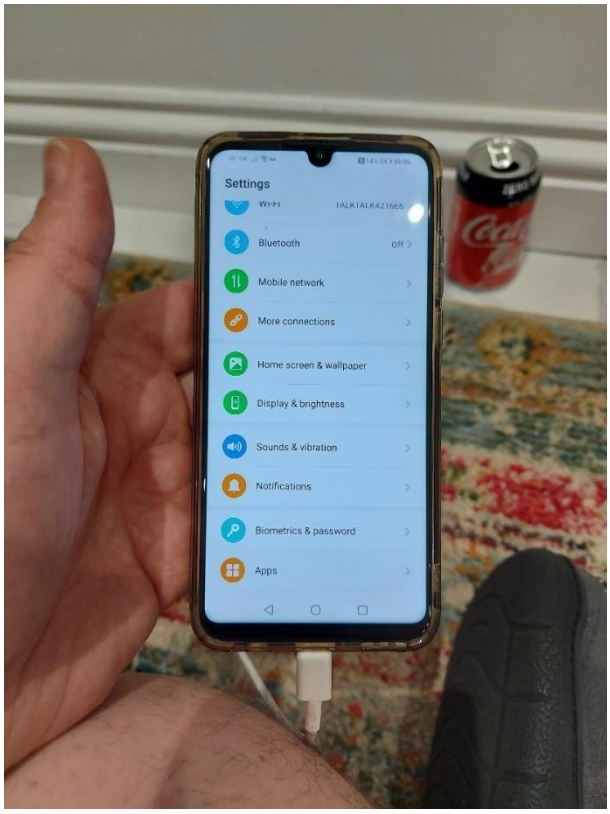
- the phone is now connected
- I join the phone to the office network by scanning for the network office WiFi and entering the WPA2-PSK password when prompted

Implementing screen lock

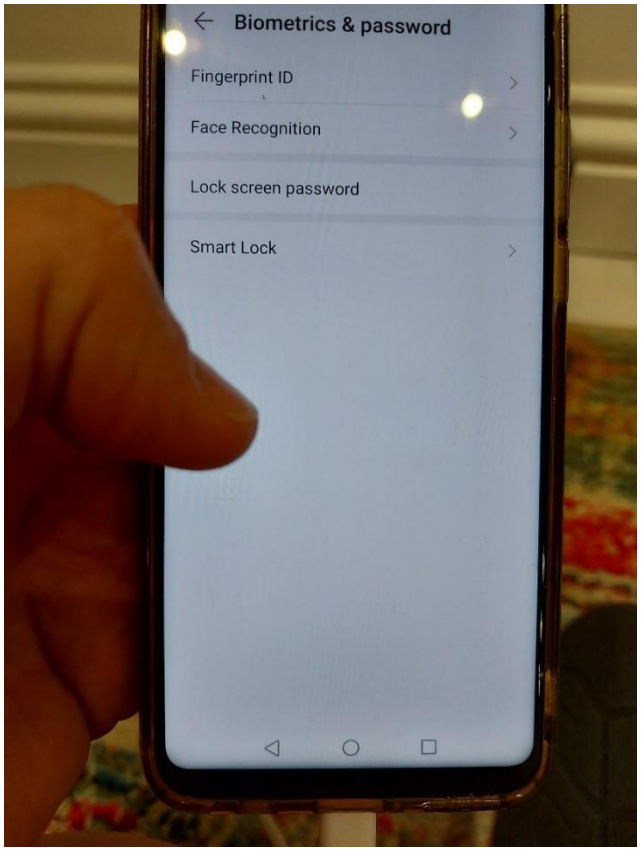
Photos:



