Windows Administration

Installing and Upgrading Windows

	Windows 10	Windows 11 (64bit only)
Processor	Min 1 GHz	1 GHz or faster (2 or more cores)
RAM	1 GB (32-Bit) 2 GB (64-Bit)	4 GB
HDD	16 GB (32-Bit) 32 GB (64-Bit)	64 GB
Graphics Card	Min DirectX 9 with WDDM 1.0	DirectX 12 with WDDM 2.0

- To obtain System Information:
  - Windows key + R, type **msinfo32**

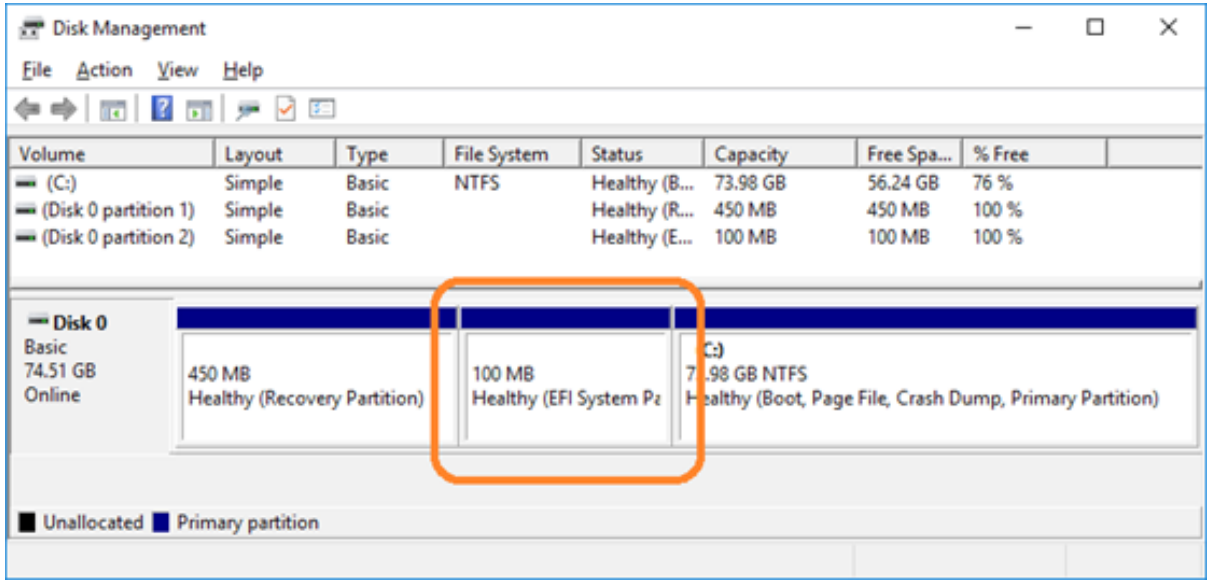
Windows Installation Options

- Can upgrade or clean install
  - Recommend Clean Install
  - If not formatting HDD then old OS is stored in WINDOWS.OLD
- You need to have carried out the installation process
- To install from USB, use the Win10Media Creation Tool
  - https://www.microsoft.com/en-gb/software-download/windows10
  - XP last version to support CD-Rom installation media (now DVD)

- Can install without a product key.
  - Key required for personal customisation
  - No key will run in RFM (reduced Functionality Mode)

Installing Windows 10

- Can install on a system with
  - BIOS – Basic Input Output System
  - UEFI – Unified Extensible Firmware Interface
    - Secure boot (Checks hardware/driver signatures)
- Default Windows10 disk layout (UEFI)
  - EFI System Partition (ESP)
    - Holds Boot Configuration Data (BCD)
- Win 11
  - UEFI only



Windows Installation

- Upgrade
  - System must be compatible
  - Updating to WIN11
    - Old OS in WINDOWS.OLD
    - 30 days to roll back to the prior OS
  - Apply all previous Windows 10 updates first
  - Cannot go from 32bit to 64bit as an upgrade

