



Cramsession™ for Windows 2000 Professional

This study guide will help you to prepare for Microsoft exam 70-210, Installing, Configuring, and Administering Microsoft Windows 2000 Professional. Exam topics include Installation, Implementing & Administering Resources, Managing & Troubleshooting Hardware Devices, Monitoring & Optimization of System Performance & Reliability, Network Protocols & Services, and Implementing, Monitoring, & Troubleshooting Security.



Check for the newest version of this Cramsession

<http://cramsession.brainbuzz.com/checkversion.asp?V=2451898&FN=microsoft/win2kpro.pdf>



Rate this Cramsession

<http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Win2K+Professional>



Feedback Forum for this Cramsession/Exam

<http://boards.brainbuzz.com/boards/vbt.asp?b=635>

More Cramsession Resources:



Search for Related Jobs

<http://jobs.brainbuzz.com/BrowseJobSearchRes.asp>



CramChallenge - practice questions

<http://www.cramsession.com/signup/default.asp#day>



IT Resources & Tech Library

<http://itresources.brainbuzz.com>



Certification & IT Newsletters

<http://www.cramsession.com/signup/>



SkillDrill - skills assessment

<http://www.skilldrill.com>



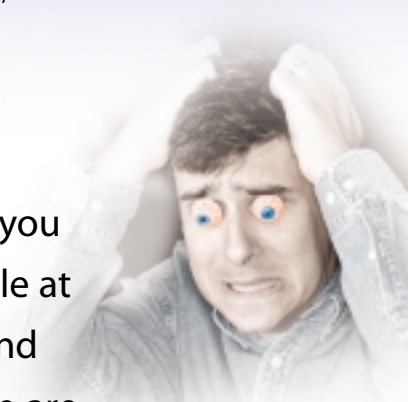
Discounts, Freebies & Product Info

<http://www.cramsession.com/signup/prodinfo.asp>

Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, visit our [legal page](#).



Training so
INTENSE
you'll end up
positively
certifiable!



When success is critical and failure is not an option you need the kind of Intense training that is only available at Intense School. Information Technology training and certification through Intense School and Intense Prep are not for the weak of heart. They're for IT professionals who have the will to succeed and the conviction to reach their career goals. Our training isn't easy. It's **INTENSE!**

Intense School offers a wide range of **INTENSE** Information Technology Boot Camps specializing in:

- **Windows 2000® MCSE® certification in 14 days**
- **CCNA™ & CCDA™ certification in 6 days**
- **CCNP™ certification in 16 days**

Intense School for intense reasons:

- 95%+ pass rate in all Intense Boot Camps in 2000 – the highest in the industry
- Proprietary certification focused Windows 2000® curriculum
- Intense instructors are tops in the field – including well-known IT author/guru Kurt Hudson
- Expanded schedule and new locations for 2001

Classes are filling fast! To check availability go to:
www.IntenseSchool.com

Or, call now:

1-800-330-1446 or 954-370-7583

Intense Prep provides **INTENSE** Information Technology practice tests to prepare IT professionals for certification on:

- **Microsoft® including Windows 2000®**
- **Novell®**
- **Cisco®**
- **A+/Network+**

Jump start you career!

- Study in the comfort of your own home
- Intense Prep CD's are put together by industry leading professionals
- Certification focused Windows 2000® practice tests
- All materials are competitively priced

Download a FREE demo today:
www.IntensePrep.com/downloaddemo/

Or, for more information, call now:

1-877-996-3100 or 954-577-3100

FT. LAUDERDALE, FL | COLUMBUS, OH | SAN DIEGO, CA



This material is not sponsored, endorsed or affiliated with Cisco® Systems, Inc. Cisco®, Cisco Systems®, CCNA™, CCDA™, CCNP™, are the trademarks or registered trademarks of Cisco® Systems, Inc. All other trademarks are trademarks of their respective owners.

The evolution of NT School to Intense School/ Intense Prep enables us to offer a host of new products and services in the field of accelerated IT training and certification.





Contents:

Contents:	1
Installing Windows 2000 Professional.....	4
Requirements.....	4
Attended installations.....	5
Unattended installations	8
Remote installations.....	8
Working with SYSDIFF.....	9
System preparation tool (SYSPREP.EXE): (KB# Q240126)	9
Upgrading from a previous version: (KB# Q232039).....	10
Troubleshooting failed installations.....	10
Choosing a file system.....	11
NTFS file and folder permissions: (KB#S Q183090, Q244600).....	12
Miscellaneous:	12
Windows File Protection Feature (WFP): (KB# Q222193)	13
Local and network print devices.....	13
Managing file systems: (KB# Q222189).....	14
There are three volume types.....	14
Dynamic Volume States.....	14
Dynamic Volume Limitations	15
Translation of terms between Basic and Dynamic Disks	15
When using the Disk Management Snap-in Tool.....	16
Implementing, Managing, and Troubleshooting Hardware Devices and Drivers: (KB#Q199276)	16
Miscellaneous	16
Disk devices.....	16
Display devices.....	17
Mobile computer hardware.....	17
Input and output (I/O) devices.....	18
Updating drivers	18
Managing/configuring multiple CPUs.....	18
Install and manage network adapters.....	18
Troubleshooting the boot process.....	19
ARC paths in BOOT.INI: (KB# Q113977 & Q119467)	19
BOOT.INI switches: (KB# Q239780)	20
Bootting in Safe Mode: (KB# Q202485).....	20
Windows 2000 Control Sets: (KB# Q142033).....	20



Running the Recovery Console: (KB# Q229716).....	21
Startup and Recovery Settings	22
Windows Report Tool: (KB# Q188104)	22
Emergency Repair Disk:	23
Monitoring and Optimizing System Performance and Reliability	23
Driver signing: (KB# Q224404).....	23
Configuring Driver Signing: (KB# Q236029).....	23
Using System File Checker (sfc.exe): (KB# Q222471)	23
Windows Signature Verification (sigverif.exe)	23
Task scheduler: (KB# Q235536 & Q226262).....	24
Using offline files	24
Performance Console: (KB# Q146005)	24
Performance Alerts and Logs: (KB# Q244640)	25
Virtual memory/Paging file.....	25
Hardware profiles.....	26
Data recovery	26
The Windows 2000 Registry:	26
Secondary Logon Service (Run As): (KB# Q225035)	27
Configuring and Troubleshooting the Desktop Environment	27
User profiles.....	27
Multiple languages and locations.....	28
Using Microsoft Installer Packages: (KB# Q242479).....	28
Configure and troubleshoot desktop settings	28
Fax support.....	28
Accessibility services: (KB# Q210894)	29
TCP/IP protocol	29
Miscellaneous	29
Automatic Private IP Addressing	30
TCP/IP Server Utilities	30
TCP/IP Client Utilities	30
Services for UNIX 2.0	31
Miscellaneous	31
Client for NFS.....	31
Server for NFS.....	32
Gateway for NFS.....	32
Server for PCNFS.....	32
Server for NIS	33



Troubleshooting: (KB# Q102908)	33
NWLink (IPX/SPX) and NetWare Interoperability	33
(KB# Q220872).....	33
Other protocols.....	34
Remote Access Services (RAS)	34
Authentication protocols	34
Virtual Private Networks (VPNs).....	34
Multilink Support: (KB# Q235610).....	35
Setting Callback Security	35
Dial-up networking.....	35
Using shared resources on a Microsoft Network	36
Security levels for network access to shared folders	36
Implementing, Monitoring, and Troubleshooting Security	37
Active Directory Overview	37
Active Directory Structure.....	37
Site Replication	38
Active Directory Concepts	39
Active Directory Naming Conventions	39
Local user accounts: (KB# Q217050)	39
Local user authentication	40
Group Policy.....	41
Incremental Security Templates for Windows 2000	42
Local Group Policy.....	42
Non-local Group Policy (stored in Active Directory).....	42
Config.pol, NTConfig.pol and Registry.pol.....	42
Security configuration	43
Encrypting File System (EFS): (KB# Q223316 & Q230520)	44
Using the CIPHER command.....	45
IPSec: (KB# Q231585).....	45

Installing Windows 2000 Professional

Requirements

Component	Recommended Minimum	Suggested Configuration
CPU	Pentium-based	Pentium II or higher
Memory	32 MB	64 MB or higher
Hard disk space	685 MB	2 GB or higher
Networking	NIC	NIC
Display	VGA	SVGA
CD-ROM	needed when not installing over the network	needed when not installing over the network
Keyboard and mouse	required	Required
Sound card	not required	required for visually impaired users needing narrative voice to guide installation

- All hardware should appear on the Windows 2000 Hardware Compatibility List (HCL) (KB# [Q142865](#))
- Windows 2000 Professional supports Symmetric Multi-processing with a maximum of two processors, and up to 4 GB of RAM.

Attended installations

Setup has four stages

1. Setup Program (text mode)- preps hard drive for following stages of install and copies files needed for running Setup Wizard. Requires reboot.
2. Setup Wizard (graphical mode) - prompts for additional info such as product key, names, passwords, regional settings, etc.
3. Install Windows Networking - detects adapter cards, installs networking components (Client for MS Networks, File & Printer Sharing for MS Networks), and installs TCP/IP protocol by default (other protocols can be installed later). Choose to join a workgroup or domain at this point (must be connected to network and provide credentials to join a domain). After all choices are made components are configured, additional files copied, and the system is rebooted.
4. Setup Completion - installs Start Menu items, register's components, saves configuration, removes temporary files and system rebooted one final time.

Installing from CD-ROM

- Setup disks are not required if your CD-ROM is bootable or you are upgrading a previous version of Windows.
- To make boot floppies, type **makeboot a:** in the \i386 directory of your W2K CD. Creates set of four 1.44 MB boot floppies. (KB# [Q197063](#))
- If installing using a MS-DOS or Win95/98 boot floppy, run **winnt.exe** from the i/386 to begin Windows 2000 setup.
- Setup will not prompt the user to specify the name of an installation folder unless you are performing an unattended installation or using **winnt32** to perform a clean installation. (KB# [Q222939](#))

Installing over a Network

- Create a distribution server which has a file share containing the contents of the /i386 directory from the Windows 2000 CD-ROM.
- 685 MB minimum plus 100 - 200 MB free hard drive space to hold temporary files during installation.
- Install a network client on the target computer or use a boot floppy that includes a network client (KB# [Q142857](#)). Run **winnt.exe** from file share on distribution server if installing a new operating system or **winnt32.exe** if upgrading a previous version of Windows.
- Clean installation is now possible with Windows 2000. NT 4 required a pre-existing FAT partition.

