

By Debra Littlejohn Shinder, MCSE, MVP

One of Microsoft's goals in creating Windows XP was to make a more secure operating system. Unfortunately, because security and functionality are often at odds, XP out of the box is not as secure as it can be. You can make your Windows XP computer more secure by tweaking a few registry settings—but as always, take care when editing the registry. An incorrect modification could render your system unusable. We recommend that you back up the registry before trying these edits.

1 Disable hidden administrative shares

Even if you haven't shared any of your files or folders, an administrator (or anyone who knows a valid username and password for an account you've given administrative privileges) can remotely access your data by using the hidden administrative shares that XP creates by default. There is an administrative share for every drive on your system, but it doesn't show up in the network browse list (My Network Places) because it has been marked as hidden by appending a dollar sign (\$) to the end of the drive letter. You can delete these shares, but XP will just grow them back the next time you reboot. To prevent this, disable administrative shares by performing the following registry edit:

1. In your registry editor, navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanager\parameters`.
2. In an empty portion of the right details pane, right-click and select New | DWORD Value.
3. Rename the new value `AutoShareWks`.
4. Double-click the new value and enter 0 in the Value Data field.

2 Don't show the last logon name

If you've elected to use the standard logon dialog box instead of the Welcome screen, or if the XP computer is joined to a domain, XP tries to be helpful by displaying the account name of the last user who logged onto the computer; you only have to type in the password. However, this is a security issue because it gives a hacker half of the information needed to log on. Why make it easier? Of course, you should already have renamed the administrator account and disabled the guest account so a hacker won't have those account names to use. The next step is to disable the display of the last logged-on user. Here's how:

1. In your registry editor, navigate to: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.
2. In an empty portion of the right details pane, right-click and select New | DWORD Value.
3. Rename the new value `dontdisplaylastusername`.
4. Double-click the new value and enter 1 in the Value Data field.

3 Control what applications a user can run

If you're sharing an XP computer with someone else and you're the administrator, you can restrict the other user(s) to running only applications you specify. This can be particularly useful when sharing the computer with a young family member or if your computer must be used by guests. Here's the procedure:

1. In your registry editor, logged on with the account you want to restrict, navigate to: `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`.
2. In an empty portion of the right details pane, right-click and select New | DWORD Value.

3. Rename the new value to **RestrictRun**.
4. Double-click the new value and enter 1 in the Value Data field. (You can modify this to allow all applications to run by changing the value to 0).
5. Create a new subkey named **RestrictRun**.
6. Create a new string value for each application you want to allow. Name each string value as a consecutive number.
7. Set the Value Data for each string value as the name of an application you want to allow (this should be the executable program name, such as `explore.exe` for Windows Explorer).
8. Reboot the computer to apply the change.

Warning

Don't apply this policy to yourself or you may not be able to run the programs you need to in order to administer the computer—and if you can't run the registry editor, you won't be able to change the policy.

4 Disable saved password for dialup networking

It's handy for users not to have to enter their passwords each time they start a dialup networking session, but it can also be a security risk to have Windows save the password, since anyone else can start a session, too. To disable the saved password function for DUN, do the following:

1. In your registry editor, navigate to:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters`.
2. If the entry `DisableSavePassword` doesn't already exist, right-click in an empty portion of the right details pane and select New | DWORD Value.
3. Rename the new value to `DisableSavePassword`.
4. Double-click the new value (or if it already existed, just double-click it now) and enter 1 in the Value Data field to prevent Windows from saving the DUN password. If you want to enable saving of passwords later, you can do so by setting the value to 0.

5 Prevent access to specific drives

You can prevent users from viewing and accessing the files and folders on specific drives using Windows Explorer, My Computer, or the Run command. They will not be able to map a network drive or use the DIR command to get a list of directories on the drive. This is a good way to add a layer of protection to a drive on which you store sensitive data. (You should also use access controls/permissions and encrypt the data if it's extremely sensitive.)

