

Windows 7 Security *Deep Dive*



Key New Security Features and How to Use Them



An expert's guide to Windows 7 security

How to configure the new Windows operating system to beat malware and keep data secure

By Roger A. Grimes

WINDOWS 7 has been warmly received and swiftly adopted by businesses, with the result that many IT admins are now struggling with the platform's new security features. In addition to changes to User Account Control, BitLocker, and other features inherited from Windows Vista, Windows 7 introduces a slew of new security capabilities that businesses will want to take advantage of.

Windows 7 improves on Vista with a friendlier UAC mechanism, the ability to encrypt removable media as well as hard drive volumes, broader support for strong cryptographic ciphers, hassle-free secure remote access, and sophisticated protection against Trojan malware in the form of AppLocker, to name just a few.

In this guide, I'll run through these and other significant security enhancements in Windows 7, and provide my recommendations for configuring and using them. I'll pay especially close attention to the new AppLocker application-control feature, which may be a Windows shop's most practical and affordable way to combat socially engineered Trojan malware.

NEW AND IMPROVED

Windows 7 has literally hundreds of security changes and additions, far too many to cover in one fell swoop. While this guide focuses on the ones that most organizations will be interested in, keep in mind that plenty of others may deserve your attention. A few the biggies not discussed here are built-in support for smart cards and biometrics, the ability to force the use of Kerberos in a feature called [Restrict NTLM](#), and support for the new [DNSSec standards](#), which are becoming essential to prevent DNS exploitation attacks. Also noteworthy is a new feature called [Extended Protection for Authentication](#),

which prevents many sophisticated man-in-the-middle attacks that can strike at some of our most trusted security protocols (such as SSL and TLS).

USER ACCOUNT CONTROL

A Windows Vista feature that users loved to hate, [User Account Control](#) has been significantly improved to be both less intrusive and smarter at distinguishing between legitimate and potentially malicious activities in Windows 7. However, depending on whether you are logged on as administrator or a standard user, some installs of Windows 7 may have a default UAC security setting that's one level lower than some experts (including yours truly) recommend. Standard users have UAC security default to the most secure setting, while administrator accounts reside a notch below the highest setting, which is potentially more risky.

Note too that, although UAC provides a much-needed mechanism to prevent the misuse of administrator privileges, it can be bypassed. If you need high security, users should not log on with an elevated user account until they need it.

Your domain environment should already be at the highest and most secure level ("Always notify"). If it isn't, make it so. That way, users will be prompted to input their passwords to perform high-risk administrative actions. No matter what else, UAC should be enabled.

BITLOCKER DRIVE ENCRYPTION

In Windows 7, [BitLocker Drive Encryption technology](#) is extended from OS drives and fixed data drives to include removable storage devices such as portable hard drives and USB flash drives. This new capability is called BitLocker to Go.

In Windows Vista SP1, Microsoft added official support



for encrypting fixed data drives, but it could only be done using command-line tools. Now you can encrypt operating system volumes, fixed data drives, and USB flash drives with a simple right-click, via the Windows Explorer GUI. Moreover, you can use smart cards to protect data volumes, and you can set up data recovery agents to automatically back up BitLocker keys. If you're using a Trusted Platform Module (TPM) chip, you can enforce a minimum PIN length; five characters should suffice for most environments.

In Windows 7, there is no need to create separate partitions before turning on BitLocker. The system partition is automatically created and does not have a drive letter, so it is not visible in Windows Explorer and data files will not be written to it inadvertently. The system partition is smaller in Windows 7 than in Windows Vista, requiring only 100MB of space.

With BitLocker to go, you can encrypt removable drives one at a time or require that all removable media be encrypted by default. Further, encrypted removable media can be decrypted and re-encrypted on any Windows 7 computers – not just the one it was originally encrypted on.

BitLocker to Go Reader (bitlockertogo.exe) is a program that works on computers running Windows Vista or Windows XP, allowing you to open and view the content of removable drives that have been encrypted with BitLocker in Windows 7.

