



# **T Level Technical Qualification in Digital Support Services**

Occupational specialism assessment (OSA)

## **Digital Support**

Assignment 3 - Pass

Guide standard exemplification materials

## T Level Technical Qualification in Digital Support Services

### Occupational specialism assessment

# Guide standard exemplification materials

## Digital Support

### Assignment 3

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Assignment 3 .....</b>	<b>4</b>
<b>Scenario.....</b>	<b>4</b>
<b>Task 1 .....</b>	<b>4</b>
<b>Task 2.....</b>	<b>13</b>
Examiner commentary .....	59
Grade descriptors.....	60
<b>Document information .....</b>	<b>62</b>
Change History Record.....	62

# 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 3, the student must first analyse a penetration test of a network in order to identify any maintenance requirements. The second task requires the student to remotely carry out updates to the system.

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

# Assignment 3

## Scenario

Monitoring and maintaining all infrastructure whilst documenting the process is the key to an efficient and functional system. During this process, you will analyse the recent penetration test report that has been produced on a network. This will lead to you identifying vulnerabilities, providing solutions, and identifying trends and underlying problems, all of which will be documented in a continuous improvement plan.

Alongside this, to save time and improve efficiency, you are required to create and deploy an image remotely which consists of an operating system and software applications.

## Task 1: network analysis

### Time limit

6 hours

You can use this time how you want but task 1 must be completed within the time limit.

(12 marks)

### Student instructions

In this assignment, you need to monitor, maintain and demonstrate continuous improvement of a network. For this, you will need to produce an infrastructure status log (worksheet in appendix 3) for the equipment listing (worksheet in appendix 3) and network overview diagram provided (appendix 4). You will log and update the infrastructure status log and produce maintenance notes for each of these devices.

You must also analyse the penetration test report provided (appendix 5) and filter your findings and solutions in the penetration test remediation log (worksheet in appendix 3), into your future planning to demonstrate understanding of continuous improvements. This will include how current and future vulnerabilities will be mitigated, and will also identify trends and document underlying problems to produce solutions faster.

Documentation and screenshots, where applicable, will need to be provided to show the work you have conducted and any future planning.

- 1) You are required to monitor, maintain and demonstrate continuous improvement of the new network, including:
  - log infrastructure status
  - maintenance notes for the installations
  - analysis of penetration testing report
  - mitigation of vulnerabilities
  - future planning, identifying trends and documenting underlying problems

You will have access to the following equipment:

- 1 x workstation set-up with office software installed
- internet access for developer notes and help pages
- digital camera

## 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 issues identified in the penetration test report and maintenance notes for the installations within the infrastructure status log (worksheet in appendix 3)
- infrastructure status log (worksheet in appendix 3)
- penetration test remediation log (worksheet in appendix 3)
- documented/planned improvements (word processing document)
- internet browsing history

## Student evidence

Following the penetration test report and subsequent risk assessment, it can be summarised that the following vulnerabilities were identified with the current network:

- workstations:
  - vulnerability:
    - all workstations within the infrastructure were found to be missing 4 distinct critical updates:
      - KB4511552 for x64
      - KB4511552 for ARM64
      - KB4505657 for x64
      - KB4505657 for ARM64

## About

### Windows specifications

Edition	Windows 10 Pro
Version	1803
Installed on	26/04/2021
OS build	17134.1

[Change product key or upgrade your edition of Windows](#)

[Read the Microsoft Services Agreement that applies to our services](#)

[Read the Microsoft Software License Terms](#)

### Related settings

[System info](#)

Windows 10 1803 is the installed operating system, therefore missing a significant number of updates (image a):

As you can see, a number of updates were missing (image b):

## Windows Update



Updates available

Last checked: Today, 21:31

**Your device is missing important security and quality fixes.**

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1735.0)

**Status:** Downloading - 0%

Windows Malicious Software Removal Tool x64 - v5.88 (KB890830)

**Status:** Initializing...

2021-03 Update for Windows 10 Version 1803 for x64-based Systems (KB4023057)

**Status:** Initializing...

2020-06 Update for Windows 10 Version 1803 for x64-based Systems (KB4480730)

**Status:** Initializing...

2020-02 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4537762)

**Status:** Initializing...

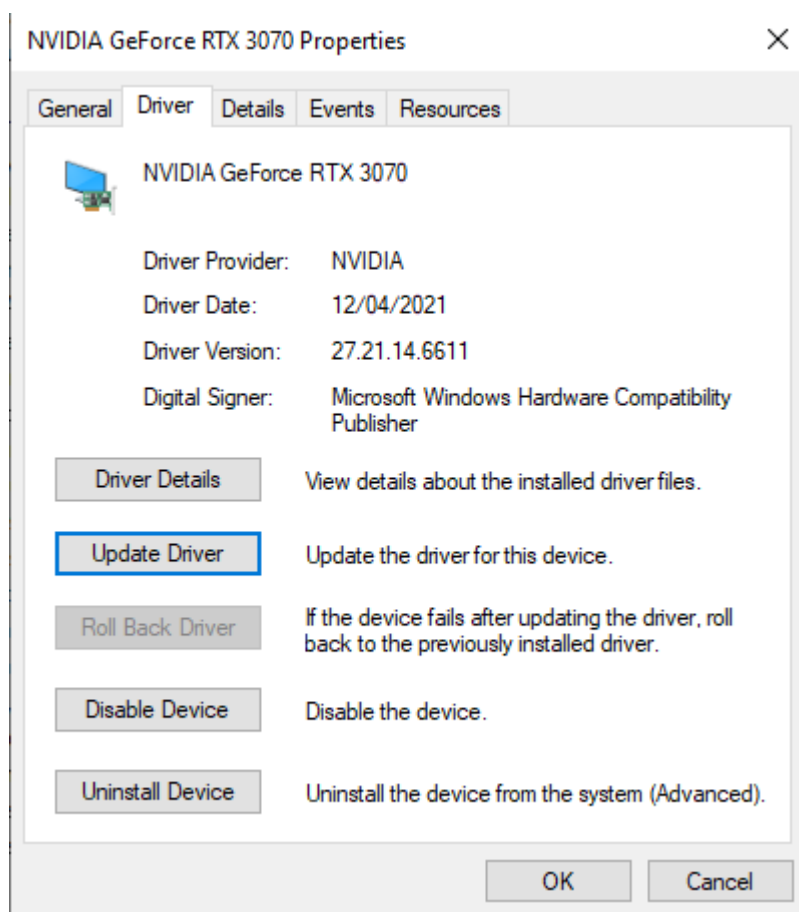
Microsoft .NET Framework 4.8 for Windows 10 Version 1803 for x64 (KB4486153)

**Status:** Downloading - 100%

2019-02 Update for Windows 10 Version 1803 for x64-based Systems (KB4346084)

**Status:** Initializing...

- action:
  - all patches need to be updated on the workstations
- vulnerability:
  - the NVIDIA video driver on all workstations was out of date and needs to be updated to prevent exploitation



This computer did not have the most up to date video drivers available (image c):

- action:
  - all workstations to have drivers updated during next routine maintenance

- servers:

<u>Title</u>	<u>Classification</u>	<u>Last Updated</u>
<a href="#">2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4501835)</a>	Updates	5/1/2019
<a href="#">2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4497934)</a>	Updates	5/20/2019
<a href="#">2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4505056)</a>	Updates	5/19/2019
<a href="#">2019-05 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4499728)</a>	Security Updates	5/13/2019
<a href="#">2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4494441)</a>	Security Updates	5/13/2019
<a href="#">2019-05 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4495590)</a>	Security Updates	5/9/2019
<a href="#">2019-05 Security Update for Adobe Flash Player for Windows Server 2019 for x64-based Systems (KB4497932)</a>	Security Updates	5/13/2019
<a href="#">2019-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4499405)</a>	Security Updates	5/9/2019
<a href="#">2019-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB4495618)</a>	Security Updates	5/9/2019
<a href="#">2020-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4556441)</a>	Security Updates	5/8/2020

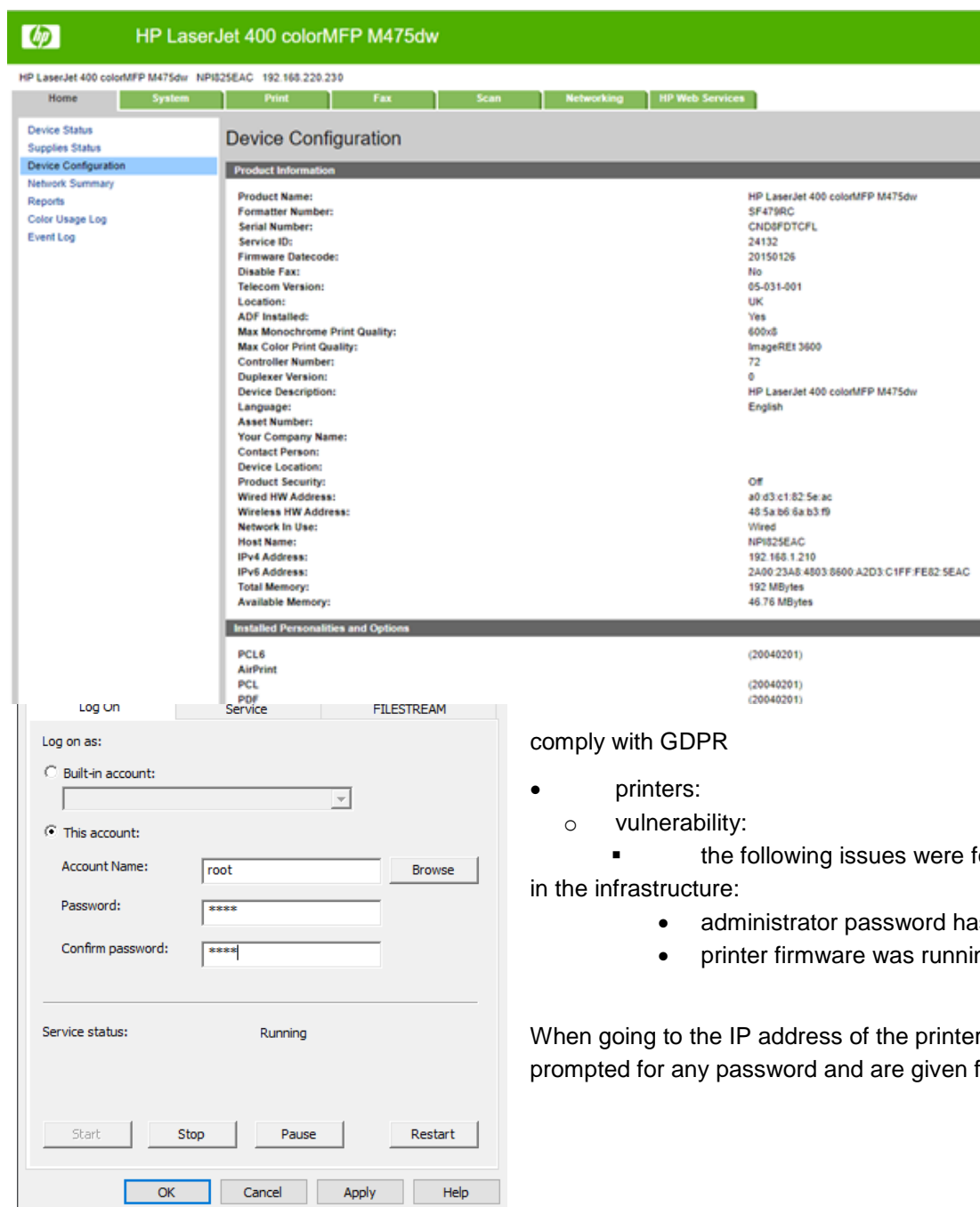
- vulnerability:
  - all 5 of the servers operating within the network had 10 updates missing:
    - KB4501835
    - KB4497934
    - KB4505056
    - KB4499728
    - KB4494441
    - KB4495590
    - KB4497932
    - KB4499405
    - KB4495618
    - KB4556441

The following updates were missing as identified (image d):

- action:
  - all patches need to be updated on the servers
- vulnerability:
  - vulnerabilities were identified in the SQL server operation on SVR09

- a weak username/password combination for the admin, allowing access to the server
- it was possible for all usernames and passwords for all users to be retrieved in plain text
- a username/password was able to be added to the database to allow exploitation

As you can see, the root account has a basic password (image e):



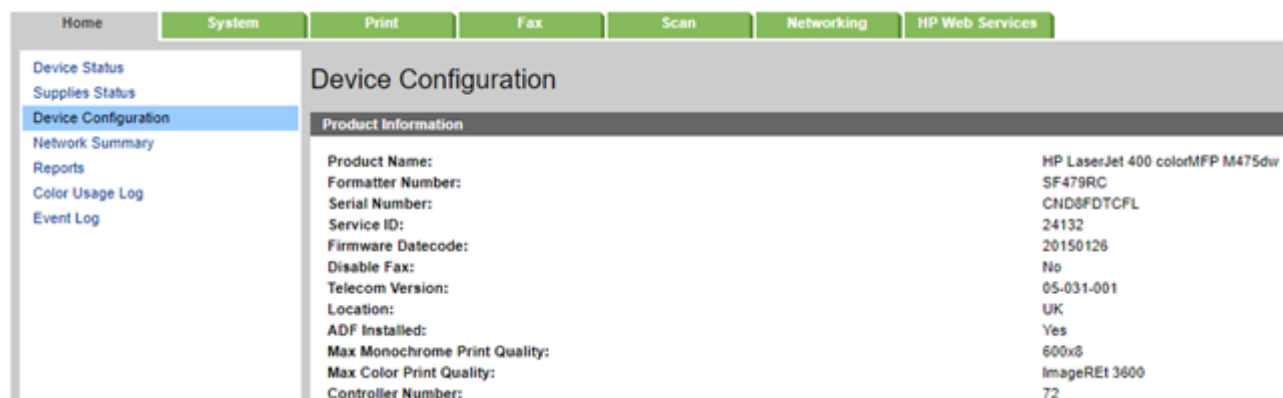
- action:
  - ad ministrative password set using a strong password
  - it would be worth introducing a form of 2 factor authentication on the server
  - the password database needs to be encrypted as it contains customers' data to

comply with GDPR

- printers:
  - vulnerability:
    - the following issues were found on all 5 printers in the infrastructure:
      - administrator password has not been set
      - printer firmware was running an old version

When going to the IP address of the printer, you are not prompted for any password and are given full access (image f):

Printer firmware is now out of date (image g):



The screenshot shows the HP LaserJet 400 colorMFP M475dw web interface. The top navigation bar includes links for Home, System, Print, Fax, Scan, Networking, and HP Web Services. The left sidebar contains links for Device Status, Supplies Status, Device Configuration (highlighted), Network Summary, Reports, Color Usage Log, and Event Log. The main content area is titled 'Device Configuration' and displays 'Product Information' in a table format.

Product Information	
Product Name:	HP LaserJet 400 colorMFP M475dw
Formatter Number:	SF479RC
Serial Number:	CND8FDTCFL
Service ID:	24132
Firmware Datecode:	20150126
Disable Fax:	No
Telecom Version:	05-031-001
Location:	UK
ADF Installed:	Yes
Max Monochrome Print Quality:	600x8
Max Color Print Quality:	ImageREt 3600
Controller Number:	72

○ action:

- all 5 printers will need their firmware updating to the latest version
- all 5 printers will need a strong administrator password setting on the management console and a login prompt set

### **Forward planning and continuous improvement**

Having looked at all the vulnerabilities, it is clear that there are concerns with patch management and routine maintenance.

#### **Patch management**

This needs to be set to automatically update the devices to prevent important updates being missed.

#### **Recommendation for continuous improvement:**

##### **Windows Server Update Services (WSUS)**

I would recommend that we complete all of the Windows updates on the servers and that we monitor them to ensure future updates are installed correctly.

### **Routine printer maintenance**

Once the initial resolution has been implemented as per the recommendations above, we should also be introducing standard checking of firmware.

### **Routine workstation maintenance**

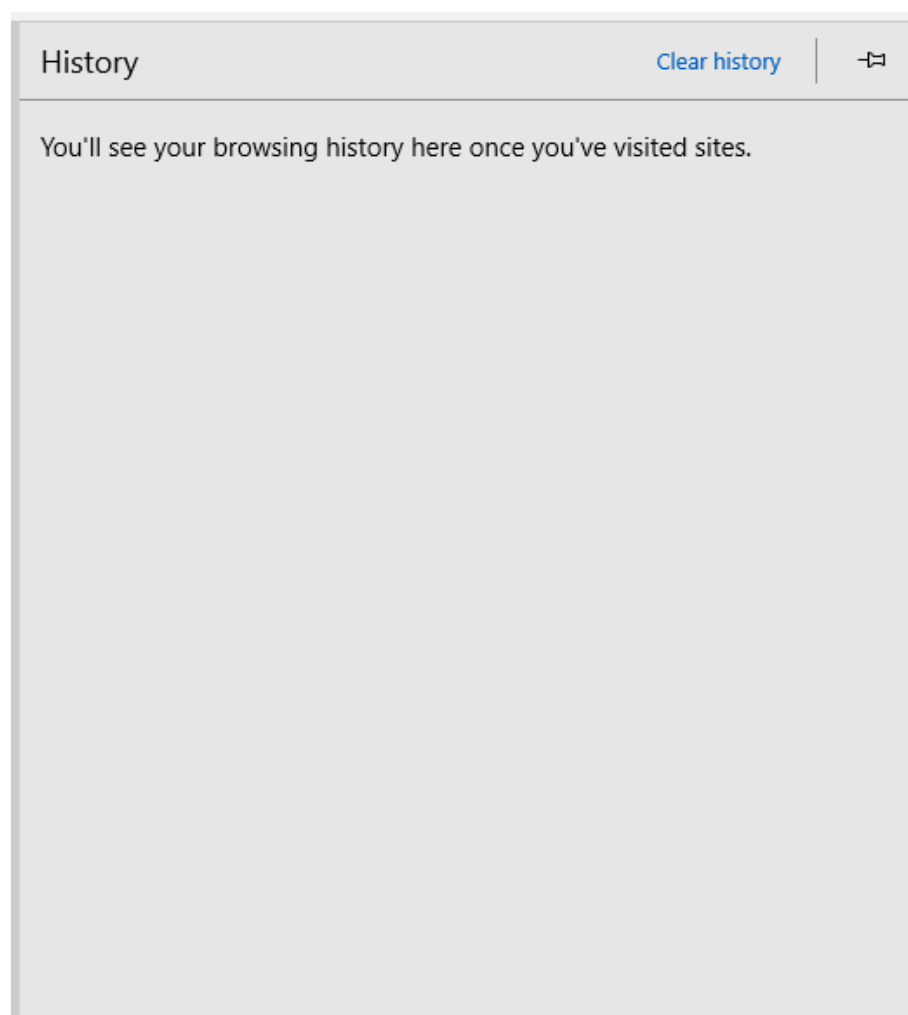
During routine workstation maintenance, technicians should also be looking at the device manager and driver information to confirm that latest drivers for all devices are installed.

### **SQL server/phpMyAdmin**

The identified vulnerabilities in the SQL server are serious and need to be resolved urgently (within 3 days as per recommendation).

### **Summary**

Implementing these recommendations will resolve the current issues and put in place, through the routine maintenance and monitoring, the ability to quickly identify and proactively resolve any further vulnerabilities that may occur.



### **Browser history**

## Task 2: deploy image remotely

### Time limit

4 hours

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

(15 marks)

### Instructions for students

As part of your continuous improvement of the network created, it has been logged that new software applications are needed for computers in an office. To save time and increase efficiency, this will be completed remotely.

For this, you must create an image which includes an operating system, office software applications, drivers, rules, active directory permissions and a deployment task sequence. You will deploy this remotely. A test plan and test log (worksheet in appendix 3) will need to be completed for this task. This is required as the image may be deployed on different hardware platforms (for example, graphic cards) as it is necessary to quality assure the device to ensure the deployed image is acting as expected.

Screenshots and notes will need to be made throughout the creation, deployment and testing of the image.

This can be performed either virtually or physically.

2) You are required to demonstrate creation of an image and deployment of that image remotely for **one** virtual or physical machine, including:

- create an image:
  - operating system
  - software applications
  - active directory joined
  - deployment task sequence
- upload image to image distribution system and make available for example, windows deployment service (WDS)
- deploy image
- create a test plan and complete log

You will have access to the following equipment:

- a machine running WDS or similar
- internet access for developer notes and help pages
- 1 end-user device or virtual machine
- access to servers, firewalls, network devices and network-based services
- operating system and office licences for basic image deployment
- a digital camera

## **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) and documented notes showing creation and deployment of image
- test plan (worksheet in appendix 3)
- test log (worksheet in appendix 3)
- internet browsing history

## Student evidence

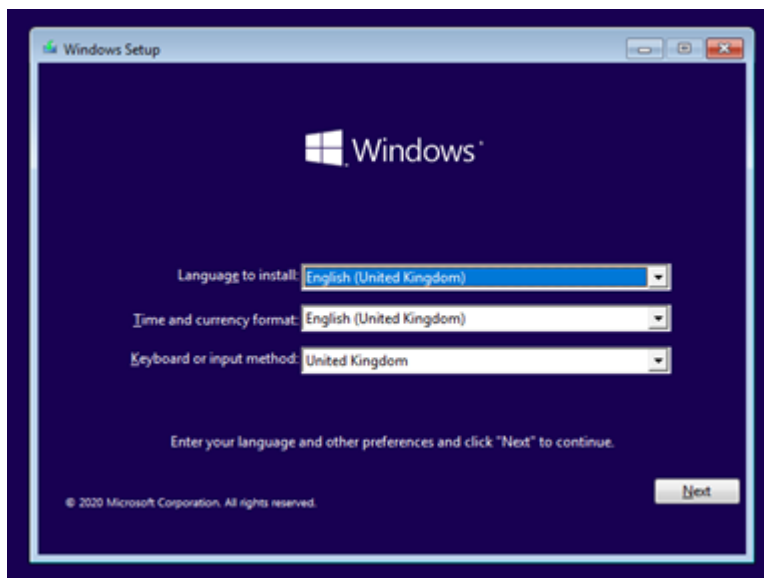
### Task 2

#### Creating a reference virtual machine

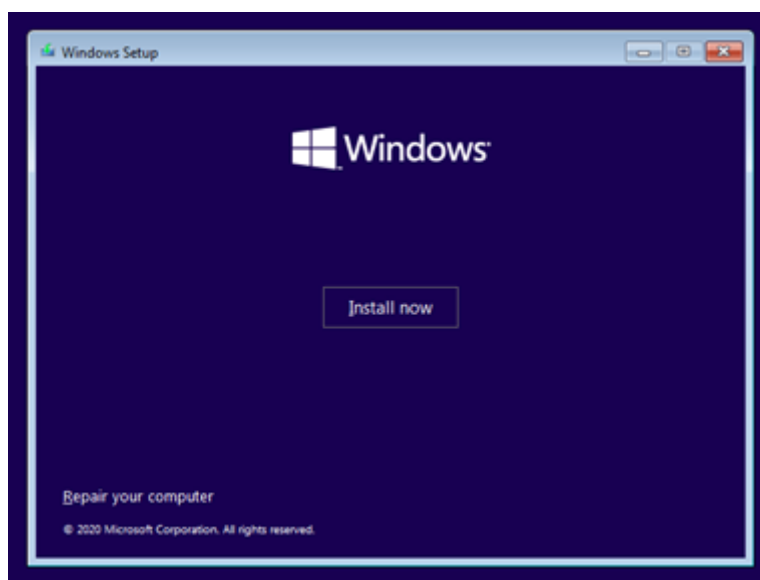
To create an image for remote deployment, I first need to create a reference image. The first steps to achieve this are to install Windows 10 on a computer and set it up exactly as I want all our client PCs to be set up.

