T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 3 - Distinction

Guide standard exemplification materials

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

Internal reference: DSS-GSEM-17

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment

Guide standard exemplification materials

Digital Support

Assignment 3

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 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, 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 document 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

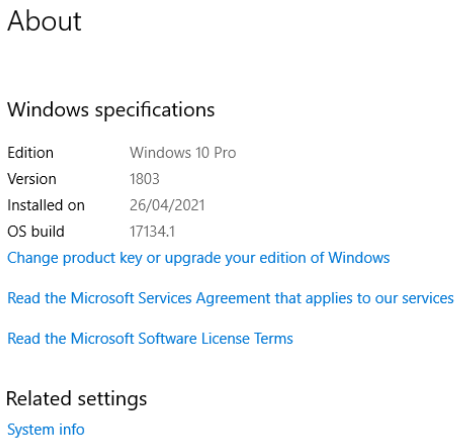
Student evidence

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 (risk: high)
            - KB4511552 for x64
            - KB4511552 for ARM64
            - KB4505657 for x64
            - KB4505657 for ARM64

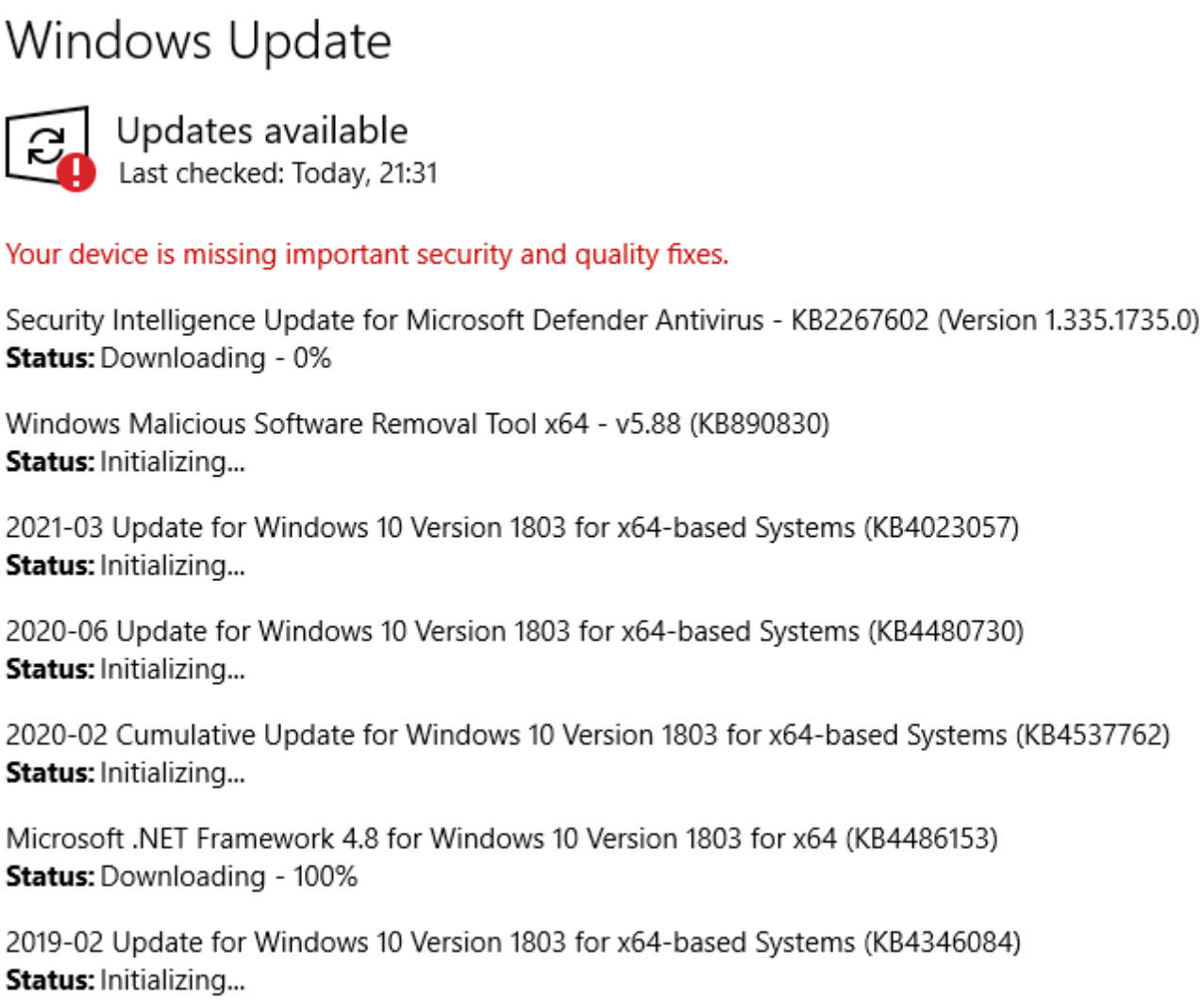
The OS version is Windows 10 1803, which is significantly behind and requires many updates to bring it completely to date, image a:

Image a



When checking for Windows Updates it has several updates that were missed, image b:

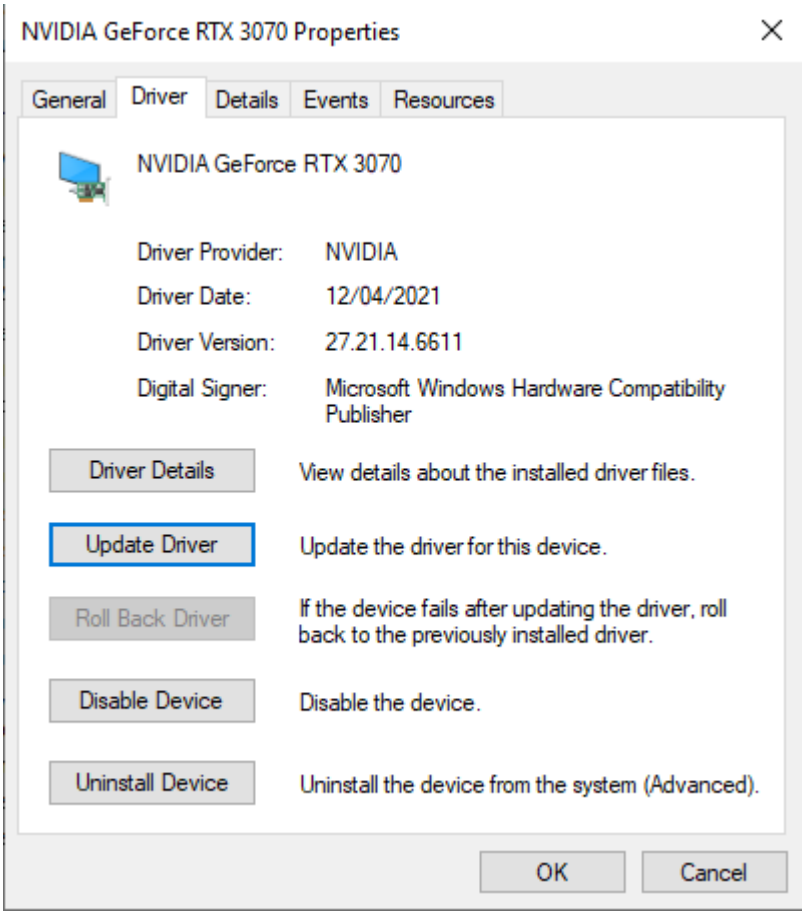
Image b



- action
  - all patches need to be updated on the workstations (timescale max 25 days)
- vulnerability
  - the NVidia video driver on all workstations was out of date, exposing all workstations to a privilege escalation vulnerability (risk: medium)

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

Image c



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

- servers
  - vulnerability
    - all 5 of the servers operating within the network had 10 updates missing (risk: high)
      - KB4501835
      - KB4497934
      - KB4505056

- KB4499728
- KB4494441
- KB4495590
- KB4497932
- KB4499405
- KB4495618
- KB4556441

As you can see below there are the updates that were missing, image d:

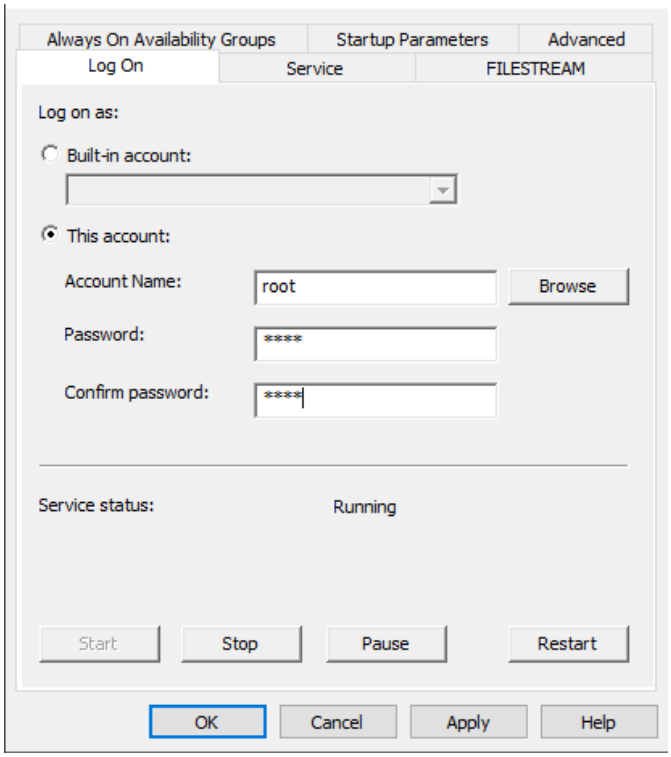
Image d

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

- action
  - all patches need to be updated on the servers (timescale: max 25 days)
- vulnerability
  - vulnerabilities were identified in the SQL server operation on SVR09 (risk: critical)
  - a weak username/password combination of root/root were configured on the SQL server allowing root access to the server
  - when running a query against the SQL database, usernames and passwords for all users were able to be retrieved in clear text
  - a rogue username/password was able to be added to the database

As you can see the SQL server only has a simple username and password, image e:

Image e

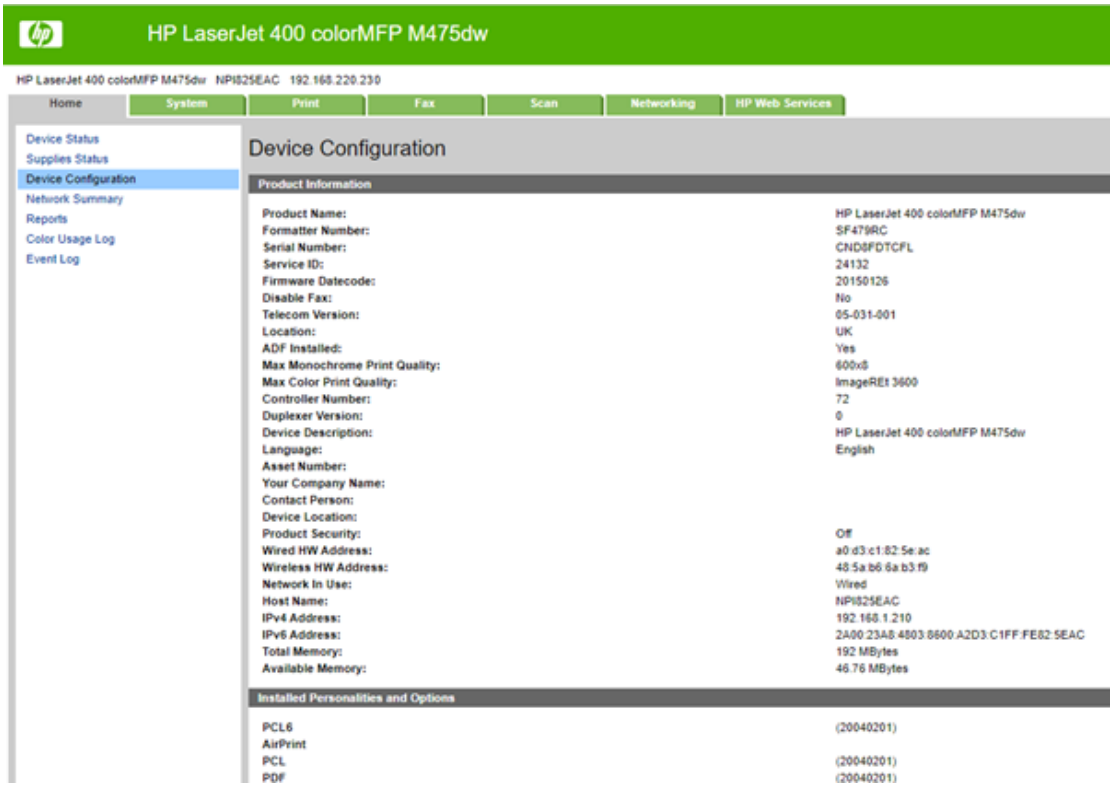


- action
  - root account should be disabled on the server, with administrative password set using a strong password
  - encryption should be introduced on the server for any usernames and passwords in the SQL database – the screenshot in the database suggests the server is currently using encryption with the Blowfish algorithm but has been configured poorly
  - it should be noted that if these passwords include external customer details then if this vulnerability were exposed in a genuine attack this alone would be a serious and notifiable breach of GDPR/Data Protection Act 2018 regulations
  - it would be worth introducing a form of 2 factor authentication on the server to help prevent unauthorised access through compromised passwords

- printers
  - vulnerability
    - the following issues were found on all 5 printers in the infrastructure (risk: medium)
      - no administrative challenge when logging into management console
      - administrator password has not been set
      - printer firmware was running an old version (20150126) which is vulnerable to a JetDirect SNMP device password disclosure vulnerability

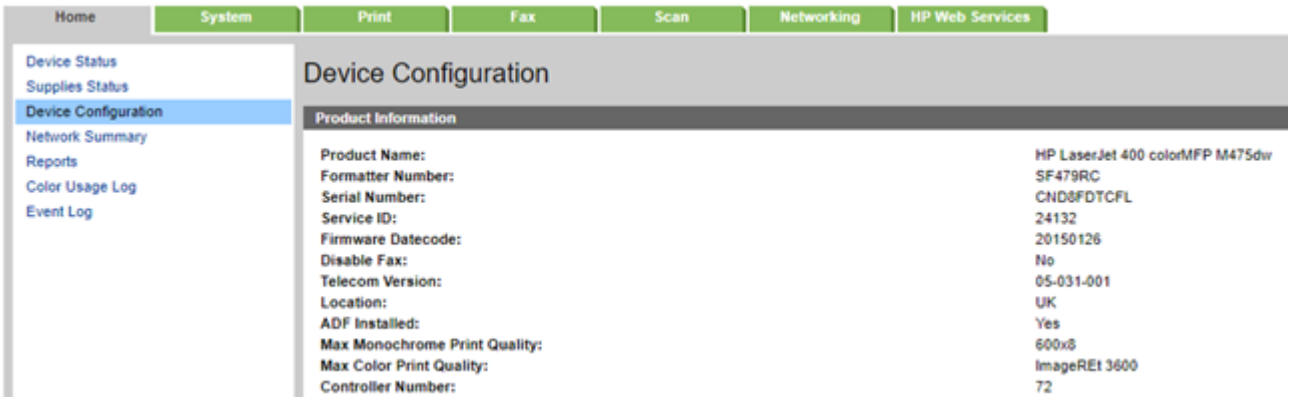
When logging in to the printer you are immediately given full access, image f:

Image f



When viewing the firmware, it has been identified that this firmware version is out of date, image g:

Image g



- action
  - all 5 printers will need their firmware updating to the latest version (20191105)
  - all 5 printers will need a strong administrator password setting on the management console
  - all 5 printers will need the settings adjusting to prompt for a password on every login to the management console

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

It is not clear from the report how patch management is being conducted across the network but with missing critical updates, it is likely that patch management is not properly centralised. This can be said for both workstations and servers.

Recommendation for continuous improvement

Windows Server Update Service (WSUS)

I would recommend we introduce a WSUS server to the infrastructure. This will allow us to centrally control the patch management and ensure patches are rolled out to all workstations and servers correctly. WSUS will allow us to download operating systems, Microsoft software and signed drivers as soon as they are released to a central server. We can test patches quickly to confirm they will work with our infrastructure and then deploy to all machines effectively.

We can further set policies via group policy to control the updating of Windows, preventing users from delaying updates and ensuring they are forced to install as soon as they are made available.

WSUS will apply to workstations and servers and will include core signed drivers which should ensure that all the workstation vulnerabilities and the server update vulnerabilities are fixed and will also minimise the risk of vulnerabilities of a similar nature becoming an issue in the future.

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, also protecting against vulnerabilities such as the NVIDIA video driver.

Routine printer maintenance

Once the initial resolution has been implemented as per the recommendations above, we should also be introducing standard checking of firmware as part of the printer maintenance cycle so that the firmware on printers is kept up to date at all times.

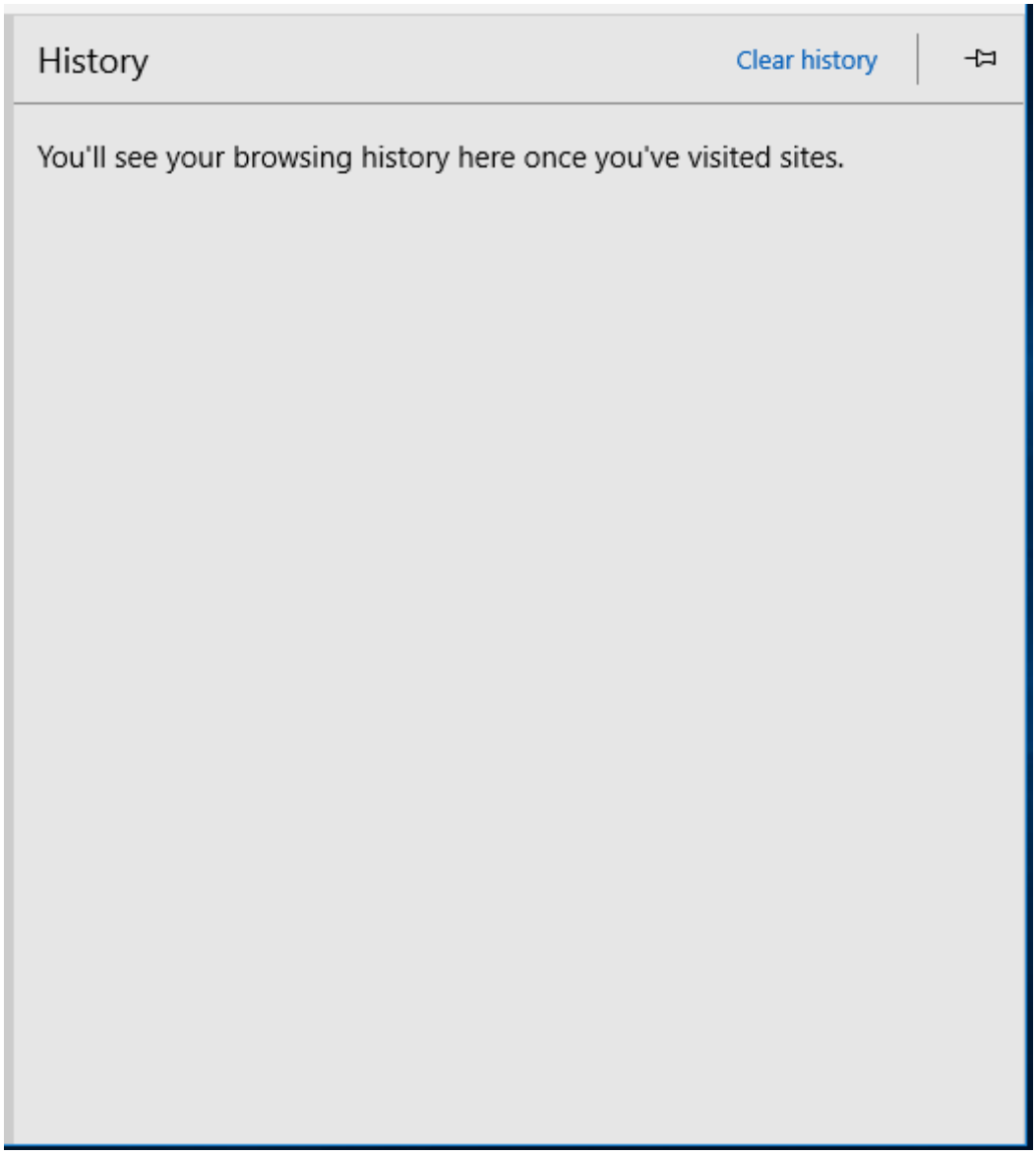
SQL server/PHPMyAdmin

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

Moving forward we need to ensure that there are no repeats of these issues. I would recommend regular auditing of user accounts to ensure that we can identify that no rogue accounts have been added to the database. The use of 2 factor authentication, preferably using a time-based one-time password (TOTP), would provide a level of authentication that would prevent access with a compromised password as TOTP will use a system such as providing a code sent to a mobile device as well as a password. TOTP will mean the code will expire quickly if not input.

Summary

Implementing these recommendations will resolve the current issues and put in place, through the routine maintenance and monitoring, the ability to identify quickly and resolve proactively 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:

- 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, network-based services
- operating system and office licenses for basic image deployment
- 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

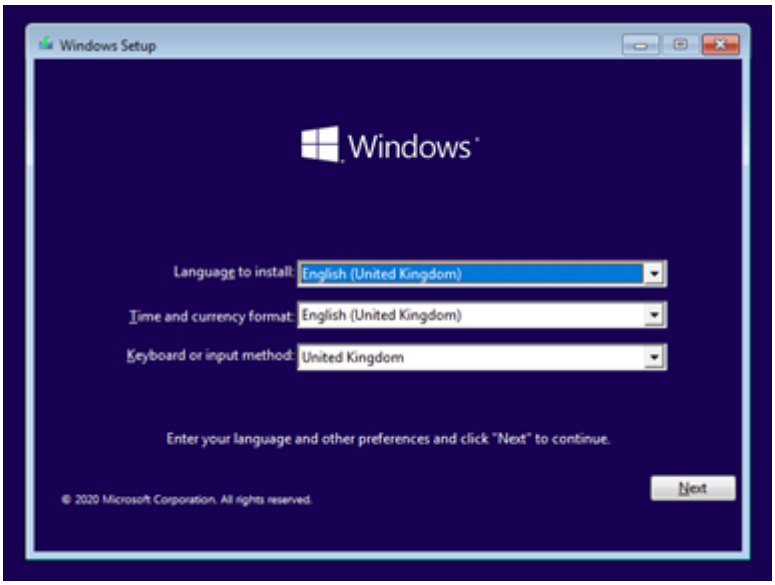
Task 2

Creating a reference virtual machine

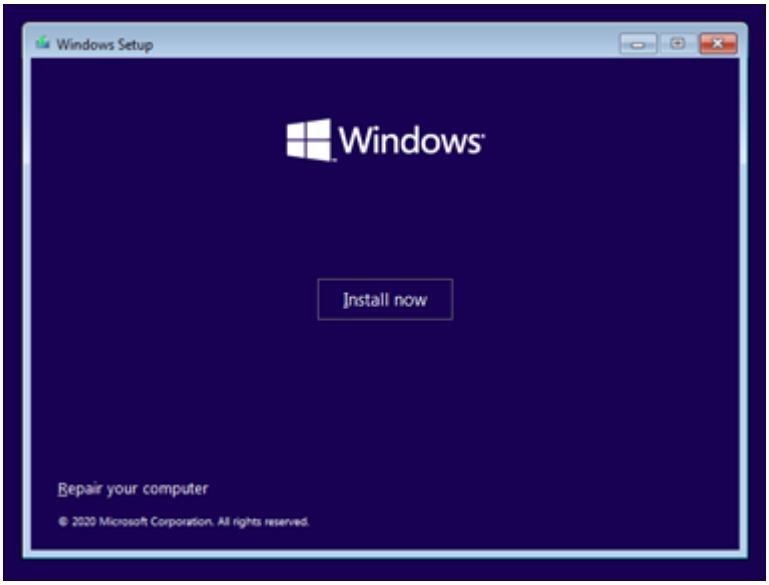
To create an image for remote deployment, I first need to create a 'reference image. The first steps to achieve this are to install Windows 10 on a computer and set it up exactly as I want all our client PCs to be set up.

Installing Windows 10

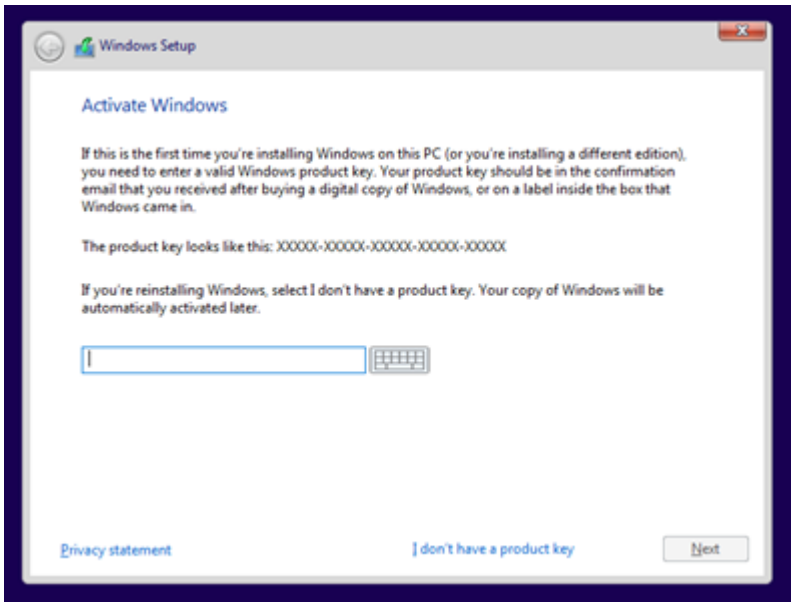
These screenshots show me installing Windows 10 Professional onto my reference PC. You can see I have followed a standard installation from installation media including setting a local administrator account (localadmin).