You should enable BitLocker (preferably with TPM and another factor) on portable computers if you do not use another data encryption product. Store the BitLocker PINs and recovery information in Active Directory or configure a domain-wide public key called a data recovery agent that will permit an administrator to unlock any drive encrypted with BitLocker. Require BitLocker to Go on all possible removable media drives.

EASILY ENCRYPTED PAGE FILE

Users who cannot utilize BitLocker but still want to prevent the memory swap page file from being analyzed in an offline sector editing attack no longer need to erase the page file on shutdown. Windows XP and earlier versions had a setting that allowed the page file to be erased on shutdown and rebuilt on each startup. It's a great security feature, but it often caused delayed shutdowns and startups – sometimes adding as much as 10 minutes to the process.

In Windows 7 (and Vista), you can enable page file encryption. Even better: There is no key management. Windows creates and deletes the encryption keys as needed, so there is no chance the user can "lose" the key or require a recovery. It's crypto security at its best.

BETTER CRYPTOGRAPHY

Windows 7 includes all the latest industry-accepted ciphers, including AES (Advanced Encryption Standard), ECC (Elliptical Curve Cryptography), and the SHA-2 hash family. In fact, Windows 7 implements all of the ciphers in [Suite B](#), a group of cryptographic algorithms that are approved by the National Security Agency and National Institute of Standards and Technology for use in general-purpose encryption software.

While Microsoft added support for Suite B cryptographic algorithms (AES, ECDSA, ECDH, SHA2) to Windows Vista, Windows 7 allows Suite B ciphers to be used with Transport Layer Security (referred to as TLS v.1.2) and Encrypting File System (EFS). Suite B ciphers should be used whenever possible. However, it's important to note that Suite B ciphers are not usually compatible with versions of Windows prior to Windows Vista.

By default, all current technologies in Windows will use industry standard ciphers. No more legacy, proprietary ciphers are used. Those legacy ciphers that still exist are included only for backward-compatibility purposes. Microsoft has shared the new ciphers in detail with the crypto world for analysis and evaluation. Key and hash sizes are increased by default.

EFS (Encrypting File System) has been improved in many ways beyond using more modern ciphers. For one, you can use a smart card to protect your EFS keys. This not only makes EFS keys more secure, but allows them to be portable between computers.

Administrators will be happy to know that they can prevent users from creating self-signed EFS keys. Previously, users could easily turn on EFS, which generated a self-signed EFS digital certificate if a compatible PKI server could not be found. Too often, these users encrypted files but did not back up their self-signed digital certificates, which frequently led to unrecoverable data loss.

With Windows 7, administrators can still allow self-signed EFS keys, while mandating ciphers and minimum key lengths. Windows 7 will prod users to back up their



EFS digital certificates to some other removable media or network drive share – and keep prodding them until they do it. A Microsoft Web page [details the EFS changes](#).

SAFER BROWSING WITH IE 8

Users don't need Windows 7 to run IE 8, and if they're running an older version of IE on an older operating system, they should upgrade to IE 8 as soon as possible. Even better, from a security standpoint, is running IE 8 on Windows 7.

Not only is IE 8 more secure by default than previous versions of the browser, but IE 8 is more secure on Windows 7 than on Windows XP. The recent [Chinese Google zero-day hacking attack](#) demonstrates this more effectively than anything I could come up with. The Chinese attacks work most effectively on IE 6 and not very well on IE 8. See the [relative risk ratings](#). Microsoft tested a number of related exploits and found that they were significantly harder to accomplish in IE 8, and harder still in IE 8 on Windows 7.

Naturally, application and Web site compatibility issues will guide how quickly Windows shops can move to the new browser. But run some tests. I have no shortage of clients who are still clinging to IE 6 and haven't done compatibility testing in over a year. Often when I goad them into retesting their troublesome application with IE 8, it works.

MULTIPLE ACTIVE FIREWALL POLICIES

Prior to Windows 7, when a user had multiple network interfaces active, only one Windows Firewall profile (i.e. Home, Domain, Work, or Public) could be used. This created potential security vulnerabilities, such as when a computer was both wired to the local network domain and connected to a less restricted wireless network. Windows 7 can now detect multiple networks and apply the appropriate firewall profile to the right interface.

