# Windows Exam 70-698 Essential Facts

Table of Contents

[Windows Exam 70-698 Essential Facts 1](#_Toc506984508)

[Windows 10 versions 3](#_Toc506984509)

[Minimum hardware requirements 5](#_Toc506984510)

[Upgrade options 5](#_Toc506984511)

[Bcdedit commands for dual booting 5](#_Toc506984512)

[Update servicing options 6](#_Toc506984513)

[Sysprep switches 6](#_Toc506984514)

[ICD switches 7](#_Toc506984515)

[DISM.exe command line commands 7](#_Toc506984516)

[Types of virtual hard disks 8](#_Toc506984517)

[Hyper-V Edit Disk 8](#_Toc506984518)

[File system capabilities 9](#_Toc506984519)

[Microsoft Azure data size availability 9](#_Toc506984520)

[One Drive Subscription 9](#_Toc506984521)

[MMC Modes 10](#_Toc506984522)

[Compact command options 10](#_Toc506984523)

[PowerShell Disk commands 10](#_Toc506984524)

[PowerShell Configuration Commands 11](#_Toc506984525)

[Windows 10 Power Plans 12](#_Toc506984526)

[Power cfg.exe switches 12](#_Toc506984527)

[Windows To Go host requirements 12](#_Toc506984528)

[Folder View Options 13](#_Toc506984529)

[Shared folder options 14](#_Toc506984530)

[ipconfig switches 14](#_Toc506984531)

[Common port numbers 14](#_Toc506984532)

[WinAppDeployCmd.exe commands and switches 15](#_Toc506984533)

[User Experience Virtualization (UE-V) components 15](#_Toc506984534)

[App-V Components 15](#_Toc506984535)

[Configurable user-account options in Control Panel 16](#_Toc506984536)

[Device Guard Protection 16](#_Toc506984537)

[Device Guard PowerShell commands 16](#_Toc506984538)

[Group policy and LGPO setting options 17](#_Toc506984539)

[gpresult switches 17](#_Toc506984540)

[Password policy options 18](#_Toc506984541)

[Account lockout policy options 18](#_Toc506984542)

[Audit policy options 19](#_Toc506984543)

[User Rights Assignment Policy Options 19](#_Toc506984544)

[MSRA (Remote Assistant) command line switches 22](#_Toc506984545)

[Windows 10 Recovery Techniques 23](#_Toc506984546)

## Windows 10 versions

Windows 10 Home

Windows 10 Professional

Windows 10 Enterprise

Windows 10 Education

|  |
| --- |
| **Windows 10 core experience** |
| **Feature** | **Home** | **Pro** | **Enterprise** | **Education** |
| Battery saver | ⚫ | ⚫ | ⚫ | ⚫ |
| Built in ink support | ⚫ | ⚫ | ⚫ | ⚫ |
| Cortana | ⚫ | ⚫ | ⚫ | ⚫ |
| Customisable Start Menu | ⚫ | ⚫ | ⚫ | ⚫ |
| Enterprise level biometric security | ⚫ | ⚫ | ⚫ | ⚫ |
| Fast startup with Hiberboot and InstantGo | ⚫ | ⚫ | ⚫ | ⚫ |
| Hey Cortana hands free activation | ⚫ | ⚫ | ⚫ | ⚫ |
| Native facial and iris recognition | ⚫ | ⚫ | ⚫ | ⚫ |
| Native fingerprint recognition | ⚫ | ⚫ | ⚫ | ⚫ |
| Personal and proactive suggestions | ⚫ | ⚫ | ⚫ | ⚫ |
| Reading view | ⚫ | ⚫ | ⚫ | ⚫ |
| Reminders | ⚫ | ⚫ | ⚫ | ⚫ |
| Search web, device and cloud | ⚫ | ⚫ | ⚫ | ⚫ |
| Snap apps (across screens on different monitors) | ⚫ | ⚫ | ⚫ | ⚫ |
| Snap assist (up to four apps on one screen) | ⚫ | ⚫ | ⚫ | ⚫ |
| Switch from PC to tablet mode | ⚫ | ⚫ | ⚫ | ⚫ |
| Talk or type naturally | ⚫ | ⚫ | ⚫ | ⚫ |
| TPM support | ⚫ | ⚫ | ⚫ | ⚫ |
| Virtual desktops | ⚫ | ⚫ | ⚫ | ⚫ |
| Windows Defender and Windows Firewall | ⚫ | ⚫ | ⚫ | ⚫ |
| Windows Update | ⚫ | ⚫ | ⚫ | ⚫ |

