5 security features of Windows 7 businesses should know

Although you can't immediately take advantage of all the new features of Windows 7, you can still plan to use and know more about them right now.

***TipsMake.com* - 2 from Windows and security - security is not always compatible. In the past, Microsoft's search for creating an easier-to-manage operating system for users meant sacrificing protection because it was vulnerable to infection and infection. The scandal of Windows XP on vulnerabilities pervaded by computer pests is an example, and Microsoft has upgraded its operating system with a firewall - firewall. However, they left it off by default.**

After loopholes in its software, Vista marked a big step in Windows security. After that, Windows 7 continues to develop this improvement by adding some new features and along with enhancing other features - the most obvious example is the User Account Control system in Windows Vista that has caused users. It must be turned off, although this may make their operating system vulnerable for hackers to take advantage of, in return they have a less unpleasant experience with the operating system. In Windows 7, UAC was 'refurbished', reduced intrusions and made more intimidating to be able to operate more efficiently.

Other Windows 7 security features are less obvious, especially those for businesses that are concerned about security protection for not just one but the entire computer network. Among the most important new features is DirectAccess, an alternative to VPN for computers operating on Windows systems; is a Windows Biometric Framework, standardizing fingerprint usage in scanners and biometric applications; and AppLocker, upgrading previous versions of Windows as Software Restriction Policies to limit software that can run on the computer.

Another notable feature is BitLocker To Go. This feature allows the BitLocker drive encryption to be extended to external hard drives and has a 'refined' method of existing firewall profiles to increase the defenses when users access the Internet.

According to the usual routine, these features are widely available without the display or guidance of the company. Let's take a look at each feature so we can know how to make Windows safer.

Note that some of these features are available in all versions of Windows 7, while others are only available in the Enterprise or Ultimate versions. Moreover, you cannot fully implement some features unless you update all users to Windows 7 or at least one - DirectAccess - requires the background that most companies do not have. However, these features work with older technologies for users who still 'steadfastly' use older versions of Windows.

So even though you can't immediately take advantage of all the new features, you can still plan to use and know more about them right now. We will start with the features you can use right away.

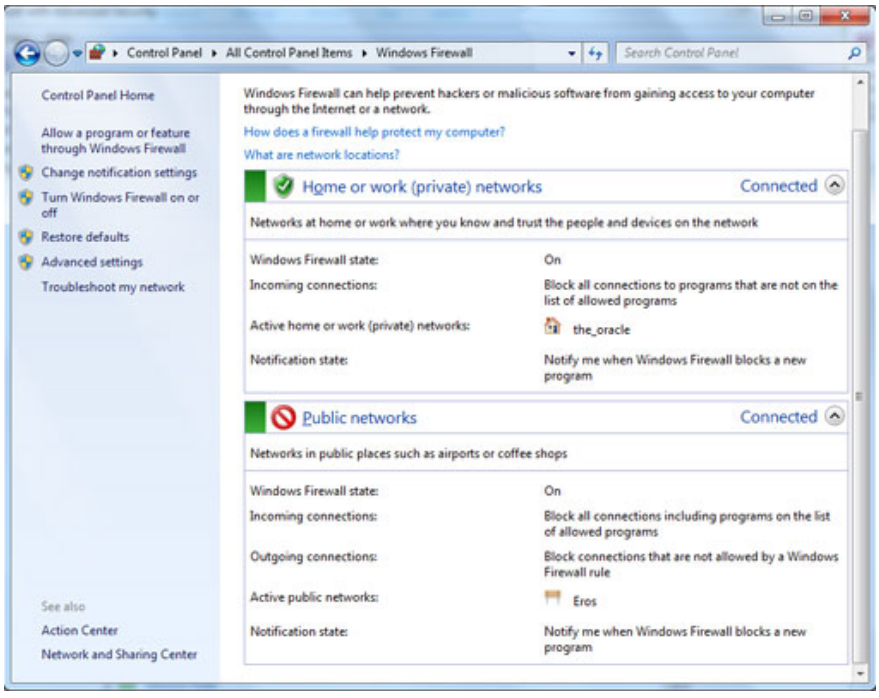
Multiple active firewall profiles

Windows 7 provides a small but important improvement from Vista in how to manage the firewall profile. Vista allows users to install different profiles for public, private and domain connections. Personal networks can be Wi-Fi, WEP or WPA, though not logged in, but you can still trust it rather than a public network or café. A domain requires assertions - passwords, fingerprints, smart cards or other combined elements - to be able to log in.