IMPROVED SYSTEM RESTORE

System Restore now includes user's personal content files. Older versions backed up and protected only the Windows system files. System Restore also allows you to see what files would be restored in each version of the System Restore files. It's not perfect, but it's nice to see what will occur if you were to choose a particular restoration point.

SMOOTH REMOTE ACCESS

[DirectAccess](#) allows remote users to securely access enterprise resources (such as shares, Web sites, applications, and so on) without connecting to traditional types of VPNs. DirectAccess establishes bi-directional connectivity with a user's enterprise network every time a user's DirectAccess-enabled portable computer connects to the Internet, even before the user logs on. The advantage here is that users never have to think about connecting to the enterprise network, and IT administrators can manage remote computers even when the computers are not connected to the VPN.

Once DirectAccess is enabled, when a user's computer connects to the Internet, it's as though he or she is on the organization's local network. Group policies work, remote management tools work, and automatic push patching works.

Unfortunately, DirectAccess has fairly involved requirements, including Windows Server 2008 R2 (to act as the RAS server), Windows 7 Enterprise or Ultimate clients, PKI, IPv6, and IPSec. But [as companies put the necessary pieces into place](#), they should look into using DirectAccess as their default VPN technology for Windows 7 and later clients.

MANAGED SERVICE ACCOUNTS

Service accounts are often highly privileged, but difficult to manage. Best-practice recommendations dictate changing service account passwords frequently, so as to avoid the risk of password attacks. However, Windows service accounts often require two or more coordinated, synchronized password changes in order for the service to continue running without interruption; prior to Windows 7 and Windows Server 2008 R2, service accounts were not easy to manage. If a service account is enabled as a [Managed Service Account](#), Windows will take over the password management and simplify management of Kerberos SPN (Service Principal Names).

Like DirectAccess, Managed Service Accounts have a lot of requirements, including a schema update and mandatory use of PowerShell 2. Still, if service accounts are a hassle in your environment – and you know they are – consider enabling this new feature when your infrastructure is prepared.

VIRTUAL SERVICE ACCOUNTS

[Virtual Service Accounts](#) (VSAs) are related to Managed



Service Accounts in that Windows takes over the password management. However, VSAs are for local service accounts and don't require a schema update or nearly the amount of effort to configure and use.

When a VSA controls a service, the service accesses the network with the computer's identity (in a domain environment), which is much like what the built-in LocalSystem and Network Service accounts do, except that VSAs allow each service to have its own separate security domain (and corresponding isolation).

Creating a Virtual Service Account is pretty easy. Open the Services console (services.msc) and modify the service's logon account name to be the same as the service's short name, such as ex. NT SERVICE\ServiceName\$. Then restart the service. That's it.

When the infrastructure can support it, consider using Managed and Virtual Service Accounts functionality to manage service account password security.

APPLOCKER APPLICATION CONTROL

The leading cause of malware infections may surprise you. Most machines aren't exploited due to missing patches (although this is the second biggest cause), or unpatched zero days (almost never a factor), or drive-by downloads, or misconfigurations. Nope, most systems are infected because users are duped into intentionally installing programs that a Web site or e-mail says they need. These socially engineered Trojans come in the guise of anti-virus scanners, codecs required for a media player, fake patches, and just about any other bait the bad guys can concoct to lure end-users into installing their Trojan executable.

The most effective means of thwarting these threats in an enterprise environment is preventing end-users from installing unapproved programs. If you leave the decision up to end-users, they will almost always make the wrong choice. If they didn't, malware wouldn't be nearly as common as it is today.

Microsoft's most sophisticated solution to the problem is AppLocker, an application-control feature included in Windows 7 (Ultimate and Enterprise editions) and Windows Server 2008 R2. AppLocker is an improvement on the Software Restriction Policies (SRP) introduced with Windows XP Professional. AppLocker allows you to define application execution rules and

exceptions based on file attributes such as path, publisher, product name, file name, file version, and so on. You can then assign policies to computers, users, security groups, and organizational units via Active Directory.