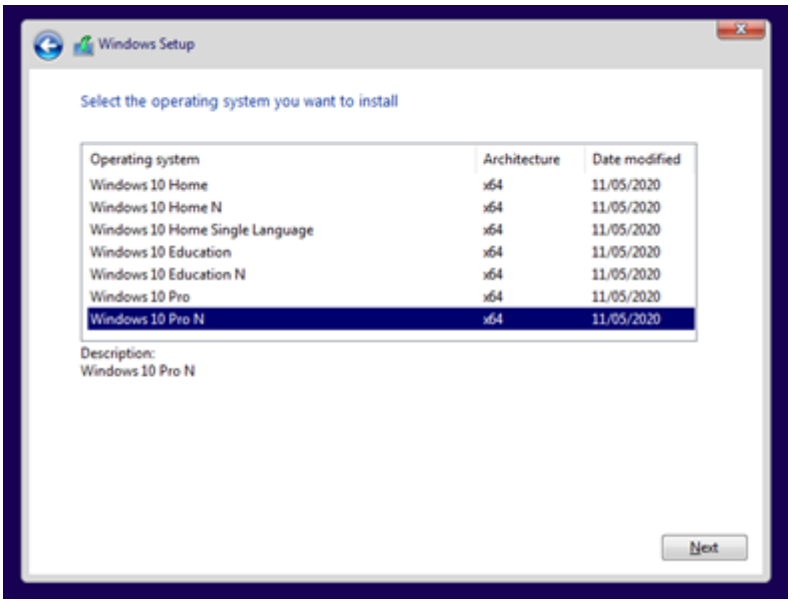
- I boot from an Iso and select the installation language. This is a replacement for a physical disc used in VMs and over networks



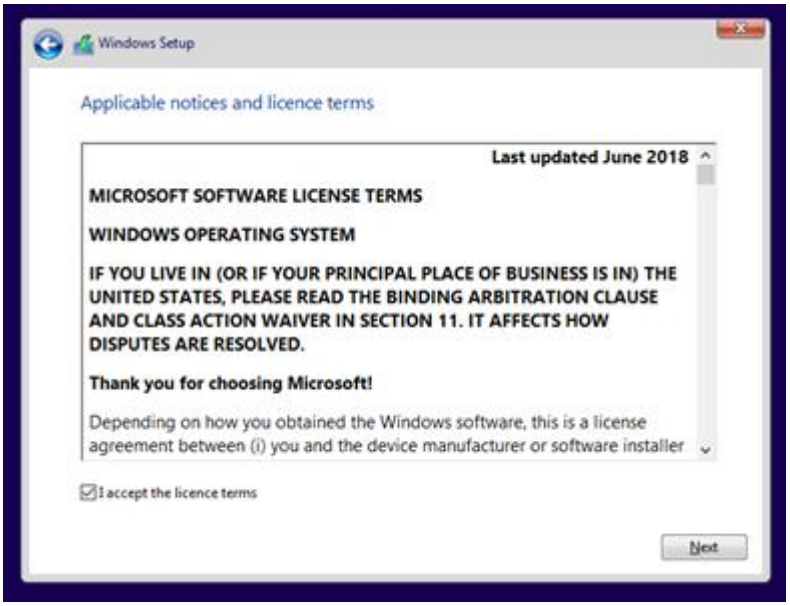
- I select install



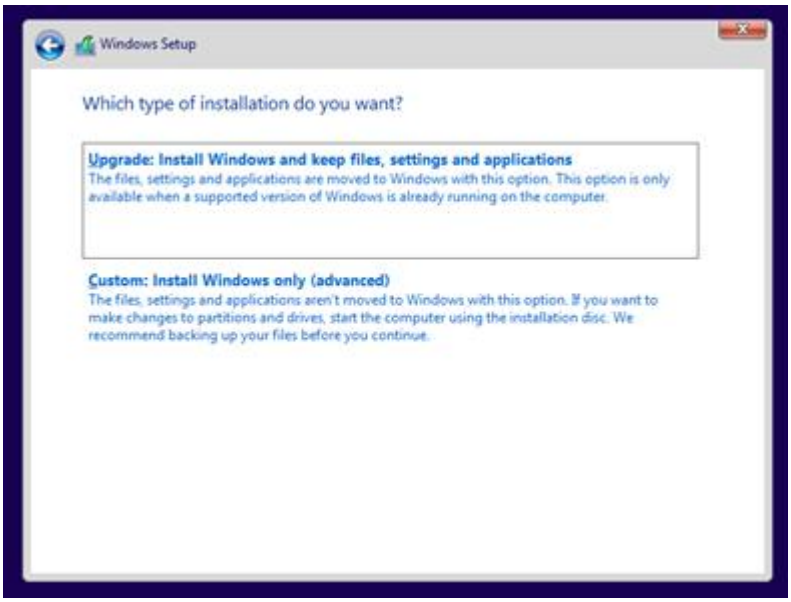
- I enter the licence key to validate the licence



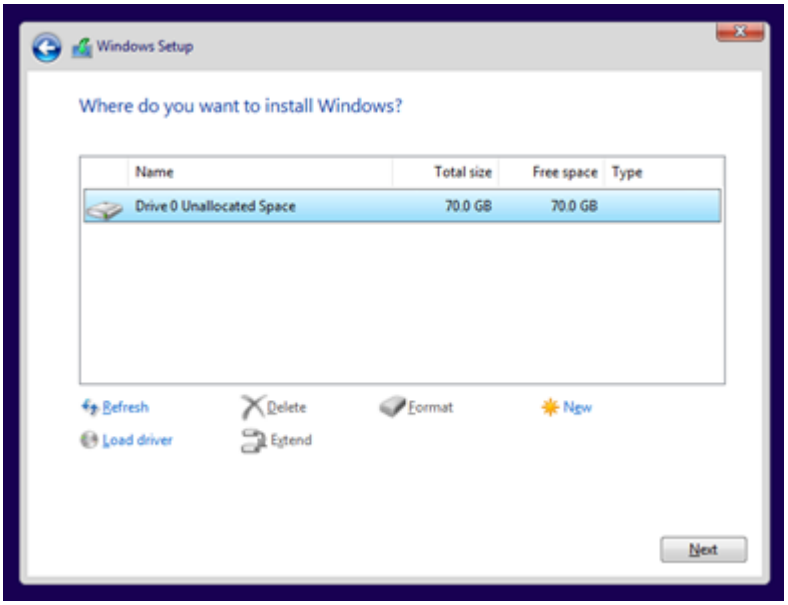
- I have selected the version of Windows I want to install. I choose Pro as it is for a business



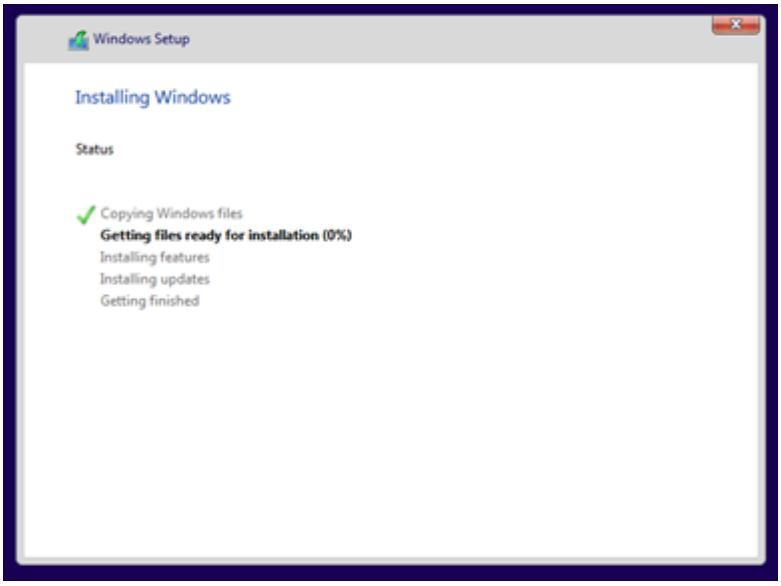
- I agree to the licence



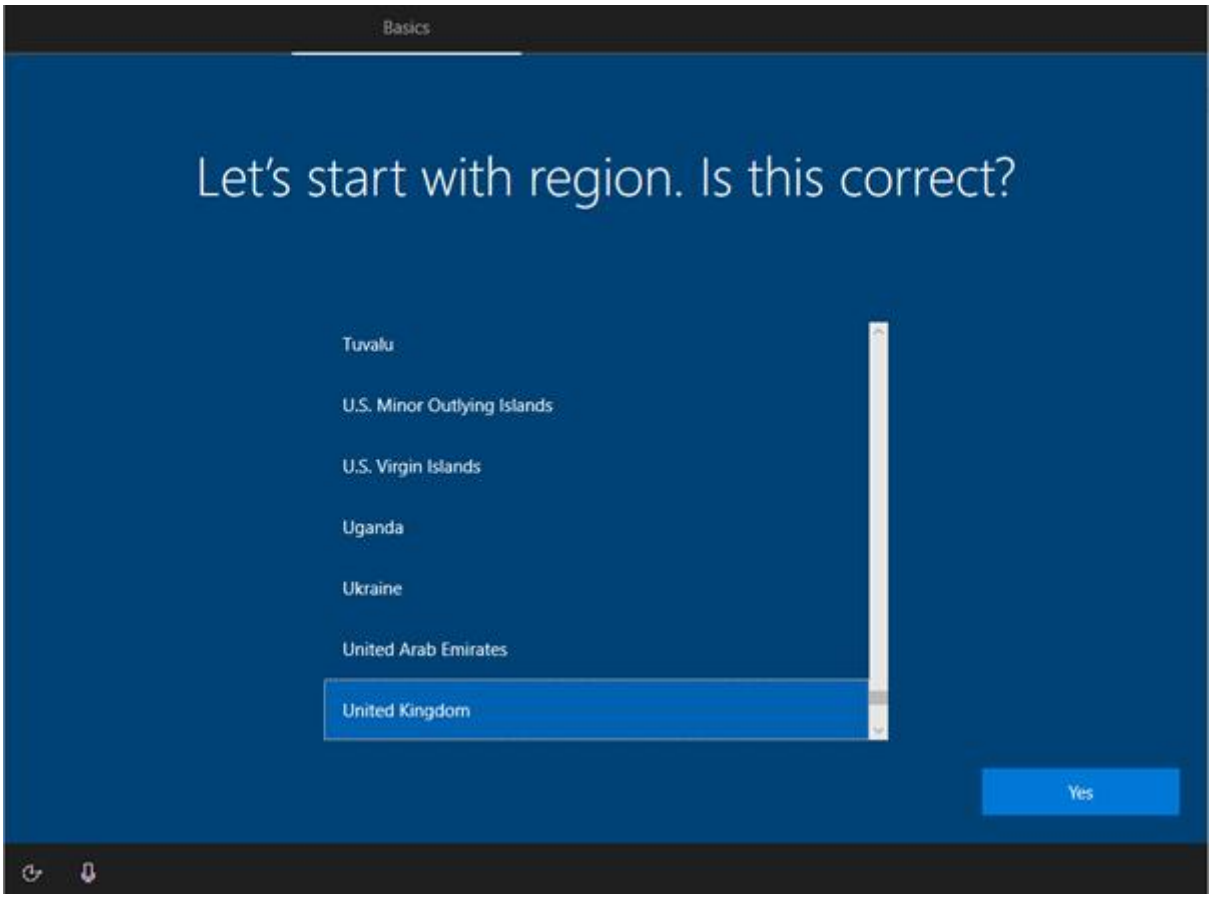
- I select the installation process I wish to use. This version will keep old data in a folder called windows.old



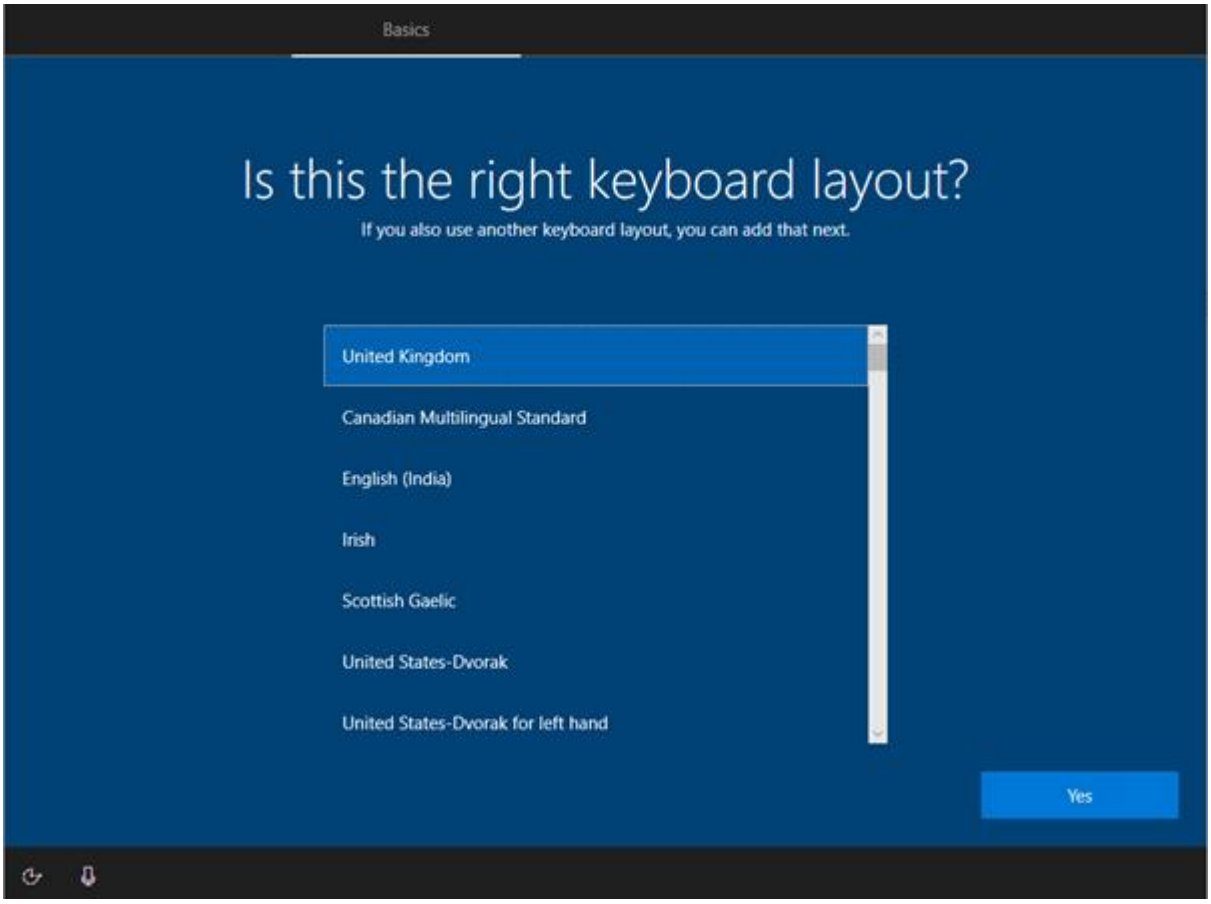
-
- I select the drive where Windows is to install. I have only one disk, so this is the one I choose



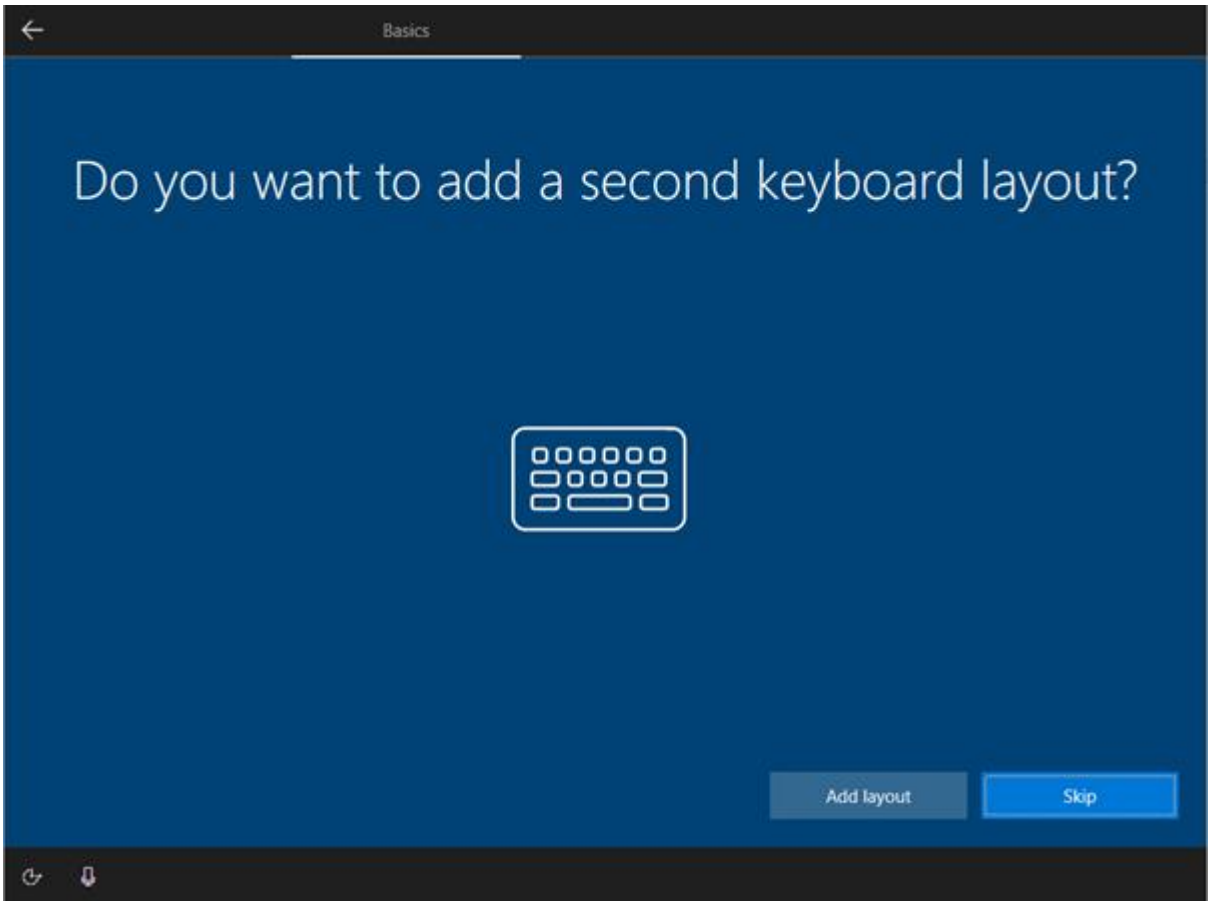
- Windows now installs



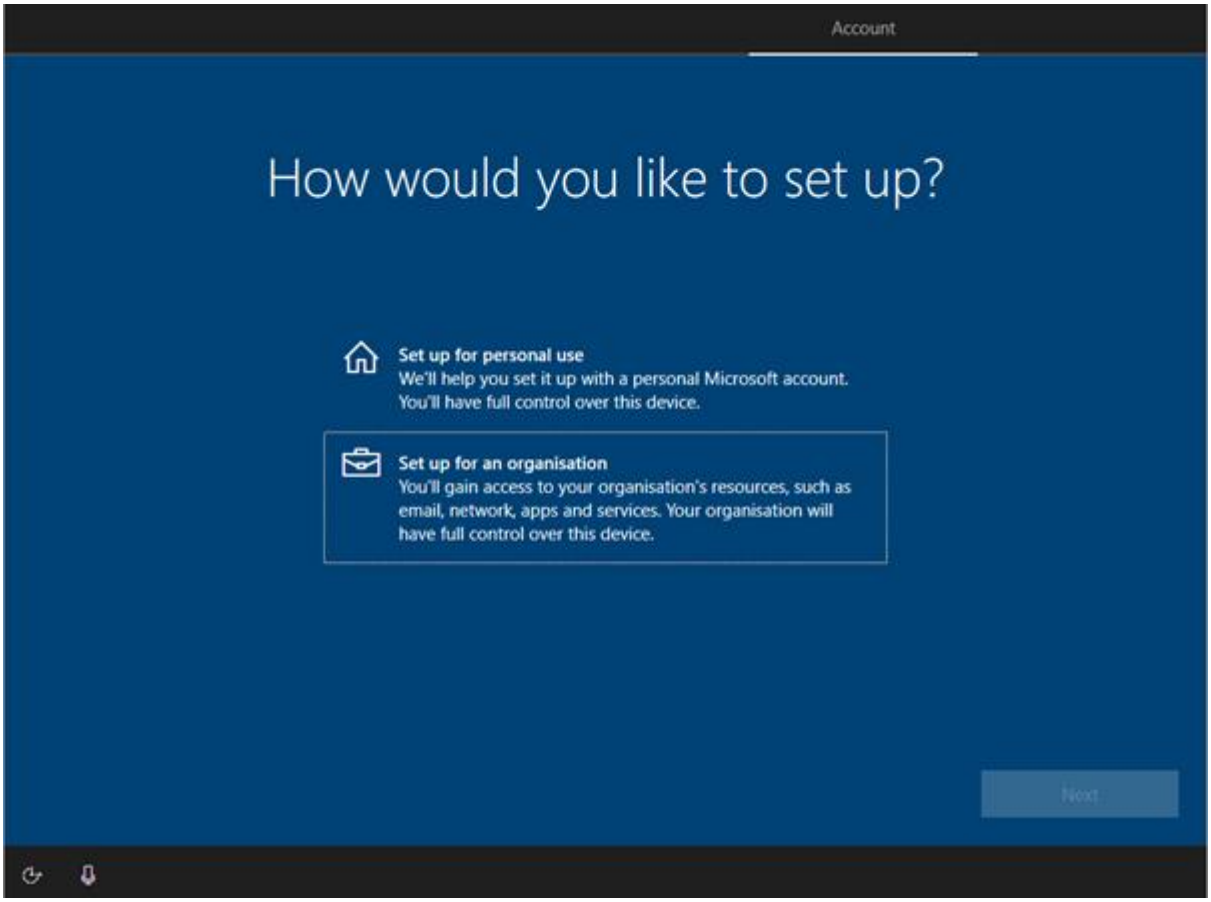
- once installed, I select the region



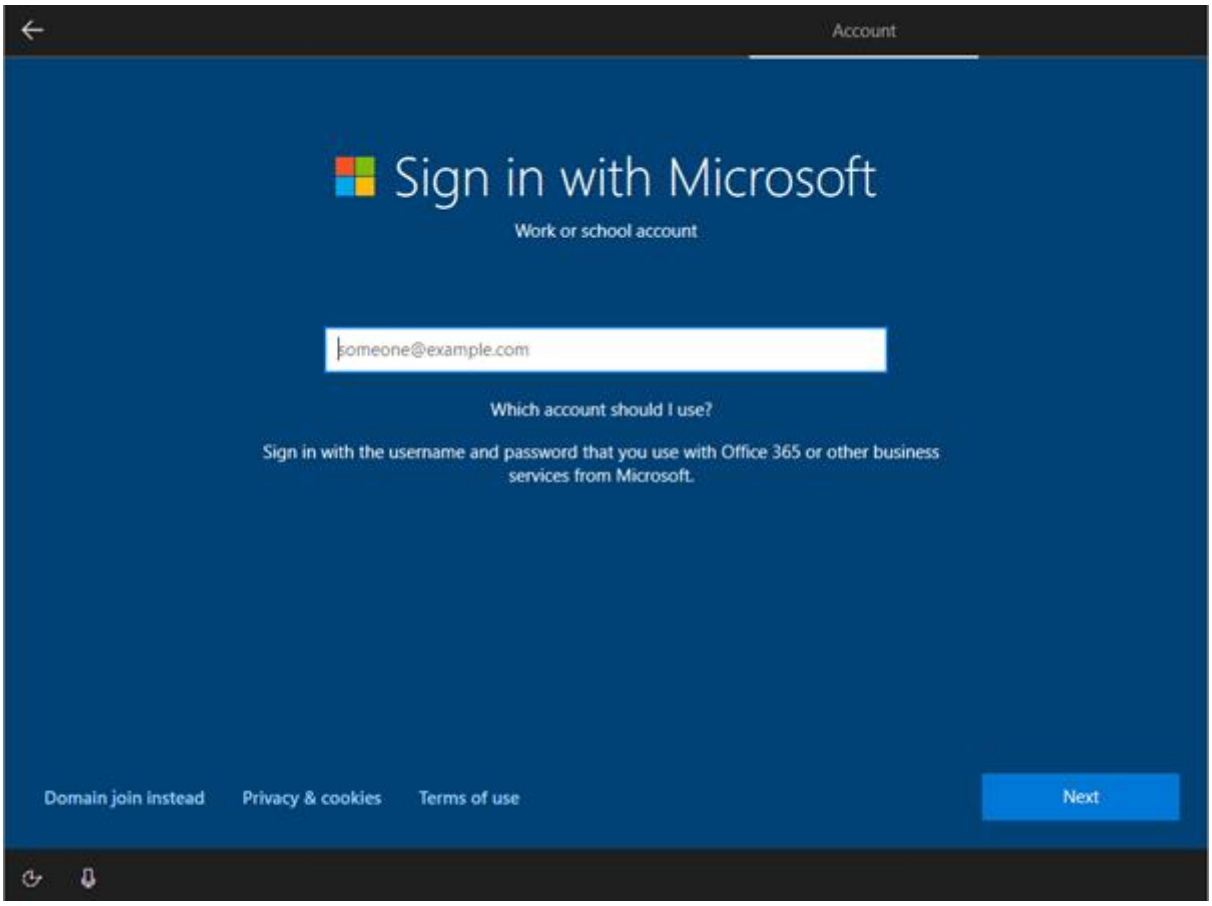
- I pick the correct keyboard for the country of the company



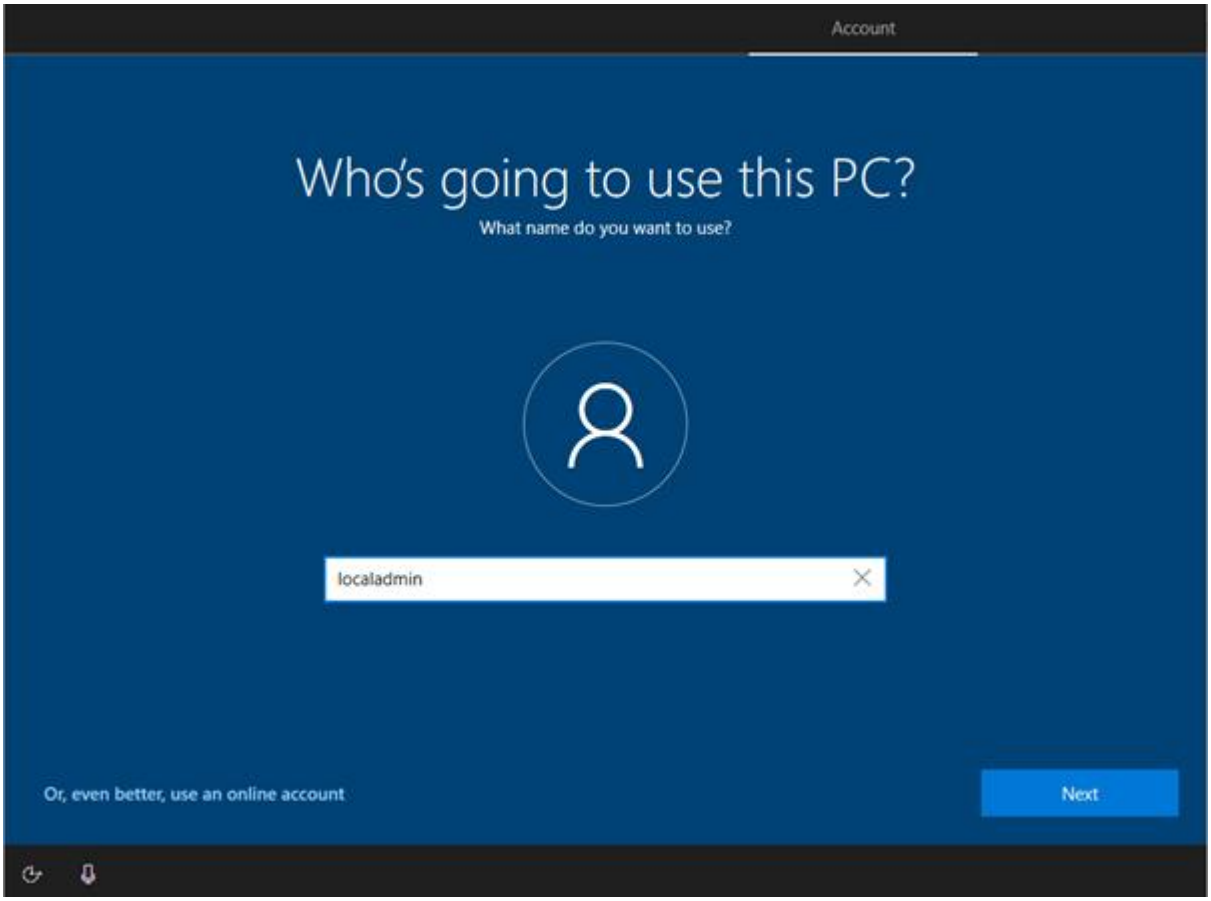
- I don’t need a second keyboard layout as I only have a UK keyboard



