

WINDOWS XP BASELINE SECURITY CHECKLISTS

WINDOWS XP HOME EDITION CONFIGURATION CHECKLIST DETAILS

VERIFY THAT ALL DISK PARTITIONS ARE FORMATTED WITH NTFS

NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your computer are formatted using NTFS. If necessary, use the Convert utility to non-destructively convert your FAT partitions to NTFS.

PROTECT FILE SHARES

Windows XP Home Edition uses a network access model called "Simple File Sharing," where all attempts to log on to the computer from across the network will be forced to use the Guest account. This means that network access through Server Message Block (SMB, used for file and print access), as well as Remote Procedure Call (RPC, used by most remote management tools and remote registry access) will be available only to the Guest account.

In the Simple File Sharing model, file shares can be created so that access from the network is read-only or access from the network is able to read, create, change, and delete files. Simple File Sharing is intended for use on a home network and behind a firewall, such as the one provided by Windows XP. If you are connected to the Internet, and are not operating behind a firewall, you should remember that any file shares you create might be accessible to any user on the Internet.

USE INTERNET CONNECTION SHARING (ICS) FOR SHARED INTERNET CONNECTIONS

Windows XP provides the ability to share a single Internet connection with multiple computers on a home or small business network through the ICS feature. One computer, called the ICS host, connects directly to the Internet and shares its connection with the rest of the computers on the network. The client computers rely on the ICS host computer to provide access to the Internet. Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet.

To enable ICS, right-click an Internet connection in Network Connections, click **Properties**, click the **Advanced** tab, and then select the appropriate check box. You can also configure ICS by using the Home Networking Wizard. For more information about ICS, see Help and Support Center in Windows XP.

ENABLE INTERNET CONNECTION FIREWALL (ICF)

Designed for use in the home or small business, Internet Connection Firewall (ICF) provides protection for Windows XP computers that are directly connected to the Internet, or for the computers or devices connected to the Internet Connection Sharing host computer that is running ICF. The Windows XP ICF makes use of stateful

packet filtering, which means incoming traffic accessing new ports is allowed only if it matches previously established outbound sessions initiated by the user.

To enable ICF, right-click an Internet connection in Network Connections, click **Properties**, click the **Advanced** tab, and then select the appropriate check box. You can also configure ICF by using the Home Networking Wizard. For more information about ICF, see Help and Support Center in Windows XP.

USE ACCOUNT PASSWORDS

Passwords should be assigned to individual accounts on Windows XP Home Edition computers that are accessed by multiple people who want to protect their data from one another. Windows XP home users get separate but accessible file storage by default, with optional password protection. When you create a password for yourself, Windows offers to lock down your "My Documents" folder, as well as any subfolders. That way, if you have a password and want privacy, you will be protected from other non-administrator users of the computer. Assigning account passwords will also prevent anyone from simply walking up to the computer and using it.

USE THE MAKE PRIVATE FEATURE

In the simple file sharing model, Windows does not directly expose the complexity of managing file access control lists to the user. Instead, the user interface features an option called "make private" that, when selected for a folder, will modify the underlying access control for that folder so that other non-administrative users cannot access it. This feature works only if the file system is NTFS.

INSTALL ANTIVIRUS SOFTWARE AND UPDATES

One of the most important things for protecting systems is to use antivirus software and ensure that it is kept up-to-date. All systems on the Internet, a corporate Intranet, or a home network should have antivirus software installed.

KEEP UP-TO-DATE ON THE LATEST SECURITY UPDATES

The Auto Update feature in Windows XP can automatically detect and download the latest security fixes from Microsoft. Auto Update can be configured to automatically download fixes in the background and then prompt the user to install them once the download is complete.

To configure Auto Update, click **System** in Control Panel and select the **Automatic Updates** tab. Choose the first notification setting to download the updates automatically and receive notification when they are ready to be installed.

Additionally, Microsoft issues security bulletins through its [Security Notification Service](#). These bulletins are issued for any Microsoft product that is found to have a security issue. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your computers.

WINDOWS XP PROFESSIONAL CONFIGURATION CHECKLIST DETAILS

VERIFY THAT ALL DISK PARTITIONS ARE FORMATTED WITH NTFS

NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your computer are formatted using NTFS. If necessary, use the Convert utility to non-destructively convert your FAT partitions to NTFS.

PROTECT FILE SHARES

By default, Windows XP Professional systems that are not connected to a domain use a network access model called "Simple File Sharing," in which all attempts to log on to the computer from across the network will be forced to use the Guest account. This means that network access through Server Message Block (SMB, used for file and print access), as well as Remote Procedure Call (RPC, used by most remote management tools and remote registry access) will be available only to the Guest account.

In the Simple File Sharing model, file shares can be created so that access from the network is read-only or access from the network is able to read, create, change, and delete files. Simple File Sharing is intended for use on a home network and behind a firewall, such as the one provided by Windows XP. If you are connected to the Internet, and are not operating behind a firewall, you should remember that any file shares you create might be accessible to any user on the Internet.

The Classic security model is used if your Windows XP Professional computer is joined to a domain or if Simple File Sharing is disabled. In the Classic security model, users who attempt to log on to the local computer from across the network must authenticate as themselves and are not mapped to the Guest account. File shares should be created so that access from the network is granted only to the appropriate groups and/or individual users.

USE INTERNET CONNECTION SHARING (ICS) FOR SHARED INTERNET CONNECTIONS

Windows XP provides the ability to share a single Internet connection with multiple computers on a home or small business network through the ICS feature. One computer, called the ICS host, connects directly to the Internet and shares its connection with the rest of the computers on the network. The client computers rely on the ICS host computer to provide access to the Internet. Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet.