#### Installing Windows 10

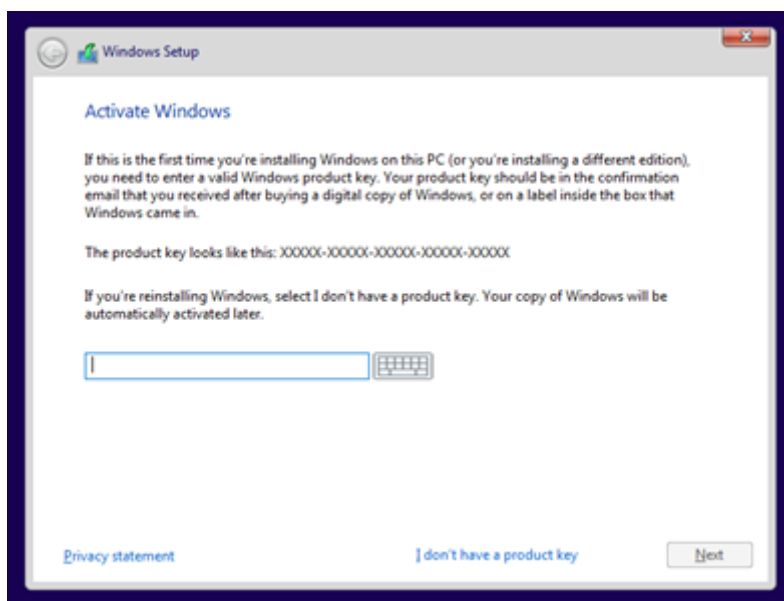
These screenshots show me installing Windows 10 Professional onto my reference PC (image 1):



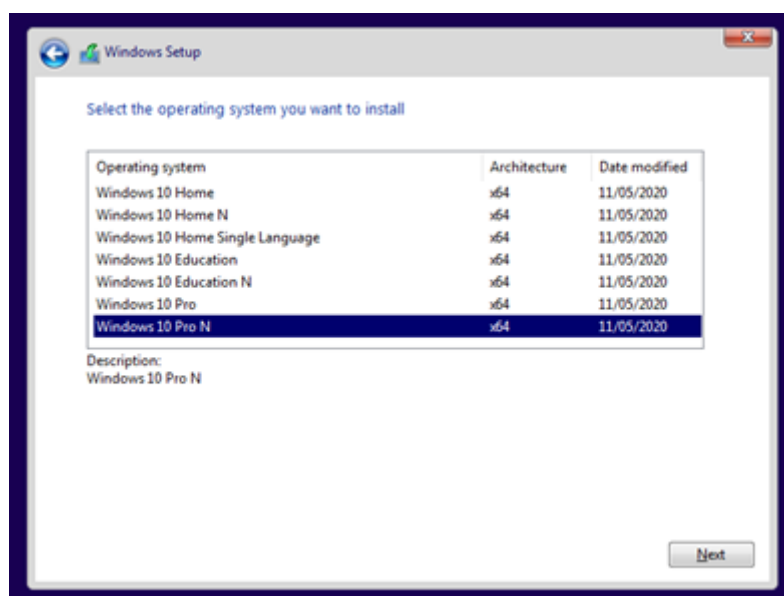
- I booted from the Iso and now select the installation language (image 2)



- I click install



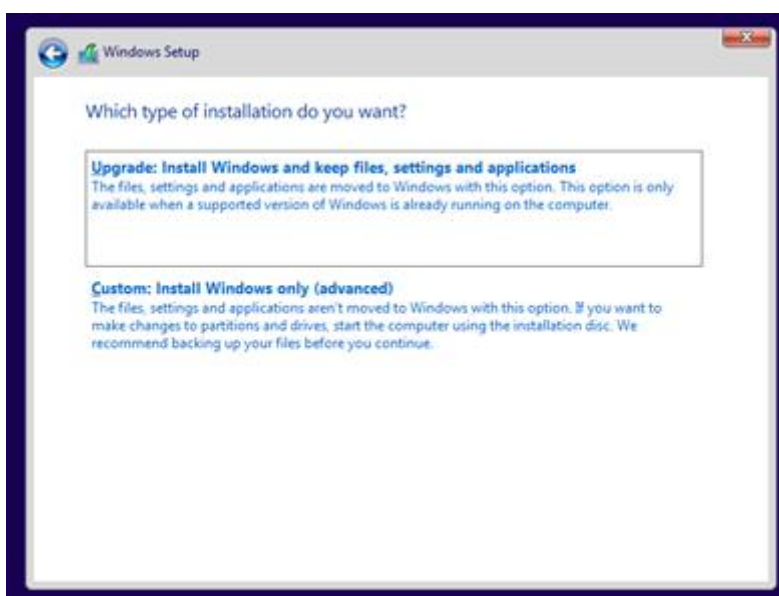
- I add licence details to prove I have a legal copy



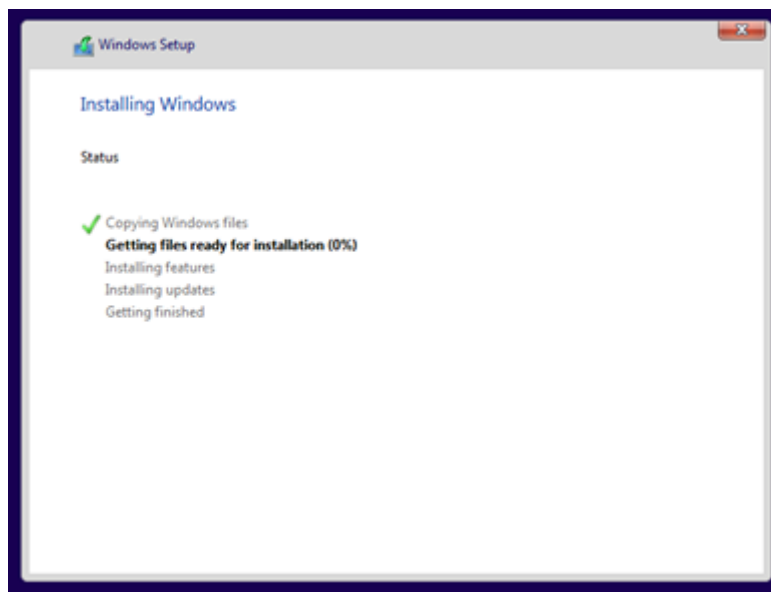
- I select the Windows version I want to include. I am going to install Windows 10 Pro as this is a corporate machine and needs to join a domain



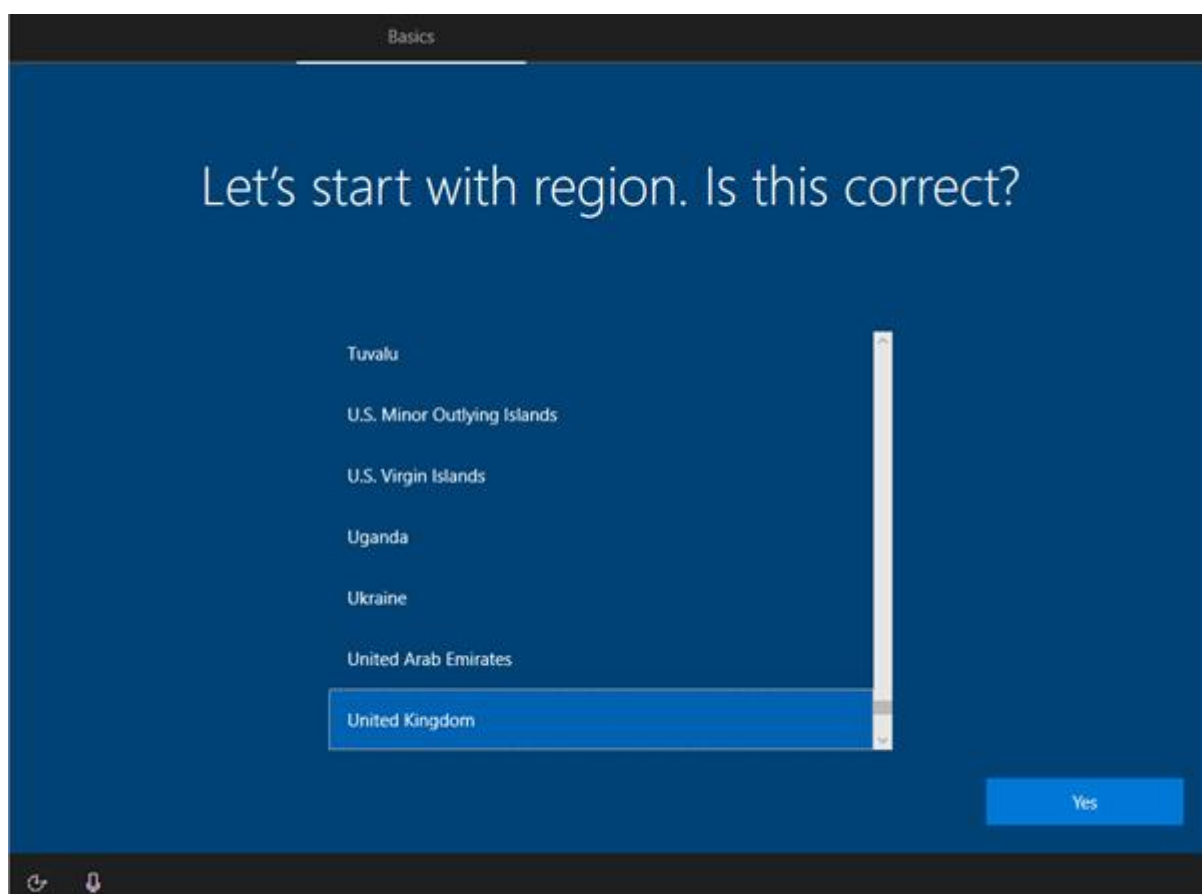
- I agree to the licence as it is essential



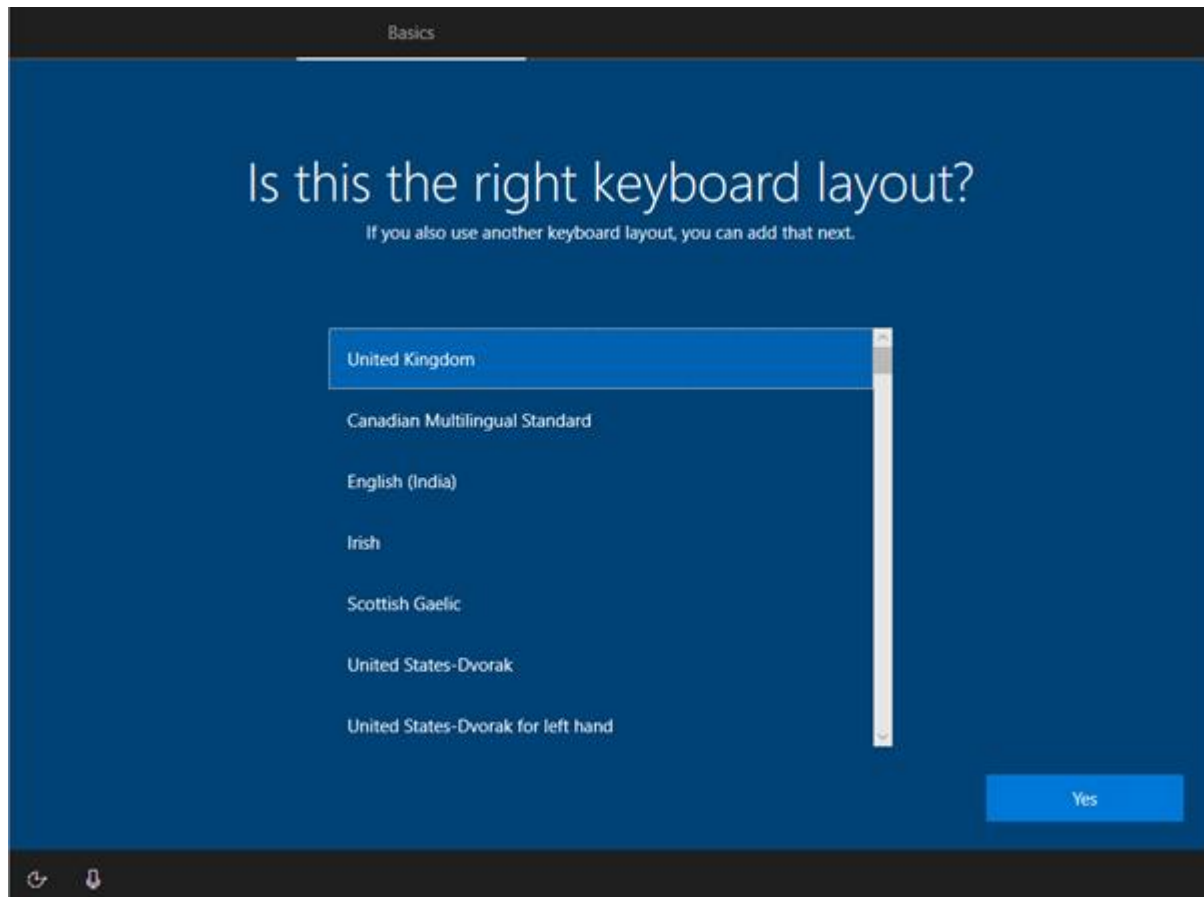
- I select the install method. This one will keep any old data that is there



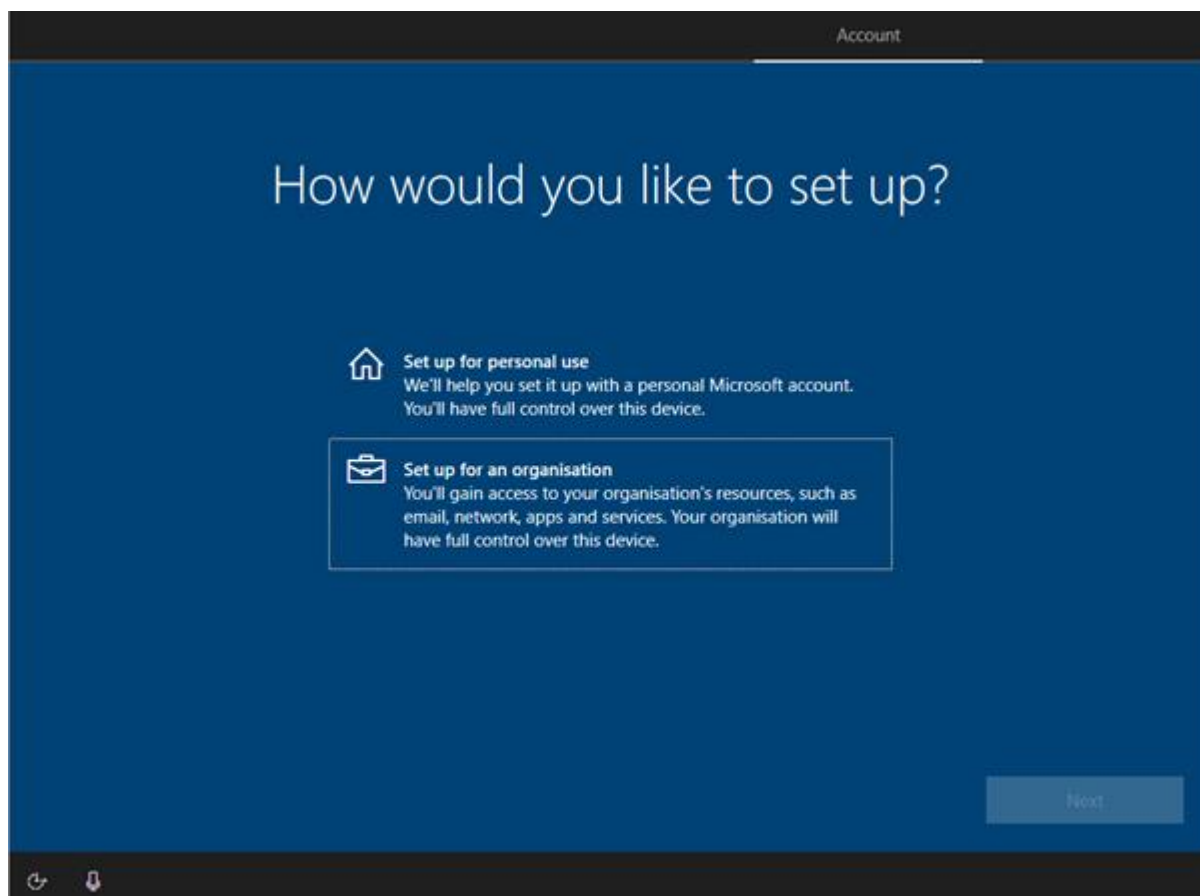
- Windows is now installing, and I wait while it installs itself



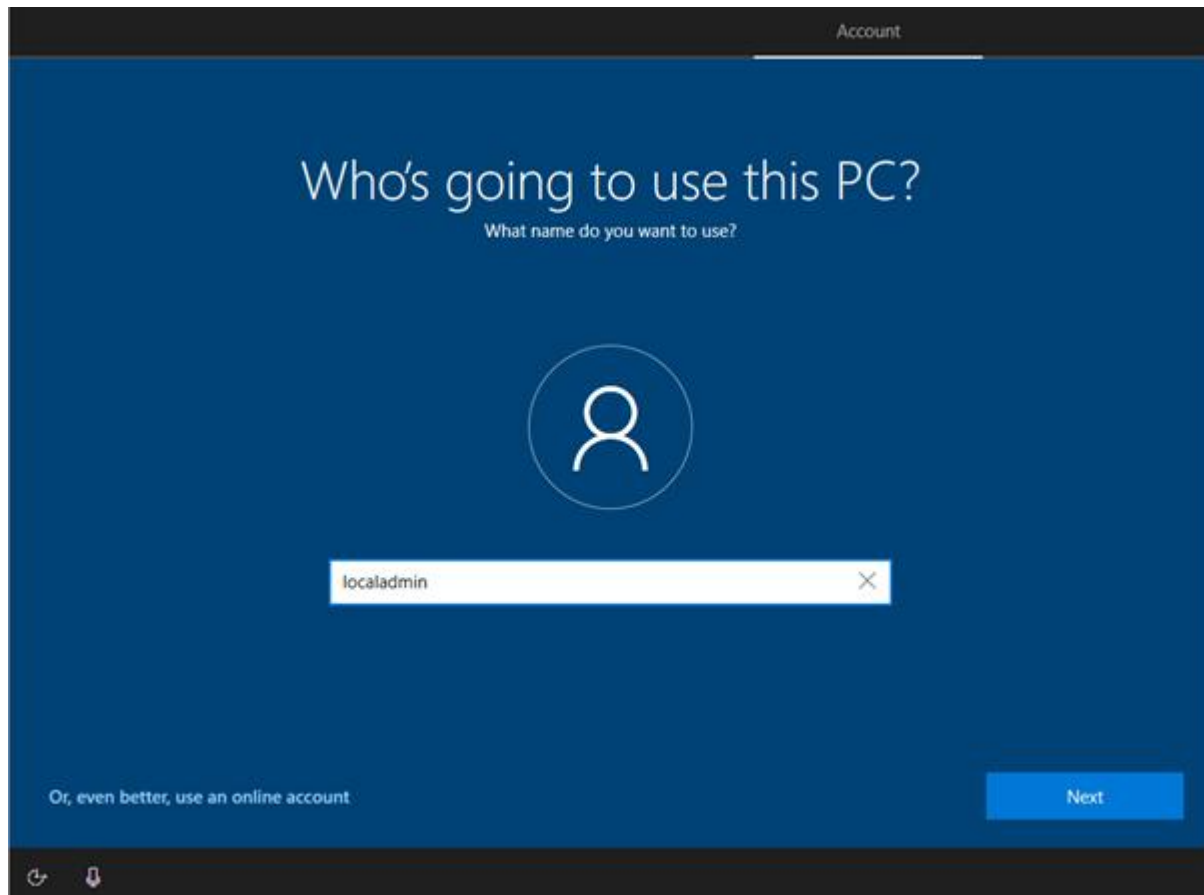
- now I select the region for this install. I choose the UK as that is where the client is located



