MODERN OPERATING SYSTEMS

LECTURE 2

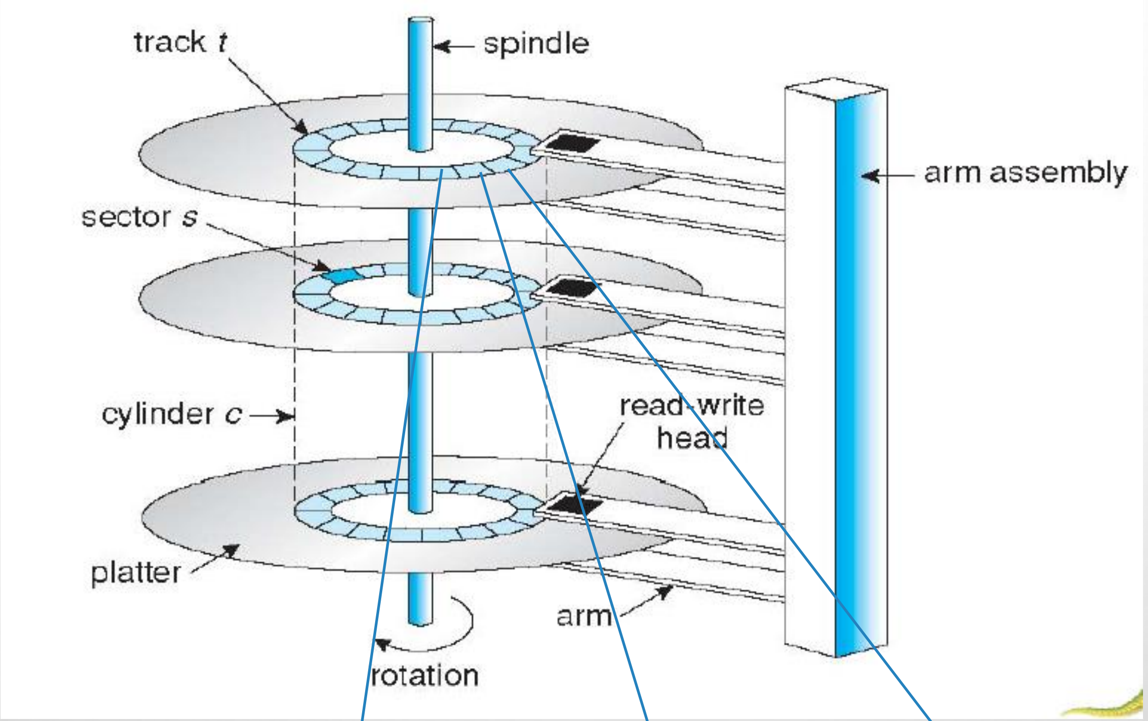
AGENDA

- WINDOWS BOOT PROCESS
- MMC – AS A SPECIFIC TOOL FOR MANAGEMENT UNIFICATION
- WINDOWS USERS AND GROUPS MANAGEMENT

LOGICAL VIEW ON DISK SYSTEM

- DISK DRIVES ARE ADDRESSED BY OS AS A 1-DIMENSIONAL ARRAYS OF **LOGICAL BLOCKS**
- THE 1-DIMENSIONAL ARRAY OF LOGICAL BLOCKS IS MAPPED INTO THE SECTORS OF THE DISK SEQUENTIALLY: LOGICAL BLOCK 0 IS MAPPED INTO THE FIRST SECTOR OF THE FIRST TRACK ON THE OUTERMOST CYLINDER
- MAPPING PROCEEDS IN ORDER THROUGH THAT TRACK (SECTOR BY SECTOR), THEN THROUGH THE REST TRACKS IN THAT CYLINDER, AND THEN THROUGH THE REST OF THE CYLINDERS FROM THE OUTERMOST TO THE INNERMOST TRACKS

DISK DRIVE SYSTEM

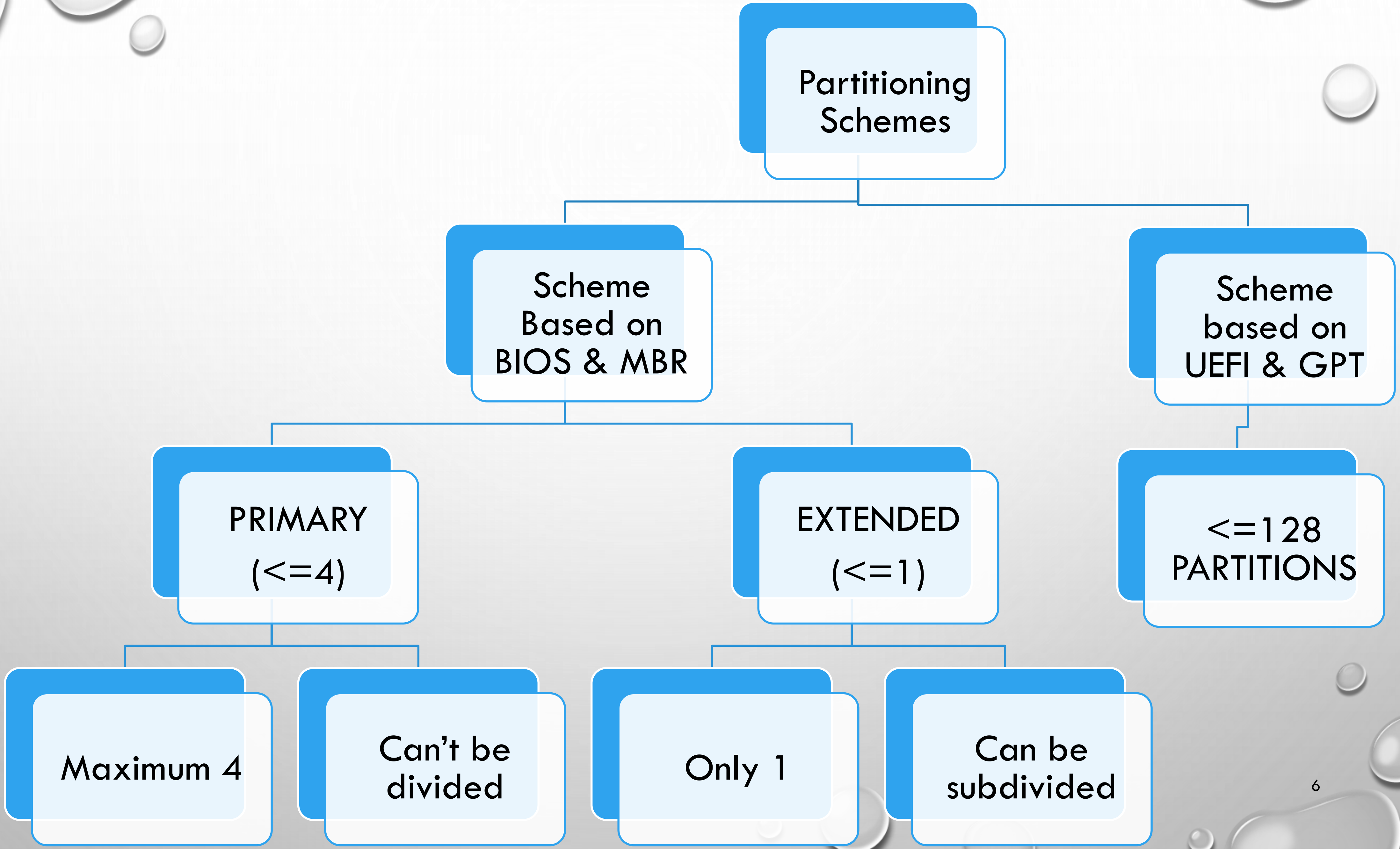


LBA	0	…	i	i+1	i+2	…	N

DISK PARTITION

- **DISK PARTITIONING** OR **DISK SLICING** IS THE CREATION OF ONE OR MORE REGIONS ON DISK, SO THAT EACH REGION CAN BE MANAGED SEPARATELY
- **DISK PARTITION** IS A SET OF CONSISTENTLY LOCATED SECTORS (LOCAL BLOCKS) WHERE A SINGLE OS (FILE SYSTEM) CAN BE INSTALLED
- DUE TO PARTITION EXISTENCE, ONE CAN HAVE SEVERAL OPERATING SYSTEMS

INSTALLED IN A SINGLE COMPUTER

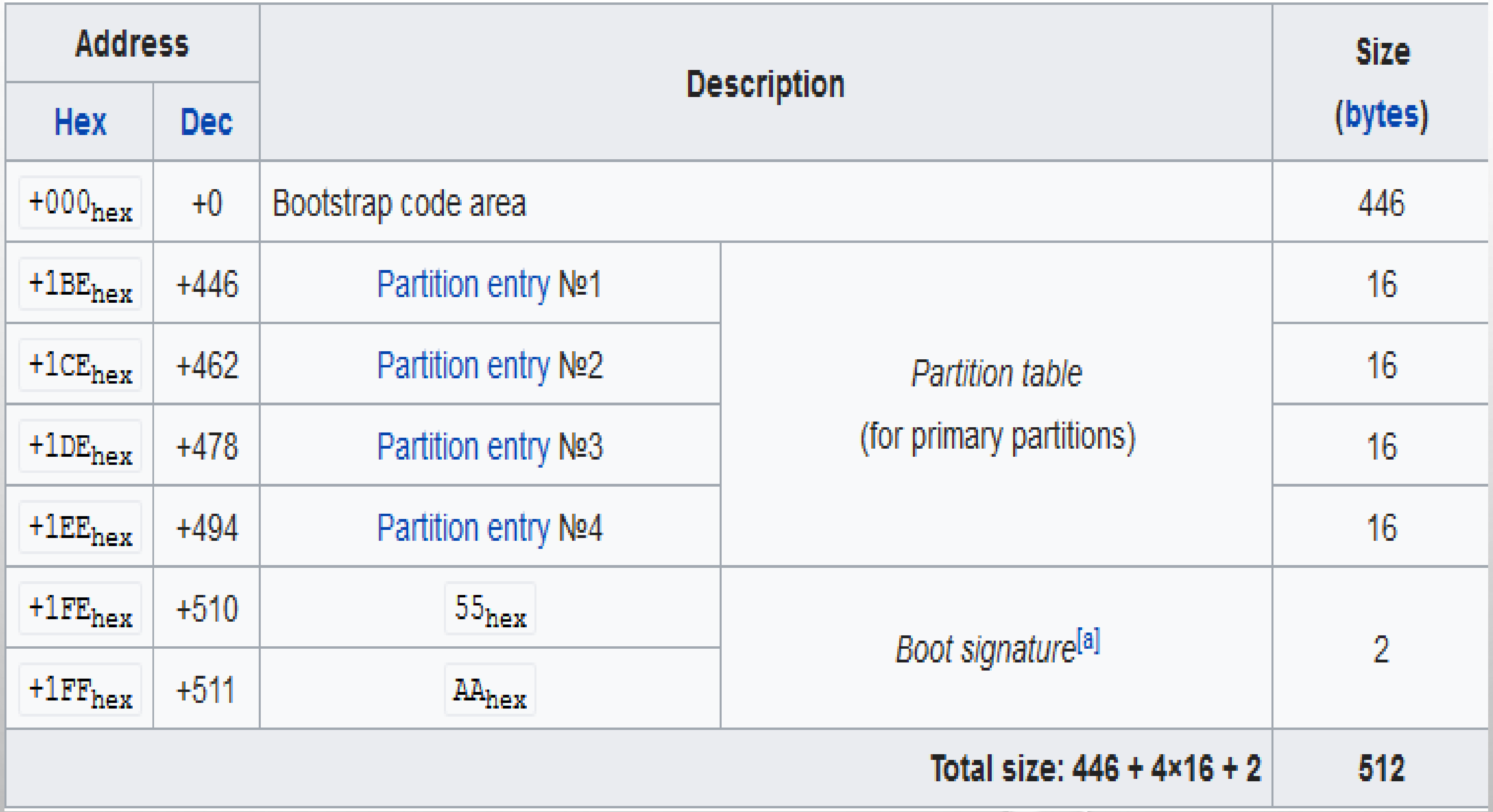


- Partitioning Schemes
  - Scheme Based on BIOS & MBR
    - PRIMARY (<=4)
      - Maximum 4
      - Can’t be divided
    - EXTENDED (<=1)
      - Only 1
      - Can be subdivided
  - Scheme based on UEFI & GPT
    - <=128 PARTITIONS

BIOS & MBR

- BIOS IS NON-VOLATILE FIRMWARE USED TO PERFORM HARDWARE TEST AND INITIALIZATION, AND TO LOAD A BOOT LOADER FROM A MASS MEMORY DEVICE WHICH THEN INITIALIZES AN OPERATING SYSTEM
- THE BIOS COMES PREINSTALLED ON A PERSONAL COMPUTER’S SYSTEM BOARD.
- MBR -> 1ST SECTOR OF THE DRIVE CONSISTS OF:
  - PARTITION TABLE
  - BOOTSTRAP CODE (INSTRUCTIONS TO IDENTIFY BOOTABLE PARTITION AND PASS THE CONTROL TO THE BOOT SECTOR OF THAT PARTITION)

MBR

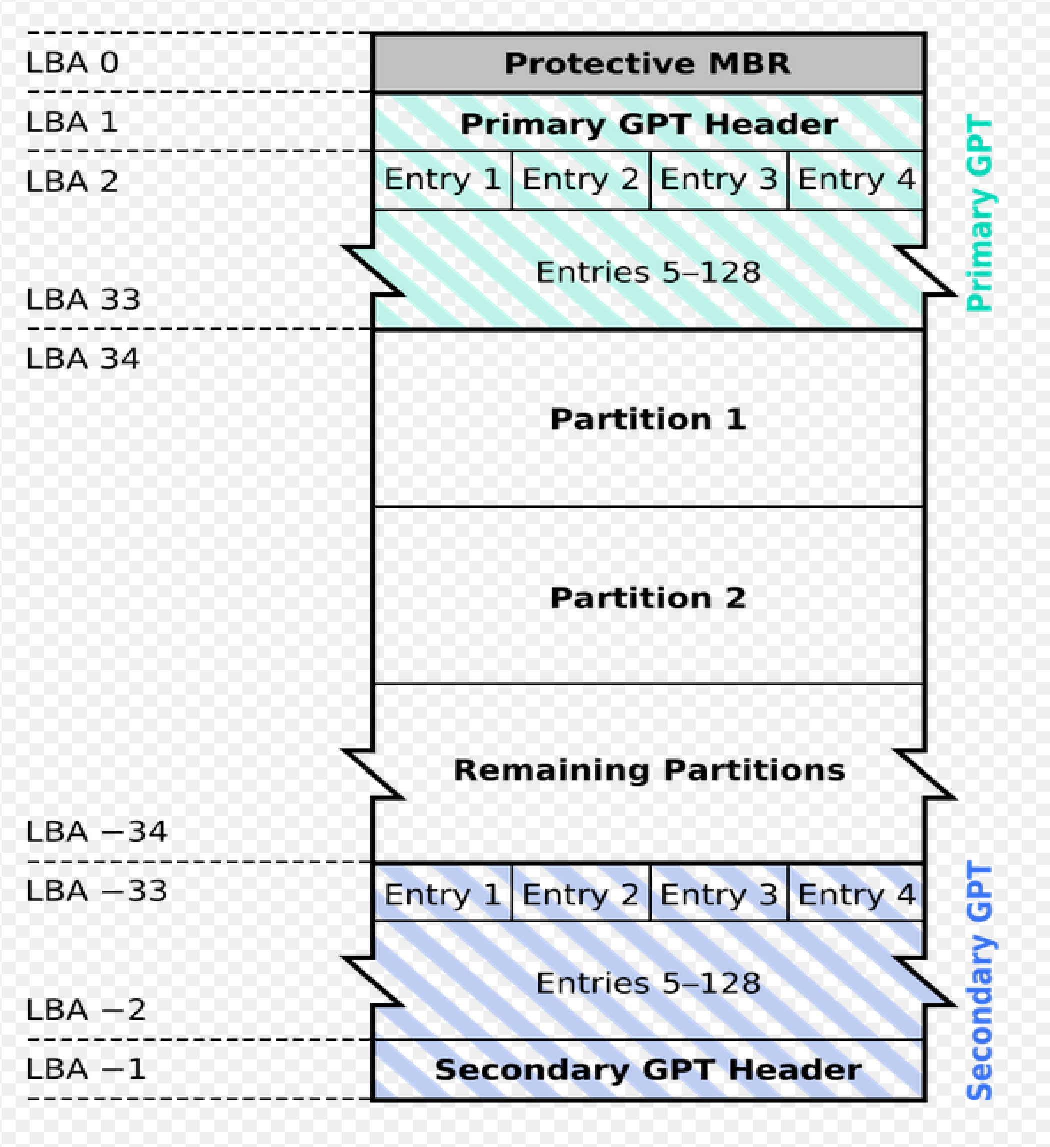


Address		Description		Size (bytes)
Hex	Dec			
$+000_{\text{hex}}$	+0	Bootstrap code area		446
$+1BE_{\text{hex}}$	+446	Partition entry №1	*Partition table* (for primary partitions)	16
$+1CE_{\text{hex}}$	+462	Partition entry №2		16
$+1DE_{\text{hex}}$	+478	Partition entry №3		16
$+1EE_{\text{hex}}$	+494	Partition entry №4		16
$+1FE_{\text{hex}}$	+510	55_{hex}	*Boot signature*[a]	2
$+1FF_{\text{hex}}$	+511	AA_{hex}		
			Total size: 446 + 4×16 + 2	**512**