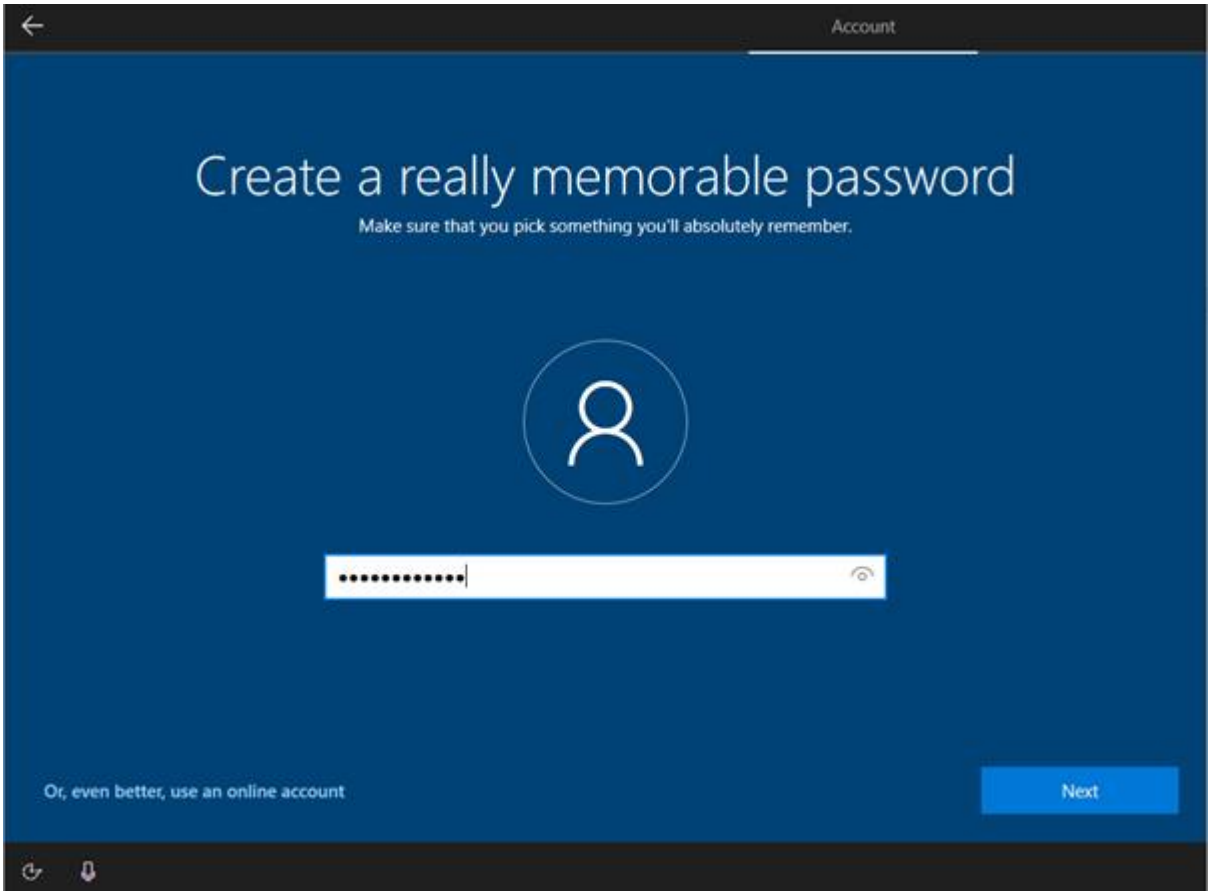
- I set the type to organisation as I will be joining to a domain


Account
Sign in with Microsoft
Work or school account
someone@example.com
Which account should I use?
Sign in with the username and password that you use with Office 365 or other business services from Microsoft.
Domain join instead
Privacy & cookies
Terms of use
Next

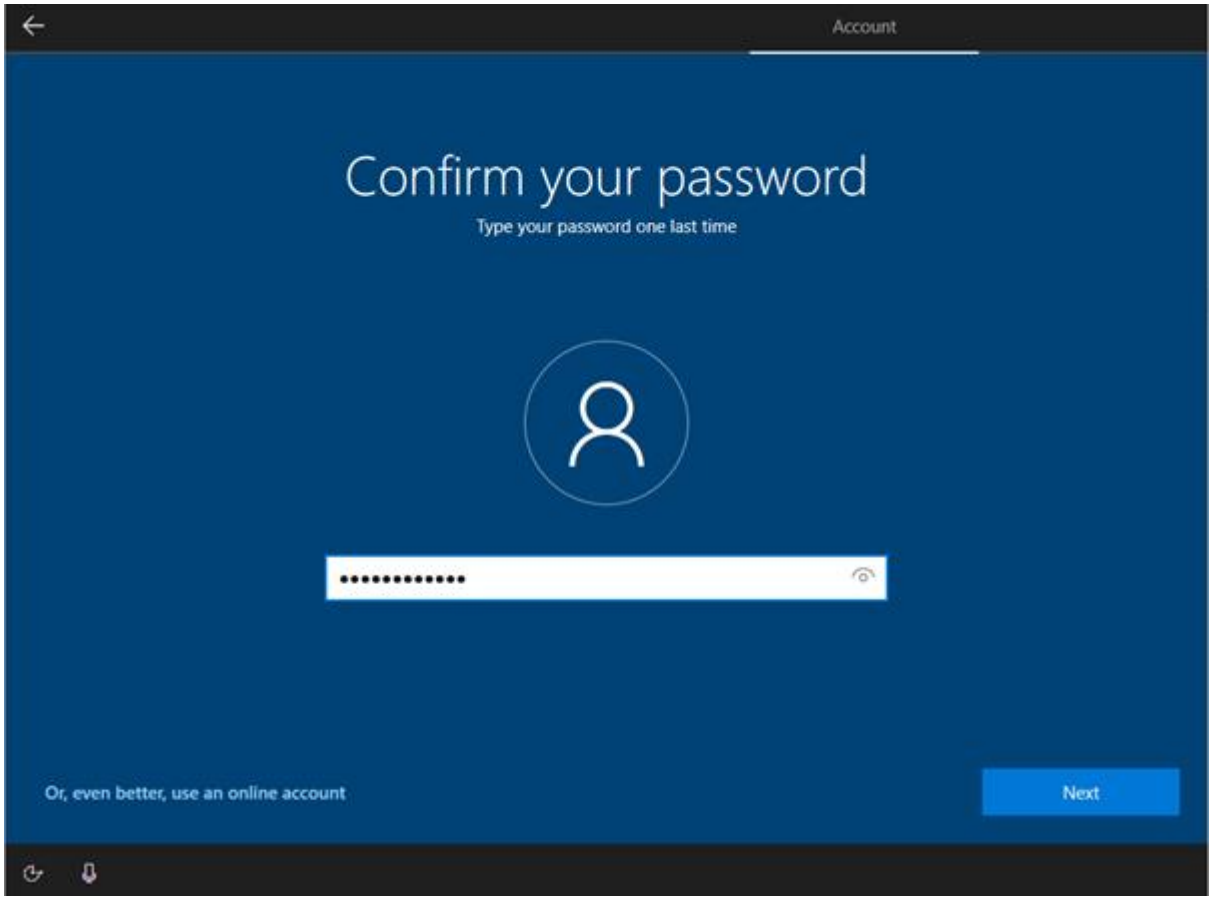
- now, I sign in



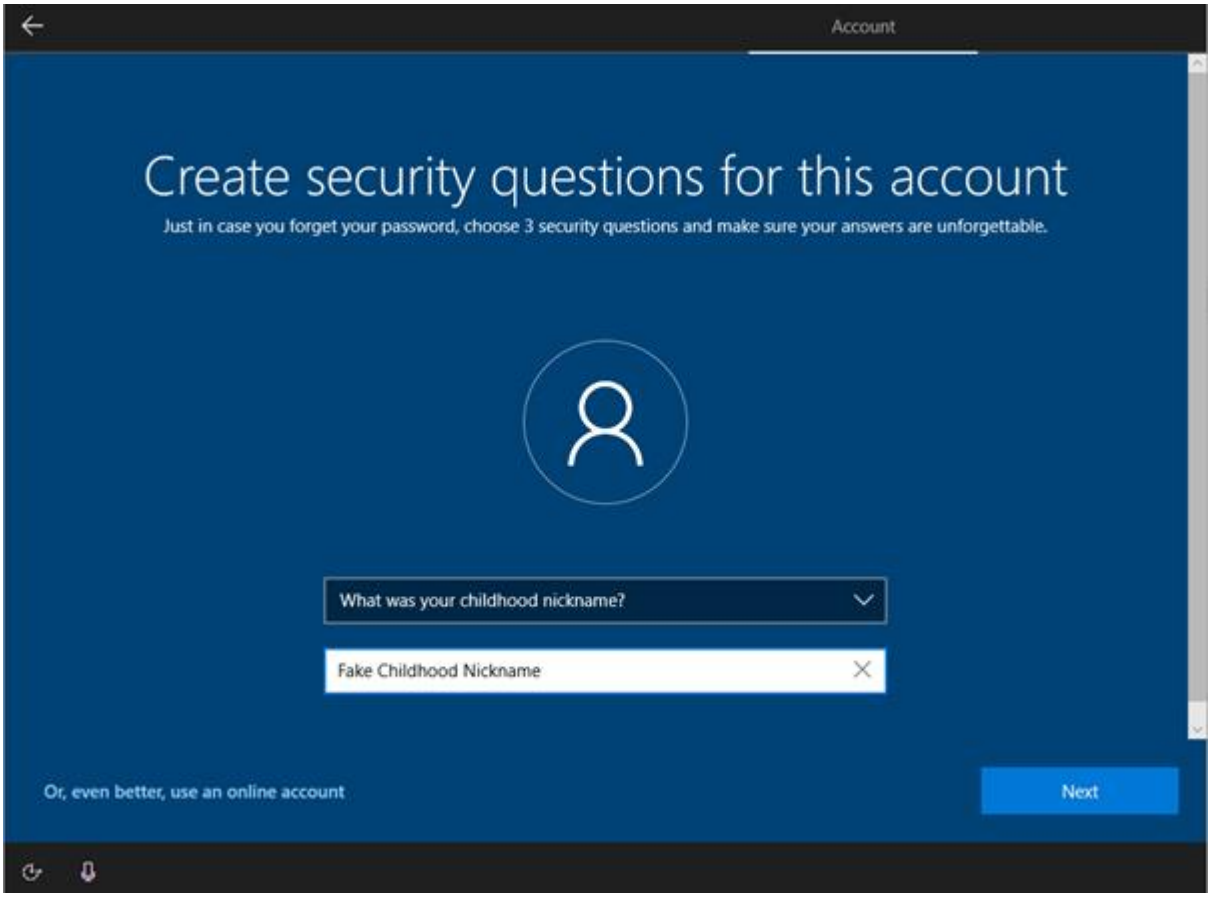
- I give the user a name. This is for the local admin



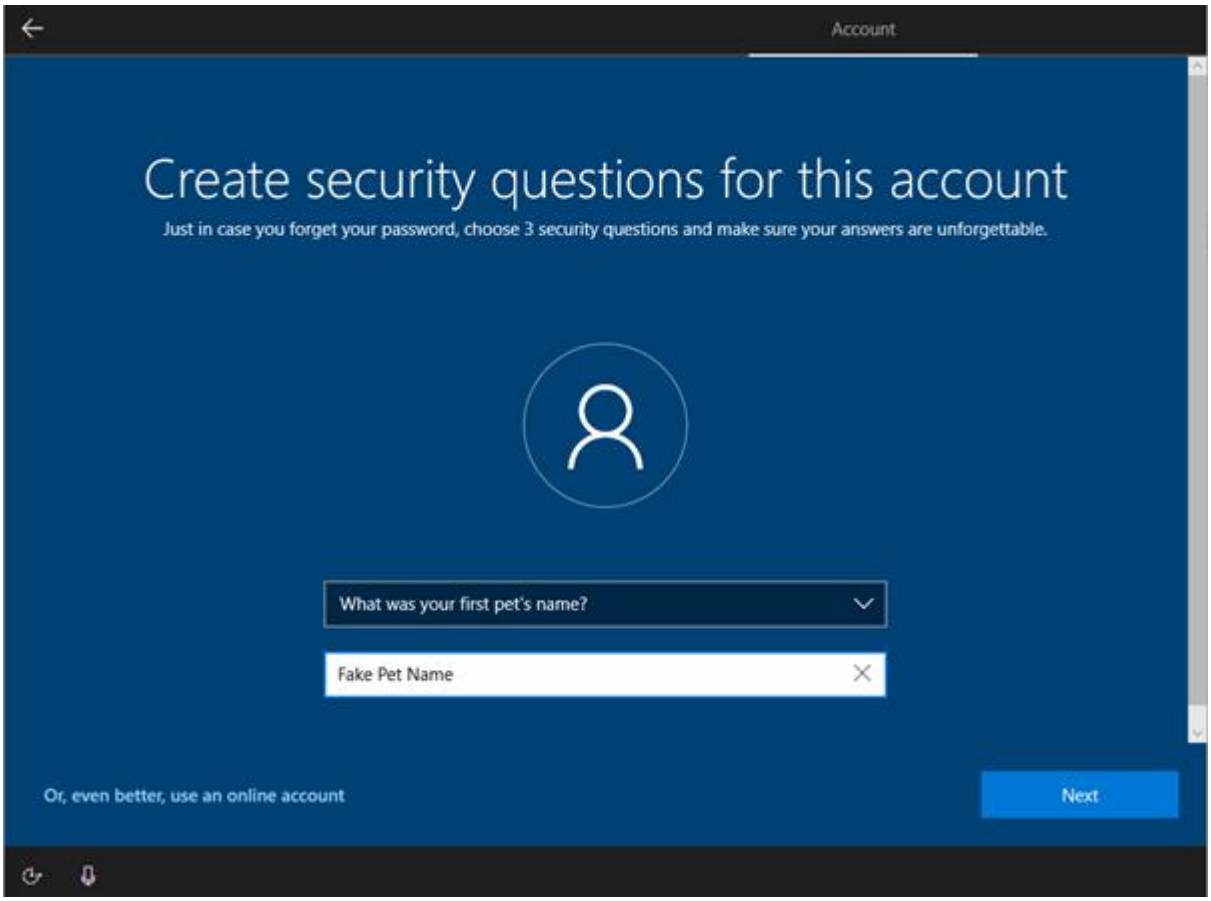
- I create a password for security



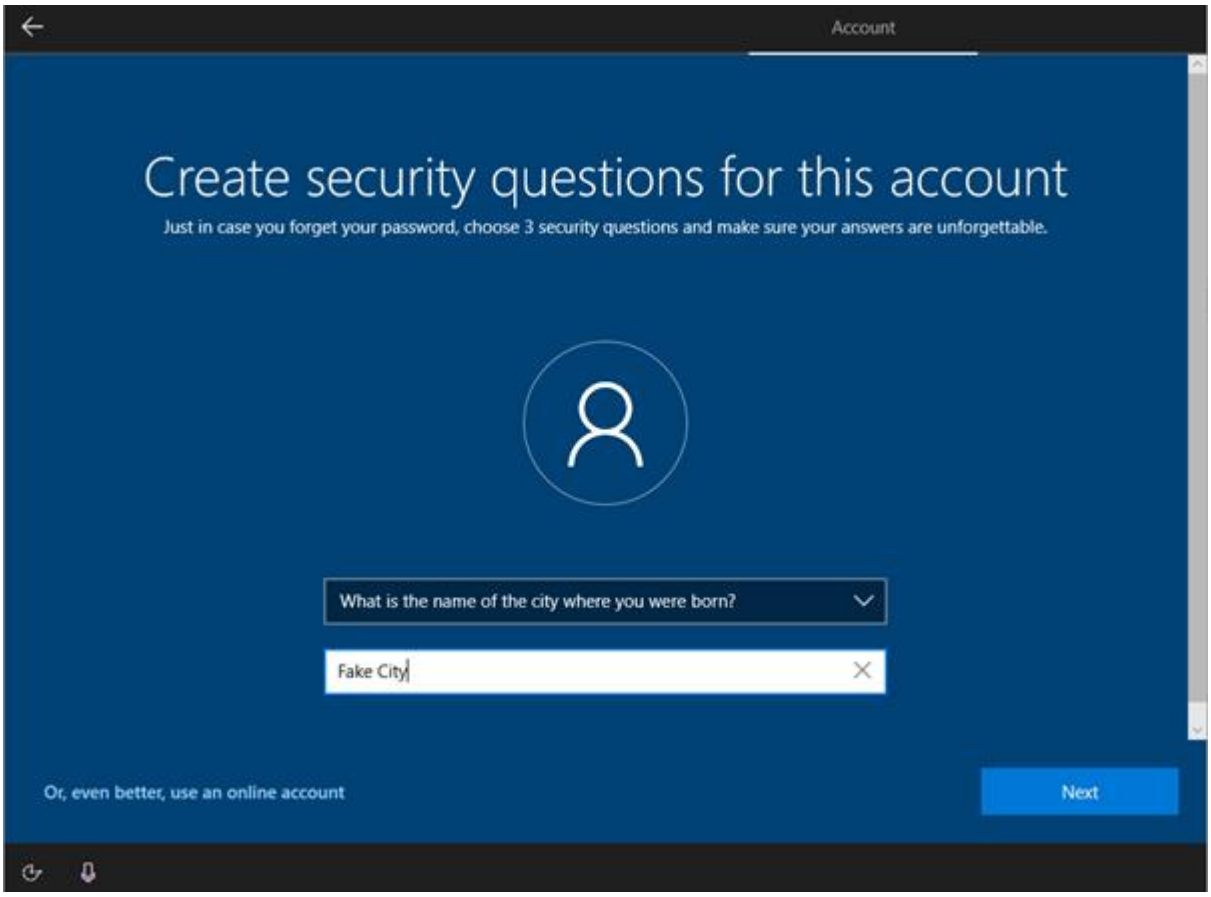
- I confirm the password



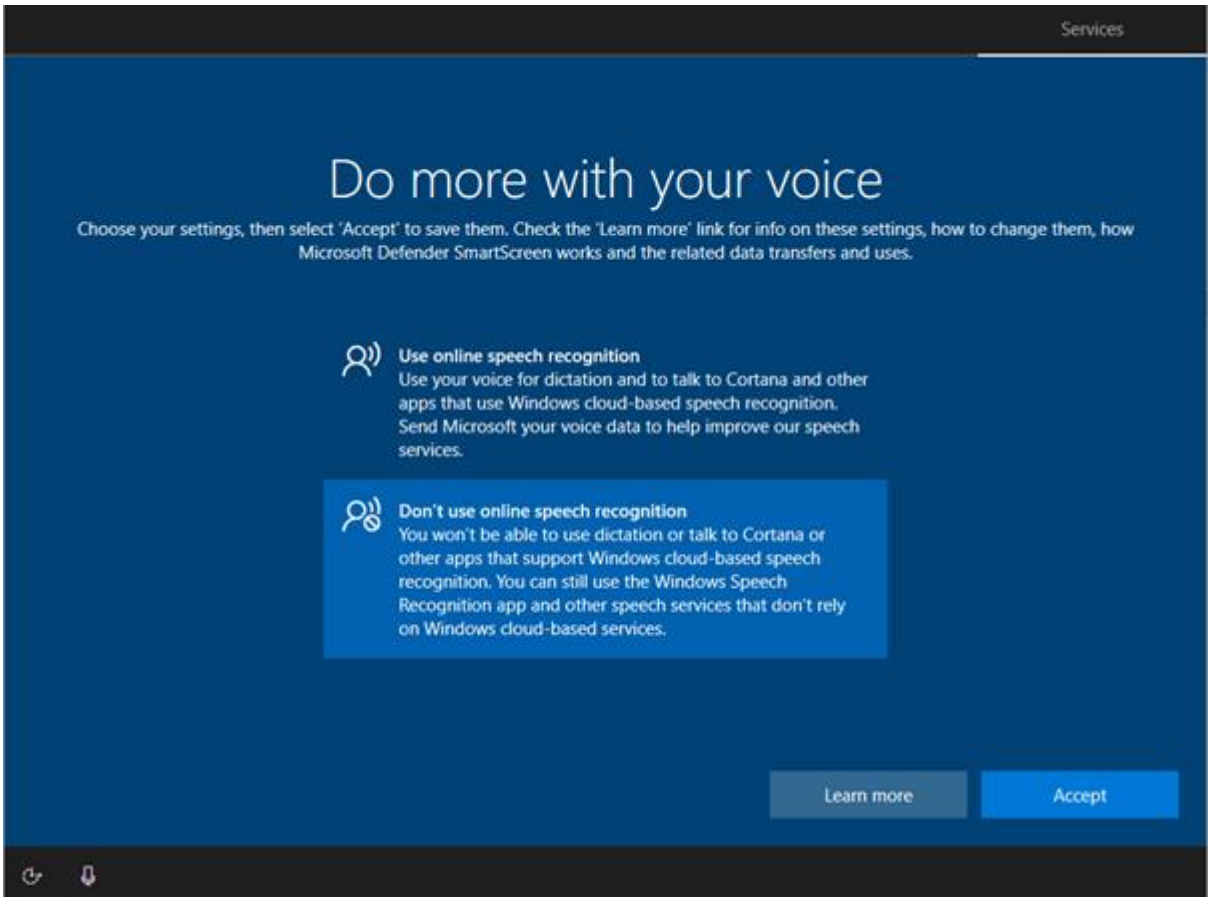
- I add some security questions in case I forget the password. This is the first one. The security questions will allow me to retrieve it account



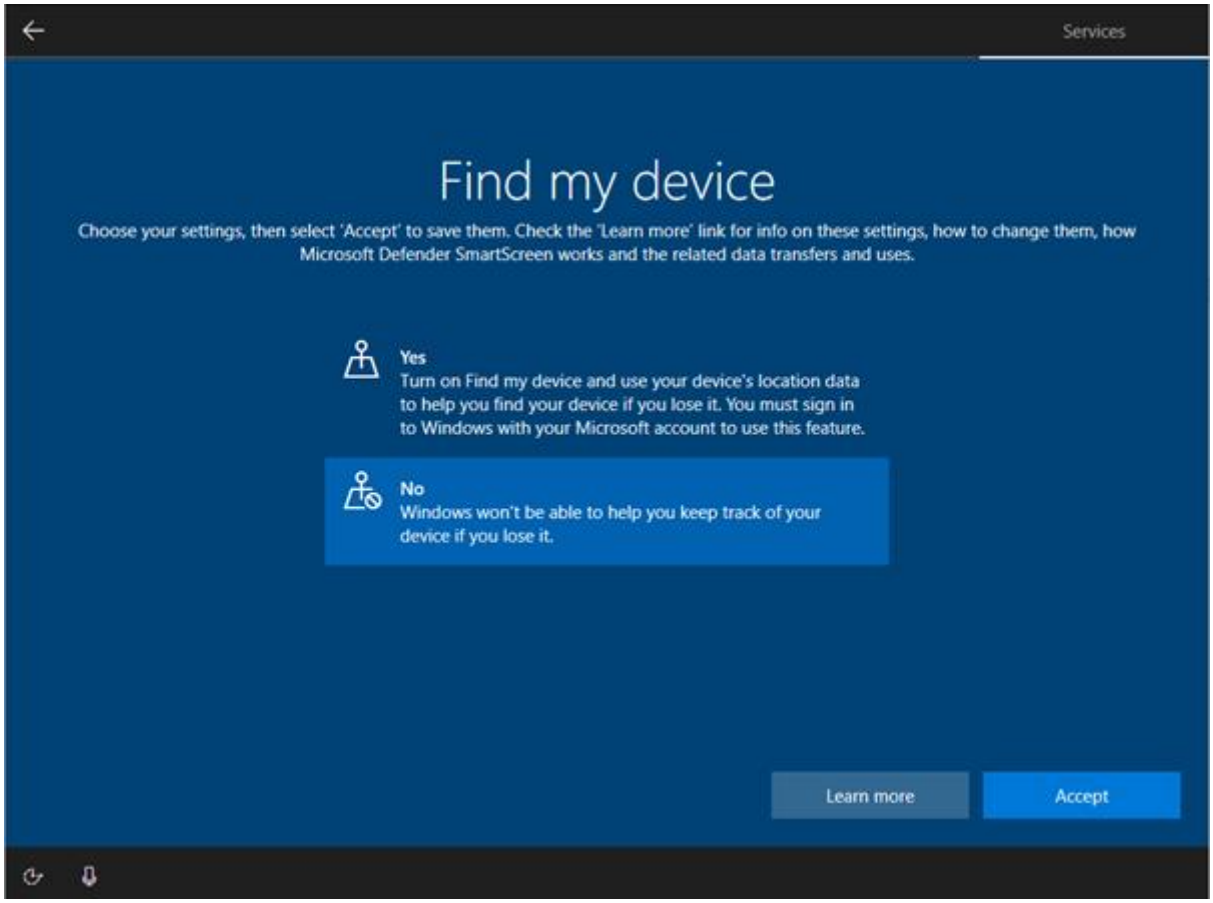
- I add a second security question



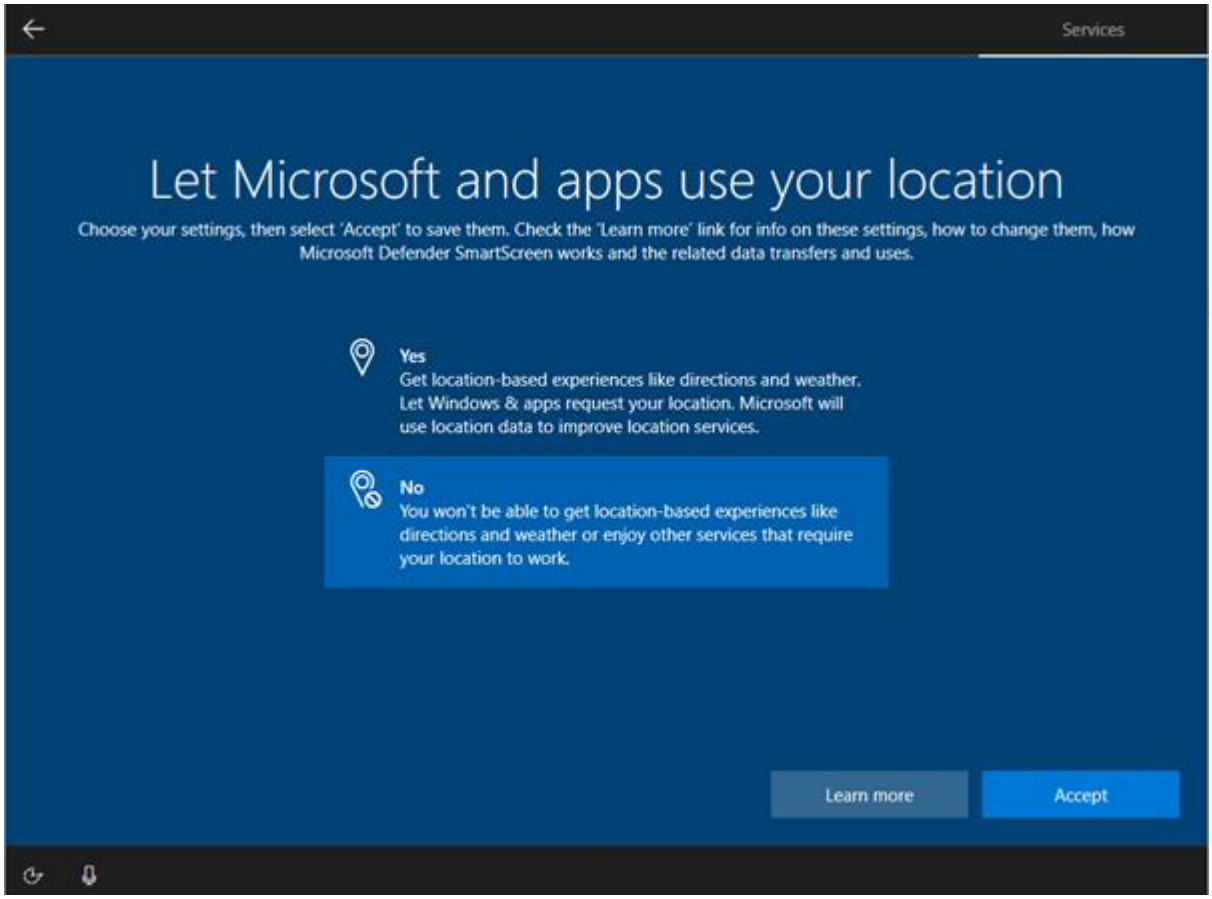
- I need to add 3 security questions in total. This is the third one. Three security questions makes it more difficult for answers to be guessed