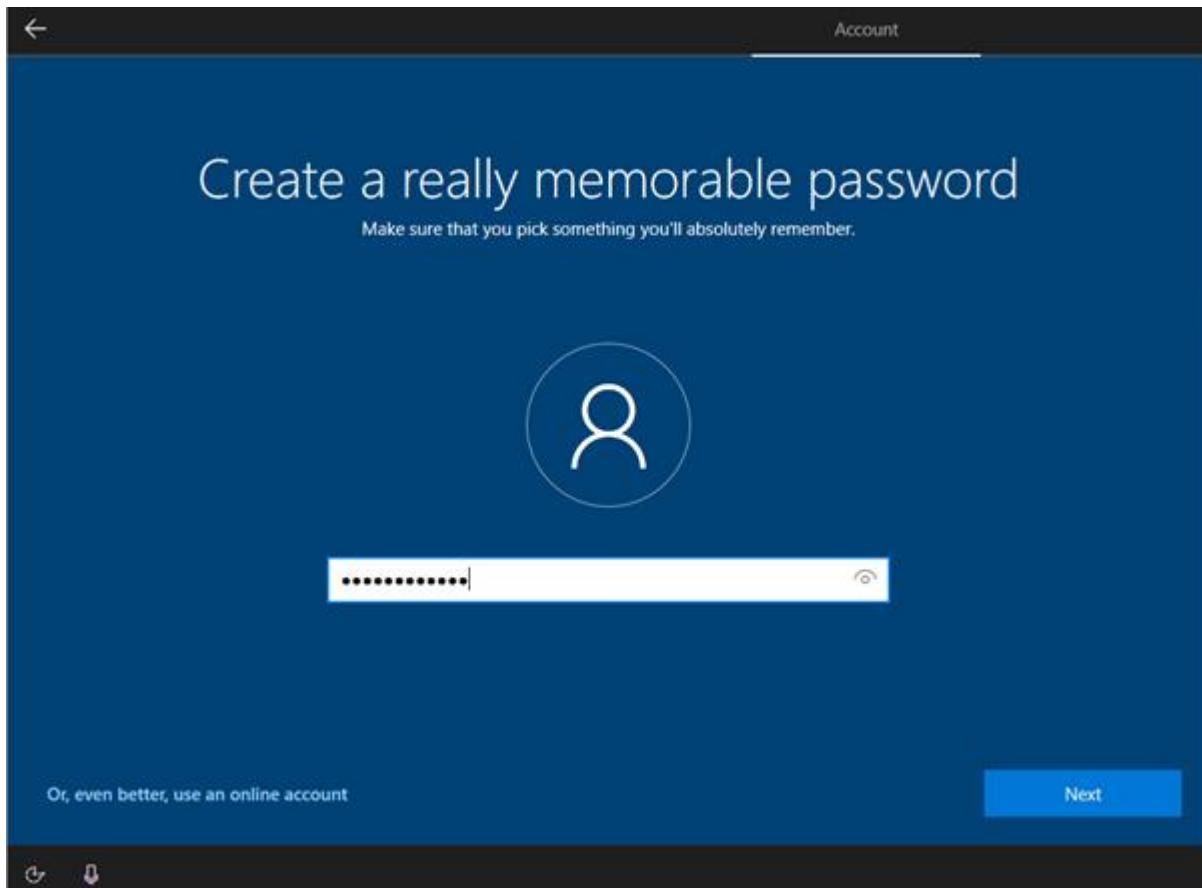
- I choose a keyboard for the UK



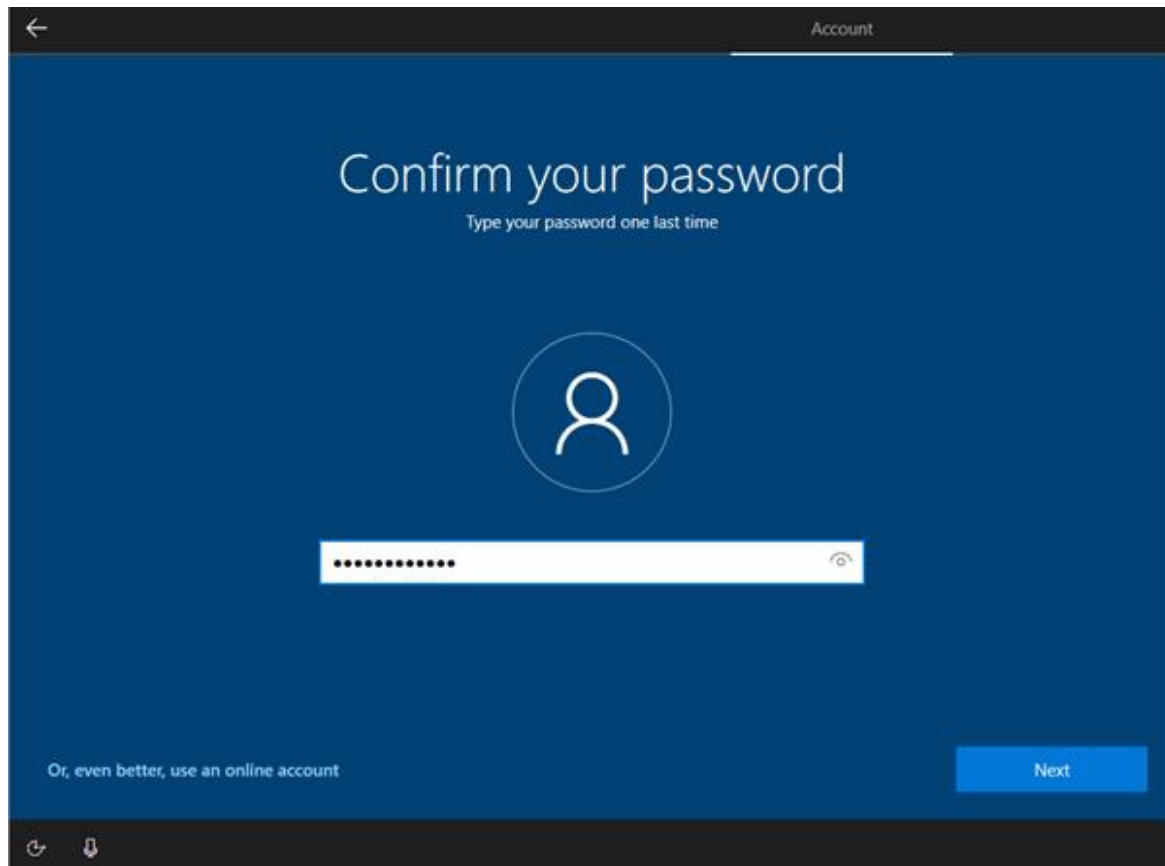
- I choose organisation as this is a company PC



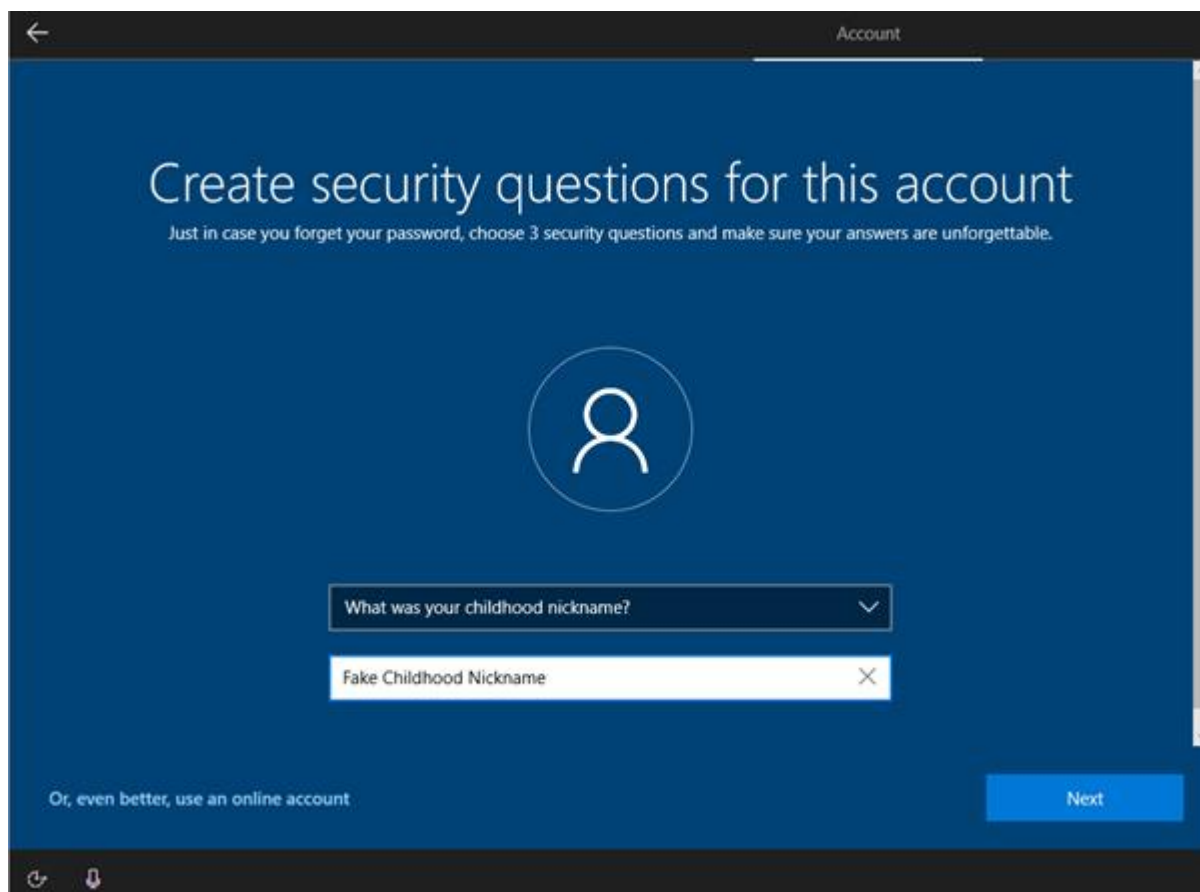
- I add an initial user. This will be an administrator



- I add a password for security



- I confirm the password so there is no mistake in entry




The screenshot shows a Windows account creation window titled "Account". The main heading is "Create security questions for this account", with a subtext: "Just in case you forget your password, choose 3 security questions and make sure your answers are unforgettable." Below this is a circular icon representing a person. A dropdown menu is open, showing the question "What was your childhood nickname?". Below the dropdown is a text input field containing the answer "Fake Childhood Nickname". At the bottom left, there is a link that says "Or, even better, use an online account". At the bottom right is a blue "Next" button. The window has a dark blue background and a dark grey header bar with a back arrow on the left and the word "Account" on the right.

- I now create a memorable question and answer. This helps me to be able to retrieve my account

← Account

## Create security questions for this account

Just in case you forget your password, choose 3 security questions and make sure your answers are unforgettable.



What was your first pet's name? ▾

Fake Pet Name ✕

Or, even better, use an online account


Next

- I add another question and answer

← Account

## Create security questions for this account

Just in case you forget your password, choose 3 security questions and make sure your answers are unforgettable.



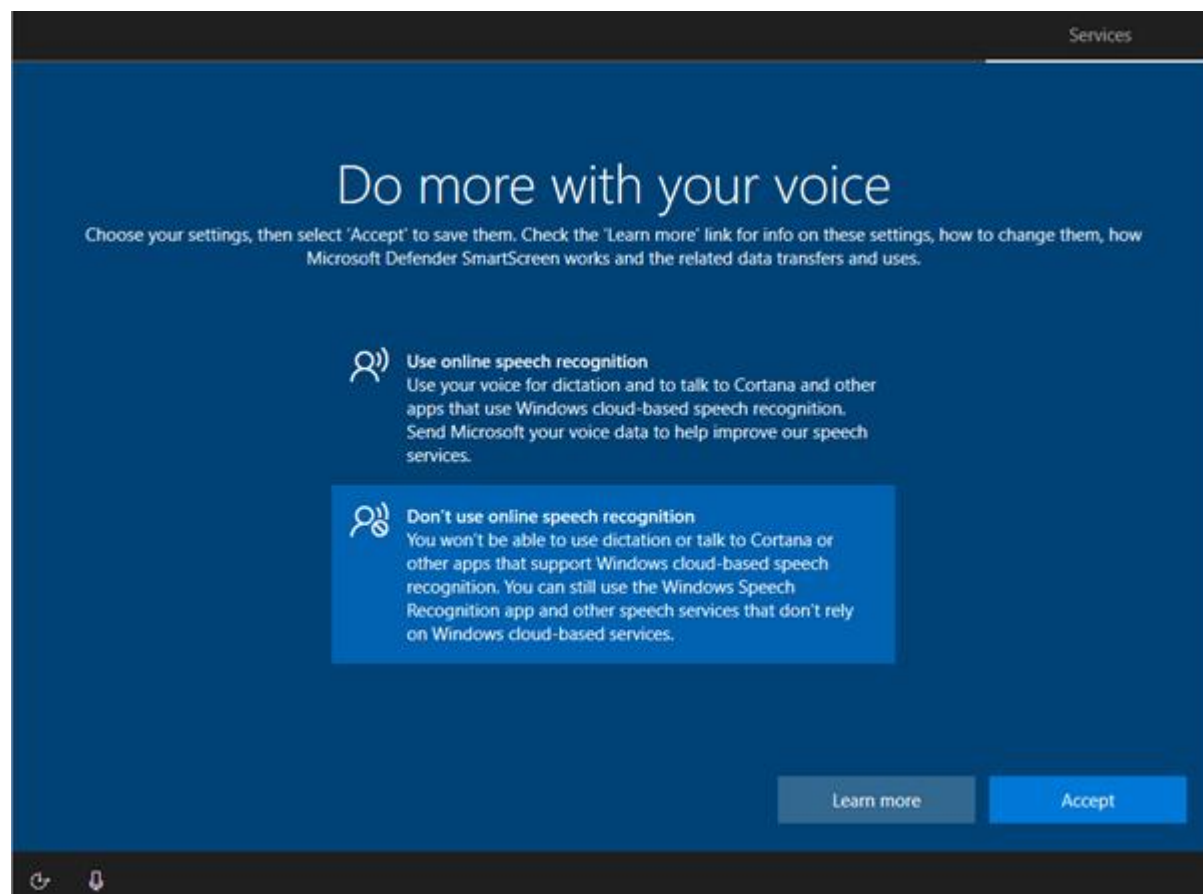
What is the name of the city where you were born? ▾

Fake City ✕

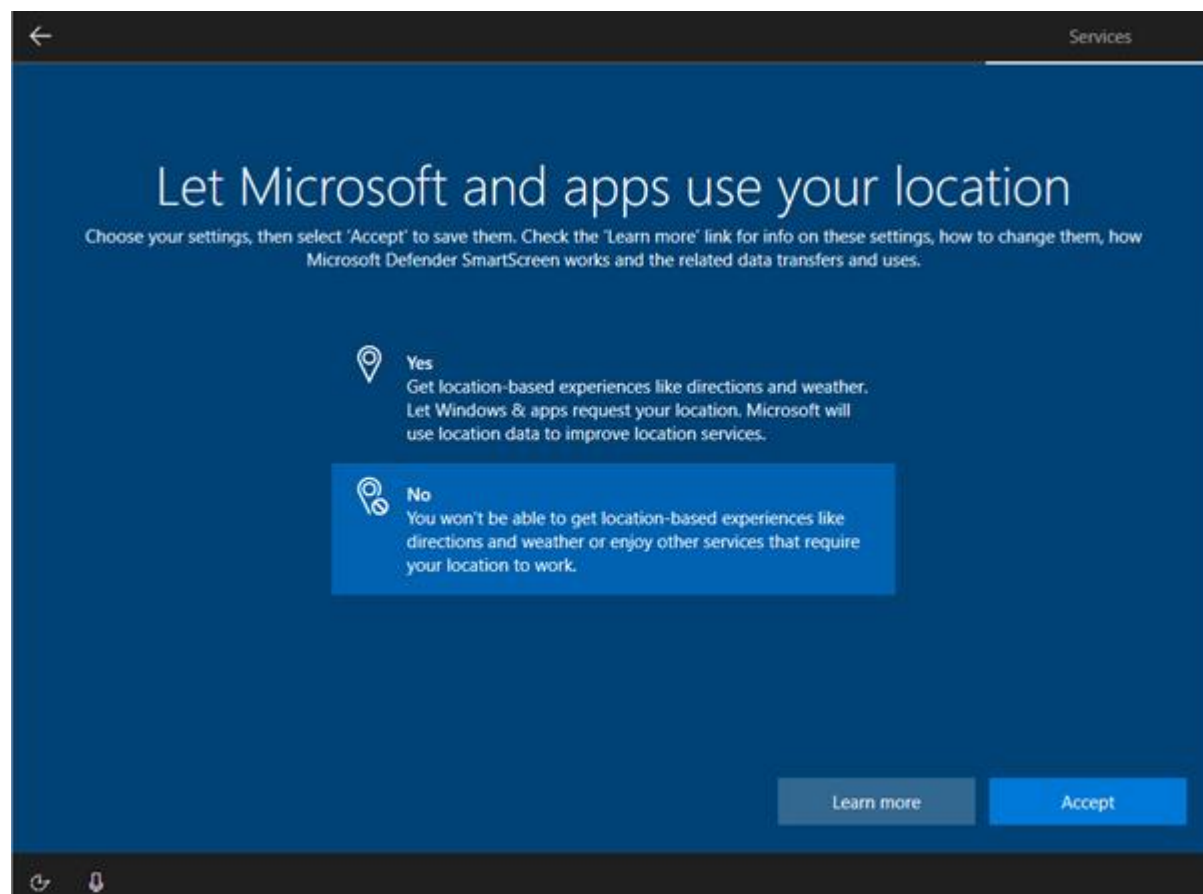
Or, even better, use an online account

Next

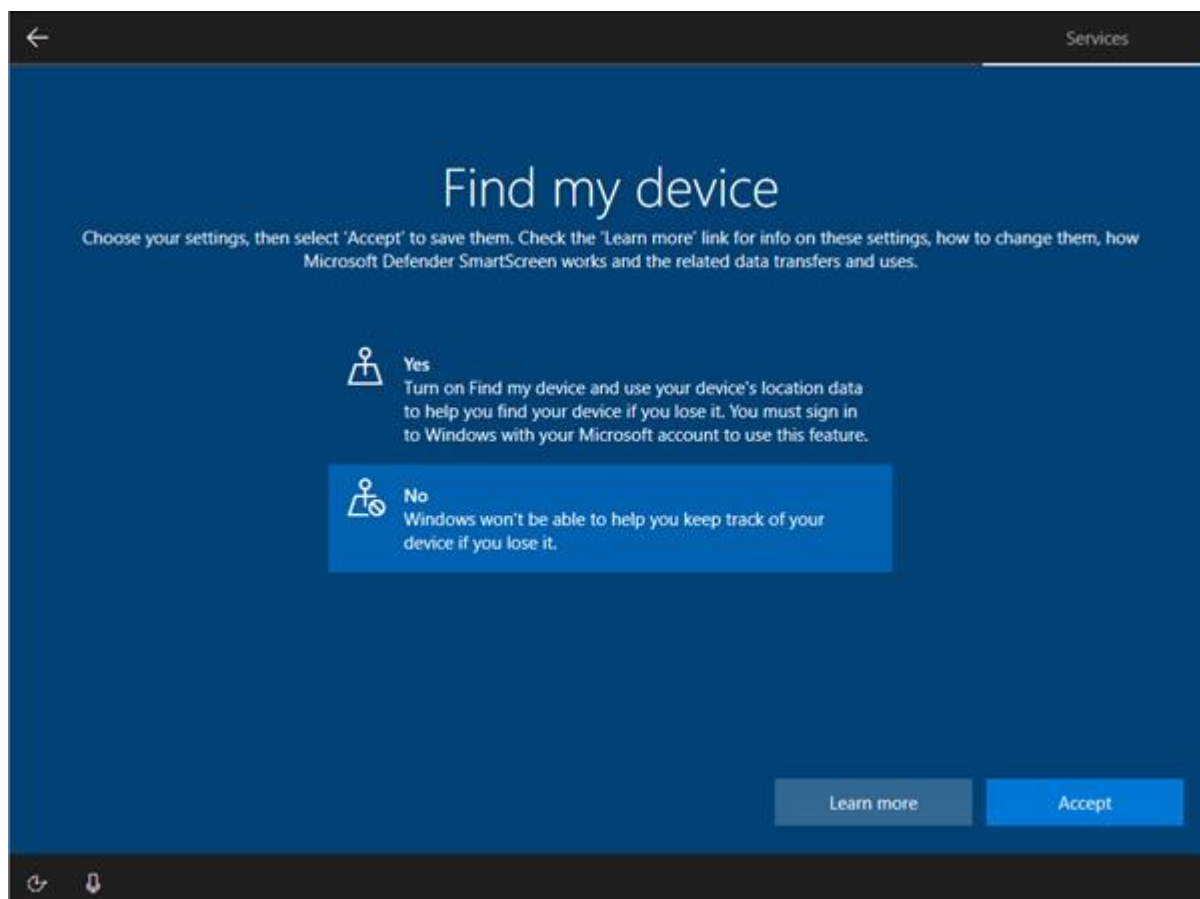
- and a third question and answer are added. These will help if I forget the password



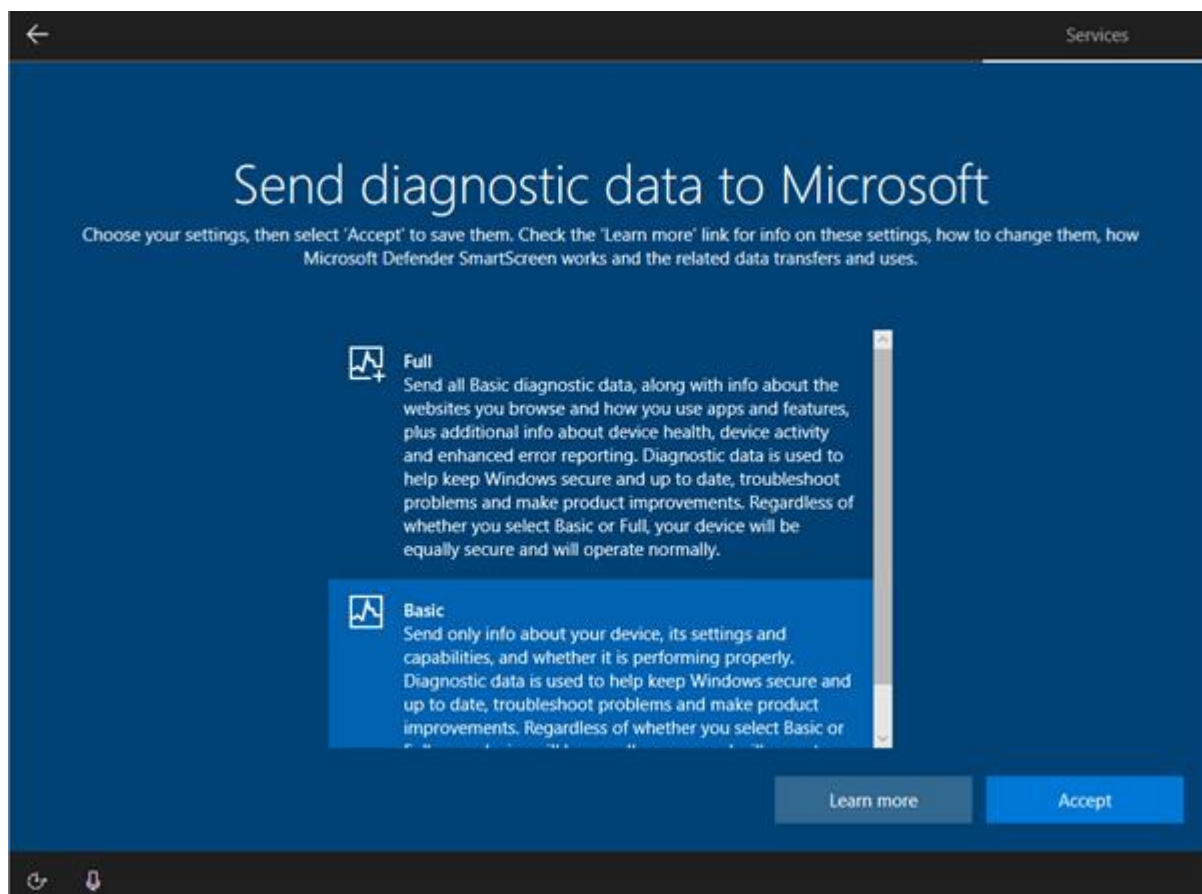
- I decline the new features of Windows (like voice) as this is a corporate machine and not requested



