

Windows XP System Requirements

	Windows XP Home / Professional Minimum Requirements	Windows XP Home / Professional Recommended Requirements
Processor / CPU	233 MHz	300 MHz or higher
Memory	64 MB RAM	128 MB RAM
Free disk space	1.5 GB	
Disk requirements	CD-ROM or DVD-ROM drive	
Video	SVGA (800x600)	
Input devices	Mouse and Keyboard	

	Windows XP Media Center Minimum Requirements	Windows XP Media Center Maximum
Processor / CPU	1.6 GHz	Two physical CPUs
Memory	256 MB RAM	4 GB RAM
Free disk space	60 GB	256 TB
Disk requirements		DVD-ROM drive
Video	1024 x 768	High resolution
Input devices	Mouse and Keyboard	Remote control, 4 Tuners

Windows Vista System Requirements

	Windows Vista Home Basic Minimum Requirements	Windows Vista Home Premium / Ultimate / Business / Enterprise Minimum Requirements
Processor	800 MHz	1 GHz
Memory	512 MB RAM	1 GB RAM
Hard drive size / Free space	20 GB / 15 GB	40 GB / 15 GB
Disk requirements	DVD-ROM Drive	DVD-ROM Drive
Video	32MB of graphics RAM	128MB of graphics RAM

Windows 7 System Requirements

	Windows 7 Minimum Requirements (x86)	Windows 7 Minimum Requirements (x64)
Processor / CPU		1 GHz processor
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video		DirectX 9 graphics device with WDDM 1.0 or higher driver

An Overview of Windows 7

	DVD Playback	Aero	ICS	IIS	Domain Member	EFS	BitLocker	x86 RAM	x64 RAM
Starter	✗	✗	✗	✗	✗	✗	✗	2 GB	N/A
Home Premium	✓	✓	✓	✓	✗	✗	✗	4 GB	16 GB
Professional	✓	✓	✓	✓	✓	✓	✗	4 GB	192 GB
Ultimate and Enterprise	✓	✓	✓	✓	✓	✓	✓	4 GB	192 GB

Aero - Windows 7 enhanced graphical interface

ICS - Internet Connection Sharing - One computer provides Internet for multiple devices

IIS - Internet Information Services - Microsoft's web server

EFS - Encrypting File System - Filesystem-level encryption of all data

Windows 7 Starter

- Built for netbooks

Windows 7 Home Premium

- The consumer edition

Windows 7 Professional

- Can connect to a Windows Domain

Windows 7 Ultimate and Enterprise

- Complete functionality
- Enterprise edition sold only with volume licenses

Upgrading Windows

In-place upgrade

- Maintain existing applications and data
- Data backup not required (but recommended)
- Start the setup from inside the existing OS

Clean install

- Wipe the partition clean and reinstall
- Requires a data backup
- Migration tool can help

Image

- Deploy a clone on every computer
- May require additional licensing after imaging

Unattended installation

- Answer Windows questions in unattend.xml
- No installation interruptions

	Vista Home Basic	Vista Home Premium	Vista Business	Vista Ultimate
Windows 2000	Install	Install	Install	Install
Windows XP Home	Upgrade	Upgrade	Upgrade	Upgrade
Windows XP Professional	Install	Install	Upgrade	Upgrade
Windows XP Professional (x64)	Install	Install	Install	Install
Windows XP Media Center	Install	Upgrade	Install	Upgrade

	Windows 7 Starter	Windows 7 Home Basic	Windows 7 Home Premium	Windows 7 Professional	Windows 7 Ultimate	Windows 7 Enterprise
Windows XP - All Editions	Install	Install	Install	Install	Install	Install
Windows Vista Home Basic	Install	Upgrade	Upgrade	Install	Upgrade	Install
Windows Vista Home Premium	Install	Install	Upgrade	Install	Upgrade	Install
Windows Vista Business	Install	Install	Install	Upgrade	Upgrade	Upgrade
Windows Vista Ultimate	Install	Install	Install	Install	Upgrade	Install
Windows Vista Enterprise	Install	Install	Install	Install	Install	Upgrade

Network Command Line Tools

ipconfig – Windows TCP/IP configuration

- ipconfig /all - Show all TCP/IP details
- ipconfig /release - Release the DHCP lease
- ipconfig /renew - Renew the DHCP lease
- ipconfig /flushdns - Flush the DNS resolver cache

ping - Test reachability

- ping <ip address> - Test reachability to a TCP/IP address
- ping -t <ip address> - Ping until stopped with Ctrl-c
- ping -a <ip address> - Resolve address to a hostname
- ping -n <count> <ip address> - Send a # of echo requests
- ping -f <ip address> - Send with Don't Fragment flag set

tracert - Determine the route a packet takes to a destination

- Takes advantage of ICMP Time to Live Exceeded error message
- Not all devices will reply with ICMP Time Exceeded messages

nslookup - Lookup information from DNS servers

- Canonical names, IP addresses, cache timers, etc.

netstat - Network statistics

- netstat -a - Show active connections
- netstat -b - Show binaries
- netstat -n - Do not resolve names

nbtstat - Query NetBIOS over TCP/IP information

- nbtstat -n - List local NetBIOS names
- nbtstat -A <ip address> - List remote NetBIOS names
- nbtstat -a <device name> - List remote NetBIOS names

net - Windows network commands

- net use - Connect to a resource
- net view - List available resources
- net start / net stop - Start or stop Windows services

Windows Recovery Console and Command Prompt

Fixing the Master Boot Record

- fixmbr [device-name] - Fix the MBR on Windows XP
- bootrec /fixmbr - Fix the MBR on Windows Vista/7

Fixing the Volume Boot Record

- fixboot [drive] - Fix the boot sector on Windows XP
- bootrec /fixboot - Fix the boot sector on Windows Vista/7

File Systems

FAT32 - File Allocation Table

- Native support in Windows 2000 and newer
- Some older Windows versions provided limited FAT32 support
- Larger (2 terabyte) volume sizes
- Maximum file size of 4 gigabytes

