

CompTIA®

The Official CompTIA

# A+

## Core 2

### Study Guide

Exam 220-1102



**Official CompTIA Content Series** for CompTIA Performance Certifications

# The Official CompTIA® A+® Core 2 Study Guide (Exam 220-1002)

COURSE EDITION: 1.0

## Acknowledgements



James Pengelly, Author  
Pamela J. Taylor, Author  
Brian Sullivan, Media Designer  
Peter Bauer, Content Editor

Thomas Reilly, Vice President Learning  
Katie Hoenicke, Director of Product Management  
James Chesterfield, Manager, Learning Content and Design  
Becky Mann, Senior Manager, Product Development

## Notices

### DISCLAIMER

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

### TRADEMARK NOTICES

CompTIA®, A+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

### COPYRIGHT NOTICE

Copyright © 2018 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit [www.help.comptia.org](http://www.help.comptia.org).

# Table of Contents

<b>Lesson 1: Supporting Operating Systems.....</b>	<b>1</b>
Topic A: Identify Common Operating Systems.....	2
Topic B: Use Windows Features and Tools.....	14
Topic C: Manage Files in Windows.....	31
Topic D: Manage Disks in Windows.....	46
Topic E: Manage Devices in Windows.....	60
 <b>Lesson 2: Installing, Configuring, and Maintaining Operating Systems.....</b>	 <b>73</b>
Topic A: Configure and Use Linux.....	74
Topic B: Configure and Use macOS.....	90
Topic C: Install and Upgrade Operating Systems.....	109
Topic D: Maintain OSs.....	125
 <b>Lesson 3: Maintaining and Troubleshooting Microsoft Windows.....</b>	 <b>145</b>
Topic A: Install and Manage Windows Applications.....	146
Topic B: Manage Windows Performance.....	165
Topic C: Troubleshoot Windows.....	176
 <b>Lesson 4: Configuring and Troubleshooting Networks.....</b>	 <b>201</b>
Topic A: Configure Network Connection Settings.....	202
Topic B: Install and Configure SOHO Networks.....	218
Topic C: Configure SOHO Network Security.....	230
Topic D: Configure Remote Access.....	247
Topic E: Troubleshoot Network Connections.....	254
 <b>Lesson 5: Managing Users, Workstations, and Shared Resources.....</b>	 <b>267</b>
Topic A: Manage Users.....	268
Topic B: Configure Shared Resources.....	277
Topic C: Configure Active Directory Accounts and Policies.....	293

<b>Lesson 6: Security Concepts.....</b>	<b>309</b>
Topic A: Logical Security Concepts.....	310
Topic B: Threats and Vulnerabilities.....	318
Topic C: Physical Security Measures.....	328
<b>Lesson 7: Securing Workstations and Data.....</b>	<b>335</b>
Topic A: Implement Security Best Practices.....	336
Topic B: Implement Data Protection Policies.....	344
Topic C: Protect Data During Incident Response.....	353
<b>Lesson 8: Troubleshooting Workstation Security Issues.....</b>	<b>359</b>
Topic A: Detect, Remove, and Prevent Malware.....	360
Topic B: Troubleshoot Common Workstation Security Issues.....	372
<b>Lesson 9: Supporting and Troubleshooting Mobile Devices.....</b>	<b>381</b>
Topic A: Secure Mobile Devices.....	382
Topic B: Troubleshoot Mobile Device Issues.....	391
<b>Lesson 10: Implementing Operational Procedures.....</b>	<b>407</b>
Topic A: Use Appropriate Safety Procedures.....	408
Topic B: Environmental Impacts and Controls.....	417
Topic C: Create and Maintain Documentation.....	426
Topic D: Use Basic Change Management Best Practices.....	435
Topic E: Implement Disaster Prevention and Recovery Methods.....	439
Topic F: Basic Scripting Concepts.....	444
Topic G: Professionalism and Communication.....	453
<b>Appendix A: Mapping Course Content to CompTIA® A+® Core 2                   (Exam 220-1002).....</b>	<b>469</b>
<b>Solutions.....</b>	<b>487</b>
<b>Glossary.....</b>	<b>491</b>
<b>Index.....</b>	<b>523</b>

# About This Guide

CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is the only industry recognized credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment. It is trusted by employers around the world to identify the go-to person in end point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

*The Official CompTIA® A+® Core 2 (Exam 220-1002)* guide provides the background knowledge and skills you will require to be a successful A+ technician. It will help you prepare to take the CompTIA A+ Core Series certification examination (exam number 220-1002), in order to become a CompTIA A+ Certified Professional.

## Guide Description

### Target Student

This guide is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This guide is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 2 220-1002 Certification Exam.

### Prerequisites

To ensure your success, you should have experience with basic computer user skills, be able to complete tasks in a Microsoft® Windows® environment, be able to search for, browse, and access information on the Internet, and have basic knowledge of computing concepts. You can obtain this level of skills and knowledge by taking the following official CompTIA courses:

- *The Official CompTIA® IT Fundamentals+ (Exam FC0-U61)*

Note: These prerequisites might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: <https://certification.comptia.org/training/exam-objectives>

### Guide Objectives

In this guide, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. You will:

- Support operating systems.
- Install, configure, and maintain operating systems.
- Maintain and troubleshoot Microsoft Windows.
- Configure and troubleshoot network connections.
- Manage users, workstations, and shared resources.
- Implement physical security.
- Secure workstations and data.
- Troubleshoot workstation security issues.
- Support and troubleshoot mobile devices.
- Implement operational procedures.

## How to Use This Book

### As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of activities designed to enable you to solidify your understanding of the informational material presented in the guide. Information is provided for reference and reflection to facilitate understanding and practice.



At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the guide. You will also find an index to assist in locating information within the instructional components of the book. In many electronic versions of the book, you can click links on key words in the content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your PDF viewing software.

### As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

### Guide Icons

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A <b>Note</b> provides additional information, guidance, or hints about a topic or task.
	A <b>Caution</b> note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions, so that you can be sure to get the desired results of an activity or task.

# Lesson 1

## Supporting Operating Systems

**LESSON TIME: 2 HOURS, 35 MINUTES**

### LESSON INTRODUCTION

As a professional IT support representative or PC service technician, your job will include installing, configuring, maintaining, and troubleshooting personal computer operating systems, applications, hardware, and networks. Before you can perform any of these tasks, you need to understand the basics of what an operating system is, including the various versions, features, components, and technical capabilities. With this knowledge, you can provide effective support for all types of system environments.

The operating system is the software that provides a user interface to the computer hardware and provides an environment in which to run software applications and create computer networks. In this lesson, you will identify the basic types, functions, features, and tools of operating systems, with a particular focus on Microsoft® Windows®.

### LESSON OBJECTIVES

In this lesson, you will:

- Compare common OSs and their purposes and features.
- Use administrative tools and system utilities in different versions of Windows.
- Perform file management using Explorer and command prompt tools.
- Use the command-line tools and the Disk Management console to configure disks, volumes, arrays, and mount points.
- Use Device Manager and Control Panel/Settings to configure power management, display and sound devices, and to remove devices.

# Topic A

## Identify Common Operating Systems



### EXAM OBJECTIVES COVERED

1002-1.1 Compare and contrast common operating system types and their purposes.  
1002-1.2 Compare and contrast features of Microsoft Windows versions.

In this topic, you will identify the types and functions of personal computer (PC) and mobile device operating systems. The first step is to learn about the various operating systems available today, and to identify those that are commonly used on PCs and those that are used on tablets and smartphones.

Without a user-friendly operating system, most people would not be capable of using their computers or mobile devices to successfully perform the tasks required of them. As an IT professional, being familiar with the different types of operating systems can help you to support a variety of computer and mobile device environments.

### WHAT IS AN OPERATING SYSTEM?

A computer requires an **operating system (OS)** in order to function. The operating system provides the interface between the hardware, application programs, and the user. The operating system handles many of the basic system functions, such as interaction with the system hardware and input/output.

An operating system is generally made up of a number of core files—called the **kernel**—with additional **device drivers** and **programs** to provide extended functionality. The earliest operating systems for PCs, such as Microsoft's Disk Operating System (DOS), used a command-line user interface or simple menu systems. Windows and software applications for Windows were marked by the use of a **Graphical User Interface (GUI)**. This helped to make computers easier to use by non-technical staff and home users.



**Note:** Actually, some DOS applications presented a GUI, of a kind. Windows is sometimes described as a WIMP (Window, Icon, Menu, Pointing device) interface.

The **desktop style** favored by a particular OS or OS version is a powerful factor in determining customer preferences for one OS over another.

### OS TYPES

The market for operating systems is divided into four main sections:

- Business client—an OS designed to work as a client in business networks.
- Network Operating System (NOS)—an OS designed to run on servers in business networks.
- Home client—an OS designed to work on standalone or workgroup PCs in a home or small office.
- Cell phone (smartphone)/Tablet—an OS designed to work with a handheld portable device. This type of OS must have a touch-operated interface.



## COMPATIBILITY ISSUES

A software application is coded to run on a particular OS. You cannot install an app written for iOS® on an Android™ smartphone. The developer must create a different version of the app. This can be relatively easy for the developer or quite difficult, depending on the way the app is coded and the target platforms. The application or app "ecosystem," or the range of software available for a particular OS, is another big driver of customer acceptance for a particular OS product.

Compatibility also affects version updates to operating system software. There is always a chance that some change in the new OS version will cause software (or hardware device drivers) written for an older version not to work properly. In the business client market, this makes companies very reluctant to update to new OS versions without extensive testing. As extensive testing is very expensive, they are generally reluctant to adopt new versions without a compelling need to do so.



**Note:** These compatibility concerns are being mitigated somewhat by the use of web applications and cloud services. A web application only needs the browser to be compatible, not the whole OS. The main compatibility issue for a web application is supporting a touch interface and a very wide range of display resolutions on the different devices that might connect to it.

Finally, compatibility also affects the way that computers running different operating systems can communicate on data networks. The computers cannot "talk" to one another directly. The operating systems must support common network protocols that allow data to be exchanged in a standard format.

## MICROSOFT WINDOWS

**Microsoft Windows** is the dominant commercial PC OS, estimated to be installed on 90% of the world's desktop and laptop computers. The **Windows Server** OS is also widely used on private network servers and Internet servers running web, email, and social networking apps.

Like most software, Windows and Windows Server® have been released in a number of versions over the years. Historically, a new version would have to be purchased, though upgrade discounts were usually available. A new version may introduce significant changes in desktop styles and user interface of Windows and add new features and support for new types of hardware. On the downside, a new version may not be compatible with hardware and software applications designed for earlier versions.

One of the main functions of an OS is to provide an interface (or **shell**) between the user and the computer hardware and software. Windows has a number of interface components designed both for general use and for more technical configuration and troubleshooting.

The top level of the user interface is the **desktop**. This is displayed when Windows starts and the user logs on. The desktop contains icons to launch applications and possibly user data files. The desktop also contains the Start Menu or **Start Screen** and taskbar, which are used to launch and control applications.