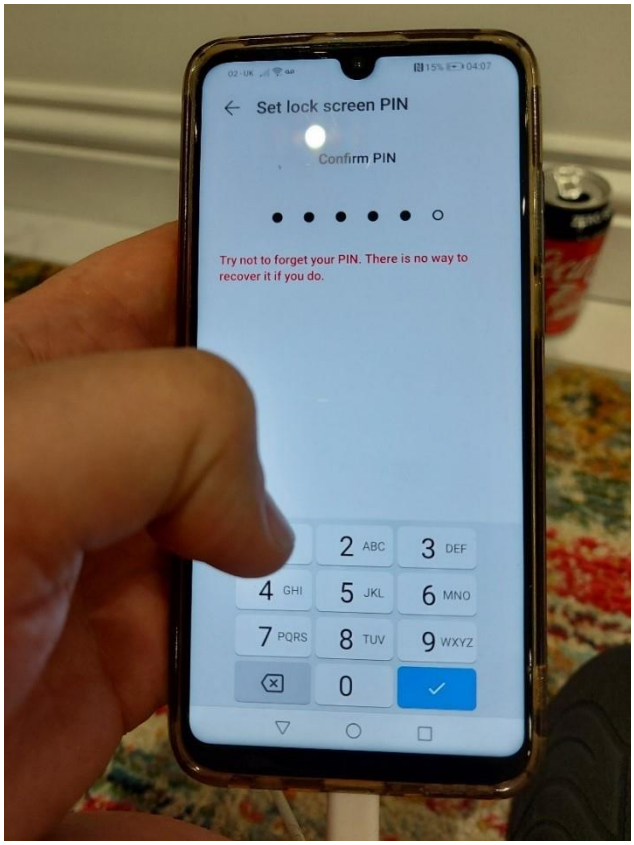
- now via settings, I need to access the security settings



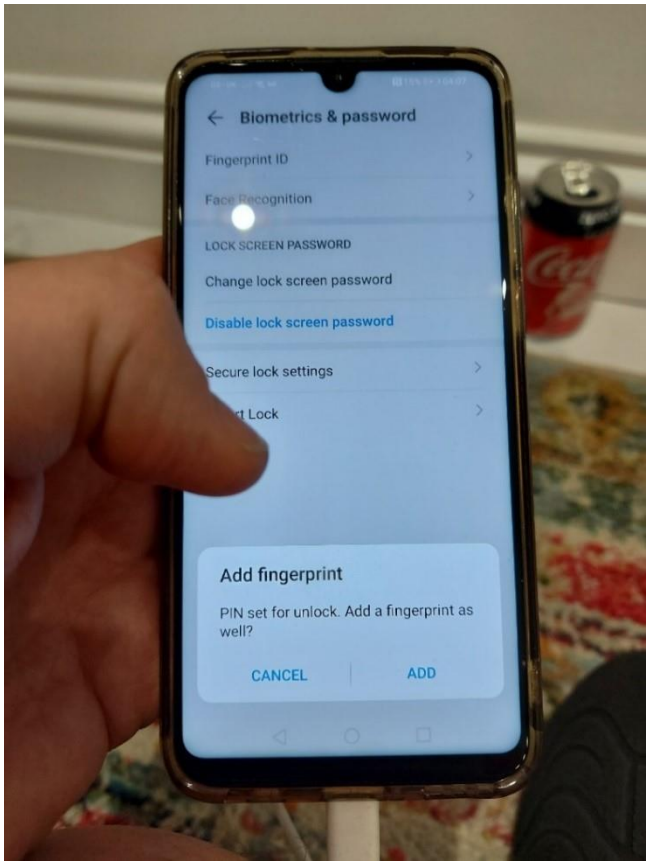
- from here, we access security



- I choose lock screen with fingerprint (biometrics)

