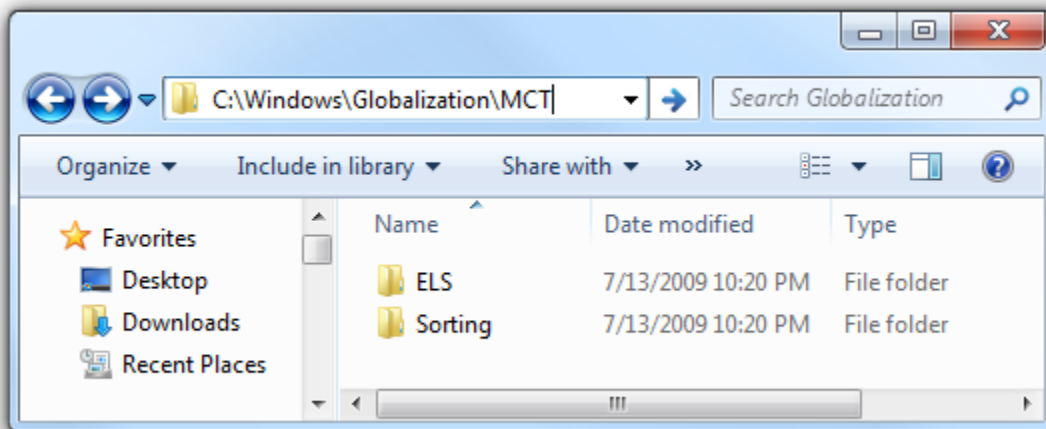


Unlock Hidden Windows 7 Themes

There are a number of regional themes with multiple unique background images hidden from Windows 7 users. On a Windows 7 install with United States regional settings only the United States theme is shown but there are actually four more themes hidden from view. Below are all the regional themes included in Windows 7:



Accessing all the themes is easy to do once you know where to find them. The trick is to navigate to the C:\Windows\Globalization\MCT directory. The MCT directory within the Globalization directory is super hidden so it will not display even if show hidden files and folders is enabled. Just click on the address bar of any folder and manually type in or copy and paste in C:\Windows\Globalization\MCT and hit Enter.



Once you have reached the MCT folder you will see five directories as listed below:

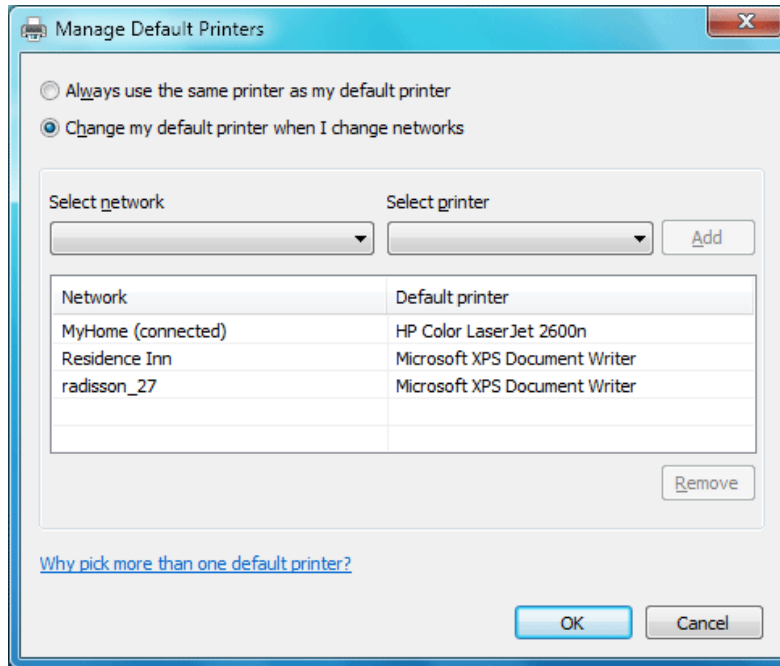
- MCT-AU
- MCT-CA
- MCT-GB
- MCT-US
- MCT-ZA

To view and use the theme for each region just navigate into each MCT-Region directory, enter the Theme sub-directory and double click the theme file.

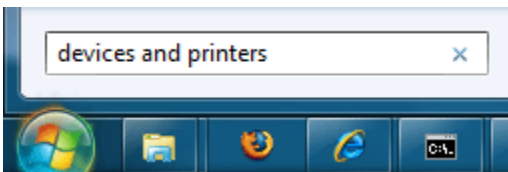
Automatic Hidden Windows 7 Themes

One of the most useful features of Windows 7 for [business laptop](#) users is automatic default printer switching based on location. In past versions of Windows it was only possible to have one default printer. In Windows 7, you can set default printers based on location. For example, when you are at work your default printer is set to the big multi-function network printer but when you go home your default printer is automatically switched to your local ink jet printer.