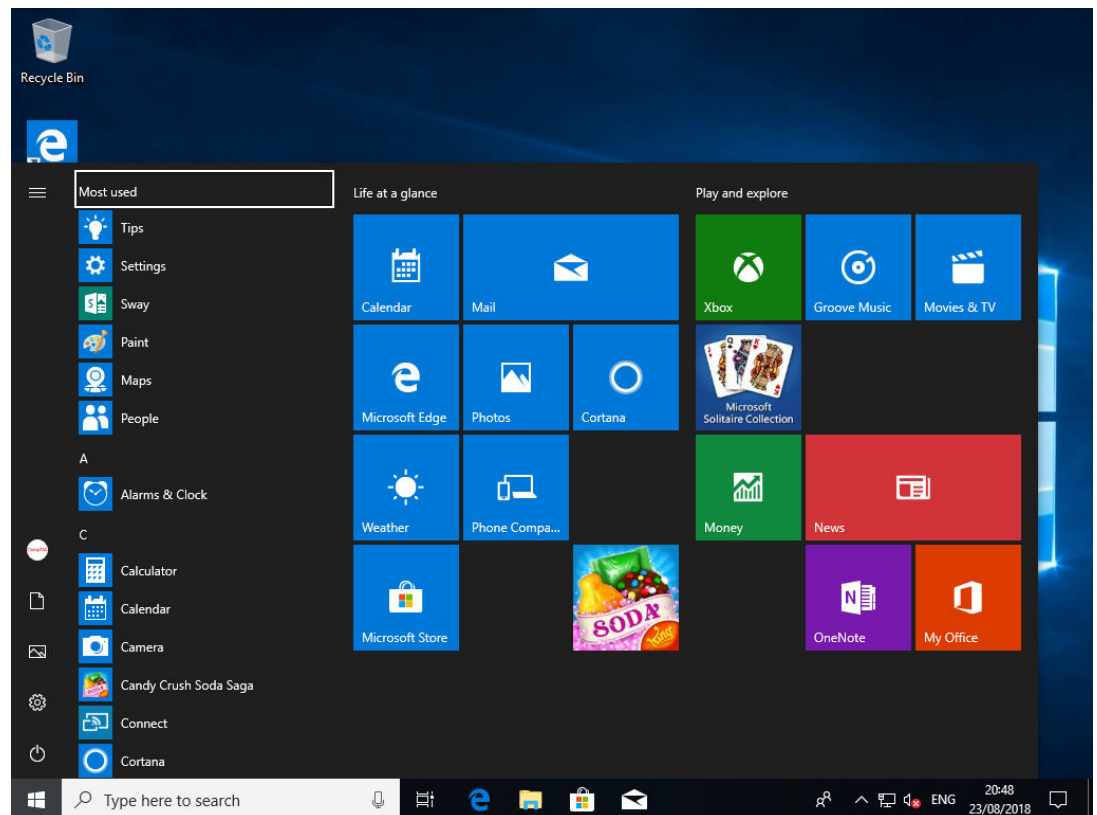
## MICROSOFT WINDOWS VERSIONS

Let's start by taking a look at the most popular versions of Windows currently in use. Other operating systems will be examined more closely later in the course.


## WINDOWS 10

Windows 10, first released in 2015, is the current version. Windows 10 aims to provide a consistent user experience across different types of devices, including desktop PCs, laptops, tablets, and smartphones.

When installed to a PC or laptop, Windows 10 retains the user desktop and taskbar familiar from legacy versions but uses a touch-optimized **Start Screen** interface to access apps and programs. This replaces the old Start Menu. As well as shortcuts, the **Start Screen** can display app tiles, which can contain live or actively updated content. These app tiles are fully customizable.



Windows 10 (1803) desktop and Start Screen. (Screenshot used with permission from Microsoft.)

The **Start Screen** is activated by selecting the **Start** button  or by pressing the **Windows** key, which might also be labeled the **Start** key.



**Note:** On a smartphone or tablet, the **Start Screen** replaces the desktop entirely.

## WINDOWS 10 FEATURE UPDATES

With Windows 10, Microsoft indicated that they would no longer release new versions of Windows, but would instead maintain the OS with **feature updates** on a periodic basis. Thus, the current version of Windows, at the time of writing, is still Windows 10. This approach is known as “Windows as a service.” Feature updates for Windows 10 are identified with a name and number. For example, in July 2016, Microsoft released a Windows 10 feature update called Windows 10 Anniversary Update. This release was identified with the number 1607, which corresponds to the year (2016) and month (07/ July) of release. The full name of the current version of Windows 10 at the time of

writing is Windows 10 Spring Creators Update (1803), replacing the Fall Creators Update (1709).

In addition to feature updates, Windows is updated periodically with **quality updates**. Quality updates do not usually make radical changes to Windows, though some do include new features. Quality updates might sometimes cause compatibility problems with some hardware devices and software applications, but this is less likely than with feature updates.

### Windows 10 Mobile

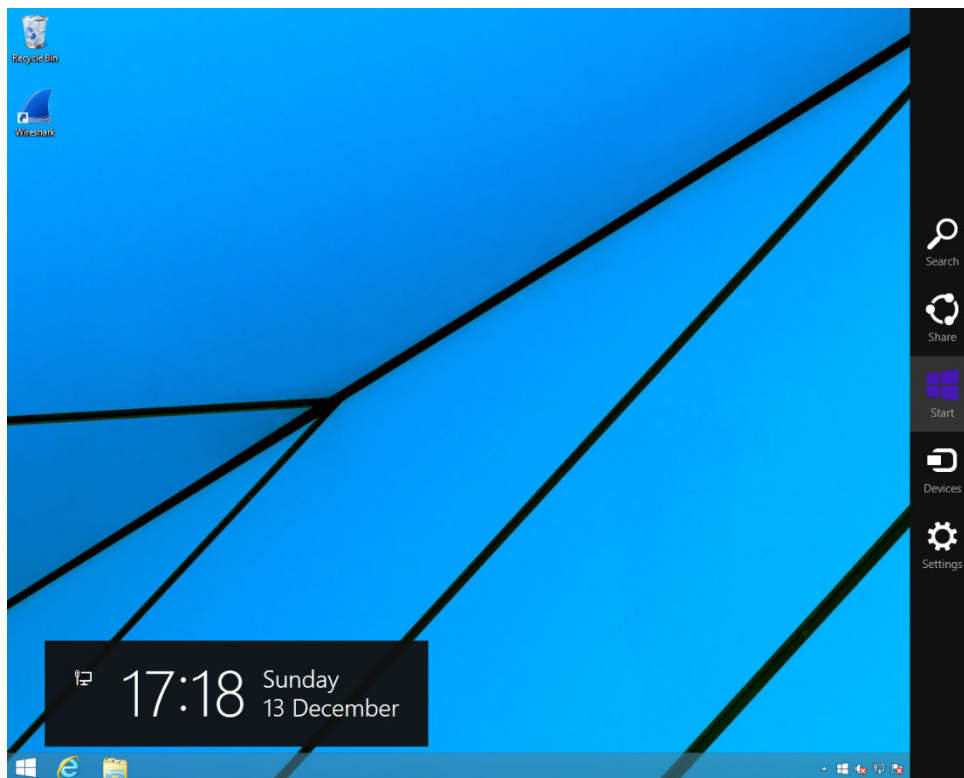
Microsoft has developed versions of Windows for mobile devices, including Windows CE, Windows Phone® 7, and Windows Phone 8. None of these have enjoyed the same sort of success as Windows has in the PC market.

With Windows 10 Mobile, Microsoft has adopted a consistent user interface and code base across all types of devices. Windows 10 Mobile has a very small smartphone market share compared to Android and iOS. Microsoft develops and sells Windows 10 Mobile smartphones and Surface® tablets.

## WINDOWS 8 AND WINDOWS 8.1

Compared to earlier versions, Windows 8 (released in 2012) and Windows 8.1 (2013) imposed significant user interface changes to provide better support for touchscreens. One of these changes was the first use of the **Start Screen**. Not all of the changes were popular with users familiar with Windows 7, however. Windows 10 addressed this feedback and was also made available as a free upgrade to Windows 8. Consequently, Windows 10 very quickly replaced Windows 8 and Windows 8 is not that widely used, having about 7% market share at the time of writing.

As well as introducing the **Start Screen** for the first time, in Windows 8, some of the search and configuration settings are accessed as **charms**. The Charms bar is opened by swiping from the right of the screen.



*Windows 8.1 showing the Charms bar. (Screenshot used with permission from Microsoft.)*

On a desktop PC, you can move the mouse pointer down from the top-right or (more simply) press **Windows+C**. The Charms bar was discontinued in Windows 10.

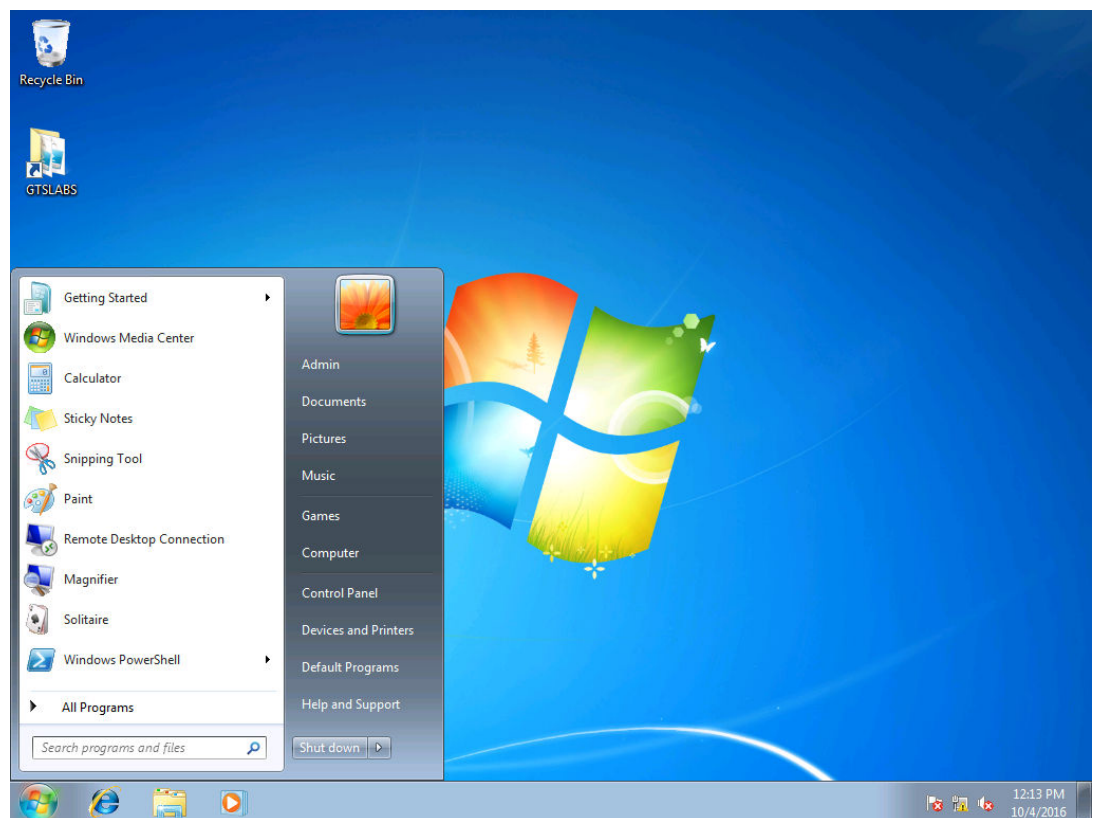


**Note:** Windows 8 was swiftly updated to Windows 8.1 to address some issues with the interface, principally the lack of a **Start** button and forcing use of the **Start Screen** at boot rather than the desktop. In other respects, references to Windows 8 in this course can be taken to apply to Windows 8.1, too. There was never a Windows 9.