|  |
| --- |
| **Windows 10 business experience** |
| **Feature** | **Home** | **Pro** | **Enterprise** | **Education** |
| Can join Azure Active Directory |  | ⚫ | ⚫ | ⚫ |
| AppLocker |  |  | ⚫ | ⚫ |
| Assigned Access 8.1 |  | ⚫ | ⚫ | ⚫ |
| BitLocker |  | ⚫ | ⚫ | ⚫ |
| BranchCache |  |  | ⚫ | ⚫ |
| Client Hyper-V |  | ⚫ | ⚫ | ⚫ |
| Current Branch for Business |  | ⚫ | ⚫ | ⚫ |
| Device Encryption | ⚫ | ⚫ | ⚫ | ⚫ |
| Device Guard |  |  | ⚫ | ⚫ |
| Direct Access |  |  | ⚫ | ⚫ |
| Domain Join |  | ⚫ | ⚫ | ⚫ |
| Easy Upgrade from Home to Education | ⚫ | ⚫ |  | ⚫ |
| Easy Upgrade from Pro to Enterprise |  | ⚫ | ⚫ |  |
| Enterprise Data Protection |  | ⚫ | ⚫ | ⚫ |
| Enterprise Mode Internet Explorer (EMIE) |  | ⚫ | ⚫ | ⚫ |
| Granular UX Control |  |  | ⚫ | ⚫ |
| Group Policy Management |  | ⚫ | ⚫ | ⚫ |
| Long Term Servicing Branch  |  |  | ⚫ |  |
| Microsoft Passport | ⚫ | ⚫ | ⚫ | ⚫ |
| Mobile Device Management | ⚫ | ⚫ | ⚫ | ⚫ |
| Remote Desktop |  | ⚫ | ⚫ | ⚫ |
| Side loading of line of business apps | ⚫ | ⚫ | ⚫ | ⚫ |
| Start Screen Control with Group Policy |  |  | ⚫ | ⚫ |
| Trusted Boot |  | ⚫ | ⚫ | ⚫ |
| Windows Store for Business |  | ⚫ | ⚫ | ⚫ |
| Windows To Go Creator |  |  | ⚫ | ⚫ |
| Windows Update | ⚫ | ⚫ | ⚫ | ⚫ |
| Windows Update for Business |  | ⚫ | ⚫ | ⚫ |

## Minimum hardware requirements

|  |  |
| --- | --- |
| **Component** | **W10**  |
| **CPU** | **1 GHz or faster** |
| **RAM** | **1GB (32 bit), 2GB (64 bit), extra 2GB for Hyper-V** |
| **Hard disk** | **16 GB (32 bit), 20 GB (64 bit)** |
| **Video adapter** | **DirectX 9 or later with WDDM 1.0 driver** |
| **Optional drive** | **DVD-R/W drive** |
| **Network device** | **Compatible NIC** |

## Upgrade options

|  |  |
| --- | --- |
| **From current edition** | **Windows 10 edition** |
| Windows 7 Starter | Windows 10 Home |
| Windows 7 Home Basic | Windows 10 Home |
| Windows 7 Home Premium | Windows 10 Home |
| Windows 7 Professional | Windows 10 Pro |
| Windows 7 Ultimate | Windows 10 Pro |
| Windows 7 Enterprise | Windows 10 Enterprise |
| Windows Phone 8.1 | Windows 10 Mobile |
| Windows 8.1 Home | Windows 10 Home |
| Windows 8.1 Pro | Windows 10 Pro |
| Windows 8.1 Enterprise | Windows 10 Enterprise |
| Windows 8.1 Pro for Students | Windows 10 Pro |

## bcdedit commands for dual booting

|  |  |
| --- | --- |
| **Command** | **Explanation** |
| /createstore | Creates a new empty boot configuration data store |
| /default | Specifies which OS starts when the timeout expires |
| /deletevalue | Deletes a specified element from a boot entry |
| /displayorder | Shows the display order the boot manager shows the user |
| /export | Exports the contents of the system store into a file |
| /import | Restores the system store using a file previously exported |
| /set | Sets an entry option value |
| /store | Specifies the store to be used |
| /timeout | Specifies the time before the default OS boots  |

## Update servicing options

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servicing option** | **Availability of updates** | **Minimum length of servicing lifetime** | **Key benefits** | **Supported editions** |
| Current branch (CB) | Immediately after first published | Approximately 4 months | New features available as soon as possible | Home, Pro, Education Enterprise |
| Current branch for business (CBB) | Approximately 4 months after first published | Approximately 8months | Provides additional test time | Pro, Education Enterprise |
| Long Term Servicing Branch (LTSB) | Immediately after first published | 10 years | For low change configurations (ATMs, manufacturing systems) | Enterprise LTSB |