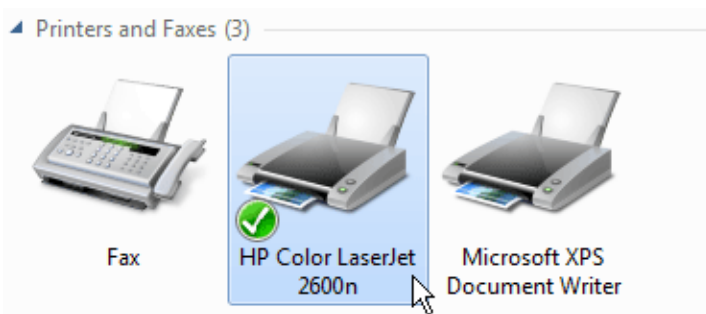
Automatic default printer switching monitors your computer for network connection changes and uses its [database](#) of printers to switch your printer. Printers and their corresponding network have to manually configured on the Manage default printers screen:



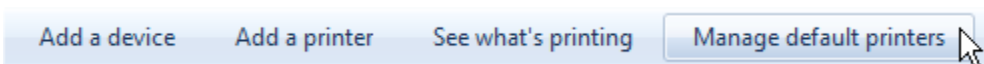
To configure automatic printer click on the Start Menu and type in Devices and Printers and hit Enter



Then, select one of your printers with your mouse.



Click the Manage default printers button on the toolbar.



Make sure Change my default printer when I change networks is selected. Then, select the network from the drop down list and then select the printer you want to use on that connection. When finished hit Add.

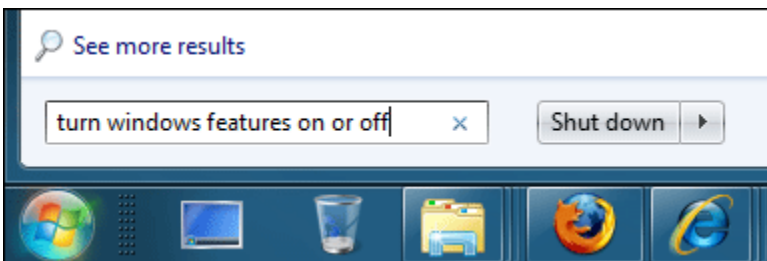
When you have finished setting up all of your default printers click OK to save your changes

How to Remove Internet Explorer from Windows 7

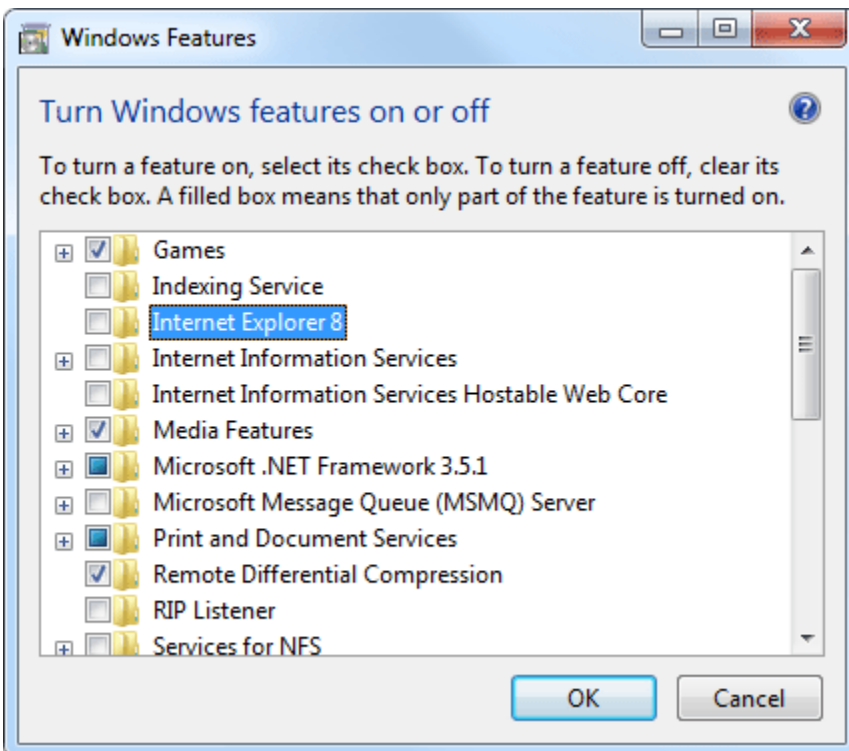
For the first time since 1997 it is possible to uninstall Internet Explorer from Windows. Now full time Firefox, Chrome and Opera users can remove Internet Explorer for good. Best of all, removing IE will not break any of the thousands of [applications](#) that depend on the Internet Explorer rendering engine. Over the years many applications including AOL Instant Messenger, MSN Messenger, Windows Media Player, Google Talk, LimeWire, MS Office and more use components of the IE rendering engine. When Internet Explorer is removed the shared rendering engine components will remain to make sure the thousands of applications that depend on the IE rendering engine continue to run.

While the rendering engine will remain for [compatibility](#) reasons the IE executables, shortcuts and settings will be removed. To uninstall IE on your computer, follow these steps:

[Click](#) on the Start Button and type in **Turn Windows features on or off** and hit Enter.