NTFS – NT File System

- Windows NT, 2000, XP, Server 2003, Server 2008, Vista and 7
- Extensive improvements
- Quotas, file compression, encryption, symbolic links, large file support, security, recoverability, and more
- Many different versions

CDFS - Compact Disk File System

- ISO 9660 standard
- All operating systems can read the CD

Quick format

- Wipes data from the drive
- No additional checks

Full format

- Wipes data from the drive
- Checks for bad sectors
- Time consuming

OS command Line Tools

diskpart – Disk Partitioner

- Replaces the Pre-Windows-XP FDISK command

format - Format a disk

- Prepare a disk for use by the operating system

chkdsk - Check Disk

- chkdsk /f - Fixes logical errors on the disk
- chkdsk /r - Locates bad sectors, recovers information

md, cd, rd

- md - Make directory
- cd - Change directory
- rd - Remove directory

dir - Directory listing

- List files and directories

del - Delete

- Remove a file from a directory or disk

copy - Duplicate files

- copy /v - Verifies that new files are written correctly
- copy /y - Suppresses overwrite prompts

xcopy - Extended copy

- Copies multiple files and directory trees

robocopy - Robust copy

- Functionally replaces xcopy
- Designed to handle NTFS file system details

tasklist - Task List

- Displays a list of currently running processes
- Local or remote device

taskkill - Task Kill

- Terminate tasks by process id (PID) or image name

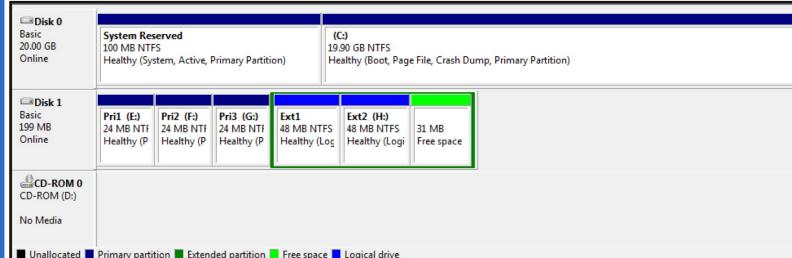
sfc - System File Checker

- sfc /scannow - Run the check
- Scan integrity of all protected system files

shutdown

- Shutdown a computer

Disk Partitions



Primary partitions

- Bootable partitions
- Maximum of four primary partitions per disk
- One of the primary partitions can be marked as active

Extended partitions

- Used for extending the maximum number of partitions
- One extended partition per hard disk (optional)
- Contains additional logical partitions
- Logical partitions inside an extended partition aren't bootable

Windows Operating System Tools

Computer Management

- A pre-built Microsoft Management Console

Device Manager

- View the status of all device drivers
- Enable and disable hardware devices

Users and Groups

- Manage access to the operating system
- Administrators and Guest users

Local Security Policy

- Administration of security rules
- Password policy, account lockout policy, etc.

Performance Monitor

- Gather long-term statistics
- Set alerts, store statistics

Windows Services

- Manage background processes
- Start, stop, manage automatic start
- Start with services.msc

System Configuration (msconfig)

- Manage boot processes, startup, services, etc.

Task Scheduler

- Schedule an application or batch file

Component Services

- Device COM+ Management, Event Viewer, Services

Data Sources

- Administer ODBC drivers and connectivity

Print Management

- Manage printers from one central console

Memory Diagnostics

- Perform a hardware check of your RAM
- Included with Windows Vista and 7

Windows Firewall

- Allows or disallows data transfer over the network
- Advanced Security provide additional security options in the rules

Task Manager

- Real-time system statistics
- CPU, memory, disk access

Disk Management

- Administer disk-related operations
- Drive status, adding drives, adding arrays

Migration Tools

- Side-by-side - Simultaneously move between two PCs
- Wipe-and-load - Export data, load new OS, and import
- File and Settings Transfer Wizard - Migrate from Windows 95, 98, 98SE, ME, NT 4.0, 2000, XP, and Server 2003 to Windows XP
- Windows Easy Transfer - Migrate from Windows XP, Vista, or 7
- User State Migration Tools (USMT) - Command-line migration

Windows Run Line Utilities

regedit - Registry editor

- Large master database
- Used by the kernel, drivers, services
- Can be used to backup and restore parts of the registry (hives)

mmc - Microsoft Management Console

- Build your own management framework
- Choose from a list of snap-ins
- The mmc framework is used by many built-in tools

mstsc - Microsoft Terminal Services Client

- Remote Desktop Connection
- Access a desktop on another computer
- Commonly used to manage "headless" servers