## Sysprep switches

|  |  |
| --- | --- |
| **Switch** | **Explanation** |
| /pnp | Forces a mini-setup wizard to start at reboot so that all Plug abd Play devices can be recognised |
| /generalize | Allows sysprep to remove all system, specific data from the Sysprep image . (A checkbox option on the GUI version) |
| /oobe | Initiates the Windows Welcome screen at the next reboot |
| /audit | Initiates in audit mode |
| /nosidgen | Does not generate a new SID. Forces a mini-setup on restart |
| /reboot | Stops and restarts the system |
| /quiet | Runs without confirmation dialogue boxes |
| /mini | Run the mini setup at next reboot |

## ICD switches

|  |  |
| --- | --- |
| **Switch**  | **Description** |
| /CustomizationXML | Identifies the location of the Windows provisioning XML file. This file holds the information for customization assets and settings  |
| /PackagePath | Identifies the location and the built-in provisioning package name where the package will be saved |
| /StoreFile | Identifies a s settings store to be used instead of the default  |
| /MSPackageRoot | Identifies the location of the root directory that holds the Microsoft packages that you downloaded from the Windows portal  |
| /OEMInputXML | Identifies the location of the OEMInput.XML file, which defines a subset if settings based on image type |
| /Variables | Identifies a macro pair separated by a semicolon <name> and <value> |
| Encrypted | Encrypts the provision package and generates a password included in the output |
| Overwrite | Overwrites existing package |
| /? | Help – listing the switches and descriptions |

## DISM.exe command line commands

|  |  |
| --- | --- |
| **Command** | **Description** |
| /Add-Driver | Adds third party driver packages to an offline image |
| /Get-CurrentEdition | Displays the edition of the specified image |
| /Get-Drivers | Displays basic information about driver packages. Default is third party only |
| /Get-DriverInfo | Displays detailed information about a specific driver package |
| /Get-Help /? | Displays information about the options and the arguments |
| /Get-TargetEditions | Displays a list of Windows editions that an image can be changed to  |
| /Remove-Driver | Removes third party drivers from an offline image |
| /Set-ProductKey:<productKey> | Can only be used to enter the product key for the current edition in an offline Windows image |

|  |  |  |
| --- | --- | --- |
| **Type** | **Description** | **When to use it** |
| Dynamically expanding | Expands on demand to maximum set during creation | To preserve host hard disk space. When you don’t know the size.Slowest type |
| Fixed size | Fixed at creation. Allocates all the space immediately. | Next fastest after pass through.  |
| Differencing | A child disk associated with a parent. The parent holds the master image and the differencing disk only stores the differences from the parent. Suitable for multiple VMs with the same OS | In test environments, not for production environments |
| Physical (or pass through) | VM gets direct access to the physical disk. Drive not available for other guest systems. Highest performance | Use in high end data centres to provide optimum performance. Also used for failover.  |

## Types of virtual hard disks

## Hyper-V Edit Disk

|  |  |
| --- | --- |
| **Action** | **Description** |
| Compact | Reduces the size of a dynamically expanding or differencing disk by removing blank spaces from deleted files |
| Convert | Converts a dynamically expanding disk to a fixed disk or vice versa |
| Expand | Increases the size of a dynamically expanding disk or a fixed disk |
| Merge | Merges the changes from a differencing disk into the parent or another differencing disk |
| Reconnect | Reconnects a differencing disk if it cannot find its parent |

## File system capabilities

|  |  |  |
| --- | --- | --- |
| **Feature** | **Fat32** | **NTFS** |
| Supporting operating systems | All Windows operating systems above Windows 95 | Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008/2008 R2 and Windows Server 2012/2012R2 |
| Long filename support | Yes | Yes |
| Efficient use of disk space | Yes | Yes |
| Compression support | No | Yes |
| Encryption support | No | Yes |
| Support for local security | No | Yes |
| Support for network security | Yes | Yes |
| Maximum volume size | 32GB | 16TB with 4KB clusters or 256 TB with 64KB clusters |

## Microsoft Azure data size availability

|  |  |
| --- | --- |
| **Operating System** | **Maximum Size of Data Store** |
| Windows Server 2012 or above | 54,000 GB |
| Windows 8 or above | 54,000 GB |
| Windows Server 2008, 2008 R2 | 1,700 GB |
| Windows 7 | 1,700 GB |

## One Drive Subscription

|  |  |  |
| --- | --- | --- |
| **Type** | **Amount of storage** | **Subscription (at 02/2018)** |
| Office 365 Home + Premium OneDrive  | 1TB per user (5TB total) | £79.99 per year |
| Office 365 Personal + Premium OneDrive | 1 TB | £59.99 per year |
| One Drive 50GB | 50 GB | £1.99 per month |
| One Drive Basic | 5 GB | Free |