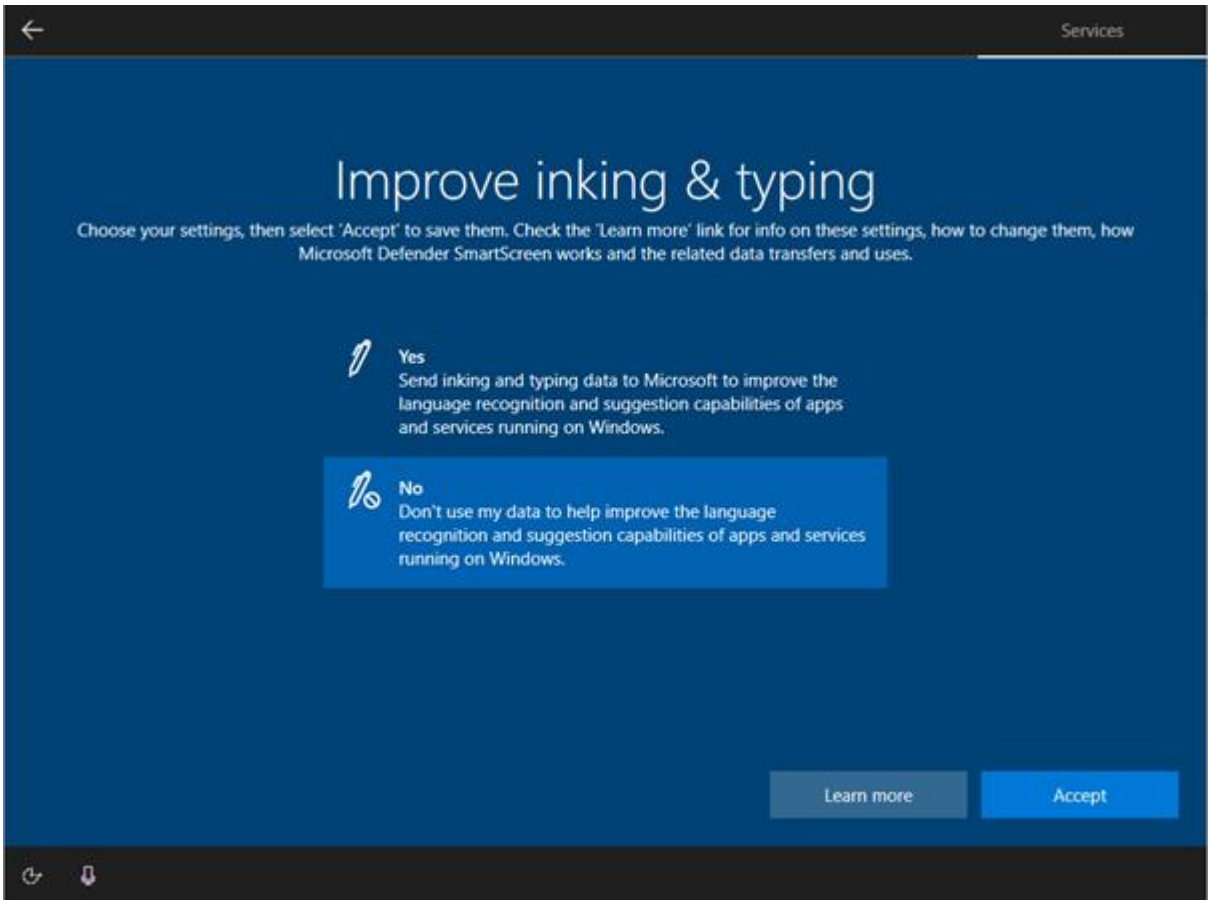
- I don't need voice control as this is a corporate machine. It is not an option that the business uses



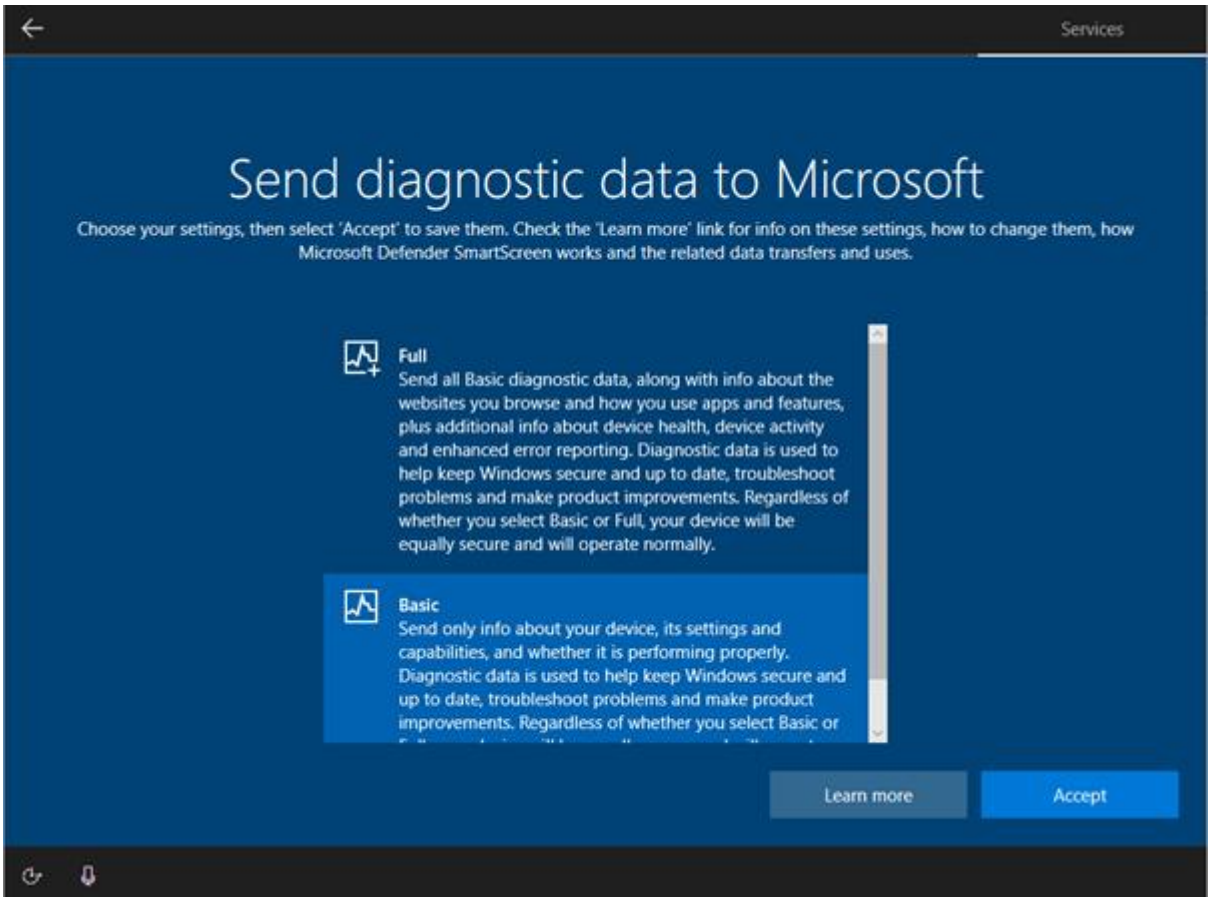
- I don't need to select location tracking as this is a desktop



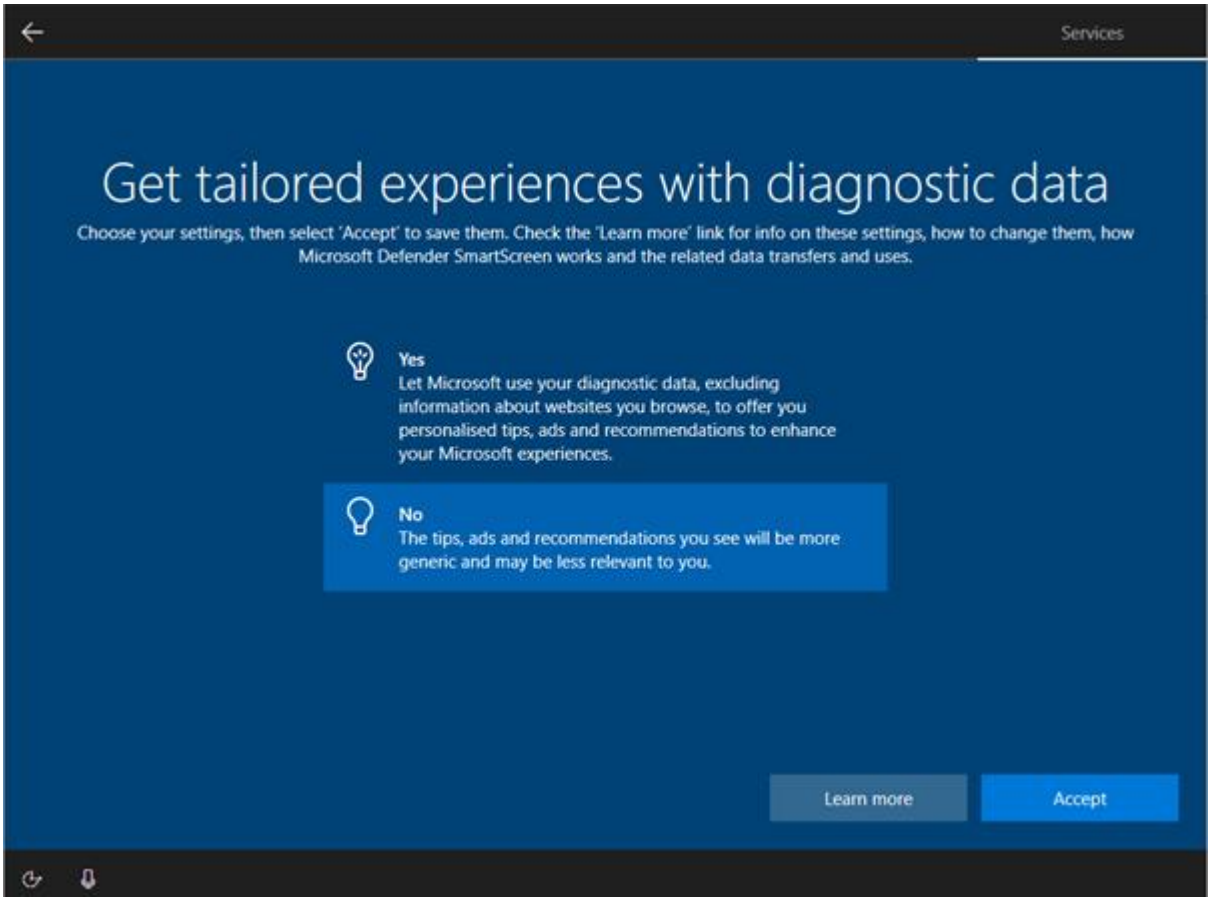
- I don't need find my device as this is a reference image. Nor do I want to allow location settings as the image will be deployed for corporate use and could be a security issue



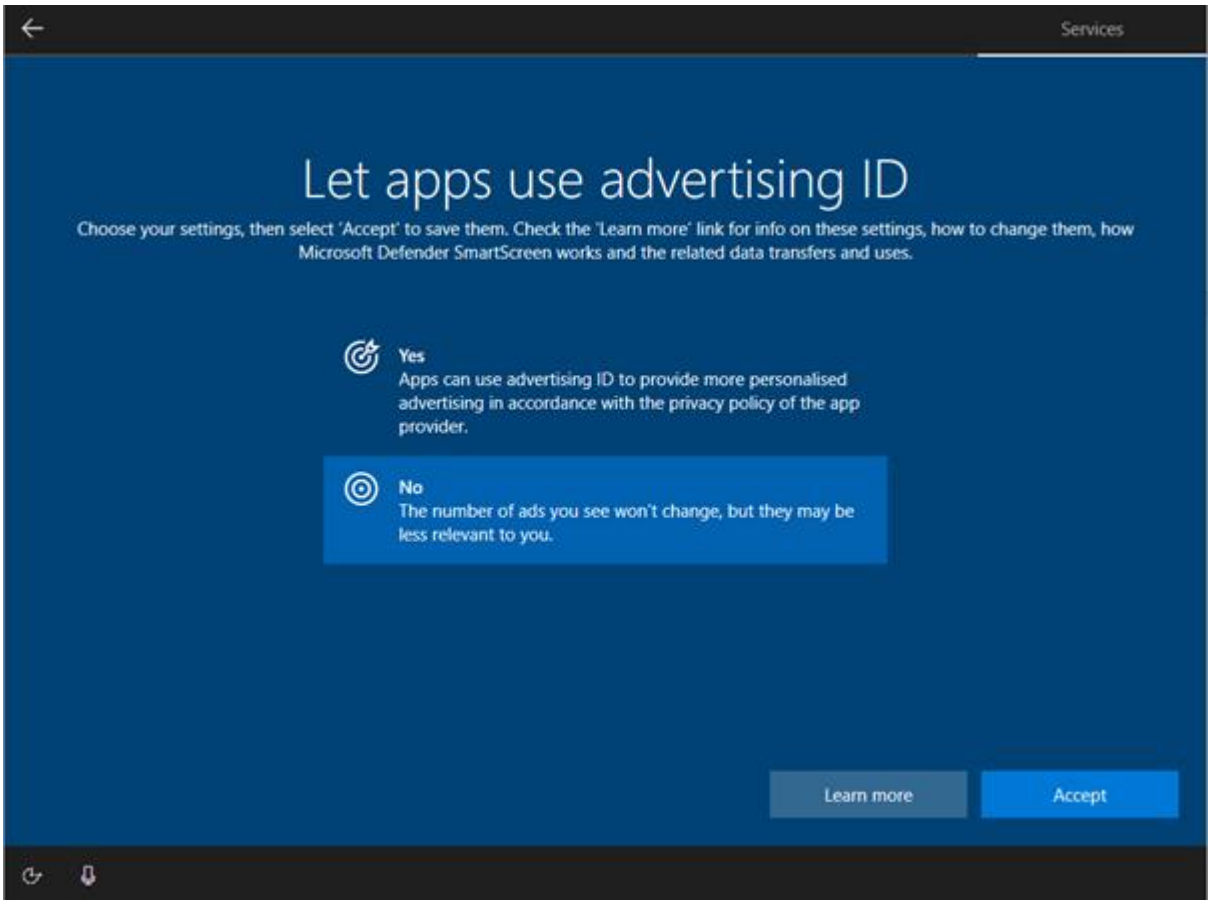
- I don't need "inking" as I will not need handwriting on the image



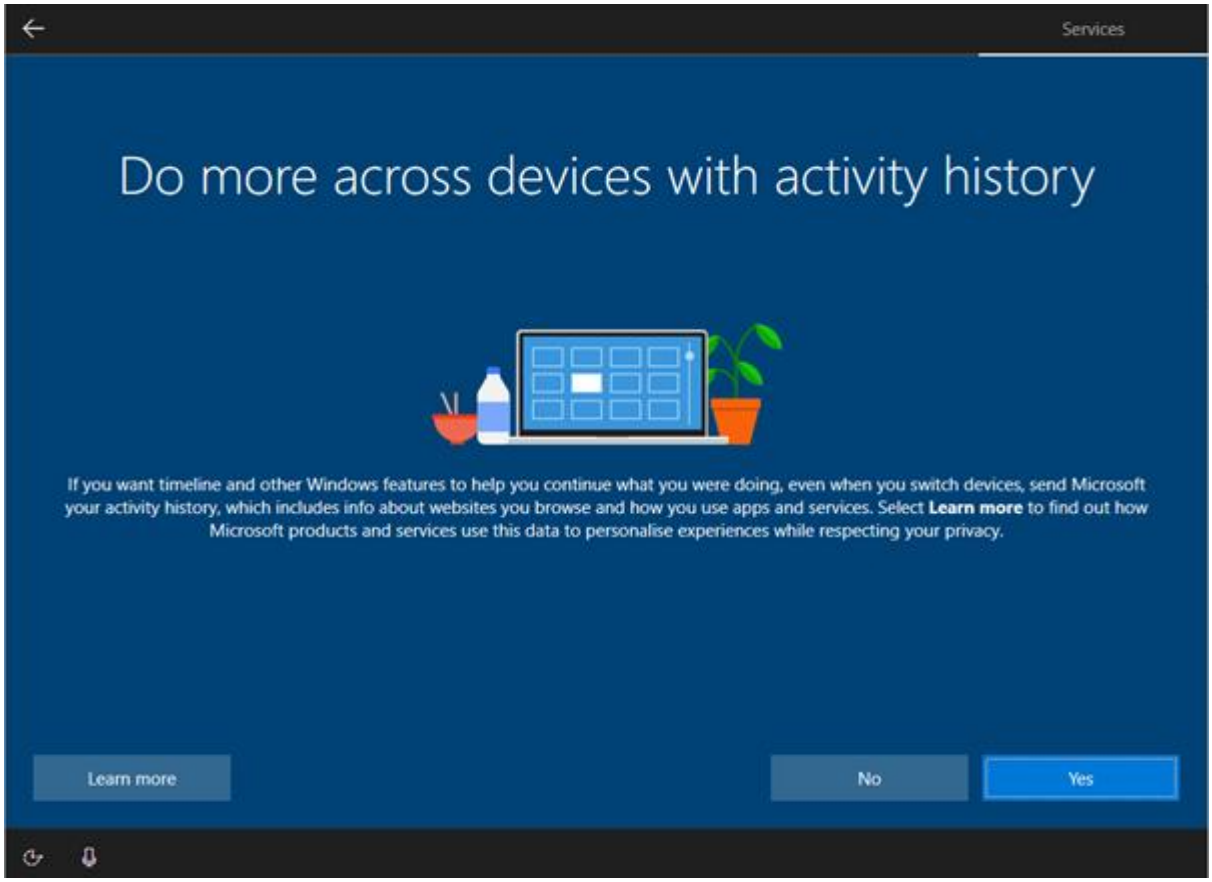
- I choose to only send basic data to Microsoft as it is a corporate image, and it could be a security risk



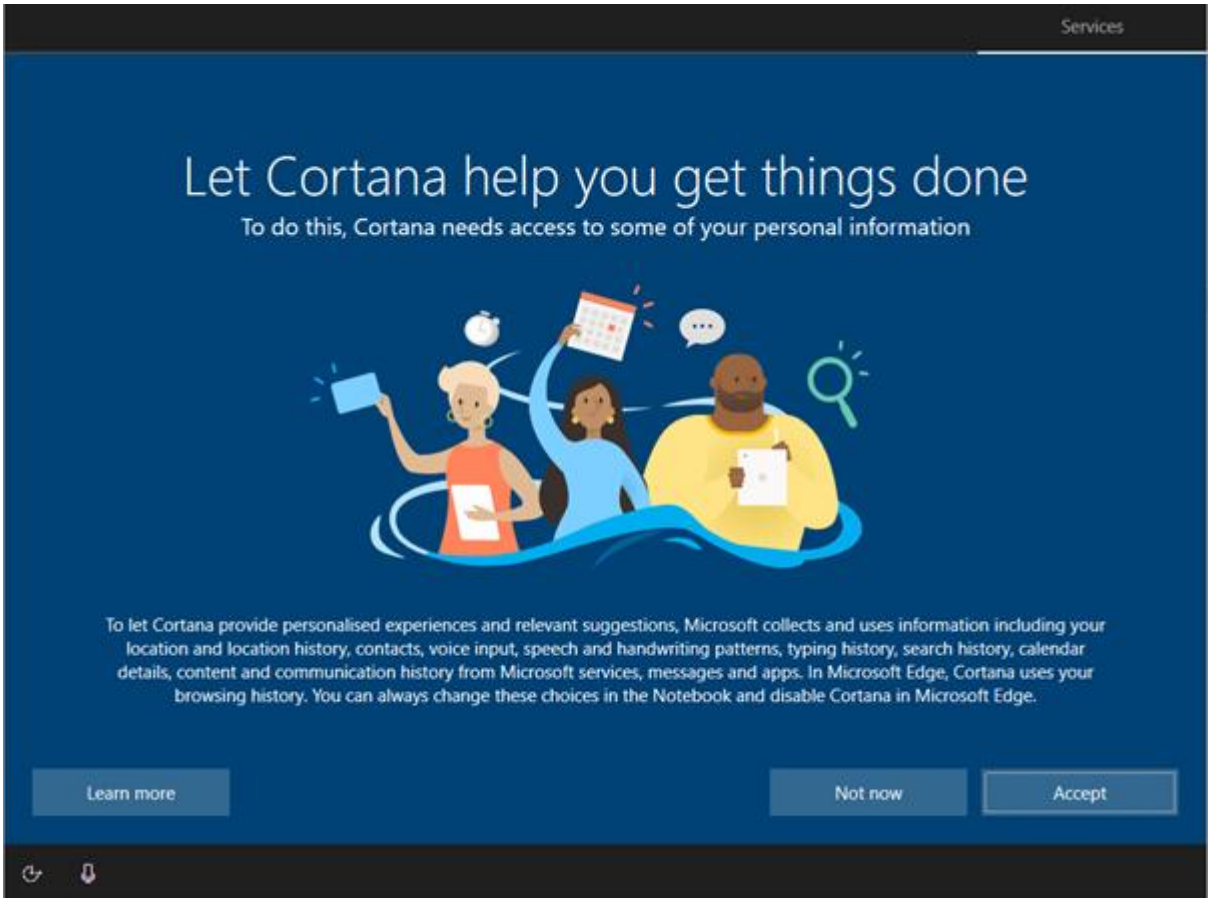
- I will not send diagnostic data to Microsoft as again it is a corporate image



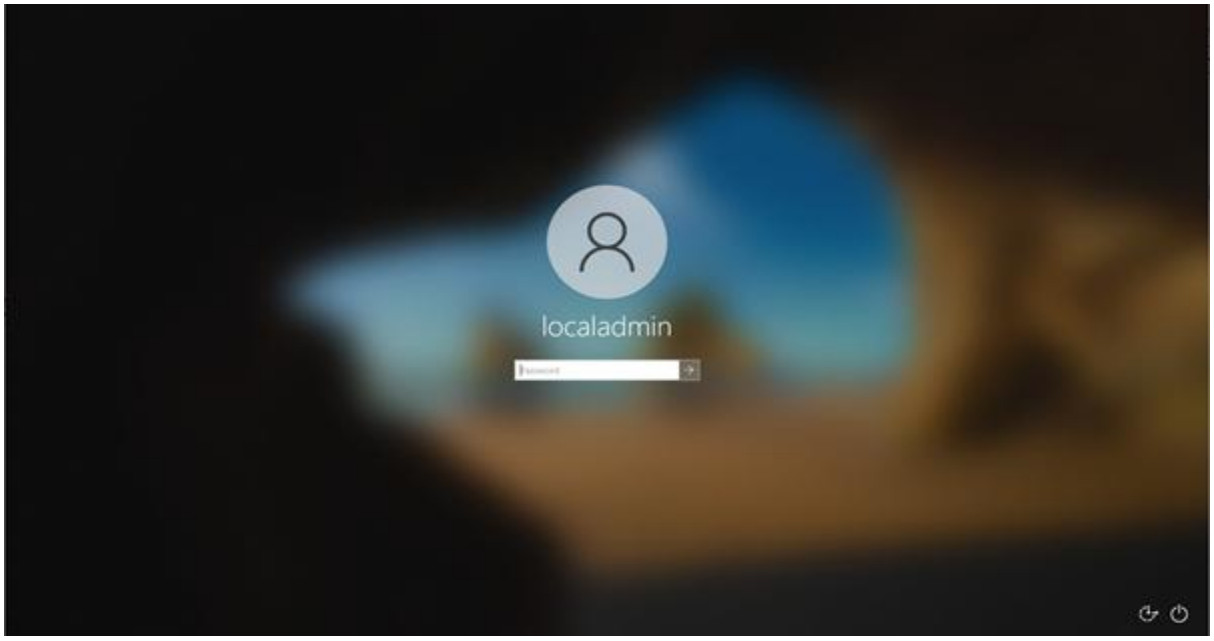
- I do not want advertising to be tailored as again it could be a security risk and this is a corporate machine