Command line switches for winnt.exe

Switch	Function
/a	Enables accessibility options
/e[:command]	Specifies a command that will be run at the end of Stage 4 of setup
/r[:folder]	Specifies optional folder to be installed. Folder is not removed with temporary files after installation
/rx[:folder]	Specifies optional folder to be copied. Folder is deleted after installation
/s[:sourcepath]	Specifies source location of Windows 2000 files. Can either be a full path or network share
/t[:tempdrive]	Specifies drive to hold temporary setup files
/u[:answer file]	Specifies unattended setup using answer file (requires /s)
/udf:id[,UDF_file]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file

Modifying Setup using winnt32.exe

Switch	Function
/checkupgradeonly	Checks system for compatibility with Windows 2000. Creates reports for upgrade installations.
/copydir: <i>folder_name</i>	Creates additional folder inside %systemroot% folder. Retained after setup.
/copysource: <i>folder_name</i>	Same as above except folder and it's contents are deleted after installation completes
/cmd: <i>command_line</i>	Runs a command before the final phase of Setup
/cmdcons	This adds a Recovery Console option to the operating system selection screen
/debug[<i>level</i>] [: <i>file_name</i>]	Creates a debug log. 0=Sever errors only. 1=regular errors. 2=warnings. 3=all messages.
/m: <i>folder_name</i>	Forces Setup to look in specified folder for setup files first. If files are not present, Setup uses files from default location.
/makelocalsource	Forces Setup to copy all installation files to local hard drive so that they will be available during successive phases of setup if access to CD drive or network fails.
/nodownload	Used when upgrading from Win95/98. Forces copying of winnt32.exe and related files to local system to avoid installation problems associated with network congestion. (KB# Q244001)
/noreboot	Tells system not to reboot after first stage of installation.
/s: <i>source_path</i>	Specifies source path of installation files. Can be used to simultaneously copy files from multiple paths if desired (first path specified must be valid or setup will fail, though).
/syspart: <i>drive_letter</i>	Copies all Setup startup files to a hard disk and marks the drive as active. You can physically move the drive to another computer and have the computer move to Stage 2 of Setup automatically when it is started. Requires /tempdrive switch. (KB# Q234037 & Q241803)
/tempdrive: <i>drive_letter</i>	Setup uses the specified tempdrive to hold temporary setup files. Used when there are drive space concerns
/unattend: [number] [: <i>answer_file</i>]	Specifies answer file for unattended installations.

/udf:id[,udf_file]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file.
--------------------	---

Unattended installations

- Unattended installations rely on an *answer file* to provide information to provide information during setup process that is usually provided through manual user input. (KB# [Q183245](#))
- Answer files can be created manually using a text editor or by using the Setup Manager Wizard (SMW) (found in the Windows 2000 Resource Kit Deployment Tools).
- SMW allows for creation of a shared Distribution Folder and OEM Branding
- If you had a CD in drive D: and an unattended installation answer file named salesans.txt in C:\, you could start your install with this command:
D:\i386\winnt32 /s:d:\i386 /unattend:c:\salesans.txt (KB# [Q216258](#))
- There are five levels of user interaction during unattended installs:
 1. *Provide Defaults* - Administrator supplies default answers and user only has to accept defaults or make changes where necessary.
 2. *Fully Automated* - Mainly used for Win2000 Professional desktop installs. User just has to sit on their hands and watch.
 3. *Hide Pages* - Users can only interact with setup where Administrator did not provide default information. Display of all other dialogs is suppressed.
 4. *Read Only* - Similar to above, but will display information to user without allowing interaction to pages where Administrator has provided default information.
 5. *GUI Attended* - Only used for automating the second stage of setup. All other stages require manual input.

Remote installations

- Only supports installation of Windows 2000 Professional at this time.
- Requires the presence of a Windows 2000 Remote Installation Services (RIS) server. Following services are also needed on the network; DNS (for locating directory service and client computer accounts), DHCP (to get an IP address), and Active Directory (to locate RIS servers). (KB# [Q239004](#))
- RIS must be mounted on a shared hard drive volume, but not the same volume that is running Windows 2000 Server and must be formatted with NTFS.
- Shared volume must be large enough to hold RIS as well as numerous Windows 2000 Professional drive (RIPRep) images.
- RIPRep images can have applications pre-installed. Unique identifiers are like SIDs are stripped from RIPRep images as they are generated.
- Uses .SIF files - variation of unattend.txt files.

- Once RIS is installed on the server and the service is running, use the Remote Boot Disk Generator (RBFGE.EXE) to create remote installation boot disks. These floppies only support the PCI-based network adapters that can be selected by using the "Adapter List" button. Alternately, if the client system has a PXE based NIC or is a NetPC, you don't need a boot floppy.
- Client computers can have differing hardware configurations so long as they use the same Hardware Abstraction Layer (HAL) (KB# [Q228908](#))
- Run **riprep.exe** to start the RIS Wizard.

Working with SYSDIFF

- Used for installing applications, usually in conjunction with an unattended installation. SYSDIFF allows you to take a snapshot of your machine's original state, install applications, and then package all of these changes into a single file which can be applied to other machines.
- Install your baseline system first. Then take a snapshot of it before installing any applications. Syntax is: **sysdiff /snap snap_file**
- Next install desired applications on target system. Use the SYSDIFF tool to create a difference file. Syntax is: **sysdiff /diff snap_file diff_file**
- You can now apply your difference file to the target system(s). Syntax is: **sysdiff /apply \\setupserver\w2k\diff_file**

System preparation tool (SYSPREP.EXE): (KB# [Q240126](#))

- Removes the unique elements of a fully installed computer system so that it can be duplicated using imaging software such as Ghost or Drive Image Pro. Avoids the NT4 problem of duplicated SIDS, computer names etc. Installers can use sysprep to provide an answer file for "imaged" installations.
- Must be extracted from DEPLOY.CAB in the \support\tools folder on the Windows 2000 Professional CD-ROM.
- Adds a mini-setup wizard to the image file which is run the first time the computer it is applied to is started. Guides user through re-entering user specific data. This process can be automated by providing a script file. (KB# [Q196667](#))
- Use Setup Manager Wizard (SMW) to create a SYSPREP.INF file. SMW creates a SYSPREP folder in the root of the drive image and places sysprep.inf in this folder. The mini-setup wizard checks for this file when it runs.
- Specifying a CMDLINES.TXT file in your SYSPREP.INF file allows an administrator to run commands or programs during the mini-Setup portion of SYSPREP. (KB# [Q238955](#))
- Available switches for sysprep.exe are: /quiet (runs without user interaction), /pnp (forces Setup to detect PnP devices), /reboot (restarts computer), and /nosidgen (will not regenerate SID on target computer).

Upgrading from a previous version: (KB# [Q232039](#))

- Run **winnt32.exe** to upgrade from a previous version of Windows. (KB# [Q199349](#))
- Windows 2000 will upgrade and preserve settings from the following operating systems: Windows 95 and 98 (all versions), Windows NT Workstation 3.51 and 4.0, and Windows NT 3.1 or 3.5 (must be upgraded to NT 3.51 or 4.0 first, then Professional).
- Upgrade installations from a network file share are not supported in Windows 2000 (this *can* be done, but only by using SMS). You must either do a CD-based upgrade or perform a clean installation of Windows 2000 and re-install needed applications.
- Because of registry and program differences between Win95/98 and 2000, upgrade packs (or migration DLLs) might be needed. Setup checks for these in the \i386\Win9xmig folder on the Windows 2000 CD-ROM or in a user specified location. (KB# [Q231418](#))
- Run **winnt32 /checkupgradeonly** to check for compatible hardware and software. Generates a report indicating which system components are Windows 2000 compatible. Same as running the **chkupgrd.exe** utility from Microsoft's site.
- All operating system files associated with Windows 95/95 will be deleted after an upgrade. (KB# [Q228986](#))

Troubleshooting failed installations

Common errors

Problem	Possible fix
Cannot contact domain controller	<i>Verify that network cable is properly connected. Verify that server(s) running DNS and a domain controller are both on-line. Make sure your network settings are correct (IP address, gateway, etc.). Verify that your credentials and domain name are entered correctly.</i>
Error loading operating system	Caused when a drive is formatted with NTFS during setup but the disk geometry is reported incorrectly. Try a smaller partition (less than 4 GB) or a FAT32 partition instead. (KB# Q234621)
Failure of dependency service to start	Make sure you installed the correct protocol and network adapter in the Network Settings dialog box in the Windows 2000 Setup Wizard. Also check to make sure your network settings are correct.
Insufficient disk space	Create a new partition using existing free space on the hard disk, delete or create partitions as needed or reformat an existing partition to free up space.
Media errors	Maybe the CD-ROM you are installing from is dirty or damaged. Try using a different CD or trying the affected CD in a different machine.

Nonsupported CD drive	Swap out the drive for a supported drive or try a network install instead. (KB# Q228852)
-----------------------	---

Log files created during Setup

Logfile name	Description
setupact.log	Action Log – records setup actions in a chronological order. Includes copied files and registry entries as well as entries made to the error log.
Setuperr.log	Error Log – records all errors that occur during setup and includes severity of error. Log viewer shows error log at end of setup if errors occur.
Comsetup.log	Used for Optional Component manager and COM+ components.
Setupapi.log	Logs entries each time a line from an .INF file is implemented. Indicates failures in .INF file implementations.
Netsetup.log	Records activity for joining a domain or workgroup.
Mmdet.log	Records detection of multimedia devices, their port ranges, etc.