## MMC Modes

|  |  |
| --- | --- |
| **Console mode** | **Description** |
| Author mode | Allows use of all MMC functions |
| User mode – full access | Gives users full access to window-management commands but they cannot add or remove snap-ins or change console properties |
| User mode – limited access, multiple window | Allows users to create new windows but not close any existing windows. Users can access only the areas of the console tree that were visible when the console was last saved. |
| User mode – limited access, single window | Users can access only the areas of the console tree that were visible when the console was last saved, and they cannot create new windows |

## Compact command options

|  |  |
| --- | --- |
| **Command** | **Description** |
| /C | Compresses the specified file or folder |
| /U | Uncompresses the specified file or folder |
| /S:dir | Specifies which folder should be compressed or uncompressed |
| /A | Displays any files that have hidden or system file attributes |
| /I | Indicates that errors should be ignored |
| /F | Forces a file to be compressed |
| /Q | Used with reporting to report only critical information |
| /? | Displays help |

## PowerShell Disk commands

|  |  |
| --- | --- |
| **PowerShell Command** | **Description** |
| Add-PhysicalDisk | Add a disk to a storage pool |
| Clear-Disk | Removes all partition information and erases all data on a disk |
| Connect-VirtualDisk | Administrators use this command for connecting a disconnected virtual disk to a computer using Storage Spaces |
| Disconnect-VirtualDisk | Disconnects a virtual disk from a computer |
| Dismount-DiskImage | Administrators use this command to dismount  |
| Format-Volume | Format the volume on a drive  |
| Get-Disk | Allows the OS to see a disk |
| Get-DiskImage | Allows the OS to see a disk image |

|  |  |
| --- | --- |
| **PowerShell Command** | **Description** |
| Get-FileIntegrity | Checks the integrity information for a file on an ReFS volume |
| Get-Partition | Get a list of the partitions on the system’s disks |
| Get-PhysicalDisk | Lists all available physical disks |
| Get-VirtualDisk | Allows an OS to see a virtual disk |
| Get-Volume | Shows the volume object |
| Initialize-Disk | Initialises a disk for first time use |
| Invoke-Command | Allows remote execution of PowerShell commands on another system |
| Mount-DiskImage | Mounts a VHD or ISO image to appear as a normal disk |
| New-Partition | Creates a new partition on an existing disk |
| New-StoragePool | Creates a new storage pool of physical disks |
| New-VirtualDisk | Creates a new virtual disk in the specified storage pool |
| New-Volume | Creates a new volume |
| Remove-Partition | Removes a partition |
| Remove-PhysicalDisk | Removes a disk |
| Remove-VirtualDIsk | Removes a virtual disk |
| Repair-VirtualDisk | Repairs a virtual disk |
| Repair-Volume | Repairs a volume |
| Resize-Partition | Resizes a partition |
| Set-Partition | Set partition attributes, such as setting active |
| Set-PhysicalDisk | Set disk attributes |
| Set-StoragePool | Modify the properties of the specified storage pool |
| Set-Volume | Set or change the file system label of a volume |
| Update-Disk | Update cached information about a specified disk |
| Update-StoragePool | Updates the metadata of a Windows Server 2012 R2 Storage pool |

## PowerShell Configuration Commands

|  |  |
| --- | --- |
| **PowerShell Command** | **Description** |
| Clear-EventLog | Deletes all entries from event logs on local or remote computers |
| Debug-Process | Allows debugging processes on a local computer |
| Get-ComputerInfo | Returns a computer’s system information |
| Get-EventLog | Finds an event in a specific event log |
| Get-Service | Finds a service on a Windows 10 system |
| Get-TimeZone | Gets the system’s time zone |
| New-EventLog | Creates a new event log |
| New-Service | Creates a new service |
| Remove-EventLog | Deletes an event log |
| Rename-Computer | Renames a computer |
| Restart-Computer | Reboots the system |
| Restart-Service | Restarts a service |
| **PowerShell Command** | **Description** |
| Resume-Service | Resumes a service |
| Set-TimeZone | Sets the system’s time zone |
| Start-Process | Starts a process |
| Start-Service | Starts a service |
| Stop-Computer | Shuts down the computer |
| Stop-Service | Stops a service |
| Test-Connection | Sends a ping to test NIC adapter settings |
| Write-EventLog | Writes an event to an event log |

## Windows 10 Power Plans

|  |  |  |  |
| --- | --- | --- | --- |
| **Power Plan** | **Turn off display** | **Put computer to sleep** | **Turn hard disks off** |
| Balanced | After 20 minutes | 1 hour |  |
| Power saver | After 20 minutes | 1 hour | After 20 minutes |
| High performance | After 20 minutes | Never |  |