## WINDOWS 7

Prior to Windows 8, there was Windows 7 (2009), Windows Vista (2007), and Windows XP (2001). Of these, Windows 7 is still widely used, with an estimated installation base of around 45% of all PCs. Despite no longer being officially supported by Microsoft, Windows XP is still installed on about 5% of devices. Windows Vista never achieved a significant market share.

Windows 7 uses the "classic" Start Menu user interface. The Start Menu contains icon shortcuts to recently used programs and some of the main folders and utilities. The All Programs submenu contains the shortcuts to all the other desktop applications installed on the computer.



Windows 7 desktop and Start Menu. (Screenshot used with permission from Microsoft.)



**Note:** According to the CompTIA exam objectives, you will not be expected to support Windows Vista or Windows XP.

## WINDOWS EDITIONS

Each version of Windows is available in different editions. Editions are used by Microsoft to create different markets for Windows. Windows 7 editions included

Starter, Home Basic, Home Premium, Professional, Enterprise, and Ultimate. Windows 10 is available in the following editions:

- Windows 10 Home—designed for domestic consumers and Small Office Home Office (SOHO) business use. The Home edition cannot be used to join a Windows domain network.
- Windows 10 Pro—designed for small and medium-sized businesses. The "Professional" edition comes with networking and management features designed to allow network administrators more control over each client device.
- Windows 10 Enterprise/Windows 10 Enterprise (Long Term Servicing Channel)—similar to the Pro edition but designed for volume licensing by medium and large enterprises.
- Windows 10 Education/Pro Education—variants of the Enterprise and Pro editions designed for licensing by schools and colleges.



**Note:** The Windows 7 Ultimate edition was a "superset" with all the features from other editions. Ultimate editions were discontinued with Windows 8. The distinction between basic and premium home editions was also abandoned. Windows 8 has an unnamed edition—sometimes referred to as "Windows 8 Core"—rather than a "Home" edition.

## WINDOWS IN THE CORPORATE WORLD

The principal distinguishing feature of the Professional/Pro, Enterprise, Ultimate, and Education editions (regardless of version) is the ability to join a **domain network**. A personal user or small business owner can just administer each machine they own individually. On a corporate network, it is necessary to manage user accounts and system policies centrally, because there are more machines to manage and security requirements are higher. This centralized management is provided by joining each computer to a domain, where the accounts are configured on Domain Controller (DC) servers. Some other notable corporate features are as follows:

- **BitLocker**—enables the user to encrypt all the information on a disk drive. Encryption means that data on the device is protected even if someone steals it (as long as they cannot crack the user password). BitLocker is included with Windows 7 Enterprise and Ultimate, Windows 8 Pro and Enterprise, and Windows 10 Pro, Enterprise, and Education editions.
- **Encrypting File System (EFS)**—where BitLocker encrypts an entire drive, EFS can be used to apply file- or folder-level encryption. EFS is included with Windows 7 Professional, Enterprise, and Ultimate, Windows 8 Pro and Enterprise, and Windows 10 Pro, Enterprise, and Education editions.
- **BranchCache**—an enterprise might have computers installed at different geographic locations needing to view and update data at a central office. As the Wide Area Network (WAN) links from each location to the office might be quite slow, it can be useful for the remote computers to share access to a single cache of data from shared folders and files or document portals such as SharePoint sites. This reduces the amount of WAN traffic because each client does not have to download its own copy individually. BranchCache is supported on Windows 7 Enterprise and Ultimate, Windows 8 Enterprise, and Windows 10 Pro, Enterprise, and Education editions.



**Note:** The Pro/Professional editions support a limited type of BranchCache for Background Intelligent Transfer Service (BITS) communications only. Most document and file sharing uses HyperText Transfer Protocol (HTTP) or Server Message Block (SMB), and these types of transfers are only supported by the Enterprise/Ultimate editions. BITS might be used for tasks such as patch deployment or image-based installs.

## WINDOWS FOR PERSONAL USE

**Windows Media Center** is a Microsoft app allowing the computer to be used as a sort of home entertainment appliance, such as playing DVDs (several other functions of the product are no longer supported). Media Center was included in the Windows 7 Home Premium, Professional, Enterprise, and Ultimate editions. It is the principal distinction between the Windows 7 Home Basic and Windows 7 Home Premium editions. It became a paid-for add-on in Windows 8 and was discontinued in Windows 10.

If Media Center is not available, a DVD player is available from Microsoft. Third-party software is required to playback commercial Blu-ray™ discs.

## 32-BIT AND 64-BIT WINDOWS

Each version and edition of Windows is available as 32-bit or 64-bit (x64) software. 64-bit editions of Windows can run most 32-bit applications software, though there may be some exceptions (you should check with the software vendor). The reverse is not true, however; a 32-bit version of Windows cannot run 64-bit applications software.

64-bit editions of Windows also require 64-bit hardware device drivers authorized ("signed") by Microsoft. If the vendor has not produced a 64-bit driver, the hardware device will not be usable.

## WINDOWS SYSTEM LIMITS

The versions and editions of Windows have different restrictions in terms of CPU types and features and memory supported. Windows 10 has the following system limits:

Feature	Home	Pro	Education	Enterprise
SMP (Multiple CPUs)	No	2-way	2-way	2-way
Multicore	Yes	Yes	Yes	Yes
RAM limitations (32-bit)	4 GB	4 GB	4 GB	4 GB
RAM limitations (64-bit)	128 GB	2 TB	2 TB	6 TB

Windows 8 has the following system limits:

Feature	Core	Pro/Enterprise
SMP	No	2-way
Multicore	Yes	Yes
RAM limitations (32-bit)	4 GB	4 GB
RAM limitations (64-bit)	128 GB	512 GB

Windows 7 has the following system limits:

Feature	Home Basic	Home Premium	Professional	Enterprise	Ultimate
64-bit Edition	Yes	Yes	Yes	Yes	Yes
SMP	No	No	2-way	2-way	2-way
Multicore	Yes	Yes	Yes	Yes	Yes
RAM limitations (32-bit)	4 GB	4 GB	4 GB	4 GB	4 GB



Feature	Home Basic	Home Premium	Professional	Enterprise	Ultimate
RAM	8 GB	16 GB	192 GB	192 GB	192 GB
limitations (64-bit)					

The Windows 7 Starter edition was only available to system builders (OEMs) for installation on netbooks and sub-notebooks. It supports up to 2 GB RAM. There is no 64-bit version of the Starter edition.

## OS LIFECYCLES

An **end of life system** is one that is no longer supported by its developer or vendor. End of life systems no longer receive security updates and so represent a critical vulnerability for a company's security systems if any remain in active use.

Microsoft products are subject to a support lifecycle policy. Windows versions are given five years of mainstream support and five years of extended support (during which only security updates are shipped). Support is contingent on the latest Service Pack being applied (non-updated versions of Windows are supported for 24 months following the release of the SP). Windows 10 retirement schedules for feature updates—referred to as "end of service"—are 18 months, except for September updates for Education/Enterprise editions only, which are supported for 30 months.

To find out when Microsoft products will be retired or how long specific products will be supported, visit the Microsoft Product Lifecycle Search tool at [support.microsoft.com/lifecycle/search](https://support.microsoft.com/lifecycle/search).

When you plan to install a new version of an operating system as an upgrade, you must check that your computer meets the hardware requirements for the new version. As operating system software such as Windows 10 moves towards more of a service model, with quite frequent feature updates, it could be the case that an update has its own system requirements that were different from the original. Plus, Microsoft points out that the core hardware requirements for Windows 10 are the same as those for Windows 7. Other factors might impact your ability to apply a feature update, including support for third-party driver or applications software.

## APPLE OPERATING SYSTEMS

In 1984, when the IBM PC was the dominant desktop standard, Steve Jobs and Steve Wozniak created a new type of personal computer—the Apple® Macintosh® (or Mac®). It was revolutionary because it came with a graphical user interface at a time when IBM's PC used the command-line/text menu DOS operating system. The Mac has never matched Windows' huge user base, although its current incarnation does have a truly devoted following.

### APPLE MAC OS/OS X/macOS

The main difference between Mac OS and other operating systems is that the OS is only supplied with Apple-built computers. You cannot purchase Mac OS and install it on an ordinary PC. This helps to make Mac OS stable but does mean that there is far less choice in terms of buying extra hardware.



macOS desktop. (Screenshot courtesy of Apple.)

The current lines—OS X® and more recently macOS®—were re-developed from the kernel of another type of operating system called UNIX. This kernel is supplemented with additional code to implement the Mac's graphical interface and system utilities and to maintain compatibility with older Mac OS applications. macOS gets periodic "dot" version updates. At the time of writing, the current version is 10.14 or "Mojave," and updates are being released to existing customers free-of-charge.

As there is a tight link between the models of Mac computers and the OS, Apple makes specific update limitations about whether a new version of macOS can be installed to a Mac computer. Check **support.apple.com** for the technical specification for any particular macOS release. Apple does not publish end of life policies.

## APPLE iOS

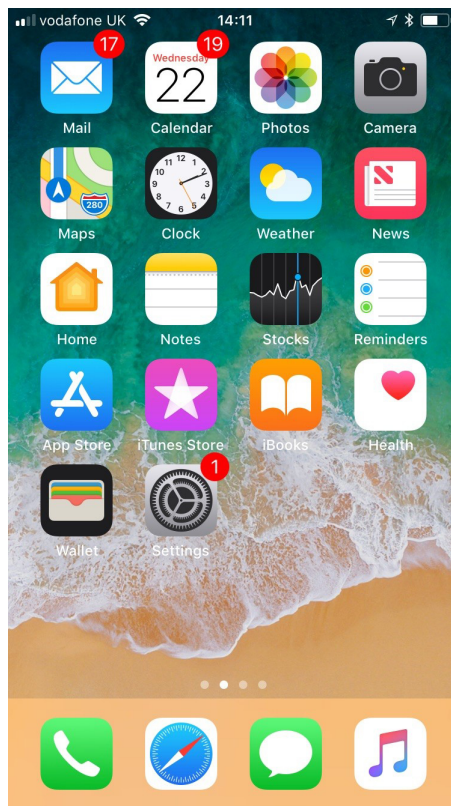
**iOS** is the operating system for Apple's iPhone® smartphone and iPad® tablet. While also derived from UNIX, iOS is a closed source operating system. This means that the code used to design the software is kept confidential and can only be modified by Apple. macOS and iOS have some similarities but they are not compatible; an app developed for iOS will not run on macOS.

On an iOS device, apart from volume and power, the only external button is the Home key, which returns the user to the home screen "desktop."

The interface is then entirely controlled via touch. Point to icons to open apps, swipe or flick from left-to-right to access the keyboard and search, or flick right-to-left to view more icons. Re-arrange icons by tapping and holding for a few seconds. The icons will then "wobble" and can be dragged to a different page or into the dock taskbar at the bottom. Press the Home key to save.

To view and manage open apps, double-click the Home key to open the Multitasking bar.





*iOS 11 running on an iPhone 7. (Screenshot courtesy of Apple.)*

Touch can be operated either with your fingers or with a special soft-touch stylus. There are many more gestures in addition to those listed above. For example, shaking the device is often used to activate undo. There are also external keyboards available and most Apple devices support Siri®, a voice recognition system and personal assistant.