- Install over the network
  - Windows Preinstallation Environment (WinPE)
    - Creates a Pre-boot Execution Environment (PXE)

Windows Installation

- Select the drive install location
  - Point of no return
  - Partition is initialised
  - Files are copied to Hard Drive
  - Reboot
  - Generalize pass
    - Hardware detected and drivers installed.
  - Reboot
  - Specialised Pass
    - Locale
    - Keyboard

Windows Installation

- Win11 – Name device during installation
- Win10 – Name was created
- Reboot
- OOBE – Out of Box Experience
  - Login setup
  - Telemetry Options
    - Privacy settings
      - Location, Find My Device, Diagnostic Data

Repair Installation

- Reinstall Windows without loosing personal data files
- Windows detects a previous installation
- Asks if you want to keep the personal files and apps

Migrating User Data

- User State Migration Tool
  - If not using OneDrive
  - user accounts
  - user files
  - operating system settings
  - application settings
  - A 2 minute read about the tool: https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-overview
  - Can migrate to a network location or Hard drive
  - Not part of 1102, but useful to know about

Upgrading Editions of Windows

- You can upgrade to a higher version of Windows 10 by entering a correct activation key
- Click Start and type Activation → Change Product key
- Downgrading retail versions not permissible
- You can downgrade from Volume License editions
  - Education to Pro
  - Not formally supported by MicroSoft

Windows Security and Feature Updates

- Versions change twice a year (semi-annually)
  - Downloaded as updates
  - Originally, versions were identified by a date code
    - Last two digits of the year and the two digit month
    - E.g. Original version of Win10 was 1507
  - Now H1 for first half of the year and H2 for second half of the year
    - E.g. 21H2
    - Normally Spring and Autumn
  - Use winver.exe to discover a version

Windows Updates

- Windows 10 changed HOW updates were delivered
  - Now mandatory
  - Updates can be defer for up to 8 days
  - Updates can be paused for up to 35 days
- Three different branches of code (updates)
  - General Availability Channel
    - Default
  - Insider Program
    - Allows latest product releases before targeted release
    - Requires enrolment
  - Long-Term Servicing Channel
    - Enterprise Edition only
    - Monthly Updates
    - No new features

Windows Servicing Channel Options

Windows Edition	General Availability Channel	Insider Program	LTSC
Home	Yes	Yes	No
Pro	Yes	Yes	No
Enterprise	Yes	Yes	No
Enterprise LTSC	No	No	Yes
Education	Yes	Yes	No

Command-Line Tools

- MS-DOS not as friendly as Windows
- Command Prompt is designed to look like an MS-DOS prompt
- cmd.exe
  - Standard and Admin modes
- Expected to know these:
  - cd, dir, md, rmdir, ipconfig, ping, hostname, netstat, nslookup, chkdsk, net user, net use, tracert, format, xcopy, copy, robocopy, gpupdate, gpresult, shutdown, sfc, diskpart, pathping, winver, and [command name] /?

dir

- Displays a list of folders and subdirectories within a directory.

- Exercise
  - Open a command prompt
  - Type dir /?

  - Record in working records what the following switches do:
  - /a
  - /o
  - /l
  - /s
  - /t
  - /p
  - /q

cd (chdir) / md (mkdir) / rd (rmdir)

- From a command prompt read and understand:

  help cd (or cd /?)

  help md (or md /?)

  help rd (or rd /?)