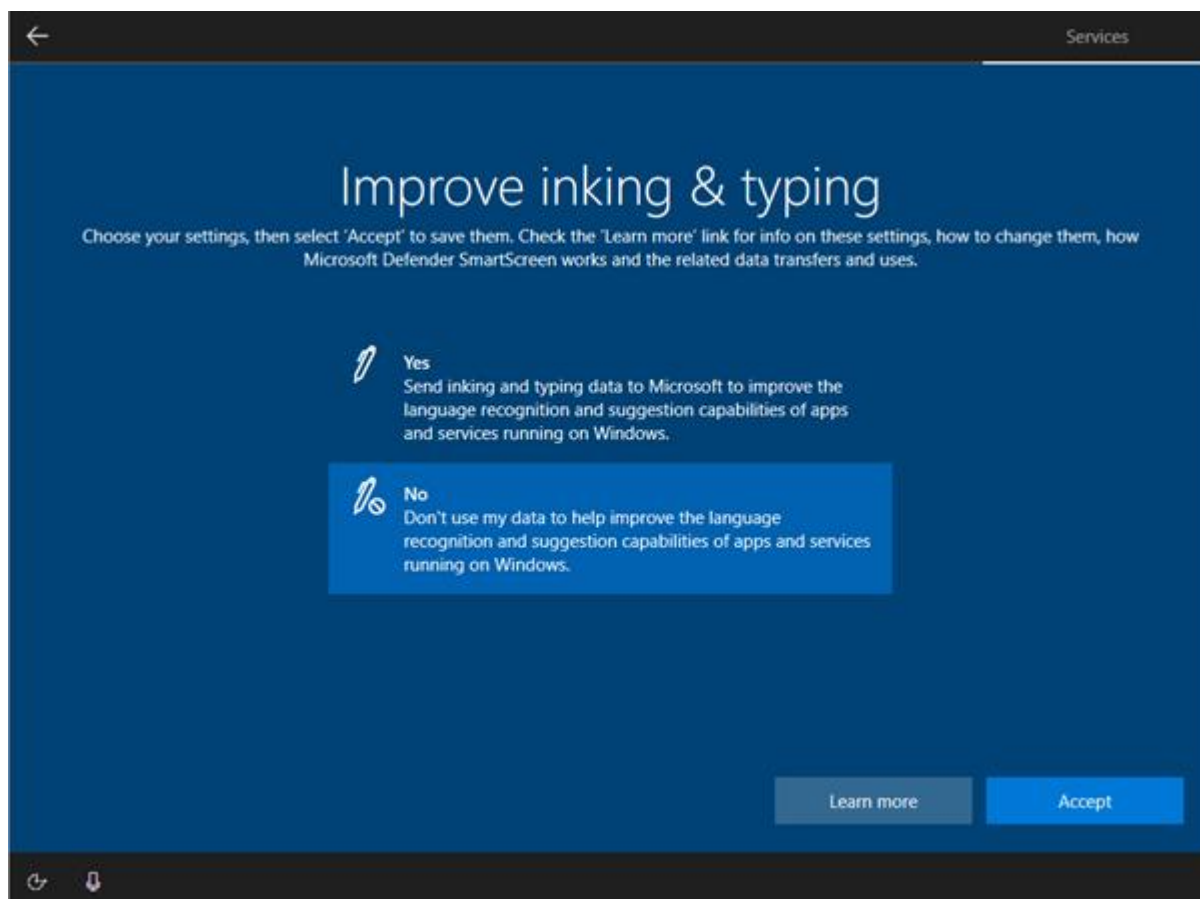
- I decline location as this could be a security issue



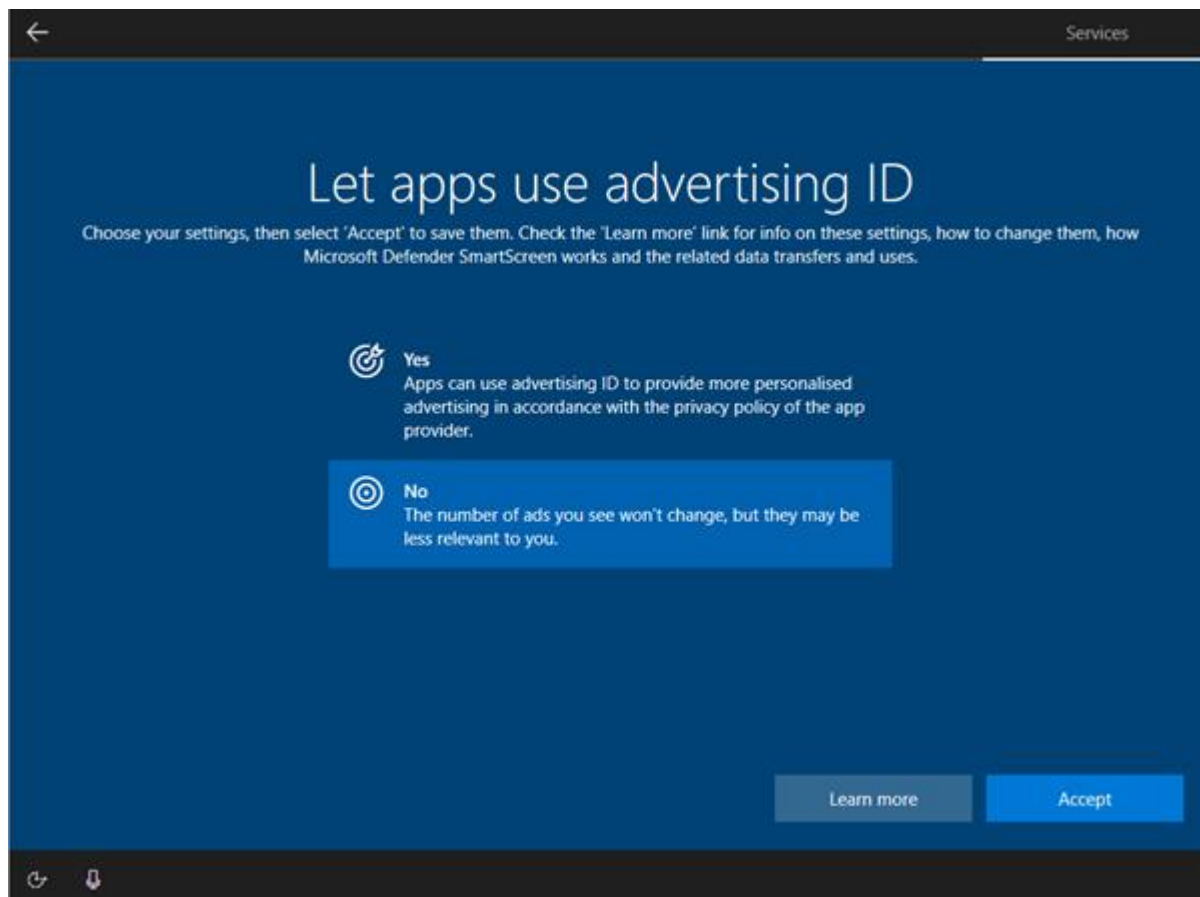
- I do not need to find my device as it is a VM



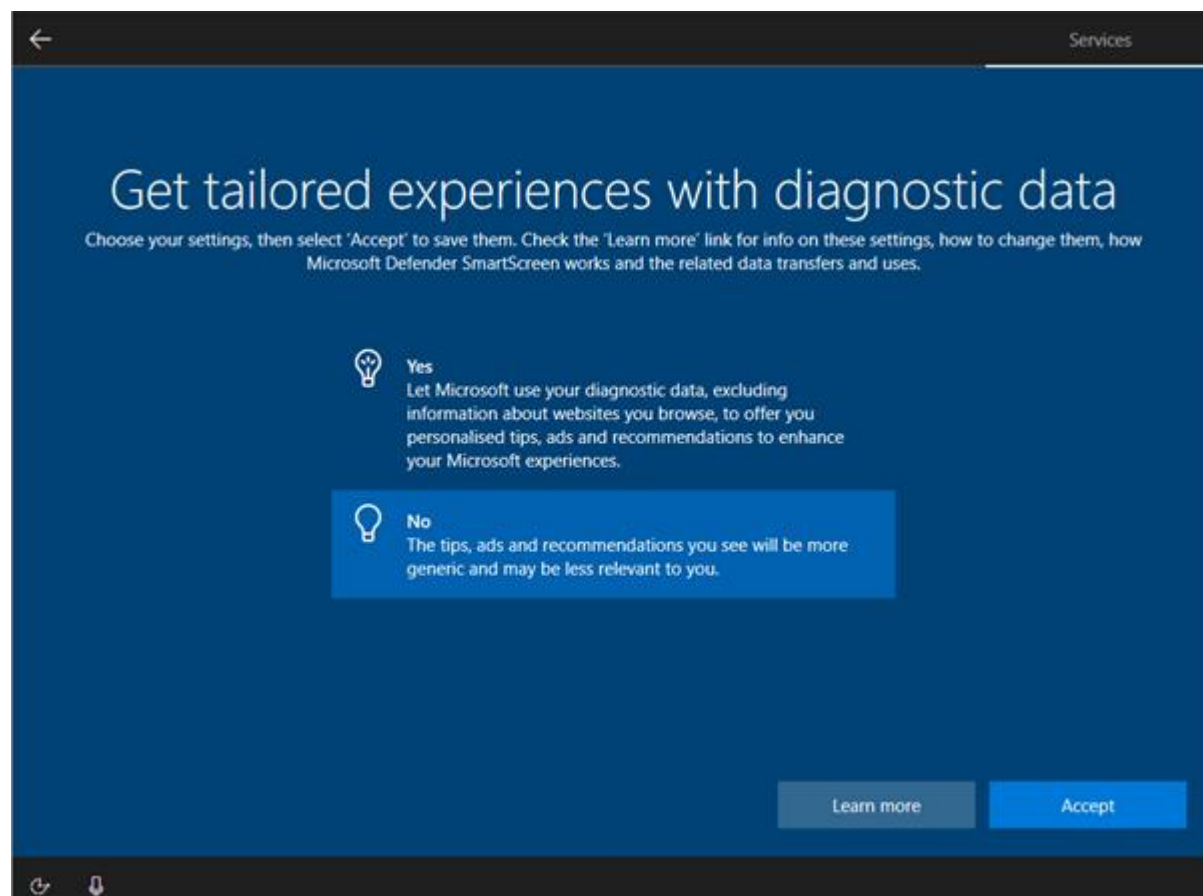
- and I do not want to send data to Microsoft as, again, this could be a security risk



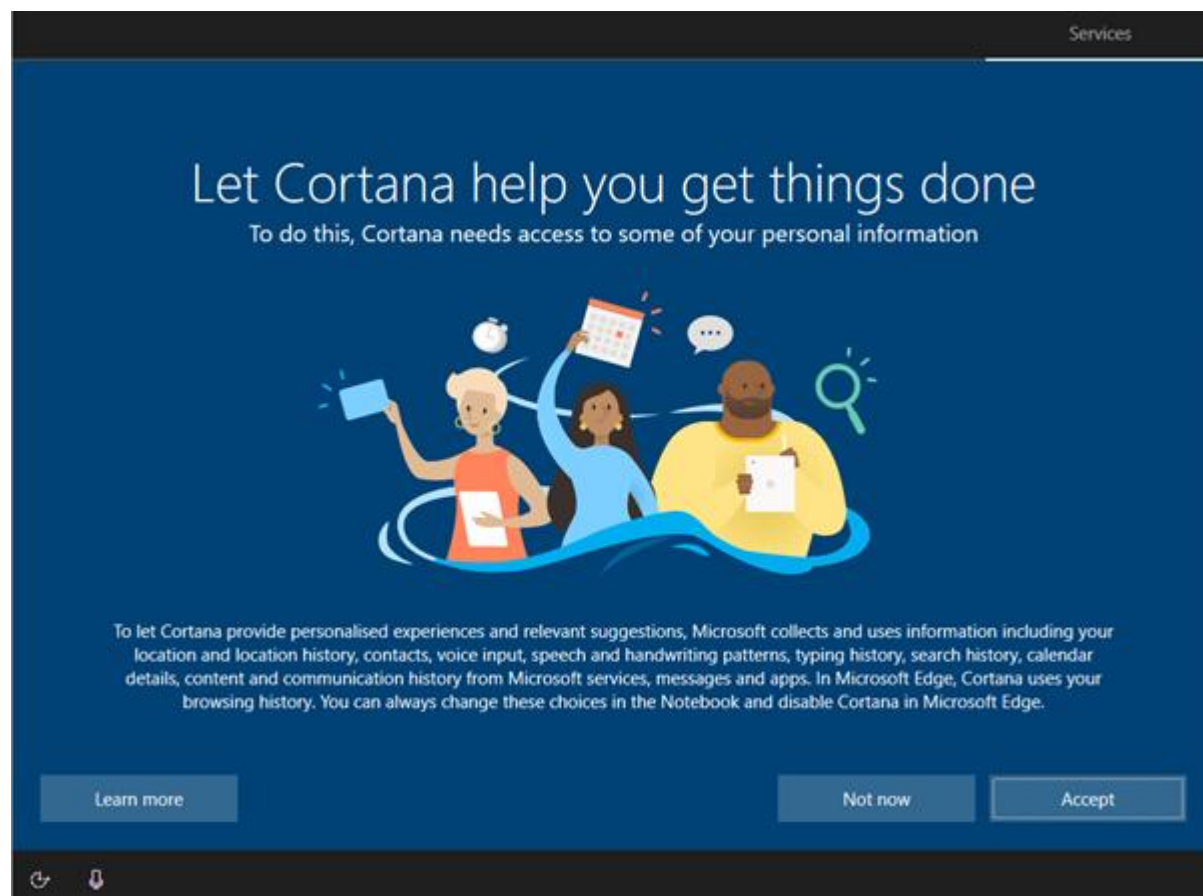
- I do not want ink as I will not be using handwriting



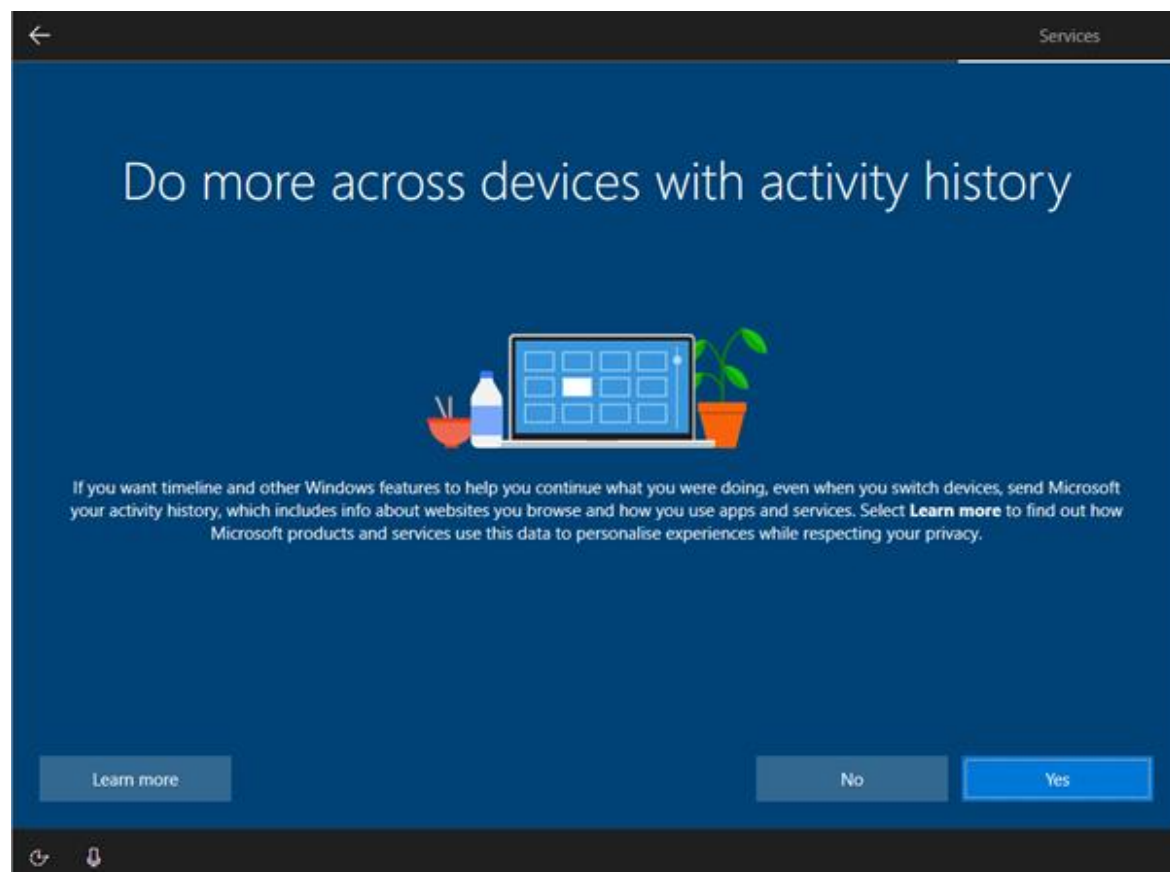
- I do not choose location as, again, this is a security risk



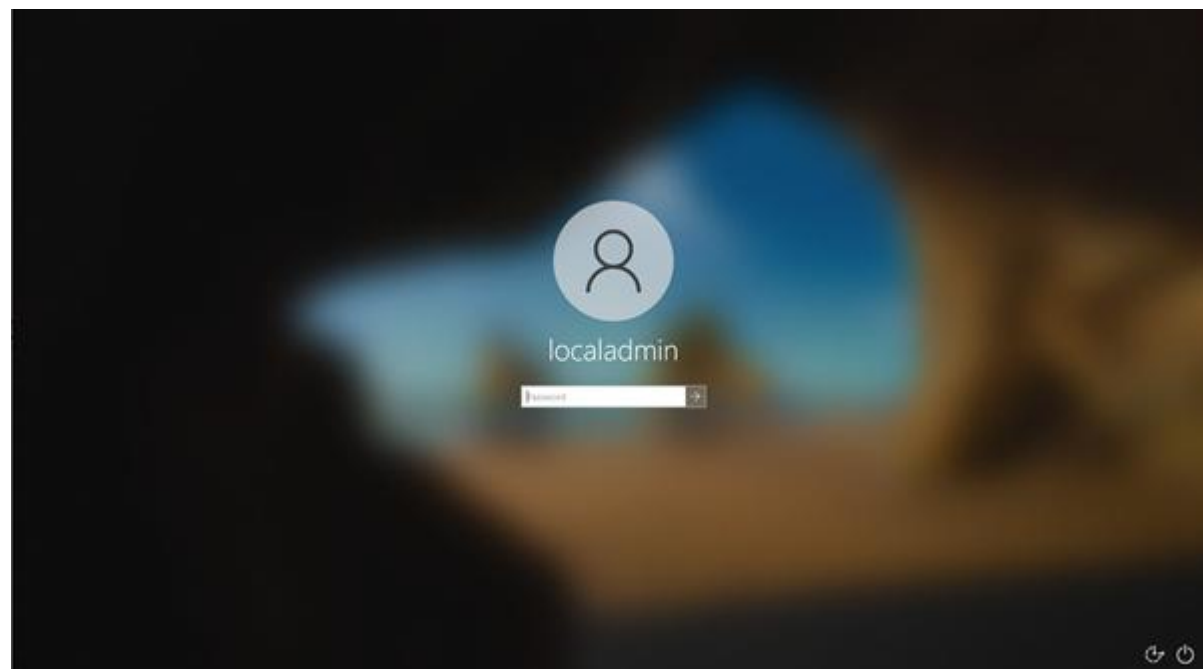
- I do not want tailored diagnostics because it could be a security risk



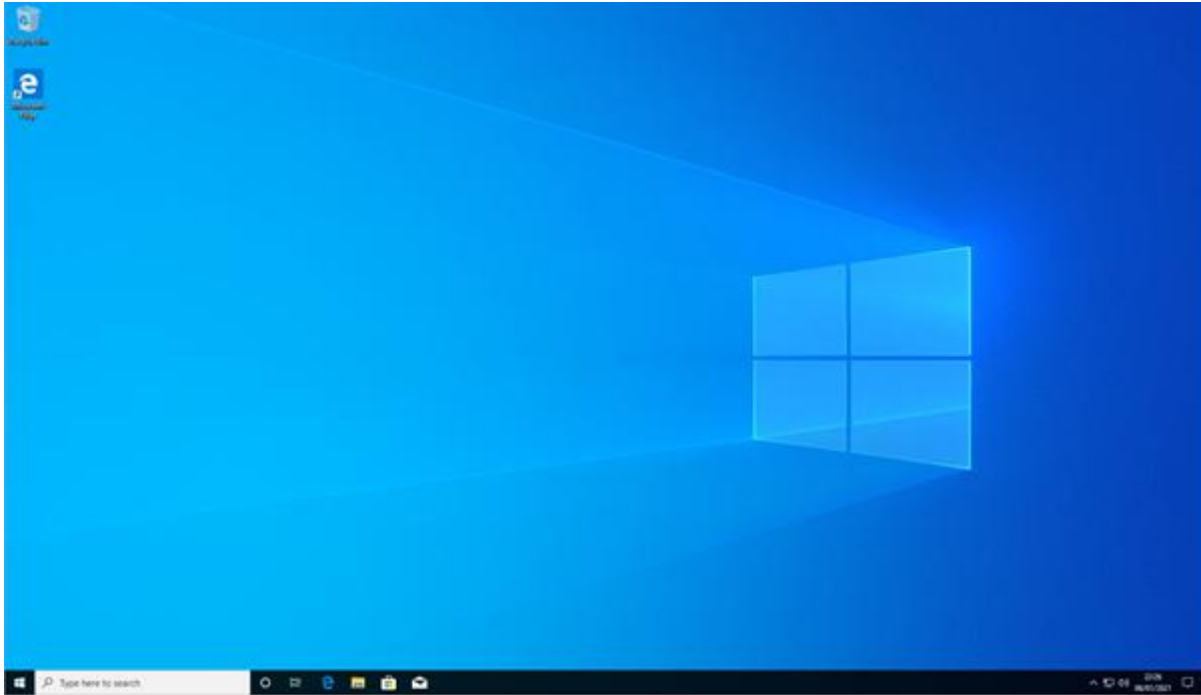
- I accept Cortana as Windows will not run properly without it



