9.1 Windows System Tools

9.1.1 Using Task Manager 19 minute video

9.1.2 Using Control Panel Video 5 minute video

9.1.3 Using Management Consoles 10 minute video

9.1.4 Viewing System Information 11 minute video

9.1.5 System Configuration and DirectX 8 minute video

9.1.6 Using Regedit 9 minute video

9.1.7 Windows Utilities Facts  
You should be familiar with the following Windows tools and utilities.

|  |  |
| --- | --- |
| Tool | Description |
| Control Panel | Use the Control Panel to customize features of devices and to configure how a computer looks and behaves. Use the various applets within the Control Panel to perform configuration tasks for specific features or devices.   * Use Ease of Access to modify the behavior of input and display devices to accommodate users with special needs. * Use Fonts to view, remove, or add to all fonts that are currently installed on the computer. * Use Devices and Printers to view, configure, add, or remove devices such as printers, scanners, and cameras. * Use Clock, Language, and Region settings to configure various settings such as language preference, default currency symbols, and date and time notation. * Use Hardware and Sound to view and configure the current system sound settings, installed audio devices, sound cards, printer settings, and other hardware settings. * Use Windows Firewall to manage network traffic that is allowed or denied through the Windows host-based firewall. * Use Security and Maintenance to review recent error messages and options for resolving issues. * Use System and Security to configure Windows Update, manage Power Options, configure File History, configure Backup and Restore, configure Storage Spaces, and use Administrative Tools. * Use Internet Options within Network and Internet to modify your Internet Properties.   + Use the General tab to modify your browser home page, startup window, tabs, history, and appearance.   + Use the Security tab to determine your security zone and security level.   + Use the Privacy tab to manage website privacy and enable and disable pop-ups and InPrivate Browsing.   + Use the Connections tab to set up Internet connections.   + Use the Programs tab to manage your default browser, add-ons, and other Internet programs and file associations.   + Use the Advanced tab to set and reset advanced browser settings. |
| Task Manager | Use Task Manager to view the current state of the system and running applications. Task Manager is made up of the following tabs:   * Use the Processes tab to view the status of all current applications running on the computer. Use this tab to terminate unresponsive applications. * Use the Performance tab to view system-wide processor, memory, disk, and network statistics. * Use the App History tab to monitor Windows Store apps running on the system. * Use the Startup tab to enable or disable applications that start automatically when the system boots. * Use the Users tab to monitor users currently logged on to the system. * Use the Details tab to view the status of all current processes running on the computer and the CPU and memory resources they use. Use this tab to modify the priority of a process or terminate unwanted processes. * Use the Services tab to view a list of services running on the computer. You can use this tab to start and stop a particular service. |
| Microsoft Management Console (MMC) | The Microsoft Management Console (MMC) is a framework that provides a common user interface for performing system administration tasks. Management of a set of related features is done by adding snap-ins to the console. The MMC provides the shell for running these snap-ins, while the snap-ins provide the details for performing specific management tasks. Microsoft provides snap-ins for managing:   * Local Users and Groups * Device Manager * Disk Management * Print Management * Component Services * Windows Firewall with Advanced Security   To open a blank console, type **mmc** in the Run box. You can then add snap-ins to work with the configuration of your system. The console consists of two or three panes:   * The tree pane (on the left) organizes objects in a hierarchy. * The results pane (in the middle) shows objects and configuration options. * The actions pane (on the right) lists the actions you can take on objects. (The actions pane was new with Windows Vista.)   You can save a console that includes the snap-ins you use most (saved consoles have the **.msc** extension). Microsoft provides a number of preconfigured consoles that include snap-ins for common tasks. |
| Computer Management | Computer Management is a saved MMC console that includes common snap-ins used to manage your computer. Some common ways to start Computer Management include:   * Right-click the Start menu and select **Computer Management**. * Select **Start** > **All Apps** > **Windows Administrative Tools** > **Computer Management**. * Search for **Computer Management**. * Double-click **Computer Management** in Administrative Tools in Control Panel. |
| Event Viewer | Use Event Viewer to view logs about programs, system events, and security. Each entry is listed as a warning, error, or information event. Events are added to the following logs:   * The Application log contains a list of all application-related events such as application installations, un-installations, and application errors. * The System log contains a list of all system-related events such as system modifications, malfunctions, and errors. * The Security log contains a list of all security-related events such as security modifications and user login events.   Additional logs might be added by applications or services. |
