

## Windows XP SP3 services that can be disabled

One of the most effective ways to secure a Windows workstation is to turn off unnecessary services. This reference sheet lists the Windows XP SP3 services, describes each service's function, specifies whether you can safely disable the service, and outlines the ramifications of disabling it. The list assumes the machine is running Windows XP SP3 in a corporate network environment, although some notes are provided for machines that reside in a workgroup instead of a domain. The list offers one of the following three possibilities for safely disabling each service:

**YES:** You can disable the service without causing any problems.

**MAYBE:** The computer's role dictates whether you should or shouldn't disable the service—read Suggested Setting and Special Considerations for further information.

**NO:** The service is critical to proper Windows operation and should not be disabled.

This version of the list includes the Windows XP SP3 default setting for each service as well as information about suggested settings. Remember that every situation is different. One area in which there are vastly different opinions, for example, is Automatic Updates. Organizations handle updates in different ways, so keep that in mind as you use this list.

This list was compiled using a clean install of Windows XP Professional SP3, 32-bit.

Service	Description	Default Setting	Safely Disable?	Ramifications if disabled	Suggested setting	Special Considerations
<b>Alerter</b>	Notifies selected users and computers of administrative alerts	<b>Disabled</b>	<b>Yes</b>	Programs that use administrative alerts will not receive them.	<b>Disable</b>	
<b>Application Layer Gateway</b>	Provides support for application-level protocol plug-ins and enables network/protocol connectivity	<b>Manual</b>	<b>Maybe</b>	Programs that rely on this service, such as MSN Messenger and Windows Messenger will not function.	<b>Enable</b>	Only enable when using the Windows firewall or another firewall. Failure to do so can result in a significant security hole.
<b>Application Management</b>	Processes installation, removal, and enumeration requests for Active Directory IntelliMirror group policy programs	<b>Manual</b>	<b>Yes</b>	Users will be unable to install, remove, or enumerate any IntelliMirror programs.	<b>Disable</b>	
<b>Automatic Updates</b>	Enables the download and installation of critical Windows updates	<b>Automatic</b>	<b>Yes</b>	The operating system cannot automatically install updates, but can still be manually updated at the Windows Update Web site.	<b>Enable</b>	Automatic updates help keep your computer current. If you do disable the service, perform regular, manual updates. Highly recommended that this service remain enabled.
<b>Background Intelligent Transfer</b>	Transfers data between clients and servers in the background	<b>Automatic</b>	<b>Yes</b>	Features such as Windows Update will not work properly.	<b>Disable</b>	Enable this services if you enable Automatic Updates.
<b>ClipBook</b>	Enables ClipBook Viewer to store information and share it with remote computers	<b>Disabled</b>	<b>Yes</b>	ClipBook Viewer will not be able to share information with remote computers.	<b>Disable</b>	
<b>COM+ Event System</b>	Allows management of Component Services by providing automatic distribution of events to subscribing COM components	<b>Manual</b>	<b>No</b>	System Event Notification stops working, which means that logon and logoff notifications will not take place. Other applications, such as Volume Snapshot service, will not work correctly.	<b>Enable</b>	
<b>COM+ System Application</b>	Manages the configuration and tracking of Component Object Model (COM)+-based components	<b>Manual</b>	<b>No</b>	COM+ applications will not function properly.	<b>Enable</b>	
<b>Computer Browser</b>	Maintains an up-to-date list of computers on your network, and supplies the list to programs that request it. The Computer Browser service is used by Windows-based computers that need to view network domains and resources.	<b>Automatic</b>	<b>Yes</b>	Your computer will be unable to locate other Windows computers on the network	<b>Enable</b>	Enable this service, if you need to share files with other Windows computers.
<b>Cryptographic services</b>	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Key Service, which helps enroll this computer for certificates	<b>Automatic</b>	<b>No</b>	The associated management services will not function properly.	<b>Enable</b>	Required if you use the Automatic Updates Windows service; Also used by other Windows services, such as Task Manager.
<b>DCOM Server Process Launcher</b>	Provides launch functionality for DCOM services.	<b>Automatic</b>	<b>No</b>	DCOM applications and services will be disrupted.	<b>Enable</b>	
<b>DHCP Client</b>	Allows the system to automatically obtain IP addressing information, WINS server information, routing information, and so forth; is required to update records in Dynamic DNS	<b>Automatic</b>	<b>Yes</b>	The system will be unable to obtain an IP address, WINS information, and the like, from a DHCP server and will need to be configured with a static address.	<b>Enable</b>	You can disabled this service if you do not use DHCP, but this is a rare situation.
<b>Distributed Link Tracking Client</b>	Ensures that shortcuts and OLE links continue to work after the target file is renamed or moved by maintaining links in the file system	<b>Automatic</b>	<b>Yes</b>	Link tracking will be unavailable. Users on other computers won't be able to track links on this computer.	<b>Disable</b>	
<b>Distributed Transaction Coordinator</b>	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems	<b>Manual</b>	<b>Yes</b>	Distributed transactions will not occur.	<b>Disable</b>	