UEFI & GPT

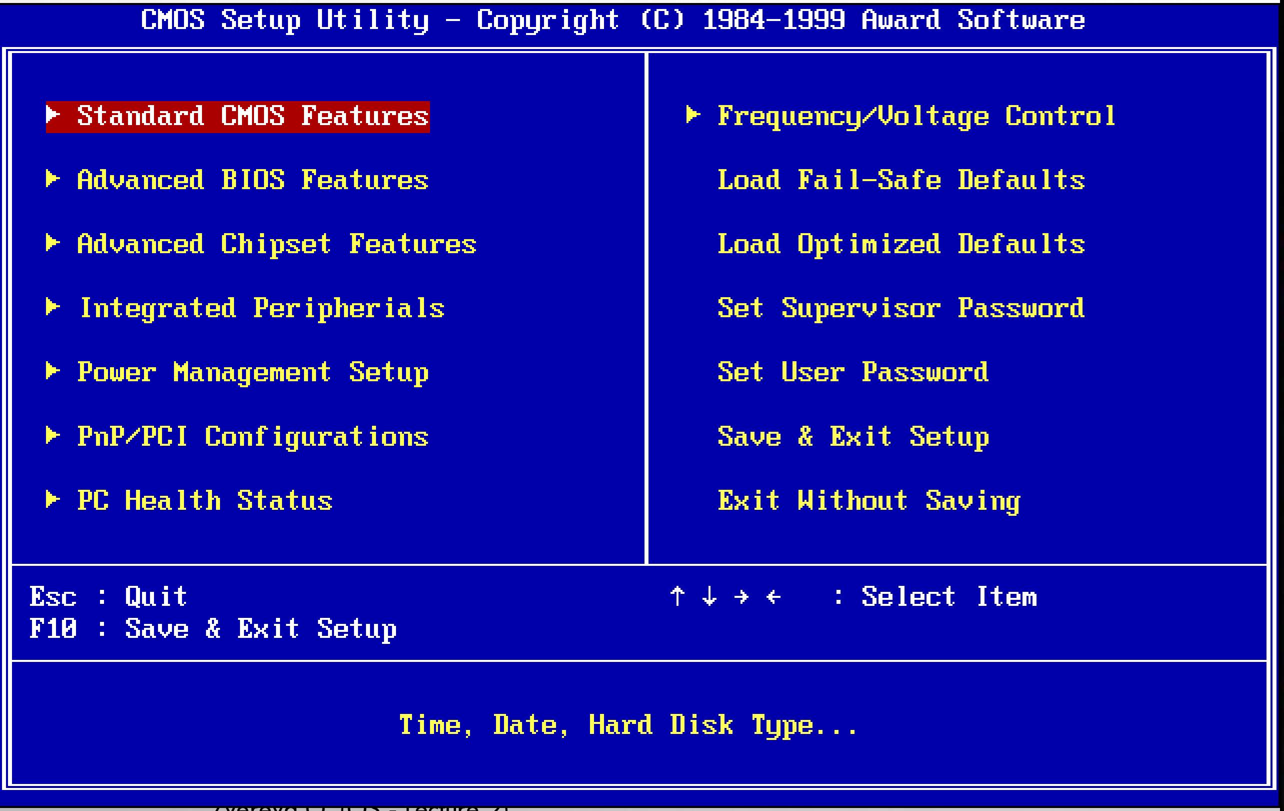
- UEFI – (UNIFIED EXTENSIBLE FIRMWARE INTERFACE) – NEW STANDARD
- UNIFIED EFI FORUM PROPOSED REPLACEMENT FOR THE PC BIOS (BECAUSE OF THE LIMITATIONS OF MBR PARTITION TABLES)
    - USES GPT – GUID PARTITION TABLE (GUID – GLOBALLY UNIQUE IDENTIFIERS)
    - USES 32 BITS FOR STORING LOGICAL BLOCK ADDRESSES (LBA)
    - HAS ITS OWN FILE SYSTEM, WITH FILES AND DRIVERS. THIS FILE SYSTEM IS TYPICALLY BETWEEN 200 AND 500MB AND FORMATTED AS FAT32.
    - IS A MINI-OPERATING SYSTEM.
    - LOADERS OF ALL OS PREINSTALLED IN THE COMPUTER ARE LOCATED IN THE SYSTEM UEFI PARTITION (THERE ARE VERSIONS OF GRUB, LILO AND BOOTMGR WITH UEFI SUPPORT)

GPT

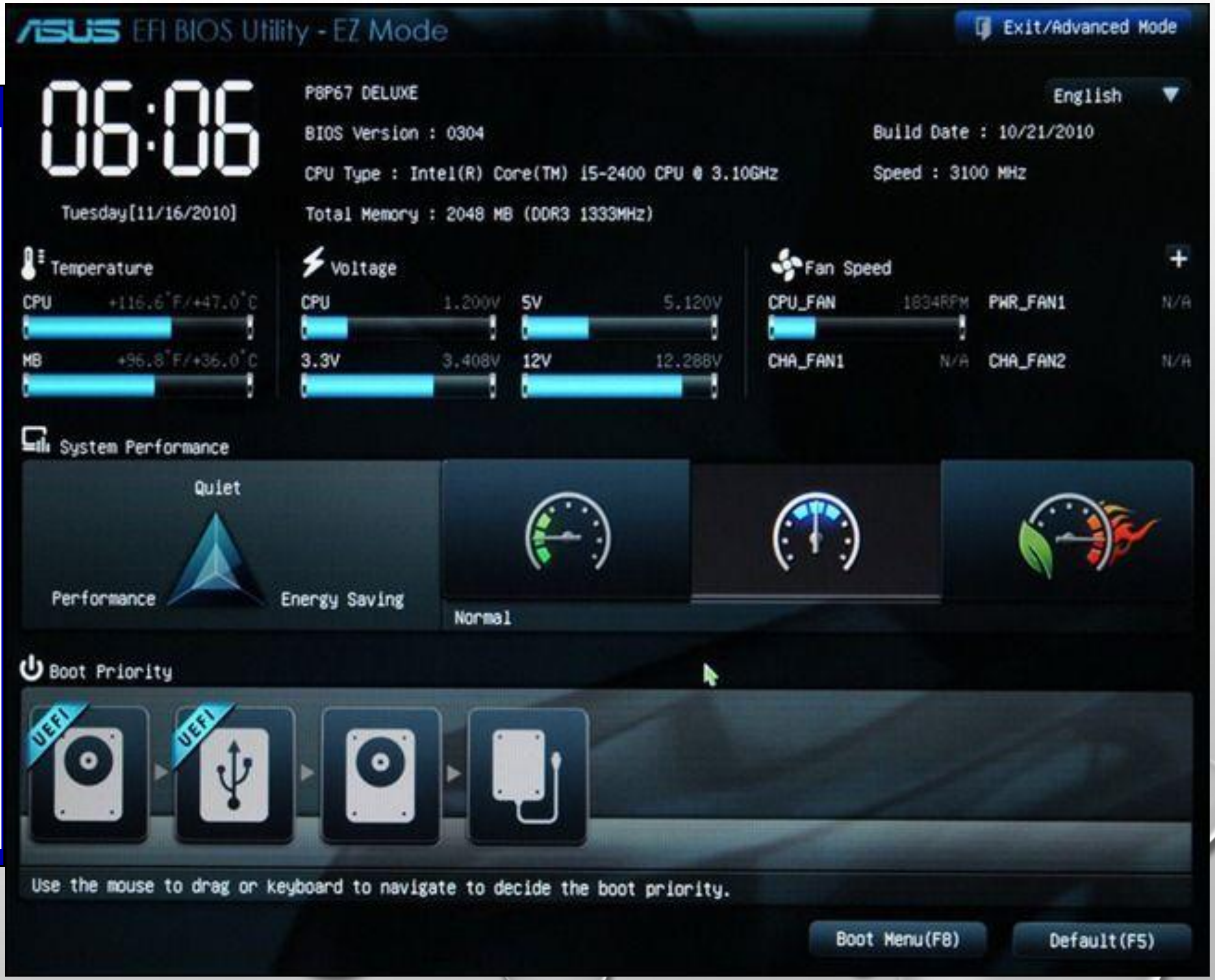


LBA 0
Protective MBR
LBA 1
Primary GPT Header
LBA 2
Entry 1
Entry 2
Entry 3
Entry 4
Entries 5–128
LBA 33
Primary GPT
LBA 34
Partition 1
Partition 2
Remaining Partitions
LBA −34
LBA −33
Entry 1
Entry 2
Entry 3
Entry 4
Entries 5–128
LBA −2
LBA −1
Secondary GPT Header
Secondary GPT

BIOS VS UEFI

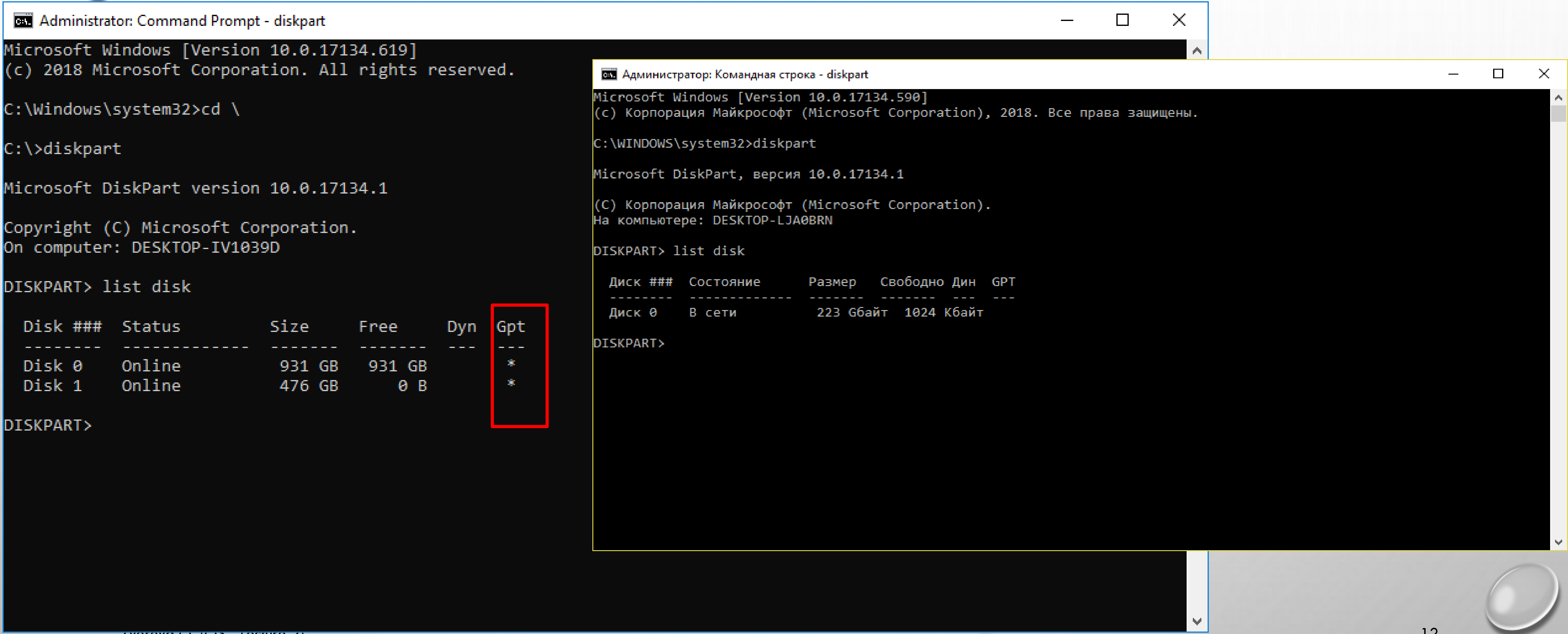


```
CMOS Setup Utility - Copyright (C) 1984-1999 Award Software

 ▶ Standard CMOS Features           ▶ Frequency/Voltage Control
 ▶ Advanced BIOS Features             Load Fail-Safe Defaults
 ▶ Advanced Chipset Features          Load Optimized Defaults
 ▶ Integrated Peripherials            Set Supervisor Password
 ▶ Power Management Setup             Set User Password
 ▶ PnP/PCI Configurations             Save & Exit Setup
 ▶ PC Health Status                   Exit Without Saving

Esc : Quit                          ↑ ↓ → ←   : Select Item
F10 : Save & Exit Setup

                 Time, Date, Hard Disk Type...
```



```
EFI BIOS Utility - EZ Mode                                Exit/Advanced Mode

06:06             P8P67 DELUXE                                       English
                  BIOS Version : 0304                    Build Date : 10/21/2010
                  CPU Type : Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz   Speed : 3100 MHz
Tuesday[11/16/2010]  Total Memory : 2048 MB (DDR3 1333MHz)

Temperature                   Voltage                           Fan Speed
CPU  +116.6°F/+47.0°C         CPU   1.200V   5V    5.120V       CPU_FAN  1834RPM  PWR_FAN1  N/A
MB   +96.8°F/+36.0°C          3.3V  3.408V   12V  12.288V       CHA_FAN1 N/A      CHA_FAN2  N/A

System Performance
        Quiet
Performance    Energy Saving     Normal

Boot Priority

Use the mouse to drag or keyboard to navigate to decide the boot priority.
                                                    Boot Menu(F8)   Default(F5)
```

DISKPART



Administrator: Command Prompt - diskpart

```
Microsoft Windows [Version 10.0.17134.619]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \

C:\>diskpart

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-IV1039D

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB   931 GB        *
  Disk 1    Online          476 GB      0 B        *

DISKPART>
```

Администратор: Командная строка - diskpart

```
Microsoft Windows [Version 10.0.17134.590]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart, версия 10.0.17134.1

(C) Корпорация Майкрософт (Microsoft Corporation).
На компьютере: DESKTOP-LJA0BRN

DISKPART> list disk

  Диск ###  Состояние      Размер   Свободно Дин  GPT
  --------  -------------  -------  -------  ---  ---
  Диск 0    В сети          223 Gбайт  1024 Кбайт

DISKPART>
```

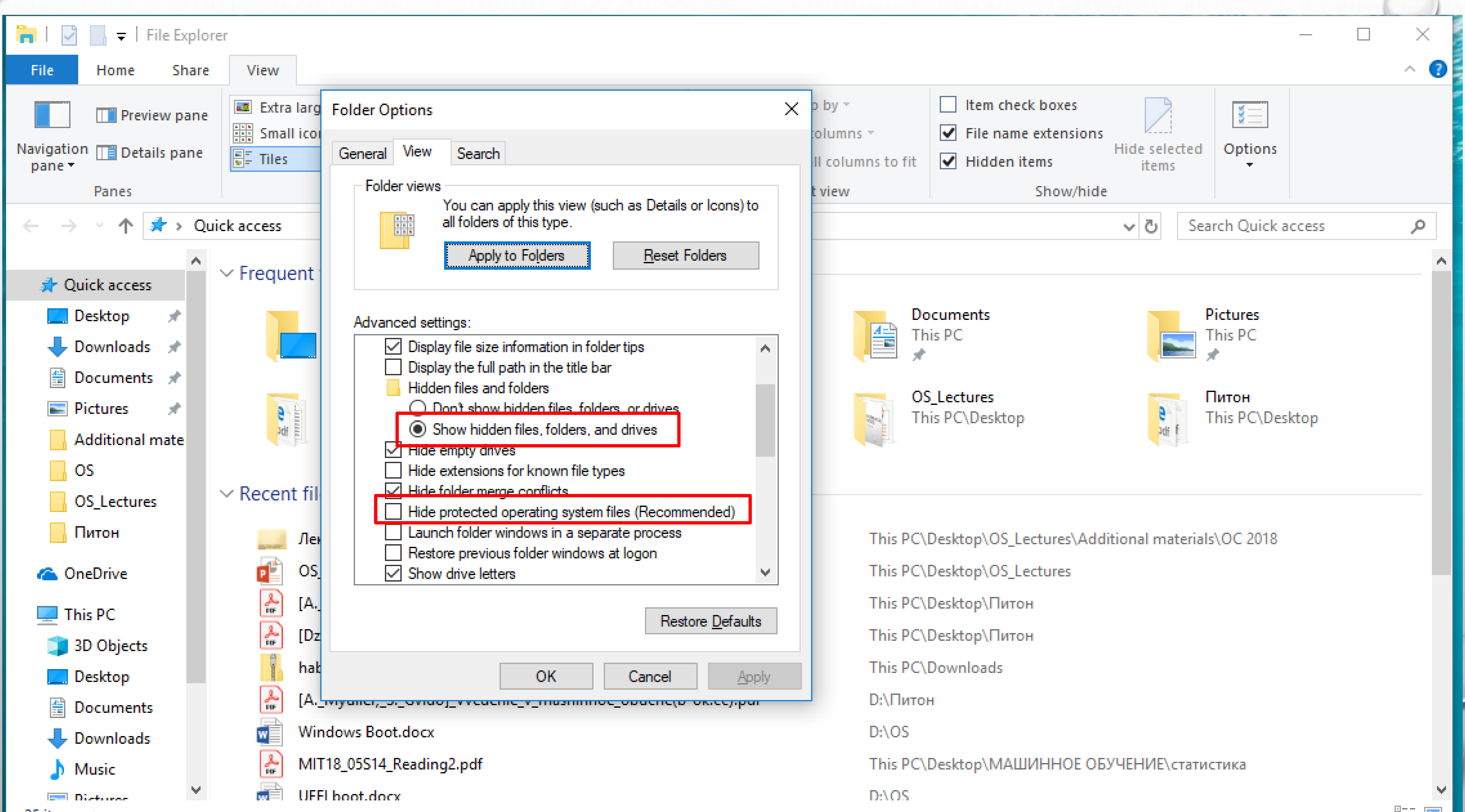
BASIC INPUT-OUTPUT SYSTEM (BIOS) VS UNIFIED EXTENSIBLE FIRMWARE INTERFACE (UEFI)

BIOS (MBR)	UEFI (GPT)
MBR – Master Boot Record (512 B)	GPT – GUID Table (200 and 500 MB is typically between and is formatted as fat32)
Restrictions on the partitions number (4 – overall, 1 – extended)	128 partitions
Maximum partition size – 2TB (2^{32} * 512B)	Maximum partition size 9.4* 10^{21}B
16 bit CPU mode	32(64)bit CPU Mode
No	Secure Boot

WINDOWS BOOT PROCESS: NECESSARY FILES

- **WINDOWS BOOT MANAGER (BOOTMGR)** –
  - FIRST INTRODUCED WINDOWS VISTA AND IS BEING USED IN ALL NEW OS (WINDOWS 7, WINDOWS 8, WINDOWS 8.1, AND WINDOWS 10, WINDOWS SERVER 2008 AND WINDOWS SERVER 2012).
  - IS READ-ONLY AND HIDDEN FILE AND IS LOCATED IN THE ROOT DIRECTORY OF THE PARTITION LABELED AS *SYSTEM RESERVED*.
  - PREVIOUS OPERATING SYSTEM LIKE XP WERE USING “NTLDR”
- **BOOT CONFIGURATION DATA (BCD) –** BCD IS A DATABASE OF STARTUP CONFIGURATION INFORMATION
  - PREVIOUS OPERATING SYSTEM LIKE XP WERE USING BOOT.INI FILE.
  - BOOT CONFIGURATION DATA ARE STORED IN A DATA FILE THAT HAS THE SAME FORMAT AS THE WINDOWS REGISTRY HIVES AND IS EVENTUALLY MOUNTED AT REGISTRY KEY (HKEY_LOCAL_MACHINE\BCD00000)
  - FOR UEFI BOOT, THE FILE IS LOCATED AT **\EFI\MICROSOFT\BOOT\BCD** ON THE EFI SYSTEM PARTITION. FOR TRADITIONAL BIOS BOOT, THE FILE IS AT **\BOOT\BCD** ON THE ACTIVE PARTITION
  - BCD CANNOT BE OPENED AND EDITED BY HAND. SPECIFICALLY DESIGNED COMMAND-LINE TOOLS LIKE BCDEDIT.EXE AND MORE USER-FRIENDLY GUI UTILITIES SUCH AS EASYBCD (CODED BY NEOSMART TECHNOLOGIES, MAY BE USED WITH DIFFERENT OS) MUST BE USED TO READ AND MODIFY THE LIST OF OPERATING SYSTEMS.

