



A guide to setting up Parental controls in Windows Vista

Introduction

With the launch of Windows [Vista](#) , Microsoft has introduced a new security feature called [Windows](#) Parental Controls. Windows Parental Controls allows a parent to configure, on a per user basis, various restrictions on what that user can do on the computer. These settings range from blocking websites to controlling what [games](#)  they can play. Having access to these types of controls allows a parent to feel comfortable with their children using a computer and at the same time gives them the flexibility to customize these settings to their specific needs.

It is important to note that not all programs are compatible with Windows Parental Controls. In order for Windows Parental Controls to properly [monitor](#) and control certain activities on the computer, the application must be compatible with this new service. For the most part, most of the settings can be enforced across all applications, but it is important to test these controls using the applications that your users will be using. This way you know for sure that any restriction you put into place can be enforced. It is also important to note that Windows Parental Controls can only be assigned to a Standard User, which is a user with limited rights on the computer, and cannot be assigned to accounts that are configured as an Administrator. This is so a user cannot remove restrictions placed on them.



One of the more powerful features of this new service is that you will be able to view reports of the activity for each user that you have configured Parental Controls. The information you see will be determined by whether or not the user is using applications that are compatible with Windows Parental Controls. Assuming that all the applications are compatible you will be able to monitor the following activity.

- Most recent websites blocked.
- Attempts to visit sites that have been specifically blocked or allowed.
- What files were downloaded.
- What file downloads were blocked.
- When the user logged on.
- What programs they have run.
- Emails sent and received
- Instant Messages sent and received.
- What games were played.
- What media such as movies and videos were played.

In this guide we will go into detail on how to use Windows Parental Controls to restrict a user's activity. If you read through this guide, at the end you will know all that you need to know about Windows Parental Controls and how to use them to provide a safe [computing](#) environment for your children.

Welcome to Windows Vista Parental Controls

In order to access and start using the Vista Parental Controls you need to log onto to your computer using an account that is an administrator. Once logged in you should do the following:

1. Click on the **Start** () button.
2. In the Start Menu Search Box () type **Parental Controls** and press **enter** on your [keyboard](#).
3. A User Account Control prompt will appear asking if you would like to continue. Click on the **Continue** button to proceed with opening the Parental Controls.

You will now be at the Vista Parental Controls welcome screen. This screen is the main launching pad for setting the global Parental Controls options as well as configuring Parental Controls for the *Standard Users* on your computer. From this screen you can create a new Standard User account, configure existing user's Parental Controls settings, configure the global game rating system, and set some other basic global settings.