<b>DNS Client</b>	Resolves and caches DNS names, allowing the system to communicate with canonical names rather than strictly by IP address	<b>Automatic</b>	<b>No</b>	The system will be unable to resolve a name and will be able to communicate only via IP address. A client may be unable to communicate with its domain controller.	<b>Enable</b>	Stopping this service will result in the inability for the computer to resolve names to IP addresses.
<b>Error Reporting</b>	Collects, stores, and reports unexpected application crashes to Microsoft	<b>Automatic</b>	<b>Yes</b>	Error Reporting will occur only for kernel faults and some types of user mode faults.	<b>Disable</b>	
<b>Event Log</b>	Allows event log messages to be viewed in Event log to assist in problem resolution	<b>Automatic</b>	<b>No</b>	Administrators won't be able to view logs, including the security log, increasing the difficulty of diagnosing problems and detecting security breaches.	<b>Enable</b>	
<b>Extensible Authentication Protocol Service</b>	Provides windows clients Extensible Authentication Protocol Service	<b>Manual</b>	<b>Yes</b>	You may experience problems connecting to networks.	<b>Disable</b>	If you're using 802.1x or the Wired AutoConfig service, enable this service.
<b>Fast User Switching Compatibility</b>	Enables management for applications that require assistance in a multiple user environment	<b>Manual</b>	<b>Yes</b>	Fast User Switching will be unavailable.	<b>Disable</b>	Doesn't work in domain environments anyway.
<b>Health Key and Certificate Management Service</b>	Manages health certificates and keys (used by NAP)	<b>Manual</b>	<b>Yes</b>	Network Access Protection may not operate correctly.	<b>Disable</b>	Enable if you use NAP.
<b>Help and Support</b>	Enables Help and Support Center to run on this computer	<b>Automatic</b>	<b>Yes</b>	The Help and Support Center will be unavailable.	<b>Enable</b>	
<b>HTTP SSL</b>	This service implements the secure hypertext transfer protocol (HTTPS) for the HTTP service	<b>Manual</b>	<b>Yes</b>	Certain Windows Media functions may fail.	<b>Disable</b>	
<b>HID Input</b>	Enables generic input access to Human Interface Devices (HID), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices	<b>Disabled</b>	<b>Maybe</b>	Hot buttons controlled by this service will no longer function.	<b>Disable</b>	Required for some "hot buttons" on newer keyboards. Can be safely enabled if these buttons don't work with this service disabled.
<b>IMAPI CD-Burning COM</b>	Manages CD recording using Image Mastering Applications Programming Interface (IMAPI)	<b>Manual</b>	<b>Maybe</b>	This computer will be unable to record CDs.	<b>Enable</b>	This service can be disabled if you don't have a CD-RW drive in your system.
<b>Indexing Service</b>	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language	<b>Manual</b>	<b>Yes</b>	Files will not be indexed. Indexing can speed searching.	<b>Disable</b>	
<b>IPSEC services</b>	Provides end-to-end security between clients and servers on TCP/IP networks	<b>Automatic</b>	<b>Maybe</b>	TCP/IP security between clients and servers on the network will be impaired.	<b>Disable</b>	If you connect over an IPSec secured connection, don't disable this service.
<b>Logical Disk Manager</b>	Waits for new drives to be added and passes required information to the LDM administrative service; required to ensure dynamic disk information is up to date	<b>Automatic</b>	<b>Yes</b>	New disks will not be detected by the system.	<b>Enable</b>	Leaving this service enabled makes it easy to add new drives to the system. In a very high security environment, this should not be allowed.
<b>Logical Disk Manager Administrative</b>	Starts and allows configuration to take place when a new drive is detected or a partition/drive is configured	<b>Manual</b>	<b>Yes</b>	None; runs only when needed.	<b>N/A</b>	Started by the Logical Disk Manager service only when needed. Do not disable if you have the Logical Disk Manager Service enabled.
<b>Messenger</b>	Transmits net send and Alerter service messages between clients and servers. This service is not related to Windows Messenger	<b>Disabled</b>	<b>Yes</b>	Alerter messages will not be transmitted.	<b>Disable</b>	
<b>Microsoft Software Shadow Copy Provider</b>	Manages software-based volume shadow copies taken by the Volume Shadow Copy service	<b>Manual</b>	<b>Yes</b>	Software-based volume shadow copies cannot be managed.	<b>Disable</b>	Leave set at Manual if you intend to use Windows Backup.
<b>Net Logon</b>	Supports pass-through authentication of account logon events for computers in a domain.	<b>Automatic</b>	<b>Maybe</b>	For a home network, no use. For a domain environment, used for authentication.	<b>Disable (workgroup) Enable (domain)</b>	
<b>NetMeeting Remote Desktop Sharing</b>	Enables an authorized user to access this computer remotely by using NetMeeting over a corporate intranet	<b>Manual</b>	<b>Yes</b>	Remote desktop sharing will be unavailable.	<b>Disable</b>	If you use NetMeeting, don't disable this service.
<b>Network Access Protection Agent</b>	Allows windows clients to participate in Network Access Protection	<b>Manual</b>	<b>Yes</b>	Your Windows XP machine will not be able to use NAP services.	<b>Disable</b>	If your network uses Network Access Protection, enable this service.
<b>Network Connections</b>	Manages the network and dial-up connections for the server, including network status notification and configuration	<b>Manual</b>	<b>No</b>	Network configuration will not be possible; new connections can't be created and services that need network information may fail.	<b>Enable</b>	
<b>Network DDE</b>	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers	<b>Disabled</b>	<b>Yes</b>	DDE transport and security will be unavailable.	<b>Disable</b>	
<b>Network DDE DSDM</b>	Manages Dynamic Data Exchange (DDE) network shares	<b>Disabled</b>	<b>Yes</b>	DDE network shares will be unavailable.	<b>Disable</b>	