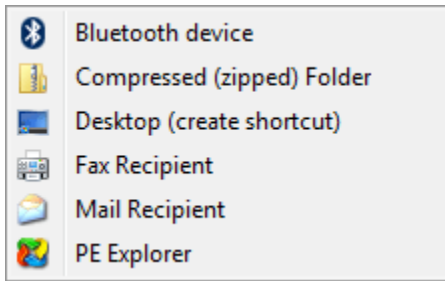
Then, scroll through the list and remove the check from Internet Explorer 8.



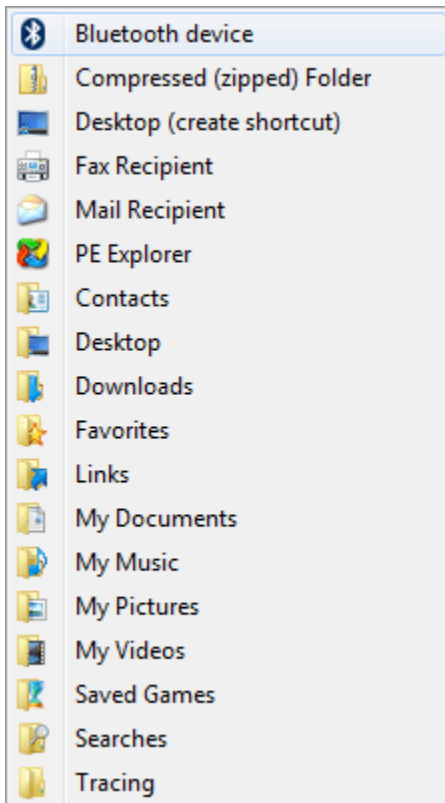
Click OK and IE will be removed.

Hidden Send To Menu in Windows 7

When you right [click](#) on an file or folder in Windows Explorer the default Send To menu contains only a few locations:



What many users do not know is that it is possible to expand the [Windows 7](#) Send To menu by pressing Shift before right-clicking on a file or folder. Pressing the Shift key before right-clicking will expand the Send To menu with more than ten new entries like My Documents folders, Downloads or Contacts.



Projector Tricks in Windows 7

In older versions of Windows using an external projector with your laptop can be a difficult task. It seems like every laptop has a different function key combination to enable output for a projector. In [Windows 7](#) that has finally been improved. Now, all you have to do is hit the Windows Key + P and the projector menu will be displayed.



The on-screen display will allow you to:

- Show [Desktop](#) only on Computer
- Duplicate Desktop on Projector
- Extend Desktop to Projector
- Show Desktop only on projector

If you don't like keyboard shortcuts you can also create a desktop or taskbar shortcut to the projector menu. To do that, create a shortcut to "C:\Windows\System32\DisplaySwitch.exe".

Displayswitch.exe also has command line parameters that allow you to create a shortcut that will set a specific display mode.

- /internal
- /clone
- /extend
- /external

If you wanted to create a shortcut that would turn off your external [monitor](#) then point a shortcut to "C:\windows\system32\displayswitch.exe /internal".

Share Your Screen in Windows 7 with Shareview

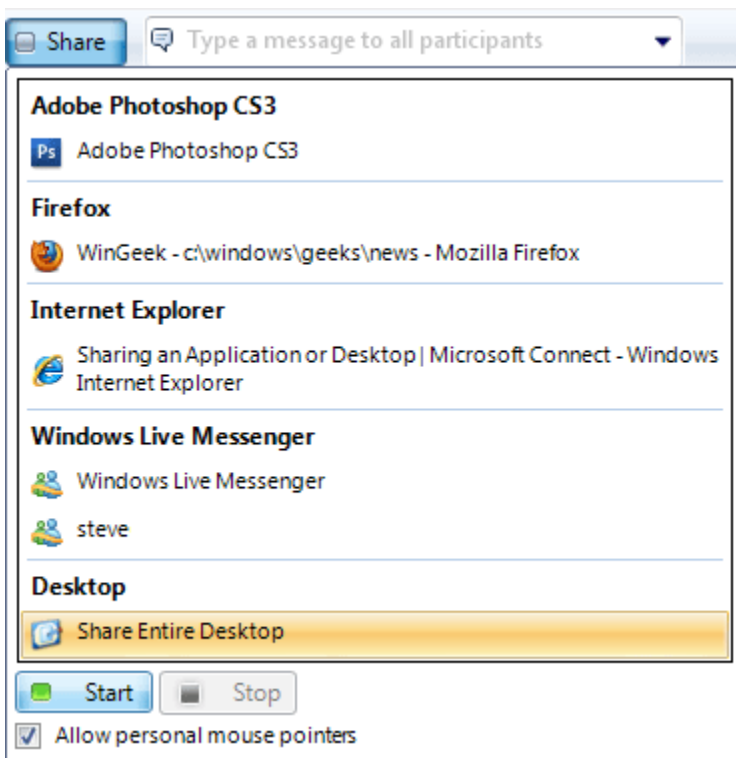
[Microsoft](#) SharedView is a free utility that allows you to share your desktop, applications and documents with up to 15 people online at a time. It is perfect to hold a small meeting or to show a family member how to do something. Best of all it works well through firewalls and routers so you don't have to worry about connection issues.