New versions are released approximately every year with various .x updates. Version 12 is current at time of writing. Apple makes new versions freely available, though older hardware devices may not support all the features of a new version, or may not be supported at all. As with macOS, update limitations are published at [support.apple.com](https://support.apple.com) but there are no end of life policies.

## UNIX-BASED OPERATING SYSTEMS

Windows and macOS dominate the desktop/workstation/laptop market, but a third "family" of operating systems is very widely used on a larger range of devices.

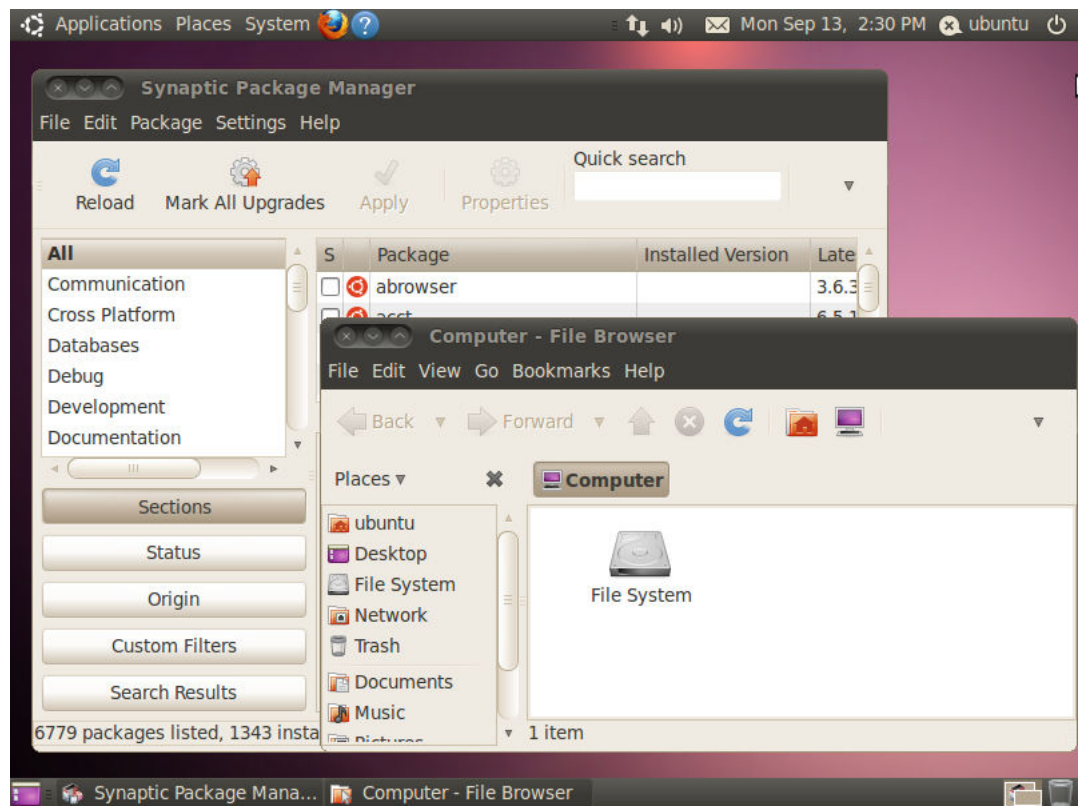
### UNIX

**UNIX** is a trademark for a family of operating systems originally developed at Bell Laboratories beginning in the late 1960s. All UNIX® systems share a kernel/shell architecture, with the kernel providing the core functionality and the interchangeable shells providing the user interface. Unlike Windows and macOS, UNIX is portable to different hardware platforms; versions of UNIX can run on everything from personal computers to mainframes and on many types of computer processors.

### LINUX

Originally developed by Linus Torvalds, **Linux** is based on UNIX. UNIX was developed over decades by various commercial, academic, and not-for-profit organizations. This resulted in several versions, not all of which are compatible, and many of which are

proprietary or contain copyrighted or patented code or features. Linux® was developed as a fully open source alternative to UNIX (and for that matter, to Windows and macOS and iOS).



Ubuntu Linux.

Linux can be used as a desktop or server OS. There are many distributions or distros, notably SUSE®, Red Hat®, CentOS, Fedora®, Debian®, Ubuntu®, and Mint®. Each distro adds specific packages and interfaces to the generic Linux kernel and provides different support options. Linux does not require a graphical interface, though many distributions provide one.

IBM®, Sun/Oracle®, and Novell® are among the vendors producing end-user applications for Linux. As a desktop OS it tends to be used in schools and universities more than in business or in the home. As a server OS, it dominates the market for web servers. It is also used very widely as the OS for "smart" appliances and Internet of Things (IoT) devices.

## CHROME OS

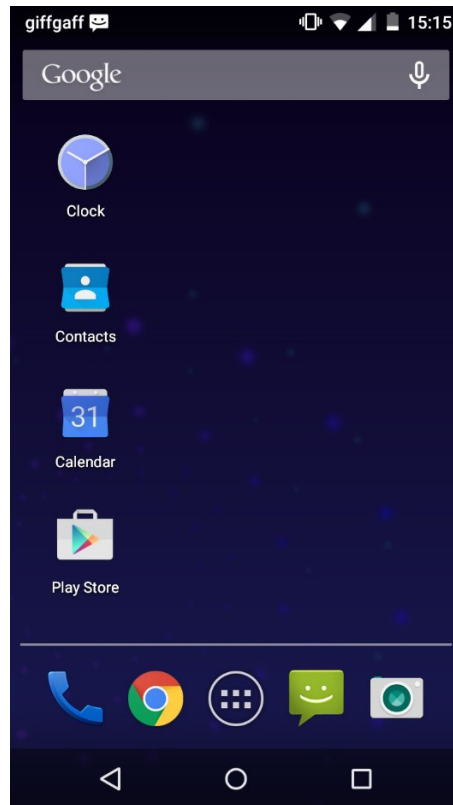
**Chrome OS** is derived from Linux, via an open source OS called Chromium™. Chrome OS™ itself is proprietary. Chrome OS is developed by Google to run on specific laptop (Chromebook) and PC (Chromebox) hardware. This hardware is designed for the budget and education markets.

Chrome OS was primarily developed to use web applications. In a web application, the software is hosted on a server on the Internet and the client connects to it using a browser. The client computer does not need to be particularly powerful as the server does most of the processing. Chrome OS provides a minimal environment compared to Windows. This means that there is less chance of some other software application or hardware device driver interfering with the function of the browser.

There are also "packaged" apps available for use offline and Chrome OS can run apps developed for Android.

## ANDROID

**Android** is a smartphone/tablet OS developed by the Open Handset Alliance, primarily driven by Google. Unlike iOS, it is an open-source OS, based on Linux. The software code is made publicly available (**source.android.com**). This means that there is more scope for hardware vendors, such as Acer®, Asus®, HTC®, Huawei®, LG, Motorola®, OnePlus, Oppo™, Samsung®, Sony®, and Xiaomi to produce vendor-specific versions.



*Android lollipop home screen.*

Like iOS, Android is updated with new major (1.x) and minor (x.1) versions, each of which is named after some kind of sweet stuff. At the time of writing, current versions include 7.1 (Nougat) and 8.1 (Oreo). Because handset vendors produce their own editions of Android, device compatibility for new versions is more mixed compared with iOS.

End of life policies and update restrictions for particular handsets are determined by the handset vendor rather than any kind of overall Android authority. Companies ordering handsets in bulk as employee devices may be able to obtain their own guarantees.

# Topic B

## Use Windows Features and Tools



### EXAM OBJECTIVES COVERED

- 1002-1.4 Given a scenario, use appropriate Microsoft command line tools.
- 1002-1.5 Given a scenario, use Microsoft operating system features and tools.
- 1002-1.6 Given a scenario, use Microsoft Windows Control Panel utilities.
- 1002-2.6 Compare and contrast the differences of basic Microsoft Windows OS security settings.

As an administrator, you will manage the computer through a graphic user interface (GUI) for some tasks and through a command line interface for others. In this topic, you will examine some of the administrative tools and utilities for Windows computers.

When you configure or troubleshoot a computer, you need to do so with an account that has sufficient privileges to make major changes to OS settings and files. If misused, these privileges could be a significant threat to the security of the computer system and network. In this topic, you will also learn how to exercise administrative privileges safely.

## WINDOWS SETTINGS AND CONTROL PANEL

Many tools are used to configure Windows settings and hardware devices. Some of the tools are accessible to ordinary users; others need administrative privileges to run.

### CONTROL PANEL

In Windows 7, the **Control Panel** is the best place to start configuring your system. The icons in the Control Panel represent applets used to configure a part of the system.




Windows 7 Control Panel showing 1) Task groups; 2) Configuration applets; 3) Navigation breadcrumb; 4) Search box. (Screenshot used with permission from Microsoft.)

Most applets are added by Windows but some software applications, such as antivirus software, add their own applets. Configuration information entered via Control Panel is ultimately stored in the Windows registry database.

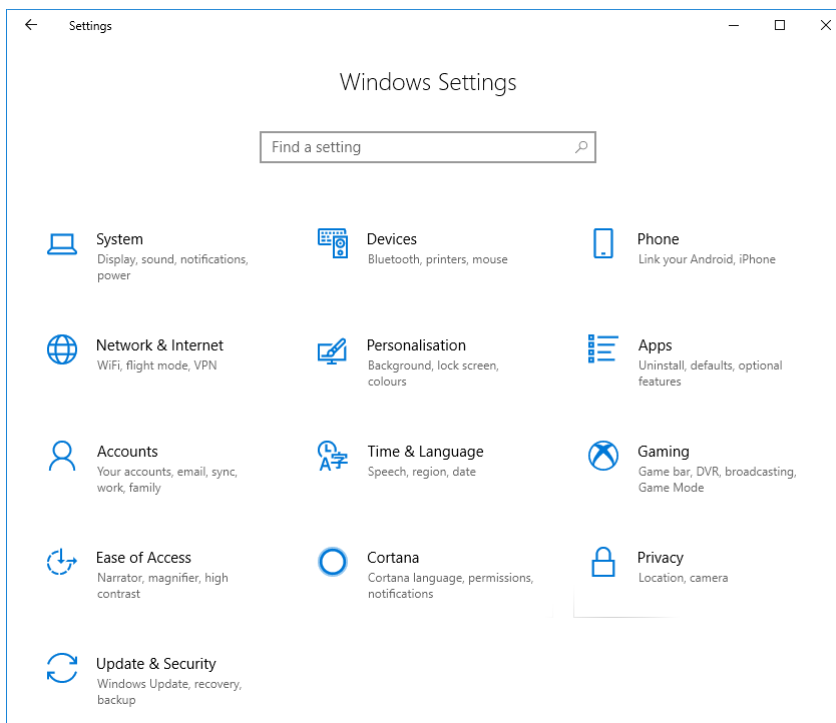
You can access Control Panel through the Start Menu. In addition, certain applets are accessible by viewing object properties straight from the desktop or from Explorer.

Control Panel applets are arranged by category by default, although you can display

"All items" via the breadcrumb or the "View by" menu. Note that options with the  icon on or next to them will require you to authorize use of the command through User Account Control (UAC).