Each type of profile has its own application and connection options that can be allowed to pass through the firewall. For example, for private or small business networks, using Private is that you can allow file and printer sharing, while with Public using networks, you can prevent access to your files.

Firewall profiles work well unless a computer is connected simultaneously with a lot of networks, such as Ethernet and wireless networks. In this case, the system must default to using a most restrictive profile. However, this can cause problems, such as when connecting to a VPN via Wi-Fi network, Vista can identify simultaneous connections to both public and private networks and apply public profiles. for both.

All versions of Windows 7 allow computers to operate a number of firewall profiles at the same time, keeping access and operation of trusted networks while it will prevent less reliable networks. more reliable. Because there are so many remote access functions, firewall installation requirements are less 'strict', now users can work more safely while still being protected from threats outside the network.



Windows Biometric Framework

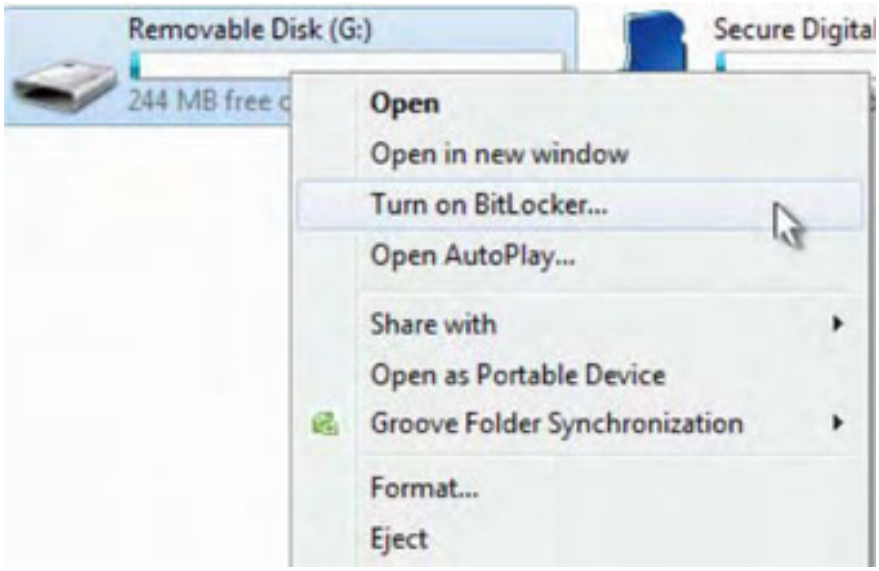
With fingerprint recognition becoming more and more popular on laptops, the task of setting a benchmark in biometric data storage has become more important than ever. With the Windows Biometric Framework, a standard for storing fingerprint data and accessing it through API application reference interface. Although most of these subsystem features are only suitable for programmers, there are two important things businesses should know:
First, while the fingerprint scanner can only be used to log on to a computer that cannot log into a company domain, the Windows Biometric Framework can log on to the domain.

Secondly, users can save up to 10 fingerprints, each with a hand. Although most of us do not want to lose fingerprints, there are up to 10 fingerprints to use in case of a bad situation. For example, if you are burned while you are cooking or do not notice getting stuck in the door. In this case, you will be thankful for the Windows Biometric Framework when you have saved up to 10 fingerprints, because you don't have to wait for the saved finger to recover but still have access to your computer.

Fingerprints are added using the Biometric Device, available in the Control Panel of any Windows 7-based computer, with a built-in fingerprint scanner. From there you can start the computer and access the domain. Note that you will have to log in as a new manager to add or manage fingerprints in Windows 7.

BitLocker To Go

One of the most serious security problems businesses face today is the loss of precious mobile phones containing important information. Windows Vista's BitLocker has begun to emphasize this issue by allowing users to encrypt the entire hard drive of our laptop. Therefore, when lost or stolen, no one can access the information stored in it. BitLocker To Go even extends protection to external hard drives.



Integrated in Windows 7 Enterprise and Ultimate editions, BitLocker To Go is easy to use: right-click on the drive and select Turn on BitLocker to open a wizard that has a series of steps to encrypt your drive. Wait until the operation is successful, you have an encrypted drive. The waiting time depends on the speed of the computer and the hard drive. However, the encoding speed will fall to about 20 minutes for a 2GB flash drive.

In addition, BitLocker To Go drives will be decrypted by passwords or for businesses, they can use smart cards with different certifications.