Notepad

- View and edit text files
- Included with all Windows versions

Explorer

- File management
- View, copy, launch files

msinfo32 - Windows System Information

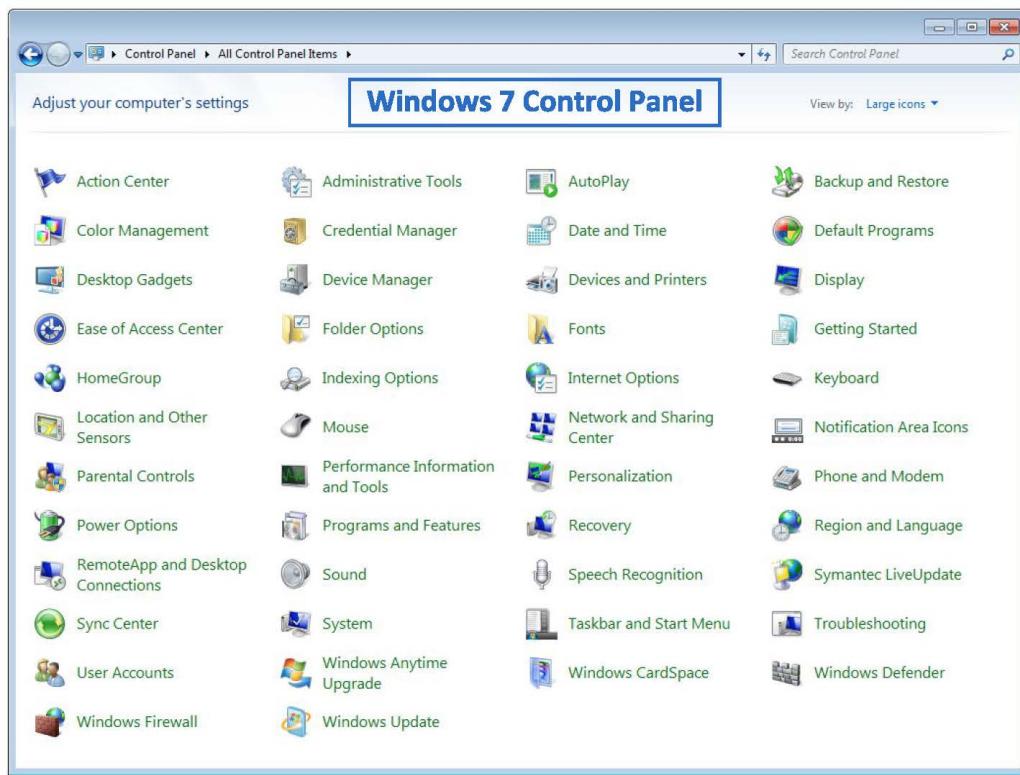
- Hardware resources - Memory, DMA, IRQs
- Components - Multimedia, input, network
- Software environment - Drivers, print jobs

System Information	
File	Edit
System Summary	
Hardware Resources	
Conflicts/Sharing	
DMA	
Forced Hardware	
I/O	
IRQs	
Memory	
Components	
Multimedia	
CD-ROM	
Sound Device	
Display	
Infrared	
Input	
Modem	
Network	
Ports	
Item	Value
OS Name	Microsoft Windows 7 Professional
Version	6.1.7601 Service Pack 1 Build 7601
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	AUXCONTROLCTR
System Manufacturer	innotek GmbH
System Model	VirtualBox
System Type	x86-based PC
Processor	Intel(R) Core(TM) i7-3770 CPU @ 3
BIOS Version/Date	innotek GmbH VirtualBox, 12/1/200
SMBIOS Version	2.5
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "6.1.7601.17514"

dxdia - DirectX Diagnostic Tools

- Manage your DirectX installation
- Multimedia API
- Generic diagnostic tool for audio and video

The Windows Control Panel



Internet Options

- Windows browser and proxy configuration

Display

- Resolution options, text size

User Accounts

- Local user account names and types

Folder Options

- Manage Windows Explorer options

System

- Computer information, OS version

Security Center

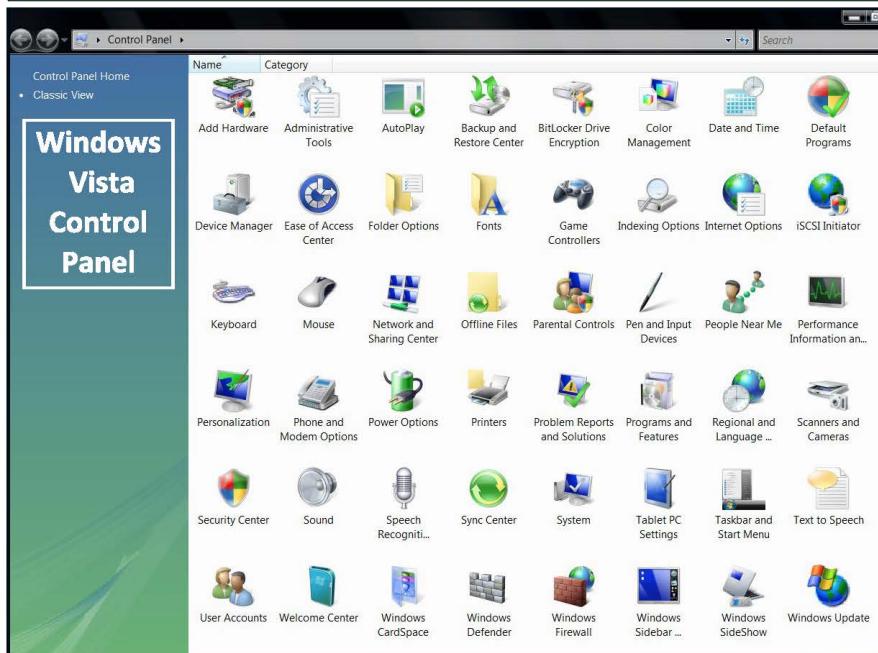
- Central security overview
- Anti-virus, anti-spyware, automatic updates

Windows Firewall

- Control network access, protect from attacks

Power Options

- Manage power use, especially on laptops
- Display, storage devices, hibernation options



Windows 7 Control Panel

Homegroup

- Easily share documents, pictures, music, video

Action Center

- Consolidated alert view for updates and security

RemoteApp and Desktop Connections

- Remote applications look like they're local
- Applications are configured on the server