## WINDOWS SETTINGS

**Windows Settings** is a touchscreen-enabled "app" interface for managing a Windows 10 computer.



*Windows Settings app. (Screenshot used with permission from Microsoft.)*

Most of the standard Windows 10 configuration settings can be located within Windows Settings, but not all of them. Some options are still configured via Control Panel. Each Windows 10 feature update tends to move more configuration options from Control Panel to Windows Settings, though.



**Note:** In Windows 8, this app is referred to as "PC Settings" and is accessed via the Charms bar.

## USER ACCOUNTS

A **user account** is the principal means of controlling access to computer and network resources and rights or privileges. Resources include access to files, folders, or printers; rights or privileges refers to the ability to make configuration changes or read/modify a data file. Each resource is configured with an access list, which is a list of users and their permissions for that resource.

A user account is protected by authenticating the account owner—making them provide some data that is known or held only by them.

Each user account is also associated with a profile, stored in a subfolder of the **Users** folder. The profile contains per-user registry settings (ntuser.dat) and the default document folders. Software applications might also write configuration information to the profile.

## ADMINISTRATOR AND STANDARD USER ACCOUNTS

When the OS is first installed, the account created or used during setup is a powerful local administrator account. The account is assigned membership of the local Administrators group. Generally speaking, you should only use this account to manage the computer—install applications and devices, perform troubleshooting, and so on.

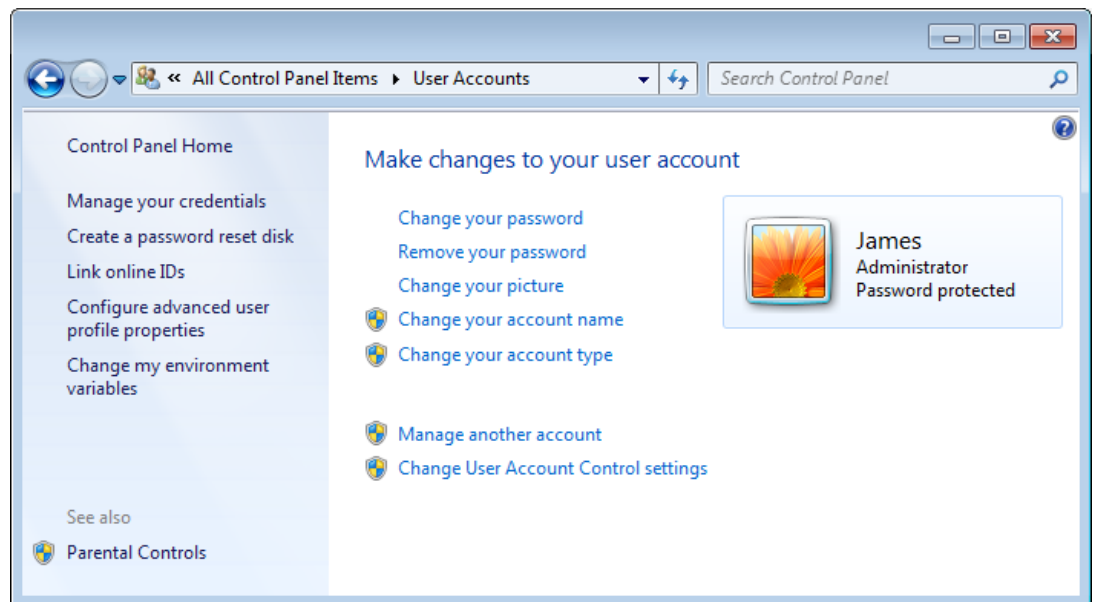
You should create ordinary user accounts for day-to-day access to the computer. This is done by putting additional users of the computer in the **Standard users** group. Standard users cannot change the system configuration and are restricted to saving data files within their own user profile folder or the Public profile. For example, a user named David with standard privileges could save files only within C:\Users\David or C:\Users\Public. Administrators can access any folder on the computer.



**Note:** Windows protects system folders from non-root administrative users. These folders are owned by a system account (such as **TrustedInstaller**). This provides more protection against malware and misconfiguration. It is possible for any administrator account to take ownership of a system folder and override these protections, though.

## USER ACCOUNTS APPLLET

The **User Accounts** applet in Control Panel allows users to manage their accounts. Users can manage local and network passwords and choose a picture to represent them on the log on screen.



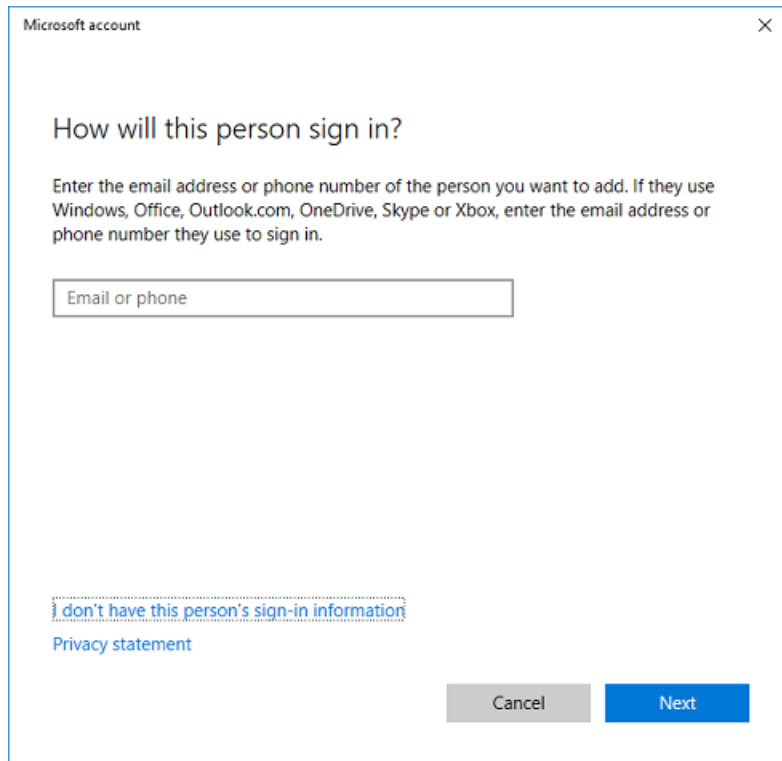
*User Accounts applet in Windows 7. (Screenshot used with permission from Microsoft.)*

Administrators can create and delete accounts or change the type of account (between administrator and user).



## LOCAL AND MICROSOFT ACCOUNTS

In Windows 8 and Windows 10, the **User Accounts** applet is still present and can still be used to change an account name or type, but it cannot be used to create new accounts. That function, plus most other account functions, is performed in the **Accounts** section of Windows Settings. Windows 8/10 accounts can either be local accounts (like Windows 7 user accounts) or linked to a **Microsoft account**, which gives access to Microsoft's cloud services and syncs desktop settings across multiple devices.



Creating a new account. (Screenshot used with permission from Microsoft.)

## HOW TO CREATE A USER ACCOUNT IN WINDOWS 10

Here is a general procedure that you can follow to create user accounts in Windows 10.

### CREATE A USER ACCOUNT IN WINDOWS 10

To create a user account in Windows 10:

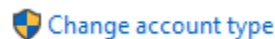
1. Open **Settings**.
2. Select **Accounts**.
3. Select **Family & other people**.
4. Select **Add someone else to this PC**.
5. If you are creating a Microsoft account, enter the email address or phone number associated with their Microsoft account, select **Next**, and then select **Finish**. The user must complete the process of signing in themselves.
6. If you are creating a local account, select **I don't have this person's sign-in information**, and then select **Add a user without a Microsoft account**. Provide a user name, password, and security question information, and then select **Next**. The user must complete the process of signing in themselves.

## UAC

**User Account Control (UAC)** is a solution to the problem of elevated privileges. In order to change important settings on the computer, such as installing drivers or software, administrative privileges are required. Previous versions of Windows make dealing with typical administrative tasks as an ordinary user very difficult, meaning that most users were given administrative privileges as a matter of course. This makes the OS more usable but it also makes it much more vulnerable, as any malicious software infecting the computer would run with the same administrative privileges.

### UAC SECURE DESKTOP

Accounts with administrative privileges are mediated by UAC. UAC counters the problem of escalated privileges by first extending some system privileges to ordinary users but then running accounts in a sandbox mode. Tasks that require UAC are shown with a Security Shield icon.

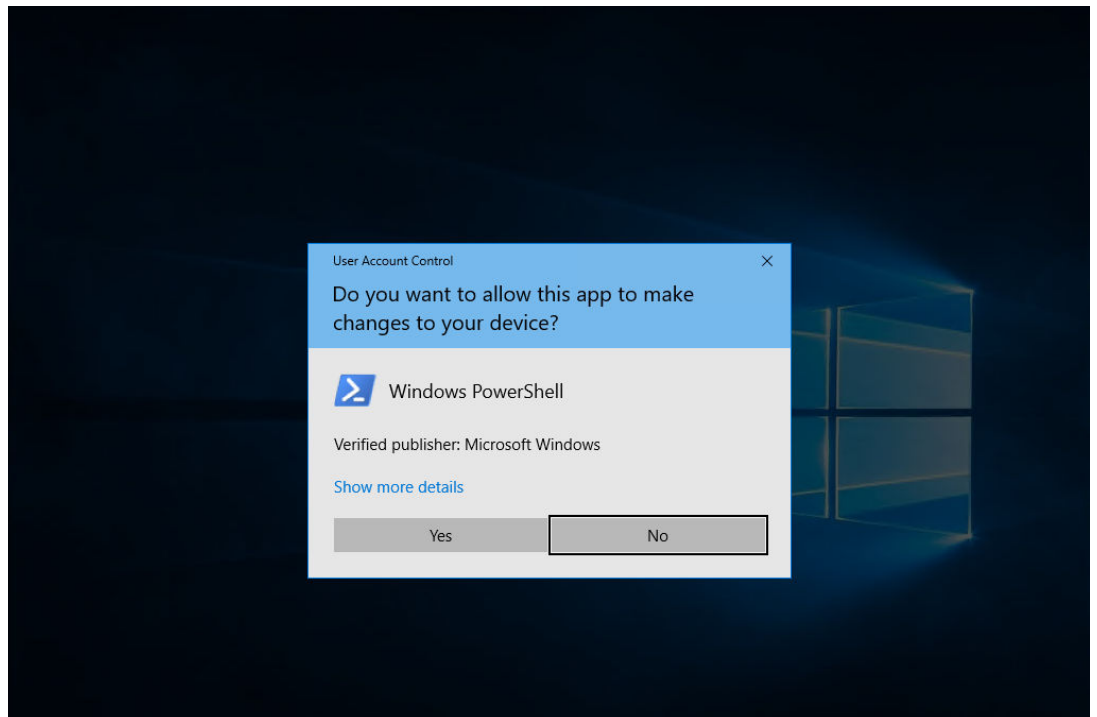


*Security Shield icon showing that changing this setting will require UAC authorization. (Screenshot used with permission from Microsoft.)*

When a user needs to exercise administrative rights, she or he must explicitly confirm use of those rights:

- If the logged in account has standard privileges, an administrator's credentials must be entered via the authorization dialog box.
- If the logged in account is already an administrator, the user must still click through the authorization dialog box.

The desktop darkens into a special secure desktop mode to prevent third-party software from imitating the authorization dialog box.