- Exercise
  1. Open a command Prompt
  2. Change Directory to your documents folder
  3. Make a directory called test
  4. Change to the test directory
  5. Make a directory called test1
  6. Change to the test1 directory
  7. Make a directory called test2
  8. Change back to the documents directory
  9. Remove the directory test directory
  10. Remove the directory test directory using /s
  11. Repeat steps 3 to 8
  12. Remove the directory test directory using /q

ipconfig

- Vital command
- Covered in 1101

- ipconfig /all
  - Displays all the interface details available
- ipconfig /release
  - Releases the current IP address from the DHCP lease
- ipconfig /renew
  - Renews an IP address lease from the DHCP server
- ipconfig /displaydns
  - Allows you to view the local dns cache
- ipconfig /flushdns
  - Clears the local dns cache. Useful when a DNS entry has changed

IPCONFIG (IFCONFIG)

- Displays network settings
- First tool to use when having issues

Switch	Function
/ALL	Displays all parameters.
/RELEASE	Releases the IP address if using DHCP
/RELEASE6	Releases the IPv6 address if using DHCP
/RENEW	Get new IP address from DHCP server
/RENEW6	Get new IPv6 address from DHCP server
/FLUSHDNS	Flushes the DNS server name resolver cache

PING

- Send Packets to another device
- Uses ICMP (Internet Control Messaging Protocol)
- Verifies network connectivity
- Gives indication of time
- ping <hostname> OR ping <ip address>

Option	Function
-t	Persistent ping. Use CTRL+C to stop. Default in Linux.
-n count	Specifies the number of requests to send
-l size	Specifies packet size
ping -4	Use IPv4
ping -6	Use IPv6

TRACERT

- Trace Root
- Shows the differing IP addresses a packet took to its destination
- Try tracert 8.8.8.8

PATHPING

- Combines tracert and ping into one command
- Helps to diagnose packet loss to a destinations website
- Try pathping 75.75.75.75

NETSTAT

- Used to check inbound and outbound connections

Option	Function
-a	Displays all connections and listening ports
-b	Display the executable creating each connection. Takes time and requires permissions
-e	Display Ethernet statistics (can use with –s option for more information)
-f	Display fully qualified domain names (FQDN) for remote addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID for each connection
-p proto	Shows connections for the protocol specified. TCP, UDP, TCPv6, UDPv6 -s options IP, IPv6, ICMP,ICMPv6,TCP,TCPv6,UDP, UDPv6
-r	Displays routing table
-s	Displays per protocol statistics

NSLOOKUP

- TCP/IP needs hostname resolution to IP addresses
- Two modes
    1. Interactive
    2. Noninteractive
- Allows verification of entries on DNS servers
- Interactive mode – type NSLOOKUP at command prompt
    - > prompt. Type HELP or ? Use EXIT to quit.
- NonInteractive mode
    - NSLOOKUP /SET TIMEOUT=<3>
    - NSLOOKUP /VIEW:*DOMAIN*

Hostname

- Tells you the hostname of the computer that the command prompt is open on.
- Useful for administrators who access several different computers

Other Network Tools

- GPUPDATE - Group Policy update for Group Policy Settings
  - Active Directory updates policies every 90 minutes
    - Background refresh cycle
  - Refreshes or changes local and AD based policies
  - Can force with the /force switch
- GPRESULT – shows the Resultant Set of Policy (RSoP) for a remote user/computer
  - For deciding which set of configuration policies take precedence
- Net
  - Net Use
    - Allows administrators to map drives
    - net use z: \\server\share
  - net user
    - Allows administrators to list all the local accounts
    - Creating users
    - net user newUser Pa55w0rd /add

NET

- All windows have a NET command
- Allows command line access to the network
- Many switches – see https://www.lifewire.com/net-command-2618094
- NET SHARE allows creation of shares at command line
  - NET SHARE <share_name>=<drive_letter>:path
  - Own subset of parameters
    - /DELETE – Stop sharing a folder
    - /REMARK – Adds a comment for browsers
    - /UNLIMITED – Set the user limit to Maximum allowed
    - /USERS – Set a specific user limited

More Commands

- FORMAT
  - Wipes data from a disk
  - FORMAT [volume] [switches]
    - /FS:[filesystem] – FAT, FAT32 or NTFS
    - /V:[label] – Specifies the volume label
    - /Q – Quick Format
- Copy
  - COPY [filename] [destination]
    - /A – ASCII text file
    - /V – verifies the copy
    - /Y – supresses the are you sure overwrite prompt
  - Not for directory copying