The encrypted drives removed can be created on the Enterprise and Ultimate versions of Windows 7. However, when encrypting a drive, you can read and add data on this drive from any computer. running Windows 7. Additionally, you can install a reader application on an encrypted drive, allowing users to read data from Vista and XP computers.

The extra security feature that can be applied in an enterprise environment through administrator rights can allow users to only store data on the BitLocker To Go drive, just in case users store data on the hard drive. not secure. Windows Server users can also keep recovery passwords in a certificate using Active Directory. Therefore, if the password is lost or forgotten, it can be restored.

AppLocker

Managing installed or running user applications is an effective way to maintain system stability, prevent malware and protect bandwidth-intensive applications like BitTorrent access.

In previous versions of Windows, this was done by the Software Restriction Policies feature. This feature can be applied to prevent certain software from locating the bundle in the file system or causing them to fail when connecting to the password of a trusted application.

Software Restriction Policies can cause a bit of trouble when implementing and maintaining efficiency. Some programs need to be installed outside a specific path, requiring a new path to be created. Although these features provide high security but fail every time a program is updated. Therefore, IT managers need to maintain and update the list of rules and cancel the automatic update function of the program.

AppLocker, available in Windows 7 Enterprise and Ultimate (also included in Windows Server 2008 R2), has a new, flexible method of managing software: publisher rule. Publisher rule is based on the program's profile information, there are many applications in use.

This information is more detailed than the file path or code of the data, allowing the administrator to create complex rules such as allowing the software to be run only from a specific publisher, with a unique name and name. Specific file or a specific version to operate. For example, a rule can allow anything from Adobe to run or only Photoshop or only current versions and future versions of Photoshop.

AppLocker rules can be applied to executable files, scripts, installation programs or system libraries, allowing users the right to install the necessary software or update without administrator rights. while still preventing them from using software that is not allowed to use.

In addition, AppLocker rules can be applied to specific people or groups of users, an accounting group or a graphic design team that uses other specialized software, but with AppLocker, only Some specific rights apply to each group with different restrictions and benefits. AppLocker can also be used to distinguish different users when they share a computer.

The real-time saving feature is the ability to create automatic rules from a trusted computer. Permissions can be shared and applied globally to the network using Windows Group Policy settings.

It is important to note that AppLocker rules only apply to computers running Windows 7 operating systems with Enterprise or Ultimate versions. If some users in the company still use older versions of Windows, you need to install Software Restriction Policies. The more users upgrade to Windows 7, you can sync Software Restriction Policies and rely on the AppLocker feature.

DirectAccess

Advertiseed by Microsoft as the next generation replacement for VPN, DirectAccess allows Windows 7 Enterprise and Windows 7 Ultimate users to connect directly with Windows 2008 R2 and other server generations in the future. While users are familiar with VPN connections, DirectAccess is completely understandable to end users: when the computer is connected to the Internet, DirectAccess automatically creates a secure network for the enterprise network without any action. User's, and automatically routing requests to the internal network through this connection.

In addition, DirectAccess has a number of improvements over traditional VPN connectivity for automatic connection. First, this feature uses IPsec and IPv6 Internet protocols to encrypt and route end to end connections. While VPN encryption is done on the VPN server, DirectAccess can keep encryption during outgoing and incoming connections from the server application within the enterprise network. (DirectAccess supports a number of other protocols to create a link for this connection through a network that does not support IPv6 or IPsec)

Because DirectAccess uses an Internet standard port for traffic, it easily passes through a firewall without additional configuration, something VPN users always face.
Another handy feature of this feature is that, because connections are created and maintained automatically, managers can continuously manage and update machines using DirectAccess, even if the user is not directly using it. source of business.

This means that VPNs need to be censored, scanned before they are allowed to access corporate networks, a process that slows down connections and limits productivity, and only provides IT managers with a Small window during remote access management. With DirectAccess, computers are updated at the same time as the rest of the corporate network and are managed whenever users want to access the corporate network.

However, you must be aware that not all businesses can immediately switch to using DirectAccess. The system relies on high-end network infrastructure - including Windows Server 2008 R2 and IPv6 - which some businesses haven't upgraded yet, it will take a few years before there are enough tools and techniques to have. can completely switch to using DirectAccess. So, in the meantime, you can use a traditional VPN connection.

However, this feature still offers an outline for the future network, security, always connecting to data when allowing remote connections can work as if they are sitting at the main office.

For businesses, Windows 7 helps companies establish collaboration between the IT security department and end users, allowing employees to work while still applying security and updates from the network. All of these sharing features are like an easy-to-use contract, cost-free for security and very convenient for businesses.