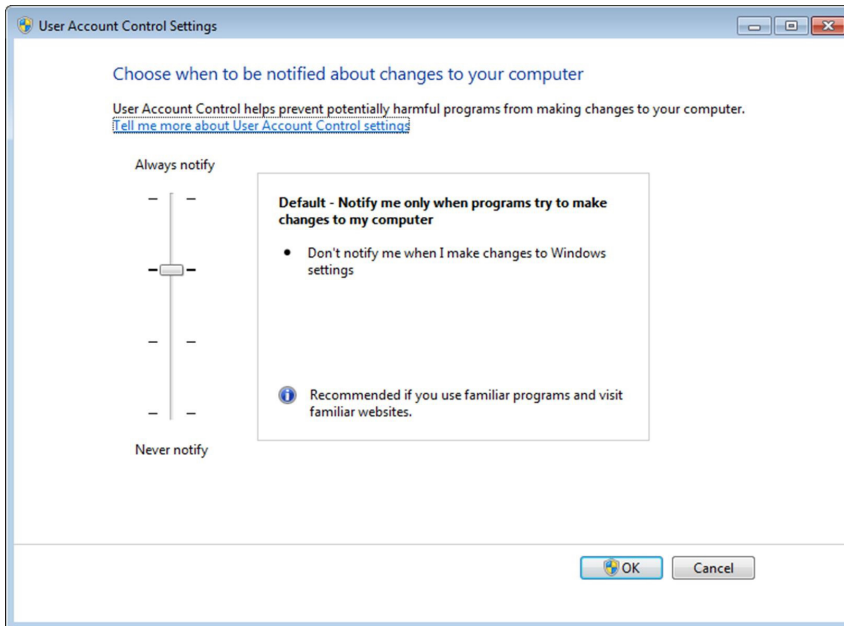


*UAC requiring confirmation of the use of administrator privileges. This account is an administrator so only a confirmation is required—no credentials have to be supplied. (Screenshot used with permission from Microsoft.)*



## CONFIGURING UAC

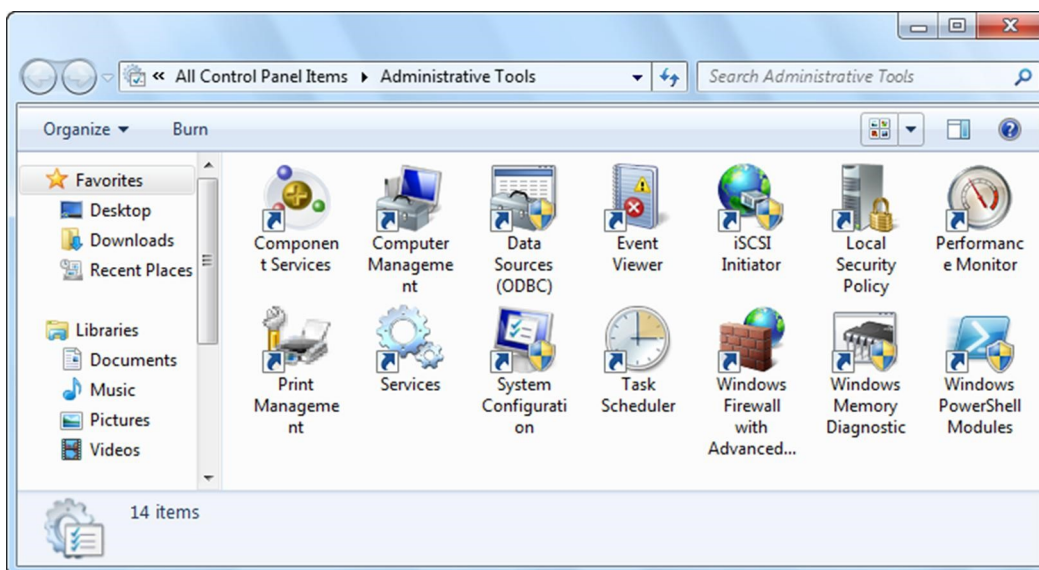
UAC protects the system from malware running with elevated administrator privileges. This is a good thing, but if you need to perform numerous system administration tasks at the same time, UAC can prove frustrating. You can configure UAC notifications to appear more or less frequently by using the configuration option in the User Accounts applet.



Configuring UAC notifications. (Screenshot used with permission from Microsoft.)

## ADMINISTRATIVE TOOLS

One of the options in Control Panel is the **Administrative Tools** shortcut.



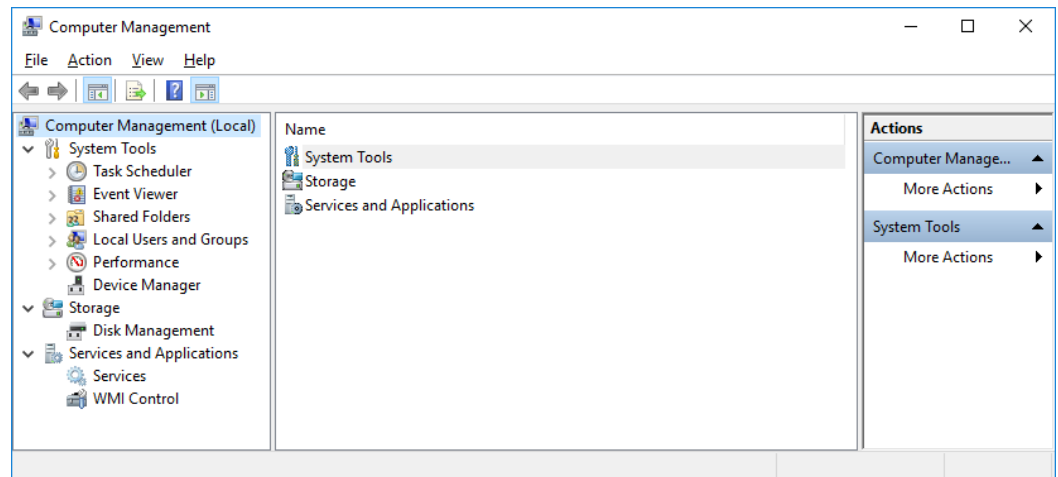
Administrative Tools in Windows 7. (Screenshot used with permission from Microsoft.)

Administrative Tools contains several shortcuts, giving you the ability to define and configure various advanced system settings and processes. There are also tools to assist with troubleshooting the system.

## DEFAULT MICROSOFT MANAGEMENT CONSOLES

Administrative Tools is a collection of pre-defined Microsoft Management Consoles (MMCs). Each console contains one or more snap-ins that are used to modify various settings. The principal consoles are:

- **Component Services**—enables you to register new server applications or reconfigure security permissions for existing services.
- **Computer Management**—the default management console with multiple snap-ins to configure local users and groups, disks, services, devices, and so on.



*The default Computer Management console in Windows 10 with the configuration snap-ins shown on the left. (Screenshot used with permission from Microsoft.)*

- **Data Sources**—control connections to databases set up on the local computer.
- **Event Viewer**—allows monitoring of Windows logs. System, security, and application events are recorded in these logs. There are also application- and service-specific logs.
- **Local Security Policy**—allows you to view and edit the current security policy. A computer that is a member of a domain will have the security settings defined in the domain security policy.
- **Print Management**—set properties and monitor local printers and manage printer sharing on the network.
- **Reliability and Performance Monitoring**—view the performance of the local computer.
- **Services**—start, stop, and pause services.



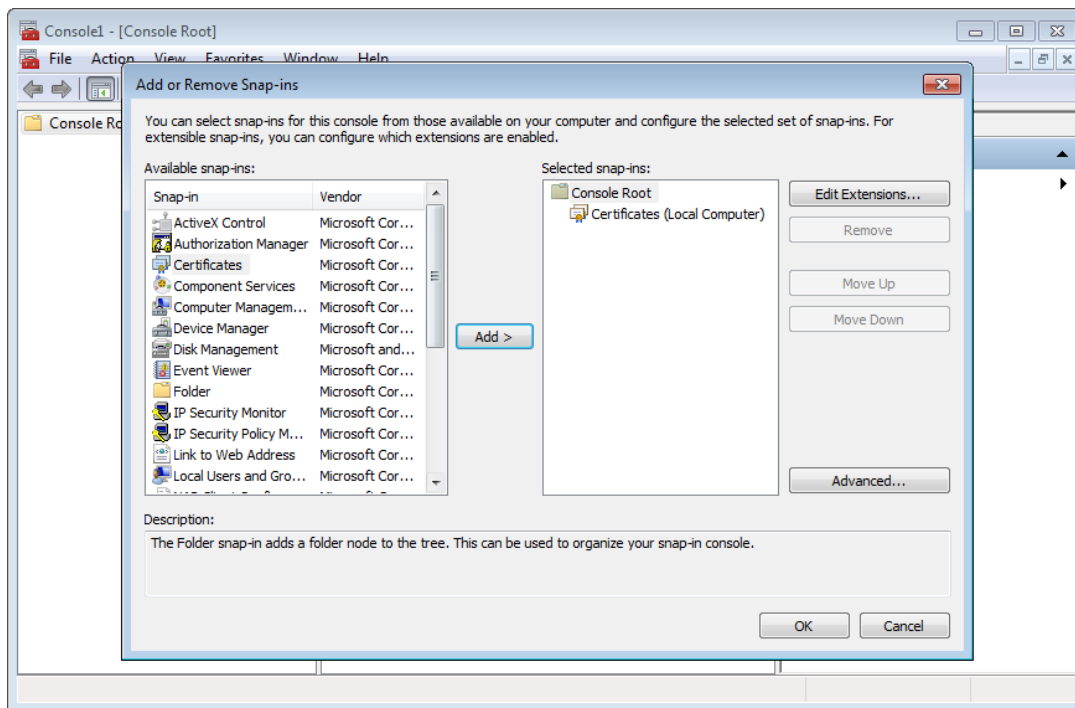
**Note:** Windows 10 adds quite a few more shortcuts under Administrative Tools, including **Disk Cleanup**, **System Configuration**, **System Information**, and **Task Scheduler**.

## MMC CUSTOMIZATION

As well as using the default consoles, you may find it useful to create your own. Consoles can be configured for each administrator and the details saved as a file with an MSC extension in their Start Menu folders.



**Note:** Most MMC snap-ins can be used to manage either the local computer or a remote computer (a computer elsewhere on the network).



*Adding a Snap-in in Windows 7. (Screenshot used with permission from Microsoft.)*

## HOW TO CREATE CUSTOM MMCs IN WINDOWS

Here is a general procedure that you can follow to create custom MMCs in Windows.

### CREATE CUSTOM MMCs IN WINDOWS

To create custom MMCs in Windows:

1. To access the management console, run the `mmc` command.
2. If necessary, in the **User Access Control** message box, select **Yes**.
3. Select **File**→**Add/Remove Snap-In**.
4. Select a snap-in and select **Add**.
5. If necessary, select a computer to manage and select **OK** or **Finish**.
6. Select and add additional snap-ins as needed.
7. Select **OK**.
8. Select **File**→**Save As** and save the custom MSC file with a unique name.

## ACCESS OPTIONS FOR SYSTEM TOOLS

Control Panel and Administrative Tools contain most of the shortcuts for the system features, but there are other ways of accessing key tools.