## Power cfg.exe switches

|  |  |
| --- | --- |
| **Switch** | **Decription** |
| -change | Changes a setting in the current power scheme |
| -changename | Changes the name and description of a power scheme |
| -delete | Deletes the power scheme of the GUID specified |
| -deletesetting | Deletes a power setting |
| -energy | Identifies issues with the power scheme and displays in HTML format |
| -list | Shows all the power schemes in the current user’s environment |
| -query | Shows the contents of a power scheme |
| -qh | Shows the contents of a power scheme, including hidden content |
| -waketimers | Enumerates the wake timers. If enabled, when the wake timer expires, the system will wake from sleep or hibernation |

## Windows To Go host requirements

|  |  |
| --- | --- |
| **Item** | **Requirement** |
| Boot process | Capable of USB boot |
| Firmware | USB boot enabled (PC’s certified for Windows 7 or later can be configured to boot from USB) |
| Processor architecture | Must support the image on the Windows To Go drive |
| External USB hubs | Not supported, must connect directly to host machine |
| Processor | 1GHz or faster |
| RAM | 2 GB or greater |
| Graphics | DirectX 9 with WDDM 1.2 or greater driver |
| USB port | USB 2.0 port or greater |

## Folder View Options

|  |  |  |
| --- | --- | --- |
| **Option** | **Description** | **Default** |
| Always Show Icons, Never Thumbnails | Shows icons, not thumbnails for files | Not selected |
| Always Show Menus | Shows the File, Edit, View, Tools and Help menus when browsing for files | Not selected |
| Display File Icon On Thumbnails | Displays the file icon on thumbnails | Selected |
| Display File Size Information In Folder Tips | Specifies whether the file size is automatically displayed when hovering over a folder | Selected |
| Display The Full Path In The Title Bar (Classic Theme Only) | Displays the full path rather than just the current folder.Eg C:\Word\Docs and not just Docs | Not selected |
| Hidden Files And Folders | Displays items with the Hidden attribute | Don’t show Hidden Files, Folders and Drives |
| Hide Empty Drives | Prevents empty drives in the computer folder being displayed | Selected |
| Hide Extensions For Known File Types | File extensions for known file types (such a .doc or .exe) are not shown  | Selected |
| Hide Protected Operating System Files (Recommended) | OS files are not shown by default, protecting them from modification or deletion by user | Selected |
| Launch Folder Windows In A Separate Process | Opens the windows in separate parts of memory, slower but more stable.  | Not selected |
| Show Drive Letters | If disabled, only the drive name is shown | Selected |
| Show Encrypted Or Compressed NTFS Files In Colour | Displays these files in an alternate colour in a folder window | Selected |
| Show Pop-Up Description For Folder And Desktop Items | Determines if a pop-up tooltip is displayed when mouse hovers over files and folders | Selected |
| Show Preview Handlers In Preview Pane | Shows the contents of files in the preview pane | Selected |
| Use Check Boxes To Select Items | Adds a check box next to each file, allowing one or more to be selected | Not selected |
| Use Sharing Wizard (recommended) | Allows sharing folders using a simplified method | Selected |
| When Typing Into List View | Selects whether text is automatically typed into the search box or whether the typed item is selected in the view | Select The Typed Item In The View |

## Shared folder options

|  |  |
| --- | --- |
| **Option** | **Description** |
| Share This Folder | Makes the folder available through local and network access |
| Share Name | A descriptive name for the share |
| Comments | Additional information about the share |
| Limit The Number Of Simultaneous Users To | The maximum number of simultaneous connections to the share (Maximum 20) |
| Permissions | How users  |
| Caching | How folders are cached when the folder is offline |

## ipconfig switches

|  |  |
| --- | --- |
| **Switch** | **Description** |
| /? | Shows all the help options  |
| /all | Shows all the information about the IP configuration |
| /release | Releases an IPv4 address assigned through DHCP |
| /release6 | Releases an IPv6 address assigned through DHCP |
| /renew | Renews an IPv4 address through DHCP |
| /renew6 | Renews an IPv6 address through DHCP |
| /flushdns | Purges the DNS resolver cache |
| /registerdsn | Refreshes DHCP leases and re-registers DNS names |
| /displaydns | Displays the contents of the DNS resolver cache |
| /showclassID | Lists the DHCP class IDs allowed by the computer |
| /setclassID | Modifies the DHCP class ID |

## Common port numbers

|  |  |
| --- | --- |
| **Port number** | **Associated service or application** |
| 20 | FTP data |
| 21 | FTP control |
| 22 | Secure shell (SSH) |
| 23 | Telnet |
| 25 | SMTP |
| 53 | DNS |
| 67/68 | DHCP/BOOTP |
| 80 | HTTP |
| 102 | Microsoft Exchange Server |
| 110 | POP3 |
| 443 | HHTPS (HTTP with SSL) |