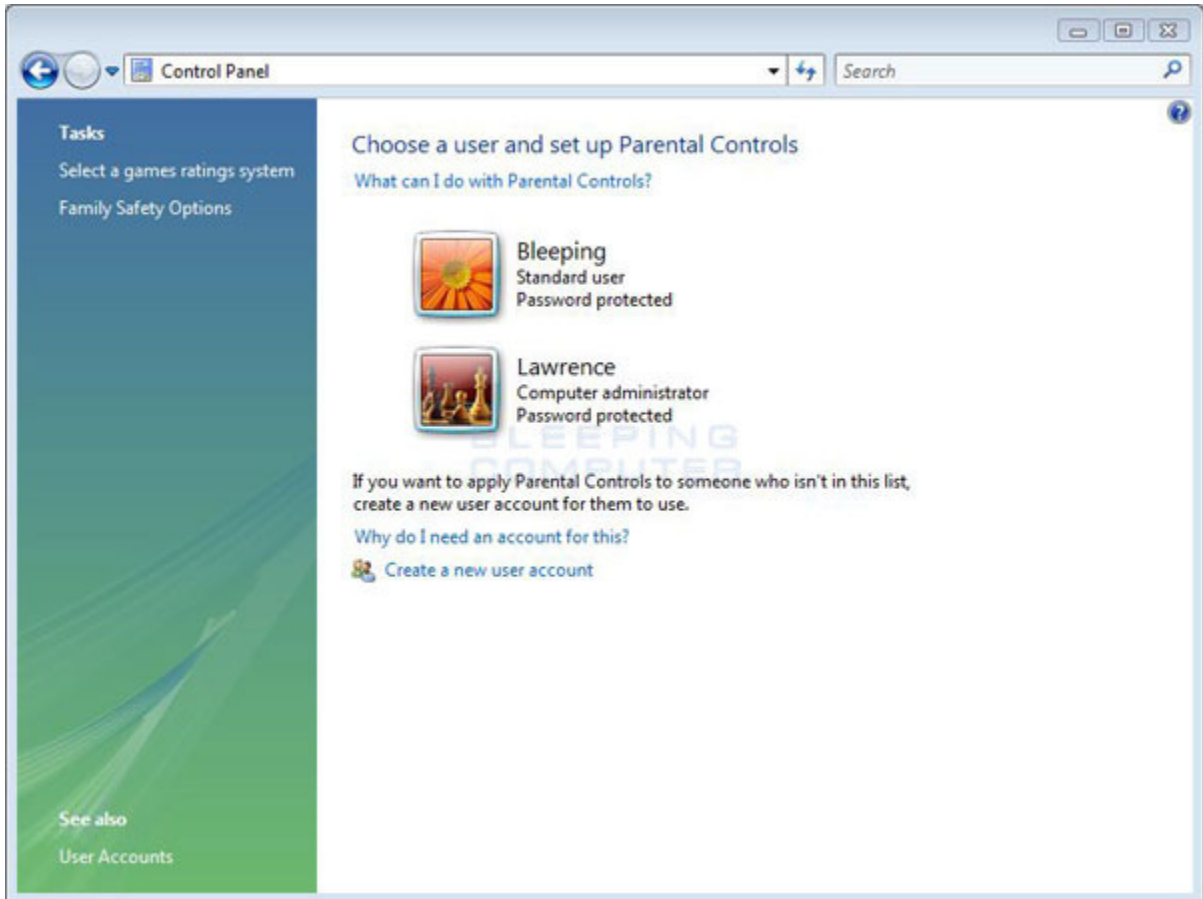


Figure 1. The Main Vista Parental Controls Screen

The first option we will explore is to create a new Standard User account that you can assign Parental Controls to. You can do this by clicking on the **Create a new user account** option which will bring up a screen that enables you to create a new account as shown below.

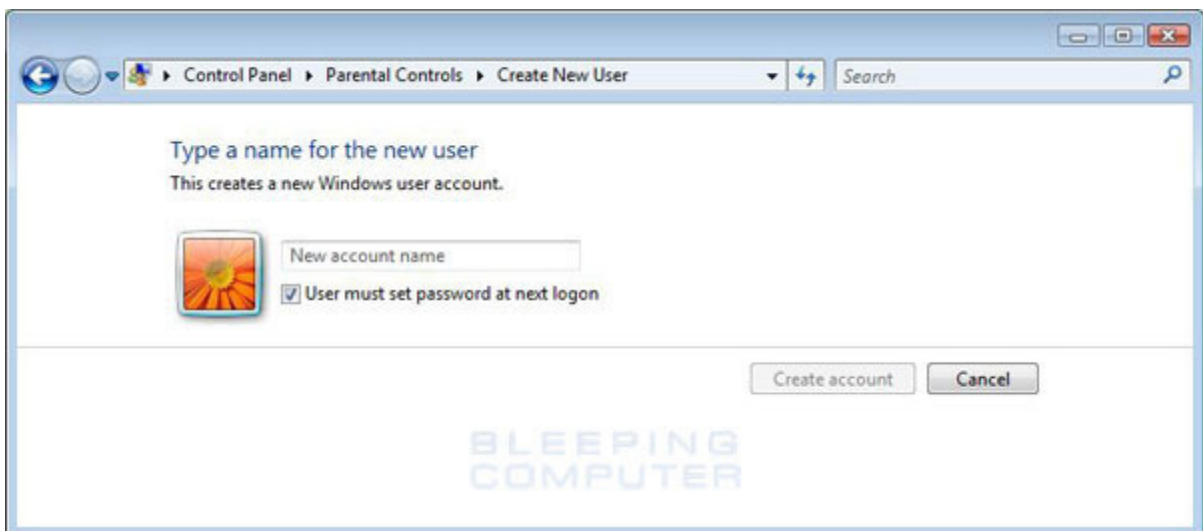


Figure 3. Create a new account

In this screen you would type the login name for the new user account that you would like to create. We also suggest that you leave the option labeled **User must set password at next logon** checked so that when the user logs on for the first time they will be prompted for a new password enabling them to keep their password private. When you are ready to create the user, you would click on the **Create Account** button to finish the

creation process. You would then be brought to the Parental Controls page for that particular user. We will go into more detail about setting user controls later in the tutorial so just press the **OK** button to get back to the welcome screen..

The first global setting you can modify from the main welcome screen is the games rating system that will be used for all Parental Controls enabled accounts. To view or modify your current setting you should on the **Select a games ratings system** option.