| Services | A *service* is a program that processes requests from other applications or users. Services can start automatically and stay constantly running in the background, waiting for service requests. Use the Services snap-in to view and manage running services. The service startup behavior determines how the service is started.   * When set to Automatic, the service is started automatically by Windows when the system boots. * When set to Manual, the service must be manually started. * When Disabled, the service will not run. |
| Performance Monitor | Performance Monitor displays statistics that tell you about the operation of your computer.   * A *counter* identifies a specific statistic, such as % Processor Time or % Disk Free Space. * You can add or remove counters to customize the statistics you can see. * Real-time data are displayed in a graph. * Performance Monitor by itself does not save any data. To save statistics over time, use a data collector set. |
| Reliability Monitor | Reliability Monitor maintains historical data that describe the operating system's stability.   * Overall system stability is given a stability index that ranges from 1 to 10 (10 being the most stable). The stability rating is affected by application, hardware, Windows, and other failures. * Reliability Monitor shows an historical chart that identifies when software installs/uninstalls and failures have occurred. By clicking on a day, you can view the changes to the system that have affected its stability. |
| System Information (Msinfo32.exe) | Use System Information to view hardware and configuration information for your computer. While much of this information is available through other tools, System Information provides a single location for viewing information such as:   * Operating system version * Computer manufacturer, processor type, available memory * Installed devices and drivers used * Running tasks * Applications that run at system startup   You can only view, not modify, configuration settings in System Information. |
| System Configuration Utility (Msconfig.exe) | Use the System Configuration Utility to configure your system to enable optimal troubleshooting and diagnosis of technical issues. Use the System Configuration Utility to:   * Configure startup preferences * Customize bootup configuration * Turn services on or off |
| DirectX Diagnostic Tool (DxDiag) | *DxDiag* is a tool that shows information related to DirectX operation. DirectX is a set of programming interfaces for multimedia (video and audio). DxDiag displays information such as:   * Operating system version * Processor and memory information * DirectX version * Settings and drivers used by display devices * Audio drivers * Input devices (mouse, keyboard, USB) |
| Microsoft Register Server (Regsvr32.exe) | *Microsoft Register Server* is a command-line tool that registers .dll files as command components in the registry. |
| Command Prompt | Use the Command Prompt to execute command-line commands. To open a command prompt,   * On Windows 7, click **Start** and type **cmd** in the Search box. * On Windows 8/10, right-click the Start menu and select **Command Prompt**.   Some commands launched from the command line require elevated privileges to run. If this is the case, run Command Prompt as Administrator. |
| Microsoft Registry Editor (Regedit.exe) | *Microsoft Registry Editor* is a tool for modifying entries in the Windows registry. The registry is a database that holds hardware, software, and user configuration settings.   * Whenever a change is made to preferences, software, hardware, and user-settings, those changes are stored and reflected in the registry. * The preferred method of modifying the registry is to use the applications or management tools that write to the registry. For example, many Control Panel applets make changes to registry settings. * There will be some advanced settings that can only be made by directly editing the registry. |
| Data Sources | You use the ODBC Data Source Administrator to create and manage ODBC data sources. To open the ODBC Data Source Administrator in Windows 7, do the following:   1. On the Start menu, click Control Panel. 2. In Control Panel, click Administrative Tools. 3. In Administrative Tools, click Data Sources (ODBC). |
| Windows Memory Diagnostics | The Windows Memory Diagnostic tests the Random Access Memory (RAM) on your computer for errors. This utility is not included with Windows and must be downloaded from Microsoft's Online Crash Analysis website. |
| Advanced Security | Everyday configuration tasks for the Windows Firewall are completed using the Windows Firewall applet in Control Panel. However, advanced firewall configuration tasks can be performed using an MMC snap-in called *Windows Firewall with Advanced Security*.  Windows Firewall with Advanced Security supports a more granular firewall configuration than can be created using the Windows Firewall applet in Control Panel. For example, it can filter traffic based on parameters such as:   * Source IP address * Destination IP address * Port number * ICMP protocol |