To enable ICS, right-click an Internet connection in Network Connections, click **Properties**, click the **Advanced** tab, and then select the appropriate check box. You can also configure ICS by using the Home Networking Wizard. For more information about ICS, see Help and Support Center in Windows XP.

ENABLE INTERNET CONNECTION FIREWALL (ICF)

Designed for use in the home or small business, ICF provides protection for Windows XP computers that are directly connected to the Internet or for the computers or devices connected to the Internet Connection Sharing host computer that is running ICF. The Windows XP ICF makes use of stateful packet filtering, which means incoming traffic accessing new ports is only allowed if it matches previously established outbound sessions initiated by the user.

To enable ICF, right-click an Internet connection in Network Connections, click **Properties**, click the **Advanced** tab, and then select the appropriate check box. You can also configure ICF by using the Home Networking Wizard. For more information about ICF, see Help and Support Center in Windows XP.

USE SOFTWARE RESTRICTION POLICIES

Software restriction policies provide administrators with a policy-driven mechanism that identifies software running in their domain and controls the ability of that software to run. Using a software restriction policy, an administrator can prevent unwanted programs from running, such as viruses and Trojan horses or other software that is known to cause conflicts when installed. Software-restriction policies can be used on a standalone computer by configuring the local security policy. Software restriction policies also integrate with Group Policy and Active Directory.

USE ACCOUNT PASSWORDS

To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can be used only to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network or for any other logon activity except at the main physical console logon screen. For example, you cannot use the secondary logon service (RunAs) to start a program as a local user with a blank password.

Assigning a password to a local account removes the restriction that prevents logging on over a network. It also permits that account to access any resources it is authorized to access, even over a network connection. As a result, it is better to leave a blank password assigned to an account rather than assigning a weak, easily guessed password. When assigning account passwords, make sure the password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character within the first seven characters.

CAUTION:

If your computer is not in a physically secured location, it is recommended that you assign passwords to all local user accounts. Failure to do so allows anyone with physical access to the computer to easily log on by using an account that does not have a password. This is especially important for portable computers, which should always have strong passwords on all local user accounts. **Note:** This restriction does not apply to domain accounts. It also does not apply to the local Guest account. If the Guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the Guest account.

If you want to disable the restriction against logging on to the network without a password, you can do so through Local Security Policy.

DISABLE UNNECESSARY SERVICES

After installing Windows XP, you should disable any network services not required for the computer. In particular, you should consider whether your computer needs any IIS Web services. By default, IIS is not installed as part of Windows XP and should be installed only if its services are specifically required.

DISABLE OR DELETE UNNECESSARY ACCOUNTS

You should review the list of active accounts (for both users and programs) on the system in the Computer Management snap-in. Disable any non-active accounts and delete any accounts that are no longer required.

MAKE SURE THE GUEST ACCOUNT IS DISABLED

This setting recommendation applies only to Windows XP Professional computers that belong to a domain or to computers that do not use the Simple File Sharing model.

On Windows XP Professional systems that are not connected to a domain, users who attempt to log on from across the network will be forced to use the Guest account by default. This change is designed to prevent hackers attempting to access a system across the Internet from logging on by using a local Administrator account that has no password. To use this feature, which is part of the Simple File Sharing model, the Guest account must be enabled on all Windows XP computers that are not joined to a domain. For those computers that are joined to a domain, or for unjoined computers that have turned off the Simple File Sharing model, the Guest account should be disabled. This will prevent users attempting to log on to the computer from across the network from using the Guest account.

SET STRONGER PASSWORD POLICIES

To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can be used only to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network or for any other logon activity except at the main physical console logon screen.

NOTE:

This restriction does not apply to domain accounts. It also does not apply to the local Guest account. If the Guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the Guest account.

Use the Local Security Policy snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

Set the minimum password length to at least eight characters.

Set a minimum password age appropriate to your network (typically between 1 and 7 days).

Set a maximum password age appropriate to your network (typically no more than 42 days).

Set a password history maintenance (using the "Remember passwords" radio button) of at least six.

SET ACCOUNT LOCKOUT POLICY

Windows XP Professional includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For example, enable local account lockout after 5-10 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)." If that's too aggressive, consider permitting the account to automatically unlock after a certain period of time.

There are two common goals for using account lockout: one is to make it obvious that multiple attempts have been made to log on to a user account with an invalid password; the second is to protect accounts from attempts to guess a password by dictionary attacks or iterative guessing. There is no one correct setting here that will apply to all environments. Consider reasonable settings for your environment.

INSTALL ANTIVIRUS SOFTWARE AND UPDATES

One of the most important things for protecting systems is to use antivirus software and ensure that it is kept up-to-date. All systems on the Internet, a corporate Intranet, or a home network should have antivirus software installed.

KEEP UP-TO-DATE ON THE LATEST SECURITY UPDATES

The Auto Update feature in Windows XP can automatically detect and download the latest security fixes from Microsoft. Auto Update can be configured to automatically download fixes in the background and then prompt the user to install them once the download is complete.

To configure Auto Update, click **System** in Control Panel and select the **Automatic Updates** tab. Choose the first notification setting to download the updates automatically and receive notification when they are ready to be installed.

Additionally, Microsoft issues security bulletins through its [Security Notification Service](#). These bulletins are issued for any Microsoft product that is found to have a security issue. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your computers.