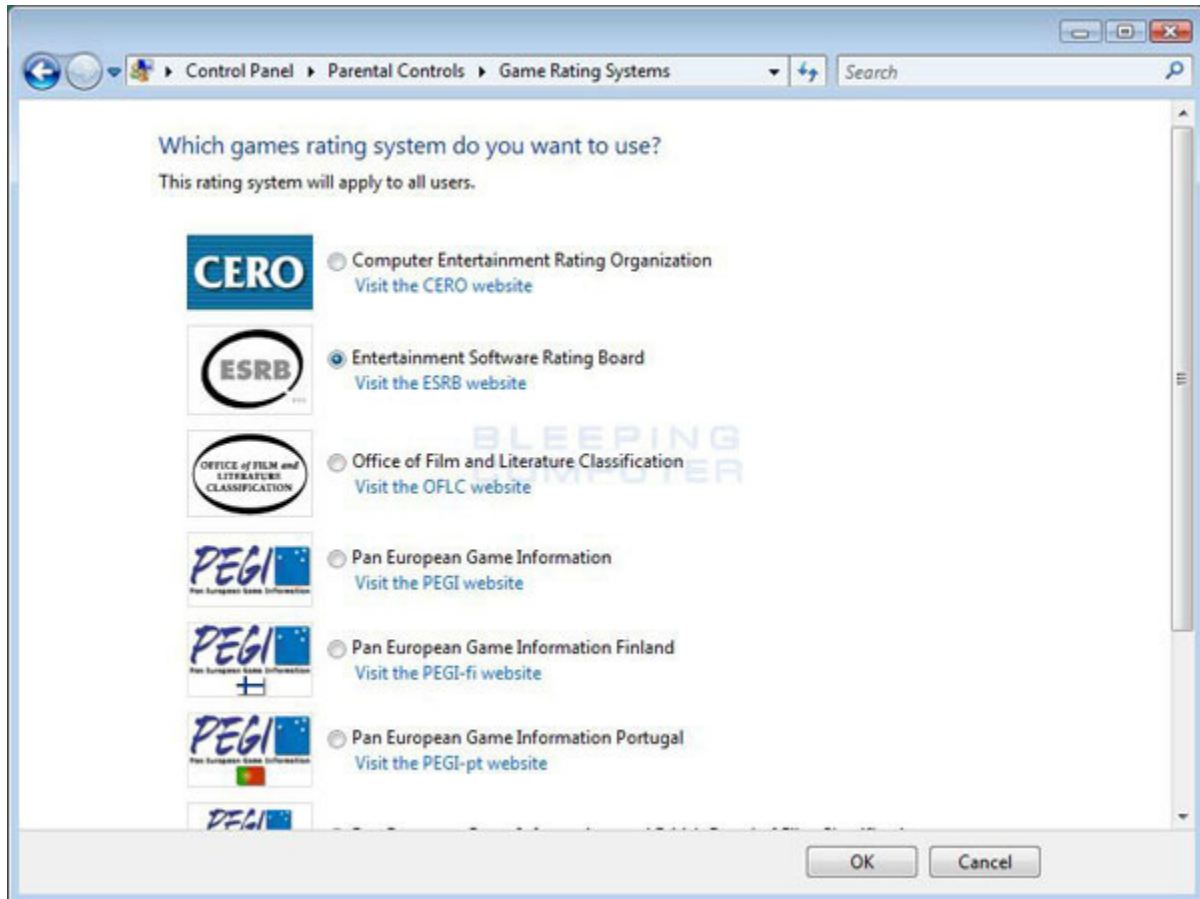


Figure 4. Global game rating systems setting

It is advised that you stick with the **Entertainment Software Rating Board, ESRB**, rating system as your default but feel free to choose another if you wish. Once you are finished selecting the rating system, or keeping the current one, press the **OK** button to exit this screen and go back to the welcome screen.

This brings us to the next set of global settings, the Family Safety Options. By clicking on **Family Safety Options** you will be brought to a page that contains two global settings.