- I keep active history as it could be useful to users



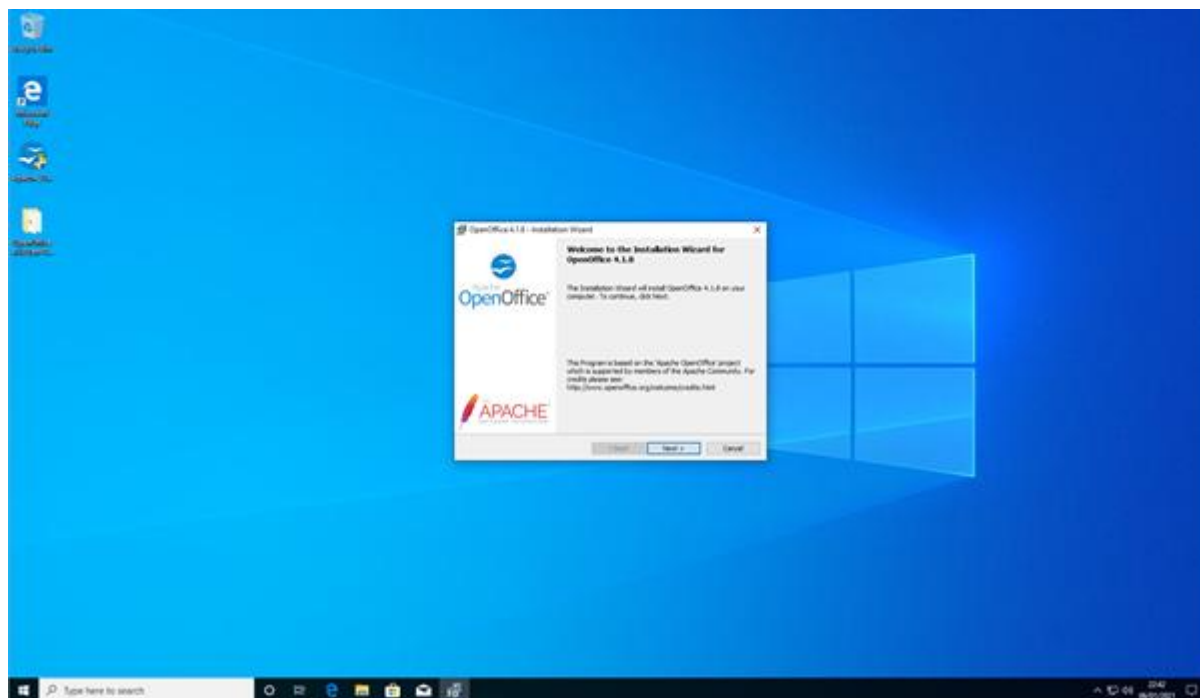
- I can now log in as the local admin



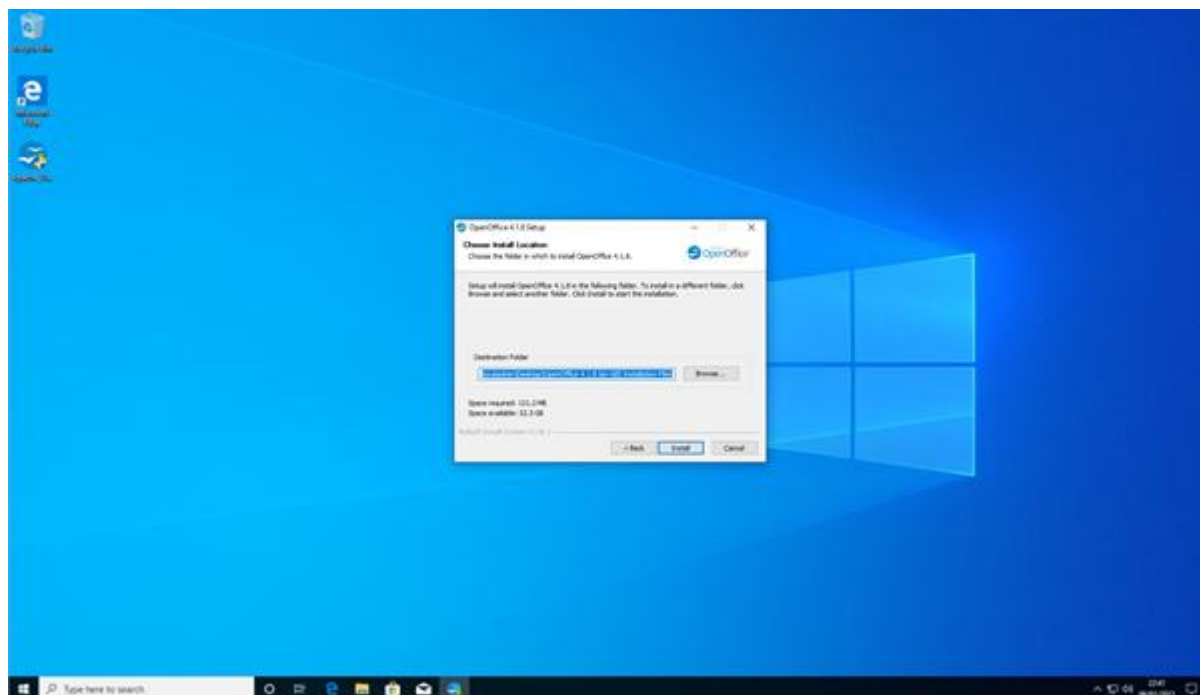
- Windows is now installed and logged in

## Installing software

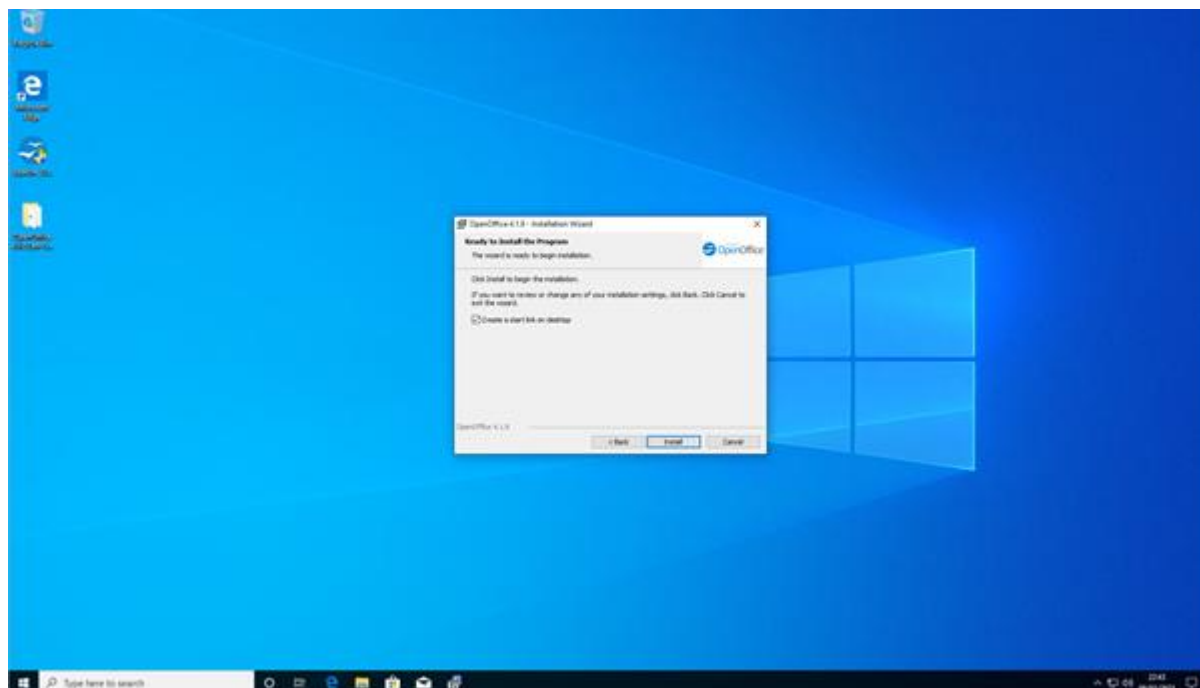
These screenshots show me installing OpenOffice:



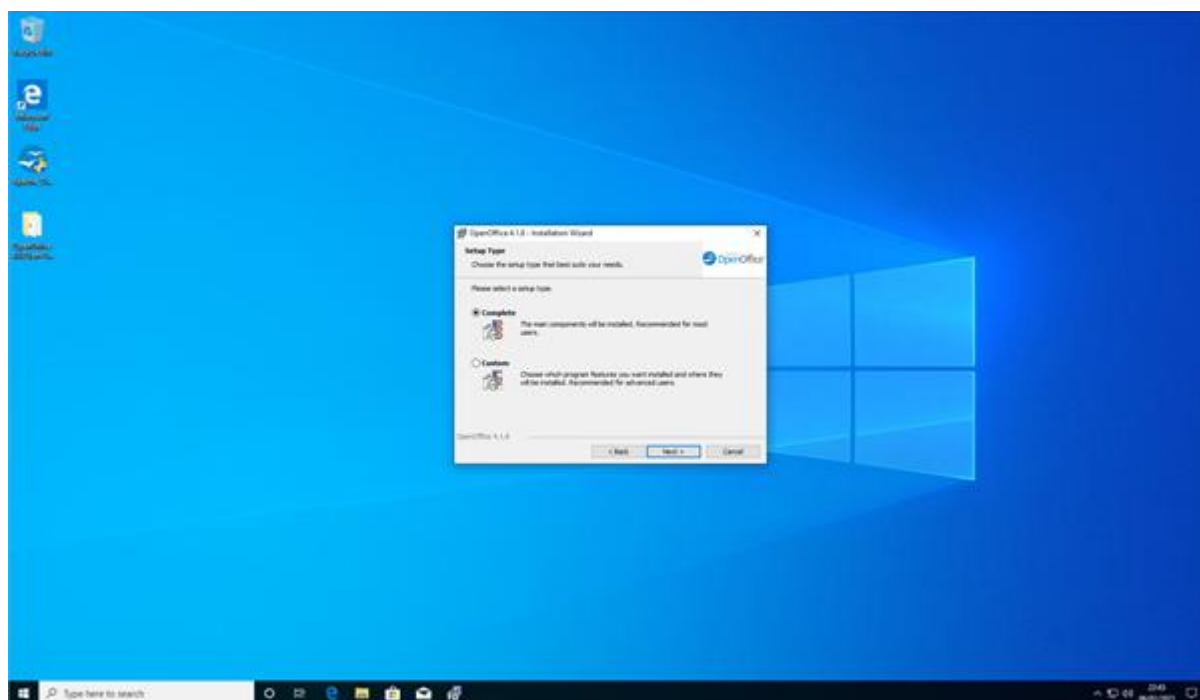
- I click next to use default settings as this is suitable for most installations



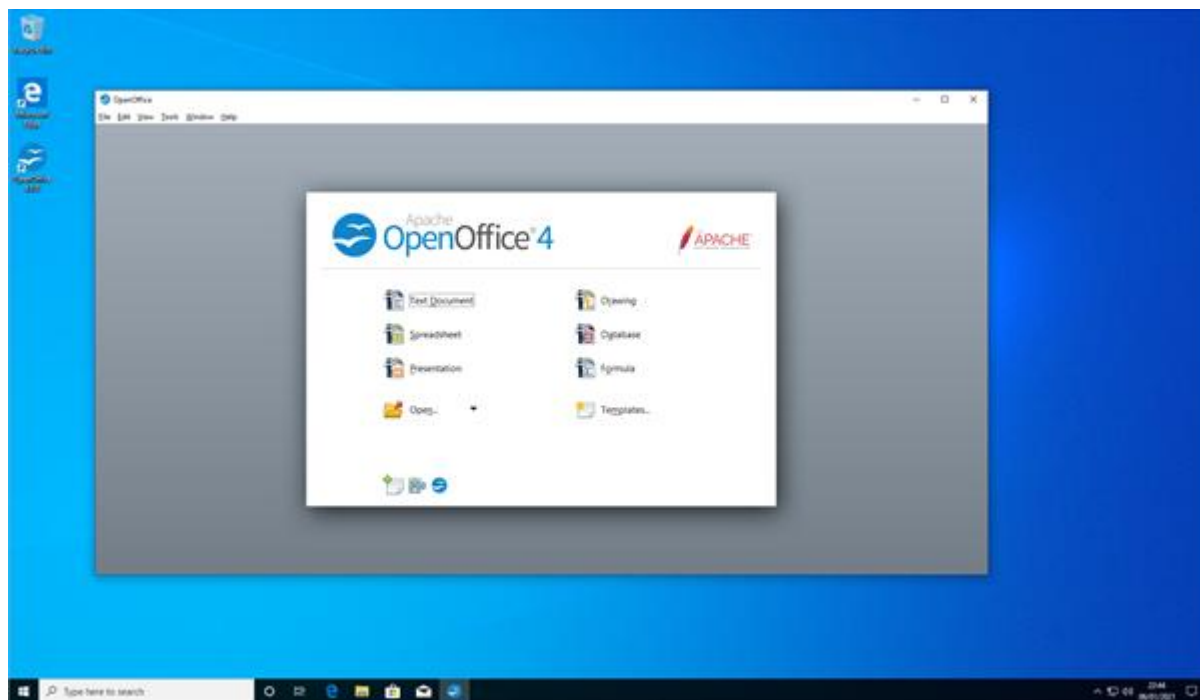
- I select the installation location. I keep the default



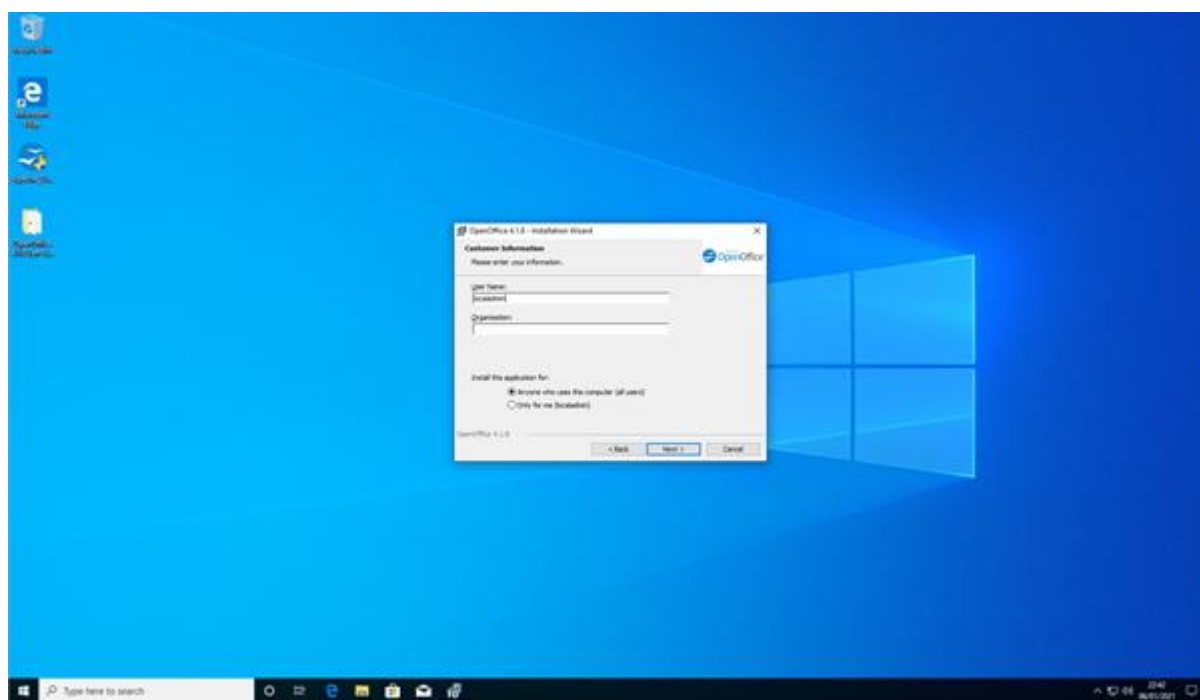
- I click next



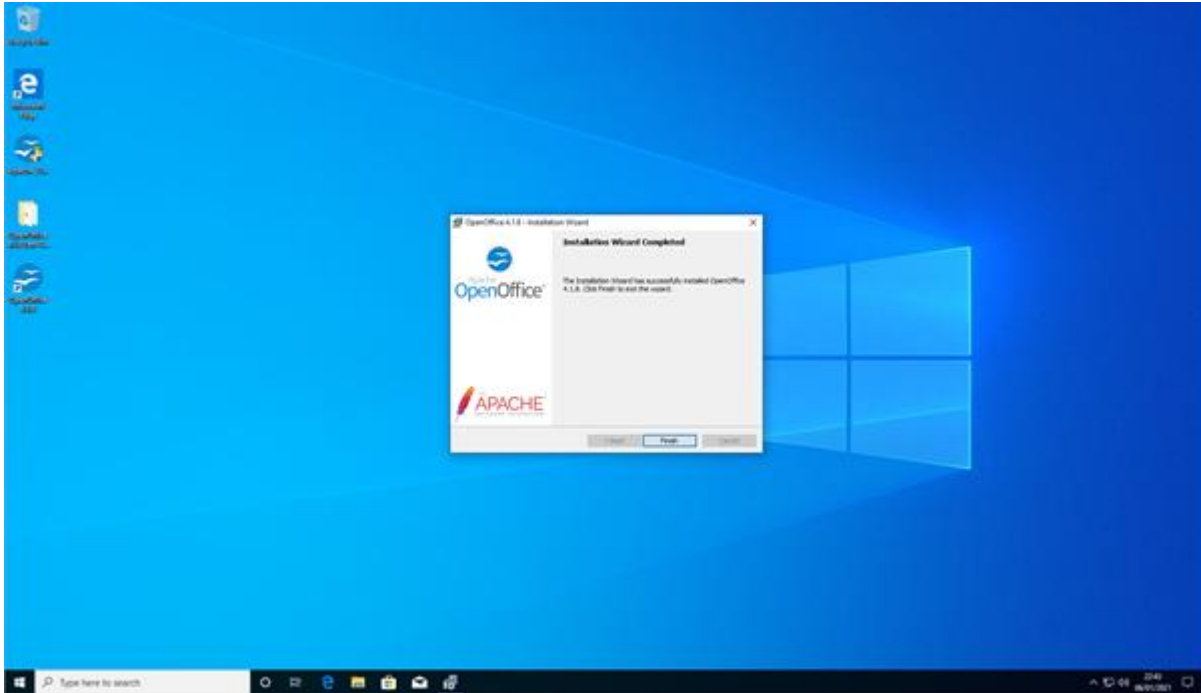
- I select installation type



- Office is installing



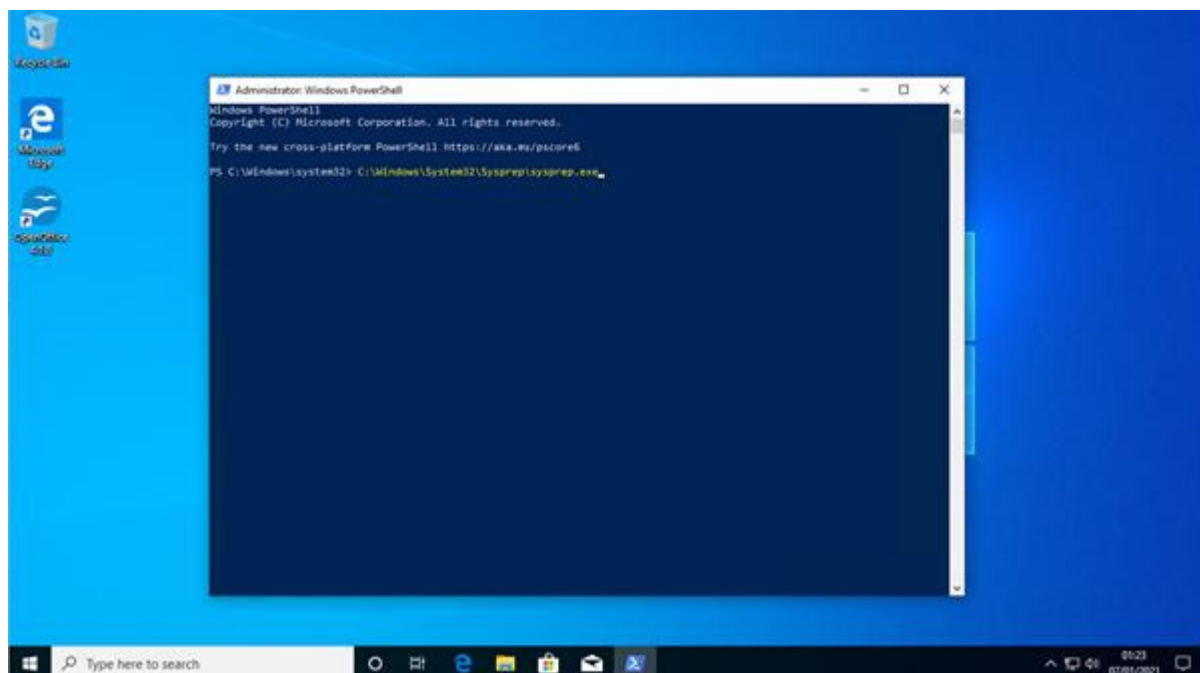
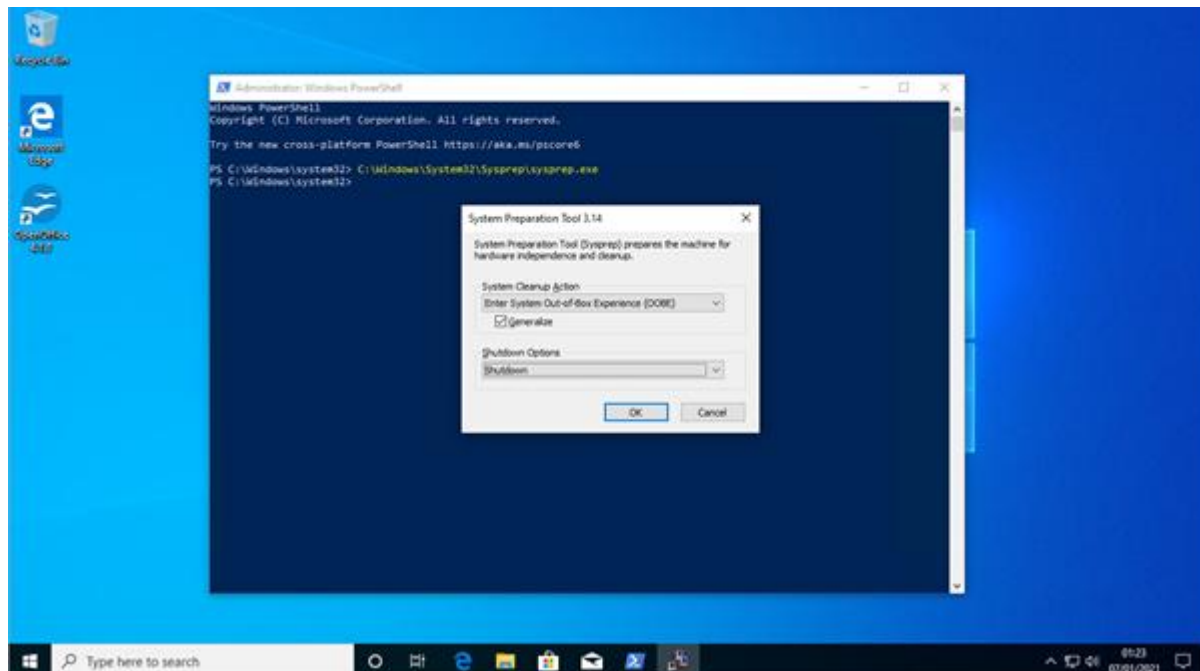
- I create a username