Troubleshooting

- High-level diagnostics

Windows Vista Control Panel

Tablet PC Settings

- Handedness, handwriting recognition, display

Pen and Input Devices

- Tap options, pointer options, flicks

Offline Files

- Disk usage, encryption, and network options

Problem Reports and Solutions

- Automatic problem identification

Printers

- Common console for printer management

Windows XP Control Panel

Add/Remove Programs

- Programs, Windows components, program access

Network Connections

- Local, VPN, serial infrared, etc.
- Change firewall settings

Network Setup Wizard

- Step-by-step network setup

Printers and Faxes

- Start, pause, share printers
- Add a fax

Automatic Updates

- Security patches, OS updates



Windows Network Connections	Network Adapter Properties	Virtualization
Wired <ul style="list-style-type: none"> • Ethernet cable • The fastest connection is the default route Wireless <ul style="list-style-type: none"> • Network Name - SSID (Service Set Identification) • Always use WPA or WPA2 encryption Wireless Wide Area Network (WWAN) <ul style="list-style-type: none"> • Network using mobile providers Dialup <ul style="list-style-type: none"> • Uses a modem and standard phone lines VPN Concentrator <ul style="list-style-type: none"> • Establish a private network from remote locations • Windows includes a built-in VPN client 	Speed and Duplex <ul style="list-style-type: none"> • Auto-negotiation isn't always foolproof • Both sides of the link must match Wake on LAN <ul style="list-style-type: none"> • Computer sleeps until needed • Designed for late-night updates Quality of Service (QoS) <ul style="list-style-type: none"> • Prioritize network traffic • Applications, VoIP, video • Infrastructure must support QoS • DSCP (Differentiated Services Code Points) • Manage through Local Computer Policy 	<ul style="list-style-type: none"> • One computer, many operating systems <ul style="list-style-type: none"> • Host-based virtualization <ul style="list-style-type: none"> - Your normal desktop plus others <ul style="list-style-type: none"> • Hypervisor <ul style="list-style-type: none"> - The virtual machine manager <ul style="list-style-type: none"> • Requires extensive resources <ul style="list-style-type: none"> - CPU processor support - Memory to support multiple OS - Disk space for multiple OS - Network connection <ul style="list-style-type: none"> - Each OS connection is virtual
Preventive Maintenance Best Practices		Digital Security Techniques
Scheduled backups <ul style="list-style-type: none"> • Full backup - Copies everything • Differential backup <ul style="list-style-type: none"> - Copies everything since the last full backup • Incremental backup <ul style="list-style-type: none"> - Backup what's changed since the last full or incremental backup Scheduled disk checks <ul style="list-style-type: none"> • S.M.A.R.T. - Self-Monitoring, Analysis, and Reporting Technology • chkdsk - Logical and physical disk check Scheduled defragmentation <ul style="list-style-type: none"> • Moves file fragments so they are contiguous • Graphical version and defrag command • Configure using Task Scheduler Windows Updates <ul style="list-style-type: none"> • Security patches, new features, driver updates • Automated - download and install, download only Patch Management <ul style="list-style-type: none"> • A well-documented process • Testing, scheduling, implementing, and fallback Driver/firmware updates <ul style="list-style-type: none"> • Usually updated if a problem is identified • Many drivers updated through Windows Update Anti-virus updates <ul style="list-style-type: none"> • Signatures are constantly updated • Automatic schedule, daily or hourly 		Anti-virus <ul style="list-style-type: none"> • Always install an anti-virus application • New viruses are created daily; keep signatures updated Anti-spyware <ul style="list-style-type: none"> • Sends personal information to others • Use anti-spyware utility for prevention Host-based firewall <ul style="list-style-type: none"> • Protect against others on the networks • Can view all local applications Network firewall <ul style="list-style-type: none"> • Filters physical network connections by port number • Can encrypt and/or proxy Account information <ul style="list-style-type: none"> • A personal identifier • Usually combined with additional credentials Password protection <ul style="list-style-type: none"> • Strong passwords prevent brute-force attacks • Build passwords with letters, numbers, and special characters User rights and permissions <ul style="list-style-type: none"> • NTFS file permissions are more granular than FAT • Assign individual user permissions
Physical Security Techniques		Workstation Security Best Practices
Hardware locks <ul style="list-style-type: none"> • Conventional locks, electronic, biometric, etc. Tailgating <ul style="list-style-type: none"> • Walk behind someone else to gain access Dumpster diving <ul style="list-style-type: none"> • Important details thrown out with the trash Shredding <ul style="list-style-type: none"> • Cut papers into small pieces before discarding Things that you have (multi-factor authentication) <ul style="list-style-type: none"> • Additional evidence of proper authentication • Smart card, USB token, hardware/software token, SMS text Shoulder surfing <ul style="list-style-type: none"> • Low-tech spying • Can be minimized with privacy filters 		Password complexity <ul style="list-style-type: none"> • No single words, no obvious passwords • Use upper/lower case, special characters Restrict user permissions <ul style="list-style-type: none"> • Everyone isn't an administrator • Assign rights based on groups • Limit access based on job requirement and responsibilities Disable unnecessary accounts <ul style="list-style-type: none"> • Guest, root, mail, etc. - not all accounts are necessary • Disable interactive logins for services • Change the default usernames Desktop Security <ul style="list-style-type: none"> • Require a screensaver password and integrate with login • Disable autorun in XP and Vista in the registry • Consider changing AutoPlay

Disposing of Sensitive Data

Disk formatting

- Low-level formatting - Erases all data, requires special utilities
- High-level formatting - Does not erase the data

Hard drive security

- Remove data with file-level or whole disk data wiping
- Physical drive destruction may be required (shredder, drill, deguasser)

Android and iOS

Google Android

- Open Handset Alliance
- Open-source OS, based on Linux
- Supported on different devices

Apple iOS

- Apple iPhone and Apple iPad OS
- Based on Unix
- Exclusive to Apple products

Display Calibration

- Older resistive touchscreens required periodic calibration
- Modern capacitive touchscreens do not require calibration

Accelerometer

- Motion Sensor
- Detects orientation

Gyroscope

- Detects pitch, roll, and yaw
- Multi-axis sensing

GPS

- Satellite location tracking
- Longitude, latitude, altitude
- Provides maps and directions

Mobile Wireless Networking

- WiFi and Bluetooth
- Enable and disable independently

Bluetooth

- 10 meter short-range network

Bluetooth pairing

- Enable Bluetooth on both devices
- Set devices to discoverable mode
- Select discovered device
- Enter or confirm PIN
- Test connectivity

Mobile Device Synchronization

Data types

- Contacts, programs, email, pictures, music, videos, etc.

