10 Windows XP services you should never disable

Version 1.0
August 20, 2009

By Scott Lowe

There are, quite literally, dozens of guides out there that help you determine which services you can safely disable on your Windows XP desktop. Disabling unnecessary services can improve system performance and overall system security, as the system's attack surface is reduced. However, these lists rarely indicate which services you should *not* disable. All of the services that run on a Window system serve a specific purpose and many of the services are critical to the proper and expected functioning of the desktop computing environment. In this article, you'll learn about 10 critical Windows XP services you shouldn't disable (and why).

Note: For a quick how-to video on the basics, see Disable and enable Windows XP services.

1 DNS Client

This service resolves and caches DNS names, allowing the system to communicate with canonical names rather than strictly by IP address. DNS is the reason that you can, in a Web browser, type http://www.techrepublic.com rather than having to remember that http://216.239.113.101 is the site's IP address.

If you stop this service, you will disable your computer's ability to resolve names to IP addresses, basically rendering Web browsing all but impossible.

2 Network Connections

The Network Connections service manages the network and dial-up connections for your computer, including network status notification and configuration. These days, a standalone, non-networked PC is just about as useful as an abacus -- maybe less so. The Network Connections service is the element responsible for making sure that your computer can communicate with other computers and with the Internet.

If this service is disabled, network configuration is not possible. New network connections can't be created and services that need network information will fail.

3 Plug and Play

The Plug and Play service (formerly known as the "Plug and Pray" service, due to its past unreliability), is kicked off whenever new hardware is added to the computer. This service detects the new hardware and attempts to automatically configure it for use with the computer. The Plug and Play service is often confused with the *Universal* Plug and Play service (uPNP), which is a way that the Windows XP computer can detect new network resources (as opposed to local hardware resources). The Plug and Play service is pretty critical as, without it, your system can become unstable and will not recognize new hardware. On the other hand, uPNP is not generally necessary and can be disabled without worry. Along with uPNP, disable the SSDP Discovery Service, as it goes hand-in-hand with uPNP.

Historical note: Way back in 2001, uPNP was implicated in some pretty serious security breaches, as described here.

If you disable Plug and Play, your computer will be unstable and incapable of detecting hardware changes.

4 Print Spooler

Just about every computer out there needs to print at some point. If you want your computer to be able to print, don't plan on disabling the Print Spooler service. It manages all printing activities for your system. You may think that lack of a printer makes it safe to disable the Print Spooler service. While that's technically true, there's really no point in doing so; after all, if you ever do decide to get a printer, you'll need to remember to re-enable the service, and you might end up frustrating yourself.

When the Print Spooler service is not running, printing on the local machine is not possible.

5 Remote Procedure Call (RPC)

Windows is a pretty complex beast, and many of its underlying processes need to communicate with one another. The service that makes this possible is the Remote Procedure Call (RPC) service. RPC allows processes to communicate with one another and across the network with each other. A ton of other critical services, including the Print Spooler and the Network Connections service, depend on the RPC service to function. If you want to see what bad things happen when you disable this service, look at the comments on this link.

Bad news. The system will not boot. Don't disable this service.

6 Workstation

As is the case for many services, the Workstation service is responsible for handling connections to remote network resources. Specifically, this service provides network connections and communications capability for resources found using Microsoft Network services. Years ago, I would have said that disabling this service was a good idea, but that was before the rise of the home network and everything that goes along with it, including shared printers, remote Windows Media devices, Windows Home Server, and much more. Today, you don't gain much by eliminating this service, but you lose a lot.

Disable the Workstation service and your computer will be unable to connect to remote Microsoft Network resources.

7 Network Location Awareness (NLA)

As was the case with the Workstation service, disabling the Network Location Awareness service might have made sense a few years ago -- at least for a standalone, non-networked computer. With today's WiFi-everywhere culture, mobility has become a primary driver. The Network Location Awareness service is 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. Further, some other services depend on this service's availability.

Your computer will not be able to fully connect to and use wireless networks. Problems abound!

8 DHCP Client

Dynamic Host Configuration Protocol (DHCP) is a critical service that makes the task of getting computers on the network nearly effortless. Before the days of DHCP, poor network administrators had to manually assign network addresses to every computer. Over the years, DHCP has been extended to automatically assign all kinds of information to computers from a central configuration repository. DHCP allows the system to automatically obtain IP addressing information, WINS server information, routing information, and so forth; it's required to update records in dynamic DNS systems, such as Microsoft's Active Directory-integrated DNS service. This is one service that, if disabled, won't necessarily cripple your computer but will make administration much more difficult.

Without the DHCP Client service, you'll need to manually assign static IP addresses to every Windows XP system on your network. If you use DHCP to assign other parameters, such as WINS information, you'll need to provide that information manually as well.

9 Cryptographic Services

Every month, Microsoft provides new fixes and updates on what has become known as "Patch Tuesday" because the updates are released on the first Tuesday of the month. Why do I bring this up? Well, one service supported by Cryptographic Services happens to be Automatic Updates. Further, Cryptographic Services provides three other 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. Finally, Cryptographic Services also supports some elements of Task Manager.

Disable Cryptographic Services at your peril! Automatic Updates will not function and you will have problems with Task Manager as well as other security mechanisms.

10 Automatic Updates

Keeping your machine current with patches is pretty darn important, and that's where Automatic Updates comes into play. When Automatic Updates is enabled, your computer stays current with new updates from Microsoft. When disabled, you have to manually get updates by visiting Microsoft's update site.

New security updates will not be automatically installed to your computer.