## WinAppDeployCmd.exe commands and switches

|  |  |
| --- | --- |
| **Command/Switch** | **Description** |
| devices | Shows the list of available network devices |
| install | Installs a Windows 10 application package to a target device |
| list | Shows the list of apps installed on a specified target device |
| uninstall | Uninstalls an application from the target device |
| update | Updates an already installed application |
| -f (file) | Shows the file path for the application package to install, update or uninstall |
| -h (help) | Shows all the commands, options and arguments for the tool |
| -ip | Specifies an IP address for a target device |

## User Experience Virtualization (UE-V) components

|  |  |
| --- | --- |
| **Component** | **Description** |
| UE-V agent | The UE-V agent gets installed on every Windows OS system that you want to synchronise settings with. The agent observes all of the applications and settings for the OS |
| Settings package | UE-V agents take all of the settings and applications on a system and turn them into an application package. They are created locally and then copied to a shared network location  |
| Settings storage share | A network share for all the settings packages. The UE-V agent verifies the share configuration and then creates a hidden system folder for the user’s setting.  |
| Settings location templates | XML templates are used to synchronise the application and settings files. UE-V contains default templates but new ones can be created.  |
| Windows apps list | The Windows apps list is used to determine which apps get synchronised.  |

## App-V Components

|  |  |
| --- | --- |
| **Component** | **Description** |
| App-V Management Server | Allows management of App-V infrastructure. Set up virtual applications to the App-V Desktop Client and Remote Desktop Services Client |
| App-V Publishing Server | Streams virtual applications and allows access to them |
| App-V Desktop Client | Accesses virtual applications. Manages environments and employee specific settings  |
| App-V Remote Desktop Services (RDS) Client | Allows RDS Host servers to work with desktop client for shared desktop sessions. Permits tablets that can’t run the app to run it remotely |
| App-V Sequencer | Converts normal apps to virtual apps |
| Disconnected Operation Mode | Allows App-V Desktop Clients to run offline |

## Configurable user-account options in Control Panel

|  |  |
| --- | --- |
| **Option** | **Explanation** |
| Change your password | Change user’s password |
| Change Your Account Name | Renames the account |
| Change Your Account Type | Switch between standard and administrator account types |
| Manage Another Account | Configures other accounts on the W10 machine |
| Change User Account Control Settings | Sets level of notifications displayed on pop ups |
| Manage Your Credentials | Sets up credentials for web sites and computers |
| Manage Your File Encryption Certificates | Manages the certificates |
| Configure Advanced User Profile Properties | Goes to User’s Profile dialogue box |
| Change My Environment Variables | Goes to Environment Variables dialogue box |

## Device Guard Protection

|  |  |
| --- | --- |
| **Security threat** | **Device Guard Feature** |
| Boot attacks | UEFI Secure Boot – locks down settings |
| Control of kernel | Virtualisation based security (VBS) – guards the Hyper-V hypervisor |
| Direct Memory Access (DMA) attacks | VBS evaluates memory usage |
| New malware | Whitelist policy to block unlisted code |
| Unassigned code | Prevents unsigned code running. Can cause problems for unsigned line of business (LOB) apps  |

## Device Guard PowerShell commands

|  |  |
| --- | --- |
| **PowerShell command** | **Description** |
| Add-SignerRule | Create a signer rule and add to a policy |
| ConvertFrom-CIPolicy | Convert an .xml file into a binary format containing code integrity policies |
| Get-CIPolicy | View the rules in a code integrity policy |
| Get-CIPolicyIdInfo | View code integrity policy information  |
| Get-SystemDriver | View drivers on a system |
| Merge-CiPolicy | Merge rules of several code integrity policy files  |
| New-CIPolicy | Create a code integrity policy as an .XML file |
| New-CIPolicyRule | Create code integrity policy rules for drivers |
| Set-CIPolicyIdInfo | Modify the name and Id of a code integrity policy |
| Set-CIPolicyVersion | Modify the version number of a policy |
| Set-HCVIOptions | Change hypervisor code integrity options for a specific policy |
| Set-RuleOption | Modify the rule options in a code integrity policy |

## Group policy and LGPO setting options

|  |  |
| --- | --- |
| Group policy setting | Available for LGPO |
| Software installation | No  |
| Remote Installation Services | Yes |
| Scripts | Yes |
| Printers | Yes |
| Security settings | Yes |
| Policy-based QOS | Yes |
| Administrative templates | Yes |
| Folder redirection | No |
| Internet Explorer configuration | Yes |