TO SHOW ALL HIDDEN AND SYSTEM FILES



Folder Options

General | View | Search

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Apply to Folders | Reset Folders

Advanced settings:

☑ Display file size information in folder tips
☐ Display the full path in the title bar
Hidden files and folders
○ Don't show hidden files, folders, or drives
● Show hidden files, folders, and drives
☑ Hide empty drives
☐ Hide extensions for known file types
☑ Hide folder merge conflicts
☐ Hide protected operating system files (Recommended)
☐ Launch folder windows in a separate process
☐ Restore previous folder windows at logon
☑ Show drive letters

Restore Defaults

OK | Cancel | Apply

☐ Item check boxes
☑ File name extensions
☑ Hidden items

WINDOWS BOOT PROCESS: NECESSARY FILES

- **WINLOAD.EXE** – WINLOAD.EXE IS THE OPERATING SYSTEM BOOT LOADER THAT BOOTMGR INVOKES (IN **%SYSTEMROOT%\SYSTEM32**\).
  - THE JOB OF WINLOAD.EXE IS TO LOAD ESSENTIAL DEVICE DRIVERS AS WELL AS OPERATING SYSTEM KERNEL (NTOSKRNL.EXE).
  - WINLOAD.EXE COMBINED WITH BOOTMGR MAKES IT FUNCTIONALLY EQUIVALENT TO NTLDR.
- **WINRESUME.EXE –** IF THE BCD CONTAINS INFORMATION ABOUT A CURRENT HIBERNATION IMAGE, BOOTMGR PASSES THAT INFORMATION TO WINRESUME.EXE.
  - WINRESUME.EXE READS THE HIBERNATION IMAGE FILE,
  - USES IT TO RETURN THE OPERATING SYSTEM TO ITS PRE-HIBERNATION RUNNING STATE SO IT IS USED IF OPERATING SYSTEM IS HIBERNATED

WINDOWS BOOT PROCESS

1. THE UEFI OR BIOS PERFORMS A **POWER-ON SELF-TEST (POST)** - QUICK TESTS ARE CONDUCTED AND ERRORS CAUSED BY INCOMPATIBLE HARDWARE, DISCONNECTED DEVICES, OR FAILING COMPONENTS ARE DISPLAYED WITH ERROR MESSAGES SUCH AS “*KEYBOARD ERROR OR NO KEYBOARD PRESENT”*.
2. THE COMPUTER USES INFORMATION IN THE UEFI OR BIOS TO LOCATE AN INSTALLED HARD DISK, WHICH CONTAINS MASTER BOOT RECORD (MBR) OR GPT.
   1. IN GASE MBR: MBR HAS INFORMATION ABOUT THE ACTIVE PARTITION ON HARD DISK. THE MBR LOADS THE FIRST 512 BYTES OF THE ACTIVE PARTITION INTO THE MEMORY AND INSTRUCTS THE CPU TO EXECUTE THEM. THE 0 SECTOR LOADER CALLS AND LOADS **BOOTMGR**
   2. IN CASE OF UEFI: THIS PROCESS IS SIMPLER - BOOTMGR IS LOADED AT ONCE (STAGE OF 0 SECTOR IS OMITTED)
3. **BOOTMGR** READS THE **BCD** FILE FROM THE ACTIVE PARTITION, GATHERS INFORMATION ABOUT THE MACHINE’S INSTALLED OPERATING SYSTEMS, AND THEN DISPLAYS A BOOT MENU, IF YOUR MACHINE IS IN DUAL BOOT OR SO.
4. USER CHOOSES OS WINDOWS IN THE BOOT MENU (OR IT IS THE ONLY SYSTEM, OR IT IS A DEFAULT SYSTEM AND THE USER DOES NOTHING)
5. **BOOTMGR** TRANSFERS CONTROL TO **WINLOAD.EXE**
6. **WINLOAD.EXE** INITIALIZES MEMORY AND LOADS DRIVERS THAT ARE SET TO BEGIN AT STARTUP. THESE DRIVERS ARE CALLED BOOT_START DRIVERS AND ARE FOR FUNDAMENTAL HARDWARE COMPONENTS SUCH AS DISK CONTROLLERS AND PERIPHERAL BUS DRIVERS. **WINLOAD.EXE** THEN TRANSFERS CONTROL TO THE OPERATING SYSTEM KERNEL, **NTOSKRNL.EXE** (IT IS LOCATED AT %SYSTEMROOT%\SYSTEM32)
7. THE KERNEL INITIALIZES, AND THEN HIGHER-LEVEL DRIVERS LOAD (EXCEPT BOOT_START AND SERVICES). DURING THIS PHASE, YOU WILL SEE THE SCREEN SWITCH TO GRAPHICAL MODE AS THE SESSION MANAGER (**SMSS.EXE**) INITIALIZES THE WINDOWS SUBSYSTEM.
8. WINDOWS LOADS THE **WINLOGON** SERVICE, WHICH DISPLAYS THE SIGN-IN SCREEN. ONCE THE USER SIGNS IN TO THE COMPUTER, WINDOWS EXPLORER LOADS.

FILES NECESSARY FOR SUCCESSFUL WINDOWS BOOT

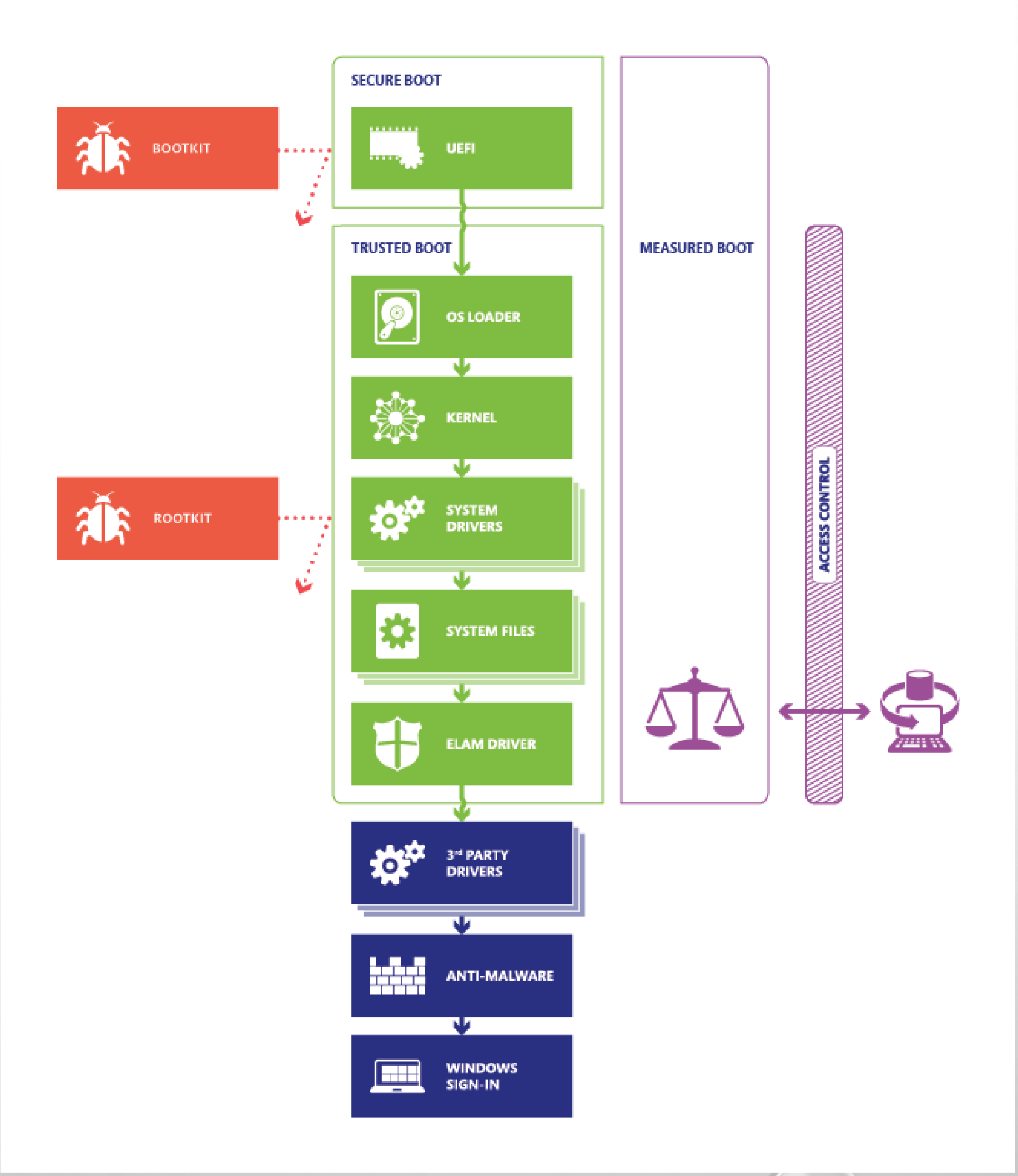
FILE	DESCRIPTION
%SYSTEMDRIVE%\BOOTMGR (BIOS & MBR) (IN SYSTEM PARTITION – UEFI & GPT)	FIRST SYSTEM LOADER
%SYSTEMROOT%\SYTEM32\WINLOAD.EXE	SECOND SYSTEM LOADER
%SYSTEMROOT%\SYTEM32\NTOSKRNL.EXE	SYSTEM KERNEL
%SYSTEMROOT%\SYTEM32\CONFIG\*.*	SYSTEM REGISTRY (SOFTWARE AND HARDWARE SETTINGS)
%SYSTEMROOT%\SYTEM32\DRIVERS\	HARDWARE DRIVERS
%SYSTEMROOT%\SYTEM32\HALL.DLL	HARDWARE ABSTRACTION LAYER

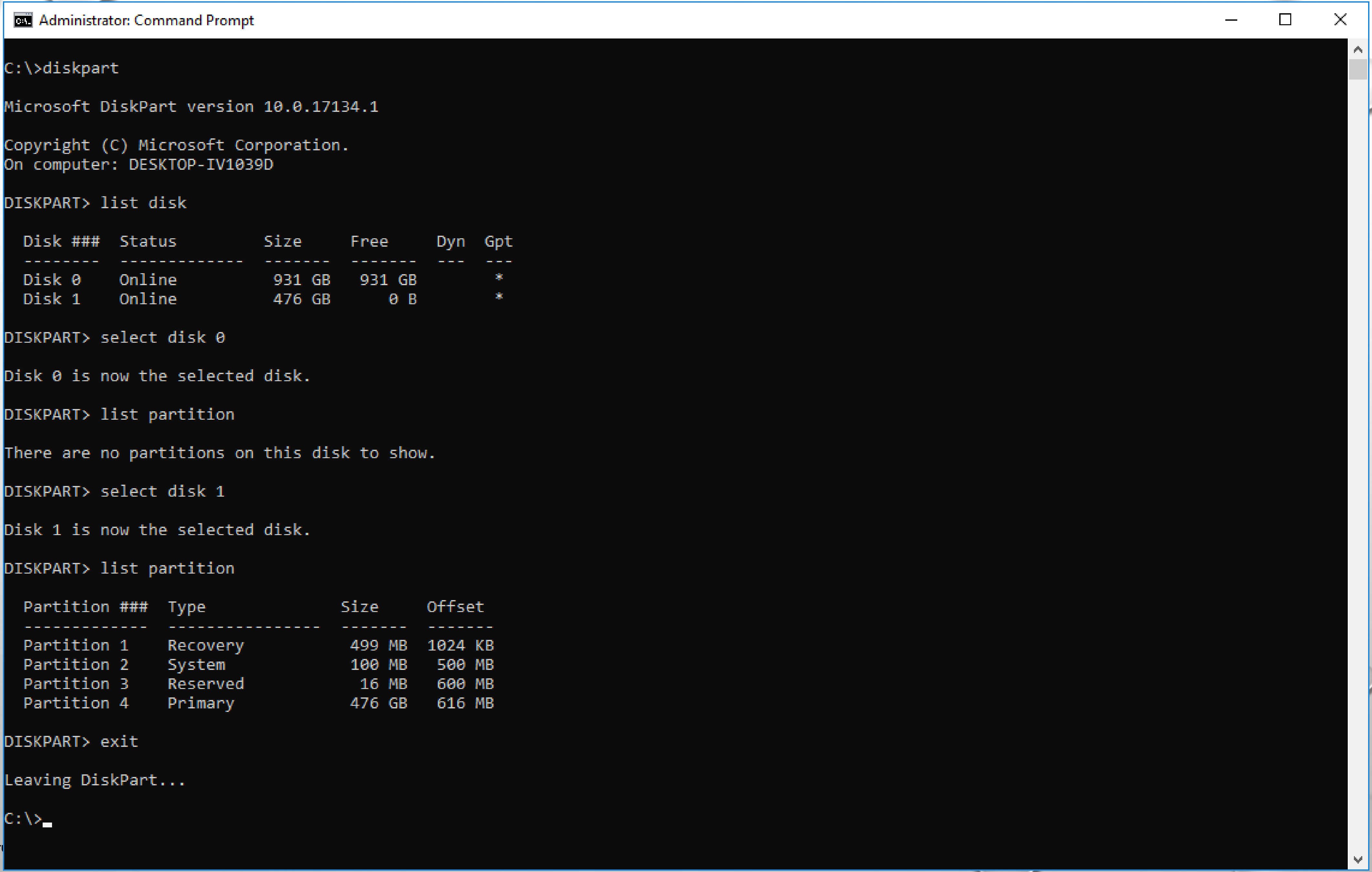
SECURE BOOT VS MALWARE

- *ROOTKITS* ARE A SOPHISTICATED AND DANGEROUS TYPE OF MALWARE THAT RUN IN KERNEL MODE, USING THE SAME PRIVILEGES AS THE OPERATING SYSTEM.
- BECAUSE ROOTKITS HAVE THE SAME RIGHTS AS THE OPERATING SYSTEM AND START BEFORE IT, THEY CAN COMPLETELY HIDE THEMSELVES AND OTHER APPLICATIONS.
- OFTEN, ROOTKITS ARE PART OF AN ENTIRE SUITE OF MALWARE THAT CAN BYPASS LOCAL LOGINS, RECORD PASSWORDS AND KEYSTROKES, TRANSFER PRIVATE FILES, AND CAPTURE CRYPTOGRAPHIC DATA.
- DIFFERENT TYPES OF ROOTKITS LOAD DURING DIFFERENT PHASES OF THE STARTUP PROCESS:
  - **FIRMWARE ROOTKITS.** THESE KITS OVERWRITE THE FIRMWARE OF THE PC’S BASIC INPUT/OUTPUT SYSTEM OR OTHER HARDWARE SO THE ROOTKIT CAN START BEFORE WINDOWS.
  - **BOOTKITS.** THESE KITS REPLACE THE OPERATING SYSTEM’S BOOTLOADER (THE SMALL PIECE OF SOFTWARE THAT STARTS THE OPERATING SYSTEM) SO THAT THE PC LOADS THE BOOTKIT BEFORE THE OPERATING SYSTEM.

SECURE BOOT: COUNTERMEASURES

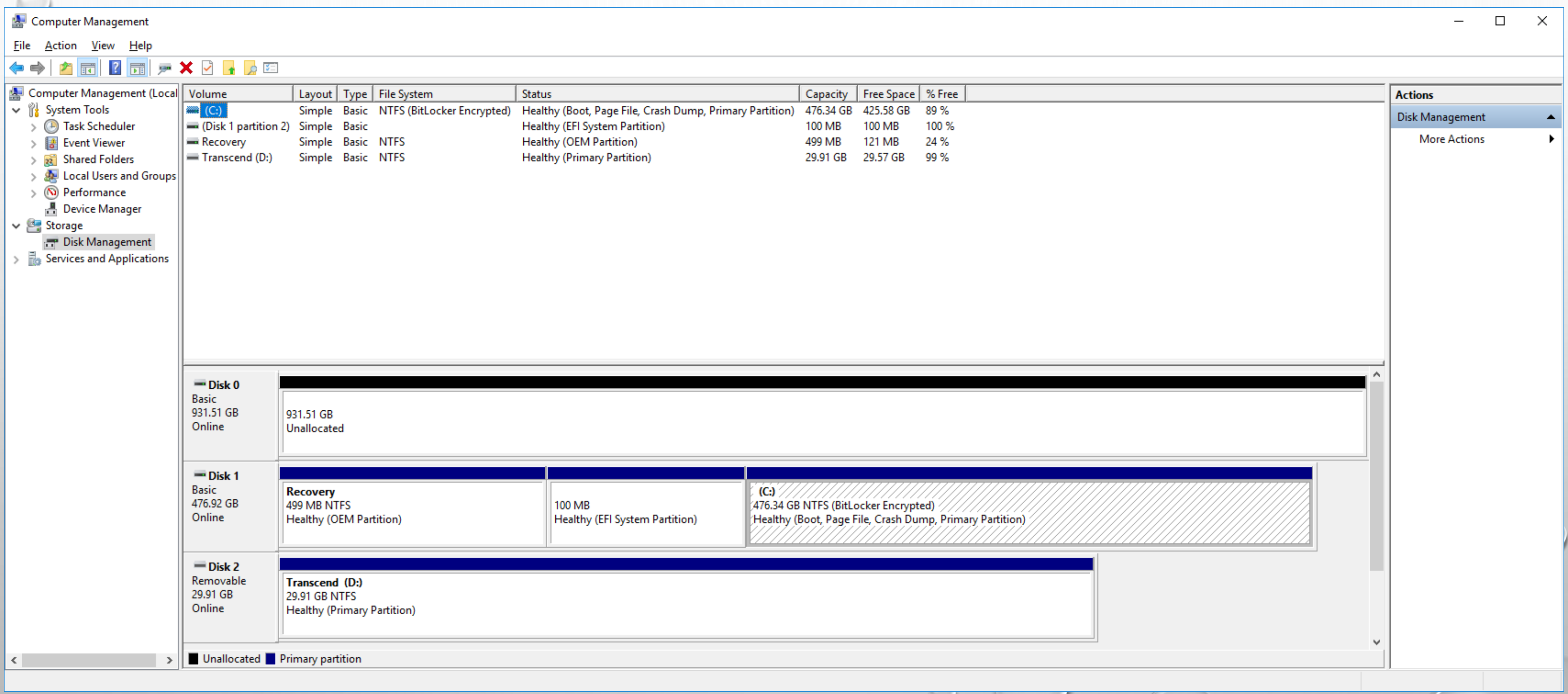
- WINDOWS 10 SUPPORTS FOUR FEATURES TO HELP PREVENT ROOTKITS AND BOOTKITS FROM LOADING DURING THE STARTUP PROCESS:
  - **SECURE BOOT.** PCS WITH UEFI FIRMWARE AND A TRUSTED PLATFORM MODULE (TPM) CAN BE CONFIGURED TO LOAD ONLY TRUSTED OPERATING SYSTEM BOOTLOADERS.
  - **TRUSTED BOOT.** WINDOWS CHECKS THE INTEGRITY OF EVERY COMPONENT OF THE STARTUP PROCESS BEFORE LOADING IT.
  - **EARLY LAUNCH ANTI-MALWARE (ELAM).** ELAM TESTS ALL DRIVERS BEFORE THEY LOAD AND PREVENTS UNAPPROVED DRIVERS FROM LOADING.
  - **MEASURED BOOT.** THE PC’S FIRMWARE LOGS THE BOOT PROCESS, AND WINDOWS CAN SEND IT TO A TRUSTED SERVER THAT CAN OBJECTIVELY ASSESS THE PC’S HEALTH.