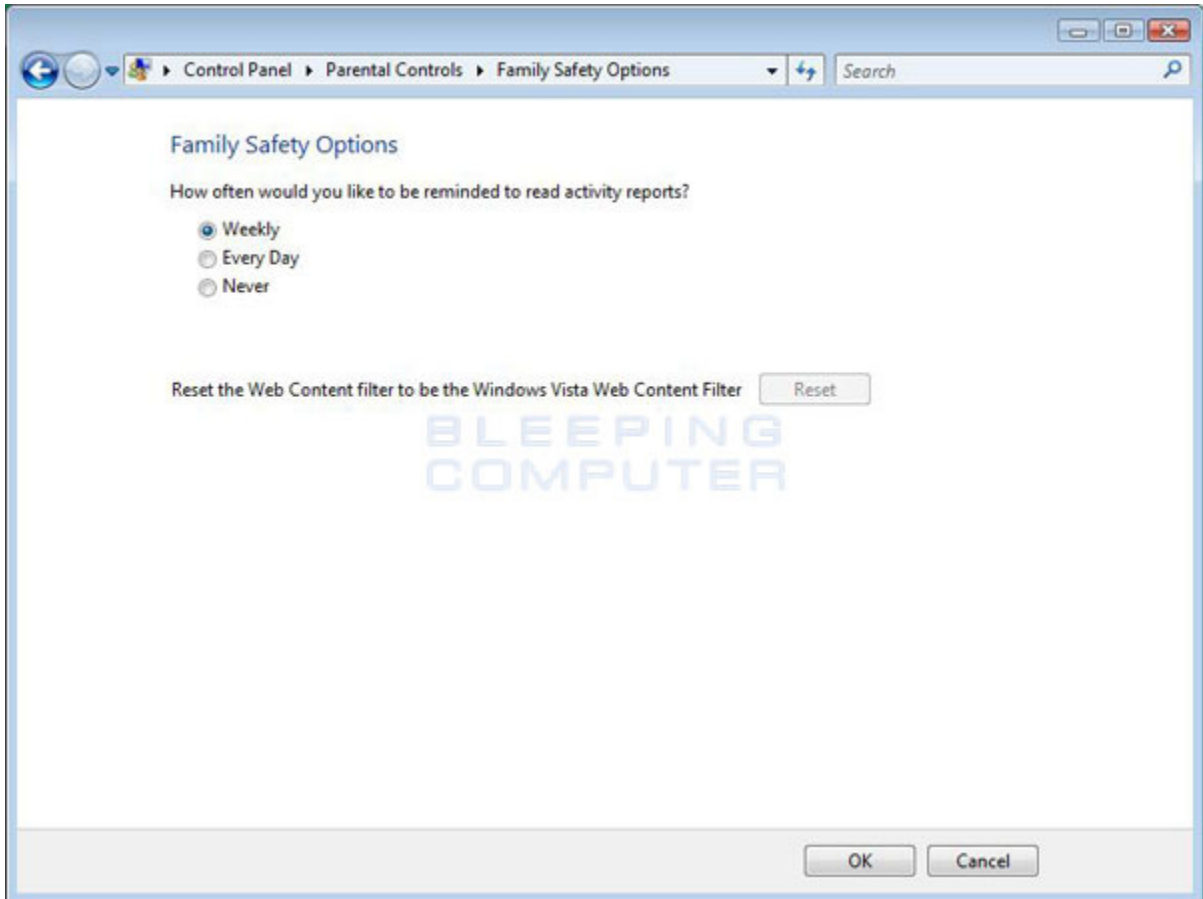


Figure 4. Family Safety Options

The first option is labelled **How often would you like to be reminded to read activity reports**. This option allows you to specify how often you should be reminded that there are Parental Controls activity reports available to be viewed. You will see these reminders when you log into an administrator account. An example of this alert is below.



Figure 5. Activity Report Reminder

The second option labeled **Reset the Web Content filter to be the Windows Vista Web Content Filter** allows you to configure Vista to use the built-in content filter rather than a [3rd party software](#) that you may have installed. If you had installed another [web content](#) filtering software and would like to reset it back to using the Vista one, you can click on the **Reset** button. When you are done configuring these options you should press the **OK** button to get back to the main welcome screen.

Now that we have explored the main welcome screen, lets dig down into configuring the Parental Controls for the individual users on your computer. To start this process you simply need to click on a Standard User listed in the welcome screen. As said previously, you can only enable Parental Controls on an account that is a **Standard User**. If you attempt to add Parental Controls to an administrator you will instead receive the following message.



Figure 6. Cannot apply controls to an administrator

Once you click on a Standard User account you will be brought to the User Controls screen where you can view the users activity log, enable or disable Parental Controls, and fine tune the various Parental Controls for this particular user. If the user that you are configure Parental Controls for is currently logged on you will receive a warning stating that the new settings may not go into affect until the user logs off and back on.