## gpresult switches

|  |  |
| --- | --- |
| **Switch** | **Explanation** |
| /F | Forces gpresult to override the filename specified in the /X or /H command |
| /H | Saves the report in HTML format |
| /P | Specifies the password for a given user context |
| /R | Displays the RSoP summary data |
| /S | Specifies the remote system to connect to |
| /U | Specifies the user context under which the command is executed |
| /V | Specifies that verbose information should be displayed  |
| /X | Saves the report in XML format |
| /Z | Specifies that super-verbose information should be displayed |
| /? | Shows all the gpresult switches |
| /scope | Specifies whether the user or computer settings are displayed |
| /User | Specifies the username for which RS0P data is to be displayed |

## Password policy options

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy** | **Description** | **Default** | **Minimum** | **Maximum** |
| Enforce password history | Keeps track of user’s passwords | Remember 0 | Remember 0 | Remember 24 |
| Maximum password age | Maximum number of days a user can keep a password | Keep for 42 days | Keep for 1 day | Keep for 999 days |
| Minimum password age | How long can a password be kept before it can be changed | 0 days (must be changed immediately) | 0 days (must be changed immediately | 998 days |
| Minimum password length | Minimum number if characters the password must contain  | 0 (no password required) | 0 (no password required) | 14 characters |
| Password must meet complexity requirements | Password must meet minimum level of complexity  | Disabled | No minimum  | No maximum |
| Store passwords using reversible encryption | Specifies higher level of encryption | Disabled  | No minimum  | No maximum |

## Account lockout policy options

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy | Description | Default | Minimum | Maximum |
| Account lockout duration | How long the account is locked if the account lockout threshold is reached | Disabled (30 minutes if the Account Lockout Threshold is enabled)  | Disabled (30 minutes if the Account Lockout Threshold is enabled) | 99,999 minutes |
| Account Lockout Threshold | Number of invalid attempts before account is locked out | 0 (Disabled account will not be locked) | 0 (Disabled account will not be locked) | 999 attempts |
| Reset Account Lockout Counter After | How long counter will remember unsuccessful logon attempts | Disabled (if Account Lockout Threshold is enabled, 30 minutes) | Disabled. If enabled, must be equal or less than the Account Lockout Duration | 99,999 minutes |

## Audit policy options

|  |  |
| --- | --- |
| **Policy** | **Description** |
| Audit account logon events | Tracks users log on or off (to local machine or domain) |
| Audit account management | Tracks user and group account creation, deletion, password changes |
| Audit directory service access | Tracks directory service access |
| Audit logon events | Audits events such as running logon scripts, accessing roaming profiles, accessing a server |
| Audit object access | Audits access to files, folder, printers |
| Audit policy change | Tracks changed to audit policies, trust policies, user rights assignment policies |
| Audit privilege use | Tracks users exercising a user right |
| Audit process tracking | Tracks events such as activating a program, accessing an object, exiting a process |
| Audit system events | Tracks events such as shutdown, restart, security events |