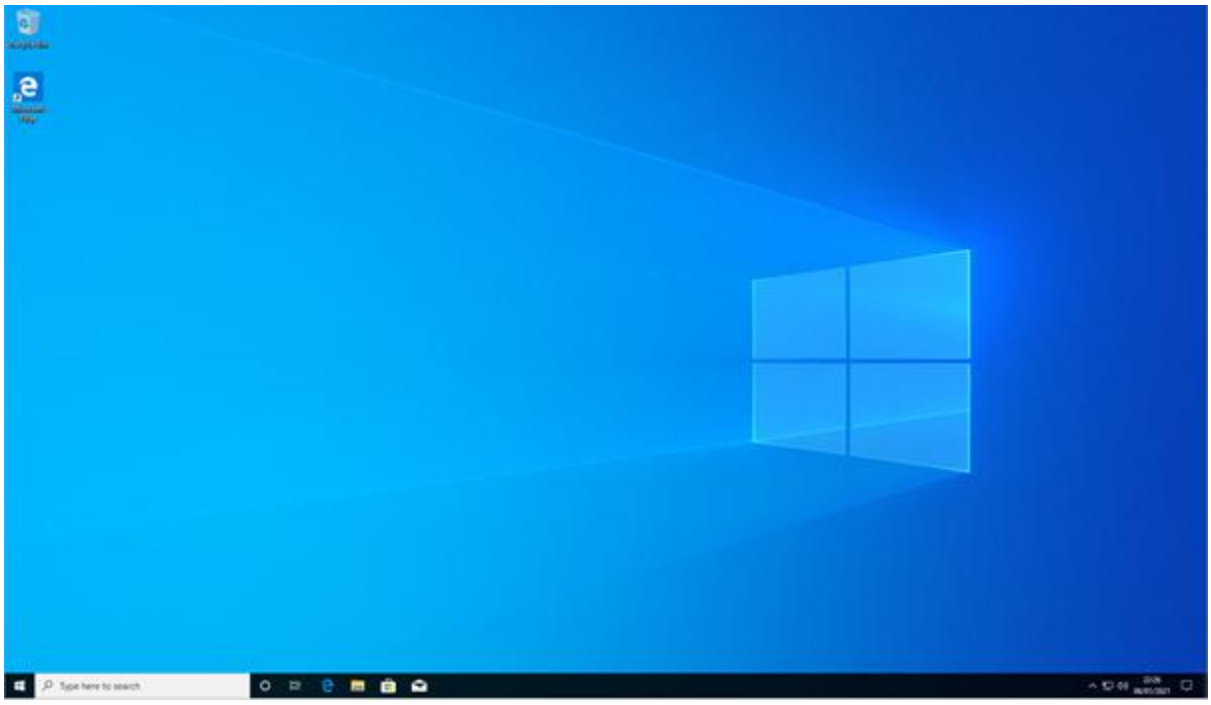
- I agree to history as this will help users to work more efficiently



- I allow Cortana as Windows will not function properly if it is not installed. It can be disabled later via a group policy



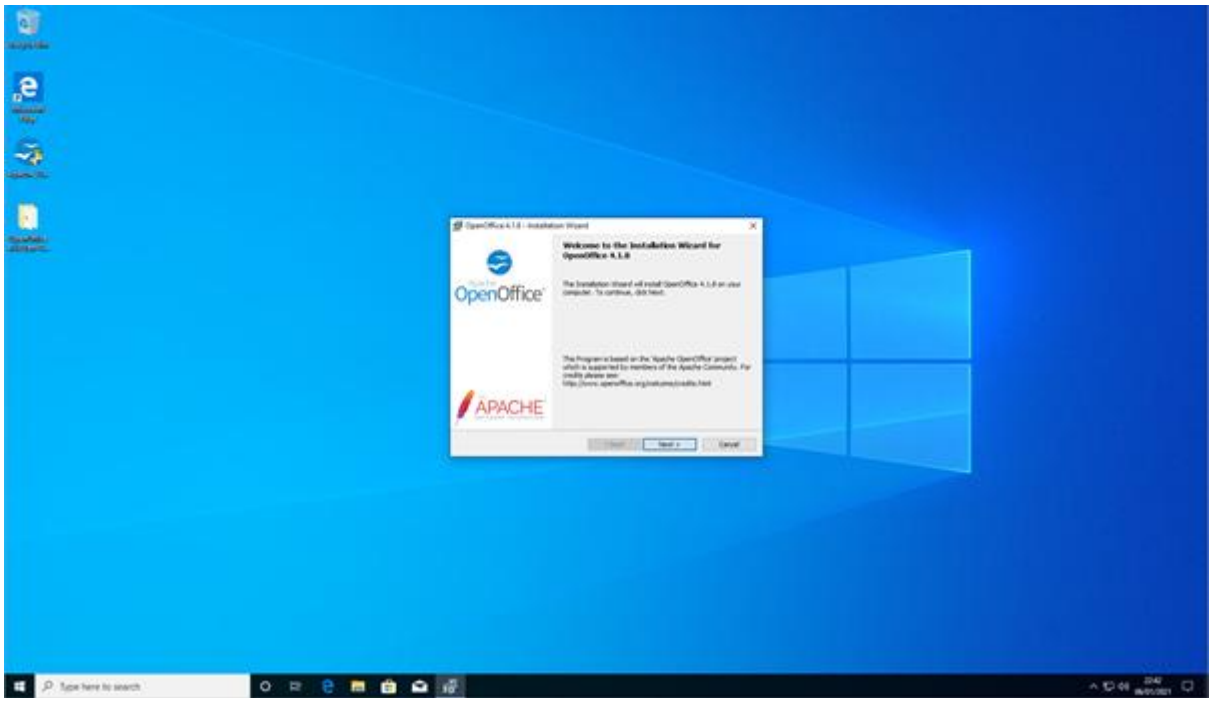
- I can now log in as local admin



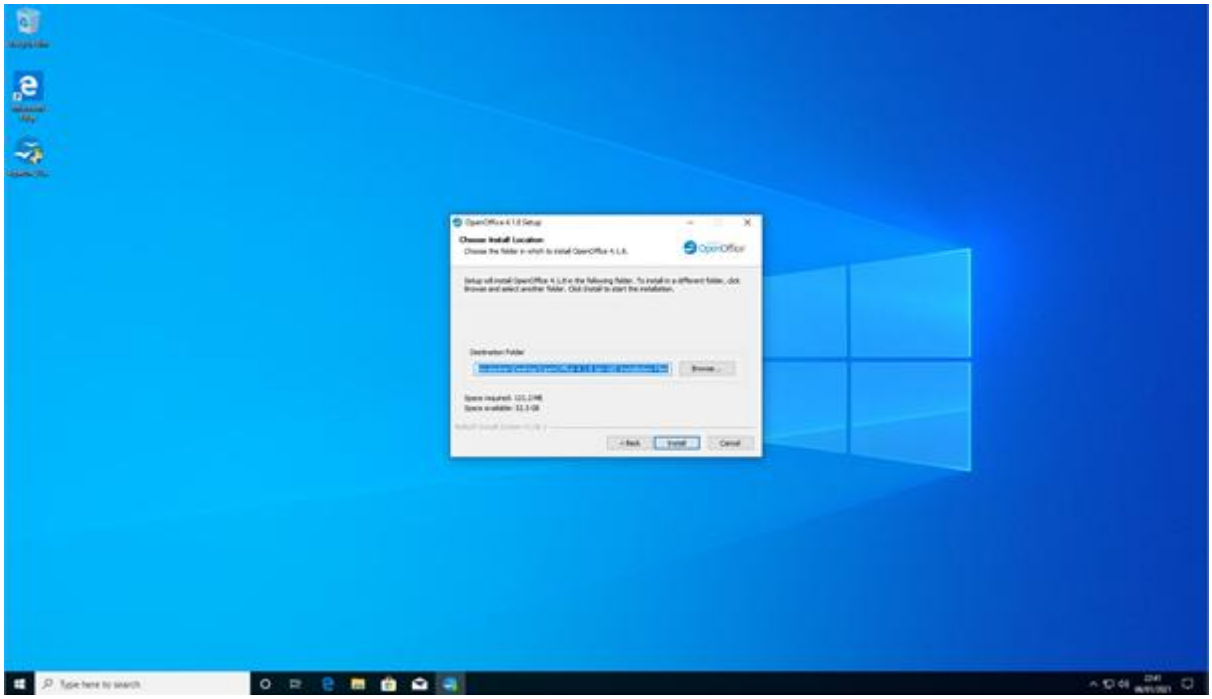
- here is my reference PC logged in for the first time

Installing software

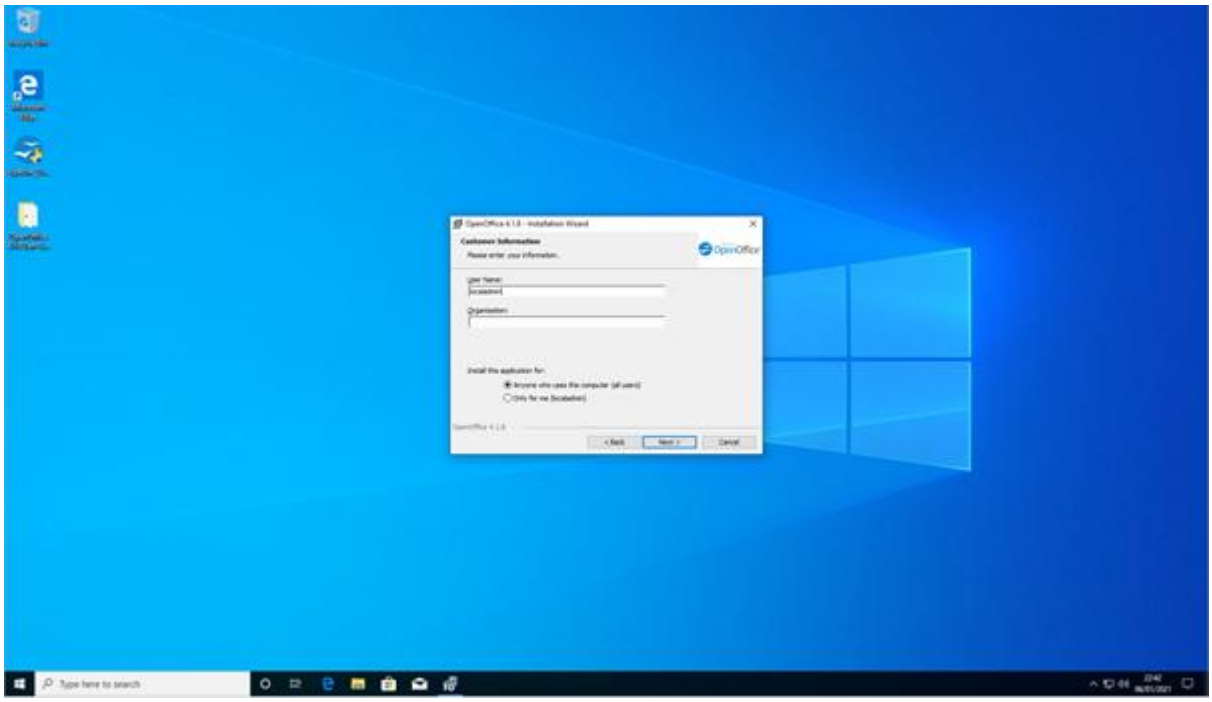
- I am also installing productivity suite OpenOffice. These screenshots show me installing the OpenOffice software, including opening the application to see that it is working ok



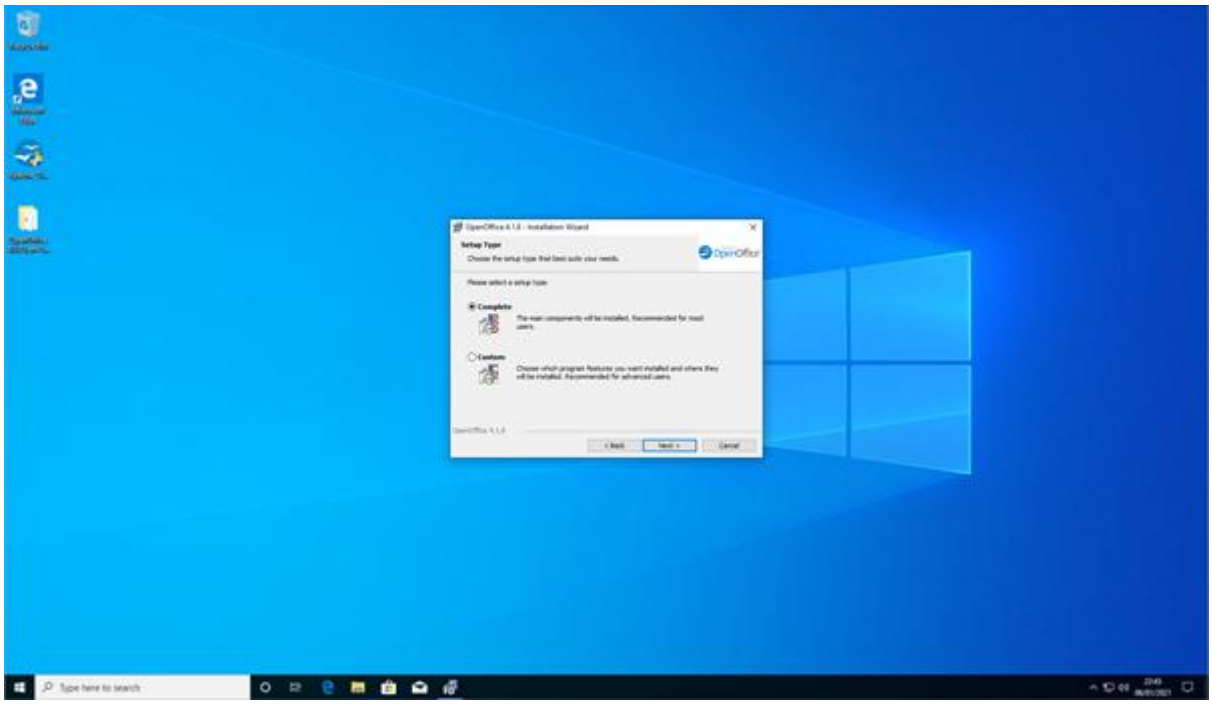
- I start the install for Open Office



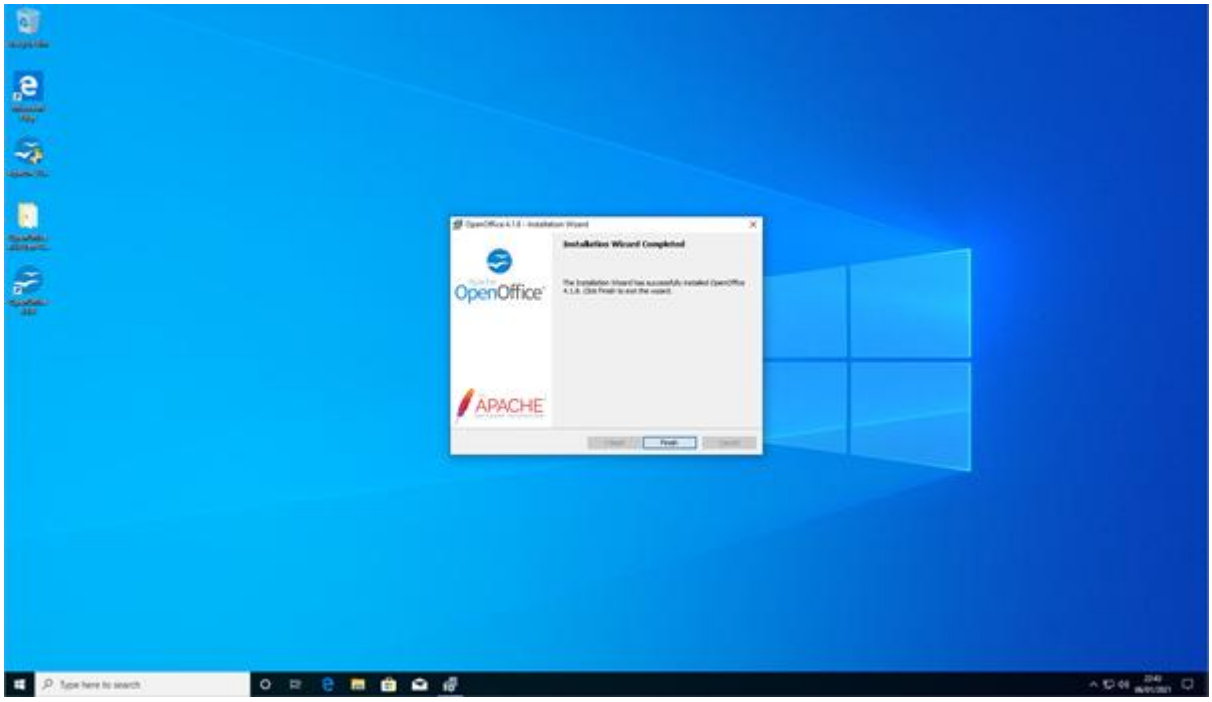
- I select an installation location



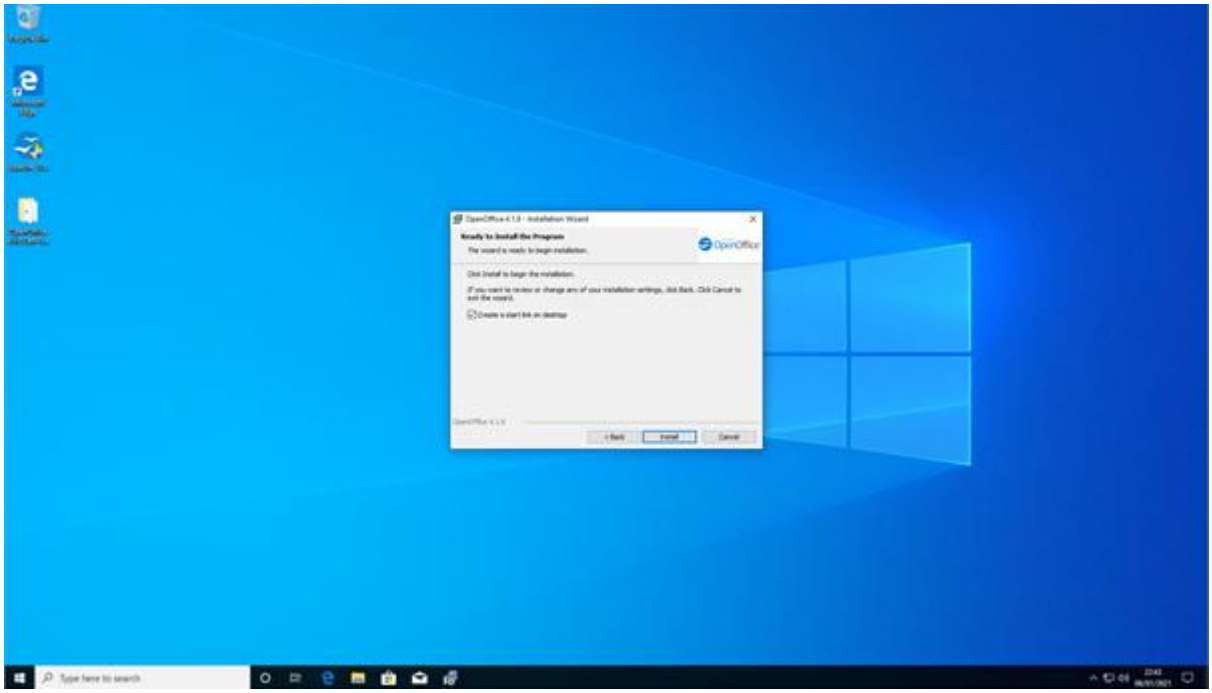
- I enter the organisation details



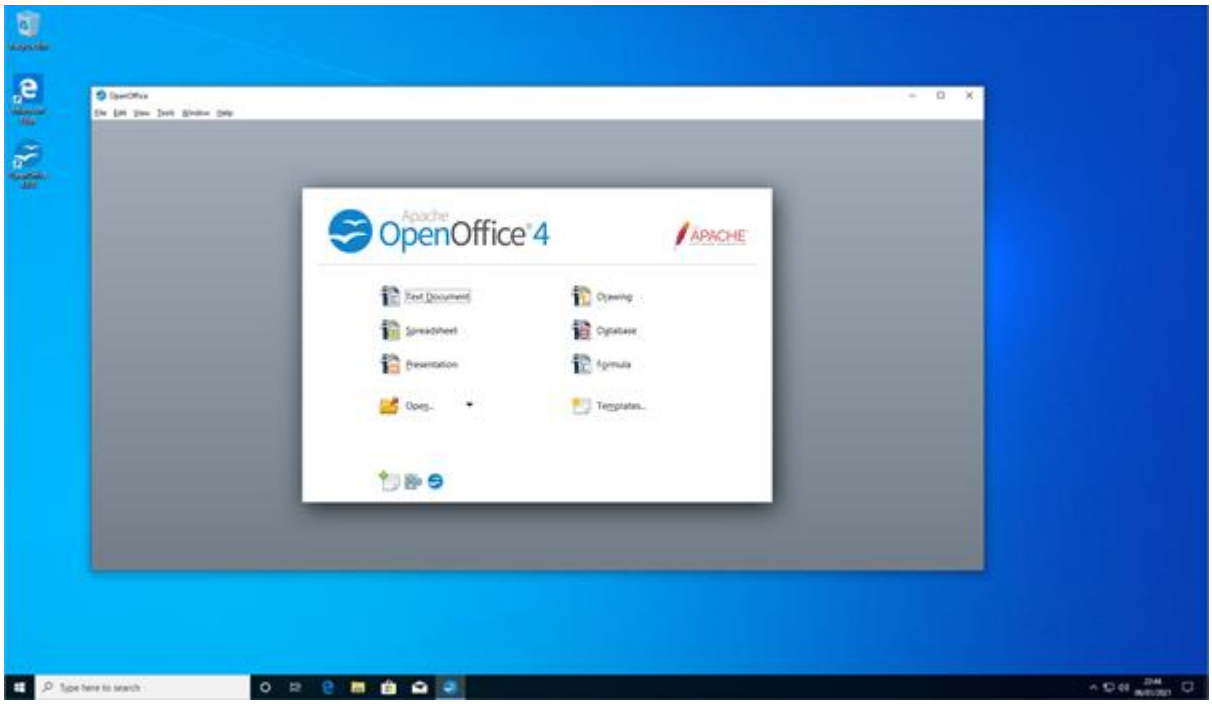
- I select the installation type



- I click next when prompted



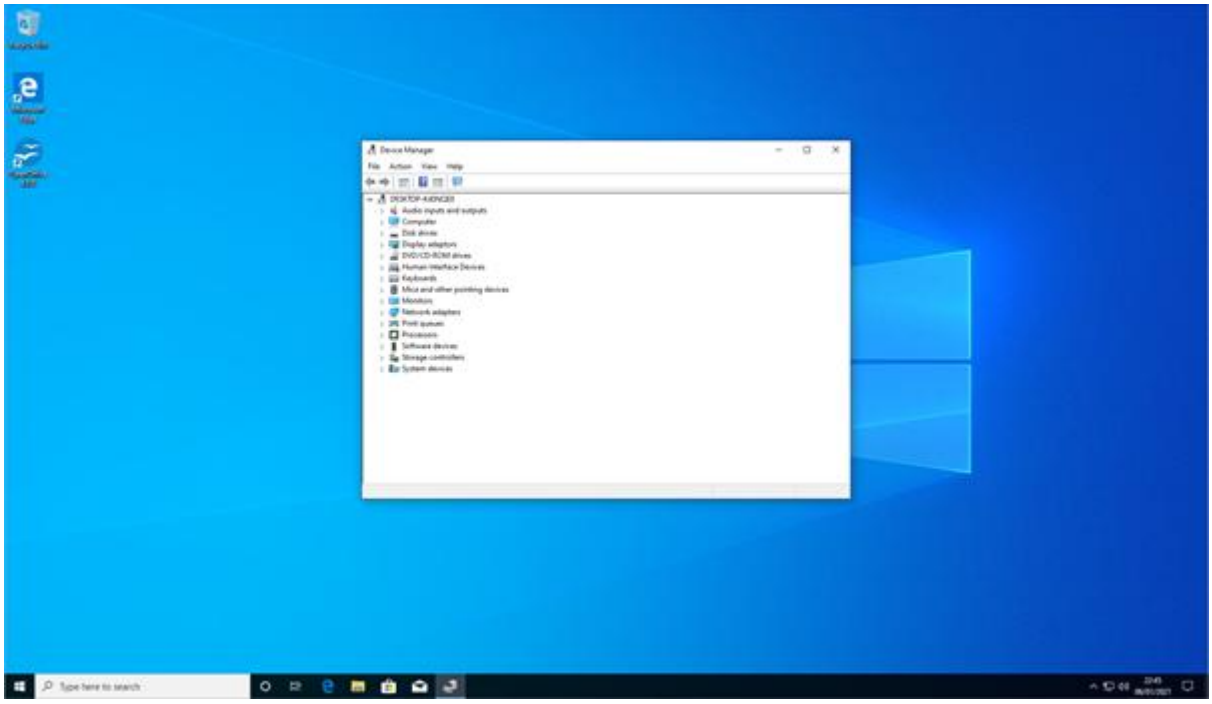
- I click next to move on to the next screen



Open Office is now installed

Checking drivers

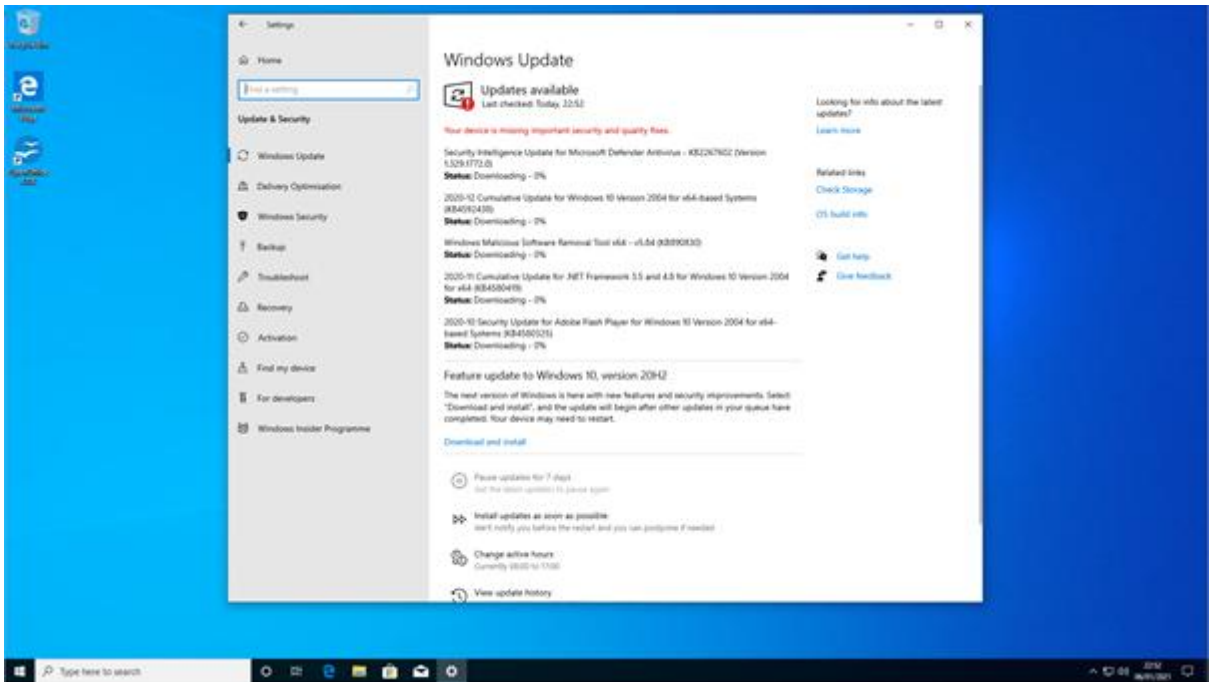
These screenshots show that all drivers on the reference computer are installed correctly. There are no conflicts, missing drivers or outdated drivers.