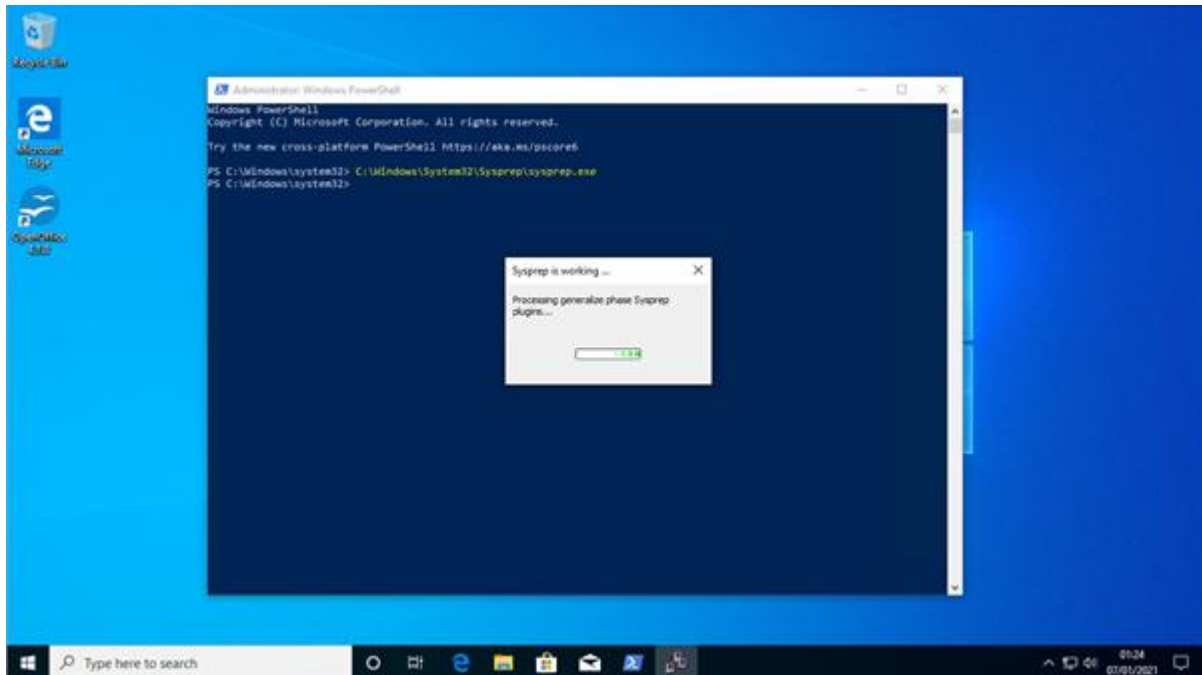
- and I follow the prompts by clicking next when required
- I have now installed OpenOffice

## Create reference image

### Sysprep



- I run Sysprep to remove the PC's unique identifiers. These will be recreated when the PC boots after being imaged

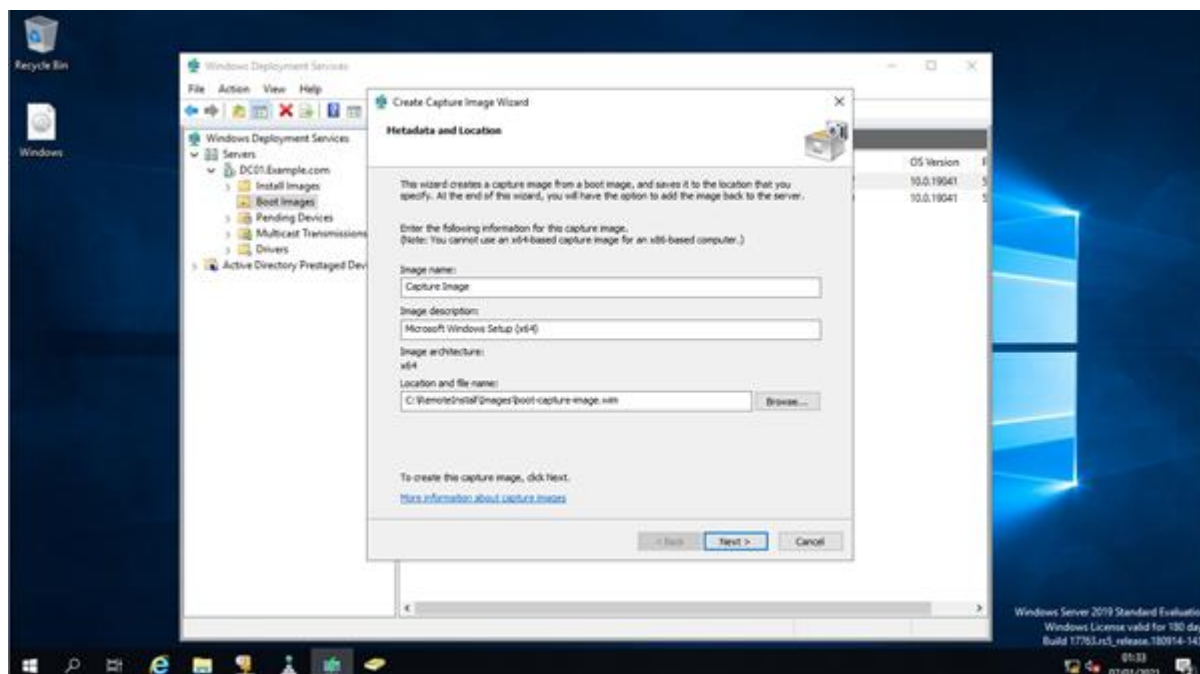


- once finished, it will close down the machine

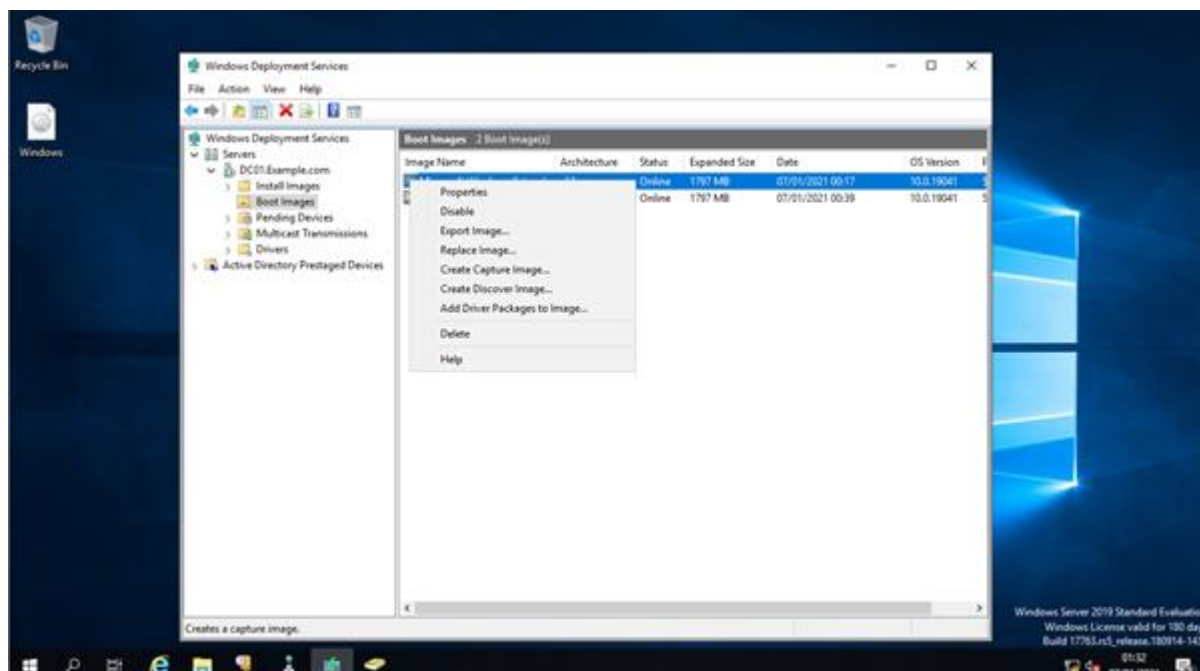
## Capturing an image using WDS

### Create a capture boot image

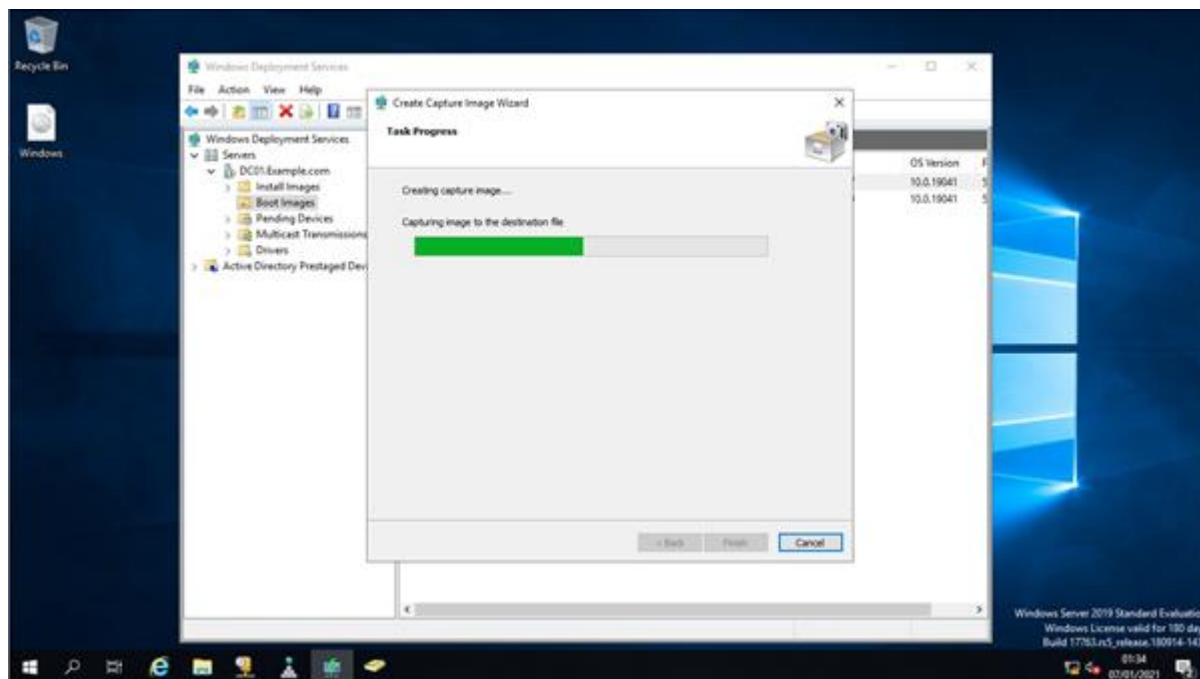
- I make a boot image



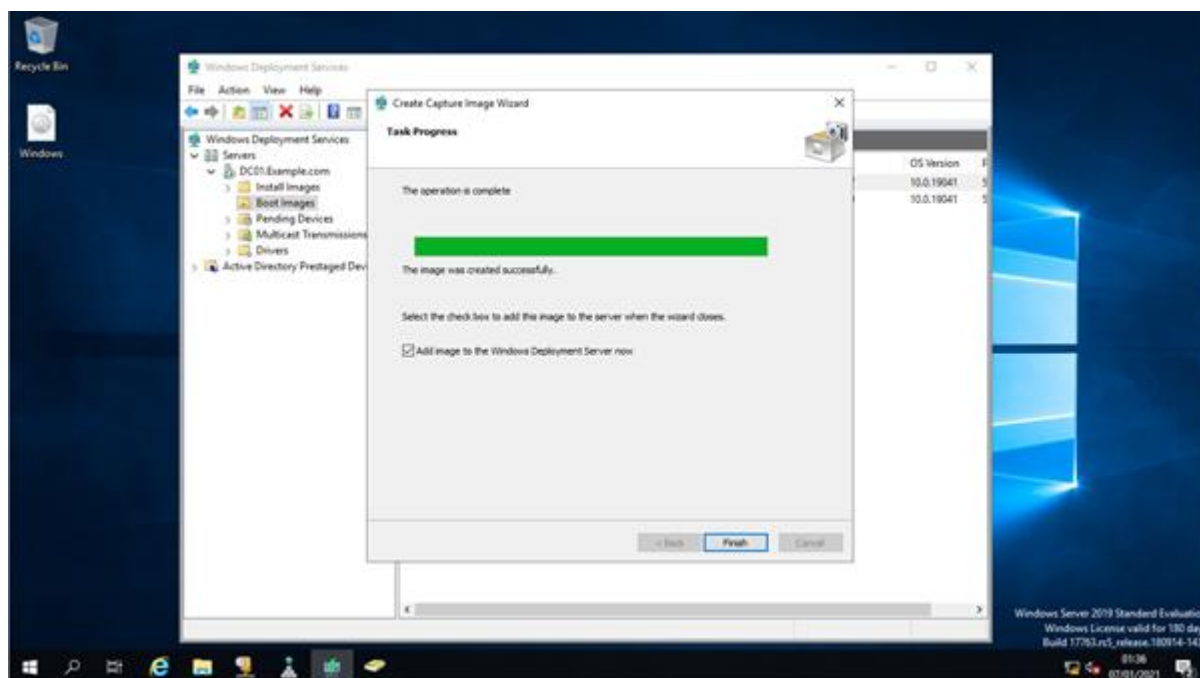
- I name the image



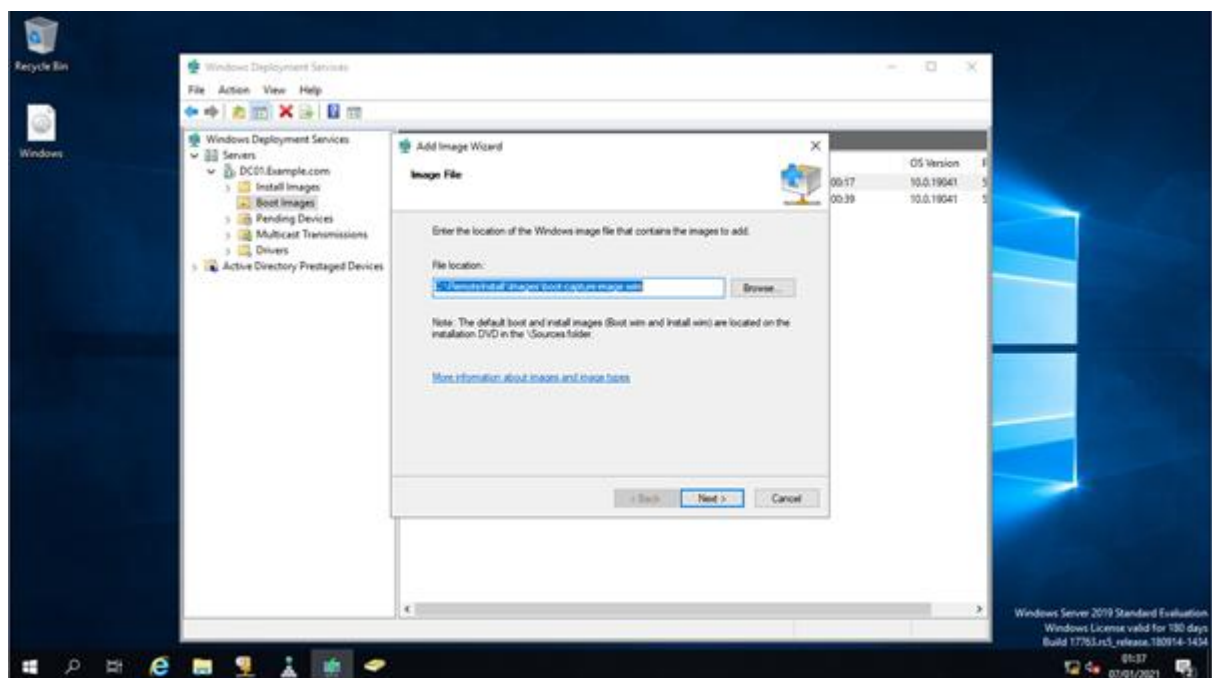
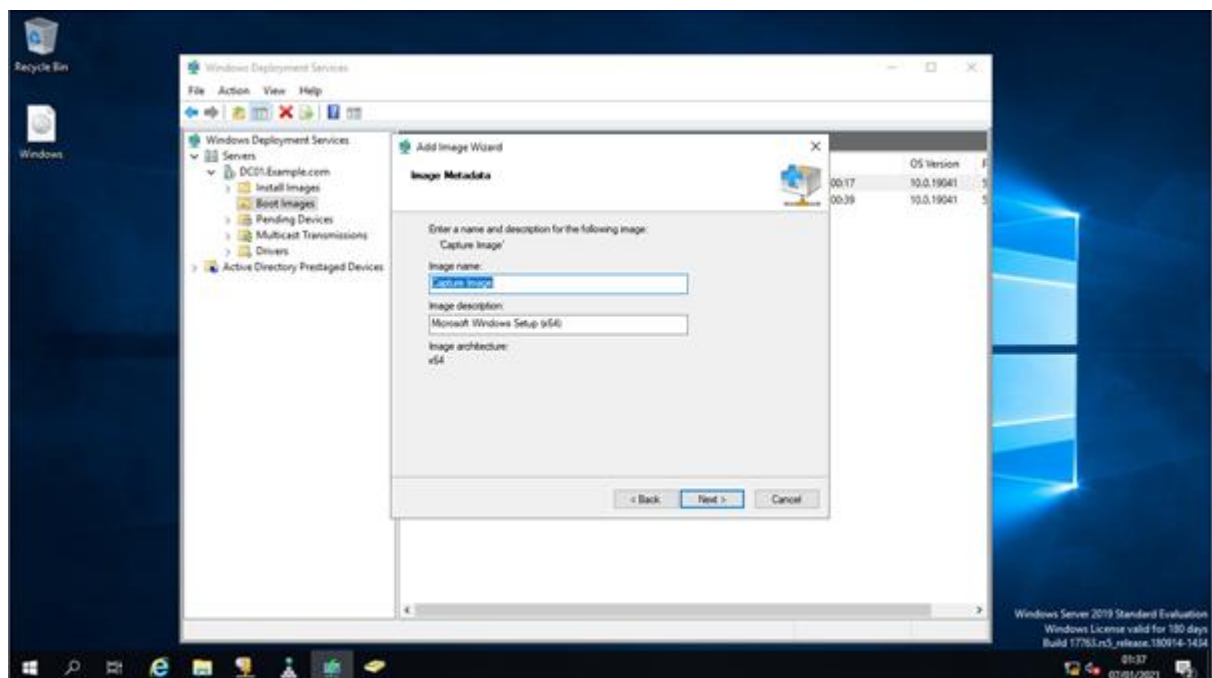
- I select a location and upload



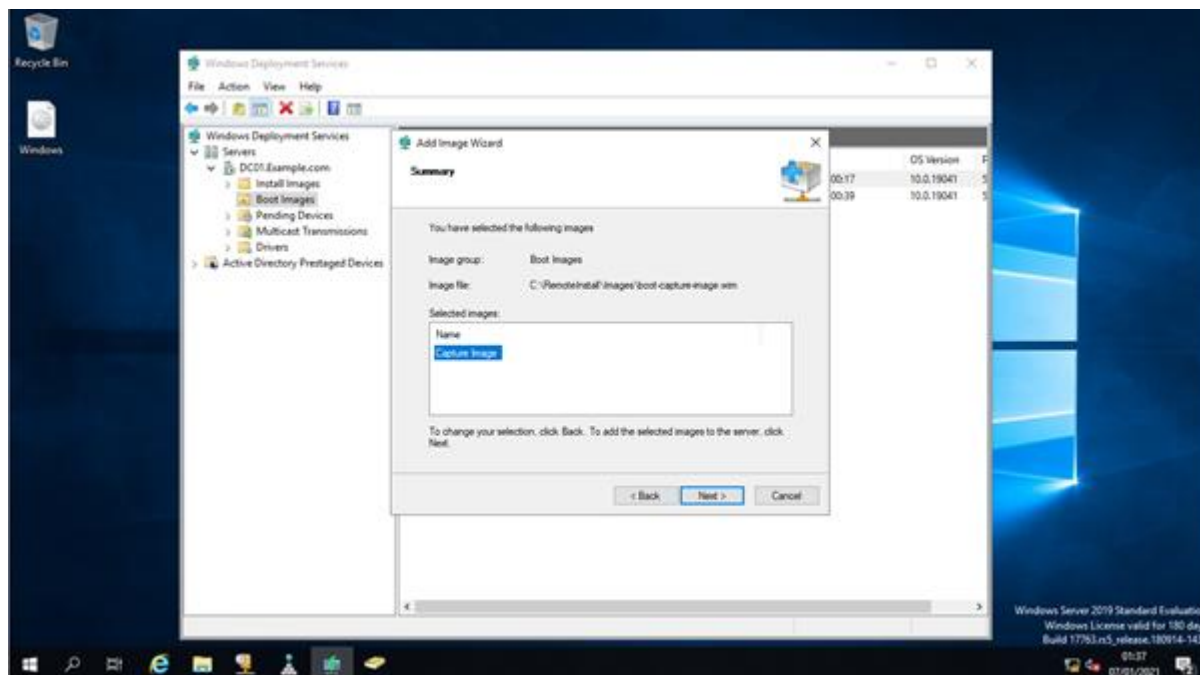
- using WDS on my management machine, I create a capture for the image