<b>Network Location Awareness (NLA)</b>	Responsible for collecting and storing network configuration and location information and notifying applications when this information changes. For example, as you make the move from the local coffee shop's wireless network back home to your wired docking station, NLA makes sure that applications are aware of the change.	<b>Manual</b>	<b>No</b>	Services such as the Internet Connection Firewall will not operate	<b>Enable</b>	Enable if this computer has Internet Connection Sharing enabled or if you are using the Internet Connection Firewall.
<b>Network Provisioning Service</b>	Manages XML configuration files on a domain basis for automatic network provisioning.	<b>Manual</b>	<b>Maybe</b>	You may experience problems connecting to networks.	<b>Disable (workgroup) Enable (domain)</b>	
<b>NT LM Security Support Provider</b>	Allows users to log on to the network using NTLM	<b>Manual</b>	<b>Maybe</b>	Users with versions of Windows prior to Windows 2000 will be unable to log in to the network.	<b>Disable</b>	Enable this service if this computer needs to log on to pre-Windows 2000 computers or domains
<b>Performance Logs and Alerts</b>	Collects performance data for the computer or other computers and writes it to a log or displays it on the screen	<b>Manual</b>	<b>Yes</b>	Performance information will no longer be logged or displayed.	<b>Disable</b>	
<b>Plug and Play</b>	Allows an administrator to add hardware to a server and have the server automatically detect and configure it	<b>Automatic</b>	<b>No</b>	The system will be unstable and incapable of detecting hardware changes.	<b>Enable</b>	
<b>Portable Media Serial Number Service</b>	Retrieves the serial number of any portable media player connected to this computer	<b>Manual</b>	<b>Yes</b>	Protected content might not be downloaded to the device.	<b>Disable</b>	
<b>Print Spooler</b>	Manages all local and network print queues and controls all printing jobs	<b>Automatic</b>	<b>Maybe</b>	Printing on the local machine will be unavailable.	<b>Enable</b>	It's not recommended to disable this service. Save yourself the hassle.
<b>Protected Storage</b>	Protects sensitive information such as private keys from exposure except to allowed persons and services	<b>Automatic</b>	<b>Yes</b>	Protected information will be inaccessible.	<b>Enable</b>	
<b>QoS RSVP</b>	Provides network signaling and local, traffic-control, set-up functionality for (Quality of Service) QoS-aware programs and control applets	<b>Manual</b>	<b>Yes</b>	QoS aware applications with either not function, or will not have their complete functionality.	<b>Disable</b>	Enable this service if you use QoS aware applications.
<b>Remote Access Auto Connection Manager</b>	Detects unsuccessful attempts to connect to a remote network or computer and provides alternative methods for connection	<b>Manual</b>	<b>Yes</b>	Users will need to manually connect to other systems.	<b>Enable</b>	
<b>Remote Access Connection Manager</b>	Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks	<b>Manual</b>	<b>Maybe</b>	The operating system may not function properly.	<b>Enable</b>	This service is run on demand by the Remote Access Manager
<b>Remote Desktop Help Session Manager</b>	Manages and controls Remote Assistance	<b>Manual</b>	<b>Yes</b>	Remote Assistance will be unavailable.	<b>Disable</b>	
<b>Remote Procedure Call (RPC)</b>	Allows processes to communicate internally and across the network with each other	<b>Automatic</b>	<b>No</b>	The system will not boot. Don't disable this service.	<b>Enable</b>	
<b>Remote Procedure Call (RPC) Locator</b>	Provides RPC name services similar to DNS services for IP	<b>Manual</b>	<b>No</b>	Systems that are running third-party utilities looking for RPC information will be unable to find it. OS components do not use this service, but programs such as Exchange do.	<b>Enable</b>	
<b>Registry</b>	Provides a mechanism to remotely manage the system registry	<b>Automatic</b>	<b>Maybe</b>	Remote systems will be unable to connect to the local registry. Hfnetchk uses this mechanism. Disabling it can affect the patch utility's operation.	<b>Disable</b>	Some programs require this functionality in order to operate.
<b>Removable Storage</b>	Manages and catalogs removable media and operates automated removable media devices	<b>Manual</b>	<b>Yes</b>	Programs that are dependent on Removable Storage, such as Backup and Remote Storage, will operate more slowly.	<b>Enable</b>	
<b>Routing and Remote Access</b>	Enables multiprotocol LAN-to-LAN, LAN-to-WAN, virtual private network (VPN), and network address translation (NAT) routing services for clients and servers on this network	<b>Disabled</b>	<b>Yes</b>	Routing and Remote Access services will be unavailable.	<b>Disable</b>	Better yet, don't install this service at all.
<b>Secondary Logon</b>	Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable	<b>Automatic</b>	<b>Yes</b>	Users will be unable to use the "Run As" feature to elevate privileges.	<b>Disable</b>	
<b>Security Accounts Manager</b>	Stores account information for local security accounts, which, when started, allows other services to access the SAM	<b>Automatic</b>	<b>Yes</b>	Services that rely on requests to the SAM database will not function properly. Group Policy objects may not operate properly.	<b>Enable</b>	If you use don't use DHCP to obtain an IP address, this service can be disabled.