Getting Microsoft SharedView up and running requires a Microsoft Live ID, broadband connection and a short [download](#).

 [Click here to download SharedView](#)

Once downloaded and installed just start up the utility from the start menu and sign in. Then click Start a new session and send your participants the link and details provided. Finally,click the Start button to start your meeting/event.

After the meeting has started you need to share something for your participants to view. Click the Share button on the top of the screen and select the app you want to share. You can also select your entire [desktop](#) on the bottom of the list.



Once selected click the Start button to begin sharing.

Disable Background Image Across Multiple Monitors

I am a multi-monitor Windows Vista user ever since I got hooked on multiple monitor at work. Two monitors make doing multiple tasks at one so much easier. If I am working on an article or trying to be creative in Photoshop, everything is just much easier because I always have multiple [applications](#) open at once. One feature that I wish I had as soon as I purchased my two monitors and hooked them up was the ability to stretch my wallpaper across both monitors. I wanted to use a very large and wide photo as my background that would like cool displayed across both monitors. Something like the Golden Gate bridge in San Francisco or a cityscape.

After installing and uninstalling Ultra Mon, a third-party shareware utility that I heard is great for multi-monitors, I wanted a easier solution and not something that I had to run in the background. A few weeks go by until I accidentally stumble across how to natively stretch your wallpaper across multiple monitors.

Follow these steps in to display a large image across multiple monitors:

1. Right click on the background and select Personalization.
2. Click on [Desktop](#) Background
3. Select a background image that is at least as wide as the combined resolution of both of your monitors.
For Example, I have two 19" monitors that have a resolution of 1280x1024. I need an image of 2560x1024 or greater so that it can be displayed across both monitors.
4. Next, this is the step that most users would never even think about trying: Select the Tile picture positioning option as shown below. This is the only option that will display your background image across multiple monitors.

How should the picture be positioned?



5. Hit OK

Your background image is now displayed across both monitors instead of having the same image displayed on both monitors.

Add Additional Clocks to the Taskbar

Ever want to keep track of the time in a different time zone? With Vista/7 you can now track two additional time zones with mini clocks that show up when you hover the mouse over the clock.

Add additional time zones:

1. Right click on the clock in the taskbar and select Adjust Date/Time.
2. Click on the Additional Clocks tab.
3. Check the box for either additional clock 1 or 2 and select the time zone.
4. Type in a display name for your clock and hit OK.

Now when you hover your mouse over or click on the clock you will see the additional time zone.

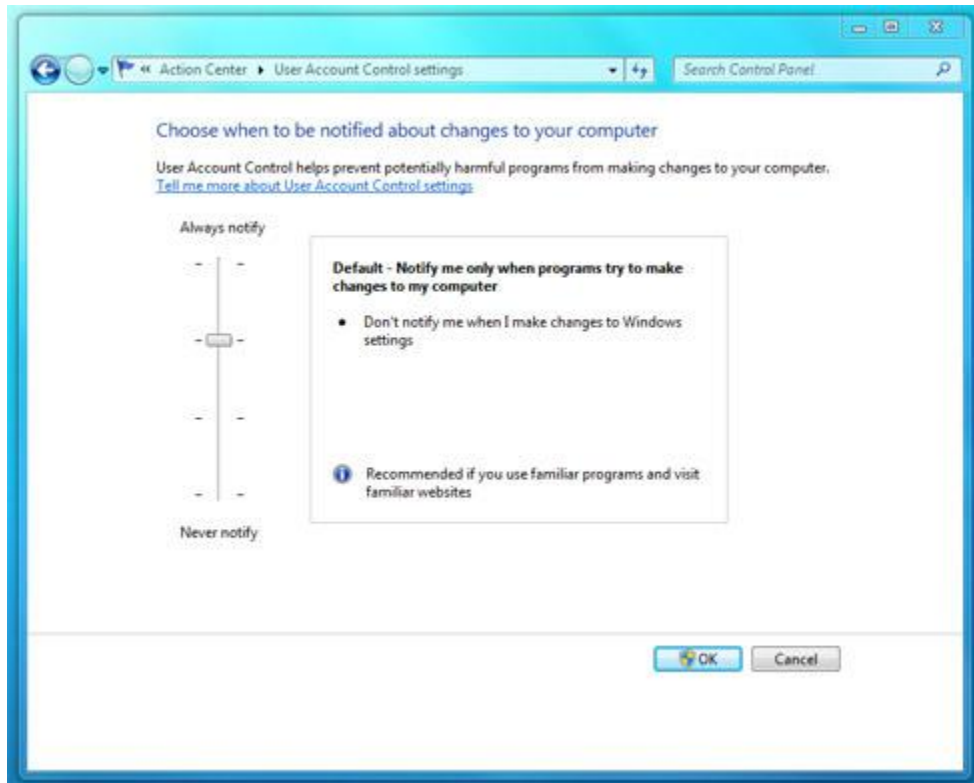
Tip: You can also add additional clocks to the sidebar/desktop by adding more clock gadgets.