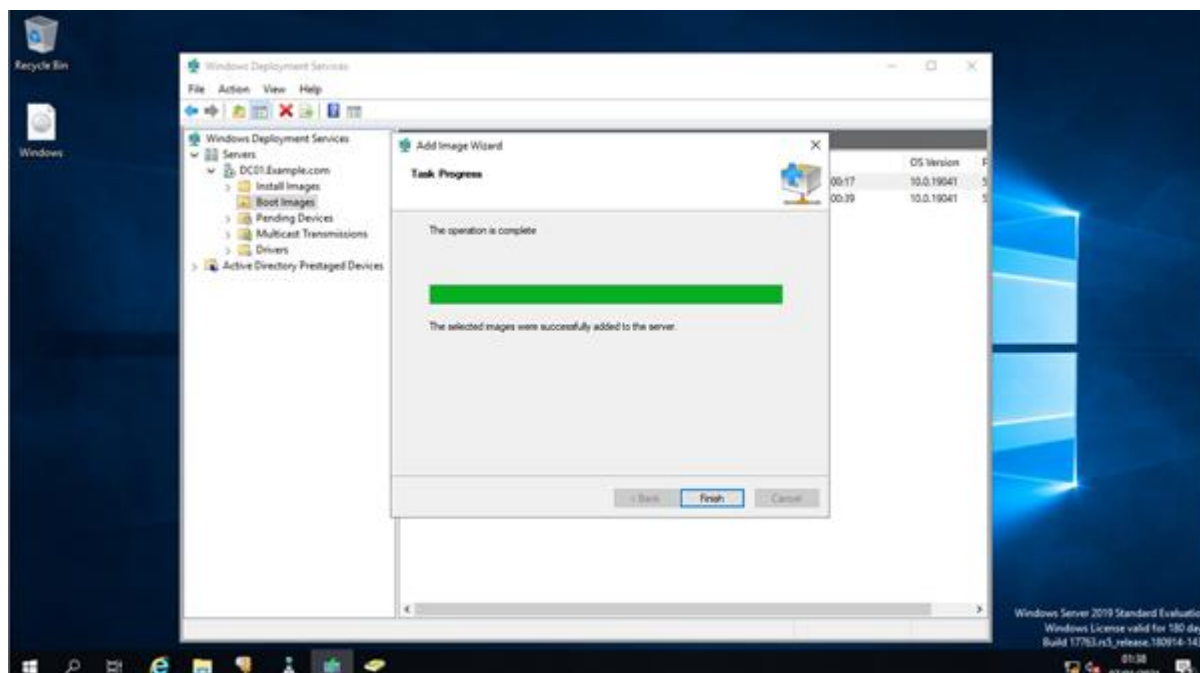
- I click finish to complete



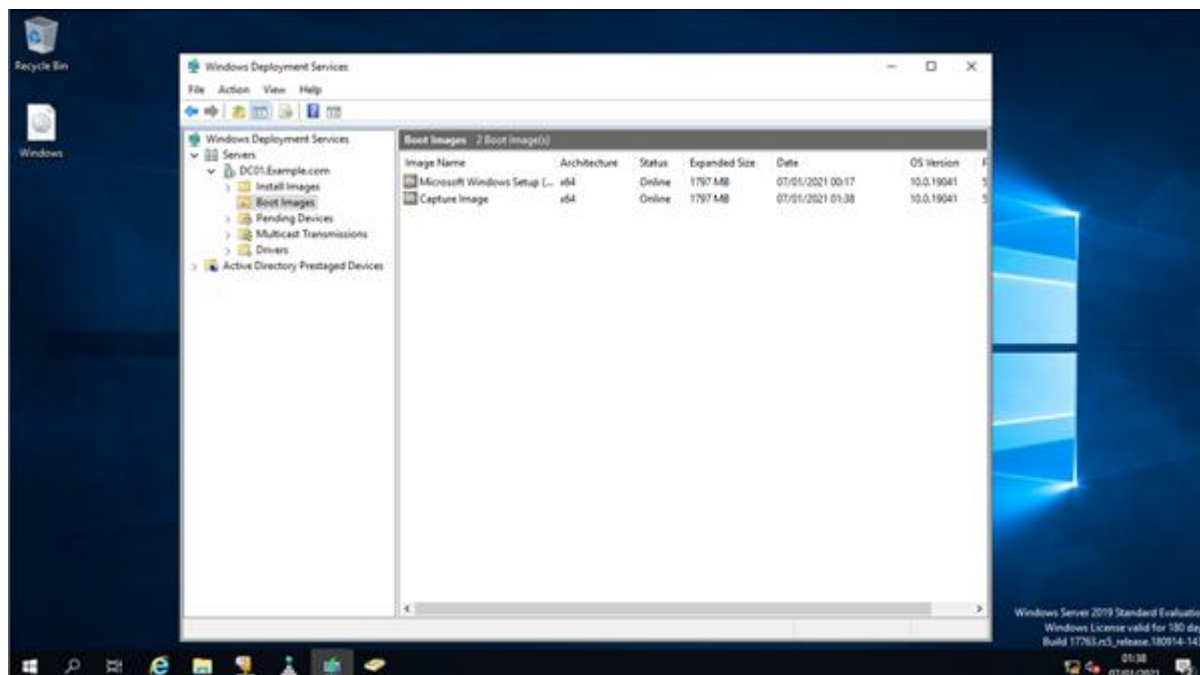
- I give it a name



- here is the summary data. I click next to move on



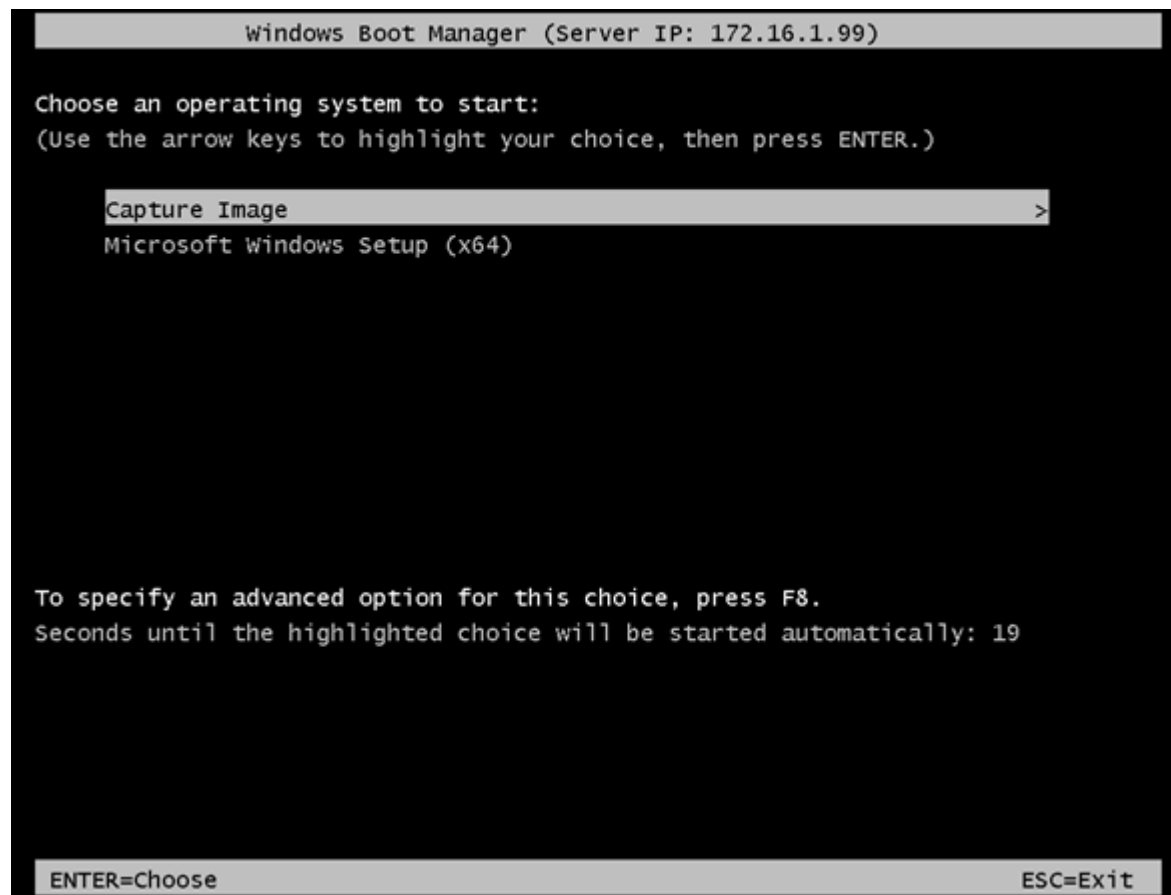
- the image capture is now complete



- here we see the WDS server ready for the reference image to be pulled across

## Capturing the reference image

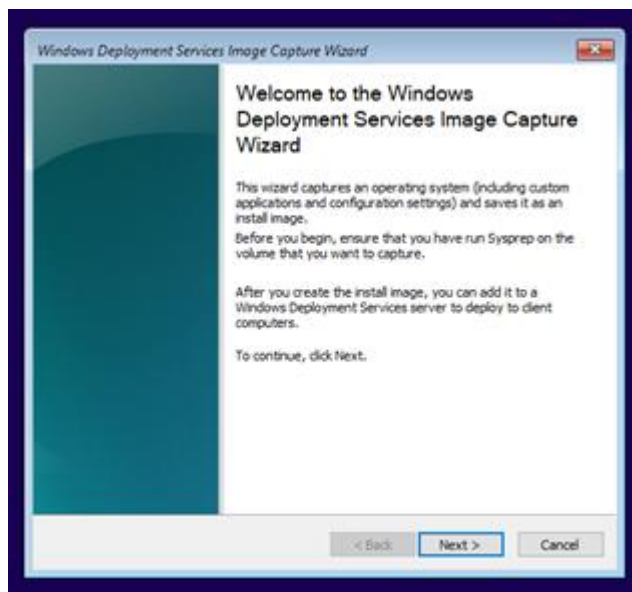
- I have created a reference image to deploy to other PCs



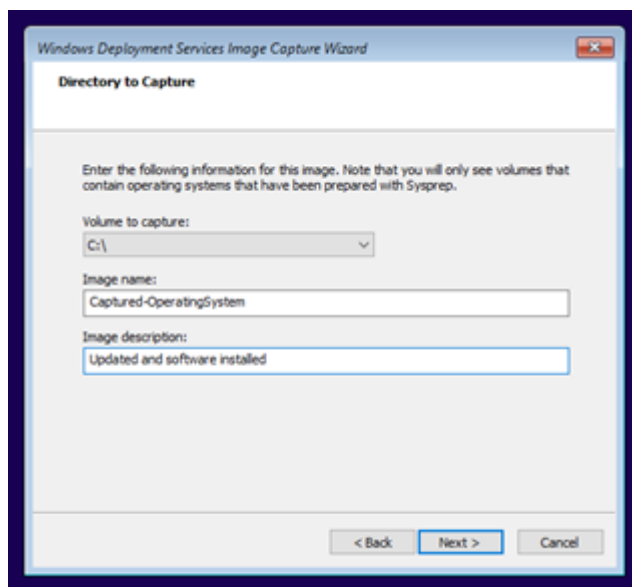
- I select capture



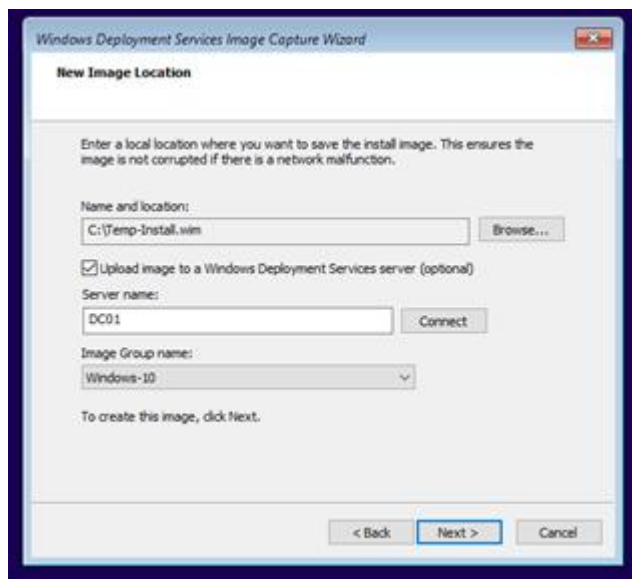
- I boot the reference machine using PXE boot
- I then select capture image



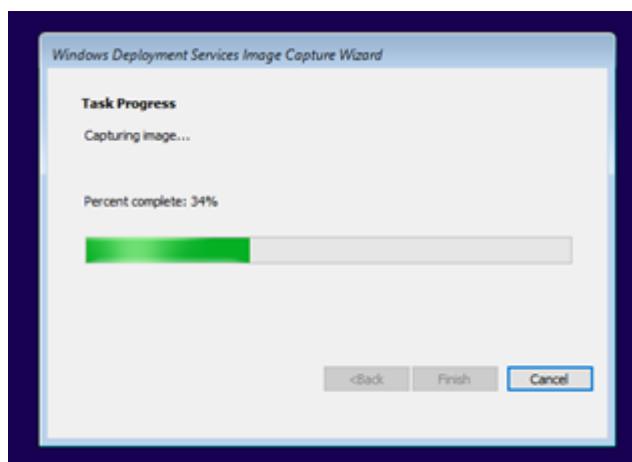
- I run the wizard



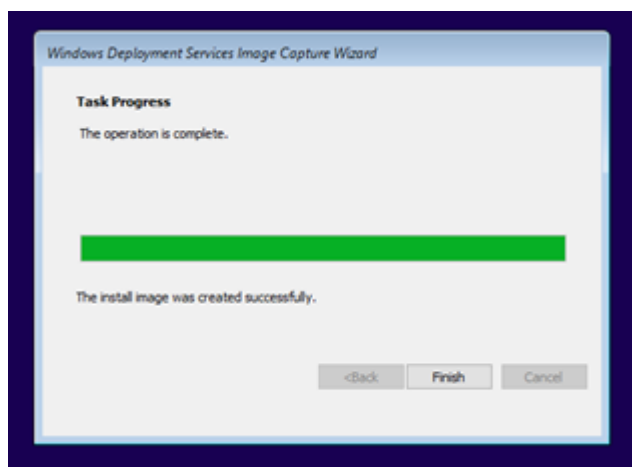
- I apply details needed for the location



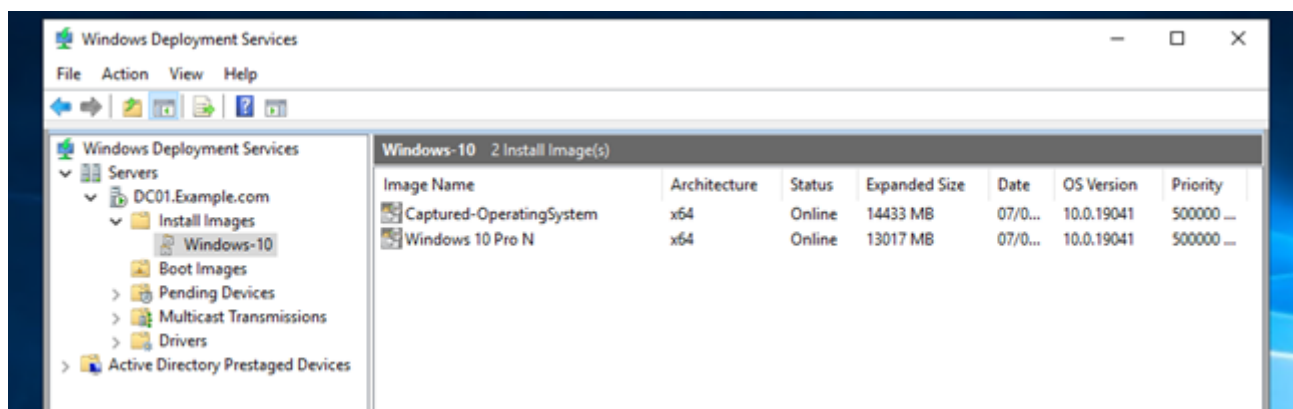
- I add location information



- the image is running



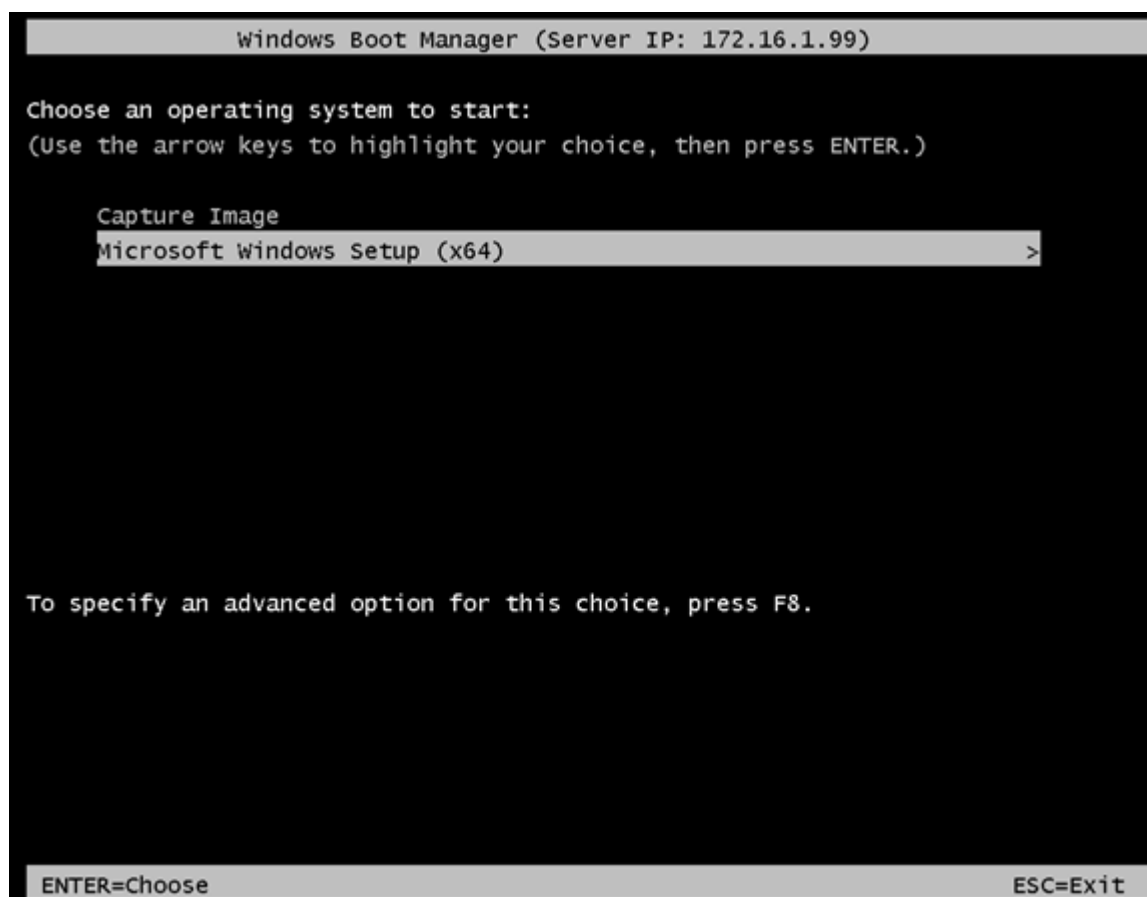
- and the image captures and then uploads to the administrative machine



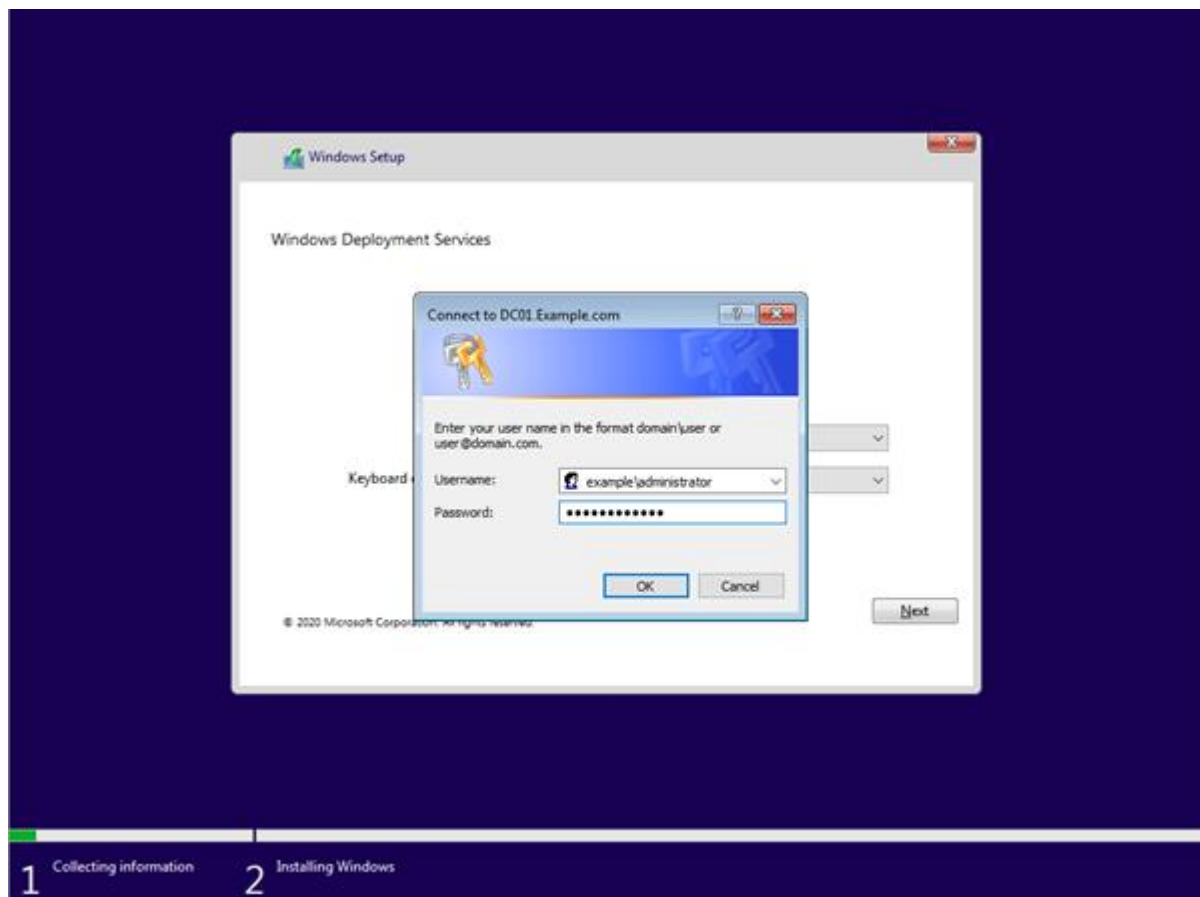
- on the administrative machine, I can see the image is captured ready to deploy