<b>Security Center</b>	Monitors system security settings and configurations.	<b>Automatic</b>	<b>No</b>	Your system will not be able to monitor updates, firewall status and virus checking status.	<b>Enable</b>	
<b>Server</b>	Allows the sharing of local resources such as files and printers, as well as named pipe communication	<b>Automatic</b>	<b>Yes</b>	Resources can't be shared, RPC requests will be denied, and named pipe communication will fail.	<b>Disable</b>	This service must be enabled on Windows XP computers that share files or printers.
<b>Shell Hardware Detection</b>	Provides notifications for AutoPlay hardware events	<b>Automatic</b>	<b>Yes</b>	CD-ROMs and other devices will not automatically function.	<b>Enable</b>	Much easier to leave this enabled, and not
<b>Smart Card</b>	Manages access to smart cards read by this computer	<b>Manual</b>	<b>Yes</b>	This computer will be unable to read smart cards.	<b>Disable</b>	If you're using a smart card reader, enable this service.
<b>SSDP Discovery</b>	Used to locate UPnP devices on your home network. Used in conjunction with Universal Plug and Play Device Host, it detects and configures UPnP devices on your home network	<b>Manual</b>	<b>Yes</b>	Your computer will be unable to locate uPnP devices on the network.	<b>Disable</b>	
<b>System Event Notification</b>	Required to record entries in the event logs; notifies COM+ subscribers about logon and power-related events	<b>Automatic</b>	<b>Yes</b>	Certain notifications will no longer work. For example, synchronization won't work, as it depends on connectivity information and Network Connect/Disconnect and Local event notifications	<b>Disable</b>	Leave enabled for laptops to that power notifications are passed to the user.
<b>System Restore</b>	Performs system restore functions, including saving periodic checkpoints	<b>Automatic</b>	<b>Yes</b>	Automatic system restoration will not be possible.	<b>Disable</b>	While this service does use up some system resources, it can be invaluable for stand alone machines, particularly when a software install goes bad.
<b>Task Scheduler</b>	Enables a user to configure and schedule automated tasks on this computer	<b>Automatic</b>	<b>Yes</b>	Tasks will not be run at their scheduled times.	<b>Disable</b>	
<b>TCP/IP NetBIOS Helper</b>	Required for software distribution in a Group Policy (may be used to distribute patches) and provides support for NetBIOS over TCP/IP and NetBIOS name lookups	<b>Automatic</b>	<b>Yes</b>	NetBIOS over TCP/IP clients including Netlogon and Messenger might stop responding. Disabling may also affect the ability to share resources.	<b>Disable</b>	For small networks, this service may be essential if you share files with others. For larger networks with central file servers, keep disabled on desktops.
<b>Telephony</b>	Provides Telephony API (TAPI) support for clients using programs that control telephony devices and IP-based voice connections	<b>Manual</b>	<b>Yes</b>	The function of all dependent programs will be impaired.	<b>Disable</b>	Only needed for modem/fax modem use.