CONFIGURING APPLOCKER

You can configure AppLocker locally using the Local Computer Policy object (gpedit.msc) or via Active Directory and Group Policy Objects (GPOs). AppLocker relies on the built-in Application Identity service, which is normally set to manual startup type by default. Administrators should configure the service to start automatically.

Within the local or group policy object, AppLocker is enabled and configured under the \Computer Configuration\Windows Settings\Security Settings\Application Control Policies container.

By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. First-time testers will benefit by allowing AppLocker to create a default set of "safe rules" using the Create Default Rules option. The default rules allow all files in Windows and Program Files to run, along with allowing members of the Administrators group to run anything.

One of the most notable improvements over SRP is the ability to run AppLocker against any computer using the Automatically Generate Rules option to quickly create a baseline set of rules. In a few minutes, dozens to hundreds of rules can be produced against a known clean image, saving administrators anywhere from hours to days of work.

RUNNING BY THE RULES

AppLocker supports four types of rule collections: Executable, DLL, Windows Installer, and Script. SRP administrators will notice that Microsoft no longer has the registry rules or Internet zones options. Each rule collection covers a limited set of file types. For example, executable rules cover 32-bit and 64-bit .EXEs and .COMs; all 16-bit applications can be blocked by preventing the ntdvm.exe process from executing. Script rules cover .VBS, .JS, .PS1, .CMD, and .BAT file types. The DLL rule collection covers .DLLs (including statically linked libraries) and OCXs.

If no AppLocker rules for a specific rule collection exist, all files that share the same format are permitted



to run. However, once a rule for a specific collection is created, only the files explicitly allowed in the rule can execute. For example, if you create an executable rule that allows .EXE files in %SystemDrive%\FilePath to run, only executable files located in that path are allowed to run.


AppLocker supports three types of rule conditions for each rule collection: Path Rules, File Hash Rules, and Publisher Rules. Any rule condition can be used to allow or deny execution, and it can be defined for a particular user or group. Path and File hash rules are self-explanatory; both accept wild card symbols. The Publisher rules are fairly flexible and allow several fields of any digitally signed file to be matched with specific values or wild cards. By using a convenient slider bar in the AppLocker GUI, you can quickly replace the specific values with wild cards. Each new rule conveniently allows one or more exceptions to be made. By default, Publisher rules will treat updated versions of files the same as the originals, or you can enforce an exact match.

RULES FOR EXCEPTIONS

If you need to make a rule for a file type that is not defined in AppLocker's policy table, you'll need to use some creativity to get the desired effect. For example, to prevent Perl script files with the .PL extension from executing, you would have to create an executable rule that blocked the Perl.exe script interpreter instead. This would block or allow all Perl scripts and require some

resourcefulness to gain finer-grained control. This is not a unique issue, as many other application control products have the same sort of limitation.

AppLocker's configuration and rules can easily be imported and exported as readable XML files. Plus, the rules can be quickly cleared in an emergency, and everything can be managed using Windows PowerShell. Reporting and alerting are limited to what can be pulled from the normal event logs. But even with the limitations, AppLocker gives up-to-date Microsoft shops an effective way to prevent users' missteps from compromising their machines – not to mention the company network.

Software makers routinely sacrifice some security for the sake of usability, and Microsoft is no exception. I've built a career on teaching people how to harden Microsoft Windows over its default state. But with Windows 7, most of that old advice is no longer necessary. Microsoft now delivers a product that is significantly more secure out of the box. Administrators don't have to download NSA security templates or modify the system in any way to make users fairly secure from the start. In most cases, they simply need to know what security capabilities Microsoft provides, and how to put them to work. 

Roger A. Grimes (CPA, CISSP) is senior contributing editor and Security Advisor columnist at InfoWorld. A 23-year Windows security consultant, instructor, and author, he currently works full-time for Microsoft, where he serves as principal security architect for the Microsoft InfoSec ACE Team.