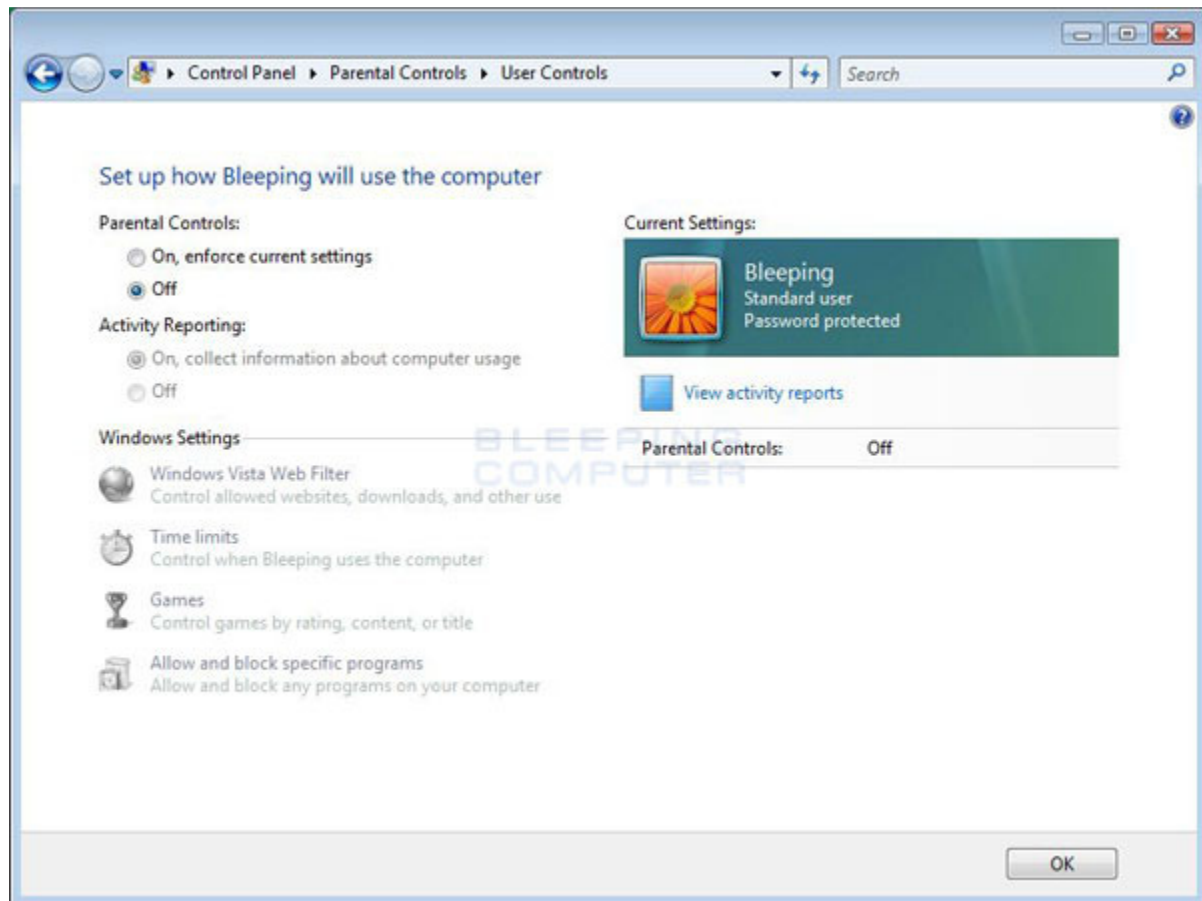


Figure 7. User Controls Screen

On the left hand side of the screen are the various options that you can configure for this user. These settings will be disabled if Parental Controls is not turned on for this user. On the right hand side of the screen you will find a summary of the user's currently configured controls as well as have the ability to view the user's activity reports by clicking on the **View activity reports** option.

Let us start by enabling the Parental Controls for this particular user. To do that you would select the option labeled **On, enforce current settings**. Once this option is selected you will now have access to the other settings on this screen. It is important to note that once you select this option, default restrictions will go into place. These default restrictions are described below. We then suggest that you enable the option under the

Activity Reporting: category labeled **On, collect information about computer usage**. With this option enabled, Vista will log to the user's activity report their activity on the computer.

Now that you have enabled Parental Controls for this user, the following options will become available under the Windows Settings category.

[Windows Vista Web Filter](#)

This section allow you to controls the sites the user is allowed to visit, whether or not they can download files, and the type of web site content they can view.

[Time Limits](#)

This section allows you to specify the specific times that the user is allowed to use the computer.

[Games](#)

This section allows you to specify what games are allowed to be played on this computer based on their rating, content or title.

[Allow and Block Specific Programs](#)

This section allows you to specify programs that a user can or cannot use.

Each of the above settings is discussed in greater detail in their own sections below. Let's move on to the first of these four sections and learn about the Windows Vista Web Filter.

[Configuring the Windows Vista Web Filter](#)

If you select the **Windows Vista Web Filter** option you will be brought to the Web Restrictions screen shown below. At this screen you have a variety of different options that enable you to control what sites the user can visit.