<b>Telnet</b>	Enables a remote user to log on to this computer and run programs; supports various TCP/IP Telnet clients, including UNIX- and Windows-based computers	<b>Disabled</b>	<b>Yes</b>	Remote user access to programs might be unavailable.	<b>Disable</b>	
<b>Terminal Services</b>	Allows users to connect interactively to a remote computer; Remote Desktop, Fast User Switching, Remote Assistance, and Terminal Server depend on this service	<b>Automatic</b>	<b>Yes</b>	May make your computer unreliable. To prevent remote use of this computer, clear the check boxes in the Remote tab of the System properties control panel item	<b>Disable</b>	
<b>Themes</b>	Provides user experience theme management	<b>Automatic</b>	<b>Yes</b>	Themes cannot be used.	<b>Disable</b>	
<b>Uninterruptible Power Supply</b>	Manages an uninterruptible power supply (UPS) connected to the computer	<b>Manual</b>	<b>Yes</b>	The UPS cannot communicate with the computer.	<b>Disable</b>	
<b>Universal Plug and Play Device Host</b>	Used in conjunction with SSDP Discovery Service, it detects and configures UPnP devices on your home network	<b>Manual</b>	<b>Yes</b>	Your computer will be unable to locate uPnP devices on the network.	<b>Disable</b>	
<b>Volume Shadow Copy</b>	Manages and implements volume shadow copies used for backup and other purposes	<b>Manual</b>	<b>Yes</b>	Shadow copies will be unavailable for backup and the backup may fail.	<b>Disable</b>	Enable this service if you use Windows Backup on this desktop.
<b>WebClient</b>	Enables Windows-based programs to create, access, and modify Internet-based files	<b>Automatic</b>	<b>Yes</b>	These functions will not be available.	<b>Disable</b>	
<b>Windows Audio</b>	Manages audio devices for Windows-based programs	<b>Automatic</b>	<b>Yes</b>	Audio devices and effects will not function properly.	<b>Enable</b>	Even though it can be disabled, without this service, you will get no sound.
<b>Windows Firewall/Internet Connection Sharing (ICS)</b>	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.	<b>Automatic</b>	<b>Yes</b>	Networking services such as Internet sharing, name resolution, addressing and/or intrusion prevention will be unavailable.	<b>Enable</b>	If you share your Internet connection, you must enable this service.
<b>Windows Image Acquisition (WIA)</b>	Provides image acquisition services for scanners and cameras	<b>Manual</b>	<b>Yes</b>	Programs that require images, such as Windows Movie Maker, won't function properly.	<b>Enable</b>	This service is required for some scanners and cameras. If you don't have a scanner or a camera, you can disable this service.
<b>Windows Installer</b>	Adds, modifies, and removes applications provided as a Windows Installer (*.msi) package	<b>Manual</b>	<b>Yes</b>	People can install no programs, or make use of Add/Remove programs.	<b>Enable</b>	
<b>Windows Management Instrumentation (WMI)</b>	Provides system management information; required to implement performance alerts using Performance Logs and Alerts	<b>Automatic</b>	<b>No</b>	System management and performance information will be unavailable.	<b>Enable</b>	