Synchronizing iOS

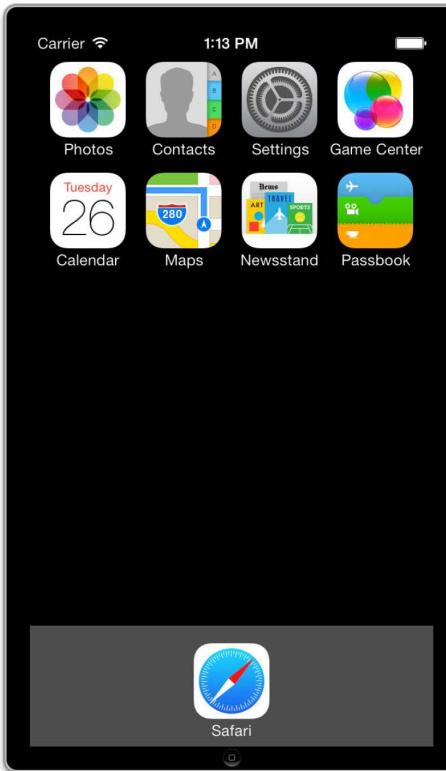
- Apple iTunes - Syncs everything in the phone
- Can sync wirelessly or wired

Synchronizing Android

- Syncs online with Google
- Transfer movies and music over USB



Google Android



Apple iOS

Securing a Wired and Wireless Network

Physical security

- Keep out unauthorized access
- Lock and key, electronic keyless, biometric

Default usernames and passwords

- All devices have default authentication
- Change defaults on all devices

Wireless encryption

- All wireless connections must be encrypted
- Use WPA/WPA2, do not use WEP

SSID Management

- Service Set Identifier - the wireless network name
- Change SSID from default
- Consider disabling SSID broadcasts

MAC address filtering

- Media Access Control - the physical address
- Limit access at the network level
- Easily spoofed, not a true security technique

Power level controls

- Limit wireless power to the bare minimum
- May require some study and testing

Automatic IP addressing

- Simplifies administration
- Simplifies security breaches

Disabling ports

- Conference rooms, break rooms
- Administratively disable
- Consider using Network Access Control (NAC), 802.1X

Mobile Device Security Best Practices

Passcode locks

- Restrict access to the device
- Choose a PIN or passphrase
- iOS: Erase everything after 10 failed attempts
- Android: Lock device and require Google login

Location apps and remote wipe

- Uses built-in GPS
- Find your phone or mobile device
- Make a sound or display a message on the device
- Wipe the phone over the Internet

Remote backup

- Backup to the cloud
- No local device required
- One-click restoration to a new device

Antivirus

- Apple iOS: Closed architecture
- Android: Apps can be installed from anywhere
- Apps run in a sandbox
- The user controls the scope of each application

Patching and OS Updates

- All devices need updates
- OS Updates, security patches
- Stay up-to-date to avoid security problems

Mobile Device Network Settings



Sending and Retrieving Mail

POP3 (Post Office Protocol 3)

- Downloads mail and deletes from server
- Used when you have only one email device

IMAP (Internet Message Access Protocol)

- Downloads mail to a device
- Keeps the email on the server
- Designed for multiple devices

SMTP (Simple Mail Transfer Protocol)

- Sends email
- Configured separately from inbound email config

Securing Email Transfers

- Configure SSL (Secure Socket Layer)
- Encrypts email between the device and server

Microsoft Exchange

- Uses its own protocols for sending and receiving
- Includes contacts, calendar, reminders, etc.
- Integrates with Active Directory database

Gmail

- Google's email service
- Web, POP, and IMAP
- Uses Google Calendar for scheduling

Hardware Troubleshooting Tools



Multimeter

- Measures voltage, current, resistance for AC and DC
- Also called a Volt-Ohm Meter (VOM)
- Check power supply voltage, cable continuity



Power supply tester

- Connect inline with devices for detailed power statistics
- Easier and faster than a multimeter



Loopback Plug

- Used for diagnostics and troubleshooting physical ports
- Determine if a received signal is the same as the sent signal



POST test cards

- Connects to expansion slots
- Runs diagnostics during boot

Mobile Device Cables



USB Standard
Type A



Apple 30-pin

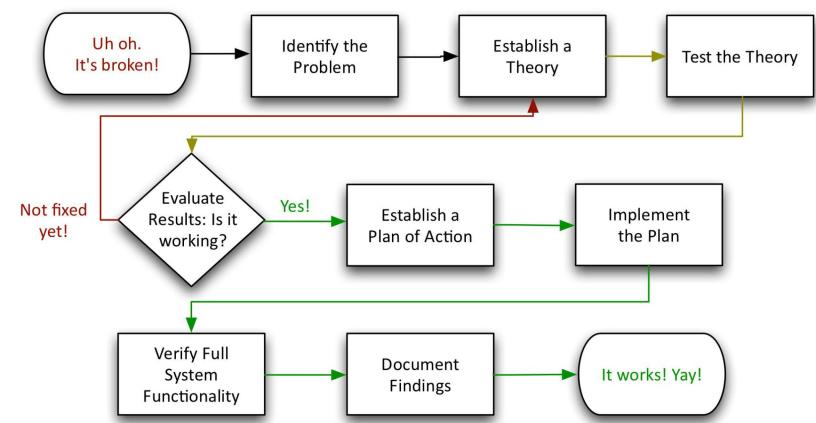


Apple 8-pin
Lightning



USB Micro-B

Troubleshooting Theory



- Identify the problem
 - Information gathering, identify symptoms, question users
- Establish a theory of probable cause
- Test the theory to determine cause
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventative measures
- Document findings, actions and outcomes

Troubleshooting Hardware Problems

Lockups

- Check for activity lights
- Update drivers and software patches
- Consider reverting to a restore point

POST (Power On Self Test)

- Tests system components before starting the OS
- Failures are noted with beeps and/or codes
- Every manufacturer uses different codes