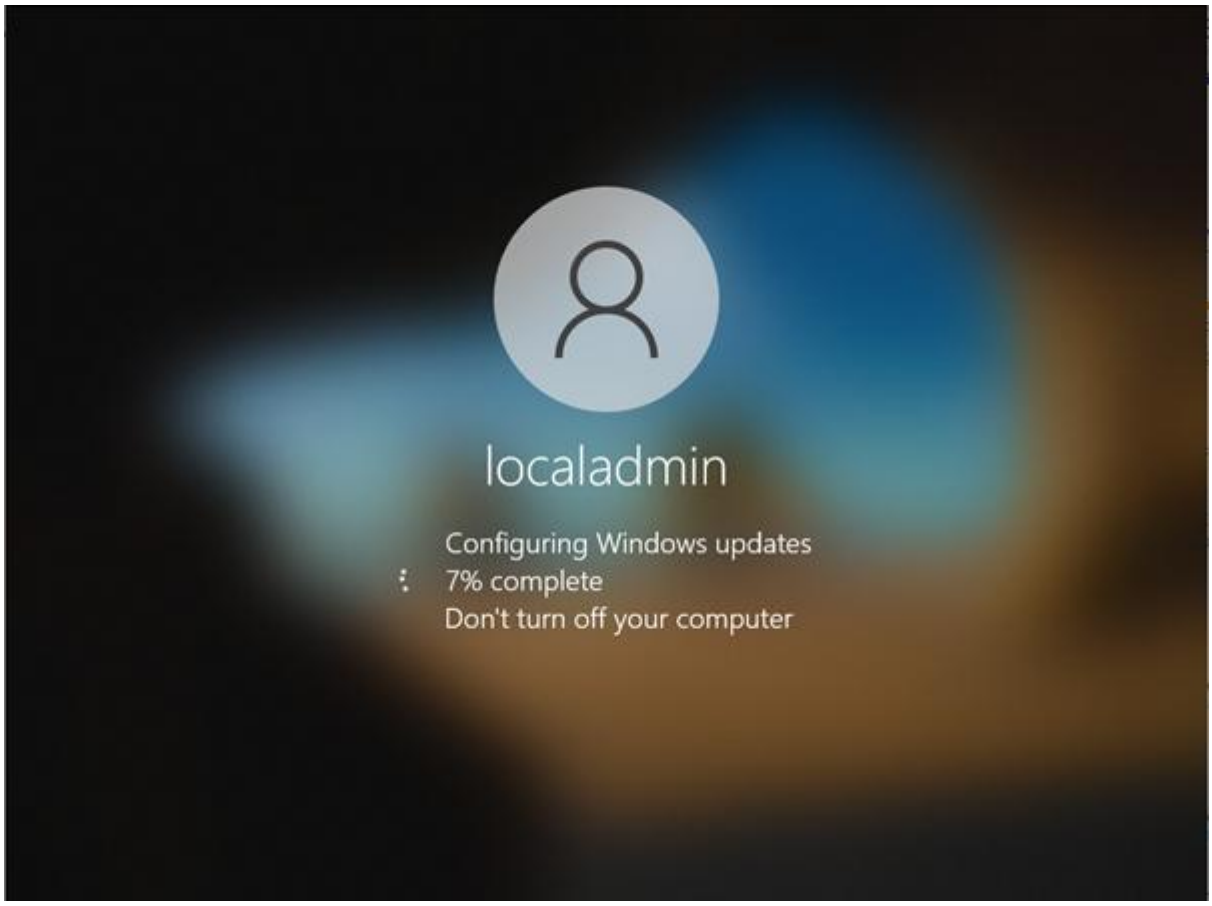
- I check that all drivers are installed correctly

Windows updates

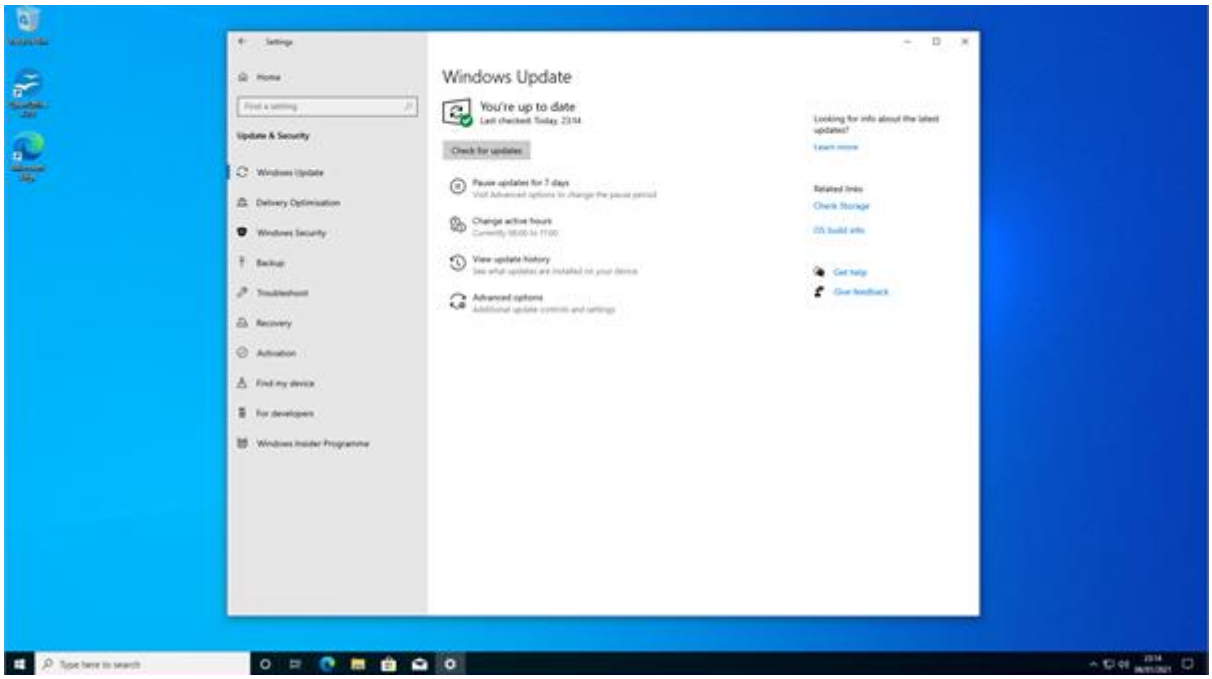
- I have ensured all available updates are downloaded and installed prior to creating a reference image from the reference computer. The screenshots show Windows is completely up to date



- I check Windows is up to date. Then I update as necessary. This helps keep the pc secure and it is better to update before we take the image



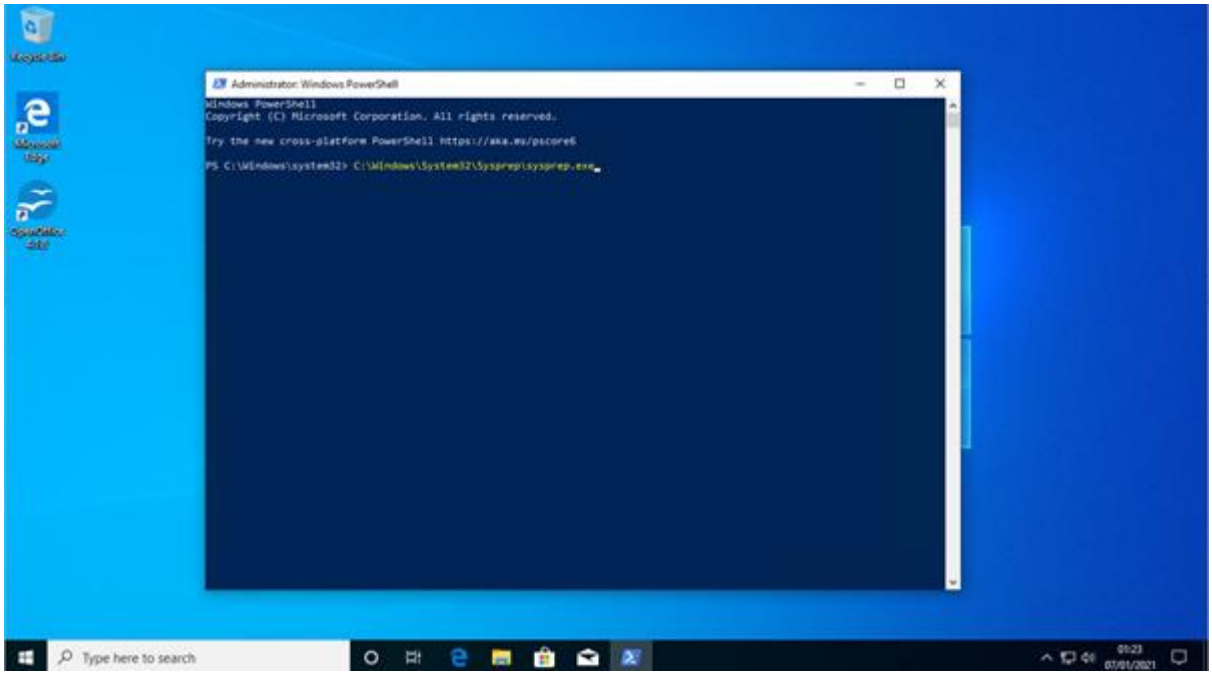
- here updates are being installed



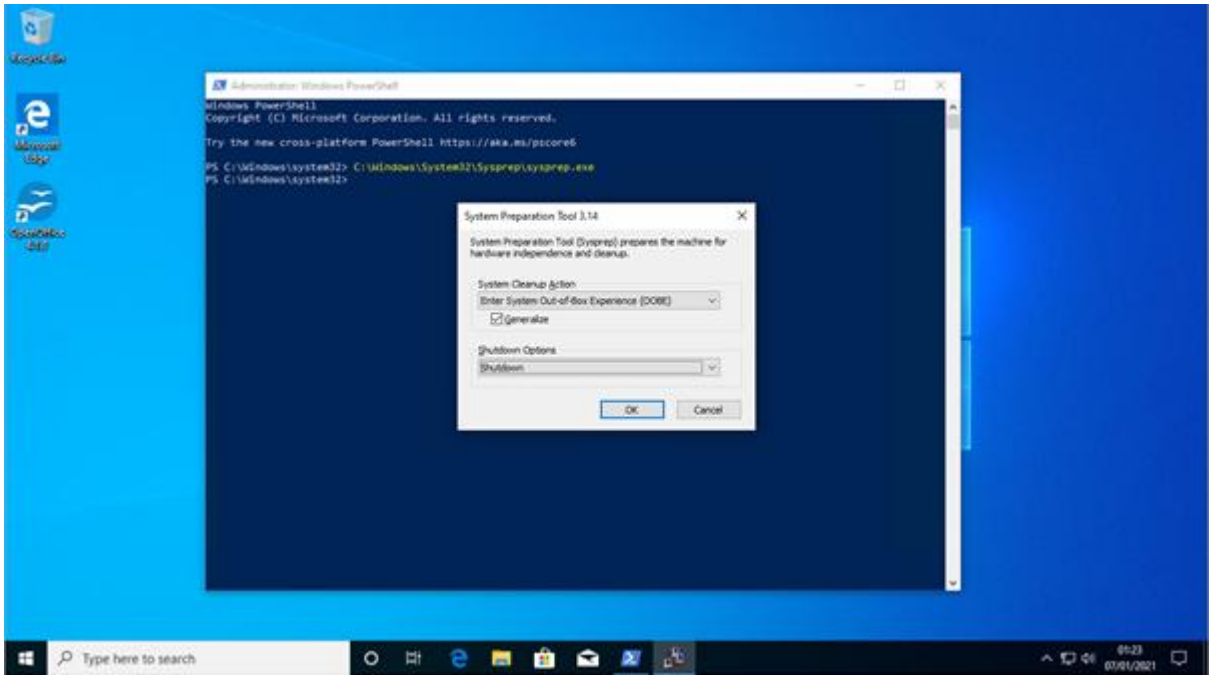
- Windows is now up to date

Create reference image

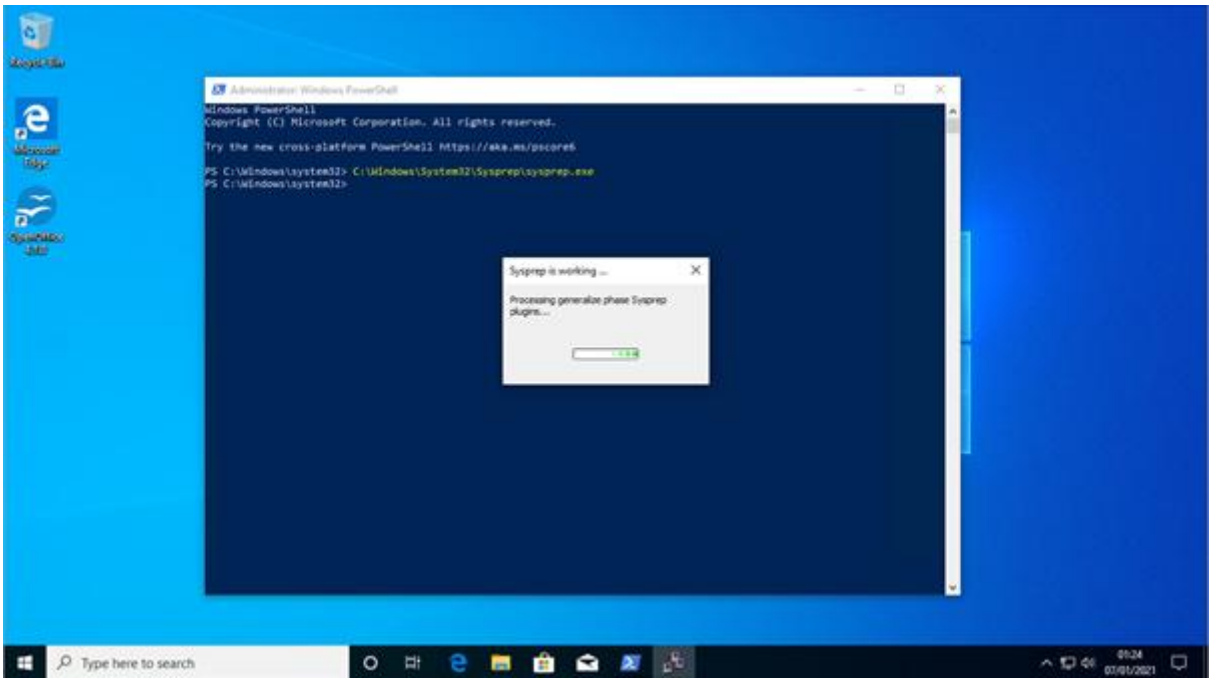
Running the Sysprep tool with the out of box experience (OOBE)/generalise settings means that I have set the Windows installation back to as if it were a new computer out of the box. Generalise tells Windows to remove any traces of user profiles so the computer is completely as new. I now have a completely clean computer set up the way I want that I can duplicate across all the computers in our infrastructure. Once completed the machine shuts itself down.



- I use Powershell to run Sysprep



- I select OOBE and shutdown as my options as this will give the user an “as new” out of box experience when it first boots

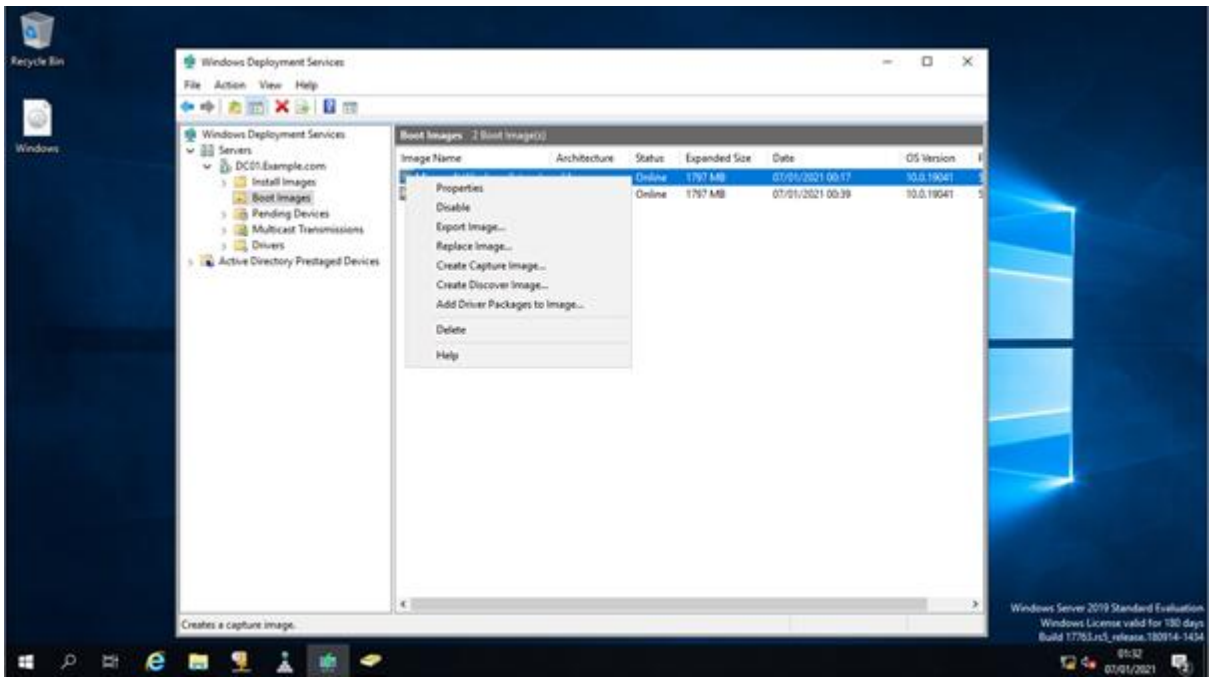


- Sysprep is running
- when finished the machine will shut down

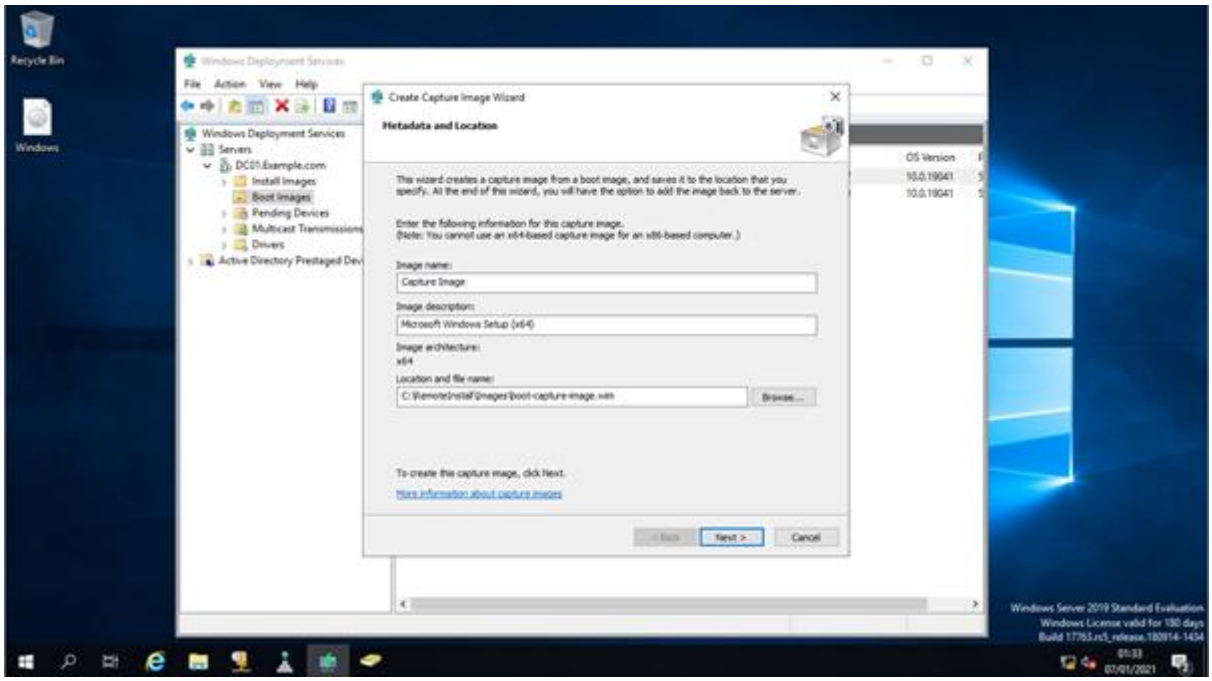
Capturing an image using WDS

Create a capture boot Image

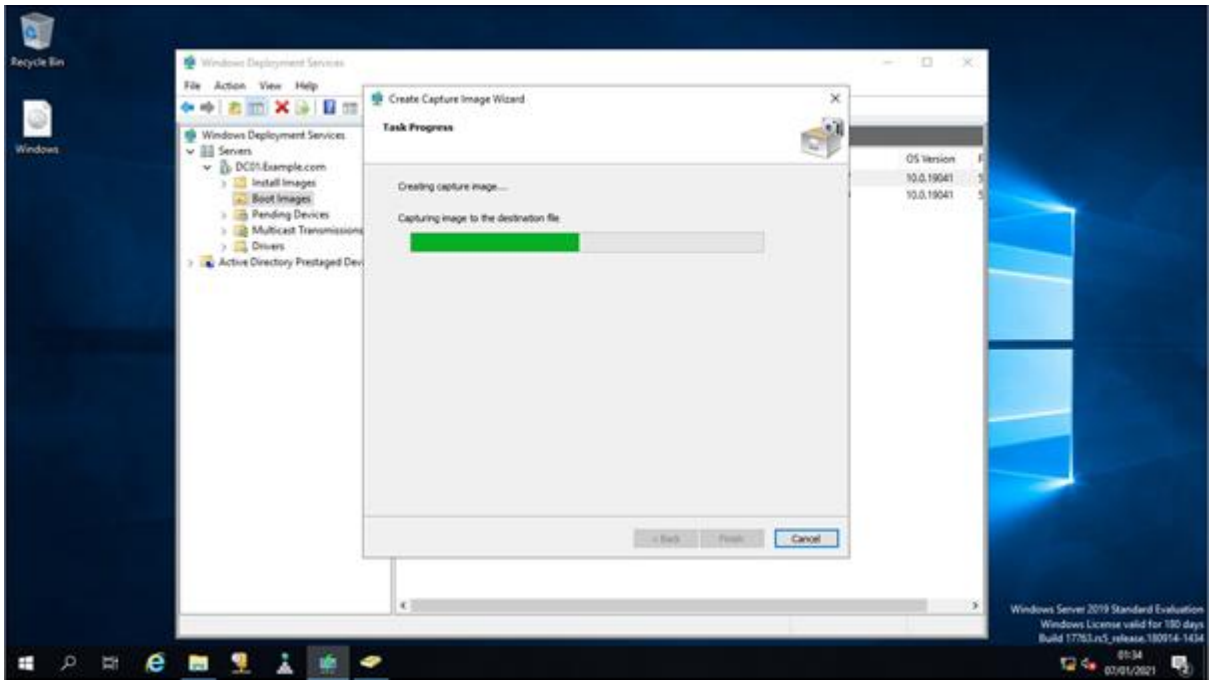
- I have opened WDS, navigated to the boot images folder and right clicked on the Windows 10 setup image. I have selected the create capture image option which has launched the create capture image wizard



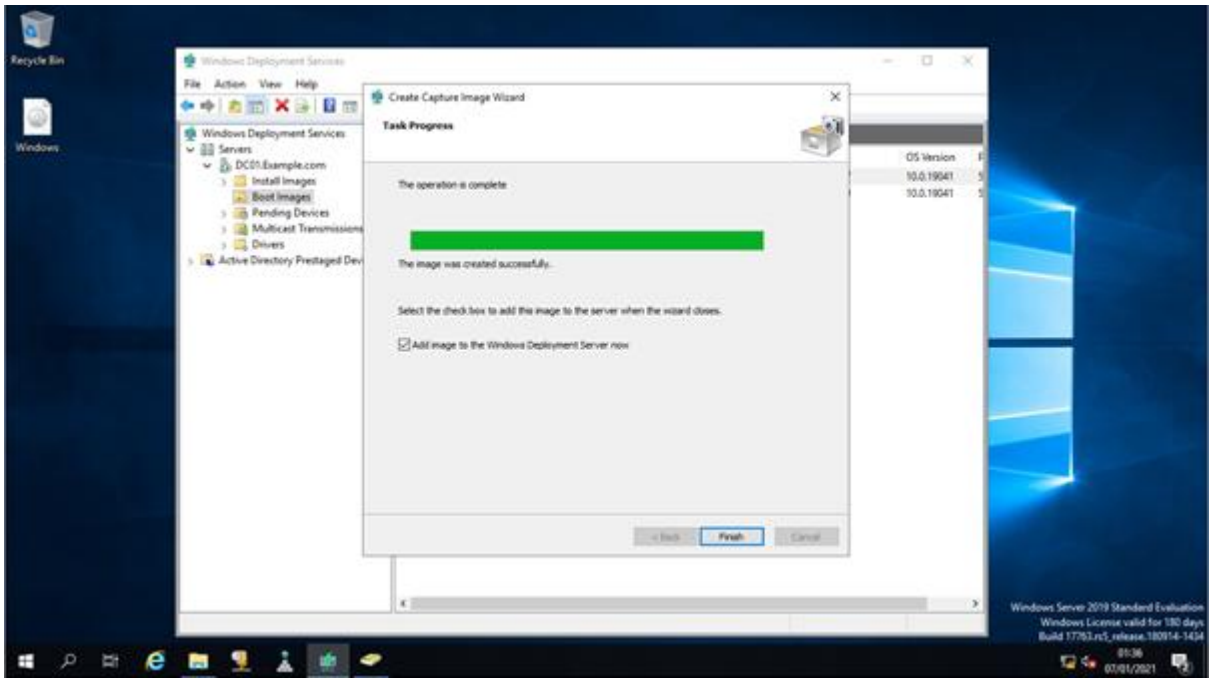
- on my admin machine, I run WDS to allow the capture of the image