SECURE BOOT
BOOTKIT
UEFI
TRUSTED BOOT
MEASURED BOOT
OS LOADER
KERNEL
ROOTKIT
SYSTEM DRIVERS
ACCESS CONTROL
SYSTEM FILES
ELAM DRIVER
3rd PARTY DRIVERS
ANTI-MALWARE
WINDOWS SIGN-IN



```
C:\>diskpart

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-IV1039D

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB   931 GB        *
  Disk 1    Online          476 GB      0 B        *

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> list partition

There are no partitions on this disk to show.

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Recovery           499 MB  1024 KB
  Partition 2    System             100 MB   500 MB
  Partition 3    Reserved            16 MB   600 MB
  Partition 4    Primary            476 GB   616 MB

DISKPART> exit

Leaving DiskPart...

C:\>
```

COMPUTER MANAGEMENT\DISK MANAGEMENT



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS (BitLocker Encrypted)	Healthy (Boot, Page File, Crash Dump, Primary Partition)	476.34 GB	425.58 GB	89 %
(Disk 1 partition 2)	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 MB	100 %
Recovery	Simple	Basic	NTFS	Healthy (OEM Partition)	499 MB	121 MB	24 %
Transcend (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	29.91 GB	29.57 GB	99 %

Disk 0
Basic
931.51 GB
Online

931.51 GB
Unallocated

Disk 1
Basic
476.92 GB
Online

Recovery
499 MB NTFS
Healthy (OEM Partition)

100 MB
Healthy (EFI System Partition)

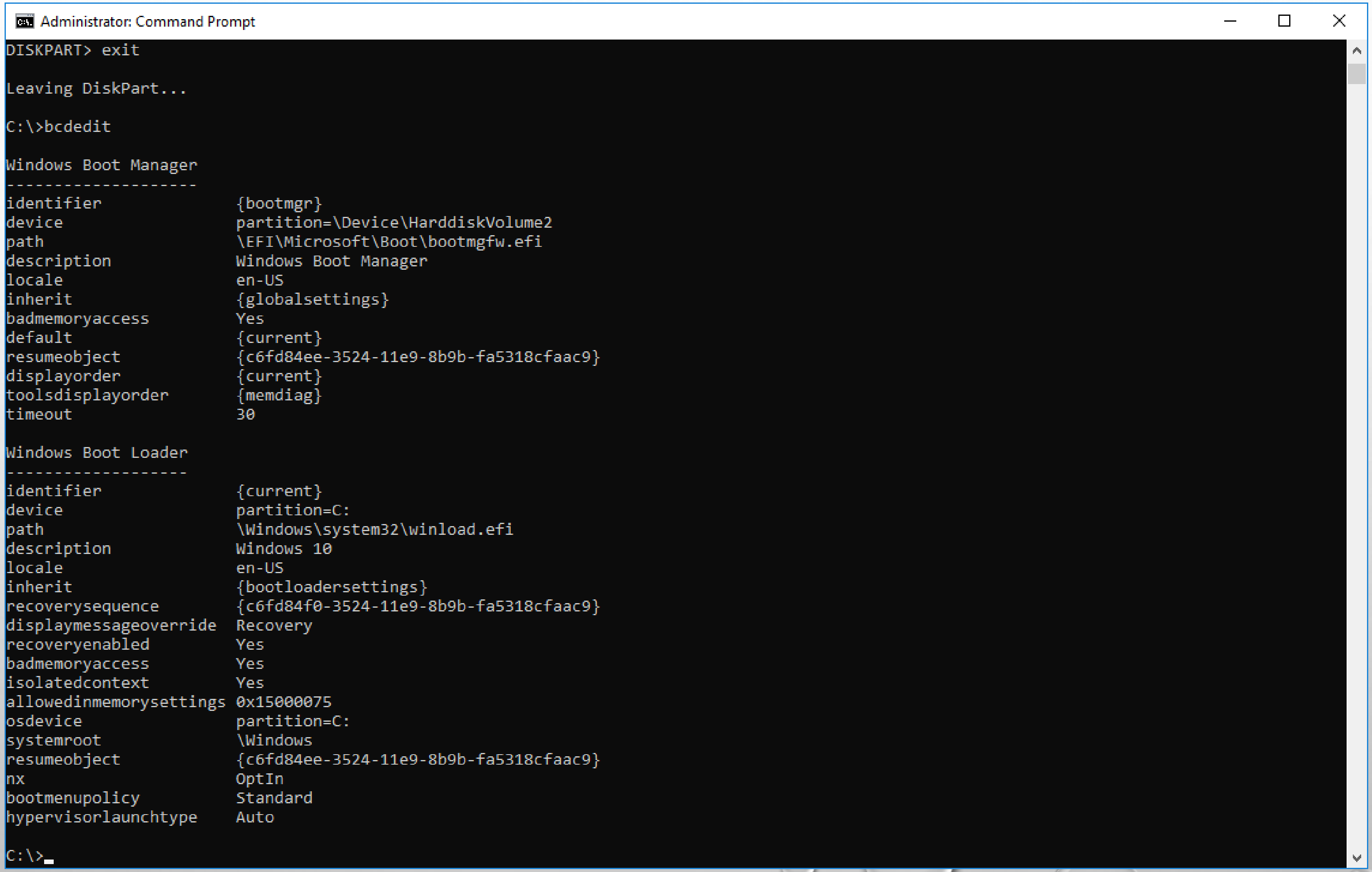
(C:)
476.34 GB NTFS (BitLocker Encrypted)
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 2
Removable
29.91 GB
Online

Transcend (D:)
29.91 GB NTFS
Healthy (Primary Partition)

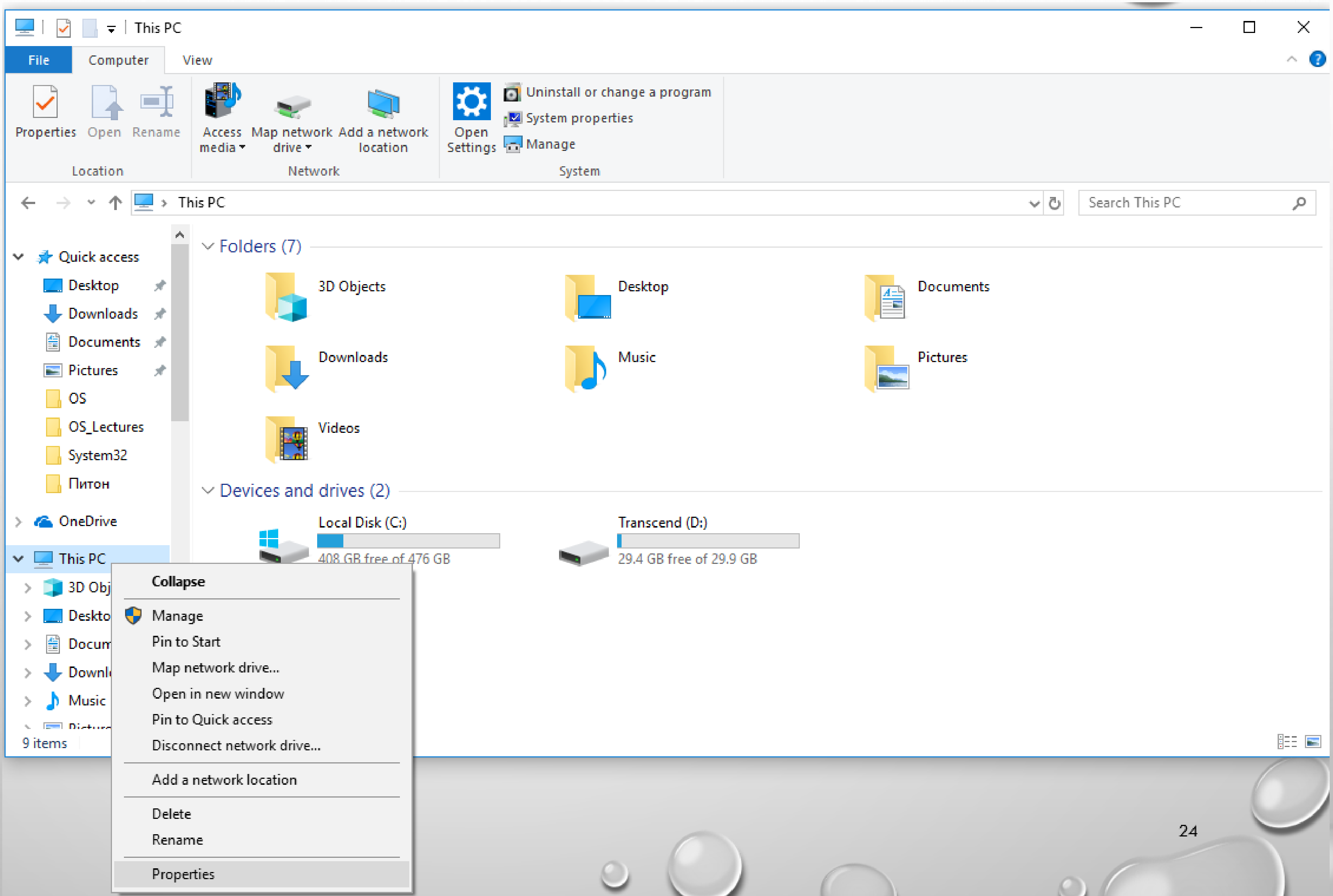
■ Unallocated ■ Primary partition

BCDEDIT.EXE

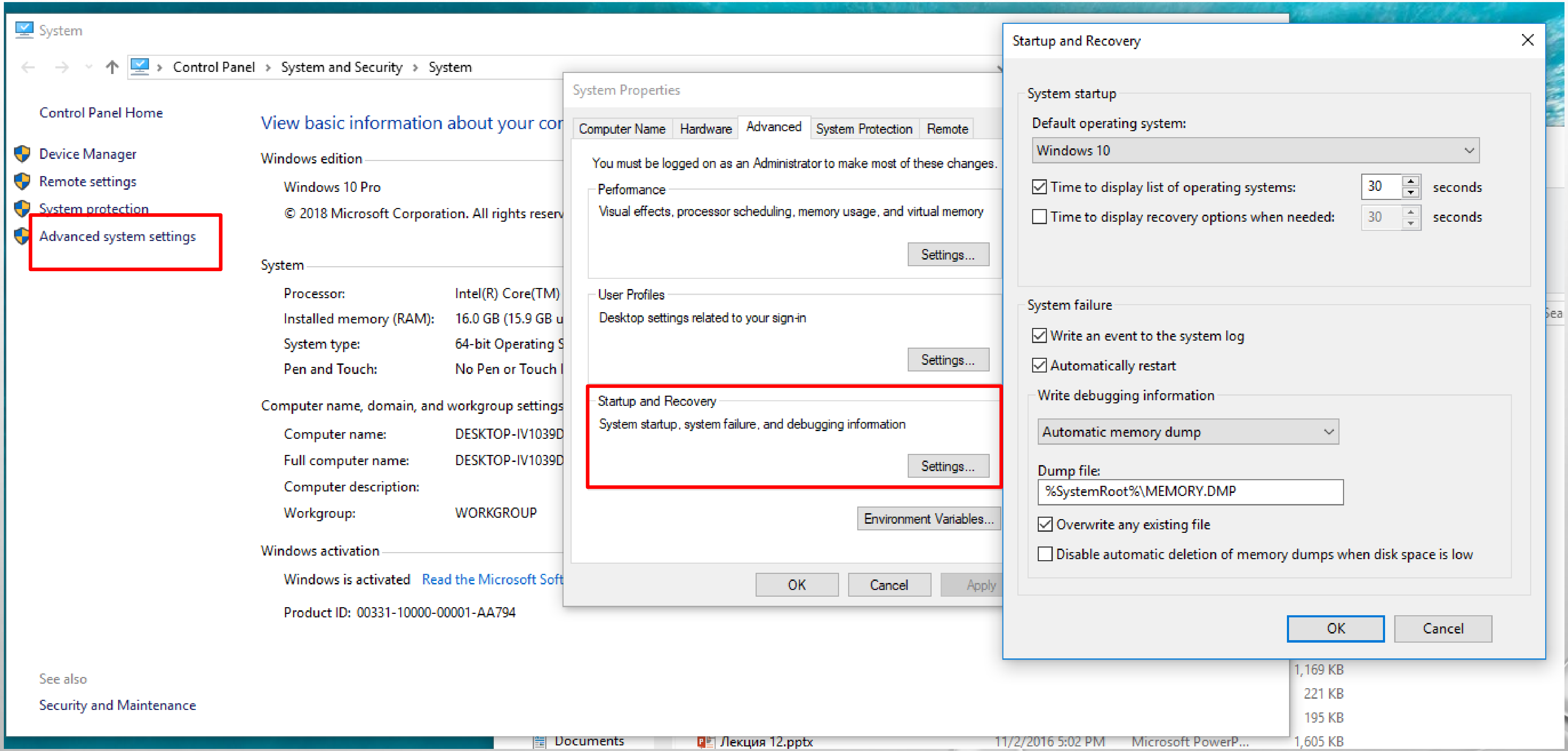


```
DISKPART> exit

Leaving DiskPart...

C:\>bcdedit

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume2
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
badmemoryaccess         Yes
default                 {current}
resumeobject            {c6fd84ee-3524-11e9-8b9b-fa5318cfaac9}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.efi
description             Windows 10
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {c6fd84f0-3524-11e9-8b9b-fa5318cfaac9}
displaymessageoverride  Recovery
recoveryenabled         Yes
badmemoryaccess         Yes
isolatedcontext         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {c6fd84ee-3524-11e9-8b9b-fa5318cfaac9}
nx                      OptIn
bootmenupolicy          Standard
hypervisorlaunchtype    Auto

C:\>
```

SYSTEM WINDOW



BOOT PARAMETERS



System

Control Panel › System and Security › System

Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings

View basic information about your cor

Windows edition

Windows 10 Pro

© 2018 Microsoft Corporation. All rights reserv

System

Processor: Intel(R) Core(TM)

Installed memory (RAM): 16.0 GB (15.9 GB u

System type: 64-bit Operating S

Pen and Touch: No Pen or Touch I

Computer name, domain, and workgroup settings

Computer name: DESKTOP-IV1039D

Full computer name: DESKTOP-IV1039D

Computer description:

Workgroup: WORKGROUP

Windows activation

Windows is activated Read the Microsoft Soft

Product ID: 00331-10000-00001-AA794

See also

Security and Maintenance

System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

Startup and Recovery

System startup

Default operating system:

Windows 10

☑ Time to display list of operating systems: 30 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Automatic memory dump

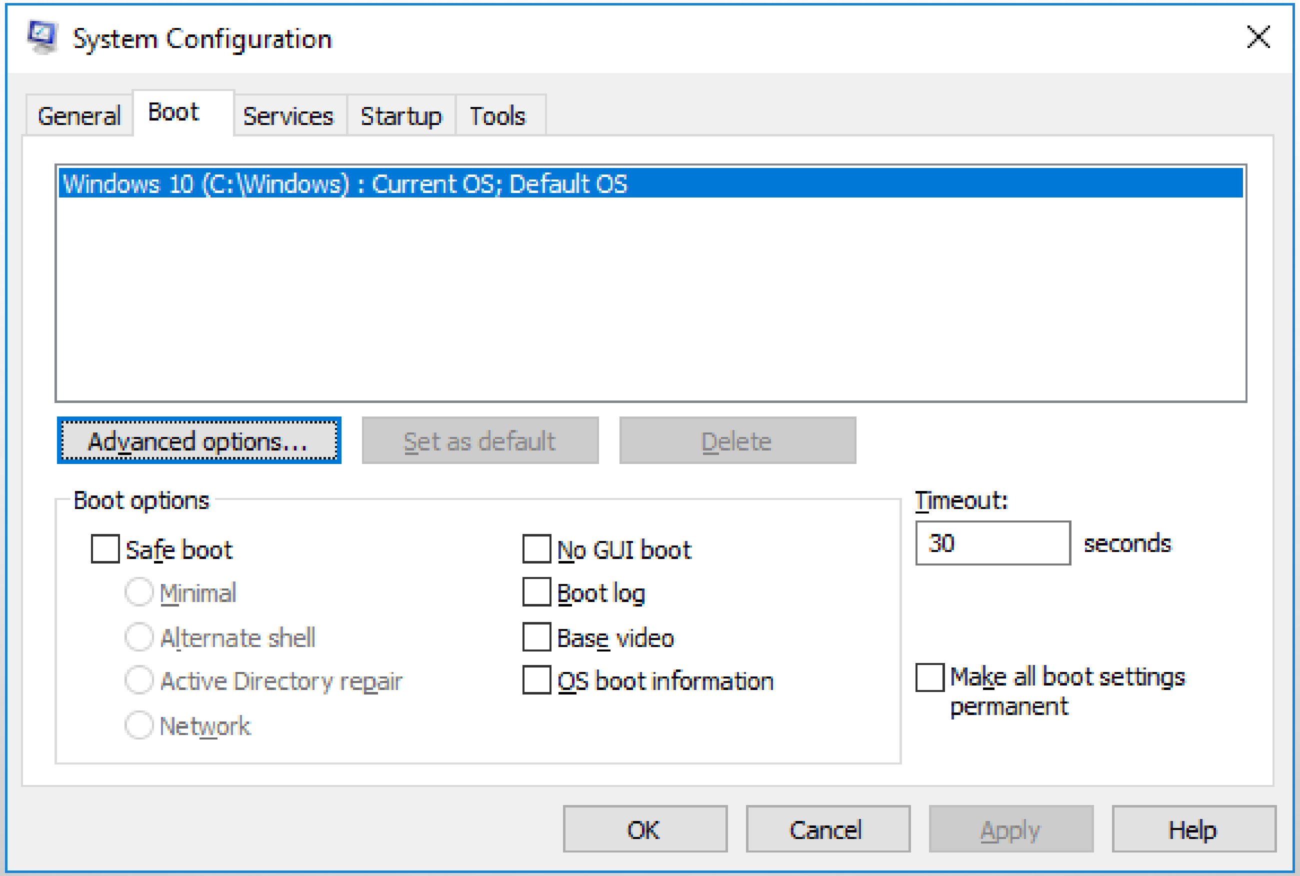
Dump file:

%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

□ Disable automatic deletion of memory dumps when disk space is low

MSCONFIG.EXE



Windows 10 (C:\Windows) : Current OS; Default OS

Boot options

□ Safe boot

○ Minimal

○ Alternate shell

○ Active Directory repair

○ Network

□ No GUI boot

□ Boot log

□ Base video

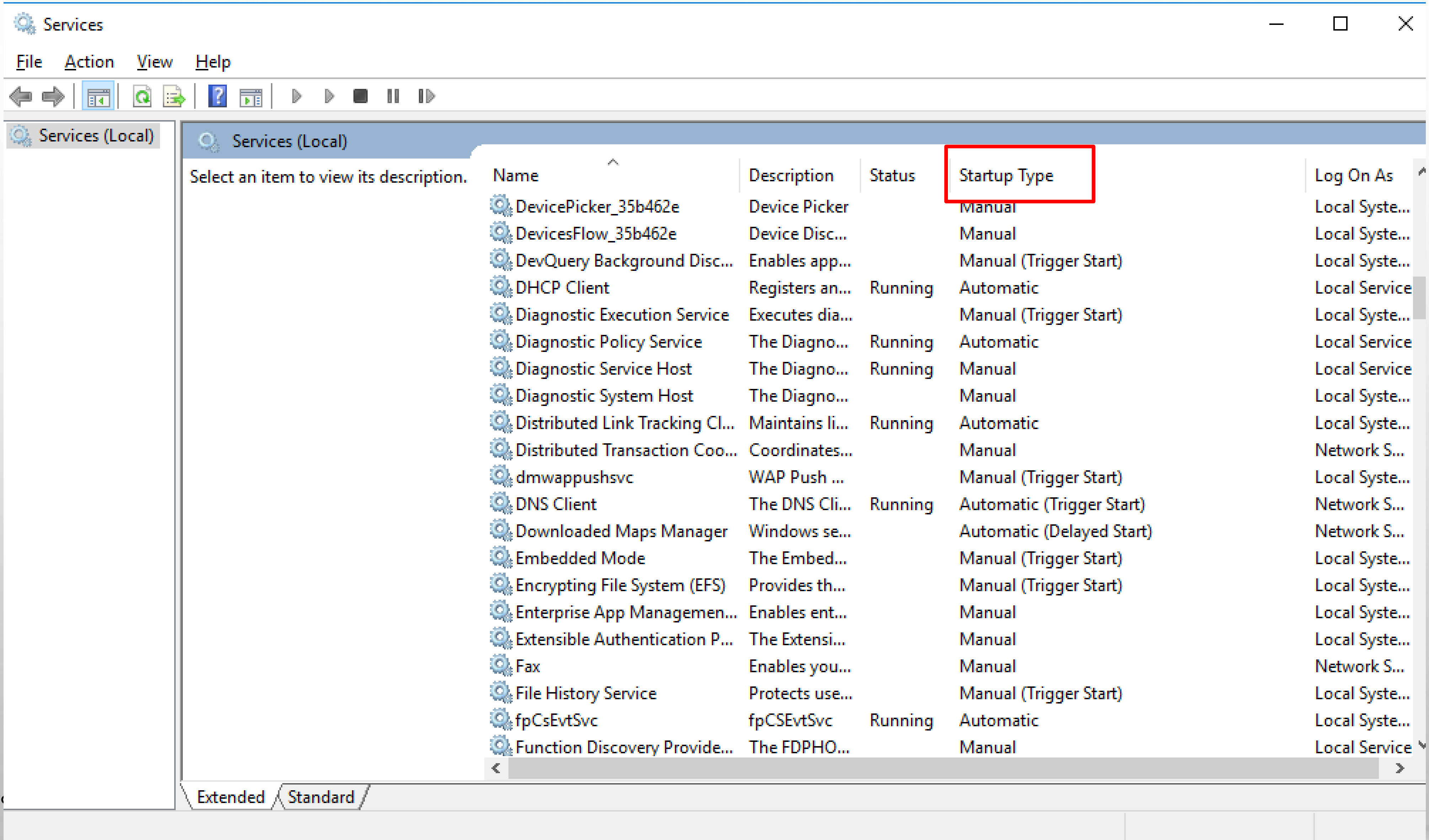
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