<b>Windows Management Instrumentation Driver Extensions</b>	Monitors all drivers and event trace providers that are configured to publish Windows Management Instrumentation (WMI) or event trace information	<b>Manual</b>	<b>Yes</b>	Provides systems management information to and from drivers.	<b>Enable</b>	
<b>Windows Time</b>	Uses NTP to keep computers in the domain synchronized	<b>Automatic</b>	<b>Yes</b>	Time synchronization won't take place.	<b>Enable</b>	
<b>Wired AutoConfig</b>	This service performs IEEE 802.1X authentication on Ethernet interfaces	<b>Manual</b>	<b>Yes</b>	This service performs IEEE 802.1X authentication on Ethernet interfaces	<b>Disable</b>	If your network uses 802.1x authentication, do not disable this service.
<b>Wireless Zero Configuration</b>	Automatically configured WiFi (802.11) network adapters	<b>Automatic</b>	<b>Yes</b>	You will have to manually configure wireless networking.	<b>Disable</b>	Enable this service if you're using wireless networking.
<b>WMI Performance Adapter</b>	Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network	<b>Manual</b>	<b>Yes</b>	This service runs only when Performance Data Helper is activated.	<b>Enable</b>	
<b>Workstation</b>	Provides network connections and communications using the Microsoft Network services	<b>Automatic</b>	<b>Yes</b>	The computer will be unable to connect to remote Microsoft Network resources.	<b>Enable</b>	

Copyright © 2009 CNET Networks, Inc., a CBS Company. All rights reserved. TechRepublic is a registered trademark of CNET Networks, Inc. For more downloads and a free TechRepublic membership, please visit <http://techrepublic.com/2001-6240-0.html>