### Deploying the image

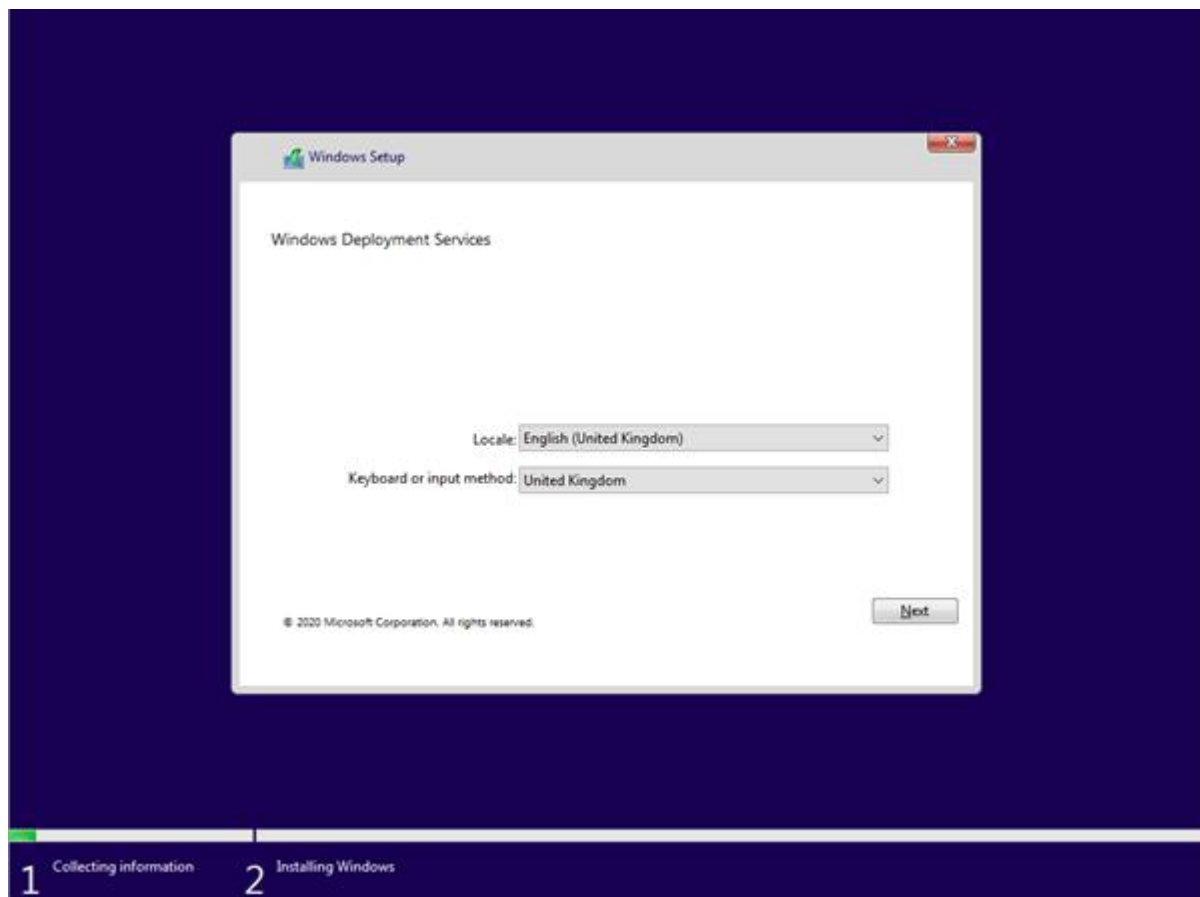
- the deployment has run correctly and is installed on the target computer



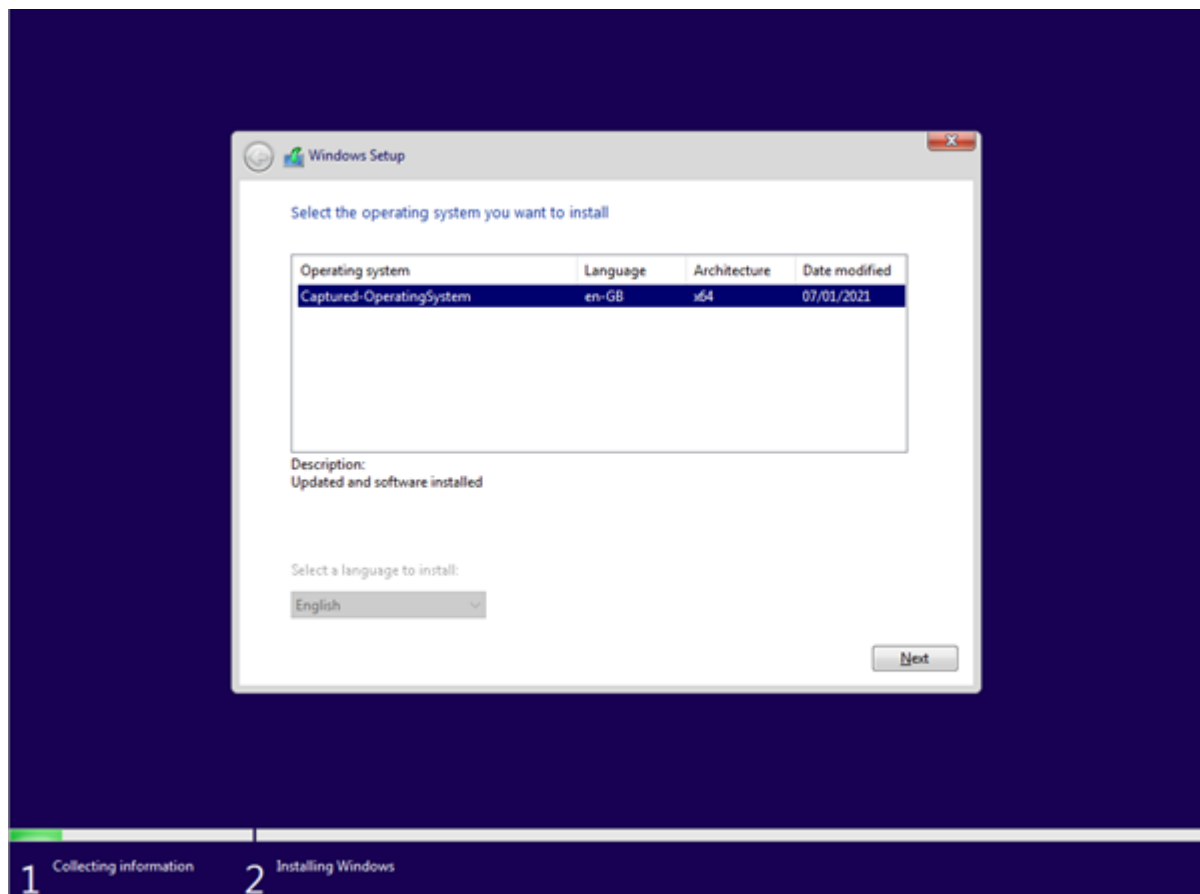
- I boot the target machine using PXE and select setup



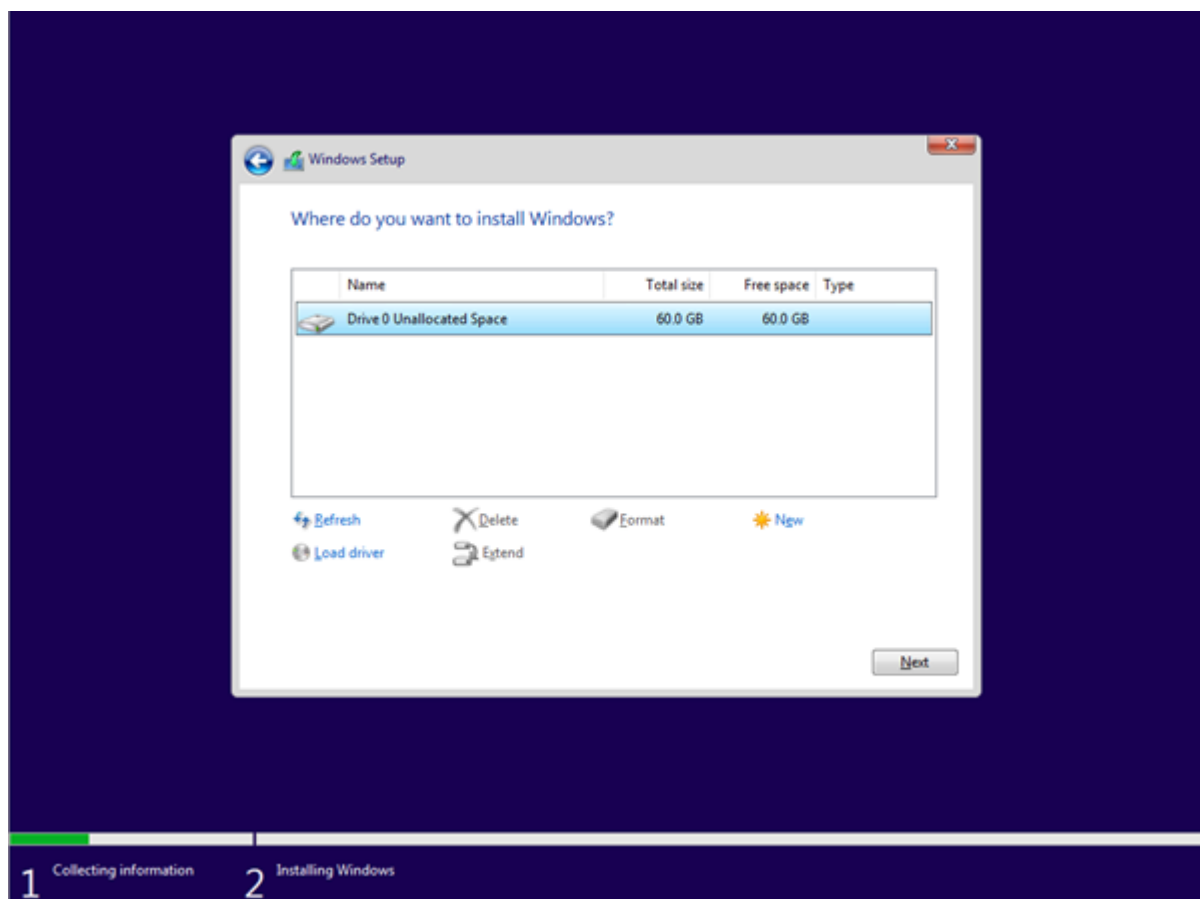
- I add the domain password so that it is not needed later



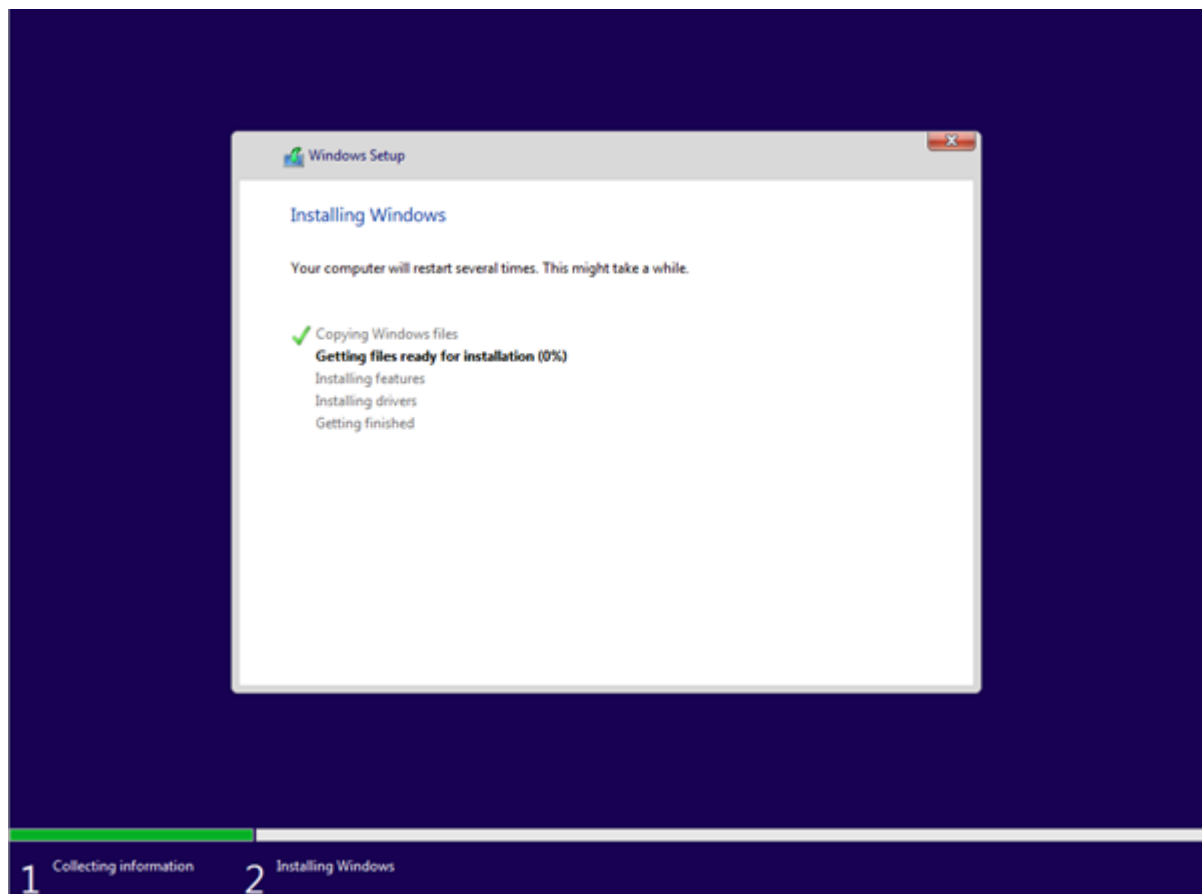
- I set location data



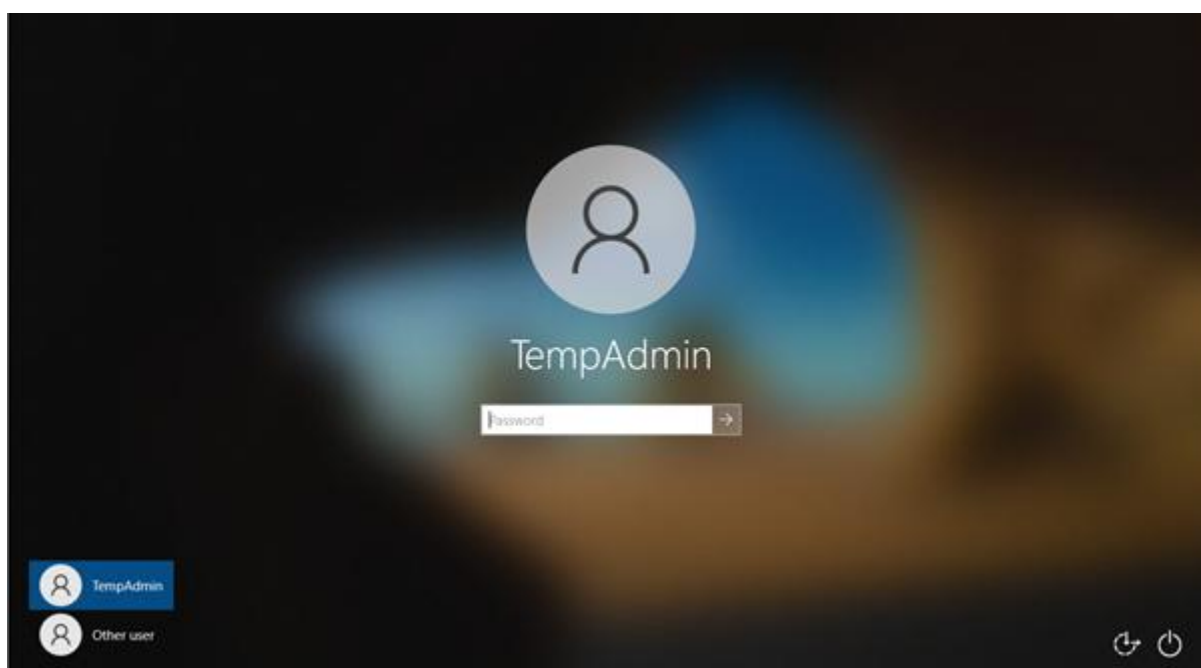
- I choose the image I want to deploy. There could be a number of images on a big network



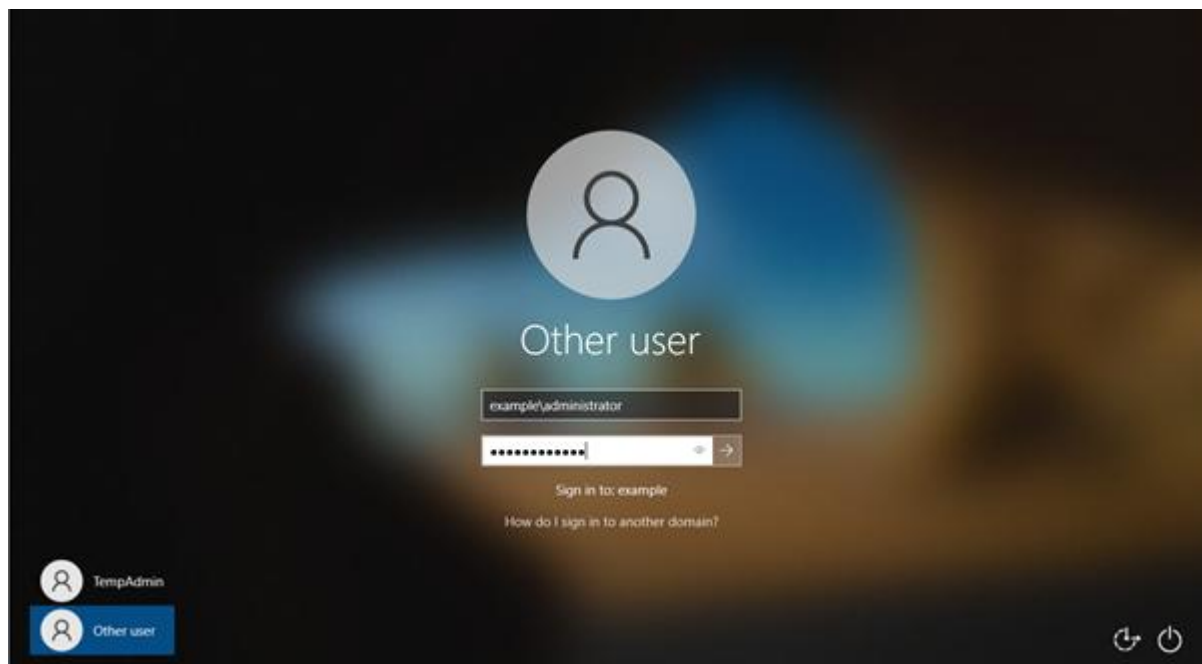
- I select the location to deploy to



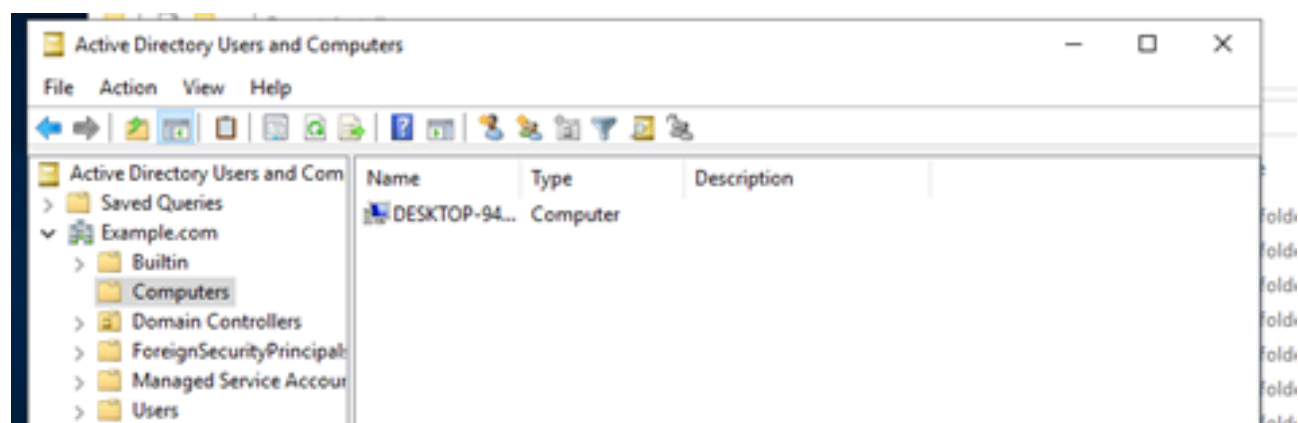
- I wait for Windows to install



- I enter the username



- I enter the password so I can now log in

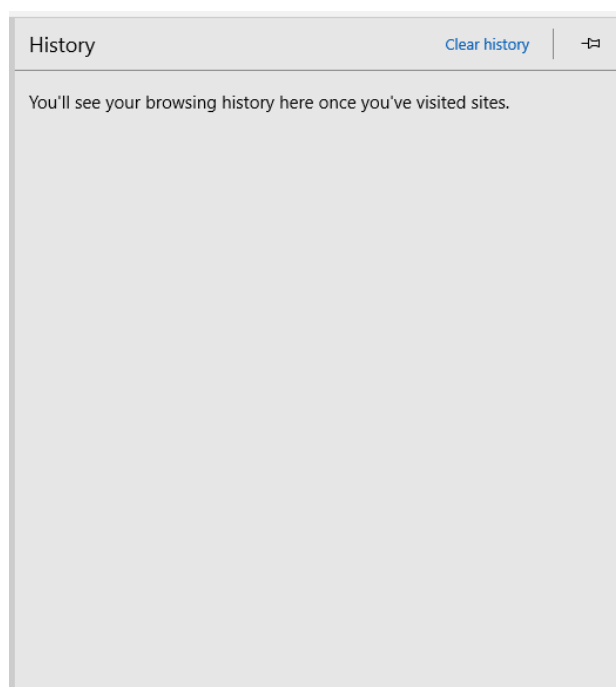


- I can see the PC in active directory



- Windows has installed and includes OpenOffice

## Browser history



## Examiner commentary

The student has achieved the grade for the following reasons:

- the student has demonstrated some understanding of the penetration test report and has completed the penetration test risk assessment template to a satisfactory level
- the student has made recommendations to resolve some of the vulnerabilities identified
- the student has given a report that recommends some actions for future improvements
- the student has broadly completed the task, deploying an image to a target computer; however, they may have failed to complete some of the more challenging technical aspects of the task (creating a working answer file/automated domain join)
- although it can be seen what the student has achieved, there is no appreciable commentary that shows detailed understanding of the subject
- the student uses limited technical language and terminology – they show a general understanding of the subject area but lack the deep understanding to describe what they are doing and why
- they are demonstrating most skills and techniques required for this task but not the most complex – they are doing this regularly but not consistently

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