Fine Tune User Account Control (UAC) in Windows 7

Aside from being incredibly annoying in Windows Vista, User Account Control reduced the number of malware infections by more than 70% compared to Windows XP [computers](#). The value and security UAC provides is well known but the way it was implemented drove users crazy. In Windows 7 UAC has been significantly improved. The amount of UAC prompts has been greatly reduced and a new control panel applet allows you to modify your protection level. For the first time Windows allows you to treat events caused by applications and user generated events differently.

Tuning User Account Control with the Action Center

All of the new UAC settings can be found in the Action Center. The best way to get directly to the settings through Control Panel and then search for Change User Account Control. Once there you will see a slider with four options:



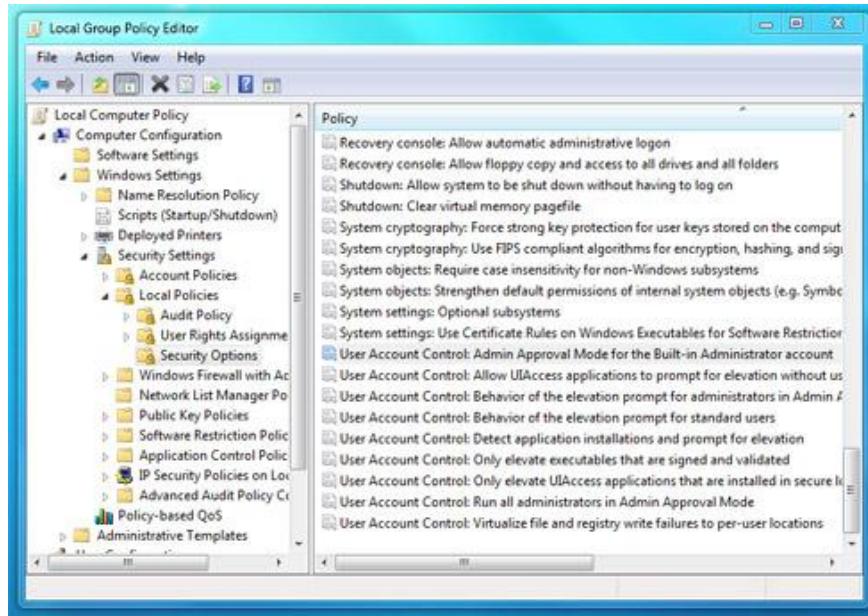
- Always notify when programs try to install software or make changes to my [computer](#) and when I make changes to Windows settings.
- Notify me only when programs try to make changes to my computer and don't notify me when I make changes to Windows settings. This is the new default setting.
- Notify me only when programs try to make changes to my computer and do not use secure [desktop](#) (do not dim my desktop). Also, do not notify me when I make changes to Windows settings.
- Never notify me when programs try to install [software](#) or make changes to my computer and when I make changes to Windows settings. This will turn UAC off.

You can change the level of UAC [protection](#) by using the slider and then clicking OK. The lower you go the less secure your computer will be.

If you want even more control over UAC you can use the local group policy editor.

Tuning User Account Control with Local Group Policy Editor

With the Local Group Policy editor you can adjust even more User Account Control settings. Click on the Start button and type in gpedit.msc and hit Enter. When the Local Group Policy editor is loaded, navigate through Computer Configuration, Windows Settings, Security Settings, Local Policies and Security Options. On the bottom of the list you will find all of the User Account Control settings.



- User Account Control: Admin Approval Mode for the Built-in Administrator account.
- User Account Control: Allow UIAccess [applications](#) to prompt for elevation without using the secure desktop.
- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode.
- User Account Control: Behavior of the elevation prompt for standard users.
- User Account Control: Detect [application](#) installations and prompt for elevation.
- User Account Control: Only elevate executables that are signed and validated.
- User Account Control: Run all users, including administrators, as standard users.
- User Account Control: Virtualizes file and registry write failures to per-user locations.

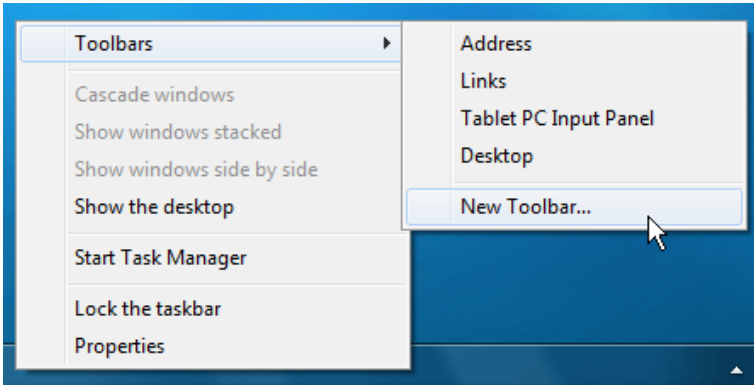
To modify a setting just right click on it and select Properties. Once you make your changes hit OK. Some settings may require a reboot.