9.1.8 Using System Commands at command prompt 15 minute videos

9.1.9 System Command Facts sheet  
The following table describes the various system commands that can be used in the Windows command prompt:

|  |  |
| --- | --- |
| Command | Description |
| expand | The **expand** command is used to expand compressed .cab files.   * **expand -d *[source\_file]*** displays the contents of the specified .cab file. * **expand *[source\_file]* *[destination]*** expands all the files in the specified .cab file to the chosen destination. * **expand *[source\_file]* f:*[filename]* *[destination]*** extracts a single file from the specified .cab file to the chosen destination. |
| tasklist | The **tasklist** command displays a list of the processes that are currently running on the system. The output of the **tasklist** command includes a process ID (PID) that can be used to end the process. |
| taskkill | The **taskkill** command is used to end running processes.   * **taskkill /in *[image\_name]*** kills the specified process by using its image name (e.g., mspaint.exe). * **taskkill /PID *[pid\_number]*** kills the specified process by using its PID (e.g., 3572).   Sometimes a process will not respond the **taskkill** command. If this is the case, use the **/f** option with the command, which forces the process to close. |
| mstsc | The **mstsc** command is used to establish a remote desktop session with another computer. To run the **mstsc** command, use the following syntax:   * **mstsc /v:*[server\_ip]*** |
| gpupdate | The **gpupdate** command refreshes local and Active Directory-based Group Policy settings, including security settings.   * **/target: { computer | user }** processes only the computer settings or the current user settings. By default, both the computer settings and the user settings are processed. * **/force** ignores all processing optimizations and reapplies all settings. * **/wait: *value*** identifies the number of seconds that policy processing waits to finish. The default is 600 seconds. 0 means "no wait"; -1 means "wait indefinitely." * **/logoff** logs off after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the user logs on, such as user software installation and folder redirection. This option has no effect if there are no extensions called that require the user to log off. * **/boot** restarts the computer after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the computer starts up, such as computer software installation. This option has no effect if there are no extensions called that require the computer to be restarted. * **/?** displays help at the command prompt.   To run the **gpupdate** command, use the following syntax:   * **gpupdate [/target:{computer|user}] [/force] [/wait:value] [/logoff] [/boot]** |
| gpresult | The **gpresult** command displays Group Policy settings and Resultant Set of Policy (RSOP) for a user or a computer.   * **/s *computer*** specifies the name or IP address of a remote computer. (Do not use backslashes.) The default is the local computer. * **/u *domain* \ *user*** runs the command with the account permissions of the user that is specified by user or domain\user. The default is the permissions of the current logged-on user on the computer that issues the command. * **/p *password*** specifies the password of the user account that is specified in the /u parameter. * **/user *target\_user name*** specifies the user name of the user whose RSOP data is to be displayed. * **/scope { user | computer }** displays either user or computer results. Valid values for the /scope parameter are user or computer. If you omit the /scope parameter, gpresult displays both user and computer settings. * **/v** specifies that the output display verbose policy information. * **/z** specifies that the output display all available information about Group Policy. Because this parameter produces more information than the /v parameter, redirect output to a text file when you use this parameter (for example, gpresult /z >policy.txt). * **/?** displays help at the command prompt.   To run the **gpresult** command, use the following syntax:   * **gpresult [/s *computer* [/u *domain*\*user* /p *password*]] [/user *target\_user name*] [/scope {user|computer}] [/v] [/z]** |
| shutdown | The **shutdown** command is used to shutdown local and remote systems. The following options can be used with the **shutdown** command:   * **/i** opens the Remote Shutdown Dialog graphical interface window. * **/l** logs off the current user from the local system. * **/r** shuts down and restarts the local computer. * **/h** causes the computer to hibernate. * **/t *[xx]*** sets a delay time (in seconds) before the computer shuts down. |
| exit | The **exit** command ends the current command prompt session and closes the Command Prompt window. |

If you need further help with a particular command, type ***[command\_name]* /?** to display information about the specified command (typing **help *[command\_name]*** will also display help information).