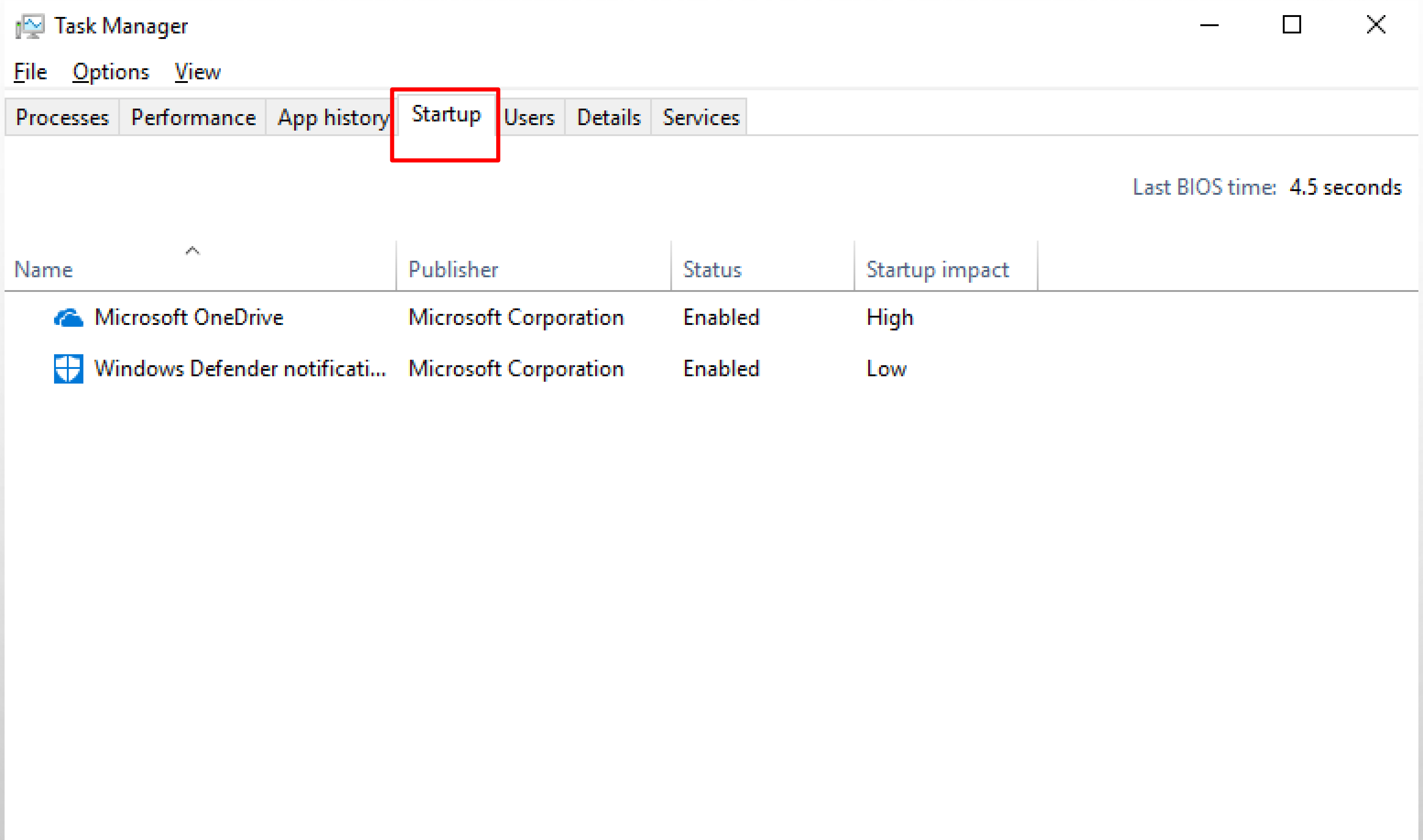
BOOT ACCELERATION

- CHECK THE SERVICES LIST : FIND THOSE WITH STARTUP TYPE “AUTOMATIC” AND DECIDE WHETHER IT IS POSSIBLE TO MAKE THEM “MANUAL” OR, AT LEAST, “DELAYED START”
- CHECK THE APPS STARTUP LIST: THINK WHETHER ALL THESE APPS ARE NECESSARY FOR STARTUP



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
DevicePicker_35b462e	Device Picker		Manual	Local Syste...
DevicesFlow_35b462e	Device Disc...		Manual	Local Syste...
DevQuery Background Disc...	Enables app...		Manual (Trigger Start)	Local Syste...
DHCP Client	Registers an...	Running	Automatic	Local Service
Diagnostic Execution Service	Executes dia...		Manual (Trigger Start)	Local Syste...
Diagnostic Policy Service	The Diagno...	Running	Automatic	Local Service
Diagnostic Service Host	The Diagno...	Running	Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local Syste...
Distributed Link Tracking Cl...	Maintains li...	Running	Automatic	Local Syste...
Distributed Transaction Coo...	Coordinates...		Manual	Network S...
dmwappushsvc	WAP Push ...		Manual (Trigger Start)	Local Syste...
DNS Client	The DNS Cli...	Running	Automatic (Trigger Start)	Network S...
Downloaded Maps Manager	Windows se...		Automatic (Delayed Start)	Network S...
Embedded Mode	The Embed...		Manual (Trigger Start)	Local Syste...
Encrypting File System (EFS)	Provides th...		Manual (Trigger Start)	Local Syste...
Enterprise App Managemen...	Enables ent...		Manual	Local Syste...
Extensible Authentication P...	The Extensi...		Manual	Local Syste...
Fax	Enables you...		Manual	Network S...
File History Service	Protects use...		Manual (Trigger Start)	Local Syste...
fpCsEvtSvc	fpCSEvtSvc	Running	Automatic	Local Syste...
Function Discovery Provide...	The FDPHO...		Manual	Local Service

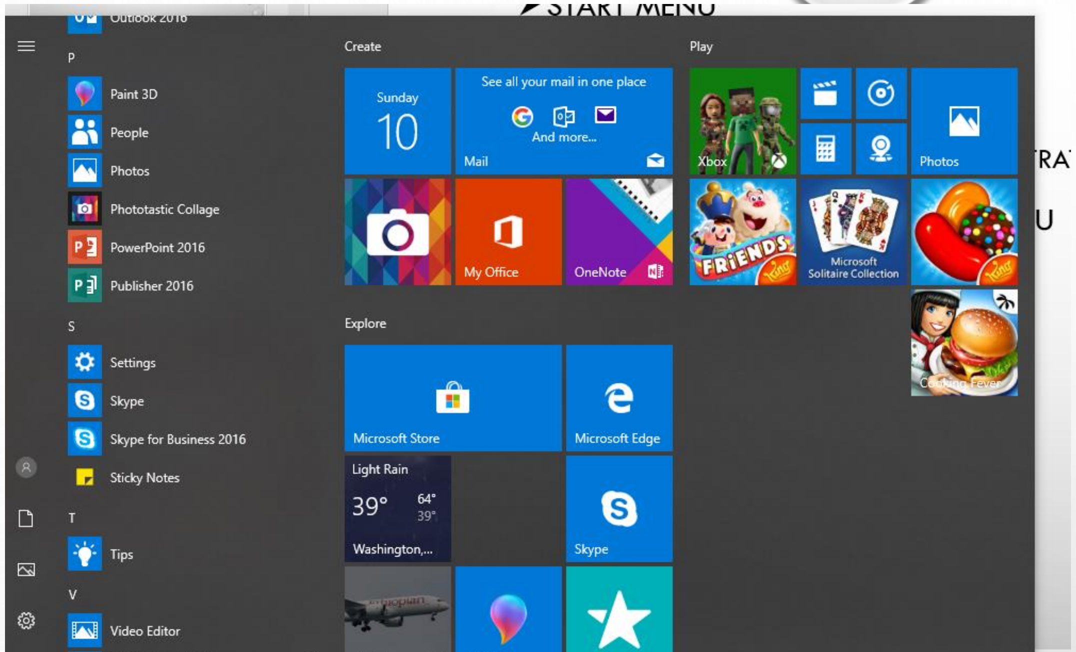


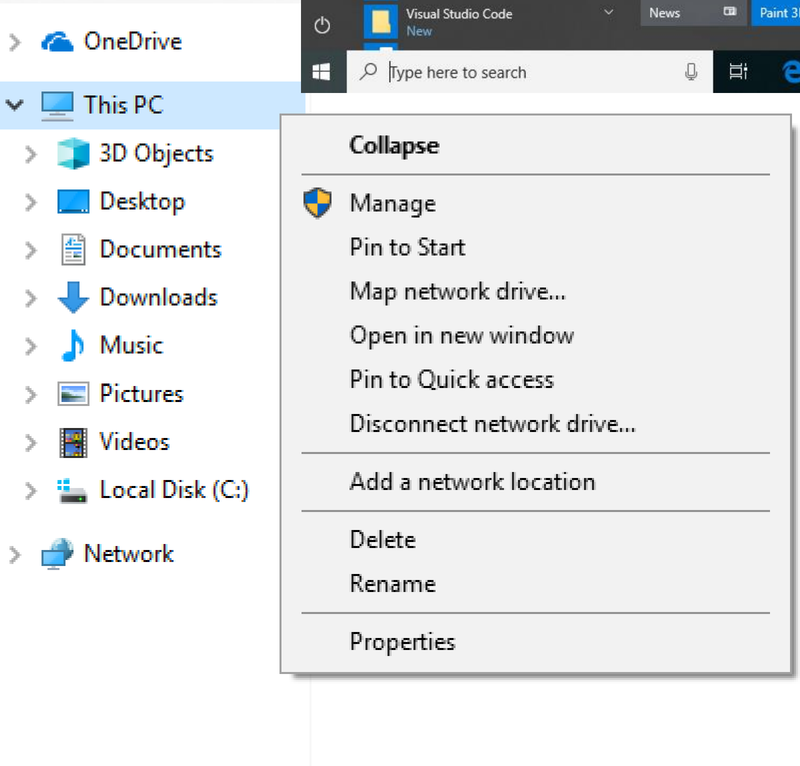
Last BIOS time: 4.5 seconds

Name	Publisher	Status	Startup impact
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Windows Defender notificati...	Microsoft Corporation	Enabled	Low

WHERE TO LOOK FOR ADMINISTRATIVE TOOLS

- START MENU
  - START MENU\SETTINGS
  - START MENU\WINDOWS SYSTEM
  - START MENU\WINDOWS ADMINISTRATION TOOLS
- ICON “THIS PC” - CONTEXTUAL MENU
  - OPTION “MANAGE”
  - OPTION “PROPERTIES”
- MMC

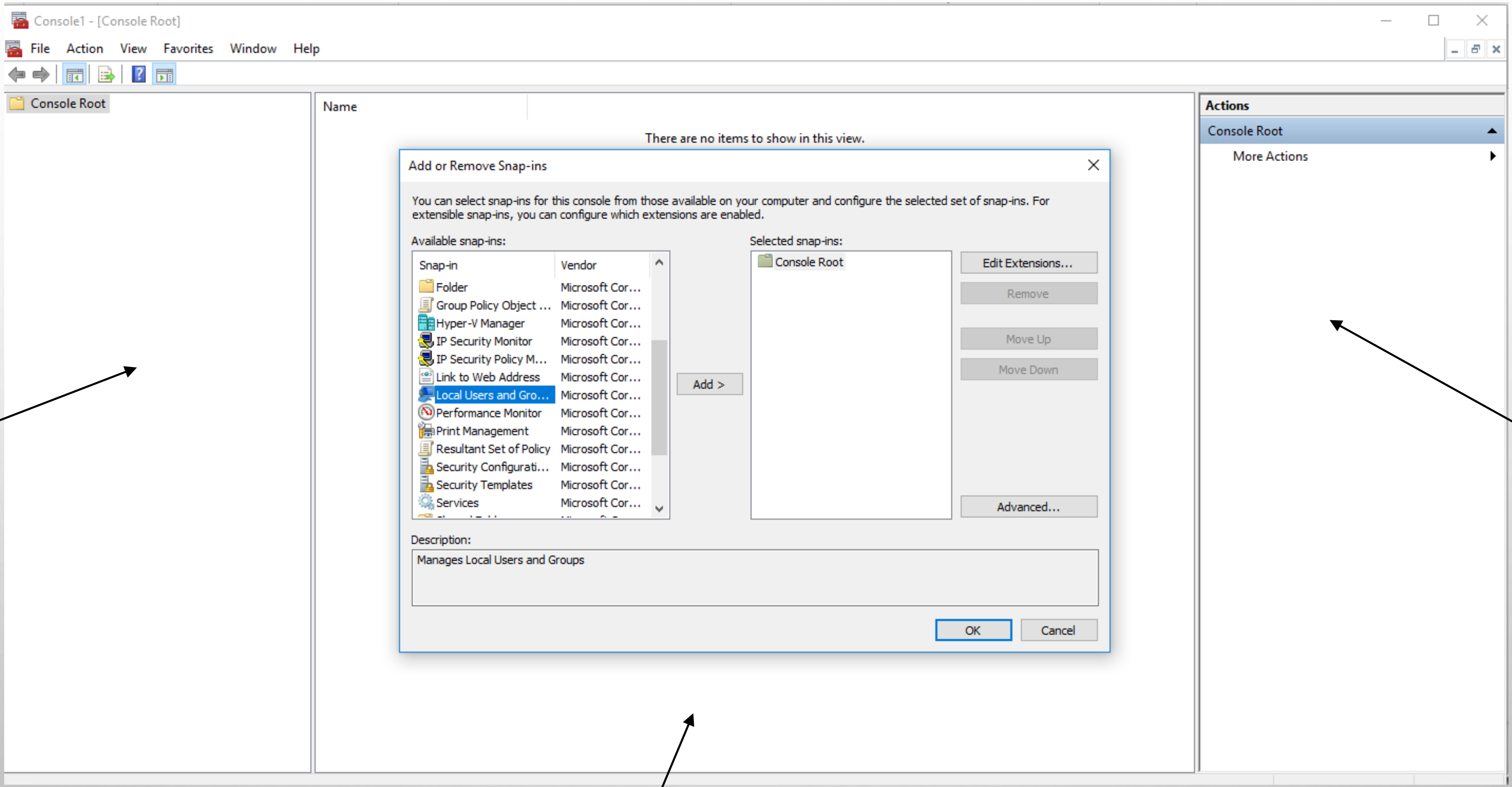




MMC – MICROSOFT MANAGEMENT CONSOLE

- IS A FRAMEWORK THAT UNIFIES AND SIMPLIFIES DAY-TO-DAY SYSTEM MANAGEMENT TASKS ON WINDOWS BY PROVIDING COMMON NAVIGATION, MENUS, TOOLBARS, AND WORKFLOW ACROSS DIVERSE TOOLS
- REDUCES THE COST OF ADMINISTERING WINDOWS-BASED APPLICATIONS BY PROVIDING AN EASY-TO-LEARN, CONSISTENT, AND INTEGRATED CONSOLE THAT HOSTS A VARIETY OF WINDOWS AND NON-MICROSOFT ADMINISTRATIVE TOOLS
- MMC IS AN EMPTY FRAMEWORK, TO USE IT IN PRACTICE, IT IS NECESSARY TO INSERT SNAP-INS IN IT
- COULD BE SAVED AND COPIED ANYWHERE (*.MSC)
- TO CREATE –> (WIN+R)-> TYPE MMC

MMC



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Hyper-V Manager	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Print Management	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...