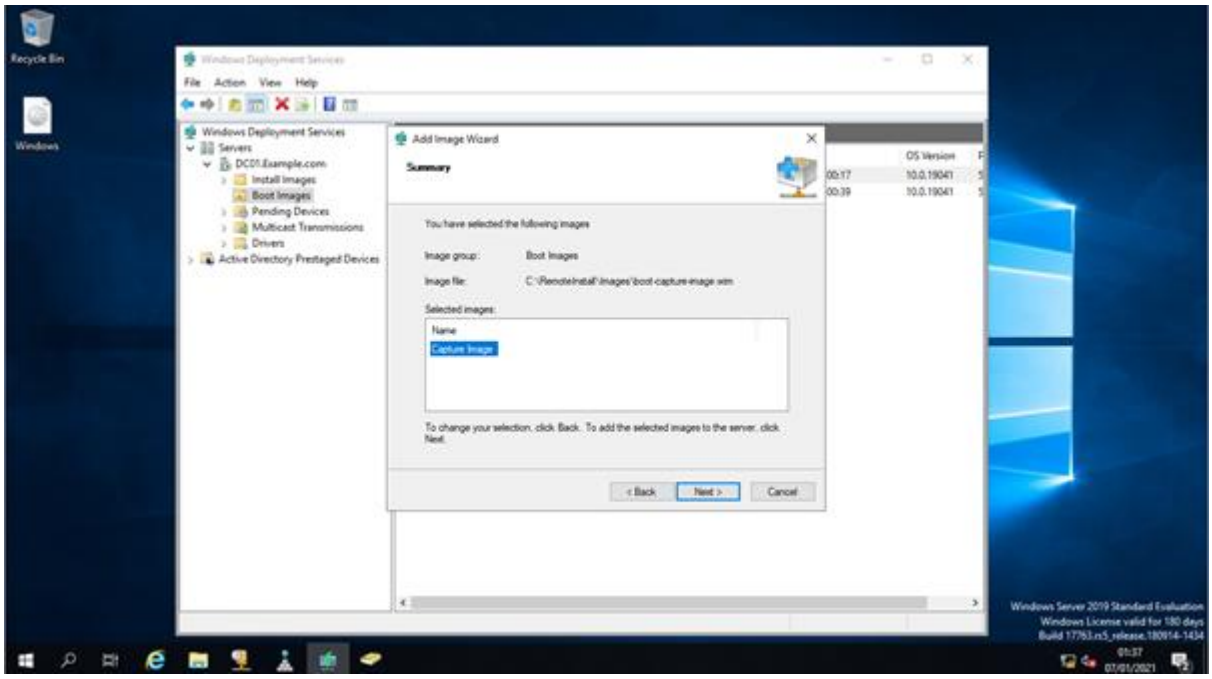
- I select capture an image



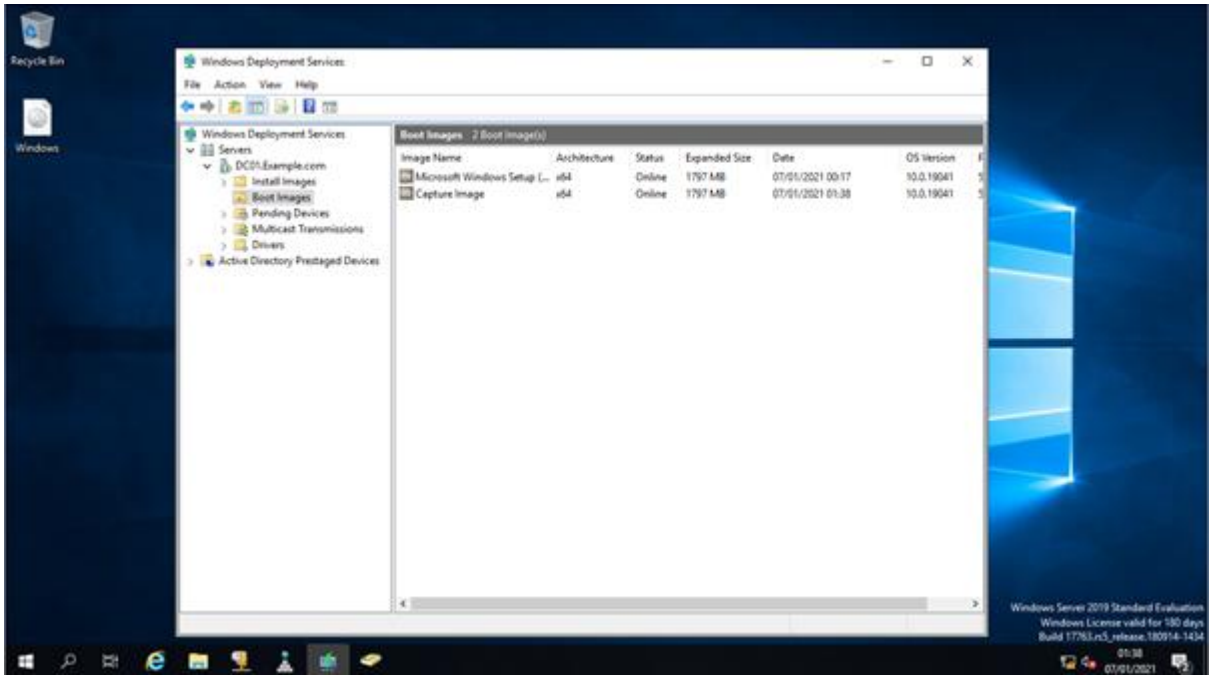
- the capture image is being created



- once done, I click finish



- this summary shows success



Here is the image on the WDS server ready for the capture of the image from the reference machine.

- I have now created a boot image that can be used to boot the reference PC remotely. The capture image includes a wizard that can be used to copy and capture the installation on the reference PC

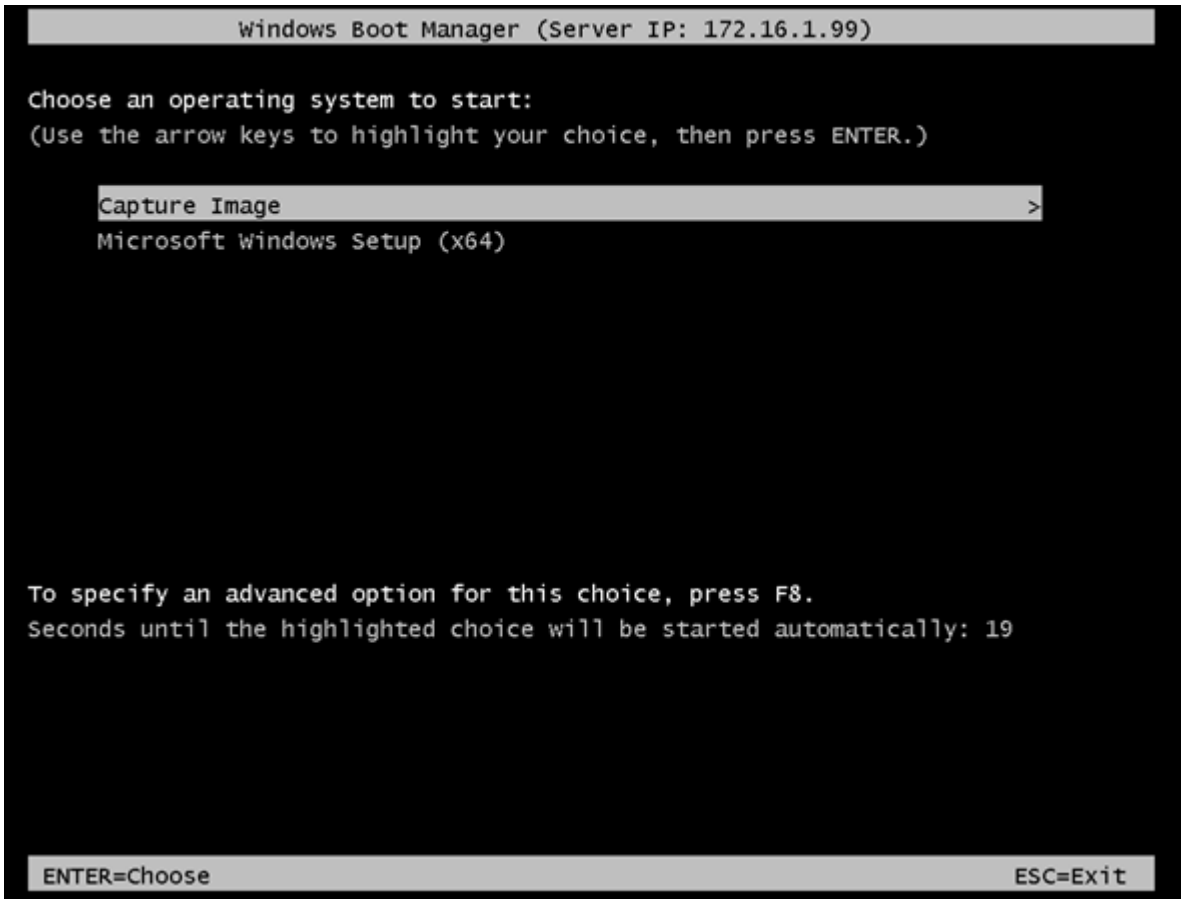
Capturing the reference image

These screenshots show me booting through PXE on the reference PC and selecting the capture image. I then follow the capture wizard with the following settings:

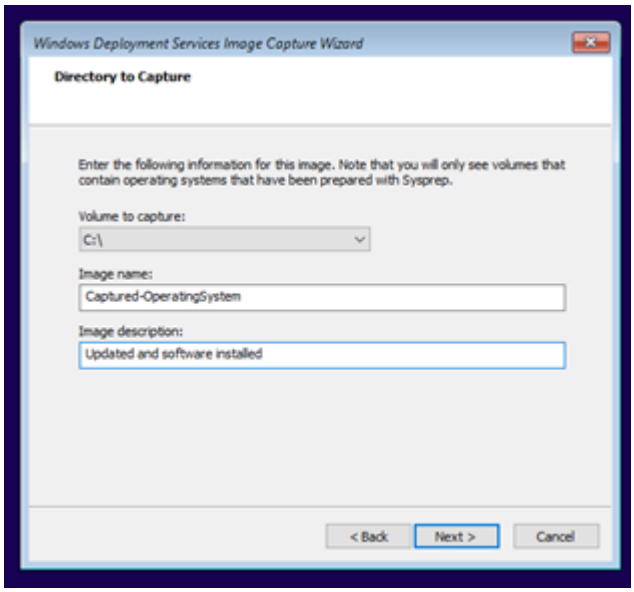
- capture C:\ on the target computer
- image name/description: Windows 10 custom image
- select an appropriate save location and, also select to upload to a Windows deployment server
- specify the server name and use the domain admin credentials to connect to the server
- the reference image is then captured and copied to the server

This answer file can now be copied to as many computers as we want.

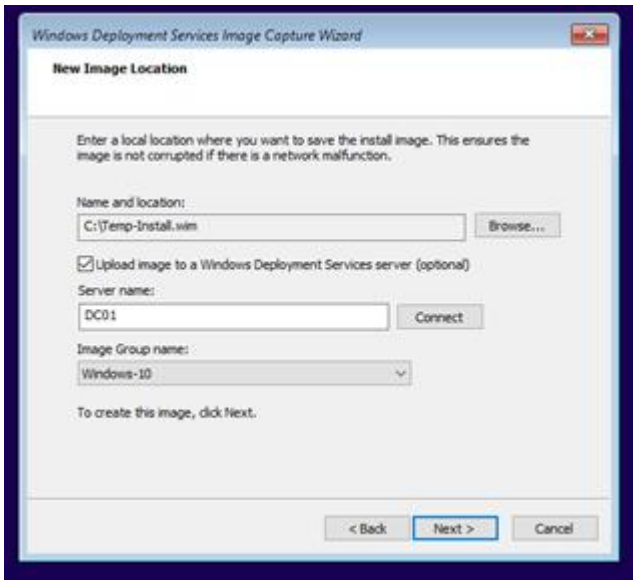
- I boot using PXE



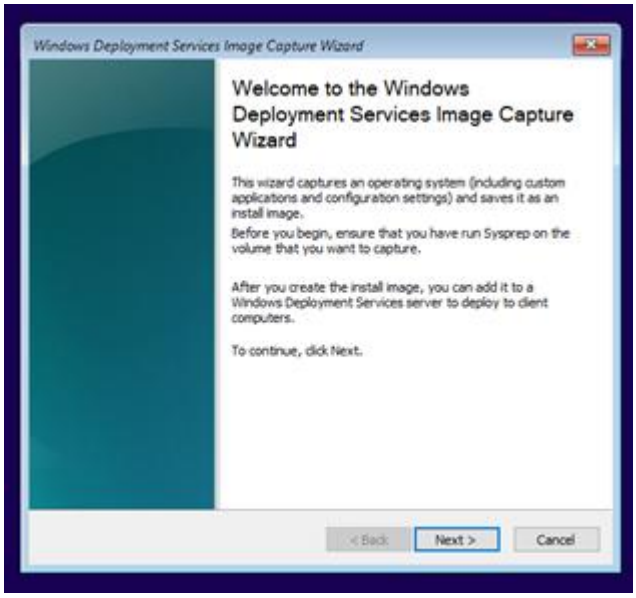
- I select the image from the server



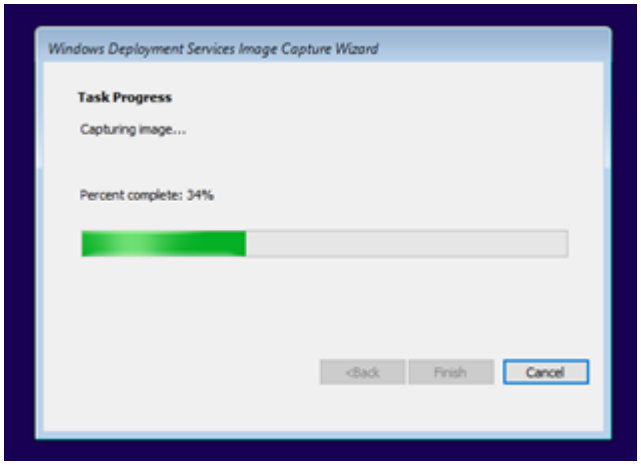
- I select the location



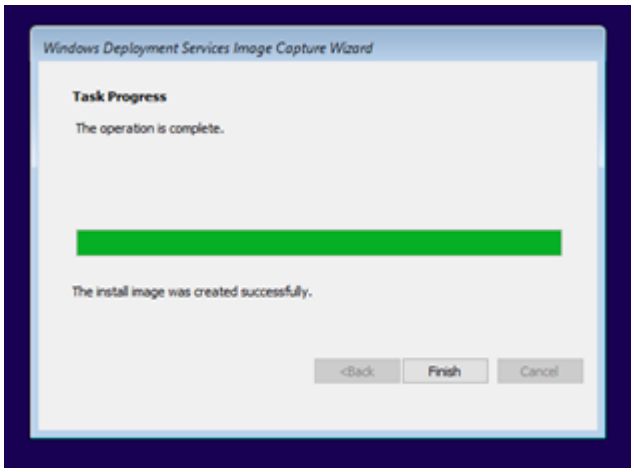
- I complete options



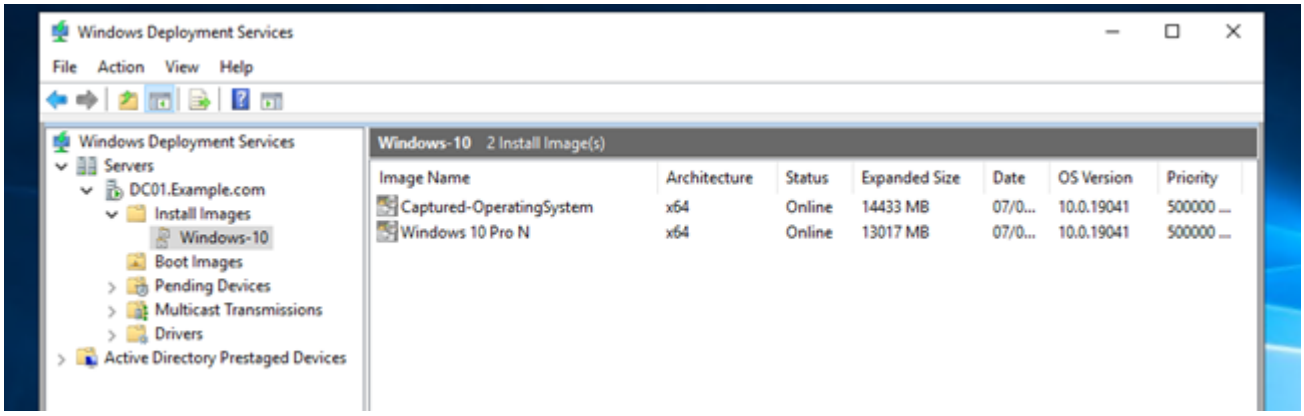
- I add further details



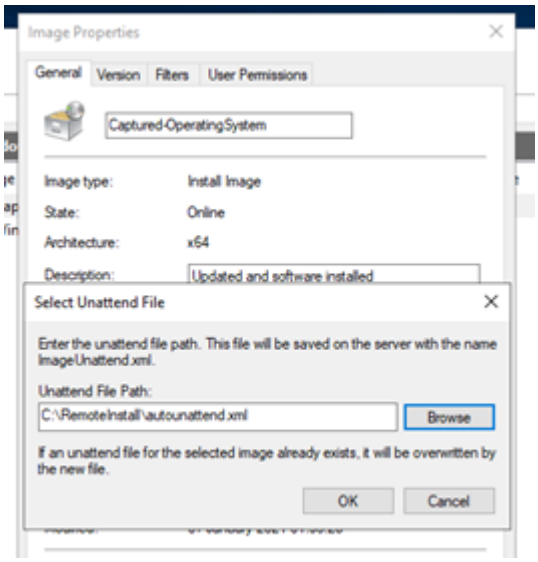
- here we see the progress



- progress is 100%



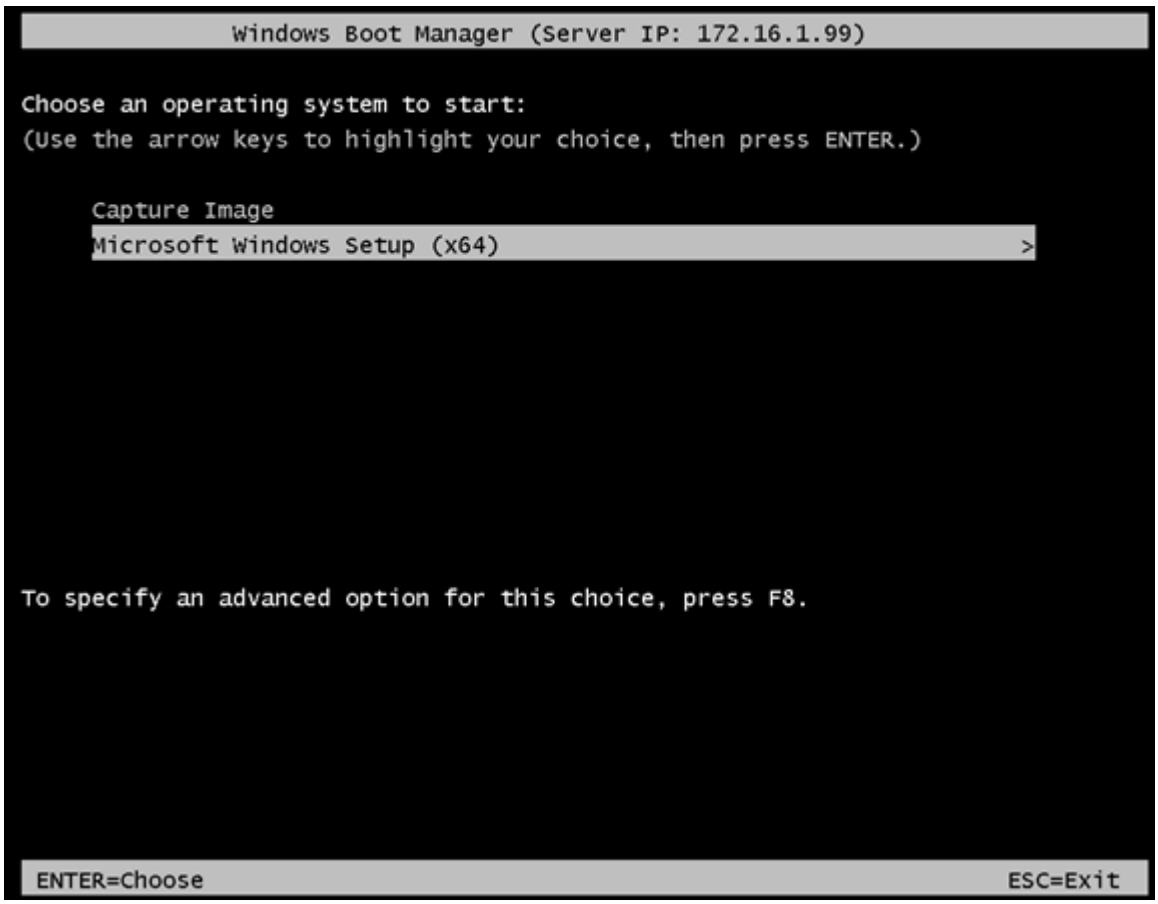
- the capture is complete
- when deploying to a target computer we want the target PC to automatically join to the domain, to achieve this, we need to configure an answer file; the answer file will be set to respond to all configuration options in the OOBE and then join the PC to the domain
- these screenshots show the use of the autoattend.xml file created to join the domain and configure other settings for the deployed system



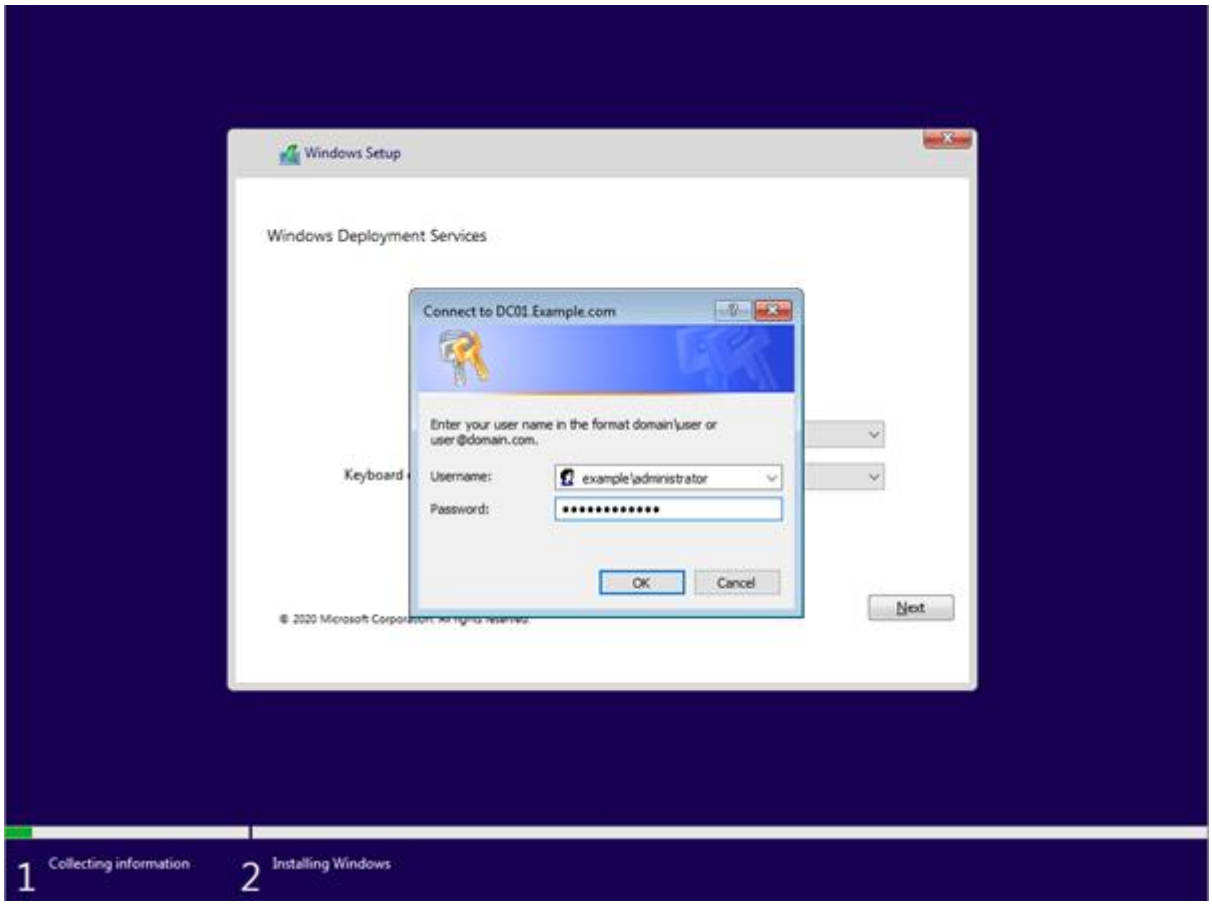
- I add an answer file

Deploying the Image

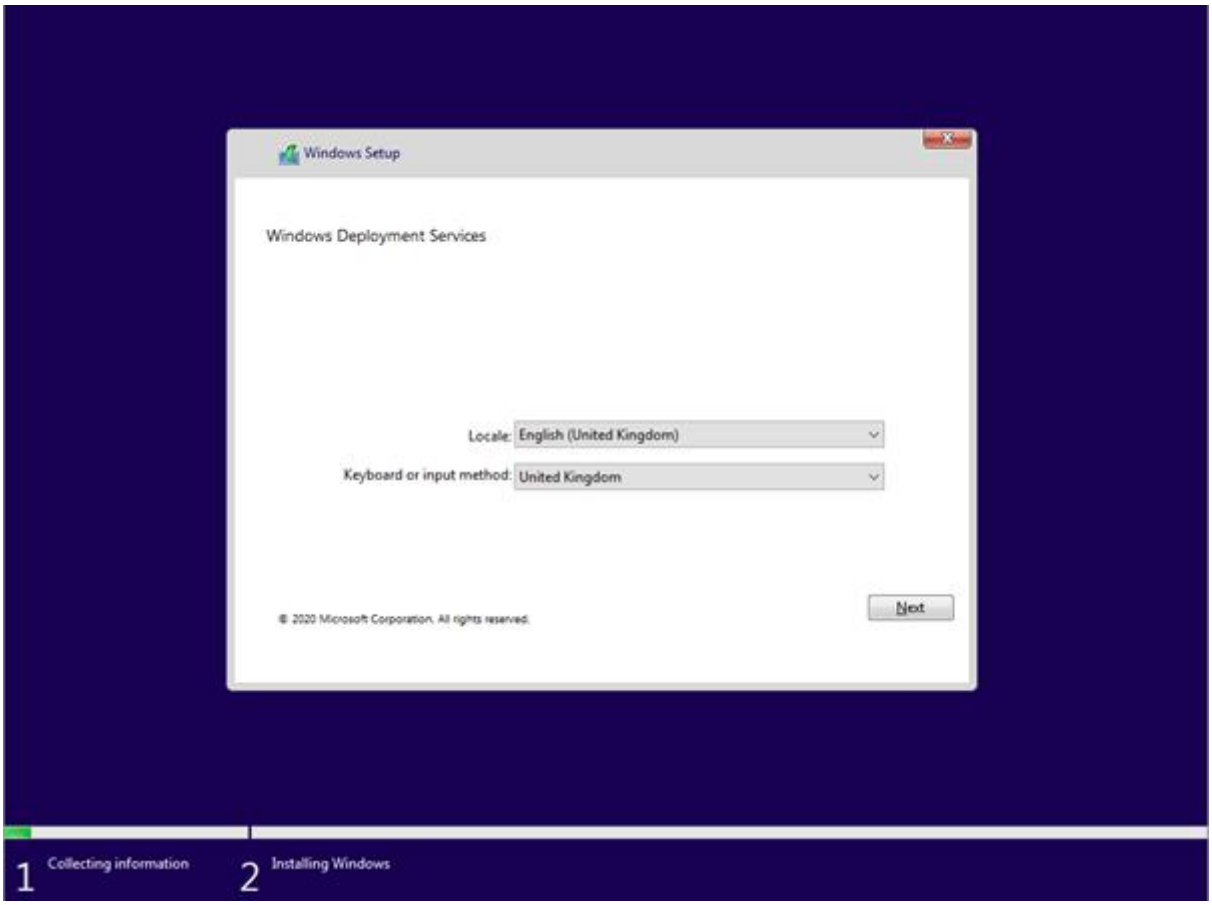
- the deployment has run correctly and is installed on the target computer