1. In your registry editor, logged on with the user account you want to restrict, navigate to:
`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`.
2. Right-click in an empty portion of the right details pane and select New | DWORD Value.
3. Rename the new value `NoViewOnDrive`.
4. Double-click the value and set the view to Decimal. In the Value Data field, add the following number(s) to hide the corresponding drive(s): A: 1, B: 2, C: 4, D:8, E:16, F: 32, G: 64, H:128, I: 256, J: 512, K: 1024, L: 2048, and so on, multiplying by 2 to get the next numbers for the rest of the alphabet.

6 Delete contents of the page file when you shut down

The XP page file contains information written from memory to the hard disk. If sensitive data is contained there, someone may be able to retrieve it. For better security, you can force XP to delete all the data from the page file each time you shut down the computer. (Note that this may cause shutdown to take longer if you have a large page file.)

1. In your registry editor, navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management.
2. If the entry **ClearPageFileAtShutdown** doesn't exist, right-click in an empty portion of the right details pane and select **New | DWORD Value**.
3. Rename the new value to **ClearPageFileAtShutdown**.
4. Double-click the new value (or if it already existed, just double-click it now) and enter 1 in the Value Data field.
5. Restart the computer to make the change take effect.

7 Disable access to System properties

Using the System properties applet in Control Panel, a user can change the name and/or domain membership of the computer, create hardware profiles, manage devices, and specify performance parameters such as memory usage, virtual memory settings, and visual effects. This registry edit allows you to disable access to System properties, both from Control Panel and My Computer/Computer Management.

1. In your registry editor, logged on as the user for whom you want to restrict access, navigate to:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer.
2. Right-click in an empty portion of the right details pane and select **New | DWORD Value**.
3. Rename the new value to **NoPropertiesMyComputer**.
4. Double-click the new value and enter 1 in the Data Value field to hide the properties. If you want to make the properties accessible later, change the value to 0.
5. Restart the computer to make the change take effect.

8 Prevent Windows from storing an LM Hash of your password

Windows stores your password in the local Security Accounts Manager (SAM) database as a "hash value," which is generated from the password using a hash algorithm. This is more secure than storing the password in plain text. However, by default, Windows creates two different hashes, an LM (Lan Manager) hash and an NT hash. The LM hash is not as strong and can be cracked. Early versions of Windows need the LM hash because they don't use Kerberos. If you won't be connecting to computers running operating systems prior to Windows 2000, you can disable the creation of the LM hash for better security.

1. In your registry editor, navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
2. Right-click in an empty portion of the right details pane and select **New | DWORD Value**.
3. Rename the new value **NoLMHash**.
4. Double-click the new value and enter 1 in the Data Value field.
5. Restart the computer to make the change take effect.
6. Change your password. (The old one will still have an LM hash for it stored in the SAM.)

9 Prevent null sessions

Null sessions allow connection of an anonymous user and no password on the NetBIOS port. This can be exploited by a hacker. NetBIOS is used for file and print sharing. If you need the NetBIOS service but don't want to allow Null sessions, you can edit the registry.

1. In your registry editor, navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa**.
2. Double-click the value **RestrictAnonymous**. (If it does not exist, create it as a DWORD Value.)
3. In the Data Value field, enter 2 to block all null sessions or 1 to allow null sessions but block sensitive data from being sent via the null session.

10 Hide the Security tab

When simple file sharing is disabled on Windows XP, you can use the Security tab on a folder or file's properties sheet to set permissions to control who can access the folder or file and what level of access each user or group has. If you don't want other users to be able to change permissions, you can edit the registry to hide the Security tab so they can't access this dialog box. Here's how:

1. In your registry editor, logged on with the user account from which you want to hide the Security tab, navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
2. Double-click the value **NoSecurityTab**. (If it doesn't exist, create it as a DWORD value.) In the Data Value field, enter 1 to hide the tab. If you want to give the user access to it later, you can change the value to 0.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- "[Configuring Windows XP security after you install Service Pack 2](#)" (TechRepublic download)
- "[Master the Windows XP Registry](#)" (TechRepublic download)
- "[Windows XP services that can be disabled](#)" (TechRepublic download)

Version history

Version: 1.0

Published: November 29, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team