Services in Windows XP - part1

Article URL
Services in Windows XP - part1

Author
SecurityHome.eu

Published: 23 September 2008

Last updated on 13 August 2011.

Â

Some smart words before you start:
* Before disabling ANY service, check out the information about each service by clicking on the name.

* Service settings are global, meaning changes apply to all users.

* Only disable a few services at a time to avoid changing "50" settings and trying to figure out "what broke it."

The explenation of the start-up type of services:
* Automatic

With a service in this state, it will start at boot time. Some services, when no longer required, will also automatically stop when not needed. However, this is very rare. If you find you do not need a service, place it into Manual or Disabled.

* Manual

Manual mode allows Windows to start a service when needed. However, very few services will start up when required in Manual mode. If you find you need a service, place it into Automatic.

* Disabled

This setting will stop a service from starting, even if needed. Errors in the Event Viewer will show up

complaining of that fact. Some services, while Disabled, will constantly complain. However, this situation is taken care of if placed in Manual. The service descriptions identifies those that should be in Manual vice Disabled.

Thanx to BlackViper, who has a full explenation of the services on his website
http://www.blackviper.com/WIN2K/win2kservice411.htm

Alter

The Alerter service notifies users of administrative alerts on a network. This service usually is not required under normal circumstances. Note: This is NOT "WinPopUp."
You can disable it.

Dependencies:
What service Alerter needs to function properly:
* Workstation

What other service require Alerter to function properly:
* None

Application Layer Gateway Service

Provides support for 3rd party plug-ins for Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS). This service is required if using Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS) to connect to the internet. This service uses about 1.5 MB of memory in an idle state.
Leave it on manual.

Dependencies:
What service Application Layer Gateway Service needs to function properly:
* None

What other service require Application Layer Gateway Service to function properly:
* Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)

Application Management

Used for Assign, Publish and Remove software services. If you cannot modify your software installation of certain applications, put this service in to Automatic or Manual. If you have Windows XP Home Version, this service may be causing problems described in this knowledge base article:
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q328213?SD=EE

Leave this service on manual

Dependencies:
What service Application Management needs to function properly:
* None

What other service require Application Management to function properly:
* None

Automatic Updates

Used to check up to see if there is any critical or otherwise updates available for download. You may choose to update manually due to the very long lag time from when an update is available and when Windows XP reports it. After the installation of Service Pack 1, you may configure how "often" updates are checked. Using default values, Windows XP "automatically" downloads the updates and asks to "install" them. A few reasons why you may think this is unacceptable in your situation:
You could have a dial-up connection. If XP feels like downloading whenever it wants, it just may not allow you to do what "you" want.
You may also:
Wish to know what, when and how an update installs BEFORE using any bandwidth.
Want to read about the update BEFORE downloading.
Want to know WHY you need it and WHAT it fixes.
It is very important that if you decide to disable this service, you check the Windows Update site often to ensure the latest patches install properly.

Dependencies:
What service Automatic Updates needs to function properly:
* None

What other service require Automatic Updates to function properly:
* None

Background Intelligent Transfer Service

This service is used to transfer asynchronous data via http1.1 servers. According to Microsoft's site, Windows Update uses this "feature." It "continues" a download if you log off or shutdown the system (that is, when you log back in). The problem with that is, I do not like having this "feature" running all of the time. Even though I have found no side effects as to this being disabled, you may require this service for some MSN Explorer, Windows Messenger, Windows Media Player or future .NET functions. Take note: Manual update via Windows Update web site requires Cryptographic Services to be running.
Disable this service.

Dependencies:
What service Background Intelligent Transfer Service needs to function properly:
* Remote Procedure Call (RPC)

Workstation
What other service require Background Intelligent Transfer Service to function properly:
* None

ClipBook

Used to store information (cut / paste) and share it with other computers. I have never found enough need for this to allow this service to always be running. This service alone uses about 1.3 MB of memory.
You can disable this service.