## User Rights Assignment Policy Options

|  |  |
| --- | --- |
| **Right** | **Description** |
| Access credential manager as a trusted caller | Used to backup and restore Credential Manager |
| Access this computer from a network | Allows a user to access the computer from the network  |
| Act as part of the operating system | Allows low level authentication services to authenticate as any user |
| Add workstations to domain | Allows a user to create a user account on the domain  |
| Adjust memory quotas for a process | Configure how much memory can be used by a process |
| Allow logon locally | Allows a user to log on at the physical computer |
| Allow log on through remote desktop services | Gives permission to logon through RDS |
| Back up files and directories | Allows backup regardless of file and directory permissions |
| Bypass traverse tracking | Allows pass through and traverse of a directory even if the user does not have permission  |
| Change the system time | Allows change of date and time |
| Change the time zone | Allows change of time zone |
| Create a pagefile | Create or change the size of a page file |
| Create a token object | Allows a process to create a token if the process uses an internal API to create the token |
| Create global objects | Allows a user to create global objects when connected using Terminal Server |
| Create permanent shared objects | Create directory objects through Object Manager |
| Create symbolic links | Allows a user to create symbolic links |
| Debug programs | Allows a user to attach a debugging program to any process |
| Deny access to this computer from the network | Denies specific users or groups access to this computer from the network. Overrides the Access This Computer From The Network policy for accounts present in both policies  |
| Deny logon as a batch job | Denies specific users or groups from logging on as a batch file. Overrides Logon as a batch job for accounts present in both policies |
| Deny logon as a service | Denies specific users or groups from logging on as a service. Overrides Logon as a service for accounts present in both policies |
| Deny logon locally | Denies specific users or groups access locally to the computer. Overrides Logon locally for accounts present in both policies |
| Deny logon through terminal services | Specifies user is not able to logon through terminal services |
| Enable computer and user accounts to be trusted for delegation | Allows a user or computer trusted for delegation to access resources on another computer using delegated credentials  |
| Force shutdown from a remote system  | Allows shutdown by a user on a remote network location |
| Generate security audits | Allows users, groups or processes to make entries in the security log |
| Impersonate a client after authentication | Enables programs running on behalf of a user to impersonate a client |
| Increase a process working set | The working set of a process is the current set of pages in virtual address space residing in physical memory. This setting allows you to increase the size of the process working set |
| Increase scheduling priority | Allows a process to increase or decrease the priority that is assigned to another process.  |
| Load and unload device drivers | Allows a user to dynamically unload and load device drivers. Does not apply to plug and play drivers. |
| Lock pages in memory | Allows an account to create a process that only runs in physical RAM., preventing it from being paged.  |
| Log on as a batch job | Allows a process to log on to the system and run a file that contains one or more operating system commands |
| Log on as a service | Allows a service to log on in order to run |
| Manage auditing and security log | Allows a user to enable object access auditing for files and other Active Directory objects. This right does not allow a user to enable general object access auditing in the Local Security Policy  |
| Modify an object label | Allows the user to change the integrity level of files, folders or other object |
| Modify firmware environment variables | Allows a user to install or upgrade Windows. Also allows a user or process to modify the firmware environment variables stored in NVRAM of non-x86 based computers. It does not affect the modification of system environment variables or user environment variables  |
| Perform volume maintenance tasks | Allows a user to perform volume maintenance tasks such as defrag and error checking |
| Profile single process | Allows a user to monitor non-system processes through performance monitoring tools  |
| Profile system performance | Allows a user to monitor system processes through performance monitoring tools |
| Remove computer from docking station | Allows a user to undock a laptop through the Windows 10 user interface |
| Replace a process level token | Allows a process, such as task scheduler, to call an API to start another service |
| Restore files and directories | Allows a user to restore files and directories regardless of file and directory permissions |
| Shut down the system  | Allows the user to shutdown locally |
| Synchronise directory service data | Allows a user to synchronise Active Directory data |
| Take ownership of files or other objects | Allows a user to take ownership of system objects such as files, folders, printers and processes.  |

## MSRA (Remote Assistant) command line switches

|  |  |  |
| --- | --- | --- |
| **Switch** | **OS availability** | **Functionality** |
| /? | Vista and above | Displays the help option |
| /novice | Vista and above | Starts RA at the Invite screen |
| /expert | Vista and above | Starts RA at the Help Someone screen |
| /offerRA *ip* | *computer* | Vista and above | Starts RA at the Expert Initiated screen or with the options, by automatically initiating with the novice user (used with Group Policy configured in an enterprise environment) |
| /email *password* | Vista and above | Creates an email invitation to be sent to an expert user to request assistance using the novice user’s default email program. A random password will be generated and needs to be conveyed to the expert, or a password can be specified with the password option and conveyed to the expert |
| /saveasfile *path password* | Vista and above | Creates an file invitation to be sent to an expert user to request assistance using the novice user’s default email program. A random password will be generated and needs to be conveyed to the expert, or a password can be specified with the password option and conveyed to the expert |
| /openfile | Vista and above | Used to open the invitation file sent to the expert. Can be local or on a network share. Needs the password sent to open. |
| /geteasyhelp | Windows 7 and above | Starts a novice user’s Remote Assistance session using Easy Connect. Presents the password to convey to the expert user |
| /offereasyhelp | Windows 7 and above | Starts an expert user’s Remote Assistance session using Easy Connect. Presents the expert user with the screen to enter the password from the novice user |
| /getcontacthelp *address* | Windows 7 and above | Re-establishes a Remote Assistance session from a novice user’s machine to the address from the previous session. The address is in the RAContactHistory.xml file as a 20 byte hex string with a .RAContact extension |
| /offercontacthelp *address* | Windows 7 and above | Re-establishes a Remote Assistance session from an expert user’s machine to the address from the previous session. The address is in the RAContactHistory.xml file as a 20 byte hex string with a .RAContact extension |

## Windows 10 Recovery Techniques

|  |  |
| --- | --- |
| **Recovery technique** | **When to use** |
| Event Viewer | If the W10 operating system can be loaded through normal or safe mode, look for hints about the problem in the Event Viewer logs.  |
| Safe Mode | Starting point for system recovery. Safe Mode loads the minimum set of services and drivers required for boot. In safe mode you can temporarily disable applications or processes, troubleshoot services or uninstall software |
| Startup Repair Tool  | Use this tool to replace corrupted system files. Does not help with hardware issues.  |
| Backup and Restore | Use this utility to safeguard the computer. Can be used to restore personal files from backup media or restore a complete image.  |
| Driver Rollback | Access from device manager to return the driver to its previous level |
| System Restore | Creates known checkpoints of the system configuration. Allows restore to previous versions.  |