Restore Quick Launch Toolbar

Many Windows users have grown accustomed to using the quick launch bar to quickly start [applications](#) and access folders. The new taskbar is kind of like a quick launch bar on steroids but there are some things it can't do. For example, a folder or a drive shortcut can't be pinned directly on the new taskbar. Instead it places the shortcut into the Explorer folder organizer. For some that is fine but many quick launch geeks want the icons directly on the taskbar. Thankfully, there is a way to bring back the quick launch toolbar.

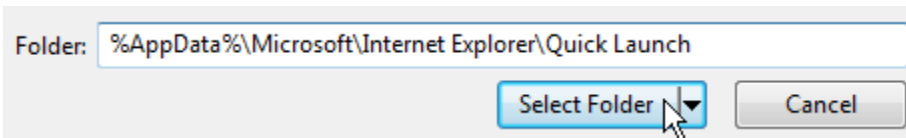


First, right click on the taskbar and select Toolbars and then New Toolbar.



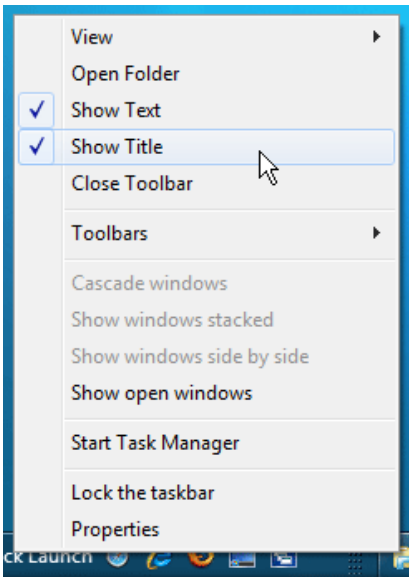
Enter in the following folder location and then click Select Folder:

%AppData%\Microsoft\Internet Explorer\Quick Launch



The quick launch toolbar will now be displayed but you will need to move it to the correct location on the taskbar. Just click on the Quick Launch label and drag it all the way to the left.

After you adjusted the width of the quick launch bar the last step is to remove the Quick Launch label. Right click on the text and click on Show Title to remove the option.



You have now restored the classic Windows Quick Launch toolbar.

Windows 2008 Tips & Tricks

Control How Group Policy Is Applied At Logon

By default, the Fast Logon Optimization feature is set for both domain and workgroup members. This setting causes policy to be applied asynchronously when the computer starts and the user logs on. The result is similar to a background refresh. The advantage is that it can reduce the amount of time it takes for the logon dialog box to appear and the amount of time it takes for the desktop to become available to the user. Of course, it also means that the user may log on and start working before the absolute latest policy settings have been applied to the system.

Depending on your environment, you may want to disable Fast Logon Optimization. You can do this with Group Policy, using the **Always wait for the network at computer startup and logon** policy setting. To access this setting:

Open the Group Policy Object Editor.

Under **Computer Configuration** in the navigation tree on the left side, navigate to **Administrative Templates\System\Logon**. Here you can simply enable (or disable) the setting.

Delegate Control to Users to Work with GPOs

You can allow a nonadministrative user or a group (including users and groups from other domains) to work with a domain, site, or OU GPO by granting one of three specific permissions:

Read Allows the user or group to view the GPO and its settings.

Edit Settings Allows the user or group to view the GPO and its settings and also change settings. The user or group cannot delete the GPO or modify security.

Edit Settings, Delete, Modify Security Allows the user or group to view the GPO and its settings and also change settings, delete the GPO, and modify security.

To grant these permissions to a user or group, follow these steps:

- In the GPMC, expand the entry for the forest you want to work with and then expand the related Domains node.
- Expand the node for the domain you want to work with. If you don't see the domain you want to work with, right-click Domains and then click Show Domains. You can then select the domains you want to display.
- Select the Group Policy Objects node, and then select the GPO you want to work with in the left pane. In the right pane, select the Delegation tab.
- The current permissions for individual users and groups are listed. To grant permissions to another user or group, click Add.
- In the Select User, Computer, Or Group dialog box, select the user or group and then click OK.
- In the Add Group Or User dialog box, select the permission to grant: Read; Edit Settings; or Edit Settings, Delete, Modify Security. Click OK.

The list of users and groups on the Delegation tab is updated to reflect the permissions granted. If you want to remove this permission in the future, display the Delegation tab, click the user or group, and then click Remove.

Delegate Privileges for Group Policy Management

- In Active Directory, administrators are automatically granted permissions for performing different Group Policy management tasks. Other individuals can be granted such permissions through delegation. Here's how.