Dependencies:
What service ClipBook needs to function properly:
* Network DDE

* Network DDE DSDM

What other service require ClipBook to function properly:
* None

COM+ Event System

You will receive, in the Event Log, an entry from "DCOM" complaining about not having this service running if disabled. I am unaware of any application that uses COM+, but if set to manual, many services report to it, so it will start anyway. This service is required for System Event Notification.
On your system, see if you have any installed "COM+" Applications. If not, you can probably disable this service with no side effects (besides the Event Log complaining upon reboots). Take note: BootVis requires Task Scheduler and COM+ Event System to be running if you wish to take advantage of the "optimize system" function. Why is it required? It is due to the pre-fetching function built into Windows XP. Another Note: Pre-fetching only occurs on boot up and application start, so if you do not care about a few extra seconds of boot time, you may decide to not even bother with it and disable Task Scheduler. Depending on the system, pre-fetching may increase performance. Windows Media Player may also require this service for some "features" to function. MS' .NET may require this service in the future. I recommend disabled for Super Tweaking, automatic for "safe", and manual for most other configurations.

Dependencies:
What service COM+ Event System needs to function properly:
* Remote Procedure Call (RPC)

What other service require COM+ Event System to function properly:
* System Event Notification

COM+ System Application

You will receive, in the Event Log, an entry from "DCOM" complaining about not having this service running if disabled. I am unaware of any application that uses COM+, but if set to manual, many services report to it, so it will start anyway.
On your system, see if you have any installed "COM+" Applications. If not, you can probably disable this service with no side effects (besides the Event Log complaining upon reboots). This service is required for System Event Notification.
Leave it on manual.

Dependencies:
What service COM+ System Application needs to function properly:
* Remote Procedure Call (RPC)

What other service require COM+ System Application to function properly:
* None

Computer Browser

Computer Browser service maintains a listing of computers and resources located on the network. This service is not required on a standalone system. In fact, even if you want to browse the network (workgroup or domain) or have mapped network shares as local hard drives, you can still do so. On a large network, one computer is designated the "master" browser and another one is the "backup" browser. All others just announce they are available every 12 minutes to "take over" duties if one of the other computers fail. No lag time is discernable if this service remains disabled on all but one computer. Honestly, I do not even believe one needs to be running. You could, "just in case," but it sure does not need to be running on all computers, all of the time.
I disable this service.

Dependencies:
What service Computer Browser needs to function properly:
* Server

* Workstation

What other service require Computer Browser to function properly:
* None

Cryptographic Services

Mainly, it confirms signatures of Windows files. You may always get a dialog box complaining about uncertified drivers if this is disabled. This service is required for Windows Update to function in manual and automatic mode and this service is required to install Service Pack 1 unified updates and DirectX 9.0. Windows Media Player and future .NET applications may also require this service for some "features" to function. This service uses about 1.9 MB of memory.
I recommand you leave it on Automatic.

Dependencies:
What service Cryptographic Services needs to function properly:
* Remote Procedure Call (RPC)

What other service require Cryptographic Services to function properly:
* None

DHCP Client

This service automatically receives a Dynamic IP address from your DHCP server and DNS updates. Required for ICS / internet client and if you run IPSEC, disable on a standalone system or one that has a static IP address. Take note: Most DSL/cable ISP's use DHCP to provide internet access. If you disable this service and your Internet connection no longer works, place this back into automatic. Most DSL and cable hardware routers have the option of enabling a DHCP server for the internal network. Ensure that the router is configured the same as your local PC's. Leave this on automatic, unless you have a static ip.

Dependencies:
What service DHCP Client needs to function properly:

* AFD Networking Support Environment
* NetBIOS over TCP/IP
* TCP/IP Protocol Driver
* IPSEC driver
* TCP/IP Protocol Driver
* IPSEC driver

What other service require DHCP Client to function properly:

* None

Distributed Link Tracking Client

Maintains links with NTFS files within your computer or across a domain. For example, you could make a file on "Computer A." You then create a "short cut" or "link" to that file on "Computer B." If you would move the file on Computer A to a different location, this service would tell Computer B to update its information to allow uninterrupted connectivity. Even though this is rather valuable on a large network, I have not found a use for this service on a home network. It uses about 3.5 MB to 4 MB in an idle state.
Change it to manual.

Dependencies:

What service Distributed Link Tracking Client needs to function properly:
* Remote Procedure Call (RPC)

What other service require Distributed Link Tracking Client to function properly:
* None

Distributed Transaction Coordinator

Automatically takes care of transactions that span multiple resources. This service is required if using Message Queuing. You may also see complaints in the Event Log if this service is disabled, but I have experienced no side effects. Microsoft's .NET may require this service in the future. Leave it on manual.