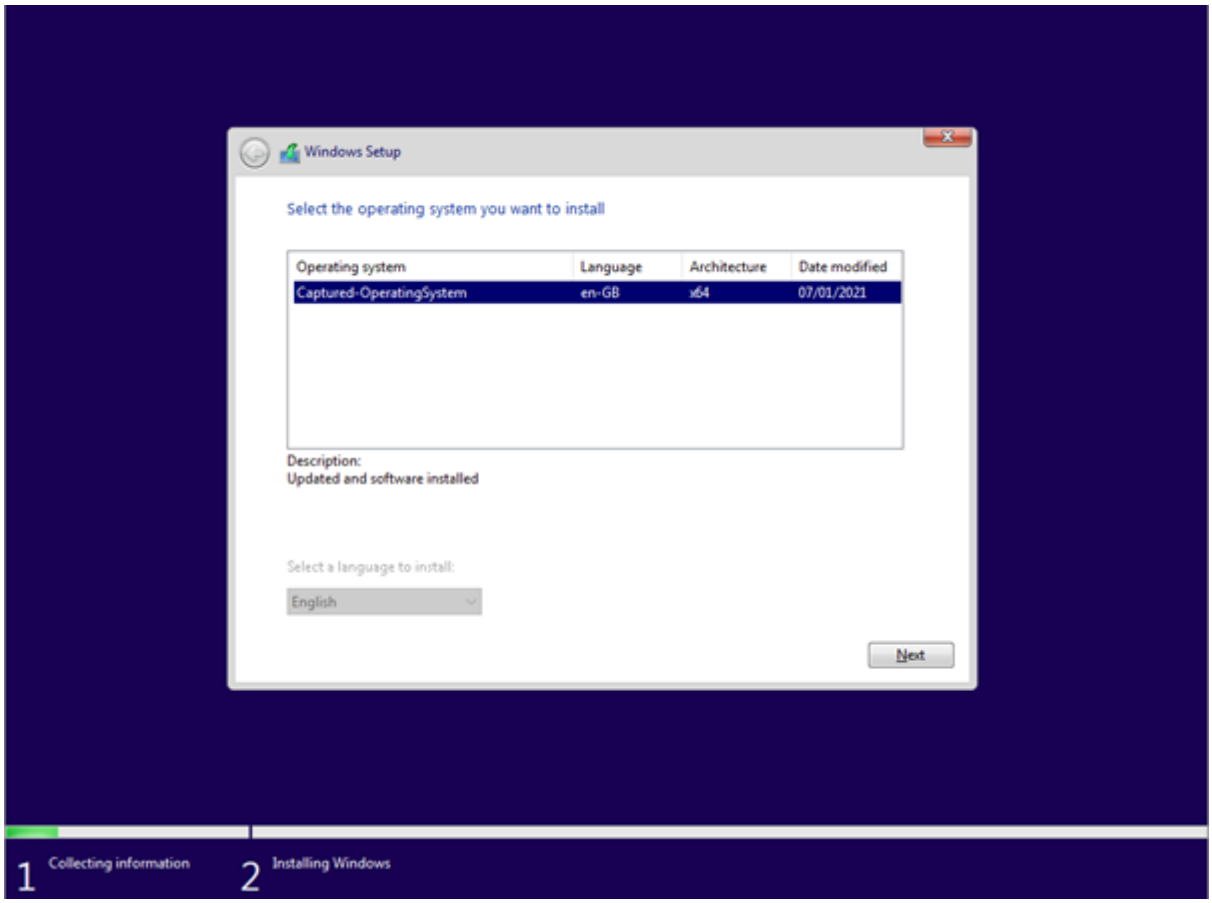
- now I boot the target machine using PXE



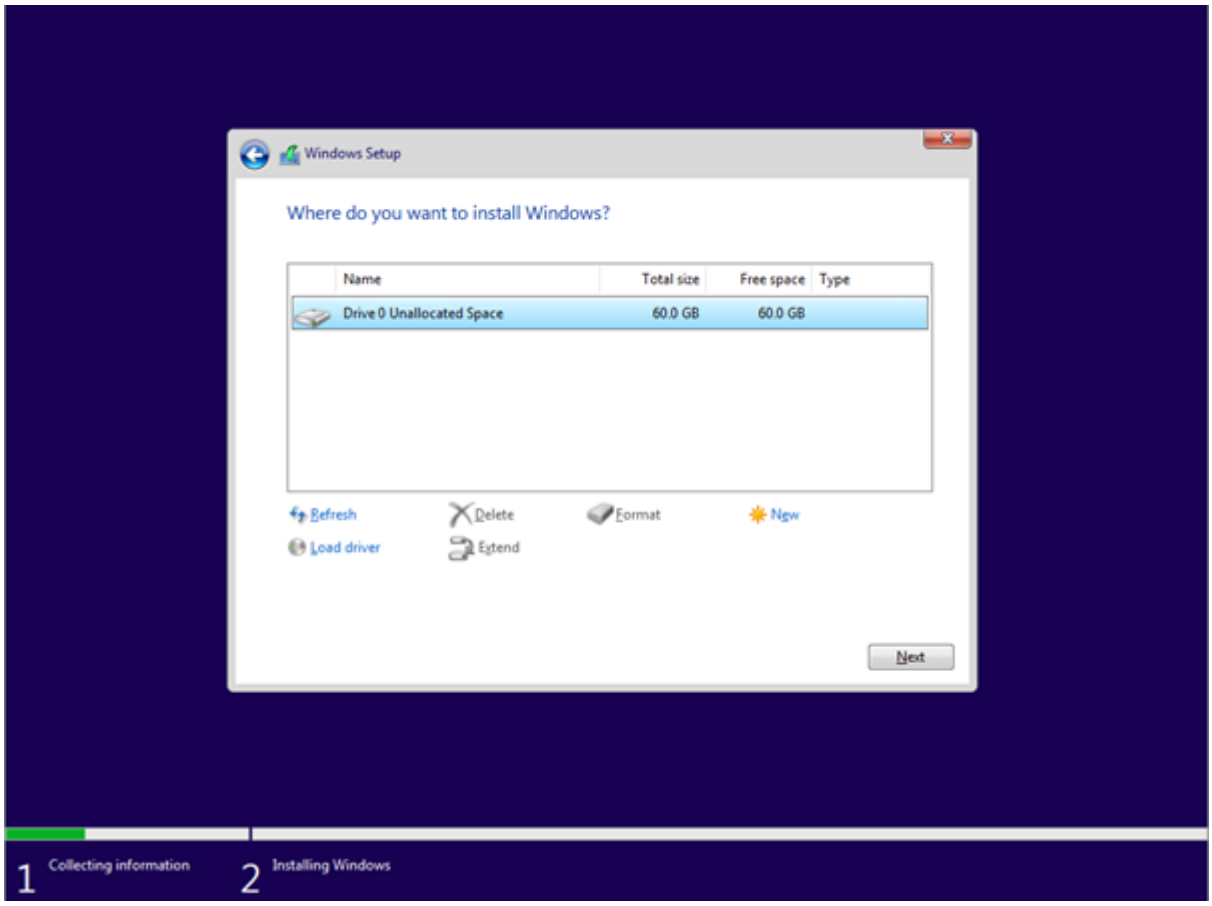
- I pre-add the domain account details so I do not need to manually add the machine after installation. This is an advantage of using an image



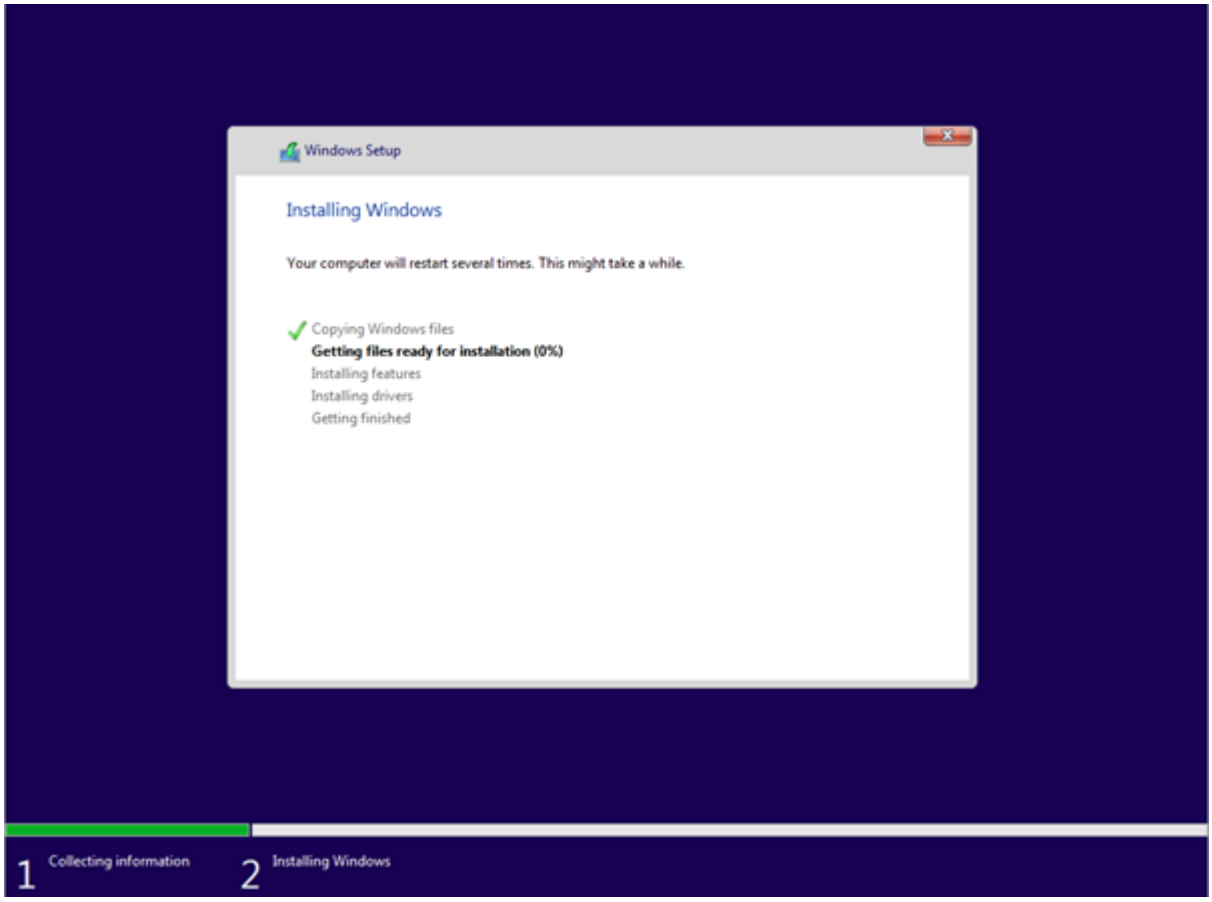
- I set languages (this could be done with an answer file if a large deployment was to be done)



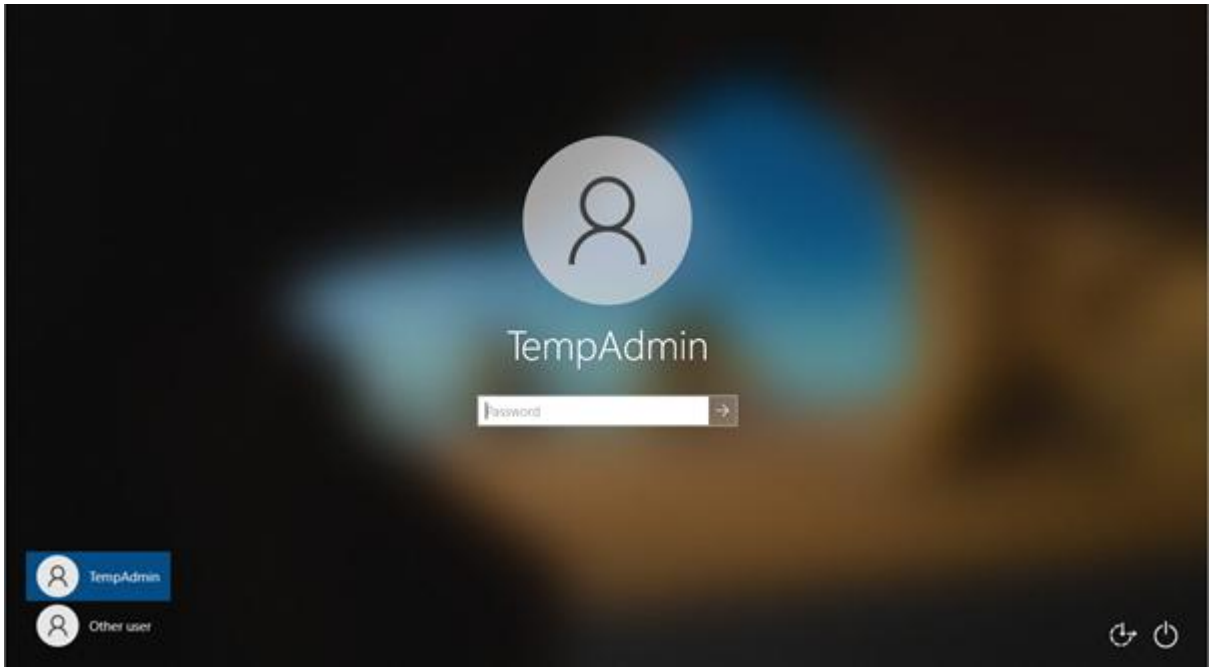
- I choose the image



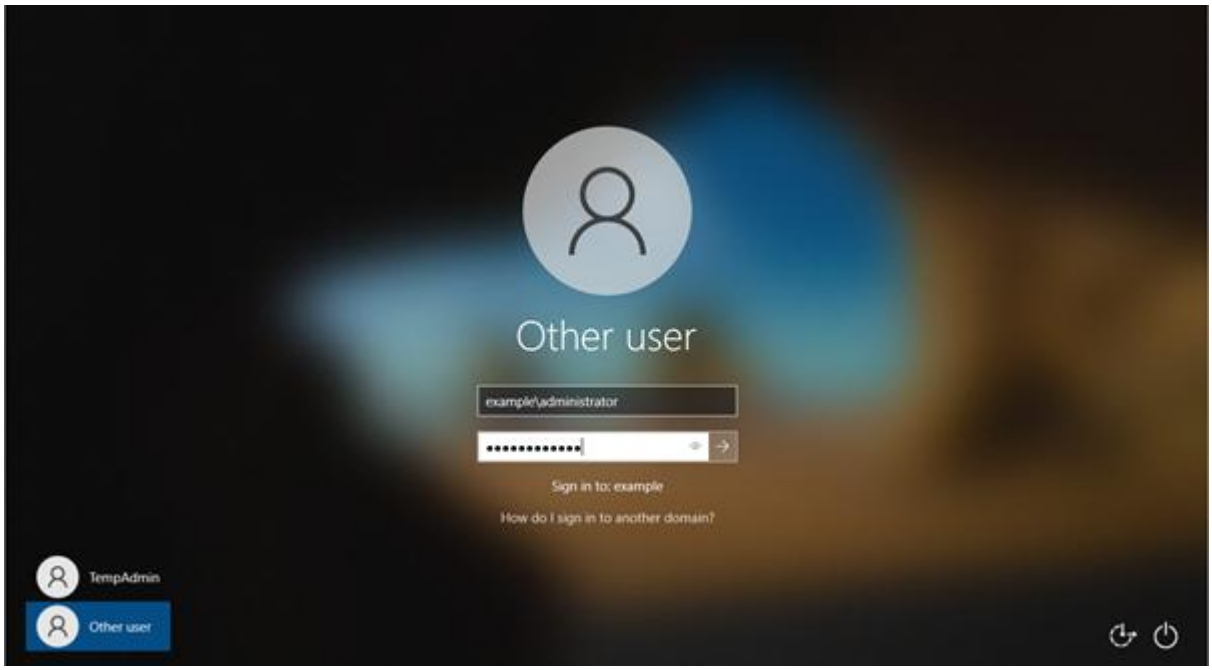
- this is the disk to image



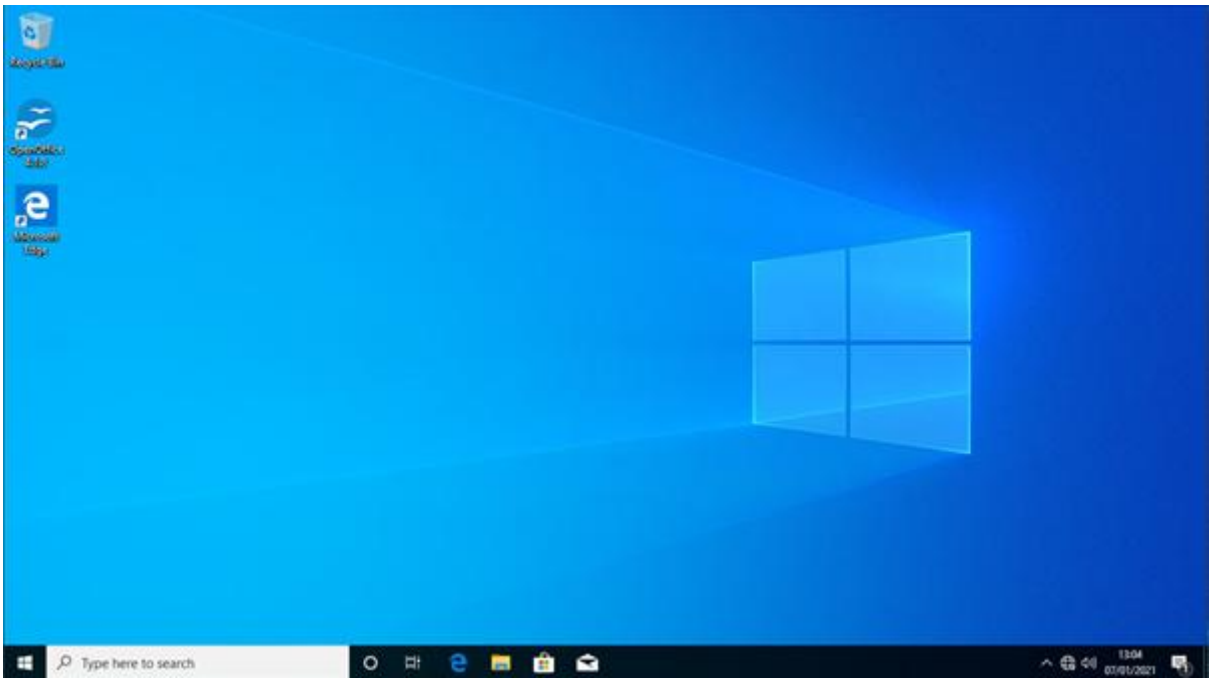
- I wait while Windows installs



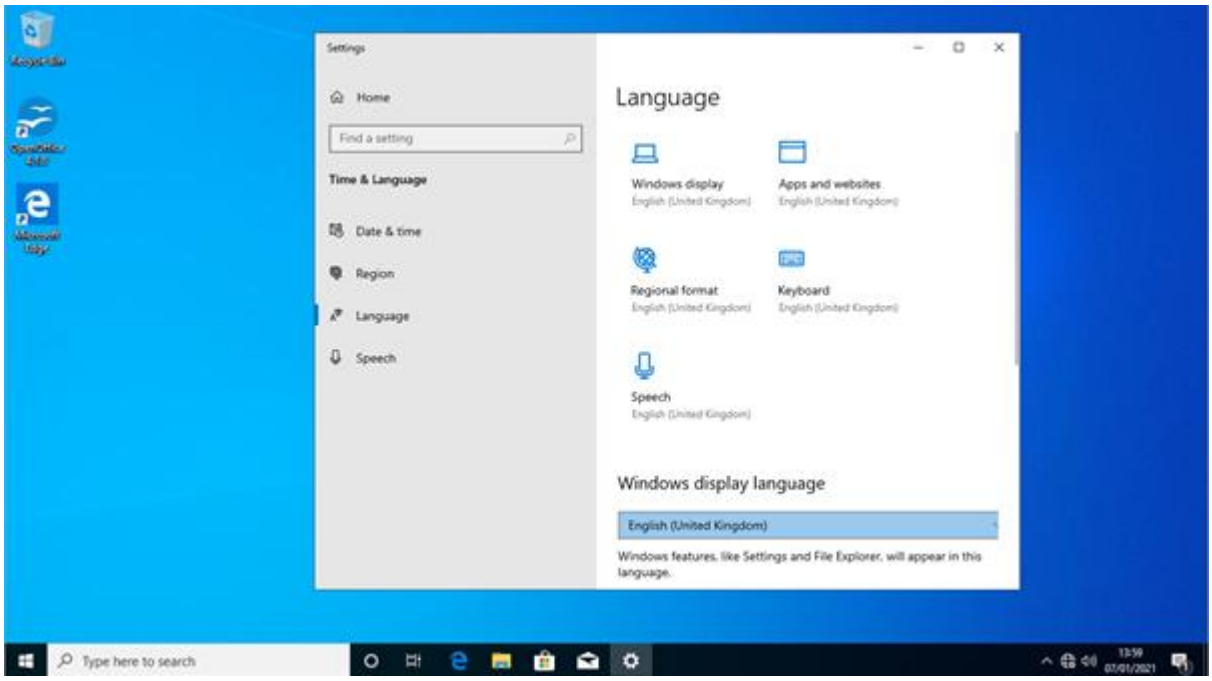
- I change to the other user



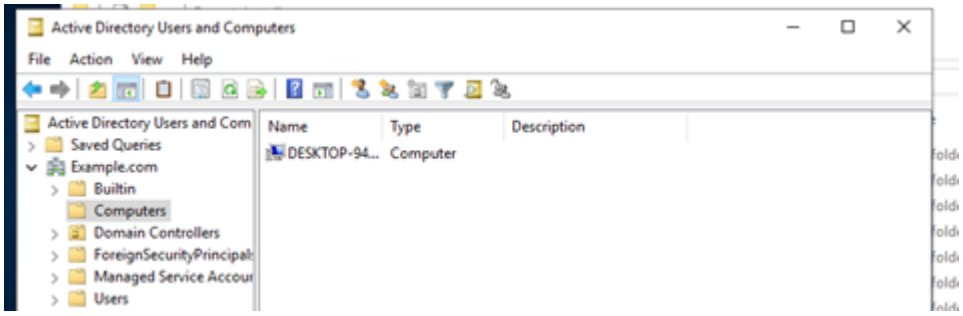
- I can log in



- here is the deployed Windows showing OpenOffice

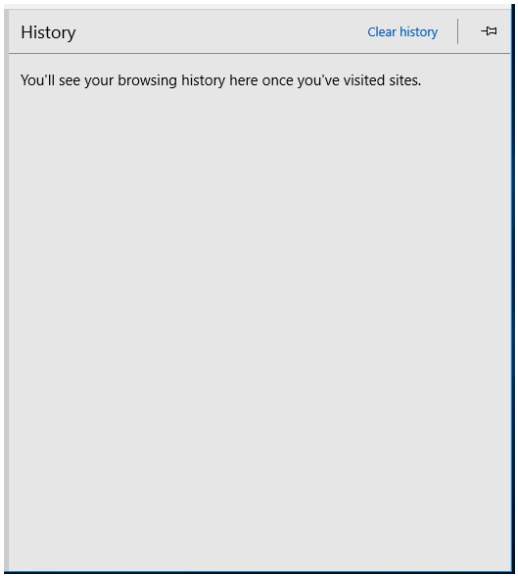


- language is also already set to UK so it does not have to be reset



- when I check active directory, I can see that the computer is joined

Browser History



Examiner commentary

The student has achieved the grade for the following reasons:

- the student has demonstrated excellent understanding of the penetration test report and has accurately completed the penetration test risk assessment template
- the student has made good recommendations to resolve all the vulnerabilities identified
- the student has given a well thought out report that recommends detailed actions for future improvements with detailed explanations why
- they have been able to fully complete the deployment exercise, with all aspects including automatically joining the domain satisfied
- they have provided a detailed commentary of their work, demonstrating complex understanding of the deployment process
- the student uses complex language and terminology that shows they have a high level of understanding of the subject area
- the student is showing an effective demonstration of the skills and techniques required to achieve this task – they are doing this 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, 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/seeks 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 and is 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/seeks clarification and guidance.
	Able to successfully tackle routine problems and make some progress on solving non-routine problems in real life situations.
	Demonstrates most skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across different contexts.
	Able to make some progress on unstructured problems that have not been seen before, using their knowledge to find solutions to problems.
	Makes some justification for strategies for solving problems, giving explanations for their reasoning.

* ‘Threshold competence’ refers to a level of competence that:

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

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