Assign GPO Creation Rights: Administrators

In Active Directory, administrators have the ability to create GPOs in domains, and anyone who has created a GPO in a domain has the right to manage that GPO. To determine who can create GPOs in a domain, follow these steps:

- In the GPMC, expand the entry for the forest you want to work with and then expand the related Domains node.
- Expand the node for the domain you want to work with. If you don't see the domain you want to work with, right-click Domains and then click Show Domains. You can then select the domains you want to display.
- Select the Group Policy Objects node. The users and groups who can create GPOs in the selected domain are listed on the Delegation tab.
- **Assign GPO Creation Rights: Non-Administrative Users**
You can allow a nonadministrative user or a group (including users and groups from other domains) to create GPOs (and thus implicitly grant them the ability to manage the GPOs they've created). To grant GPO creation permission to a user or group, follow these steps:
 - In the GPMC, expand the entry for the forest you want to work with and then expand the related Domains node.
 - Expand the node for the domain you want to work with. If you don't see the domain you want to work with, right-click Domains and then click Show Domains. You can then select the domains you want to display.
 - Select the Group Policy Objects node. In the right pane, select the Delegation tab. The current GPO creation permissions for individual users and groups are listed. To grant the GPO creation permission to another user or group, click Add.
 - In the Select User, Computer, Or Group dialog box, select the user or group you want to grant permissions to and then click OK.

The list of users and groups on the Delegation tab are updated as appropriate. If you want to remove the GPO creation permission in the future, access the Delegation tab, click the user or group, and then click Remove.

Best Practices for Enforcing Password Policies

No matter how secure you make a user's password initially, she will eventually choose her own password. Therefore, you should set account policies that define a secure password for your systems. Account policies are a subset of the policies configurable in Group Policy. Here's a look at the key settings you will work with.

Enforce Password History

This sets how frequently old passwords can be reused. With this policy, you can discourage users from alternating between several common passwords. Windows Server 2008 R2 can store up to 24 passwords for each user in the password history. To disable this feature, set the value of the password history to 0. To enable this feature, set the value of the password history using the Passwords Remembered field. Windows Server 2008 R2 then tracks old passwords using a password history that's unique for each user, and users aren't allowed to reuse any of the stored passwords.

Note: To prevent users from working around the Enforce Password History settings, you should prevent users from changing passwords immediately. This stops users from changing their passwords several times to wipe the history and get back to the old password. You can set the time required to keep a password with the Minimum Password Age policy.

Maximum Password Age

This determines how long users can keep a password before they have to change it. The aim is to force users to change their passwords periodically. Generally, you use a shorter period when security is very important and a longer period when security is less important. You can set the maximum password age to any value from 0 to 999, where a value of 0 specifies that passwords don't expire. Although you might be tempted to set no expiration date, users should change passwords regularly to ensure the network's security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.

Note: Windows Server 2008 R2 notifies users when the password expiration date is approaching. Any time the expiration date is less than 30 days away, users see a warning when they log on that they have to change their password within a specific number of days.

Minimum Password Age

This determines how long users must keep a password before they can change it. You can use this field to prevent users from bypassing the password system by entering a new password and then changing it right back to the old one. If the minimum password age is set to 0, users can change their passwords immediately. To prevent this, set a specific minimum age. Reasonable settings are from three to seven days. In this way you make sure that users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to.

Note: Keep in mind that a minimum password age could prevent a user from changing a compromised password. If a user can't change the password, an administrator has to make the change.

Minimum Password Length

This sets the minimum number of characters for a password. If you haven't changed the default setting, you should do so immediately. The default in some cases is to allow empty passwords (passwords with zero characters), which is definitely not a good idea. For security reasons you'll generally want passwords of at least eight characters because long passwords are usually harder to crack than short ones. If you want greater security, set the minimum password length to 14 characters.

Passwords Must Meet Complexity Requirements

Beyond the basic password and account policies, Windows Server 2008 R2 includes facilities for creating additional password controls. These facilities enforce the use of secure passwords that follow these guidelines:

- Passwords must have at least six characters.
- Passwords can't contain the user name or parts of the user's full name, such as his first name.
- Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

To enforce these rules, enable the Passwords Must Meet Complexity Requirements policy.

Store Password Using Reversible Encryption For All Users

Passwords in the password database are encrypted. This encryption can't normally be reversed. The only time you would want to change this setting is when your organization uses applications that need to read the password. If this is the case, enable Store Password Using Reversible Encryption For All Users. But with this policy enabled, passwords might as well be stored as plain text—it presents the same security risks. With this in mind, a much better technique is to enable the option on a per-user basis and then only as required to meet the user's actual needs.

Detect and Avoid IP Address Conflicts

IPv4 address conflicts are a common cause of problems with DHCP. No two computers on the network can have the same unicast IP address. If a computer is assigned the same unicast IPv4 address as another, one or both of the computers might become disconnected from the network.

To better detect and avoid potential conflicts, you can enable IPv4 address conflict detection by following these steps:

1. In the DHCP console, expand the node for the server you want to work with, right-click IPv4, and then click Properties.
2. On the Advanced tab, set Conflict Detection Attempts to a value other than 0. The value you enter determines the number of times the DHCP server checks an IP address before leasing it to a client. The DHCP server checks IP addresses by sending a ping request over the network.