Implementing and Conducting Administration of Resources

Choosing a file system

- NTFS provides optimum security and reliability through its ability to lock down individual files and folders on a user by user basis. Advanced features such as disk compression, disk quotas and encryption make it the file system recommended by 9 out of 10 MCSEs. (KB# [Q244600](#))
- FAT and FAT32 are only used for dual-booting between Windows 2000 and another operating system (like DOS 6.22, Win 3.1 or Win 95/98). (KB# [Q184006](#))
- Existing NT 4.0 NTFS system partition will be upgraded to Windows 2000 NTFS automatically. If you wish to dual-boot between NT4.0 and 2000 you must first install Service Pack 4 on the NT4.0 machine. This will allow it to read the upgraded NTFS partition, but advanced features such as EFS and Disk Quotas will be disabled. (KB# [Q197056](#) & [Q184299](#))
- Use **convert.exe** to convert a FAT or FAT32 file system to NTFS. NTFS partitions cannot be converted to FAT or FAT32 - the partition must be deleted and recreated as FAT or FAT32 (KB# [Q156560](#) & [Q214579](#))
- You cannot convert a FAT partition to FAT32 using **convert.exe**. (KB# [Q197627](#))

NTFS file and folder permissions: (KB#S [Q183090](#), [Q244600](#))

File attributes when copying/moving within a partition or between partitions:

Copying within a partition	Creates a new file resembling the old file. Inherits the target folders permissions.
Moving within a partition	Does not create a new file. Simply updates directory pointers. File keeps its original permissions.
Moving across partitions	Creates a new file resembling the old file, and deletes the old file. Inherits the target folders permissions.

Miscellaneous:

- NTFS in Windows 2000 (version 5) features enhancements not found in Windows NT 4.0 version 4). Reparse Points, Encrypting File System (EFS), Disk Quotas, Volume Mount Points, SID Searching, Bulk ACL Checking, and Sparse File Support. (KB# [Q183090](#))
- Volume Mount Points allow new volumes to be added to the file system without needing to assign a drive letter to it. Instead of mounting a CD-ROM as drive E:, it can be mounted and accessed under an existing drive (e.g., C:\CD-ROM). As Volume Mount Points are based on Reparse Points, they are only available under NTFS5 using *Dynamic Volumes*.
- NTFS4 stored ACLs on each file. With bulk ACL checking, NTFS5 uses unique ACLs only once even if ten objects share it. NTFS can also perform a volume wide scan for files using the owner's SID (SID Searching). Both functions require installation of the Indexing Service.
- Sparse File Support prevents files containing large consecutive areas of zero bits from being allocated corresponding physical space on the drive and improves system performance.
- NTFS partitions can be defragmented in Windows 2000 (as can FAT and FAT32 partitions). Use Start > Programs > Accessories > System Tools > Disk Defragmenter.
- Local security access can be set on a NTFS volume.
- Files moved from an NTFS partition to a FAT partition do not retain their attributes or security descriptors, but will retain their long filenames.
- Permissions are cumulative, except for No Access, which overrides anything.
- File permissions override the permissions of its parent folder.
- Anytime a new file is created, the file will inherit permissions from the target folder.
- The **cacls.exe** utility is used to modify NTFS volume permissions. (KB# [Q237701](#))

Windows File Protection Feature (WFP): (KB# [Q222193](#))

- New to Windows 2000 - prevents the replacement of certain monitored system files (important DLLs and EXEs in the %systemroot%\system32 directory).
- Uses file signatures and code signing to verify if protected system files are the Microsoft versions.
- WFP does not generate signatures of any type.
- Critical DLLs are restored from the %systemroot%\system32\dllcache directory. Default maximum size for Professional is 50MB. This can be increased by editing the Registry. (KB# [Q229656](#))

Local and network print devices

- Windows 2000 Professional supports the following printer ports: Line Printer (LPT), COM, USB, IEEE 1394, and network attached devices.
- Print services can only be provided for Windows and UNIX clients on Windows 2000 Professional (KB# [Q124734](#))- Windows 2000 Server is required to support Apple and Novell clients.
- Windows 2000 Professional automatically downloads the printer drivers for clients running Win2000, WinNT 4, WinNT 3.51 and Windows 95/98. (KB# [Q142667](#))
- Internet Printing is a new feature in Windows 2000. You have the option of entering the URL where your printer is located. The print server must be a Windows 2000 Server running Internet Information Server or a Windows 2000 Professional system running Personal Web Server - all shared printers can be viewed at: `http://servername/printers`
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each. Priority ranges from 1, the lowest (default) to 99, the highest.
- Enabling "Availability" option allows Administrator to specify the hours the printer is available.
- Use Separator Pages to separate print jobs at a shared printer. A template for the separator page can be created and saved in the %systemroot%\system32 directory with a .SEP file extension. (KB# [Q102712](#))
- You can select Restart in the printer's menu to reprint a document. This is useful when a document is printing and the printer jams. Resume can be selected to start printing where you left off.
- You can change the directory containing the print spooler in the advanced server properties for the printer. (KB# [Q123747](#))
- To remedy a stalled spooler, you will need to stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel. (KB# [Q240683](#) &
- Use the **fixprnsv.exe** command-line utility to resolve printer incompatibility issues. (KB# [Q247196](#))

Managing file systems: (KB# [Q222189](#))

- Windows 2000 supports both *Basic* and *Dynamic* storage. In basic storage you divide a hard disk into partitions. Windows 2000 recognizes primary and extended partitions. A disk initialized for basic storage is called a *Basic disk*. It can contain primary partitions, extended partitions and logical drives. Basic volumes cannot be created on dynamic disks. Basic volumes should be used when dual-booting between Windows 2000 and DOS, Windows 3.x, Windows 95/98 and all version of Windows NT. (KB# [Q175761](#))
- *Dynamic* storage (Windows 2000 only) allows you to create a single partition that includes the entire hard disk. A disk initialized for dynamic storage is called a *Dynamic disk*. Dynamic disks are divided into volumes which can include portions of one, or many, disks. These can be resized without needing to restart the operating system. (KB# [Q225551](#))

There are three volume types

- *Simple volume* - contains space from a single disk
- *Spanned volume* - contains space from multiple disks (maximum of 32). First fills one volume before going to the next. If a volume in a spanned set fails, all data in the spanned volume set is lost. Performance is degraded as disks in spanned volume set are read sequentially.
- *Striped set*- contains free space from multiple disks (maximum of 32) in one logical drive. Increases performance by reading/writing data from all disks at the same rate. If a disk in a stripe set fails, all data is lost.

Dynamic Volume States

State	Description
Failed	Volume cannot be automatically restarted and needs to be repaired
Healthy	Is accessible and has no known problems
Healthy (at risk)	Accessible, but I/O errors have been detected on the disk. Underlying disk is displayed as Online (Errors)
Initializing	Volume is being initialized and will be displayed as healthy when process is complete

Dynamic Volume Limitations

- Cannot be directly accessed by DOS, Win95/98 or any versions of Windows NT if you are dual-booting, as they do not use the traditional disk organization scheme of partitions and logical volumes. MBR on dynamic disks contains a pointer to disk configuration data stored in the last 1 MB of space at the end of the disk. (KB# [Q197738](#))
- Dynamic volumes which were upgraded from basic disk partitions cannot be extended, especially the system volume which holds hardware-specific files required to start Windows 2000 and the boot volume. Volumes created after the disk was upgraded to dynamic can be extended. (KB# [Q222188](#))
- When installing Windows 2000, if a dynamic volume is created from unallocated space on a dynamic disk, Windows 2000 cannot be installed on that volume. (KB# [Q216341](#))
- Not supported on portable computers or removable media. (KB# [Q232463](#))
- A boot disk that has been converted from basic to dynamic cannot be converted back to basic. (KB# [Q217226](#))

Translation of terms between Basic and Dynamic Disks

Basic Disks	Dynamic Disks
Active partition	Active volume
Extended partition	Volume and unallocated space
Logical drive	Simple volume
Mirror set	Mirrored volume (Server only)
Primary partition	Simple volume
Stripe set	Striped volume
Stripe set with parity	RAID-5 volume (Server only)
System and boot partitions	System and boot volumes
Volume set	Spanned volumes

- There is NO fault-tolerance with Windows 2000 Professional. Fault-tolerance (RAID levels 1 and 5) is only available in the Windows 2000 Server family. (KB# [Q113932](#))
- To manage disks on a remote computer you must create a custom console focused on another computer. Choose Start > Run and type mmc. Press Enter. On console menu click Add/Remove Snap-in. Click Add. Click Disk Management then click Add. When Choose Computer dialog box appears choose the remote system.

- Windows 2000 now supports disk-based quotas. Quotas can be set on NTFS volumes, but not on FAT or FAT32 volumes. Quotas cannot be set on individual folders within a NTFS partition. (KB# [Q183322](#))
- Disk information is now stored on the physical disk itself, facilitating moving hard drives between systems. As managing disk numbering can become quite complex, the **dmtool.exe** utility has been provided. (KB# [Q222470](#))

When using the Disk Management Snap-in Tool

- Whenever you add a new disk in a computer it is added as Basic Storage
- Every time you remove or add a new disk to your computer you must choose Rescan Disks
- Disks that have been removed from another computer will appear labeled as Foreign. Choose "Import Foreign Disk" and a wizard appears to provide instructions.
- For multiple disks removed from another computer, they will appear as a group. Right-click on any of the disks and choose "Add Disk".
- Disks can be upgraded from Basic to Dynamic storage at any time but must contain at least 1 MB of unallocated space for the upgrade to work.

Implementing, Managing, and Troubleshooting Hardware Devices and Drivers: (KB#[Q199276](#))

Miscellaneous

- Windows 2000 now fully supports Plug and Play. (KB# [Q133159](#))
- Use the "System Information" snap-in to view configuration information about your computer (or create a custom console focused on another computer - powerful tool!!).
- "Hardware Resources" under System Information allow you to view Conflicts/Sharing, DMAs, IRQs, Forced Hardware, I/O and Memory.
- Hardware is added and removed using the "Add/Remove Hardware" applet in the Control Panel (can also be accessed from Control Panel > System > Hardware > Hardware Wizard).
- All currently installed hardware is managed through the "Device Manager" snap-in.
- To troubleshoot a device using Device Manager, click the "Troubleshoot" button on the General tab.

Disk devices

- Managed through "Computer Management" under Control Panel > Administrative tools or by creating a custom console and adding the "Disk Management" snap-in. Choosing the "Computer Management" snap-in for

your custom console gives you the following tools: Disk Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.

- Using Disk Management, you can create, delete, and format partitions as FAT, FAT32 and NTFS. Can also be used to change volume labels, reassign drive letters, check drives for errors and backup drives.
- Defragment drives by using "Disk Defragmenter" under "Computer Management" or add the "Disk Defragmenter" snap-in to your own custom console. (KB# [Q227463](#))
- Removable media are managed through the "Removable Media" snap-in.