Blank screen on boot

- Bad video, BIOS configuration issue
- Listen for the beeps

Booting to an incorrect device

- Set boot order in BIOS configuration
- Confirm that the boot device has a valid OS

Conginuous reboots

- How far does the boot process get?
- Try safe mode or OS recovery options

The CMOS battery

- Bad battery will display messages on every boot
- Can reset the BIOS by removing the battery

Excessive heat

- Heat generated from CPUs, video adapters, memory
- Check cooling fans and heat sinks
- Verify temperatures with monitoring software

Noise

- Loose components can rattle
- Hard drive scraping noises and clicking
- Check fans for obstructions

Odors

- Electrical problems
- Always disconnect power
- Locate and replace bad components

Status light indicators

- Seen often on network devices
- Power, link, speed, activity

Power and reboots

- No power - check the power supply
- Unexpected shutdown - run hardware diagnostics
- Only fans spin - check power supply output

Troubleshooting Hard Drives

Disk failures

- Read/write failure - "Cannot read from the source disk"
- BSOD (Blue Screen of Death) - Corrupted files, severe read/write failures
- Bad sectors - Identify with chkdsk
- Constant LED activity - Disk is constantly retrying
- Noise - Clicking and/or grinding

Boot failures

- Drive not recognized - Look for lights, noises, messages
- Check boot sequence in BIOS
- Check your cables
- For new install, check hardware config, i.e., PATA jumpers

File system problems

- OS not found - Rebuild the MBR and/or boot sector
- Windows XP - fixmbr, fixboot
- Windows Vista/7 - bootrec /fixmbr, bootrec /fixboot

RAID not found

- Missing or faulty RAID controller
- Reseat or replace controller card
- Confirm the RAID array drivers

RAID stops working

- Check the status of the drives
- Replace the bad drive
- Confirm status from the RAID console

Hard Drive Troubleshooting Tools

Physical tools

- Screwdriver with flat, crosspoint, and torx bits
- External disk enclosure can be used to move and troubleshoot drives

File recovery software

- Recover deleted and lost files
- Useful for recovery from deleted volumes or bad sectors

chkdsk (Check Disk)

- Fixes errors on the disk
- chkdsk /f - Repairs logical filesystem errors
- chkdsk /r - Finds bad sectors and attempts data recovery

format

- Initializes a disk with a fresh filesystem
- All data is erased

diskpart (Disk partitioning)

- Replaces the fdisk command
- Manage partitions from the command line

Network Troubleshooting Tools



Crimper

- "Pinches" the connector onto the wire
- The final step of a cable installation



Cable Tester

- Measure the quality of a cable installation
- Near end crosstalk, attenuation, etc.



Toner Probe

- Find a specific wire
- 2 pieces; tone generator and inductive probe



Punch-down tool

- Forces wires into a wiring block
- Trims the wires and breaks the insulation
- Organize your cables and document



Wireless locator

- Identify frequency usage
- Manage known and unknown signals
- Find interference from appliances, fluorescent lights, and other building tenants

No video image

- Check physical connection
- Confirm input selection on monitor
- Check brightness
- Swap the monitor with a known-good
- Start Windows in VGA mode (F8)

Image quality problems

- Flickering, colors missing, blur
- Check for bent interface connector pins
- Match Windows video refresh rate and resolution settings to the monitor specifications
- Disable hardware acceleration
- Degauss a CRT monitor

Pixel problems

- Stuck pixels (constantly bright)
- Dead pixels (always black)

Video artifacts

- Unusual graphics - check adapter
- Image persistency - turn off display
- Motion trails - Disable advanced video features

BSOD and overheating

- Update video drivers
- Monitor the PC's internal temperature

Printer Troubleshooting Tools**Laser printer maintenance kit**

- Feed rollers, new fuser unit, and additional parts
- Reset the page counters when work is complete

**Toner vacuum**

- Toner dust is very fine
- Wipe outside with a damp cloth
- Use toner vacuum to clean internal toner spills

**Compressed air**

- Canned fluorocarbon gas or powered air compressor
- Not a great choice for cleaning toner from printers
- Best used in an open area outside

Slow system performance

- Use Windows Update - Install latest patches and drivers
- Check for available disk space and defragment the drive
- Check for a laptop's power-saving mode
- Use Task Manager to find high CPU utilization and problem apps
- Scan for viruses and malware

Starting the system

- Device not starting - check Device Manager
- Event Viewer can provide additional details
- "One or more services failed to start"
 - Try starting manually
 - Check account permissions
 - Confirm service dependencies
 - Check system files of the service
 - Reinstall the application

Managing DLLs (Dynamic Link Library)

- Applications are written to use specific DLL versions
- Windows File Protection, Windows Resource Protection
 - Preserves DLL version to avoid conflicts

Files and compatibility errors

- File types/extensions are associated with applications
- Configure file associations
 - Windows XP: Folder Options / File Types tab
 - Windows Vista/7: Default Programs applet
- Compatibility tab
 - Run application as an older Windows app
 - Modify in file or shortcut properties

Boot problems

- Invalid boot disk
 - USB drive may be connected
 - Check the BIOS boot order
- Operating System Not Found
 - Boot device does not have a boot loader
 - Use Recovery Console to run chkdsk or repair MBR
- NTLDR missing
 - Boot files are missing; replace and reboot

Boot errors

- boot.ini errors
 - Vista/7 Boot Configuration Database (BCD)
 - Recovery Console: bootcfg /rebuild
- Improper shutdown
 - Windows Error Recovery window; may run autochk
- Missing GUI
 - There's no login dialog and/or no desktop
 - Driver corruption, update drivers in Safe Mode
- OS Repair or recover from backup

Bluescreens and spontaneous shutdowns

- BSOD on startup and shutdown; bad hardware or bad drivers
- Use Last Known Good, System Restore, or Rollback Driver
 - Safe Mode may help start a basic OS desktop
- Reseat or remove hardware
- Run hardware diagnostics