Dependencies:
What service Distributed Transaction Coordinator needs to function properly:
* Remote Procedure Call (RPC)

* Security Accounts Manager

* Remote Procedure Call (RPC)

What other service require Distributed Transaction Coordinator to function properly:
* Message Queuing

* Message Queuing Triggers

DNS Client

Resolves and caches DNS names and Active Directory domain controller functions. This service is not required for DNS lookups, but if it makes you happy to have it running, you may. However, DNS Client is required if using IPSEC. If you attempt to "repair" your network connection and a dialog box complains that the "DNS resolver failed to flush the cache," this service is the reason. Leave this on automatic.

Dependencies:

What service DNS Client needs to function properly:
* TCP/IP Protocol Driver

* IPSEC driver

What other service require DNS Client to function properly:
* None

Error Reporting Service

Calls home to Microsoft when application errors occur. I personally do not like this. I feel it is a waste of memory and resources. On the other hand, if you are experiencing system crashes often, the best way to deal with them is to report them using this tool.
Disable this service.

Dependencies:
What service Error Reporting Service needs to function properly:
* Remote Procedure Call (RPC)

What other service require Error Reporting Service to function properly:
* None

Event Log

View Event Log messages from applications in Event Viewer. Always helpful to check out the Event Log to see what problems with applications are popping up that is "hidden" from the normal user. To see quickly what, if anything has resulted in your adjustments, you may consider clearing the Event Log. Windows Management Instrumentation also requires Event Log Service to be running. If you disable the Event Log Service, but do not disable Windows Management Instrumentation, your computer may have an extended boot time while Windows Management Instrumentation is waiting for the Event Log to start. It is just best to keep Event Log active for troubleshooting purposes and normal operations.
Leave this on automatic.

Dependencies:

What service Event Log needs to function properly:
* None

What other service require Event Log to function properly:
* Simple Mail Transfer Protocol (SMTP)

* SNMP Service

* SNMP Trap Service

* Windows Management Instrumentation

Fast User Switching Compatibility

Unless you have many users on a system, you probably do not even need this service to be running. You could benefit, however, greatly if you use this service in conjunction with many users on your local computer to allow switching users without closing all existing applications running under a different account.
Leave it on manual.

Dependencies:
What service Fast User Switching Compatibility needs to function properly:
* Terminal Services *
* Remote Procedure Call (RPC)

What other service require Fast User Switching Compatibility to function properly:
* None

Fax Service

Not installed by default, but if needed, you may install it later off the Windows XP CD. Maintains the ability to send and receive FAX documents on your computer.

Dependencies:

What service Fax Service needs to function properly:
* Plug and Play
* Print Spooler
* Remote Procedure Call (RPC)
* Telephony
* Plug and Play
* Remote Procedure Call (RPC)

What other service require Fax Service to function properly:
* None

FTP Publishing Service

This feature is not available on Windows XP Home or installed by default on Windows XP Pro, but if you need it, you may install it later off the Windows XP CD. This service provides a FTP server on your network.

Dependencies:
What service FTP Publishing Service needs to function properly:
* IIS Admin
* Remote Procedure Call (RPC)
* Security Accounts Manager
* Remote Procedure Call (RPC)

What other service require FTP Publishing Service to function properly:
* None

Help and Support

This service is required for Microsoft's online (or offline) help documents. If you ever "attempt" to use Help and Support, the service places itself back into "Automatic" and starts even if you already had this service on disabled.
Put this on disabled.

Dependencies:
What service Help and Support needs to function properly:
* Remote Procedure Call (RPC)

What other service require Help and Support to function properly:
* None

Human Interface Device Access

You may not have any peripherals that require this service. If one of yours magically does not function anymore, set it to automatic. Namely, scanners with function buttons (fax, copy) or even an "Internet" keyboard with volume or play controls. Leave this on disabled.

Dependencies:
What service Human Interface Device Access needs to function properly:
* Remote Procedure Call (RPC)

What other service require Human Interface Device Access to function properly:
* None

IIS Admin

This feature is not available on Windows XP Home or installed by default on Windows XP Pro, but if needed, you may install it later off the Windows XP CD. This service usually operates in conjunction with a local web site or FTP server. Leave it uninstalled mainly because IIS has been "popular" for crackers to break.