Display devices

- Desktop display properties (software settings) are managed through the Display applet in Control Panel.
- Display adapters are installed, removed and have their drivers updated through "Display Adapters" under the Device Manager.
- Monitors are installed, removed, and have their drivers updated through "Monitors" under the Device Manager.
- Windows 2000 Professional supports multiple monitors running concurrently.

Mobile computer hardware

- PCMCIA (PC Card) adapters, USB ports, IEEE 1394 (FireWire), and Infrared devices now supported. These are managed through Device Manager.
- Hot (computer is fully powered) and warm (computer is in suspend mode) docking and undocking are now fully supported for computers with a PnP BIOS.
- Support is provided for Advanced Power Management (APM) and Advanced Configuration and Power Interface (ACPI). (KB# [Q242495](#))
- Hibernation (complete power down while maintaining state of open programs and connected hardware) and Suspend (deep sleep with some power) modes are now supported, extending battery life.
- When a PC Card, USB or Infrared device is installed, Windows 2000 will automatically recognize and configure it (if it meets PnP specifications). If Windows does not have an entry in its driver base for the new hardware, you will be prompted to supply one.
- Equipping mobile computers with SmartCards and Encrypting File System decreases the likelihood of confidential corporate data being compromised if the computer is stolen or lost.
- Use hardware profiles for mobile computers. Accessed through Control Panel > System applet > Hardware tab > Hardware Profiles. Multiple profiles can be created and designated as a docked or undocked portable computer.

Input and output (I/O) devices

- Keyboards are installed under "Keyboards" in Device Manager.
- Mice, graphics tablets and other pointing devices are installed under "Mice and other pointing devices" in Device Manager.
- Troubleshoot I/O resource conflicts using the "System Information" snap-in. Look under Hardware Resources > I/O for a list of memory ranges in use.

Updating drivers

- Drivers are updated using Device Manager. Highlight the device, right-click and choose Properties. A properties dialog appears. Choose the Drivers tab and then the Update Driver... button.
- Microsoft recommends using Microsoft digitally signed drivers whenever possible. (KB# [Q244617](#))
- The Driver.cab cabinet file on the Windows 2000 CD contains all of the drivers the OS ships with. Whenever a driver is updated, W2K looks here first. The location of this file is stored in a registry key and can be changed: HKLM\Software\Windows\CurrentVersion\Setup\DriverCachePath (KB# [Q230644](#))
- The Driver Verifier is used to troubleshoot and isolate driver problems. It must be enabled through changing a Registry setting. The Driver Verifier Manager, **verifier.exe**, provides a command-line interface for working with Driver Verifier. (KB# [Q244617](#))

Managing/configuring multiple CPUs

- Adding a processor to your system to improve performance is called scaling. Typically done for CPU intensive applications such as CAD and graphics rendering.
- Windows 2000 Professional supports a maximum of two CPUs. If you need more consider using Windows 2000 Server (up to 4 CPUs), Advanced Server (up to 8 CPUs) and Datacentre Server (maximum of 32 CPUs).
- Windows 2000 supports Symetric Multiprocessing (SMP). Processor affinity is also supported. Asymmetric Multiprocessing (ASMP) is not supported.
- Upgrading to multiple CPUs might increase the load on other system resources.
- Update your Windows driver to convert your system from a single to multiple CPUs. This is done through Device Manager > Computer > Update Driver. (KB# [Q234558](#))

Install and manage network adapters

- Adapters are installed using the Add/Remove Hardware applet in Control Panel

- Change the binding order of protocols and the Provider order using Advanced Settings under the Advanced menu of the Network and Dial-up Connections window (accessed by right-clicking on My Network Places icon)
- Each network adapter has an icon in Network and Dial-up connection. Right click on the icon to set it's properties, install protocols, change addresses, etc.

Troubleshooting the boot process

Files used in the Windows 2000 boot process: (KB# [Q114841](#))

File:	Location:
Ntldr	System partition root
Boot.ini	System partition root (KB# Q99743)
Bootsect.dos	System partition root
Ntdetect.com	System partition root
Ntbootdd.sys*	System partition root
Ntoskrnl.exe	%systemroot%\System32
Hal.dll	%systemroot%\System32
System	%systemroot%\System32\Config

Optional - only if system partition is on SCSI disk with BIOS disabled

ARC paths in BOOT.INI: (KB# [Q113977](#) & [Q119467](#))

The Advanced Risc Computing (ARC) path is located in the BOOT.INI and is used by NTLDR to determine which disk contains the operating system. (KB# [Q102873](#))

multi(x)	Specifies SCSI controller with the BIOS enabled, or non-SCSI controller. x=ordinal number of controller.
scsi(x)	Defines SCSI controller with the BIOS disabled. x=ordinal number of controller.
disk(x)	Defines SCSI disk which the OS resides on. When <i>multi</i> is used, x=0. When <i>scsi</i> is used, x= the SCSI ID number of the disk with the OS.
rdisk(x)	Defines disk which the OS resides on. Used when OS does not reside on a SCSI disk. x=0-1 if on primary controller. x=2-3 if on multi-channel EIDE controller.

partition(x)	Specifies partition number which the OS resides on. x=cardinal number of partition, and the lowest possible value is 1.
--------------	--

multi(0)disk(0)rdisk(0)partition(1). These are the lowest numbers that an ARC path can have.

BOOT.INI switches: (KB# [Q239780](#))

- **/basevideo** - boots using standard VGA driver
- **/fastdetect=[comx,y,z]** - disables serial mouse detection or all COM ports if port not specified. Included by default
- **/maxmem:n** - specifies amount of RAM used - use when a memory chip may be bad
- **/noguiboot** - boots Windows without displaying graphical startup screen
- **/sos** - displays device driver names as they load
- **/bootlog** - enable boot logging
- **/safeboot:minimal** - boot in safe mode
- **/safeboot:minimal(alternateshell)** - safe mode with command prompt
- **/safeboot:network** - safe mode with networking support (KB# [Q236346](#))

Bootting in Safe Mode: (KB# [Q202485](#))

- Enter safe mode by pressing F8 during operating system selection phase
- Safe mode loads basic files/drivers, VGA monitor, keyboard, mouse, mass storage and default system services. Networking is not started in safe mode. (KB# [Q199175](#))
- **Enable Boot Logging** - logs loading of drivers and services to nbtlog.txt in the *windir* folder
- **Enable VGA Mode** - boots Windows with VGA driver
- **Last Known Good Configuration** - uses registry info from previous boot. Used to recover from botched driver installs and registry changes.
- **Recovery Console** - only appears if it was installed using **winnt32 /cmdcons** or specified in the unattended setup file.
- **Directory Services Restore Mode** - only in Server, not applicable to Win2000 Professional.
- **Debugging Mode** - again, only in Server
- **Boot Normally** - lets you boot, uh, normally. ;-)

Windows 2000 Control Sets: (KB# [Q142033](#))

- Found under HKEY_LOCAL_MACHINE\System>Select - has four entries
- **Current**- CurrentControlSet. Any changes made to the registry modify information in CurrentControlSet



- **Default** - control set to be used next time Windows 2000 starts. Default and current contain the same control set number
- **Failed** - control set marked as failed when the computer was last started using the LastKnownGood control set
- **LastKnownGood** - after a successful logon, the Clone control set is copied here

Running the Recovery Console: (KB# [Q229716](#))

- Insert Windows 2000 CD into drive, change to i386 folder and run **winnt32 /cmdcons** (KB# [Q216417](#))
- After it is installed, it can be selected from the "Please Select Operating System to Start" menu
- When starting Recovery Console, you must log on as Administrator. (KB# [Q239803](#))
- Can also be run from Windows 2000 Setup, repair option.
- Allows you to boot to a "DOS Prompt" when your file system is formatted with NTFS.
- Looks like DOS, but is very limited. By default, you can copy from removable media to hard disk, but not vice versa - console can't be used to copy files to other media (KB# [Q240831](#)). As well, by default, the wildcards in the copy command don't work (KB# [Q235364](#)). You can't read or list files on any partition except for system partition.
- Can be used to disable services that prevent Windows from booting properly (KB# [Q244905](#))

Command	Description
attrib	changes attributes of selected file or folder
cd or chdir	displays current directory or changes directories.
chkdsk	run CheckDisk
cls	clears screen
copy	copies from removable media to system folders on hard disk. No wildcards
del or delete	deletes service or folder
dir	lists contents of selected directory on system partition only
disable	disables service or driver
diskpart	replaces FDISK - creates/deletes partitions
enable	enables service or driver

extract	extracts components from .CAB files
fixboot	writes new partition boot sector on system partition
fixmbr	writes new MBR for partition boot sector
format	formats selected disk
listsvc	lists all services on W2K workstation
logon	lets you choose which W2K installation to logon to if you have more than one
map	displays current drive letter mappings
md or mkdir	creates a directory
more or type	displays contents of text file
rd or rmdir	removes a directory
ren or rename	renames a single file
systemroot	makes current directory system root of drive you're logged into

Startup and Recovery Settings

- Accessed through Control Panel > System applet > Advanced tab > Startup and Recovery
- Memory dumps are always saved with the filename memory.dmp (KB# [Q192463](#))
- Small memory dump needs 64K of space. Found in %systemroot%\minidump
- A paging file must be on the system partition and the pagefile itself at least 1 MB larger than the amount of RAM installed for Write debugging information option to work
- Use dumpchk.exe to examine contents of memory.dmp (KB# [Q156280](#))

Windows Report Tool: (KB# [Q188104](#))

- Used to gather information from your computer to assist support providers in troubleshooting issues. Reports are composed in Windows 98 and Windows 2000 and then uploaded to a server provided by the support provider using HTTP protocol.
- Reports are stored in a compressed .CAB format and include a Microsoft System Information (.NFO) file.
- The report generated by Windows Report Tool (**winrep.exe**) includes a snapshot of complete system software and hardware settings. Useful for diagnosing software and hardware resource conflicts.