Automated System Recovery

- ASR does not back up or restore your data!
- This is the last resort of Windows XP recovery
- Accessories / System Tools / Backup; requires a floppy disk
- Recovery requires ASR floppy, system backup, and Windows CD
 - Restores disk signatures, volumes, and partitions
 - This is destructive! You will lose your data!
- The ASR process starts a data restore from a separate backup
- You should have a complete backup for this step

System Repair Disk

- System recovery options for Windows Vista/7
- Create a repair disk with Windows Backup and Restore
- The repair process does not format or modify data

Pre-installation environment

- A PE is a minimal Windows operating environment
- Used often for troubleshooting and recovery

msconfig

- Microsoft System Configuration
- Manage OS boot and startup configurations

regedit and regsvr32

- The Windows registry is the master database for the OS
- regedit - Registry editor
 - Modify registry settings, import/export
- regsvr32 - Microsoft Register Server
 - Register/unregister a DLL
 - Updates the registry

Event Viewer

- Central event log consolidation of OS information
- Events for Application, Security, Setup, System

Options at boot time

- Press F8 before the OS boots
 - Loads the Windows Advanced Options
- Provides options for Safe Mode, Windows Recovery Console, Last Known Good Configuration

Using Safe Mode

- Safe Mode
- Safe Mode with Networking
- Safe Mode with Command Prompt
- Enable low-resolution (VGA Mode)

Windows Recovery Console

- Windows XP - Start from Windows installation media
- Windows Vista/7 - System Recovery Options / Command Prompt
- Very powerful, very dangerous
- Use, copy, rename, replace files and folders
- Enable/disable service or device startup
- Repair the file system or Master Boot Record
- Create and format drive partitions

Browser pop-ups

- May look like a legitimate application
- Clicking the pop-up may load malicious software
- Can usually be enabled/disabled in the browser config

Browser redirection

- Instead of your intended location, browser goes elsewhere
 - Hijack Google search and send the browser elsewhere
- Usually caused by malware
- Creates a revenue stream for the malware authors

Browser security alerts

- The browser is warning you of a problem
- Problem with Security certificate trust issue, expiration, etc.

**Malware symptoms**

- Slow performance and lock-ups
- Internet connectivity issues
 - Limits your access to useful security sites
- Windows update failures
 - Keeps you vulnerable
- Malware can rename or delete files
 - File permissions can also change
 - The malware locks itself away from you

Virus alerts and hoaxes

- Appear to be legitimate warning messages
- May require money to "unlock" your PC
- Can sometimes be cleaned and removed
- Some malware may not be a hoax, always check

**Email security**

- Spam can include malware links and malicious software
- Hijacked computers can become spam broadcasters
- Hijacked devices can also be controlled remotely

Best Practices for Malware Removal

Identifying malware

- Odd application errors and security alerts
- System performance problems, slow boot time
- Hoax anti-virus or malware messages may appear
- Network activity may be more active

Quarantining infected systems

- Disconnect from the network
- Isolate all removable media
- Hold down the shift key to disable Autorun
- Don't transfer files or try to backup

Disable System Protection

- Restore Points can re-infect the computer
- Disable System Protection before cleaning
- Delete all Restore Points

Update anti-virus software

- Update anti-virus signatures and engines
- Configure automatic updates
- Existing malware may block the update process

Remediate infected systems

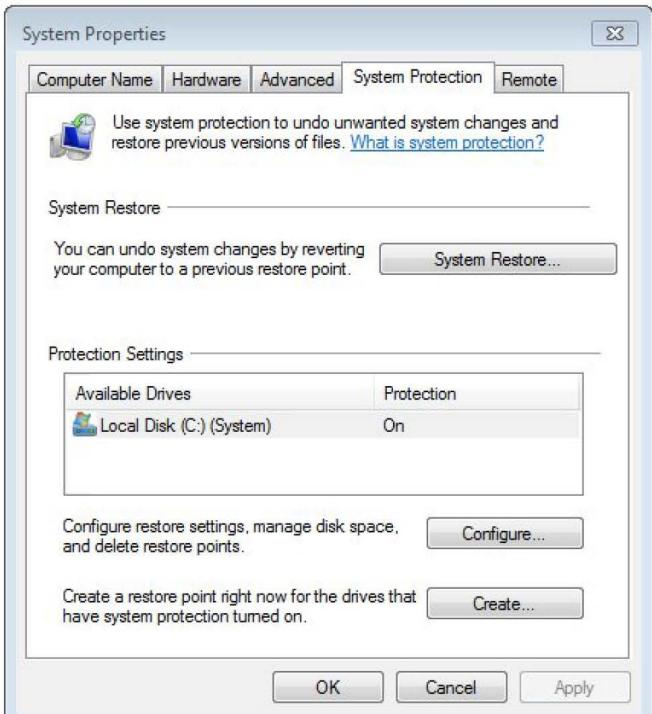
- Use anti-virus software to remove the malware
- May require a stand-alone removal app
- Best possible removal is delete and rebuild

Scan and removal techniques

- Use safe mode to load a minimum OS
- Boot to a preinstalled environment (PE)
- May need to repair the MBR and/or boot sectors

Enable System Protection

- After system is clean, resume normal operation
- Create a Restore Point right away



Training the user community

- Posters, signs, email, login messages, seminars
- Make sure that everyone is watching for infections

Troubleshooting Laptop Issues

LCD issues

- Dim video may be caused by a bad backlight
- Video may be barely visible without the backlight
- May need to replace the LCD inverter or display

Blurry video

- LCD displays have an optimal native resolution
- Check the manual to determine the correct resolution

The native resolution is the maximum resolution difference is that CRT runs lower resolution without



Flickering video

- Laptop LCDs are always opening and closing
- Connector issue, bad video cable or hardware

External monitor issues

- Usually toggled with the secondary Fn keys
- Toggles between LCD / external monitor / both
- Use an external monitor to bypass the LCD