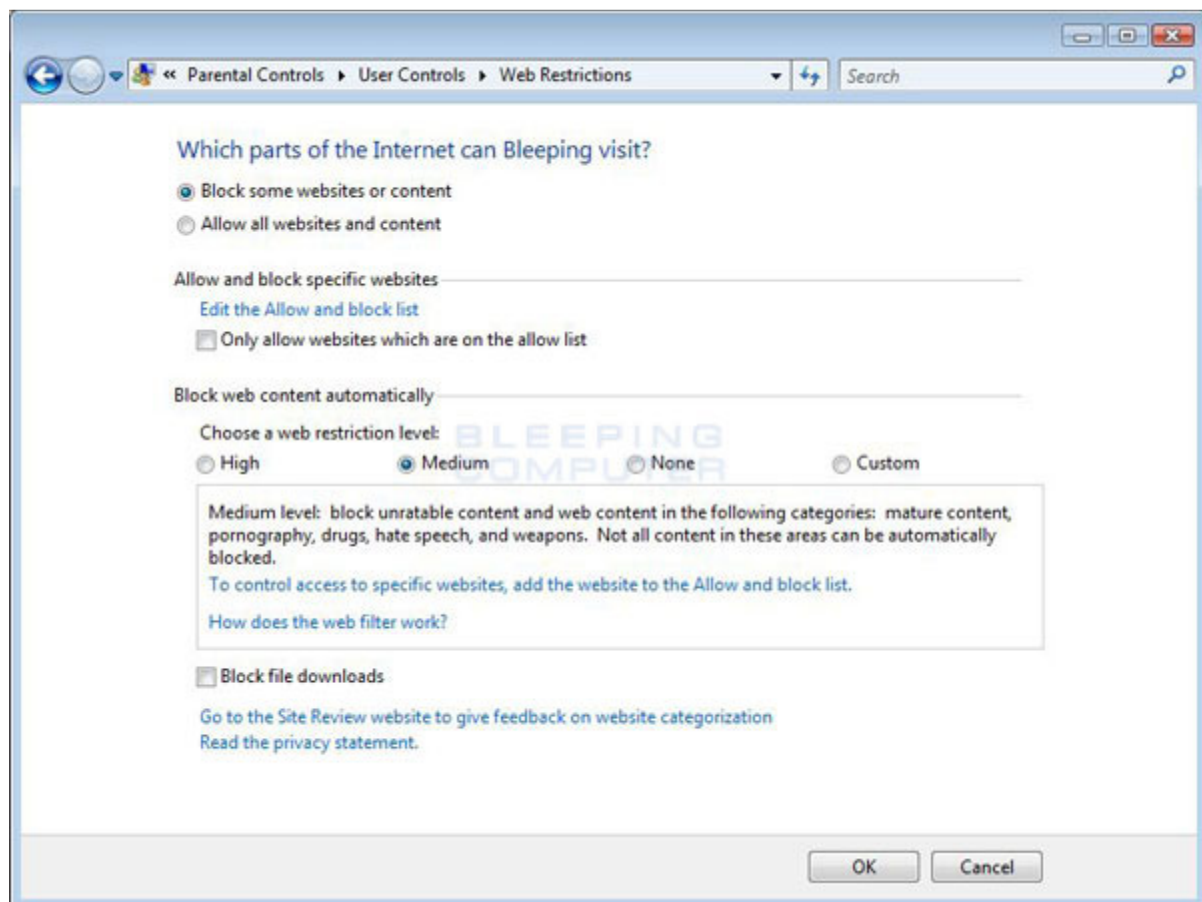


Figure 8. Web Restrictions Page

By default, when you enable Parental Controls on an account Web Restrictions are automatically enabled and the **Block some websites or content** option will be selected. To disable restrictions select the **Allow all websites and content** option. When web restrictions are enabled, Vista will automatically set your restriction level, which can be set under the **Block web content automatically** category, to **Medium**. If the medium setting is too relaxed or too strict you can modify it one of the following settings:

Custom - If you select this category you will be brought to a new screen where you can select the specific site categories that you would like to restrict this user from visiting.




Figure 9. Custom Content Filtering Level

None - There will not be any web content restrictions on any sites this user visits.

Medium - This level will block upgradeable content and content that fits in the following categories: **mature content, pornography, drugs, hate speech, and weapons.**

High - Block all websites except those approved for children.

It is important to note when using web restrictions that these settings may not block every site that fits these categories due to the fact that what some people find objective others do not. The restrictions will, though, be able to block a large amount of sites that fall under the particular category. When a user attempts to visit a site blocked by Parental Controls, the user will see a screen in Internet Explorer , or another browser, similar to the one below:

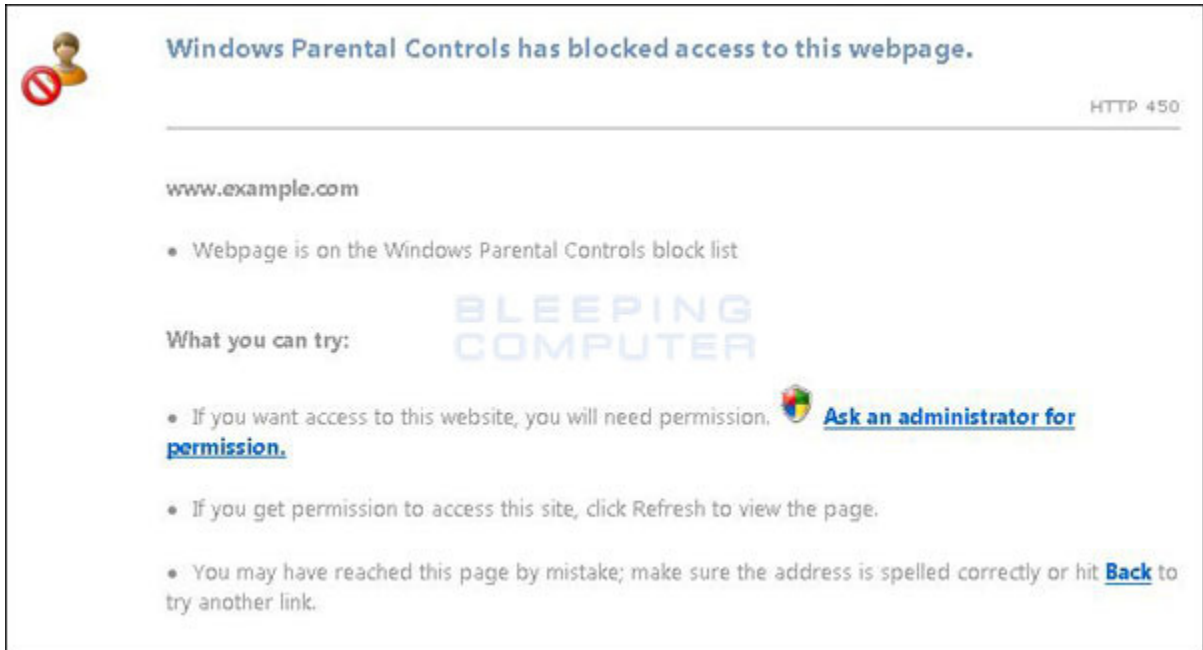


Figure 10. Site blocked by Parental Controls

If the user knows the administrator password then they can click on the **Ask administrator for permission** link in the blocked site's message. They will then be prompted to enter the administrator's login information to unblock the site.

Under the **Block web content automatically** category is another option labelled **Block file downloads**. If you enable this option then the user will not be able to download files through Internet Explorer. When using this feature, it is fairly easy to circumvent it as not all browsers are blocked. For example though Internet Explorer is able to block downloads, users of Firefox will have no problems downloading anything. Therefore you should not rely on these features entirely, but rather test them with the various applications your users will be using. When Parental Controls blocks a download it will show an alert similar to the one below.

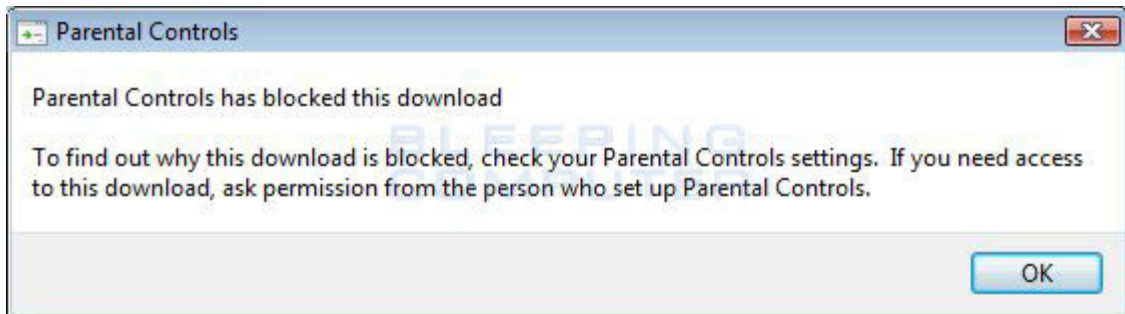


Figure 11. Download blocked by Parental Controls

The last category under web restrictions is **Allow and block specific sites**. This section allows you to specify specific sites that you want to deny or allow the user to visit. When adding sites to the block or allow list they override any restrictions based on the sites content that were configured previously. In this way you can use this section to fine tune the content filters based on a specific site. To configure this setting click on the **Edit the Allow and block list** option. This will bring you to the Allow Block Webpages screen as shown below.