Emergency Repair Disk:

- Windows NT 4 users - the RDISK utility is gone, ERDs are now made exclusively with the backup utility. It has been changed from a repair disk to a boot disk which lets you run repair tools on the CD (KB# [Q216337](#))
- To make an ERD, run **ntbackup**, choose Emergency Repair Disk and insert a blank formatted floppy into the A: drive. You will also have the option to copy registry files to the repair directory - it's a good idea to do so (%systemroot%\repair\regback). Also use backup to copy these registry files to a tape or Zip disk. (KB# [Q231777](#))
- ERD contains the following files: autoexec.nt, config.nt and setup.log

Monitoring and Optimizing System Performance and Reliability

Driver signing: (KB# [Q224404](#))

Configuring Driver Signing: (KB# [Q236029](#))

- Open System applet in Control Panel and click Hardware tab. Then in the Device Manager box, click Driver Signing to display options:
- **Ignore** - Install all files, regardless of file signature
- **Warn**- Display a message before installing an unsigned file
- **Block**- Prevent installation of unsigned files
- The *Apply Setting As System Default* checkbox is only accessible to Administrators

Using System File Checker (sfc.exe): (KB# [Q222471](#))

- **/scannow** - scans all protected system files immediately
- **/scanonce** - scans all protected system files at next startup
- **/scanboot**- scans all protected system files at every restart
- **/cancel**- cancels all pending scans
- **/quiet** - replaces incorrect files without prompting
- **/enable** - sets Windows File Protection back to defaults
- **/purgecache** - purges file cache and forces immediate rescan
- **/cachesize=x**- sets file cache size

Windows Signature Verification (sigverif.exe)

- running **sigverif** launches File Signature Verification
- checks system files by default, but non-system files can also be checked
- saves search results to Sigverif.txt

Task scheduler: (KB# [O235536](#) & [O226262](#))

- used to automate events such as batch files, scripts and system backups
- tasks are stored in the Scheduled Tasks folder in Control Panel
- running task with a user name and password allows an account with the required rights to perform the task instead of an administrative account
- set security for a task by group or user

Using offline files

- Offline files replaces My Briefcase and works a lot like Offline Browsing in IE5.
- Share a folder and set it's caching to make it available offline - three types of caching:
 - **manual caching for documents** - default setting. Users must specify which docs they want available when working offline
 - **automatic caching for documents** - all files opened by a user are cached on his local hard disk for offline use - older versions on users machine automatically replaced by newer versions from the file share when they exist
 - **automatic caching for programs** -same as above, but for programs
- When synchronizing, if you have edited an offline file and another user has also edited the same file you will be prompted to keep and rename your copy, overwrite your copy with the network version, or to overwrite the network version and lose the other user's changes (a wise SysAdmin will give only a few key people write access to this folder or everyone's work will get messed up).
- Using Synchronization Manager, you can specify which items are synchronized, using which network connection and when synchronization occurs (at logon, logoff, and when computer is idle).

Performance Console: (KB# [O146005](#))

- Important objects are *cache* (file system cache used to buffer physical device data), *memory* (physical and virtual/paged memory on system), *physicaldisk* (monitors hard disk as a whole), *logicaldisk* (logical drives, stripe sets and spanned volumes), and *processor* (monitors CPU load)
- *Processor - % Processor Time* counter measure's time CPU spends executing a non-idle thread. If it is continually at or above 80%, CPU upgrade is recommended
- *Processor - Processor Queue Length* - more than 2 threads in queue indicates CPU is a bottleneck for system performance
- *Processor - % CPU DPC Time* (deferred procedure call) measures software interrupts.

- *Processor - % CPU Interrupts/Sec* measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or upgrade CPU.
- *Logical disk - Disk Queue Length* - If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set
- *Physical disk - Disk Queue Length* - same as above
- *Physical disk - % Disk Time*- If above 90%, move data/pagefile to another drive or upgrade drive
- *Memory - Pages/sec* - more than 20 pages per second is a lot of paging - add more RAM
- *Memory - Committed bytes* - should be less than amount of RAM in computer
- *diskperf* command for activating disk counters is not supported in Windows 2000

Performance Alerts and Logs: (KB# [Q244640](#))

- *Alert logs* are like trace logs, but they only log an event, send a message or run a program when a user-defined threshold has been exceeded
- *Counter logs* record data from local/remote systems on hardware usage and system service activity
- *Trace logs* are event driven and record monitored data such as disk I/O or page faults
- By default, log files are stored in the \Perflogs folder in the system's boot partition
- Save logs in CSV (comma separated value) or TSV (tab separated value) format for import into programs like Excel
- CSV and TSV must be written all at once, they do not support logs that stop and start. Use Binary (.BLG) for logging that is written intermittently
- Logging is used to create a baseline for future reference

Virtual memory/Paging file

- Recommended minimum paging file size is 1.5 times the amount of RAM installed. A system with 64 MB should have a 96 MB page file. Maximum page file size should not exceed 2.5 times the amount of RAM installed
- Set through Control Panel > System applet > Advanced tab > Performance Options > Change
- The most efficient paging file is spread across several drives, but is not on the system or boot partitions. (KB# [Q123747](#))
- Maximum registry size can also be changed through the Virtual Memory dialog box

Hardware profiles

- Created to store different sets of configuration settings to meet a users different needs (usually used with portables) such as whether a computer is docked or undocked.
- User selects the desired profile at Windows 2000 startup
- Profiles are created through Control Panel > System applet > Hardware tab > Hardware Profiles
- Devices are enabled and disabled in particular profiles through their properties in the Device Manager snap-in

Data recovery

- Windows 2000 Backup is launched through Control Panel > System applet > Backup or by running **ntbackup** from the Start menu (KB# [Q241007](#))
- Users can back up their own files and files they have read, execute, modify, or full control permission for
- Users can restore files they have write, modify or full control permission for
- Administrators and Backup Operators can backup and restore all files regardless of permissions

Backup type	Description
Normal	All selected files and folders are backed up. Archive attribute is cleared if it exists (fast for restoring)
Copy	All selected files and folders are backed up. Archive attribute is not cleared (fast for restoring)
Incremental	Only selected files and folders that have their archive attribute set are backed up and then archive markers are cleared
Differential	Only selected files and folders that have their archive attribute set are backed up but archive attributes are not cleared
Daily	All selected files and folders that have changed throughout the day are backed up. Archive attributes are ignored during the backup and are not cleared afterwards

The Windows 2000 Registry:

Database that stores Windows 2000 configuration information for all installed software, hardware and users in a hierarchical structure. Consists of five main subtrees:

- **HKEY_CLASSES_ROOT** - holds software configuration data, file associations and object linking and embedding (OLE) data

- **HKEY_CURRENT_CONFIG** - holds data on active hardware profile extracted from SOFTWARE and SYSTEM hives
- **HKEY_CURRENT_USER** - contains data about current user extracted from HKEY_USERS and additional info pulled down from Windows authentication
- **HKEY_LOCAL_MACHINE** - contains all local computer hardware, software, device driver and startup information. Remains constant regardless of the user
- **HKEY_USERS** - holds data for user identities and environments, custom settings, etc

The Registry Editor (Regedt32.exe) has a read-only mode, a security menu, and supports the REG_EXPAND_SZ and REG_MULTI_SZ data types. Regedit.exe (another registry editing tool installed by Windows 2000) does not. Registry Editor automatically saves changes as they are made.

Secondary Logon Service (Run As): (KB# [Q225035](#))

- Similar to the SU (Super User) command in UNIX
- Used to test setting using a particular user account while logged in with a different account
- Select the application icon using a single left-click, hold down the **Shift** key and right-click the icon. When the pop-up menu appears, click **Run As**. This brings up a dialog box titled "Run program as other user" - enter your credentials and click OK

Configuring and Troubleshooting the Desktop Environment

User profiles

- Is a collection of data and folders that store the user's desktop environment and application settings along with personal data.
- When a user logs onto a client computer running W2K Pro, he/she always receives his/her individualized desktop settings and all of their network connections regardless of how many users share the same computer.
- A user can change their user profile by changing their desktop settings - when they log off, Windows 2000 incorporates the changes into their user profile.
- Setting a profile as mandatory forces Windows to discard any changes made during the session so the next time the user logs on, the session remains unchanged from their last login.
- User profiles are stored in the *%systemroot%\Documents and Settings\%username%* folder.
- Roaming profiles are used in Windows 2000 domains for users who move from one computer to another but require a consistent desktop environment.

Multiple languages and locations

Changed through the Regional Options applet in Control Panel. Open Region Options and click Input Locale tab to add more locales. Check each locale or language you want your system to support. (KB# [Q177561](#))

On the Regional Options applet General tab, scroll through the items in the box labeled "Your System is Configured to Read and Write Documents in Multiple Languages" to see the available languages as well as the current default.

Using Microsoft Installer Packages: (KB# [Q242479](#))

- Recognized by their .MSI extension.
- Integrates software installation into Windows 2000 so that it is now centrally controlled, distributed, and managed from a central-point.
- Completely integrated with Active Directory's Group Policies.
- You can *assign* or *publish* software packages. Software that is published has a shortcut appear on a user's Start > Programs menu, but is not installed until the first time they use it. Assigned software is installed the next time the user logs on regardless of whether or not they run it.
- Software package is installed on a Windows 2000 Server in a shared directory. A Group Policy Object (GPO) is created. Behavior filters are set in the GPO to determine who gets the software. Then add the package to the GPO under User Configuration > Software Settings > Software Installation (this is done on the server). You are prompted for a publishing method - choose it and say OK.
- Non-MSI programs are published as .ZAP files. They cannot take advantage of MSI features such as elevated installation privileges, rolling back an unsuccessful installation, install on first use of software or feature, etc. (KB# [Q231747](#))

Configure and troubleshoot desktop settings

Desktop settings can be configured using the Display applet in Control Panel or by right clicking on a blank area of the desktop and selecting properties.

User can change the appearance of the desktop, desktop wallpaper, screen saver settings and more.

Fax support

- If a fax device (modem) is installed, the Fax applet appears in Control Panel. Does not appear when no fax device installed
- If the Advanced Options tab is not available in the Fax applet log off then log back on as Administrator

- Use the Fax applet to setup rules for how device receives faxes, number or retries when sending, where to store retrieved and sent faxes, user security permissions, etc.
- The Fax printer in your printer folder cannot be shared

Accessibility services: (KB# [0210894](#))

- StickyKeys allows you to press multiple key combinations (CTRL-ALT-DEL) one key at a time
- FilterKeys tells the keyboard to ignore brief or repeated keystrokes
- SoundSentry displays visual warnings when your computer makes a sound (for aurally impaired)
- ShowSounds forces programs to display captions for the speech and sounds they make
- MouseKeys lets you control the mouse pointer with the numeric keypad
- Magnifier magnifies a portion of the desktop (for visually impaired) - available during GUI phases of OS installation (KB# [0231843](#))
- Narrator reads menu options aloud using speech synthesis (for visually impaired) - available during GUI phases of OS installation.