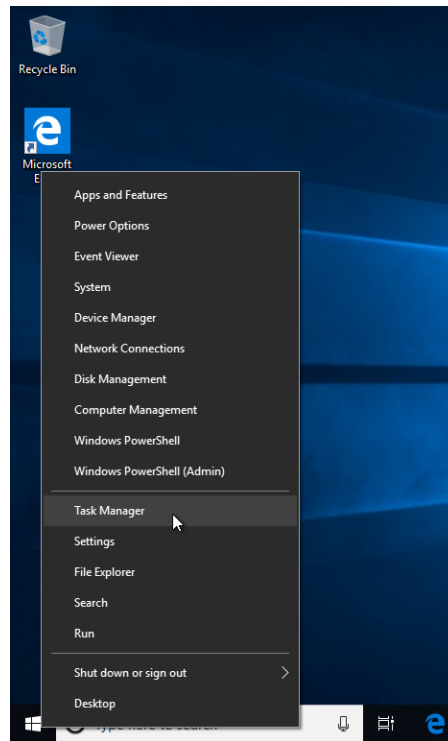
### COMPUTER/THIS PC

The **Computer** object (renamed **This PC** in Windows 8/10) provides access to your local drives, printers, and any network drives that have been mapped. To browse resources, open **Computer/This PC** then the icon that represents the resource you want to view.

By right-clicking the icon itself and selecting the **Properties** option from the menu, you can access System properties. You can also right-click and select **Manage** to open the default Computer Management console.

## WinX/POWER USERS MENU

Pressing **Windows+X** or right-clicking the **Start** button shows a shortcut menu including Control Panel, Windows Settings, and File Explorer, but also management utilities such as Device Manager, Computer Management, Command Prompt, and Windows PowerShell®.



*Windows 10 WinX menu (right-click the Start button). (Screenshot used with permission from Microsoft.)*

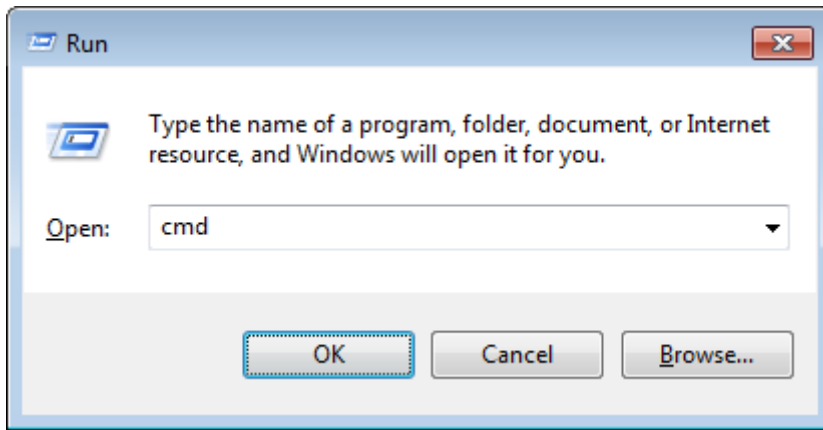


**Note:** Contents of the WinX menu do change frequently. For example, the Control Panel link is no longer included in Windows 10 (1803).

## INSTANT SEARCH BOX AND RUN COMMAND

The **Instant Search** box on the Start Menu/**Start Screen** will execute programs and configuration options using simple names. You can open any file or program by pressing the **Windows** key then typing the path to the file. In the case of registered programs and utilities, you simply need to type the program file name or utility name.

Alternatively, you can access the **Run** dialog box using **Windows+R** or entering `run` into the search box.



Run dialog box. (Screenshot used with permission from Microsoft.)



**Note:** The `run` command is useful if you want to execute a program with switches that modify the operation of the software. For example, Microsoft Office programs can be executed using safe mode switches for troubleshooting.

## .MSC EXTENSIONS AND THE RUN LINE

There are several management consoles that you can access via the Run line by using the .MSC extension. For example:

- `devmgmt.msc` opens the Device Manager console.
- `diskmgmt.msc` opens the Disk Management console.
- `compmgmt.msc` opens the Computer Management console.

## COMMAND LINE TOOLS

Most configuration of Windows can be done via convenient GUI tools, such as the management consoles and Control Panel. In some circumstances, though, it is necessary to use a command prompt to configure or troubleshoot a system. As you learn the commands, you may also find it quicker to use the command shell for actions such as file management. Learning commands is also valuable if you have to write scripts to automate Windows.

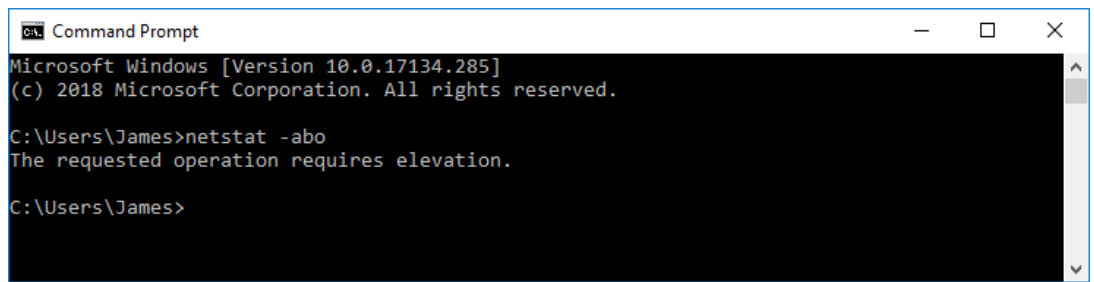
## COMMAND PROMPT

You can run any command from the **Run** dialog box. However, to input a series of commands or to view output from commands, you need to use the command shell (`cmd.exe`). To open the prompt, type `cmd` in the **Run** dialog box or **Instant Search** box.



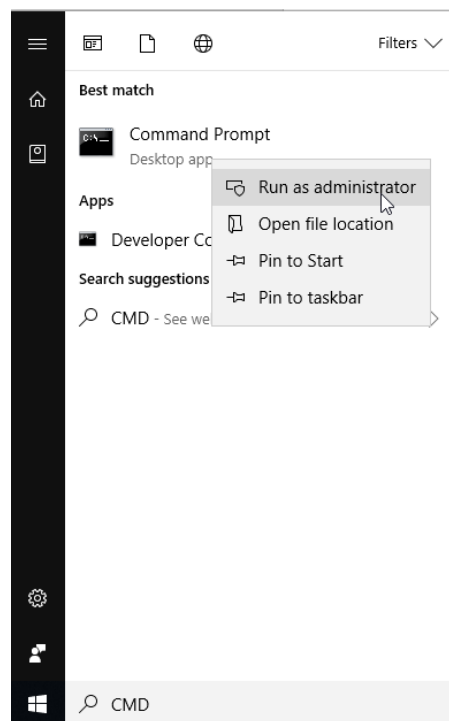
**Note:** Alternatively, you can type `command` to achieve the same thing. This used to be specifically a DOS command interpreter, but now just links to `cmd.exe`.

You may need to run the command prompt with elevated privileges in order to execute a command. If a command cannot be run, the error message "The requested operation requires elevation" is displayed.



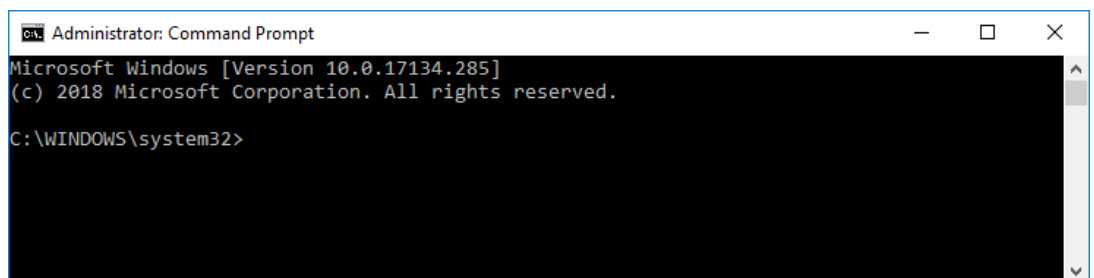
Trying to run a command that requires elevation. You must open a new command prompt window as administrator. (Screenshot used with permission from Microsoft.)

You cannot continue within the same window. You need to open a new command prompt as administrator. Right-click the command prompt shortcut and select **Run as administrator** then confirm the UAC prompt. Alternatively, type `cmd` in the Instant Search box then press **Ctrl+Shift+Enter**.



Opening an elevated command prompt. (Screenshot used with permission from Microsoft.)

When run as administrator, the title bar shows "Administrator: Command Prompt" and the default folder is `C:\Windows\System32` rather than `C:\Users\Username`.



Elevated command prompt. (Screenshot used with permission from Microsoft.)



**Note:** You can use this technique to open other utilities, such as Explorer or Notepad, with administrative privileges.

## COMMAND SYNTAX

To run a command, type it at the prompt (>) using the command name and any switches and arguments using the proper syntax. When you have typed the command, press **Enter** to execute it.

The syntax of a command lists which arguments you must use (plus ones that are optional) and the effect of the different switches. Switches are usually preceded by the forward slash escape character.



**Note:** If an argument includes a space, it may need to be entered within quotes (".").

As you enter commands, the prompt fills up with text. If this is distracting, you can use the `cls` command to clear the screen.

Some commands, such as `nslookup` or `telnet`, can operate in interactive mode. This means that using the command starts that program and from that point, the prompt will only accept input relevant to the program. To exit the program you use the `exit` or `quit` command (or press **Ctrl+C**). The `exit` command will close the cmd window if not used within an interactive command.

## GETTING HELP

The command prompt includes a rudimentary help system. If you type `help` at the command prompt then press **Enter**, a list of available commands is displayed. If you enter `help CommandName`, help on that command is displayed, listing the syntax and switches used for the command. You can also display help on a particular command by using the `/?` switch (for example, `netstat /?` displays help on the `netstat` command).

```
Administrator: Command Prompt
C:\WINDOWS\system32>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
```

*Help on the netstat command. (Screenshot used with permission from Microsoft.)*

## TEXT EDITORS

Many files used by the operating system and applications are in a binary file format that can only be interpreted by the application. A plain text file can be modified in any text editor, but if it is saved through an application other than a basic text editor, it could be converted to a binary format and so become unusable. Windows supplies the basic text editor Notepad to modify text files. There are many third-party alternatives with better features, however.

## RUN COMMAND

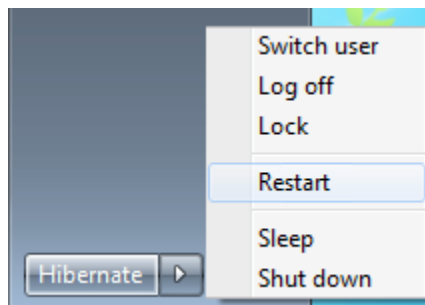
You can also execute commands from **Instant Search** or from the **Run** dialog box. If a command is interactive, it will open a command prompt window for input. If a command is non-interactive, the command prompt window will open briefly and close again as the command executes. If you want to force a command into interactive mode, use the `cmd /k` keyword before the command (for example, `cmd /k ipconfig`).

## WINDOWS SHUTDOWN OPTIONS

When the user wants to finish using Windows, simply disconnecting the power runs a risk of losing data or corrupting system files. There are various choices for closing or suspending a session:

- Shut down (/s)—close all open programs and services before powering off the computer. The user should save changes in any open files first but will be prompted to save any open files during shut down.
- Standby/Sleep—save the current session to memory and put the computer into a minimal power state.
- Hibernate (/h)—save the current session to disk before powering off the computer.
- Log off (/l)—close all open programs and services started under the user account but leave the computer running.
- Switch user—log on to another user account, leaving programs and files under the current account open.
- Lock—secure the desktop with a password while leaving programs running.
- Restart (/r)—close all open programs and services before rebooting without powering down. This is also called a soft reset.