Selected snap-ins:

Console Root

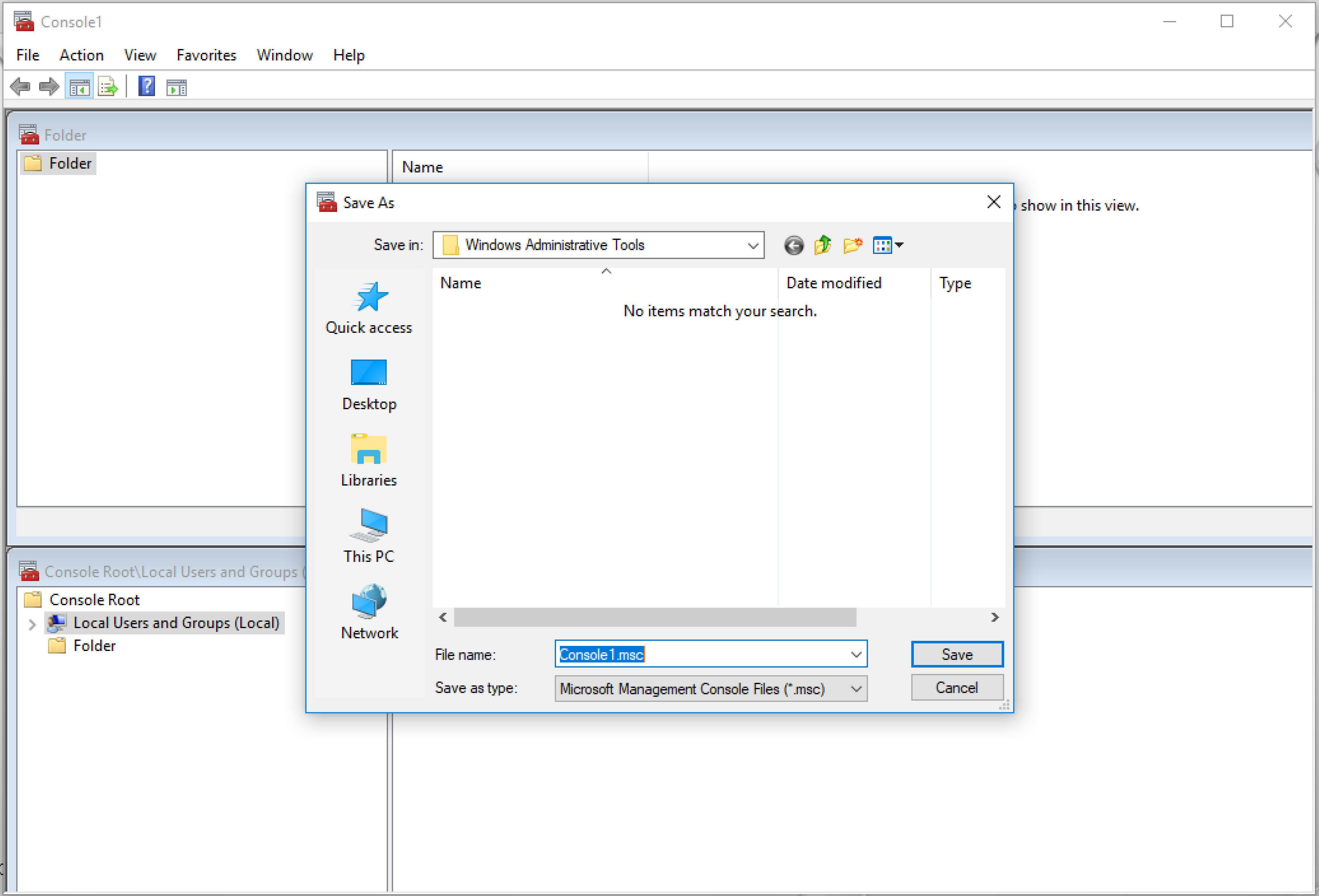
Description:

Manages Local Users and Groups

STRUCTURE PANEL

ACTION PANEL

DATA PANEL

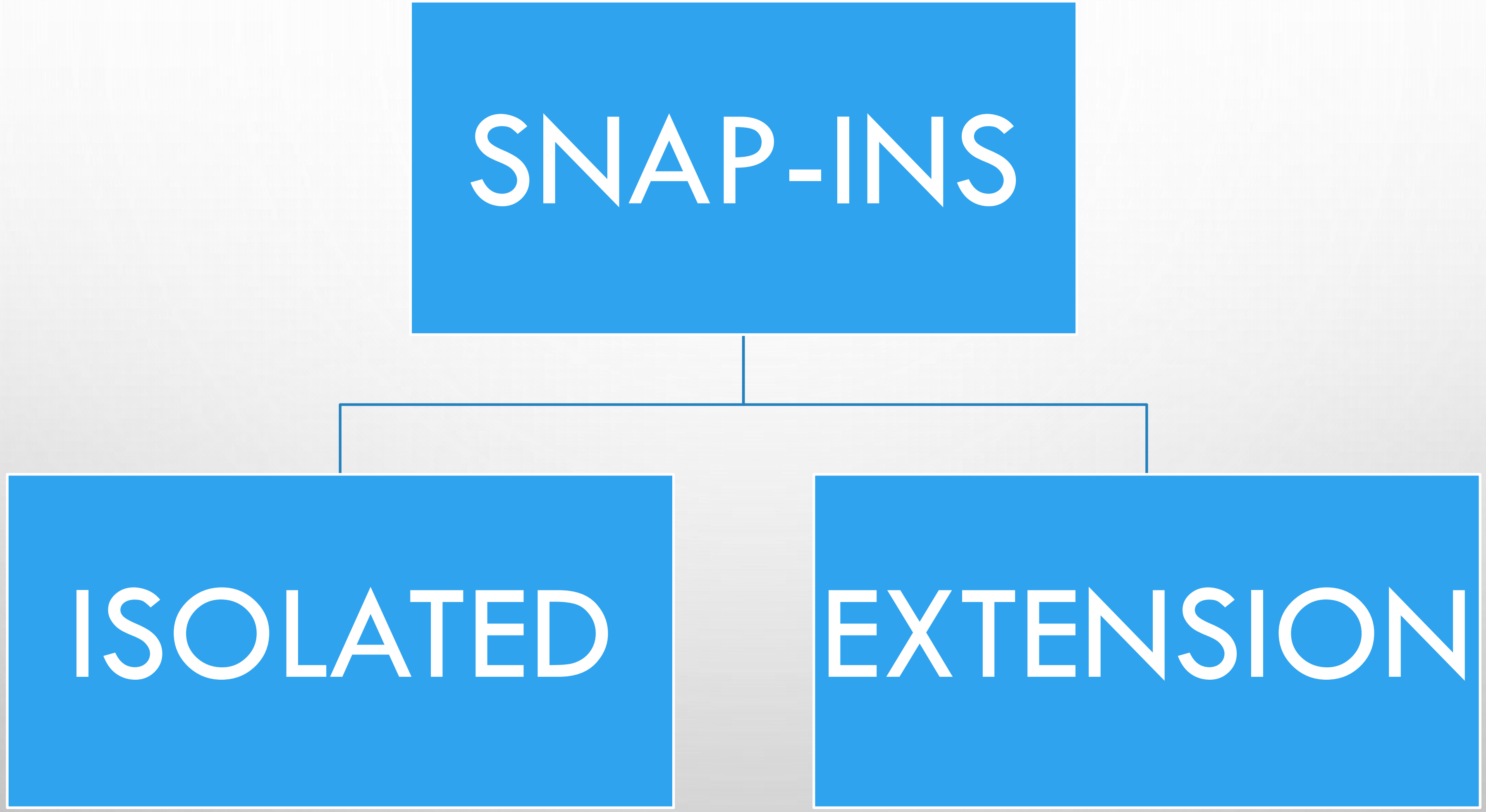


Save in: Windows Administrative Tools

No items match your search.

File name: Console1.msc

Save as type: Microsoft Management Console Files (*.msc)

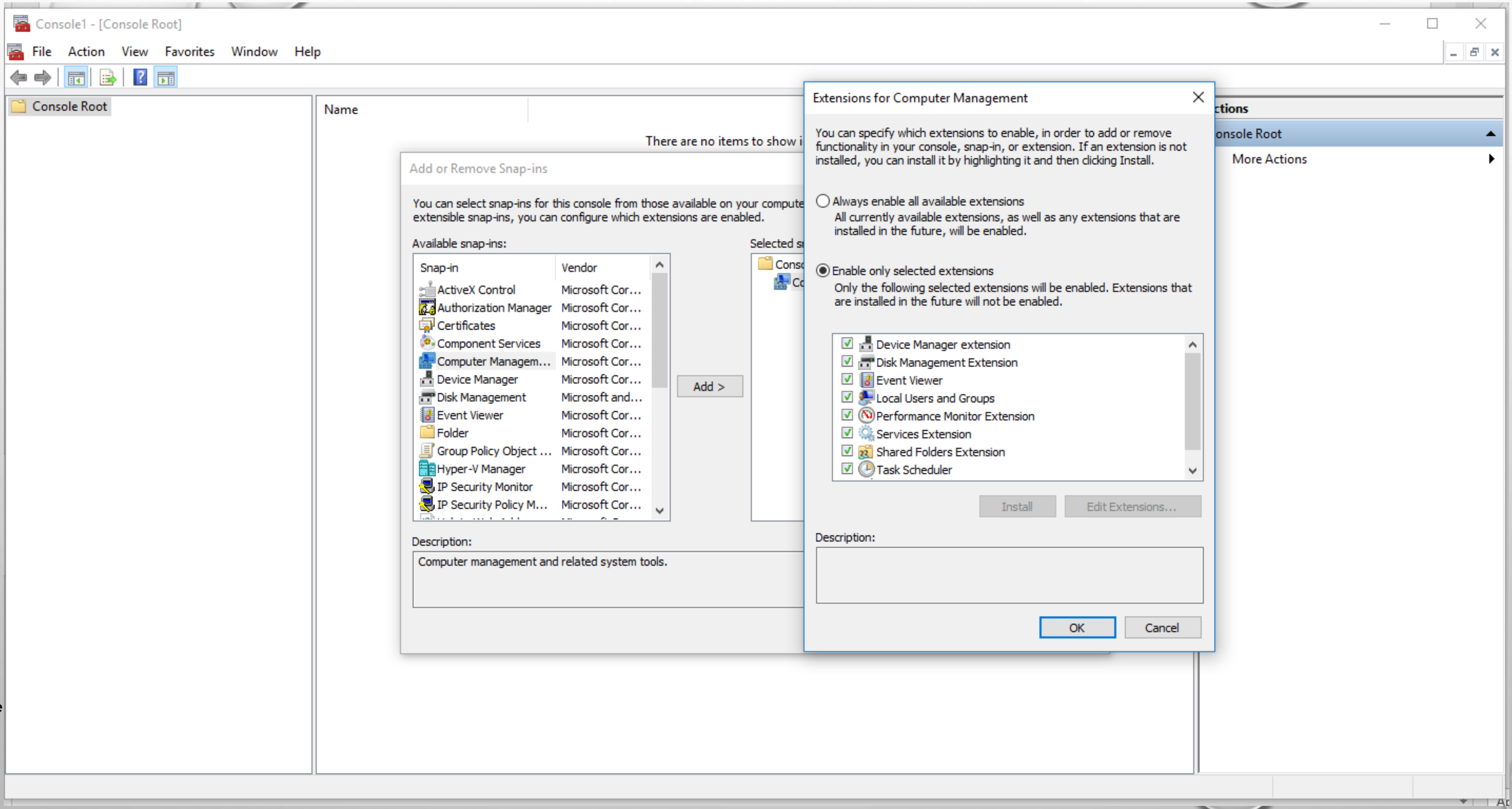


SNAP-INS

ISOLATED

EXTENSION

SNAP-IN WITH EXTENSIONS



You can select snap-ins for this console from those available on your compute
extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Hyper-V Manager	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

Description:

Computer management and related system tools.

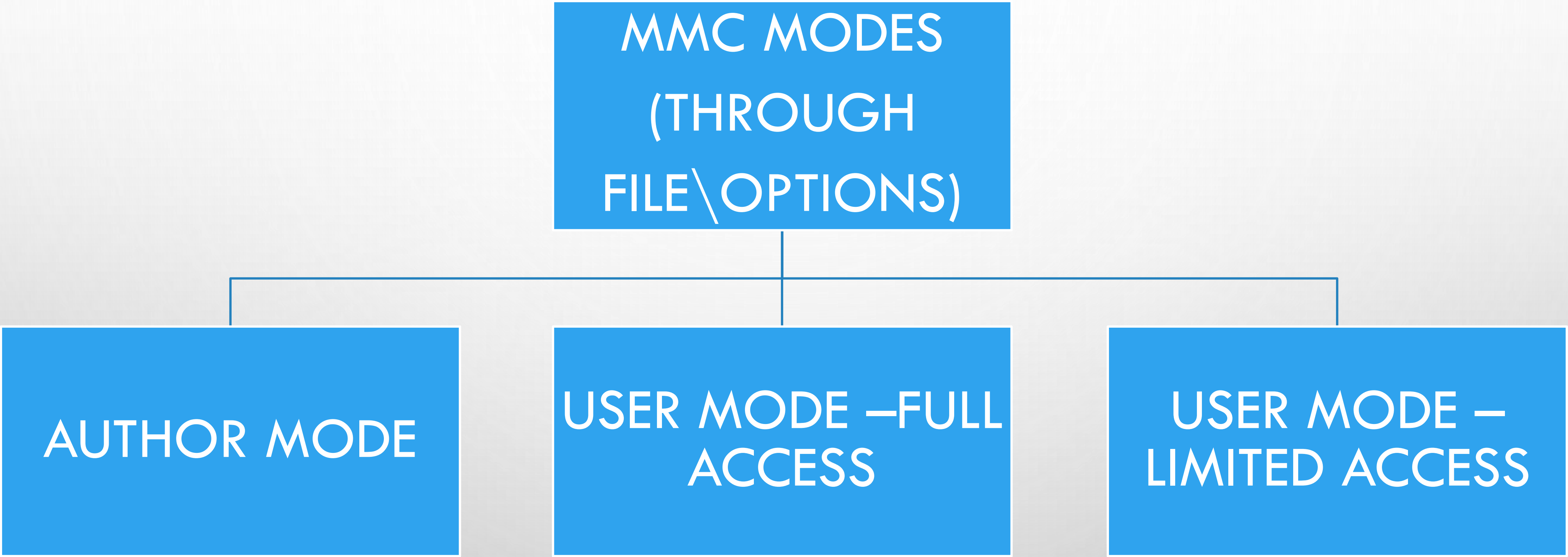
You can specify which extensions to enable, in order to add or remove functionality in your console, snap-in, or extension. If an extension is not installed, you can install it by highlighting it and then clicking Install.

○ Always enable all available extensions
All currently available extensions, as well as any extensions that are installed in the future, will be enabled.

● Enable only selected extensions
Only the following selected extensions will be enabled. Extensions that are installed in the future will not be enabled.

- ☑ Device Manager extension
- ☑ Disk Management Extension
- ☑ Event Viewer
- ☑ Local Users and Groups
- ☑ Performance Monitor Extension
- ☑ Services Extension
- ☑ Shared Folders Extension
- ☑ Task Scheduler

Description:



MMC MODES (THROUGH FILE\OPTIONS)