Implementing, Managing, and Troubleshooting Network Protocols and Services:

TCP/IP protocol

Miscellaneous

- Is an industry-standard suite of protocols
- It is routable and works over most network topologies
- It is the protocol that forms the foundation of the Internet
- Installed by default in Windows 2000
- Can be used to connect dissimilar systems
- Uses Microsoft Windows Sockets interface (Winsock)
- IP addresses can be entered manually or provided automatically by a DHCP server
- DNS is used to resolve computer hostnames to IP addresses
- WINS is used to resolve a NetBIOS name to an IP address
- Subnet mask - A value that is used to distinguish the network ID portion of the IP address from the host ID.
- Default gateway - A TCP/IP address for the host (typically a router) which you would send packets for routing elsewhere on the network.

Automatic Private IP Addressing

Windows 98 and Windows 2000 support this new feature. When "Obtain An IP Address Automatically" is enabled, but the client cannot obtain an IP address, Automatic Private IP addressing takes over:

- IP address is generated in the form of 169.254.x.y (where x.y is the computer's identifier) and a 16-bit subnet mask (255.255.0.0)
- The computer broadcasts this address to it's local subnet
- If no other computer responds to the address, the first system assigns this address to itself
- When using the Auto Private IP, it can only communicate with other computers on the same subnet that also use the 169.254.x.y range with a 16-bit mask.
- The 169.254.0.0 - 169.254.255.255 range has been set aside for this purpose by the Internet Assigned Numbers Authority

TCP/IP Server Utilities

- Telnet server - Windows 2000 includes a telnet server service (**net start tlntsvr**) which is limited to a command line text interface and two concurrent users. Set security on your telnet server by running the admin tool, **tlntadm**. (KB# [Q225233](#))
- Web Server - stripped version of IIS5 Web server. Limited to 10 connections. Must be installed and service started before sharing your printers using Web printing or Internet printing. Can be managed using IIS snap-in or Personal Web Manager, a "dumbed-down" GUI for novice users.
- FTP Server - stripped version of Internet Information Server 5 (IIS5) FTP server. Limited to 10 connections but is administered just like the server version using IIS snap-in or the Personal Web Manager.
- FrontPage 2000 Server Extensions - extends the functionality of the Web server and included in W2K Pro for developing and testing Web sites before deploying them to a production server.
- SMTP Server - does not appear to have limitations on connections but this is most likely due to its integration with LDAP and Active Directory replication. Also works with the form handlers in FrontPage Server Extensions.

TCP/IP Client Utilities

- Telnet client - Can be used to open a text based console on UNIX, Linux and Windows 2000 systems (run **telnet servername**)
- FTP client - Command line based - simple and powerful (run **ftp servername**)
- Internet Explorer 5 - Microsoft's powerful and thoroughly integrated Web browser (see [IE5 Cramsession](#) for details)
- Outlook Express 5 - SMTP, POP3, IMAP4, NNTP, HTTP, and LDAP complaint E-mail package.

Services for UNIX 2.0

Miscellaneous

- TCP/IP protocol is required for communicating with UNIX hosts
- Windows 2000 uses CIFS (Common Internet File System) which is an enhanced version of the SMB (Server Message Block) protocol
- UNIX uses NFS (Network File System)
- FTP support has been added to Windows Explorer and to Internet Explorer 5.0 allowing users to browse FTP directories as if they were a local resource.
- Install SNMP for Network Management (HP, OpenView, Tivoli and SMS).
- Print Services for UNIX allows connectivity to UNIX controlled Printers (LPR)
- Simple TCP/IP Services provides Echo, Quote of Day, Discard, Daytime and Character Generator.

Client for NFS

- Installs a full Network File System (NFS) client that integrates with Windows Explorer. Available for both W2K Professional and Server.
- Places a second, more powerful Telnet client on your system in the %windir%\system32%\%sfudir% directory. This new client has been optimized for Windows NT Telnet server and can use NTLM authentication instead of clear text. (KB# [Q250879](#))
- Users can browse and map drives to NFS volumes and access NFS resources through My Network Places. Microsoft recommends this over installing Samba (SMB file services for Windows clients) on your UNIX server.
- NFS shares can be accessed using standard NFS syntax (*servername:/pathname*) or standard UNC syntax (*\\servername\pathname*)
- If users' UNIX username/password differ from Windows username/password, click "Connect Using A Different User Name" option and provide new credentials.
- The following popular UNIX utilities are installed along with the Client for NFS (not a complete list):

Utility	Description
grep	Searches files for patterns and displays results containing that pattern
ps	Lists processes and their status
sed	Copies files named to a standard output; edits according to a script of commands
sh	Invokes the Korn shell
tar	Used to create tape archives or add/extract files from archives
vi	Invokes IV text editor

The **nfsadmin** command-line utility is used for configuration and administration of the Client for NFS. It's options are:

Option	Description
fileaccess	UNIX file permissions for reading, writing, and executing.
mapsvr	Computer name of the mapping server
mtype	Mount type, HARD or SOFT
perf	Method for determining performance parameters (MANUAL or DEFAULT)
preferTCP	Indicates whether to use TCP (YES or NO)
retry	Number of retries for a soft mount - default value is 5
rsize	Size of read buffer in KB
timeout	Timeout in seconds for an RPC call
wsize	Size of write buffer in KB

Server for NFS

- Allows NFS clients (think UNIX/Linux here) to access files on a Windows 2000 Professional or Server computer.
- Integrates with Server for PCNFS or Server for NIS to provide user authentication
- Managed using the UNIX Admin Snap-in (**sfumgmt.msc**)

Gateway for NFS

- Allows non-NFS Windows clients to access NFS resources by connecting thru an NFS-enabled Windows Server to NFS resources.
- Acts as a gateway/translator between the NFS protocol used by UNIX/Linux and the CIFS protocol used by Windows 2000.
- Not available on W2K Professional - Server only.

Server for PCNFS

- Can be installed on either W2K Professional or Server
- Provides authentication services for NFS clients (UNIX) needing to access NFS files. Works with the mapping server.

Server for NIS

- Must be installed on a Windows 2000 Server that is configured as a Domain Controller.
- Allows server to act as the NIS master for a particular UNIX domain.
- Can authenticate requests for NFS shares.

Troubleshooting: (KB# [Q102908](#))

- Ipconfig and Ipconfig /all - displays current TCP/IP configuration
- Nbtstat - displays statistics for connections using NetBIOS over TCP/IP
- Netstat - displays statistics and connections for TCP/IP protocol
- Ping - tests connections and verifies configurations
- Tracert - check a route to a remote system
- Common TCP/IP problems are caused by incorrect subnet masks and gateways
- If an IP address works but a hostname won't check DNS settings

NWLink (IPX/SPX) and NetWare Interoperability

(KB# [Q220872](#))

- NWLink (MS's version of the IPX/SPX protocol) is the protocol used by NT to allow Netware systems to access its resources. (KB# [Q203051](#))
- NWLink is all that you need to run in order to allow an NT system to run client/server applications from a NetWare server.
- To allow file and print sharing between NT and a NetWare server, CSNW (Client Services for NetWare) must be installed on the NT system. In a Netware 5 environment, the Microsoft client does not support connection to a Netware Server over TCP/IP. You will have to use IPX/SPX or install the Novell NetWare client. (KB# [Q235225](#))
- W2K Setup upgrades all Intel x86 based computers running version 4.7 or earlier of a Novell client to version 4.51. (KB# [Q218158](#))
- Gateway Services for NetWare can be implemented on your NT Server to provide a MS client system to access your NetWare server by using the NT Server as a gateway. (KB# [Q121394](#) & [Q220872](#))
- Frame types for the NWLink protocol must match the computer that the NT system is trying to connect with. Unmatching frame types will cause connectivity problems between the two systems.
- When NWLink is set to autodetect the frame type, it will only detect one type and will go in this order: 802.2, 802.3, ETHERNET_II and 802.5 (Token Ring).
- Netware 3 servers uses Bindery Emulation (Preferred Server in CSNW). Netware 4.x and higher servers use NDS (Default Tree and Context.)
- There are two ways to change a password on a netware server - SETPASS.EXE and the Change Password option (from the CTRL-ALT-DEL

dialog box). The Change Password option is only available to Netware 4.x and higher servers using NDS.

Other protocols

- DLC is a special-purpose, non-routable protocol used by Windows 2000 to talk with IBM mainframes, AS400s and Hewlett Packard printers.
- Appletalk must be installed to allow Windows 2000 Professional to communicate with Apple printers. Do not confuse this with File and Print Services for Macintosh which allow Apple Clients to use resources on a Microsoft Network (only available on Server).
- NetBEUI is used solely by Microsoft operating systems and is non-routable (it is broadcast-based)

Remote Access Services (RAS)

Authentication protocols

- EAP - Extensible Authentication Protocol. A set of APIs in Windows for developing new security protocols as needed to accommodate new technologies. MD5-CHAP and EAP-TLS are two examples of EAP
- EAP-TLS - Transport Level Security. Primarily used for digital certificates and smart cards
- MD5-CHAP - Message Digest 5 Challenge Handshake Authentication Protocol. Encrypts usernames and passwords with an MD5 algorithm
- RADIUS - Remote Authentication Dial-in User Service. Specification for vendor-independent remote user authentication. Windows 2000 Professional can act as a RADIUS client only.
- MS-CHAP (v1 and 2) - Microsoft Challenge Handshake Authentication Protocol. Encrypts entire session, not just username and password. v2 is supported in Windows 2000 and NT4 and Win 95/98 (with DUN 1.3 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data
- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients
- PAP - Password Authentication Protocol. Sends username and password in clear text

Virtual Private Networks (VPNs)

- PPTP - Point to Point Tunneling Protocol. Creates an encrypted tunnel through an untrusted network.
- L2TP - Layer Two Tunneling Protocol. Works like PPTP as it creates a tunnel, but it does not provide data encryption. Security is provided by using an encryption technology like IPSec

Feature	PPTP	L2TP
Header compression	No	Yes
Tunnel authentication	No	Yes
Built-in encryption	Yes	No
Transmits over IP-based internetwork	Yes	Yes
Transmits over UDP, Frame Relay, X.25 or ATM	No	Yes

Multilink Support: (KB# [Q235610](#))

- Multilinking allows you to combine two or more modems or ISDN adapters into one logical link with increased bandwidth. (KB# [Q233171](#))
- BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) enhance multilinking by dynamically adding or dropping links on demand. Settings are configured through RAS policies. (KB# [Q244071](#))
- Enabled from the PPP tab of a RAS server's Properties dialog box. (KB# [Q233151](#))

Setting Callback Security

- Using callback allows you to have the bill charged to your phone number instead of the number of the user calling in. Also used to increase security
- For roving users like a sales force, choose "Allow Caller to Set The Callback Number" (less secure)

Dial-up networking

- Microsoft technical documentation generally refers to dial-up networking when describing outbound connections. Inbound connections are usually associated with Remote Access Services (RAS).
- All new connections are added using the "Make New Connection" wizard.
- To create a VPN connection, choose Dial-Up To A Private Network Through The Internet, specify whether you need to establish a connection with an ISP first, enter the host name or IP address of the computer/network you are connecting to, and select whether connection is for yourself or all users.
- Dial-up networking entries can be created for modem connections, LAN connections, direct cable connections and Infrared connections.
- PPP is generally preferred because it supports multiple protocols, encryption, and dynamic assignment of IP addresses (KB# [Q124036](#)). SLIP is an older protocol that only supports TCP/IP and is used for dialing into legacy UNIX systems.