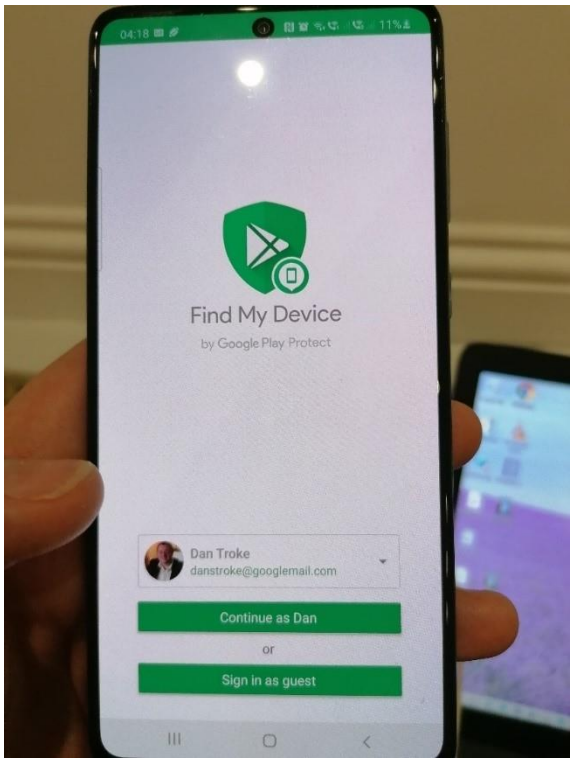


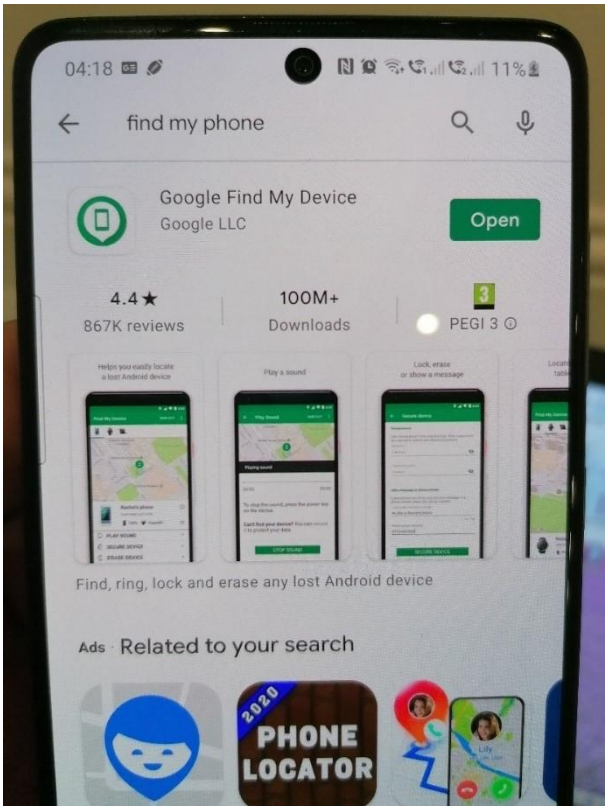
- I enter the password as part of the security



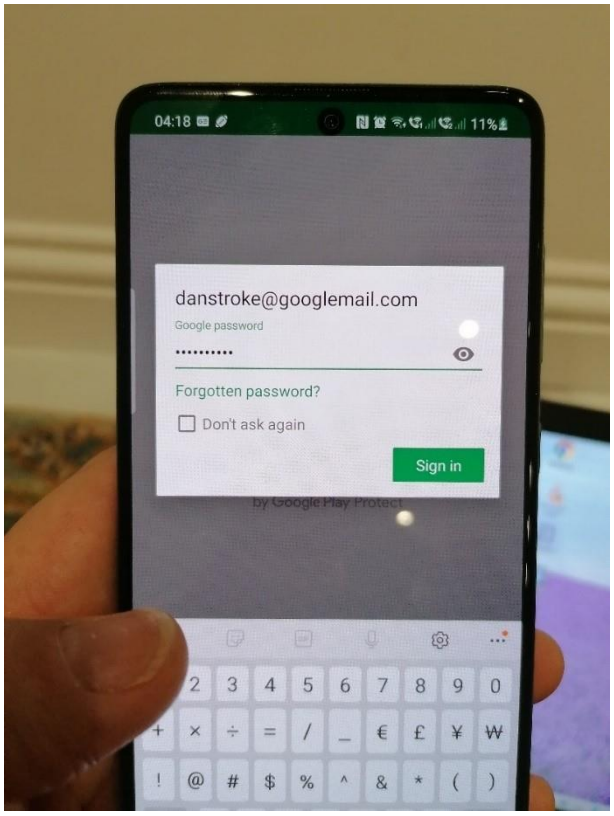
- now I can add a fingerprint
- to improve security of the mobile device, I have added a screen lock with a PIN number of 833011 which needs to be entered to unlock the phone when using biometrics

