
Services in windows 7

Article URL

[Services in windows 7](#)

Author

SecurityHome.eu

Published: 01 May 2015

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.
- * Before you start making changes, you should first create a system restore point. This way, if something doesn't work, you can always reverse the changes you made.

You can speed up your system by disabling or setting to manual unneeded services in Windows 7.
You can directly opening Services by typing services.msc

in RUN or start command searchbox.

Here is a list of services that in most cases can be safely disabled or set to manual:

* Bluetooth Support Service: unless you use Bluetooth devices such as keyboards, mice, printers or phones, you can disable this service. Keep in mind that, if you choose to disable this service, then no Bluetooth devices will be recognized. Also, the already connected Bluetooth devices may fail to work properly. Safe setting: Manual;

* BitLocker Drive Encryption Service: unless you use Microsofts Encryption Software (included in Windows 7 Ultimate and Enterprise Edition, and in Windows 8 Pro and Enterprise), you can disable this service. BitLocker Drive Encryption is a feature that allows users to protect data by providing encryption for

entire volumes. Safe setting: Manual;

* Certificate Propagation: if you don't use SmartCards (sometimes used in large organizations), it is safe to disable this service. Safe setting: Manual;

* Encrypting File System: EFS provides file encryption technology for storing encrypted files on NTFS file systems. If you don't need to encrypt data on your hard drives, it is OK to disable it. Safe setting: Manual;

* Fax: unless you use your computer to send or receive faxes using fax resources available on your system (for ex. by using a fax-modem), you can disable it. Safe setting: Manual;

* Microsoft iSCSI Initiator Service: iSCSI is an abbreviation for Internet Small Computer System Interface - an IP-based storage networking standard for linking data storage facilities. It allows client computers to access data over long distances on remote data centers, by using existing infrastructure (ex. over LAN, Internet). iSCSI devices are disks, tapes, CDs, and other storage devices on another networked computer that you can connect to. Sometimes these storage devices are part of a network called a storage area network (SAN). Unless you need to connect to iSCSI devices, it is safe to disable this service. Safe setting: Manual;

* Netlogon: this service is not needed in a home computer. It maintains a secure channel between the local computer and the domain controller for authenticating users. Unless you are connecting to a network domain, this service will never be used. Safe setting: Manual;

* Offline Files: unless you use the Offline Files functionality from Windows, you can disable it. Safe setting: Manual;

NOTE: This service is available only in Windows 7 Professional, Ultimate and Enterprise. In Windows 8 it is available only in the Pro and Enterprise editions.

* Parental Controls (in Windows 7) / Family Safety (in Windows 8): unless you have children using your computer and you want to monitor and control their activities, this service is not required. Safe setting: Manual;

* Print Spooler: if you don't have a printer attached to your computer and you don't use virtual printers (e.g.: PDF creator, Microsoft XPS Document Writer, Snagit, etc) you can disable it. Safe setting: Manual;

* Remote Desktop Configuration: Remote Desktop Protocol is a protocol developed by Microsoft which provides Windows users with a graphical interface to another computer. The client used by Microsoft is called Remote Desktop Connection. If you don't need to connect remotely to another computer or allow incoming remote connections to yours, then it is safe to disable this service. Safe setting: Manual;

* Remote Desktop Services: same as above. Safe setting: Manual;

* Remote Desktop Services UserMode Port Redirector: same as above. Safe setting: Manual;

* Remote Registry: this service enables remote users to modify the Windows Registry. Some say that having this service turned on can pose security issues, and therefore, choose to disable it. In Windows Vista and Windows 7, this service is set to a manual start by default, while in Windows 8 it is disabled. After disabling it, I encountered some problems while updating my system, so I really think that it is safe to leave it set to Manual, at least in Windows 7. Safe setting: Manual;

* Routing and Remote Access Service: This service offers routing services to businesses in local area and wide area networks. It allows computers to dial in to the local computer in order for it to get access to the local network. On a home computer you wont need such features. Safe setting: Manual;

* Secondary logon: if you are the only user of your computer, it can be disabled. But only if you dont plan to use more than one user account. Safe setting: Manual;

* Smart Card: Smart Cards are generally used for safety reasons in large organizations or corporations. The typical home user wont probably need this service to be running. Safe setting: Manual;

* Smart Card Removal Policy: same as above. Safe setting: Manual;

* Tablet PC Input Service (in Windows 7) / Touch Keyboard and Handwriting Panel Service (Windows 8): you can safely disable this service, unless you use Tablet PC. Some "Tablet PC Components" like the Snipping tool or Windows Journal will continue to function, while the Tablet PC Input Panel will not. The default startup type is Manual. You can set it even to Disabled without negatively impacting your computing experience;

* Windows Connect Now: this service is used by laptops and other mobile computers to connect to Wireless Networks. If you are on a desktop computer, you can disable this service. Safe setting: Manual;

* Windows Defender: if you use a third-party security solution (antivirus and antispysware), then disabling this service is a safe choice. You should also check this tutorial: [Windows Defender - How to Turn it On or Off](#). Safe setting: Manual.

* Windows Error Reporting Service: this service is used to report system errors to Microsoft. Although disabling this service wont affect your Windows computer, letting it run when needed may help you solve problems and issues that occur on your system, by searching solutions available from Microsoft. Safe setting: Manual;

* Windows Firewall: This service should be disabled only if you are using a third-party security solution that provides firewall protection. Safe setting: Manual;

* Windows Time: if your computer doesnt have access to the Internet then you dont need to update the system time from online servers. You can safely disable this service. But if you do, then this service will keep your system time accurate. Safe setting: Manual;