- All network connections, inbound and outbound, are represented by separate icons under Dial-up networking and properties, protocols, addresses and services can be individually configured for each.

Using shared resources on a Microsoft Network

The Administrators and Power Users groups can create shared folders on a Windows 2000 Professional workstation

Windows 2000 creates administrative shared folders for administrative reasons. These shares are appended with dollar sign (\$) which hides the share from users browsing the computer. The system folder (Admin\$), the location of the printer drivers (Print\$) and the root of each volume (C\$, D\$, etc.) are all hidden shared folders.

Shared folder permissions apply only when the folder is accessed via the network. By default, the Everyone group is assigned Full Control for all new shared folders. Share level permissions can be applied to FAT, FAT32 and NTFS file systems.

Security levels for network access to shared folders

Full Control	<ul style="list-style-type: none"> • Is assigned to the Everyone group by default. • Allows user to take ownership of files and folders. • Users can change file access rights. • Grants user all permissions assigned by the Change and Read levels.
Change	<ul style="list-style-type: none"> • User can add and create files. • Grants ability to modify files. • User can change the attributes of the file. • User can delete files. • Grants user all permissions assigned by the Read level.
Read	<ul style="list-style-type: none"> • User can display and open files. • User can display the attributes of the file. • User can execute program files.
No Access	<ul style="list-style-type: none"> • User cannot display, access, or modify files.

When a resource has both File-Level (NTFS) and Share-Level Securities enabled, you combine the highest two securities (assuming that there is not a "no access") and use the most restrictive of the two.

Windows 2000 Professional is limited to 10 concurrent connections for file and print services.

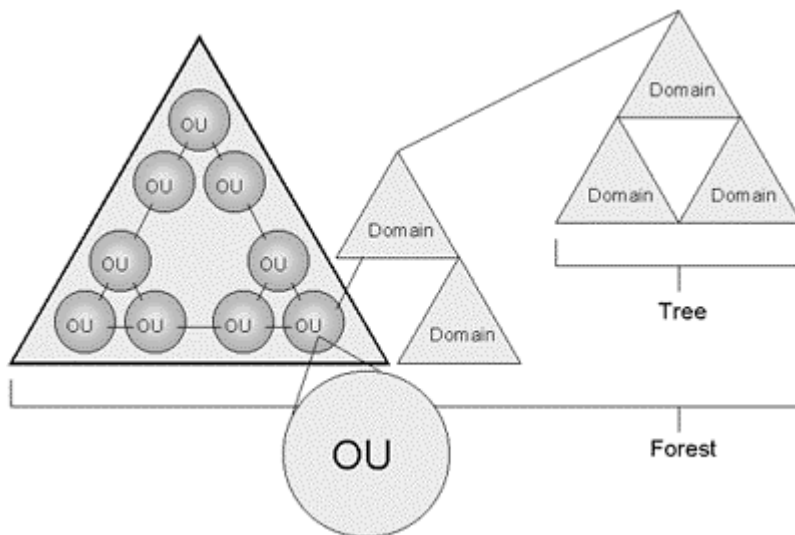
Implementing, Monitoring, and Troubleshooting Security

Active Directory Overview

Active Directory (AD) services provide a single point of network management, allowing you to add, remove, and relocate resources easily. It offers significant enhancements over the limitations of the older Windows NT domain based security model. Its features are:

- *Simplified Administration* - AD provides a single point of logon for *all* network resources - an administrator can logon to one computer and administer objects on any computer in the network.
- *Scalability* - NT 4 domains had a practical limitation of about 40,000 objects. AD scales to millions of objects, if needed.
- *Open standards support* - uses DNS as its domain naming and location service so Windows 2000 domain names are also DNS domain names. Support for LDAP v2 and v3 makes AD interoperable with other directory services that support the same, such as Novell's NDS. HTTP support means that AD can be searched using a Web browser. Kerberos 5 support provides interoperability with other products that use the same authentication mechanism.

Active Directory Structure



- *Object* - distinct named set of attributes that represents a network resource such as a computer or a user account.
- *Classes* - logical groupings of objects such as user accounts, computers, domains or organizational units.



- *Organizational Unit (OU)* - container used to organize objects inside a domain into logical administrative groups such as computers, printers, user accounts, file shares, applications and even other OUs.
- *Domain* - all network objects exist within a domain with each domain storing information only about the objects it contains. A domain is a security boundary - access to objects is controlled by Access Control Lists (ACLs). ACLs contain the permissions associated with objects that control which users or types of users can access them. In Windows 2000, all security policies and settings (like Administrative rights) do not cross from one domain to another. The domain admin only has right to set policies within his/her domain.
- *Tree* - a grouping or hierarchical arrangement of one or more Windows 2000 domains that share a contiguous names space (e.g. cramsession.brainbuzz.com, sales.brainbuzz.com, and jobs.brainbuzz.com). All domains inside a single tree share a common schema (formal definition of all object types that can be stored in an AD deployment) and share a common Global Catalog.
- *Forest* - a grouping or hierarchical arrangement of one or more domain trees that form a disjointed namespace (e.g. cramsession.com and brainbuzz.com). All trees in the forest share a common schema and Global Catalog, but have different naming structures. Domains in a forest operate independently of each other, but the forest enables communication across the domains.
- *Sites* - combination of one or more IP subnets connected by high-speed links. Not part of the AD namespace, and contains only computer objects and connection objects used to configure replication between sites.

Site Replication

- Active Directory information is replicated between Domain Controllers (DCs) and ensures that changes to a domain controller are reflected in all DCs within a domain. A DC is a computer running Windows 2000 server which contains a replica of the domain directory (member servers do not).
- DCs store a copy of all AD information for their domain, manage changes to it and copy those changes to other DCs in the same domain. DCs in a domain automatically copy all objects in the domain to each other. When you change information in AD, you are making the change on one of the DCs.
- Administrators can specify how often replication occurs, at what times, and how much data can be sent.
- DCs immediately replicate important changes to AD like a user account being disabled.
- AD uses *multimaster* replication meaning that no one DC is the master domain controller - all DCs within a domain are peers.
- Having more than one DC in a domain provides fault-tolerance. If a DC goes down, another is able to continue authenticating logins and providing required services using its copy of AD.
- Replication is automatically generates a *ring topology* for replication in the same domain and site. The ring ensures that if one DC goes down, it still has an available path to replicate its information to other DCs.

Active Directory Concepts

Schema - contains a formal definition of contents and structure of AD such as attributes, classes and class properties. For an object class, the schema defines what attributes an instance of a class must have, additional attributes that are allowed and which object class can be its parent. Installing AD on the first computer in a network creates the domain and default schema, which contains commonly used objects. Extensions can be made to the schema whenever needed. By default, write access to the schema is limited to members of the Administrators group. (KB# [Q229691](#))

Global Catalog - central repository of info about object in a tree or forest. AD automatically creates a global catalog from the domains that make up AD through the replication process. Attributes stored in the global catalog are usually those most often used in Search operations (like user names, logon names, etc.) and are used to locate a full replica of the object. Because of this, the global catalog can be used to find objects anywhere in the network without replication of all information between DCs.

Active Directory Naming Conventions

- **Distinguished Name (DN)** - every object in AD has one. Uniquely identifies object and contains sufficient info for an AD client to retrieve it from the Directory. Includes the name of the domain that holds the object and also the complete path through the container hierarchy to it. DNs must be unique - AD will not allow duplicates.
- **Relative Distinguished Name (RDN)** - if the DN is unknown, you can still query an object by its attributes. The RDN is a part of the name that is an attribute of the object itself (e.g. a user's first name and location).
- **Globally Unique Identifier (GUID)** - unique 128-bit number assigned to objects when they are created. The GUID never changes so even if the object is renamed or moved, the GUID can be used to locate it.
- **User Principal Name (UPN)** - "friendly name" given to a user account (e.g. johndoe@brainbuzz.com).

Local user accounts: (KB# [Q217050](#))

- Resides only on the computer where the account was created in its local security database. If computer is part of a peer-to-peer workgroup, accounts for that user will have to be created on each additional machine that they wish to log onto locally. Local accounts cannot access Windows 2000 domain resources and should not be created on computers that are part of a domain.
- Domain user accounts reside in AD on domain controllers and can access all resources on a network that they have been accorded privileges for.
- Built in user accounts are Administrator (used for managing the local system) and Guest (for occasional users - disabled by default)



- Usernames cannot be longer than 20 characters and cannot contain the following illegal characters: " / \ [] : ; | = , + * ? < >
- User logon names are not case sensitive. You can use alphanumeric combinations to increase security, if desired.
- Passwords can be up to 128 characters (we're not kidding!!) but Microsoft recommends limiting them to about eight characters.
- The same characters that are considered illegal in usernames are also verboten for use in passwords
- User accounts are added and configured through the Computer Management snap-in.
- Users should be encouraged to store their data in their My Documents folder which is automatically created within their profile folder and is the default location that Microsoft applications use for storing data.
- Creating and duplicating accounts requires only two pieces of information: username and password. Disabling an account is typically used when someone else will take the user's place or when the user might return.
- Delete an account only when absolutely necessary for space or organization purposes.
- When copying a user account, the new user will stay in the same groups that the old user was a member of. The user will keep all group rights that were granted through groups, but lose all individual rights that were granted specifically for that user.