Photos:

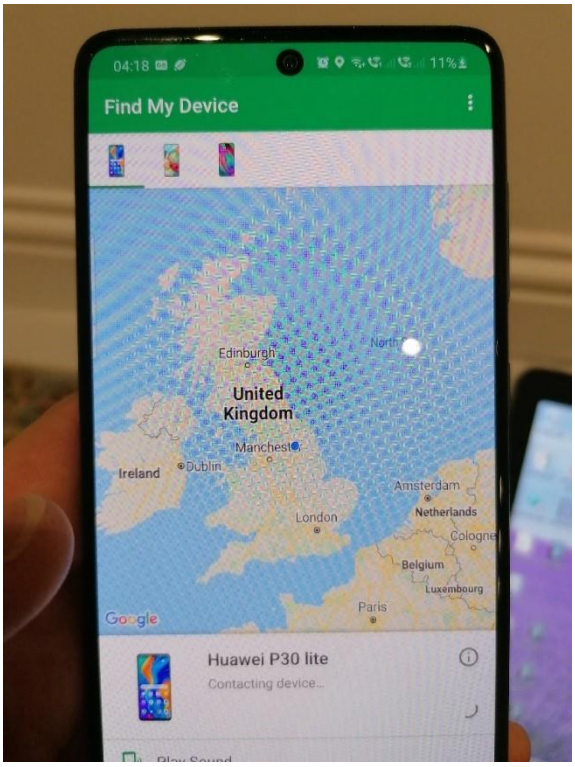




- I now want to be able to find my device if it is lost so I access the app ‘Find My Device’



- I add the relevant details



- now I can see the location is active
- in case of loss of the phone, I have added the ‘Find My Device’ app; this will allow me to locate a lost device on a map or make it ring to help find it, it also allows the phone to be remotely locked or remotely wiped to protect personal or company data if lost or stolen - this helps to protect company data

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

Examiner commentary

This project meets the requirement of the brief, fully considering the needs of the client:

- there was a full assessment of the security considerations and legislation such as GDPR and ISO27001. This included suggestions for how this could be dealt with
- the student has taken health and safety and security considerations such as signs to prevent access to dangerous areas, cooling for the server room to prevent overheating
- 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)
- they have provided a detailed commentary of the tasks they have undertaken and consistently use appropriate technical terms. It is clear they know and understand the technical terminology used in the sector
- the student has given the scenario deeper thought, looking beyond the assignment brief (for example, considering gateway routers on the network or the number of switches needed to achieve the project)
- where technical understanding of concepts is required, a high level of detail is seen (for instance when looking at IP addressing the solution is comprehensive with all information required)

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 and 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
Pass	The evidence showing installations and setup is logical and displays sufficient knowledge in response to the demands of the brief.
	The student makes some use of relevant knowledge and understanding of setting up systems and demonstrates an adequate understanding of perspectives or approaches associated with industry standards in digital support services roles.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their configurations.
	The student is able to identify some information from appropriate sources and apply the appropriate information/appraise relevancy of information and can combine information to make decisions.
	The student makes sufficient judgements/takes appropriate action/seeks clarification with guidance and is able to make adequate progress towards prioritising and solving non-routine problems in real life situations.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques to plan, install, configure and test software systems and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to attempt to prioritise and solve problems with some attempt at reasoning.
Distinction	The evidence is precise, logical and provides a detailed and informative response to the demands of the brief.
	The student makes extensive use of relevant knowledge and has extensive understanding of the practices of the sector and demonstrates a depth of understanding of the different perspectives/approaches associated with digital support.
	The student makes decisive use of facts/theories/approaches/concepts, demonstrating extensive breadth and depth of knowledge and understanding and selects highly appropriate skills/techniques/methods.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.

	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in a digital support role.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in a digital support role and precisely applies this across a variety of contexts and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine data/information in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify strategies for solving problems, giving concise 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. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

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
v2.0	Annual review 2023: Amends to grade descriptors to ensure clarity	June 2023	19 June 2023