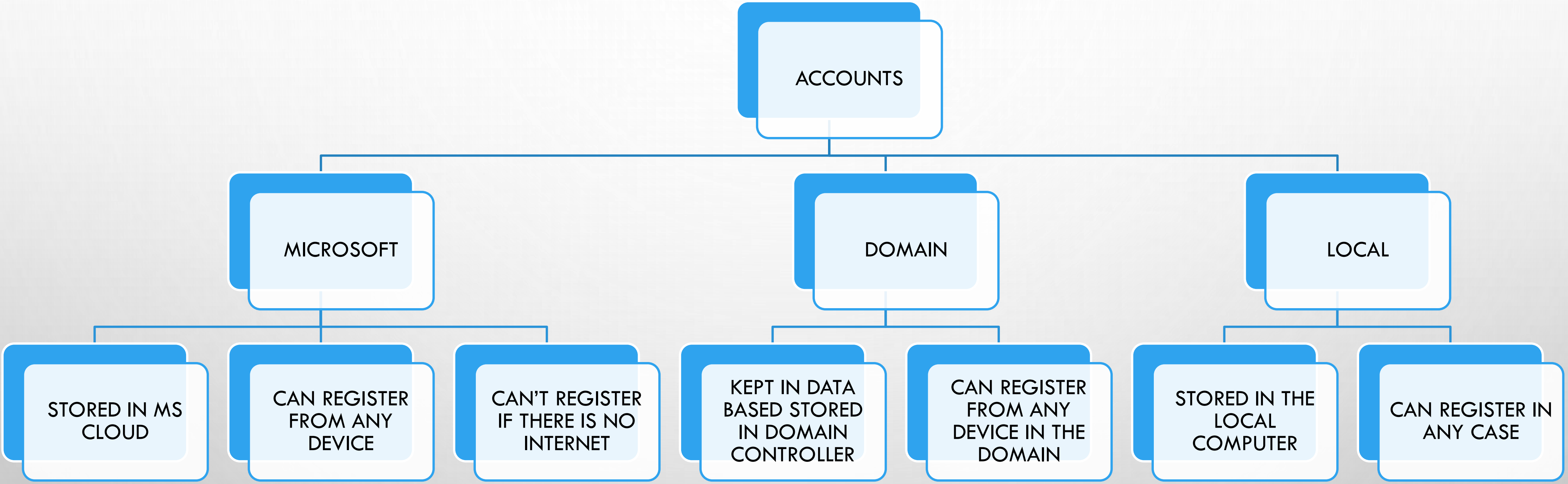
AUTHOR MODE

USER MODE –FULL ACCESS

USER MODE – LIMITED ACCESS

USERS AND GROUPS

SYSTEM ADMINISTRATION TASKS

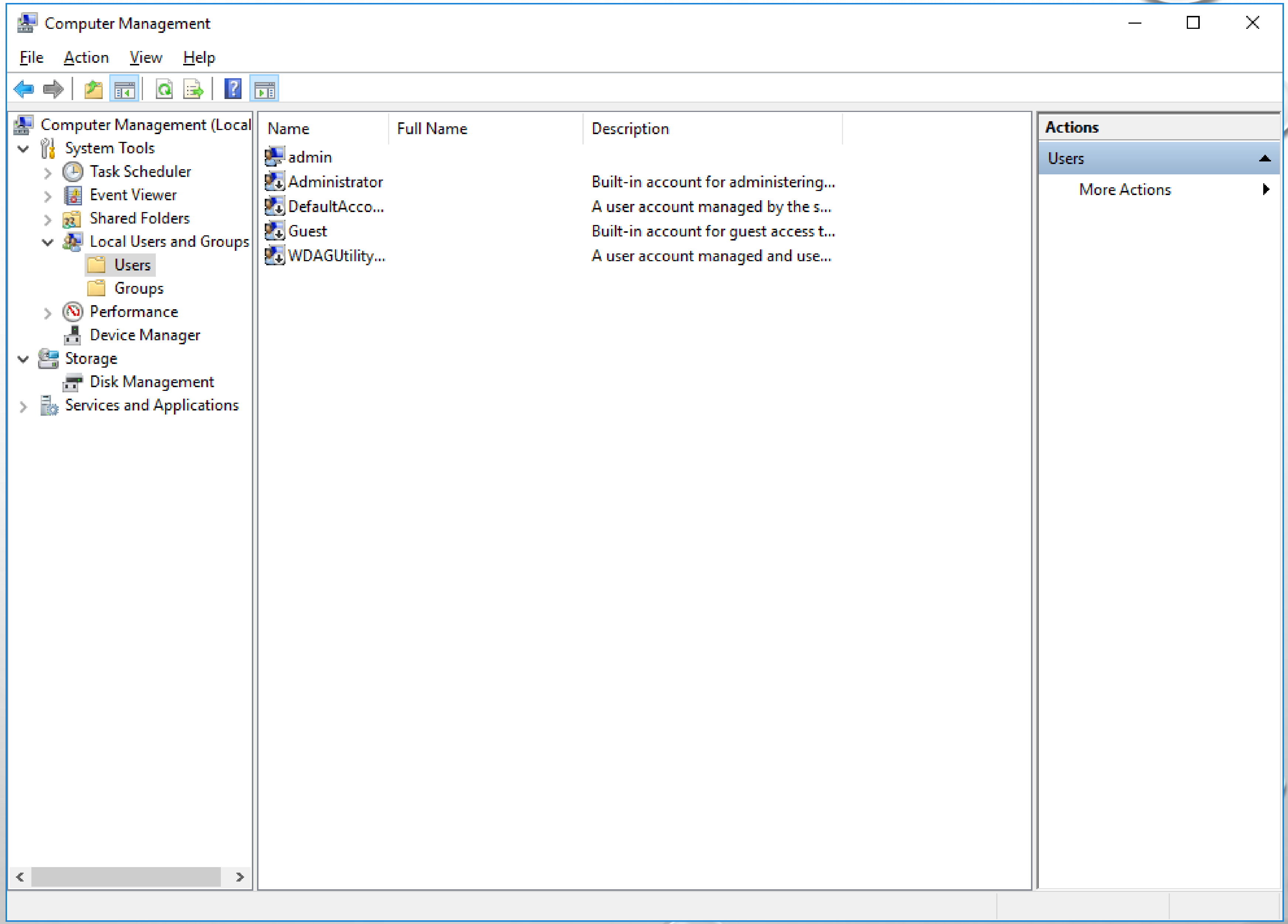


ACCOUNTS

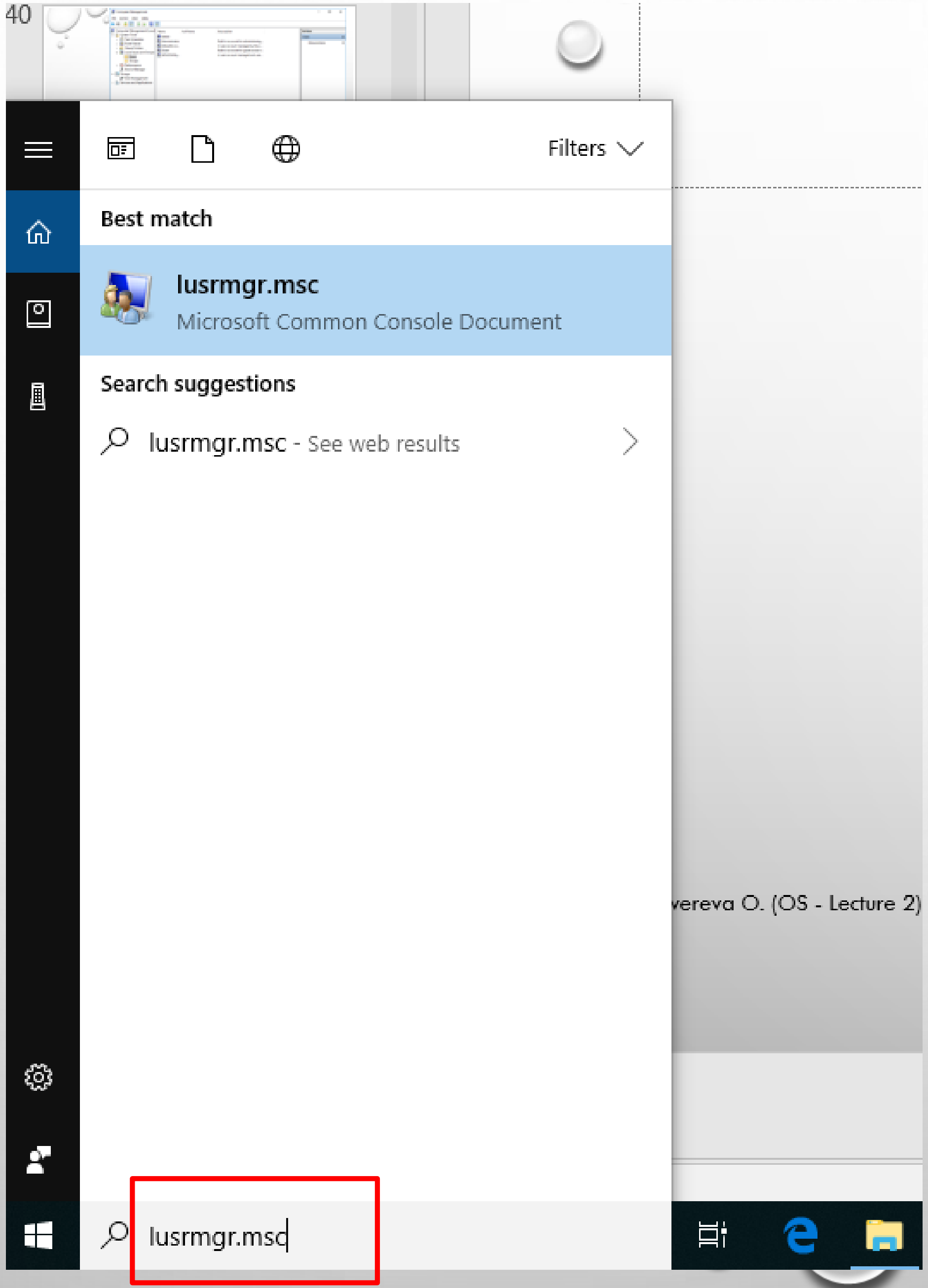
- MICROSOFT
  - STORED IN MS CLOUD
  - CAN REGISTER FROM ANY DEVICE
  - CAN'T REGISTER IF THERE IS NO INTERNET
- DOMAIN
  - KEPT IN DATA BASED STORED IN DOMAIN CONTROLLER
  - CAN REGISTER FROM ANY DEVICE IN THE DOMAIN
- LOCAL
  - STORED IN THE LOCAL COMPUTER
  - CAN REGISTER IN ANY CASE

SOME TERMS

- A **WINDOWS DOMAIN** IS A FORM OF A COMPUTER NETWORK IN WHICH ALL USER ACCOUNTS, COMPUTERS, PRINTERS AND OTHER SECURITY PRINCIPALS, ARE REGISTERED WITH A CENTRAL DATABASE LOCATED ON ONE OR MORE CLUSTERS OF CENTRAL COMPUTERS KNOWN AS DOMAIN CONTROLLERS.
- **A USER'S ACCOUNT** ALLOWS A USER TO AUTHENTICATE TO A SYSTEM AND POTENTIALLY TO RECEIVE AUTHORIZATION TO ACCESS RESOURCES PROVIDED BY OR CONNECTED TO THAT SYSTEM



Name	Full Name	Description
admin		
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...



Best match

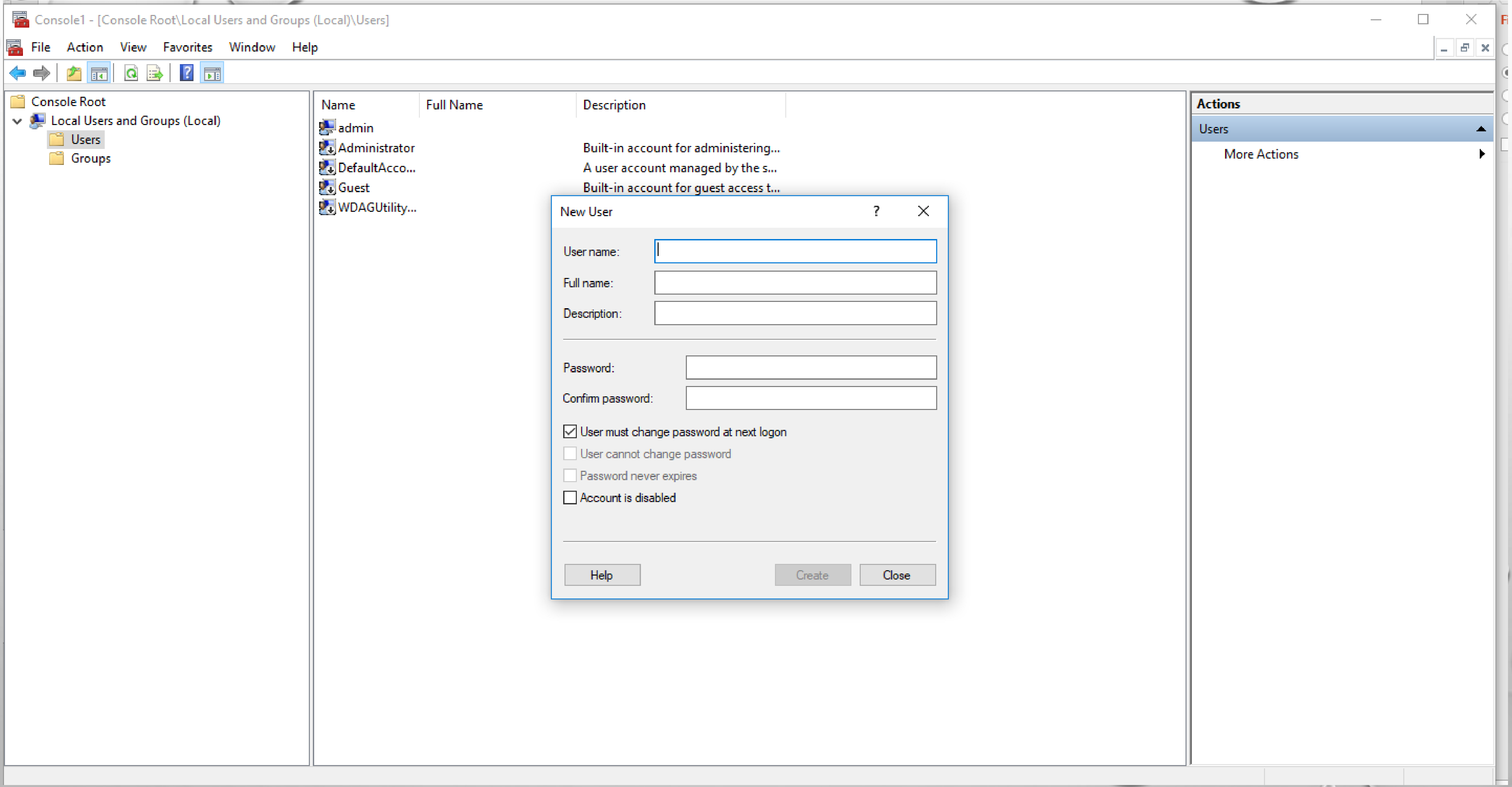
lusrmgr.msc
Microsoft Common Console Document

Search suggestions

lusrmgr.msc - See web results

lusrmgr.msc

A LOCAL USER’S ACCOUNT CREATION



Name	Full Name	Description
admin		
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtility...		

User name:

Full name:

Description:

Password:

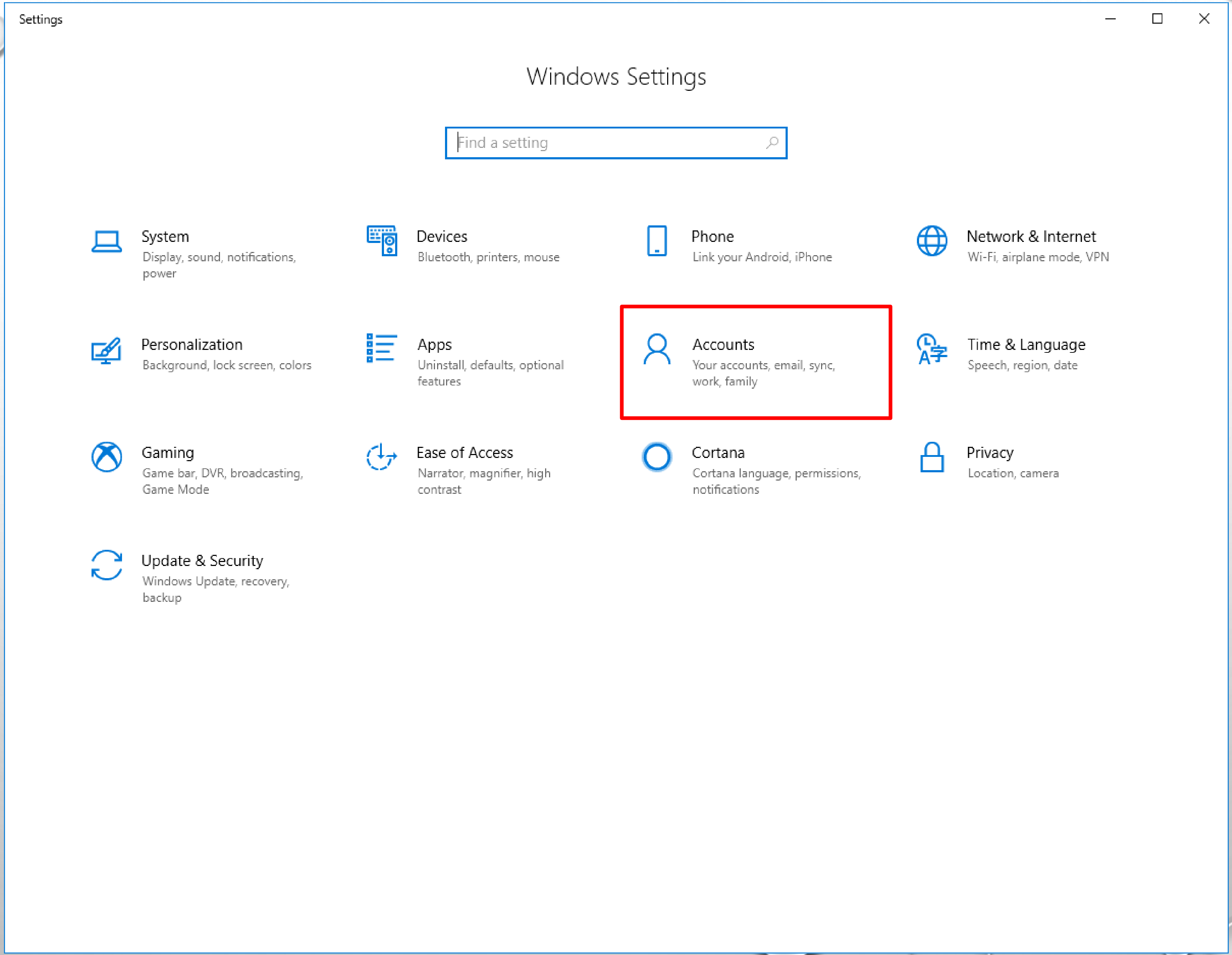
Confirm password:

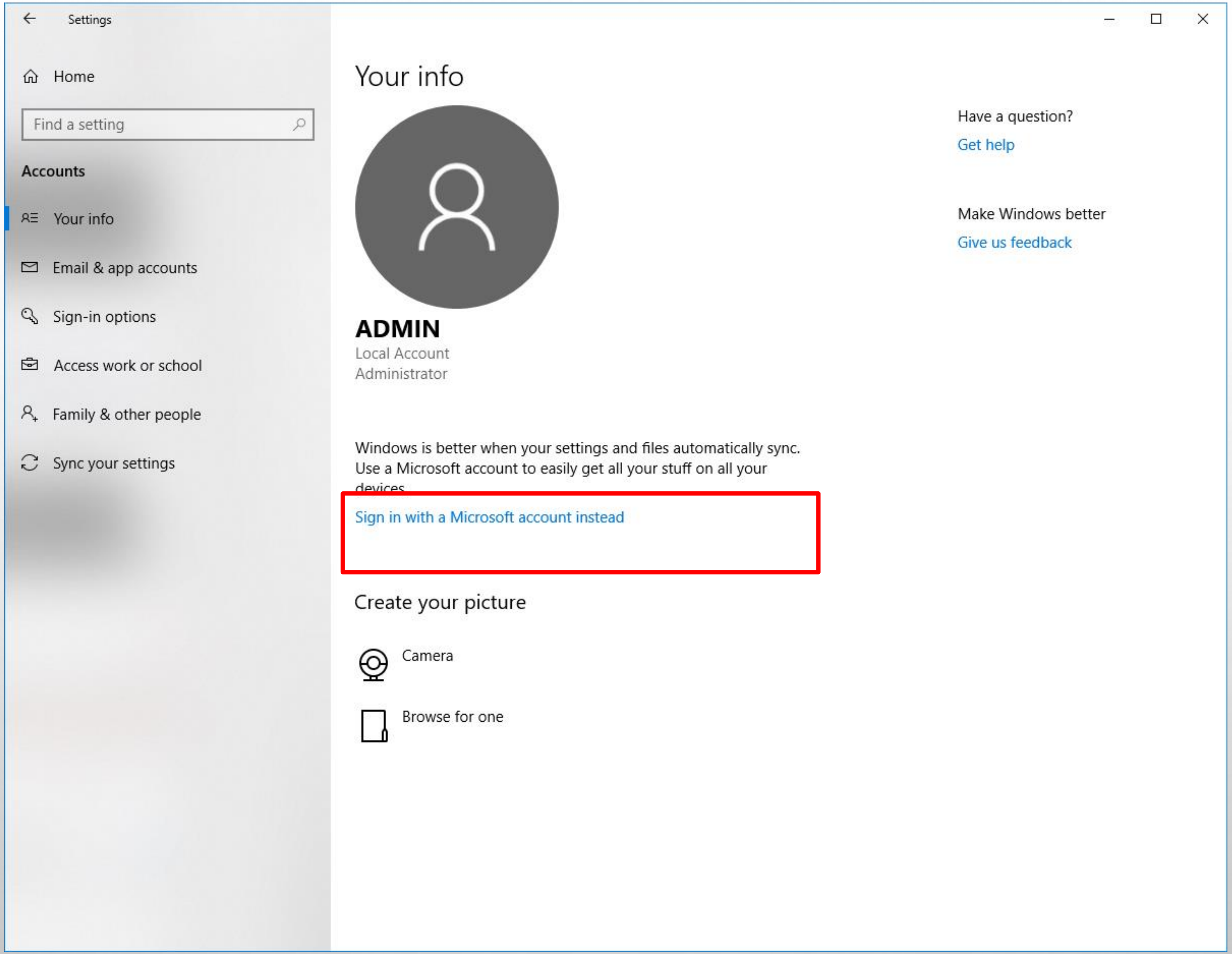
☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled


Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup



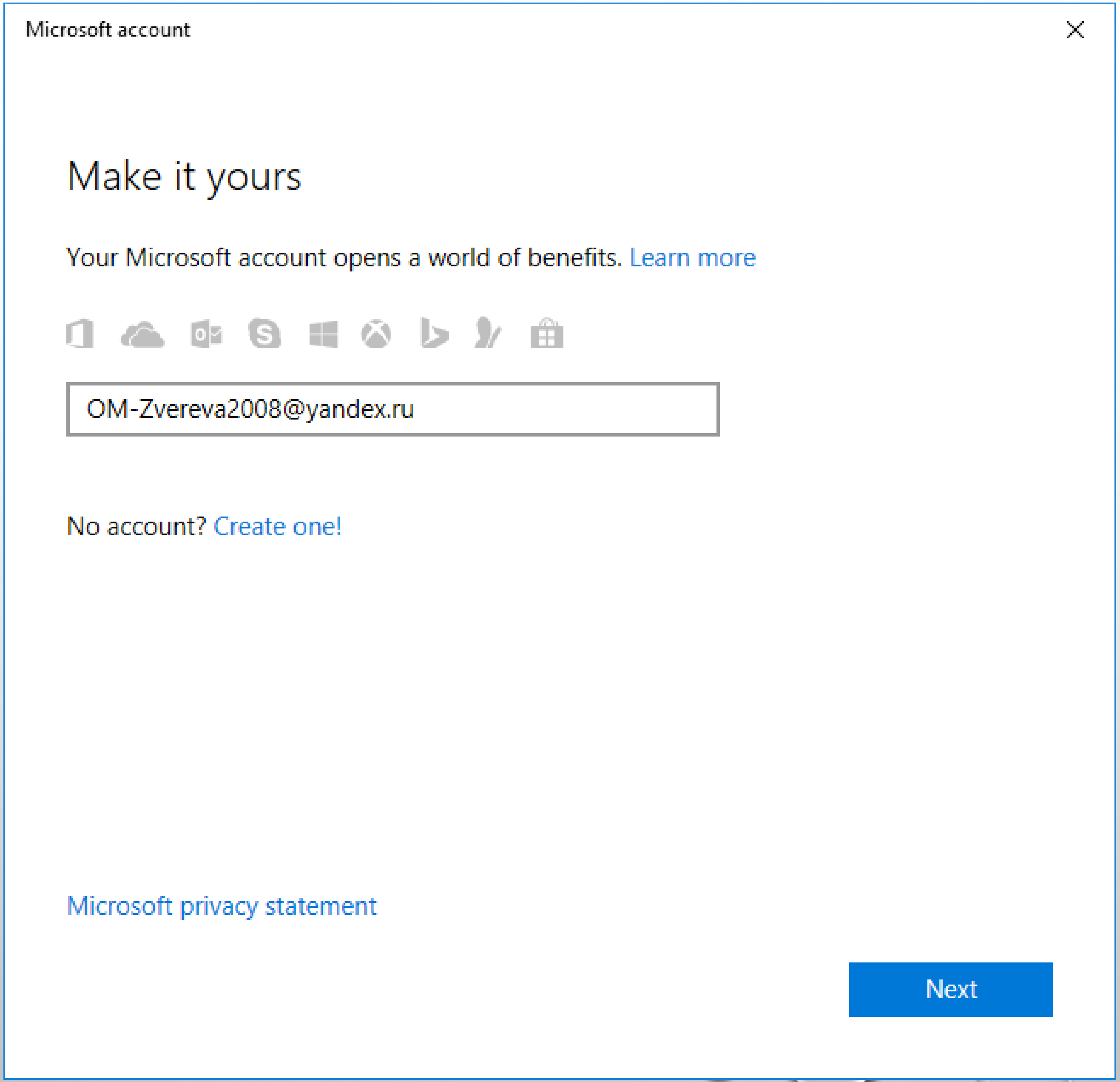
Your info

ADMIN
Local Account
Administrator

Windows is better when your settings and files automatically sync. Use a Microsoft account to easily get all your stuff on all your devices.