Local user authentication

Built-in local groups

Local Group	Description
Administrators	Can perform all administrative tasks on the local system. The built-in Administrator account is made a member of this group by default.
Backup Operators	Can use Windows Backup to back up and restore data on the computer
Guests	Used for gaining temporary access to resources for which the Administrator has assigned permissions. Members can't make permanent changes to their desktop environment. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain Guests to the local Guests group.
Power Users	Can create and modify local user accounts on the computer, share resources and can install drivers for legacy software.
Replicator	Supports file replication in a domain
Users	Can perform tasks for which they have been assigned permissions. All new accounts created on a Windows 2000 machine are added to this group. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain users to the local Users group.

Built-in system groups

Local Group	Description
Everyone	Includes all users who access the computer.
Authenticated Users	Includes all users with a valid user account on the computer or domain - used to prevent anonymous access to a resource
Creator Owner	Includes user account for the user who created or took ownership of a resource.
Network	Includes any user with a current connection from another computer on the network to a shared resource on the computer
Interactive	Includes the user account for the user who is logged on at the computer. Members of this group gain access to the resources on the computer they are physically located at.
Anonymous Logon	Any user that Windows 2000 didn't authenticate.
Dialup	Any user who currently has a dial-up connection.

Group Policy

Group Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refer to the environment settings that users can change.

System Policy Editor (poledit.exe) - *Windows NT 4, Windows 95 and Windows 98 all use the System Policy Editor (poledit.exe) to specify user and computer configuration that is stored in the registry.*

- Not secure because settings can be changed by a user with the Registry Editor (regedit.exe). Settings are imported/exported using .ADM templates.
- Are considered "undesirably persistent" as they are not removed when the policy ends.
- Windows 2000 comes with system.adm (system settings), inetres.adm (Internet Explorer settings) and conf.adm (NetMeeting settings) although the latter is not loaded by default.

Group Policy snap-in (gpedit.msc) - Exclusive to Windows 2000 and supercedes the System Policy Editor. Uses Incremental Security Templates.

- Should only be applied to Windows 2000 systems that have been clean installed onto an NTFS partition. NTFS computers that have been upgraded from NT4 or earlier, only the Basic security templates can be applied.
- Settings can be stored locally or in AD. Are secure and cannot be changed by users - only Administrators.

- More flexible than System Policies as they can be filtered using Active Directory.
- Settings are imported/exported using .INF files. The Group Policy snap-in can be focused on a local or remote system.

Incremental Security Templates for Windows 2000

Template:	Filename:	Description:
Compatibility	compatws.inf	Compatibility template, but also referred to in MS documentation as Basic template. Sets up permissions for local users group so that legacy programs are more likely to run. Not considered a secure environment.
Secure	securews.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group. ACLs are not modified.
High Secure	hisecws.inf	Secure template provided for Workstations running in W2K native mode only. Requires all network communications to be digitally signed and encrypted. Cannot communicate with down level Windows clients. Changes ACLs to give Power Users ability to create shares and change system time.

Local Group Policy

- There are two types of Group Policy objects: local Group Policy objects and non-local Group Policy Objects. Each Windows 2000 system can have only one local Group Policy object.
- Order of application is Local, Site, Domain and Organizational Unit. Local Policies have the least precedence whereas OU Policies have the highest.

Non-local Group Policy (stored in Active Directory)

- Can be linked to a site with AD Sites and Services and applies to all domains at the site
- When applied to a domain it affects all users and computers in the domain and (by inheritance) all users and computers in Organizational Units.

Config.pol, NTConfig.pol and Registry.pol

- Windows 2000 uses the **registry.pol** format. Two files are created, one for Computer Configuration (stored in the \Machine subdirectory) and one for User Configuration (stored in the \User subdirectory).

- Registry.pol files can be used with Windows 95/98, Windows NT 4.0 and Windows 2000 as it is a text file embedded with binary strings. NTConfig.pol is a binary file whereas Config.pol is a text file.
- .POL files can be viewed using the **regview.exe** tool from the W2K Resource Kit. Viewing them does not apply them to the registry.

Security configuration

- Security Configuration and Analysis snap-in - Stand-alone MMC snap-in that can configure or analyze W2K security. Based on contents of a security template created using Security Templates snap-in. There is a text based version of this tool that can be run from the command line - **secedit.exe**.
- By default, Windows 2000 Professional doesn't require users to press CTRL-ALT-DEL to logon. Increase security by disabling this feature and forcing users to press CTRL-ALT-DEL, which is a key combination recognized only by Windows (set using the Group Policy snap-in).
- To disable access to the workstation, but allow programs to continue running, use the Lock Workstation option (from the CTRL-ALT-DEL dialog box).
- To disable access to the workstation, and not allow programs to continue running, use the Logoff option (from the CTRL-ALT-DEL dialog box).
- To lock the workstation after a period of idle time, use a screensaver password.

Auditing can be enabled by clicking Start > Programs > Administrative Tools > Local Security Policy. In the Local Security Settings window double-click Local Policies and then click Audit Policy. Highlight the event you want to audit and on the Action menu, click Security. Set the properties for each object as desired then restart computer for new policies to take effect.

- Clear the Virtual Memory Pagefile when the system shuts down. By default it is not cleared, but this can be changed under Local Security Policy Settings and will prevent unauthorized person from extracting information from your system's pagefile. (KB# [Q182086](#))
- Prevent the last user name from being displayed at logon (W2K Pro does this by default). Use the Group Policy snap-in, Local Computer Policy, to change this.
- When using Event Viewer, only local administrators can see the security log, but anyone (by default) can view other logs.

Encrypting File System (EFS): (KB# [Q223316](#) & [Q230520](#))

About EFS

- Only works on Windows 2000 NTFS portions (NTFS v5).
- Encryption is transparent to the user.
- Uses public-key encryption. Keys that are used to encrypt the file are encrypted by using a public key from the user's certificate. The list of encrypted file-encryption keys is kept with the encrypted file and is unique to it. When decrypting the file encryption keys, the file owner provides a private key which only he has. (KB# [Q241201](#) & [Q230490](#))
- If the owner has lost his private key, an appointed recovery system agent can open the file using his/her key instead. (KB# [Q242296](#))
- There can be more than one recovery agent, but at least one public recovery key must be present on the system when the file is encrypted.
- EFS resides in the Windows OS kernel and uses the non-paged memory pool to store file encryption keys - this means no one will be able to extract them from your paging file.
- Encrypted files can be backed up using the Backup Utility, but will retain their encrypted state as access permissions are preserved. (KB# [Q227825](#) & [Q223178](#))
- Microsoft recommends creating an NTFS folder and encrypting it. In the Properties dialog box for the folder click the General tab then the Advanced button and select the "Encrypt Contents To Secure Data" check box. The folder isn't encrypted, but files placed in it will be automatically encrypted. Uncheck the box if you want to decrypt the file.
- Default encryption is 56-bit. North Americans can upgrade to 128-bit encryption.
- Compressed files can't be encrypted and vice versa. (KB# [Q223093](#))
- You can't share an encrypted files
- Use the Cipher command to work with encrypted files from the command line. (KB# [Q229530](#)) & [Q229546](#))
- The **efsinfo.exe** utility in the W2K Resource Kit allows an administrator to determine information about encrypted files (KB# [Q243026](#))

Using the CIPHER command

Switch	Function
/a	performs the specified operation on files as well as folders
/d	decrypts specified folders and they are marked so files added to them will not be encrypted
/e	encrypts specified folders and they are marked so any files added later on are encrypted as well
/f	forces encryption operation on all specified files, even those already encrypted
/h	shows files with hidden/system attributes (not shown by default)
/l	specified operation continues even after errors have been reported
/k	creates a new file encryption key for user running Cipher command – cannot be used in conjunction with other options
/q	reports only essential information
/s	applies the specified operation to sub-folders as well
file_name	specifies a pattern, file, or folder

IPSec: (KB# [Q231585](#))

- IPSec can be implemented in a Windows 2000 domain using Active Directory or on a Windows 2000 machine through its Local Security settings. It is not available for Windows 95/98 or Windows NT.
- IPSec itself is a protocol, not a service. It consists of two separate protocols, Authentication Headers (AH) and Encapsulated Security Payload (ESP). AH provides *authentication*, *integrity* and *anti-replay* but does not encrypt data and is used when a secure connection is needed but the data itself is not sensitive. ESP provides the aforementioned plus *confidentiality* (data encryption) and is used to protect sensitive or proprietary information but is associated with greater system overhead for encrypting and decrypting data.
- Supported IPSec authentication methods are Kerberos v5 Public Key Certificate Authorities, Microsoft Certificate Server, and Pre-shared Key. (KB# [Q240262](#))
- The IPSec Policy Agent is a Windows 2000 service that runs within the LSASS.EXE process and shows up in the Services snap-in in MMC. It is loaded and started at system startup and retrieves an IPSec policy from either Active Directory or the local registry. After the IPSec Policy has been obtained, it will be applied to **all** IP traffic sent or received by that system (default behavior - IPSec policy can be modified to allow "soft associations" KB# [Q234580](#)).

- Before two computers can communicate they must negotiate a Security Association (SA). The SA defines the details of how the computers will use IPSec, with which keys, key lifetimes, and which encryption and authentication protocols will be used.
- When participating in a Windows 2000 domain, IPSec policies are stored in Active Directory. Without AD, they are stored in these registry keys... (KB# [Q231588](#))
- Group Policy:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Cache
- Local Policy:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Local
- Use IPSec Monitor (**ipsecmmon.exe**) to view status of IPSec on a Windows 2000 system. Windows 2000 Server Network Monitor can be used to view AH and ESP packets (but not ESP packet data). IPSec Policy Agent logs to the IPSECPA.LOG file. (KB# [Q231587](#) & [Q234581](#))

Special thanks to
[Sean McCormick](#)
for contributing this
Cramsession.