Input issues

- Sticky keys require a cleaning - be careful, keycaps are delicate!
- Inadvertent mousepad touches cause cursor to jump around
 - Updated drivers may help
- Laptops Num lock can change the keyboard from letters to numbers

Battery not charging

- Battery may be too old to maintain a charge
- The charging hardware could be faulty
- Check the battery voltage with a multimeter

No laptop power

- Check the external power adapter with a multimeter
- Try a master laptop reset, i.e., hold power button for 10 seconds

Wireless antenna problems

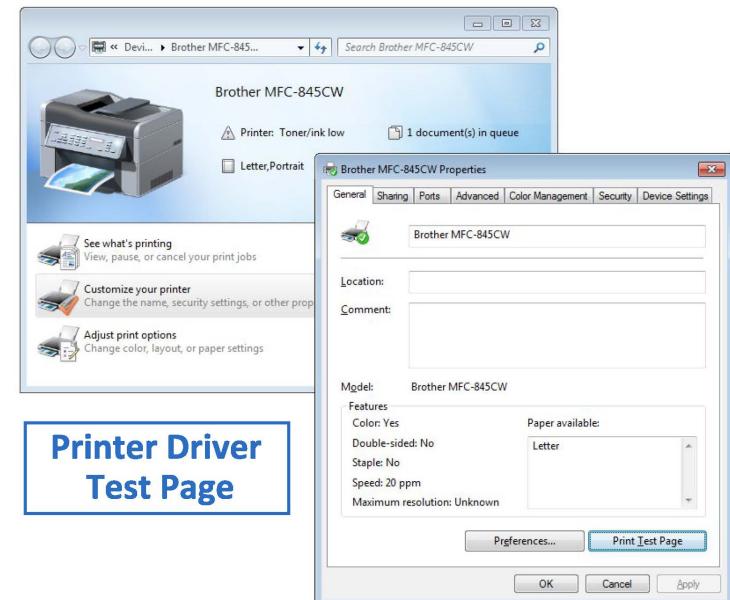
- A laptop has multiple antennas; WiFi main, WiFi aux, Bluetooth
- Antenna wires wrap around the top of the LCD to get up high
- It's easy to accidentally disconnect the wires during maintenance



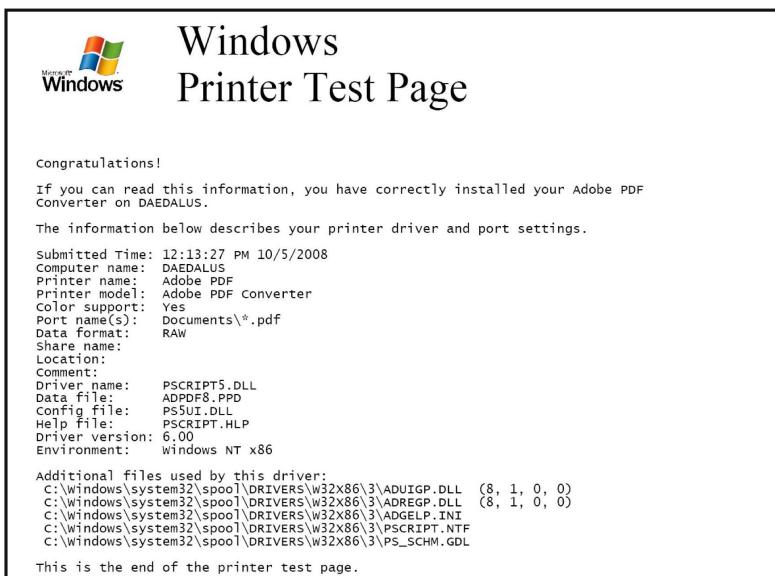
Troubleshooting Printer Problems

On-printer test page

- This checks the printer operation without any OS or application
- May be a power-on process or menu option
- If the printer's test page doesn't work, the printer is the problem



Printer Driver Test Page



Windows printer test page

- Print a test page from the Windows printer properties
- A bad Windows printer test page may be related to a driver, cable, interface, or connection

Streaks and blurs

- Inkjet - Clean the print heads
- Laser - Check for scratches on the photosensitive drum

Faded prints

- Low toner and low ink
- Poor quality toner or ink

Ghost images

- The laser printer optical drum may not be cleaning properly
- Print shows ghost or "shadow" from previous drum rotation

Garbled output

- Bad printer driver (PCL vs. PostScript)
- The application may be sending bad data
- Confirm the printer health with an on-printer test page

Laser printer smudging

- The toner isn't fusing to the paper
- The fuser unit may not be heating
- May require replacing the fuser unit

Color prints in wrong color

- Low ink in one cartridge
- Other colors should print normally

Paper jam

- Be careful when removing stuck paper
- Tray problem or bad pickup rollers may not feed paper properly
- Creased paper may cause problems in the paper path
- Check the paper weight with printer manufacturer specifications

Printer network issues

- No connectivity - Check for power and cabling
- Wireless printers may require additional network configuration
- Check Windows printer security tab for rights and permissions

Error messages

- Visible on the printer display console
- Low memory problems are related to laser printer RAM
 - Complex images and graphics consume more memory

Operating System issues

- Printer driver installation issues may be related to OS permissions
 - Make sure the correct driver is installing (32 bit vs 64 bit)
- Queue may not be moving, with print jobs "stuck" in the queue
 - The print spooler may have crashed or not working
 - Restart the spooler from the Windows Services

Study Tips

Exam Preparation

- Download the exam objectives, and use them as a master checklist
- Use as many training materials as possible. Books, videos, and Q&A guides can all provide a different perspective of the same information.
- It's useful to have some hands-on, especially with command-line features and Windows recovery options.

Taking the Exam

- Use your time wisely. You've got 90 minutes to get through everything.
- Choose your exam location carefully. Some sites are better than others.
- Get there early. Don't stress the journey.
- Manage your time wisely. You've got 90 minutes to get through everything.
- Wrong answers aren't counted against you. Don't leave any blanks!
- Mark difficult questions and come back later. You can answer the questions in any order.