These options can be selected from the Start Menu/**Start Screen** or by pressing **Ctrl +Alt+Del**.



*Options on the Windows 7 power button. (Screenshot used with permission from Microsoft.)*





**Note:** One of the "quirks" of Windows 8.0 was the lack of an obvious way to select the **Shut Down** command. Microsoft expected users to just use the physical power button, which on a modern computer invokes a shut down command (soft power) rather than a hard reset (unless you keep the power button pressed down). Users were reluctant to adopt this method, no doubt following years of IT departments telling them not to turn off a computer that way. The power options in Windows 8.0 are accessed via the Charms bar. The **Start** button and a power button on the **Start Screen** was returned in 8.1. In Windows 10, it appears right above the **Start** button, where no one can miss it.

The computer can also be shut down at a command prompt by using the `shutdown` command plus the relevant switch (shown in the previous figure). If a shutdown is in progress, `shutdown /a` aborts it (if used quickly enough). The `/t nn` switch can be used to specify delay in seconds before shutdown starts; the default is 30 seconds.

## THE WINDOWS REGISTRY

The Windows registry provides a remotely accessible database for storing operating system, device, and software application configuration information. When you boot a Windows machine, the registry is populated with information about hardware detected in your system. During boot, Windows extracts information from the registry, such as which device drivers to load and in what order. Device drivers also send and receive data from the registry. The drivers receive load parameters and configuration data. Finally, whenever you run a setup program or configure the system via Control Panel/Settings or Administrative Tools, it will add or change data in the registry.

The registry does have a dedicated tool called `regedit` for direct editing, but it is not the tool you would use on an everyday basis to modify configuration data. Control Panel/Settings and Administrative Tools are better options for most tasks.

### REGISTRY STRUCTURE

The registry is structured as a set of five root keys that contain computer and user databases. The computer database includes information about hardware and software installed on the computer. The user database includes the information in user profiles, such as desktop settings, individual preferences for certain software, and personal printer and network settings.

Root Key Name	Description
HKEY_LOCAL_MACHINE	Hardware information such as bus type, system memory, device drivers, and startup control data. HKLM also contains the Security Accounts Manager (SAM) password file (not viewable) and system-wide software settings.
HKEY_CLASSES_ROOT	Object Linking And Embedding (OLE) and file association data.
HKEY_CURRENT_USER	Contains the profile for the user who is currently logged on, including environment variables, desktop settings, network connections, printers, and application preferences.
HKEY_USERS	Contains all actively loaded user profiles, including HKEY_CURRENT_USER, which always refers to a child of HKEY_USERS, and the default profile.
HKEY_CURRENT_CONFIG	Contains system and software configuration information specific to this session.

## SUBKEYS AND VALUES

Each root key can contain subkeys and data items called value entries. Subkeys are analogous to folders and the value entries are analogous to files. A value entry has three parts: the name of the value, the data type of the value, and the value itself. The following table lists the different data types.

Data Type	Description
REG_BINARY	Raw binary data. Most hardware component information is stored as binary data and displayed in hex format.
REG_DWORD	Data represented by a 4-byte number. Many parameters for device drivers and services are this type and can be displayed in binary, hex, or decimal format.
REG_SZ	A string or sequence of characters representing human-readable text.
REG_MULTI_SZ	A multiple string. Values that contain lists or multiple text values are usually this type. Entries are separated by NULL characters.
REG_EXPAND_SZ	An expandable data string, which is text that contains a variable to be replaced when called by an application. For example, the string %SystemRoot% would be replaced by the actual location of the folder containing the Windows system files.

## REGISTRY DATABASE FILES

The registry database is stored in binary files called **hives**. A hive comprises a single file (with no extension), a .LOG file (containing a transaction log), and a .SAV file (a copy of the key as it was at the end of setup). The system hive also has an .ALT backup file. Most of these files are stored in the %SystemRoot%\System32\Config folder, but hive files for user profiles are stored in the folder holding the user's profile. The following table shows the standard hives.

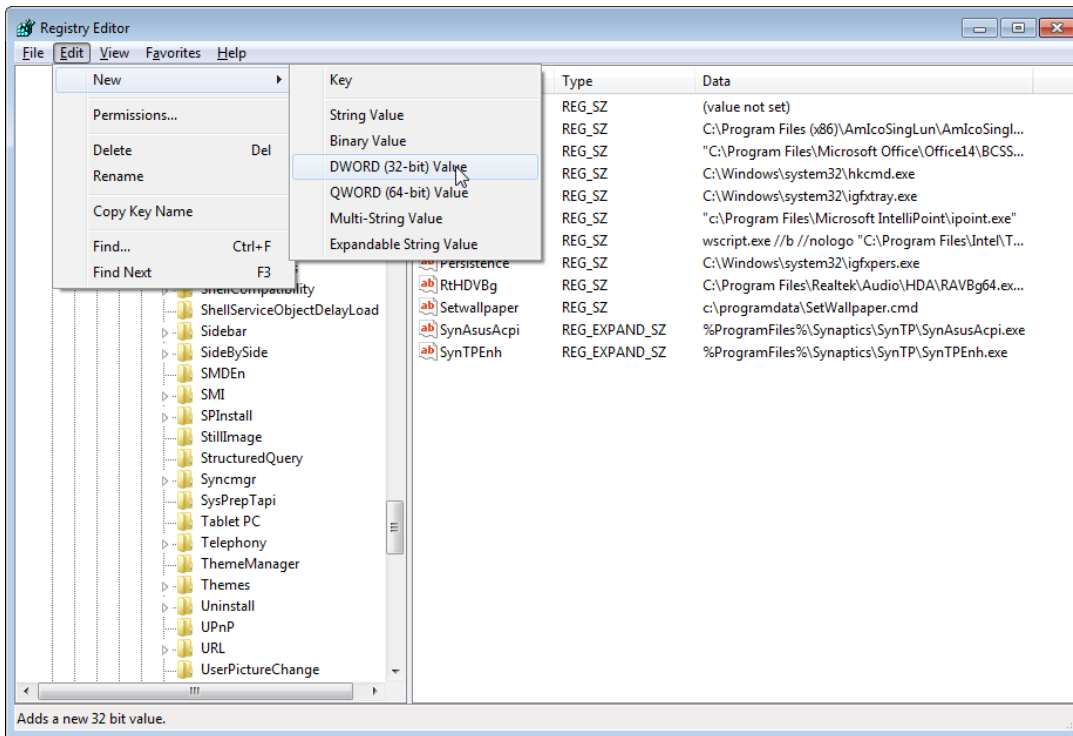
Hive	Files
HKEY_CURRENT_CONFIG	system, system.alt, system.log, system.sav
HKEY_CURRENT_USER	ntuser.dat, ntuser.dat.log
HKEY_LOCAL_MACHINE SAM	ssam, sam.log, sam.sav
HKEY_LOCAL_MACHINE\SECURITY	security, security.log, security.sav
HKEY_LOCAL_MACHINE\SOFTWARE	software, software.log, software.sav
HKEY_LOCAL_MACHINE\SYSTEM	system, system.alt, system.log, system.sav
HKEY_USERS\DEFAULT	default, default.log, default.sav
HKEY_CLASSES_ROOT	Not stored in a hive but built from the \SOFTWARE \CLASSES keys in CURRENT_USER and LOCAL_MACHINE

## EDITING THE REGISTRY

You can start the Registry Editor by running `regedit` via **Instant Search**, the **Run** dialog box, or the command prompt. You can use it to view or edit the registry and to back up and restore portions of the registry.

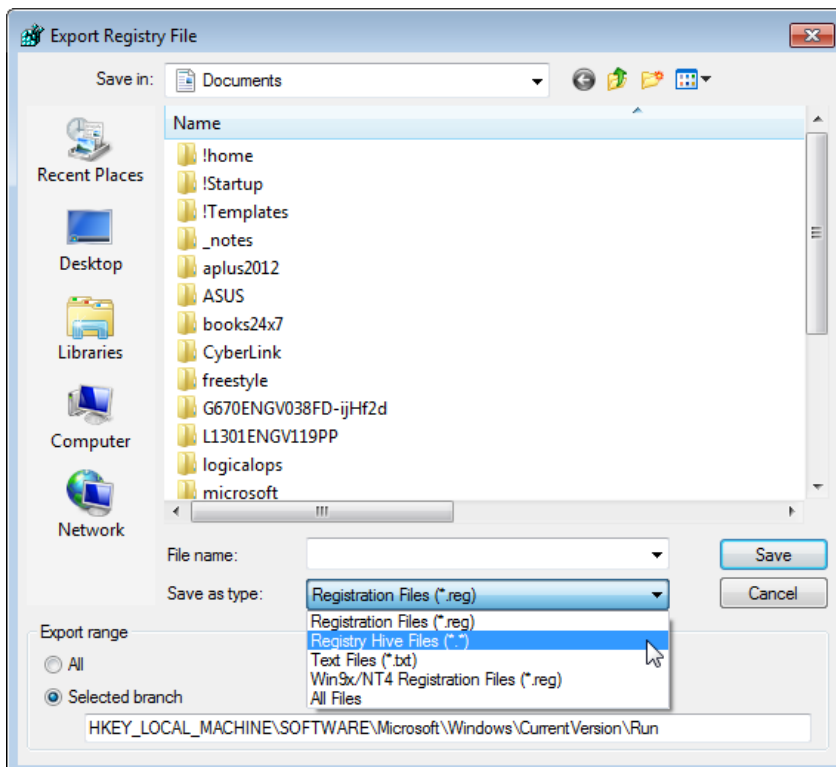
Use the **Find** tool (**Ctrl+F**) to search for a key or value. If you want to copy portions of the registry database and use them on other computers, select **File→Export Registry**

**File.** The file will be exported in a registry-compatible format and can be merged into another computer's registry by double-clicking the file (or calling it from a script).



*Editing the registry. (Screenshot used with permission from Microsoft.)*

A registration file is a plain text file. If you merge changes from a .reg file back to the registry, additions that you have made to the registry will not be overwritten.



*Selecting a file format for exporting a registry key. (Screenshot used with permission from Microsoft.)*

Use the **Registry Hive Files** format to create a binary copy of that portion of the registry. Restoring from the binary file will remove any additions you made, as well as reversing the changes.

## HOW TO EDIT THE WINDOWS REGISTRY

Here is a general procedure that you can follow to edit the Windows registry.

### EDIT THE WINDOWS REGISTRY

To edit the Windows registry:

1. Open **Instant Search**, the **Run** dialog box, or a command prompt.
2. Enter the `regedit` command.
3. If necessary, select **Yes** in the **User Access Control** dialog box.
4. To search for a key or value, select **Edit→Find** or press **Ctrl+F**, type the key or value name, and select **Find Next**.
5. To edit a key or value, double-click it in the right pane to open its dialog box; then change the necessary parameters and select **OK**.
6. To copy portions of the registry database and use them on other computers, select **File→Export**, provide a name for the export file, and select **Save**. The file will be exported in a registry-compatible format and can be merged into another computer's registry by double-clicking the file (or calling it from a script).

ISBN-13 978-1-6427-4145-2  
ISBN-10 1-6427-4145-0



9

781642 741452