Dependencies:
What service IIS Admin needs to function properly:

* Remote Procedure Call (RPC)

* Security Accounts Manager

* Remote Procedure Call (RPC)

What other service require IIS Admin to function properly:

* FTP Publishing Service

* Simple Mail Transport Protocol (SMTP)

* World Wide Web Publishing Service

IMAPI CD-Burning COM Service

This service operates that cool "drag and drop" CD burn capability. You will need this service to burn CD's. What is the good news? If you set this service to manual, the service starts and stops itself when used with some software packages. This is practically the only service that does do this! If you still cannot burn a CD with it on manual, switch to automatic and feel safe that it starts only when "needed." This service may take up about 1.6 MB of memory in an idle state. Leave it on manual or put on automatic.

Dependencies:
What service IMAPI CD-Burning COM Service needs to function properly:

* None

What other service require IMAPI CD-Burning COM Service to function properly:

* None

Indexing Service

This service always has been a major resource hog. I NEVER recommend having this service enabled. Remove the function via the "Add / Remove Programs" icon in the control panel (Windows Setup Programs). It uses about 500 K to 2 MB in an idle state, not to mention the amount of memory and CPU resources it takes to INDEX the drives. I have had people (and witnessed it on other people's computers) report to me that the Indexing Service sometimes starts up EVEN while the system is NOT idle... as in the middle of a game. You may feel, as I do, that this is unacceptable. If your computer suddenly seems "sluggish," Indexing Service is usually the cause of it. Change this to disabled.

Dependencies:
What service Indexing Service needs to function properly:

* Remote Procedure Call (RPC)

What other service require Indexing Service to function properly:

* None

Internet Connection Firewall (ICF) and Internet Connection Sharing (ICS)

Used to allow multiple computers on your network to access the internet via only one account. This service installs on the "modem" computer. If you are using a third party firewall or Internet Connection Sharing software package, this service is not required.
Put it on automatic unless you have a 'professional' firewall.

Dependencies:
What service Internet Connection Firewall (ICF) and Internet Connection Sharing (ICS) needs to function properly:

* Application Layer Gateway Service
* Network Connections
* Remote Procedure Call (RPC)
* Network Location Awareness (NLA)
* AFD Networking Support Environment
* NetBIOS over TCP/IP
* TCP/IP Protocol Driver

* IPSEC driver

* Remote Access Connection Manager

* Telephony

* Plug and Play

* Remote Procedure Call (RPC)

What other service require Internet Connection Firewall (ICF) and Internet Connection Sharing (ICS) to function properly:

* None

IPSEC Services

May be required on some domains or VPN connections, but the "average" user will not need this. Disable this service.

Dependencies:
What service IPSEC Services needs to function properly:

* IPSEC driver

* Remote Procedure Call (RPC)

* TCP/IP Protocol Driver

* IPSEC driver

What other service require IPSEC Services to function properly:

* None

Logical Disk Manager

This service is vital to run the Disk Management MMC console for dynamic volumes. If you attempt to "Manage" your hard drives and a dialog box pops up complaining about not being able to do this, start this service. Put this service on manual.

Dependencies:
What service IPSEC Services needs to function properly:
* Plug and Play

* Remote Procedure Call (RPC)

What other service require IPSEC Services to function properly:
* Logical Disk Manager Administrative Service

Logical Disk Manager Administrative Service

This service is vital to run the Disk Management MMC console for dynamic volumes.
Leave this on manual.

Dependencies:
What service Logical Disk Manager Administrative Service needs to function properly:
* Logical Disk Manager

* Plug and Play

* Remote Procedure Call (RPC)

What other service require Logical Disk Manager Administrative Service to function properly:
* None

Message Queuing

This feature is not available on Windows XP Home or installed by default on Windows XP Pro, but if needed, you may install it later off of the Windows XP CD. May be used on some domains, but the "average" home user will never need this service.

Dependencies:
What service Message Queuing needs to function properly:

* Distributed Transaction Coordinator
* Remote Procedure Call (RPC)
* Security Accounts Manager
* Message Queuing access control
* NT LM Security Support Provider
* Reliable Multicast Protocol driver
* Protected Storage
* Server

What other service require Message Queuing to function properly:

* Message Queuing Triggers

Message Queuing Triggers

This feature is not available on Windows XP Home or installed by default on Windows XP Pro, but if needed, you may install it later off the Windows XP CD. This service is required if you use Message Queuing service.