Real World Example: A unicast IPv4 address is a standard IP address for class A, B, and C networks. When a DHCP client requests a lease, a DHCP server checks its pool of available addresses and assigns the client a lease on an available IPv4 address. By default, the server checks only the list of current leases to determine whether an address is available. It doesn't actually query the network to see whether an address is in use.

Unfortunately, in a busy network environment, an administrator might have assigned this IPv4 address to another computer or an offline computer might have been brought online with a lease that it believes hasn't expired, even though the DHCP server believes the lease has expired. Either way, you have an address conflict that will cause problems on the network. To reduce these types of conflicts, set the conflict detection to a value greater than 0.

Monitor and Tune Network Bandwidth and Connectivity

No other factor matters more to the way a user perceives your server's performance than the network that connects your server to the user's computer. The delay, or latency, between when a request is made and the time it's received can make all the difference. A high degree of latency means that it doesn't matter if you have the fastest server on the planet: The user experiences a delay and perceives that your servers are slow.

Generally speaking, the latency that the user experiences is beyond your control. It's a function of the type of connection the user has and the route the request takes to your server. The total capacity of your server to handle requests and the amount of bandwidth available to your servers are factors under your control, however. Network bandwidth availability is a function of your organization's network infrastructure.

Network capacity is a function of the network cards and interfaces configured on the servers. The capacity of your network card can be a limiting factor in some instances. Most servers use 10/100 network cards, which can be configured in many ways. Someone might have configured a card for 10 Mbps, or the card might be configured for half duplex instead of full duplex. If you suspect a capacity problem with a network card, you should always check the configuration.

To determine the throughput and current activity on a server's network cards, you can check the following counters:

- Network\Bytes received/sec
- Network\Bytes Sent/sec
- Network\Bytes Total/sec
- Network Current Bandwidth

If the total bytes per second value is more than 50 percent of the total capacity under average load conditions, your server might have problems under peak load conditions. You might want to ensure that operations that take a lot of network bandwidth, such as network backups, are performed on a separate interface card. Keep in mind that you should compare these values in conjunction with PhysicalDisk\% Disk Time and Processor\% Processor Time. If the disk time and processor time values are low but the network values are very high, you might

have a capacity problem. Solve the problem by optimizing the network card settings or by adding a network card. Remember, planning is everything—it isn't always as simple as inserting a card and plugging it into the network.

Understand Implicit Groups and Identities in Windows Server 2008

Windows Server 2008 defines a set of special identities that you can use to assign permissions in certain situations. You usually assign permissions implicitly to special identities. However, you can assign permissions to special identities when you modify Active Directory objects. The special identities include the following:

The Anonymous Logon identity Any user accessing the system through anonymous logon has the Anonymous Logon identity. This identity allows anonymous access to resources, such as a Web page published on the corporate presence servers.

The Authenticated Users identity Any user accessing the system through a logon process has the Authenticated Users identity. This identity allows access to shared resources within the domain, such as files in a shared folder that should be accessible to all the workers in the organization.

The Batch identity Any user or process accessing the system as a batch job (or through the batch queue) has the Batch identity. This identity allows batch jobs to run scheduled tasks, such as a nightly cleanup job that deletes temporary files.

The Creator Group identity Windows Server 2008 uses this special identity group to automatically grant access permissions to users who are members of the same group(s) as the creator of a file or a directory.

The Creator Owner identity The person who created the file or the directory is a member of this special identity group. Windows Server 2008 uses this identity to automatically grant access permissions to the creator of a file or directory.

The Dial-Up identity Any user accessing the system through a dial-up connection has the Dial-Up identity. This identity distinguishes dial-up users from other types of authenticated users.

The Enterprise Domain Controllers identity Domain controllers with enterprise-wide roles and responsibilities have the Enterprise Domain Controllers identity. This identity allows them to perform certain tasks in the enterprise using transitive trusts.

The Everyone identity All interactive, network, dial-up, and authenticated users are members of the Everyone group. This special identity group gives wide access to a system resource.

The Interactive identity Any user logged on to the local system has the Interactive identity. This identity allows only local users to access a resource.

The Network identity Any user accessing the system through a network has the Network identity. This identity allows only remote users to access a resource.

The Proxy identity Users and computers accessing resources through a proxy have the Proxy identity. This identity is used when proxies are implemented on the network.

The Restricted identity Users and computers with restricted capabilities have the Restricted identity.

The Self identity The Self identity refers to the object itself and allows the object to modify itself.

The Service identity Any service accessing the system has the Service identity. This identity grants access to processes being run by Windows Server 2008 services.

The System identity The Windows Server 2008 operating system itself has the System identity. This identity is used when the operating system needs to perform a system-level function.

The Terminal Server User identity Any user accessing the system through Terminal Services has the Terminal Server User identity. This identity allows terminal server users to access terminal server applications and to perform other necessary tasks with Terminal Services.