Copying Files and Directories

- XCOPY
  - Copies folders and files
  - XCOPY [source] [destination] [switches]
    - /A – only files with archive attribute
    - /E – include empty directories
    - /F – display full filenames when copying
    - /G – copy encrypted file to destination that doesn’t support encryption
    - /H – copy hidden and system files
    - /K – Copies attributes (XCOPY will reset Read-Only by default)
    - /O – Copies ownership and ACL info (important as NTFS default in inheritance from parent)
    - /R – Overwrites read-only files
    - /S – Copy directories and Subdirectories (not empty ones)
    - /U – Copies only files that already exist in the destination
    - /V – Verifies the size of each new file

ROBOCOPY

- Robust File Copy
- Very useful for NTFS
- For example the /mir switch mirrors a complete directory tree
- See https://technet.microsoft.com/en-us/library/ee851678.aspx

Quick Commands

- DISKPART (requires admin privileges as a user)
  - Shows and allows partition management
- SFC – System File Checker (again admin privileges required)
  - Switches:
    - /SCANFILE – Scans file for problems and fixes them
    - /SCANNOW – Immediately scans all protected system files
    - /VERIFYONLY – Scans protected system files but not change them
    - /VERIFYFILE – Identifies the integrity of the specified file and will repair if needed
    - /OFFBOOTDIR – Repairs an offline boot directory
    - /OFFWINDIR – Repairs an offline windows directory
  - Will overwrite file if issue is found from C:\Windows\WinSxS (protected dir)
  - Most system files are in C:\Windows\System32

More Commands

- chkdsk
  - Create and display status reports for HDD
- Shutdown
  - Allows scheduled shutdown of a local or remote PC
  - /s - Shutdown the computer
  - /r - Shutdown and restart
  - /g - Shutdown and restart. After reboot, restart any registered applications.
  - /a - Abort a system shutdown
  - /h - Hibernate the computer
  - /o – Go to the advanced boot options menu. Must be used with /r
  - /m \\computer – Shutdown the remote computer specified
  - /t xxx – Set the timeout period before shutdown to xxx seconds

More commands

- SFC – System File Checker (again admin privileges required)
  - Switches:
    - /SCANFILE – Scans file for problems and fixes them
    - /SCANNOW – Immediately scans all protected system files
    - /VERIFYONLY – Scans protected system files but not change them
    - /VERIFYFILE – Identifies the integrity of the specified file and will repair if needed
    - /OFFBOOTDIR – Repairs an offline boot directory
    - /OFFWINDIR – Repairs an offline windows directory
  - Will overwrite file if issue is found from C:\Windows\WinSxS (protected dir)
  - Most system files are in C:\Windows\System32
- Help and /?

Networking in Windows

- HomeGroup
  - Introduced in Win7
  - Allowed sharing of files and printers with a single password
  - Password required to join
  - Removed since Win10 (1803) update
- WorkGroup
  - Existed since windows was first released
  - Limited to 20 simultaneous clients
  - loose associations
  - Ideal for 10 or less workstations
- Domains
  - Creates a trust between a client and authentication server
  - Allows files and printers to be secured with domain credentials
  - Very scaleable

User Authentication

- SAM – Security Account Manager
  - Local database of all users
  - Grants local access tokens for use with local resources
- Domain
  - Authenticates against an Active Directory
  - Provides a GUID
  - Local logins normally just administrators once Domain has been joined
- SSO – Single Sign On
  - Access to multiple systems with a single login
  - https://blog.miniorange.com/what-is-single-sign-on-sso/

Windows Network Connection

- Make sure you have connected Windows to a network so that you know how to do it.
  - Both Static and Auto

- VPN – Virtual Private Network
  - Provides a level of privacy
  - Allows encryption to an anonymous server for browsing
  - For 1102 – a secure connection between two endpoints
  - Need a network connection first

- WWAN – Wireless Wide Area Network
  - Cellular data providers