Dependencies:
What service Message Queuing needs to function properly:

* Message Queuing
* Distributed Transaction Coordinator

* Remote Procedure Call (RPC)
* Security Accounts Manager
* Message Queuing access control
* NT LM Security Support Provider
* Reliable Multicast Protocol driver
* Protected Storage
* Server

What other service require Message Queuing to function properly:
* None

Messenger

This service provides the ability to send messages between clients and servers. This service needs not to be running under normal "home" conditions. It is also advisable to make this service go away to avoid the possibility of "net send" messages hitting your computer from the internet. This has nothing to do with MSN Messenger, nor is it "WinPopUp."

To test for this security vulnerability, at the command prompt, (run: cmd.exe) type:
net send 127.0.0.1 hi

If you get a popup "hi" message, you should disable the Messenger service.
If you get an error stating, "The message alias could not be found on the network," you are safe.

If, for whatever reason, you need the Messenger service running but wish not to have spam popups active, you can disable the particular ports at your firewall. The Messenger service uses UDP ports 135, 137, and 138; TCP ports 135, 139, and 445.

I recommand to disable this function.

Dependencies:
What service Messenger to function properly:
* NetBIOS Interface

* Plug and Play

* Remote Procedure Call (RPC)

* Workstation

What other service require Messenger to function properly:
* None

MS Software Shadow Copy Provider

Used in conjunction with the Volume Shadow Copy service, Microsoft Backup uses these services. You will receive, in the Event Log, an entry complaining about not having this service running if disabled. I have yet to find a side effect, though, but to avoid the messages, you can place the service in manual. Some third party hard disk "ghost" or "imaging" software may require this service to be running.
Leave this on manual.

Dependencies:
What service MS Software Shadow Copy Provider to function properly:
* Remote Procedure Call (RPC)

What other service require MS Software Shadow Copy Provider to function properly:
* None

Net Logon

Used for logging onto a Domain Controller. This service is not required on a standalone system, or for a "home" network.
Disable this service.

Dependencies:
What service Net Logon to function properly:
* Workstation

What other service require Net Logon to function properly:
* None

NetMeeting Remote Desktop Sharing

Enables a user to access your computer using NetMeeting. This may create a BIG open door for the unwanted. If you are paranoid about security, disable this function. Even if you were not worried, I would still get rid of it.
Disable this service.

Dependencies:
What service NetMeeting Remote Desktop Sharing to function properly:
* None

What other service require NetMeeting Remote Desktop Sharing to function properly:
* None

Network Connections

Required for managing network connectivity. Set to disabled if you have no network or you do not toy with the configurations a lot. If your internet connectivity no longer operates after disabling this function, set it back to Automatic! Note: While disabling this service, you will no longer see the system tray icon (lower right) displayed, even for modem connections. Connectivity, however, still exists even on incoming shared network drives. Leave this on manual.

Dependencies:
What service NetMeeting Remote Desktop Sharing to function properly:
* Remote Procedure Call (RPC)

What other service require NetMeeting Remote Desktop Sharing to function properly:
* Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)

Network DDE

I have not found a good use for this service. Unless you use remote ClipBook, disable it. This uses about 1.5 MB idle.
Disable this service.

Dependencies:
What service Network DDE to function properly:
* Network DDE DSDM

What other service require Network DDE to function properly:
* ClipBook

Network DDE DSDM

I have not found a good use for this service. Unless you use remote ClipBook, disable it.

Dependencies:
What service Network DDE to function properly:
* None

What other service require Network DDE to function properly:
* Network DDE

* ClipBook

Network Location Awareness (NLA)

This service is required for use with the Internet Connection Sharing service (server only).
Leave this on manual.

Dependencies:
What service Network Location Awareness (NLA) to function properly:
* AFD Networking Support Environment

* NetBIOS over TCP/IP

* TCP/IP Protocol Driver

* IPSEC driver

What other service require Network Location Awareness (NLA) to function properly:
* Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)

NT LM Security Support Provider

Manages local system security information on the computer. You need this service if you are running Message Queuing or Telnet server.
Leave this on manual.

Dependencies:
What service NT LM Security Support Provider to function properly:
* None

What other service require NT LM Security Support Provider to function properly:
* Message Queuing

* Message Queuing Triggers

* Telnet

Continue to Services in Windows XP - part 2