Sign in with a Microsoft account instead

Create your picture



Microsoft account

Make it yours

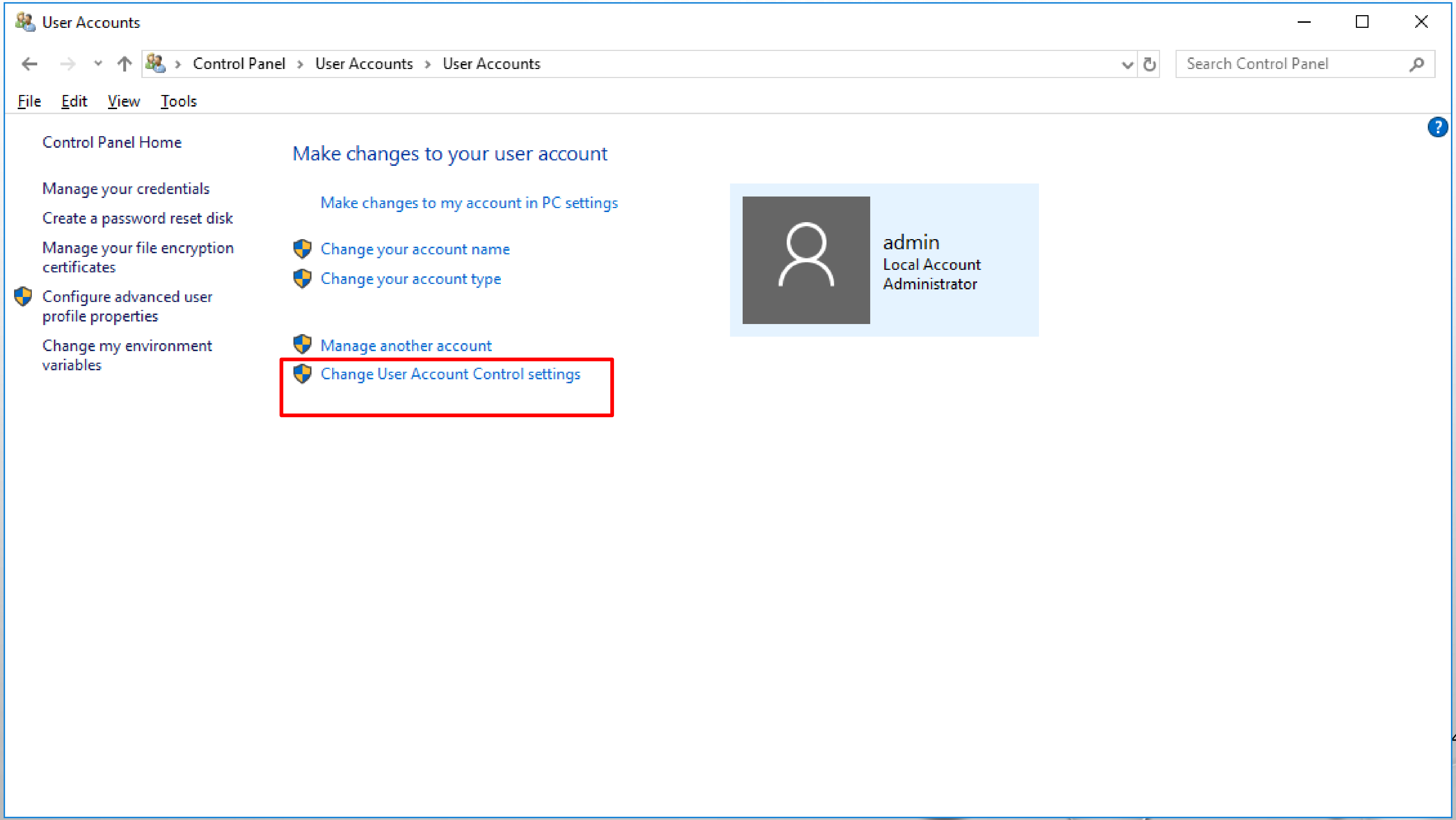
Your Microsoft account opens a world of benefits. Learn more

OM-Zvereva2008@yandex.ru

No account? Create one!

Microsoft privacy statement

CONTROL PANEL\USER ACCOUNTS



User Accounts

Control Panel > User Accounts > User Accounts

Search Control Panel

File Edit View Tools

Control Panel Home

Manage your credentials

Create a password reset disk

Manage your file encryption certificates

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Make changes to my account in PC settings

Change your account name

Change your account type

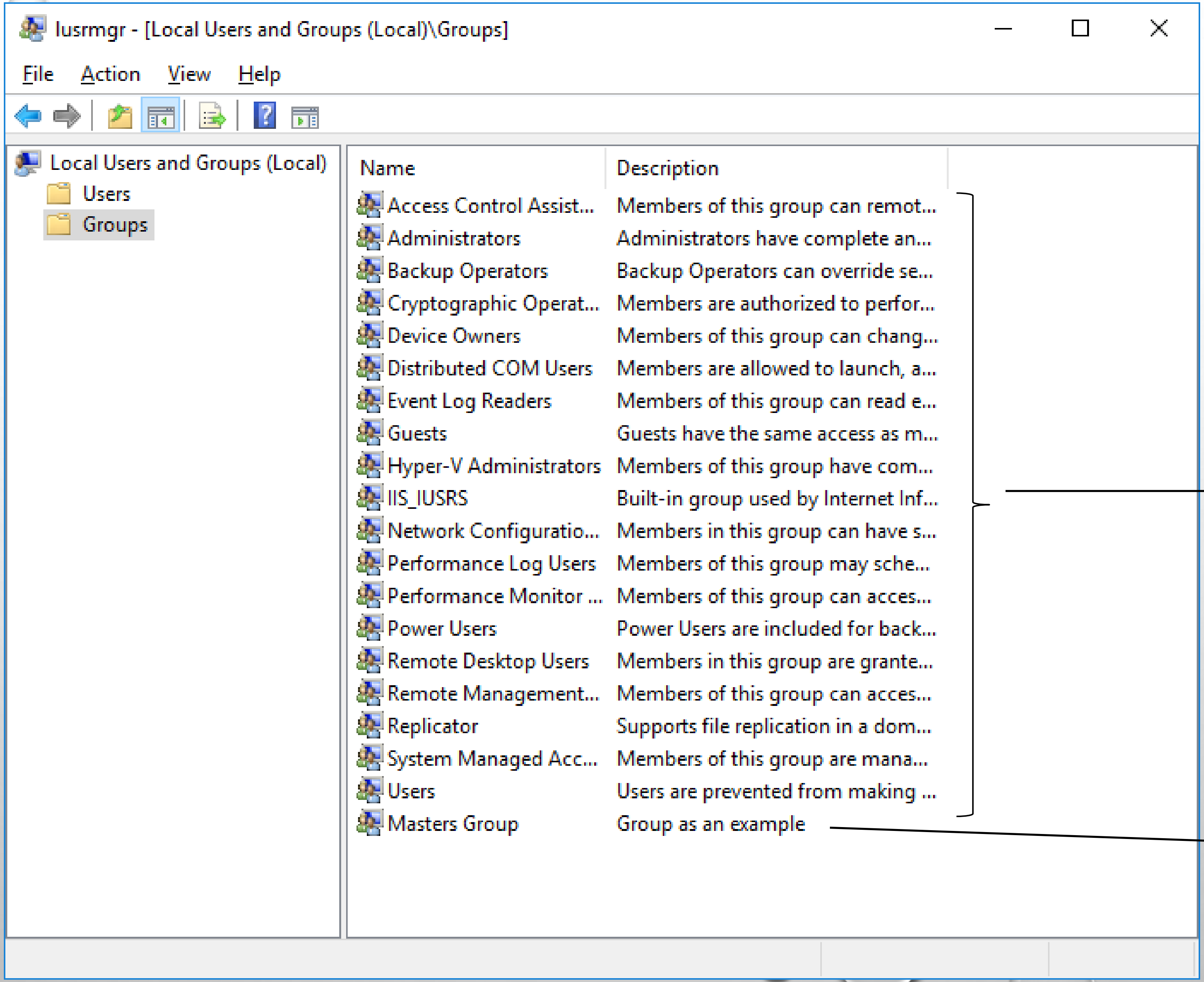
Manage another account

Change User Account Control settings

admin
Local Account
Administrator

GROUPS

- A *LOCAL GROUP* CAN CONTAIN USER ACCOUNTS OR GLOBAL GROUP ACCOUNTS FROM ONE OR MORE DOMAINS.
- A LOCAL GROUP SHARES COMMON PRIVILEGES AND RIGHTS


lusrmgr - [Local Users and Groups (Local)\Groups]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups

Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...
Masters Group	Group as an example

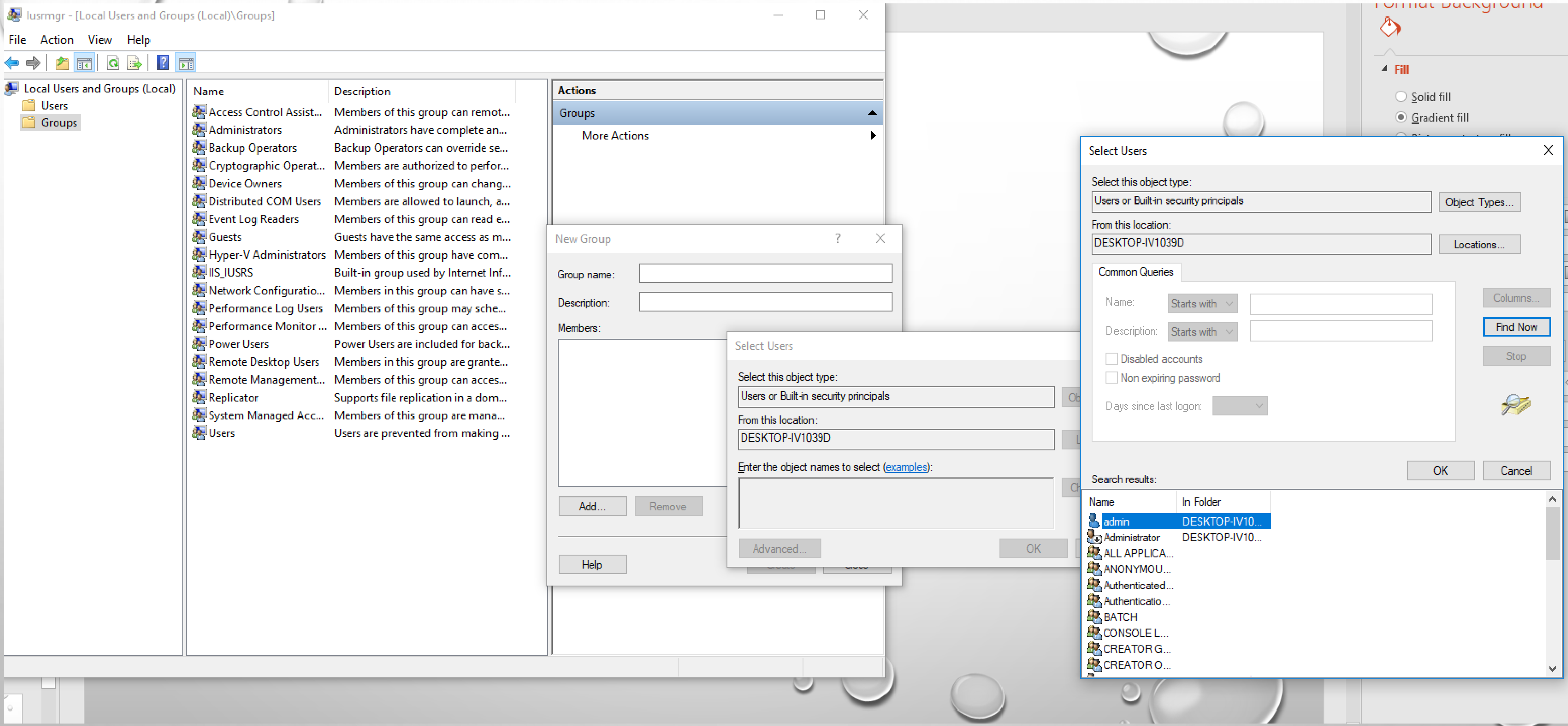
BUILT-IN GROUPS

CREATED GROUP

ADMINISTRATIVE GROUP

ADMINISTRATORS - MEMBERS OF THE ADMINISTRATORS GROUP ON LOCAL COMPUTERS CAN DO ANYTHING ON THAT COMPUTER.

THE LOCAL ADMINISTRATOR ACCOUNT IS A MEMBER OF THIS GROUP, AND THE FIRST ACCOUNT CREATED ON A WINDOWS COMPUTER WHEN IT IS INSTALLED IS ALSO A MEMBER OF THIS GROUP



lusrmgr - [Local Users and Groups (Local)\Groups]

Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...

New Group

Group name:

Description:

Members:

Select Users

Select this object type:
Users or Built-in security principals

From this location:
DESKTOP-IV1039D

Enter the object names to select (examples):

Select Users

Select this object type:
Users or Built-in security principals

From this location:
DESKTOP-IV1039D

Name: Starts with

Description: Starts with

□ Disabled accounts

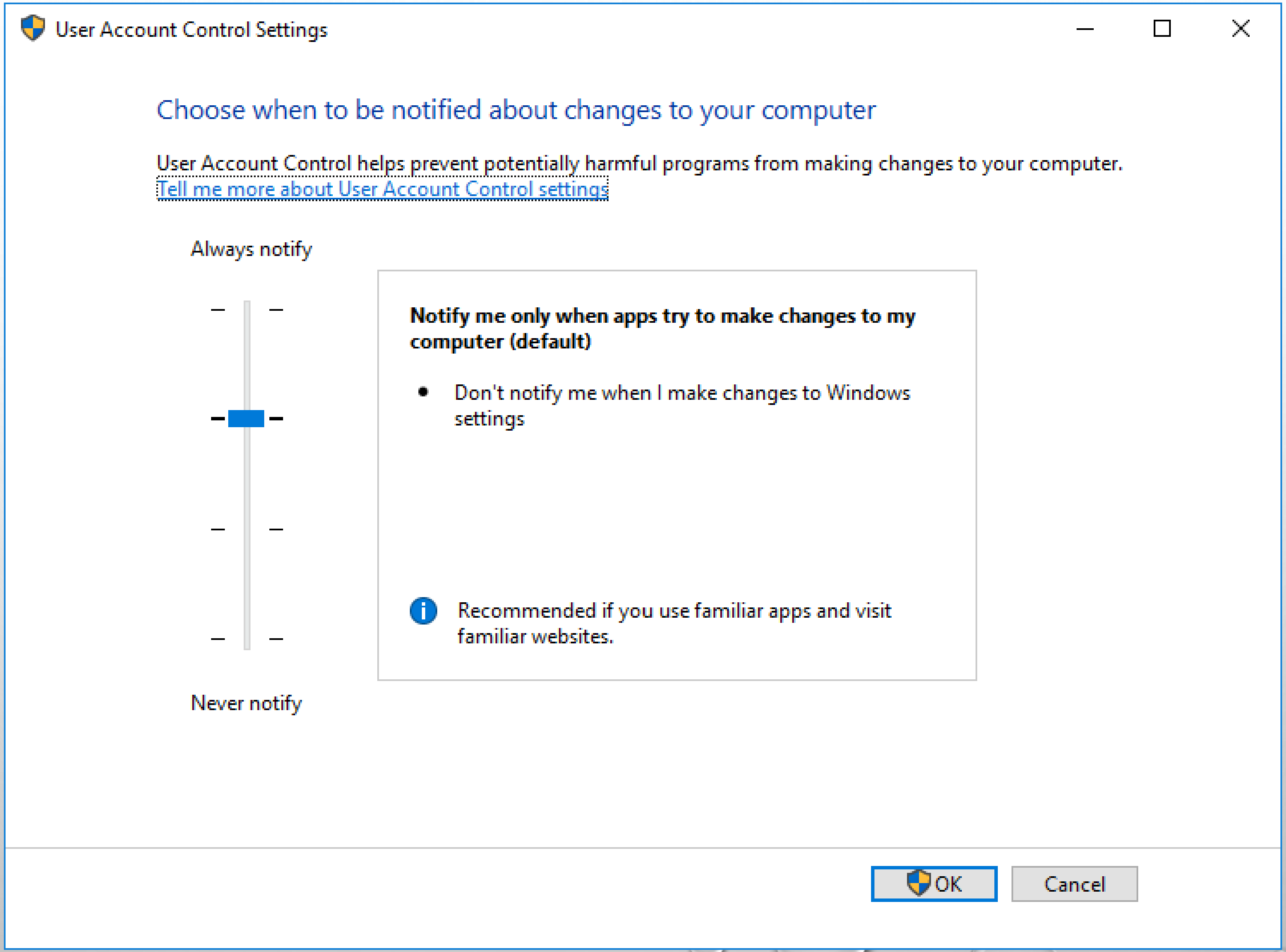
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
admin	DESKTOP-IV10...
Administrator	DESKTOP-IV10...
ALL APPLICA...	
ANONYMOU...	
Authenticated...	
Authenticatio...	
BATCH	
CONSOLE L...	
CREATOR G...	
CREATOR O...	

UAC



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.

PRACTICAL WORK

- TRY TO FIND ALL FILES NECESSARY FOR SUCCESSFUL BOOT PROCESS IN YOUR SYSTEM
- CREATE SEVERAL MMC(S) WITH DIFFERENT SET OF SNAP-IN(S)
- CREATE A NEW USER ACCOUNT WITH THE PASSWORD THAT NEVER EXPIRES
- CREATE NEW GROUP, GIVE IT THE NAME OF YOUR MASTER’S GROUP, INCLUDE SEVERSL USERS AND ONE LOCAL GROUP INTO IT
- INCLUDE THE CREATED USER INTO “ADMINISTRATORS” GROUP
- COULD YOU FIND PARAMETERS OF YOUR COMPUTER (HARDWARE: MAIN MEMORY VOLUME, DISK STORAGE VOLUME, NUMBER AND SIZES OF EXISTING PARTITIONS, OS VERSION)?