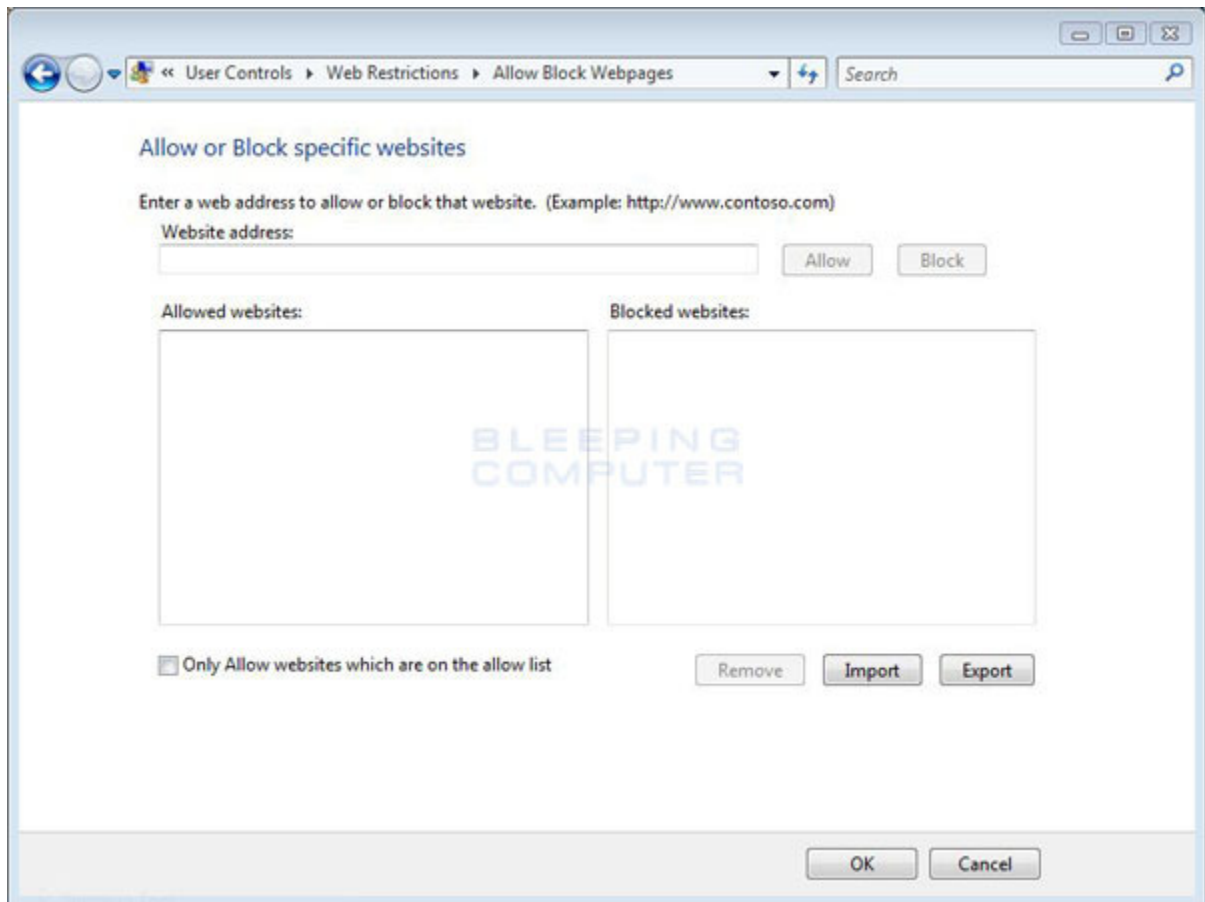


Figure 12. Allow Block Webpage's Screen

At this screen you can enter specific URLs, with only **http://** URLs currently being supported, into the **Website address:** field and then either press the **Allow** or **Block** button. If you press the Allow button it will add that URL into the allow list and the site will always be accessible by the user. If you add it to the block list then the user will not be allowed to access it. When adding URLs to these lists, any URL in the allow list overrides the same URL, or a more general URL, in the block list. For example, if you add the broad and general URL, **http://www.example.com**, to the block list it would block every page that started with **http://www.example.com/**. Now if you added a more specific URL for that domain, **http://www.example.com/safepage.html**, to the allow list, that one URL would be accessible overriding the block list.

If you really want to harden the system so that almost no sites can be accessed you can put a checkmark in the **Only Allow websites which are on the allow list** checkbox. With this checked only URLs that you enter into the allow category will be able to be visited. It is strongly suggested that you do not select this option, as you will be seriously curtailing the amount of useful sites available on the web.

Last but not least, you also have the ability to export and import your Allow and Block lists to a file. This is useful if you want to use the same rules on a different computer or if you have compiled a really good list and want to share it with your friends. If you want to save your Allow and Block list to a file you would click on the **Export** button. This will bring up a prompt where you give your list a name and then save it in the folder of your choice. If you would like to import a list, you would click on the **Import** button and browse to the Web Allow Block Lists file that you would like to import. We will go into more detail about these types of files later in the tutorial. When you are done configuring the Allow and Block lists, press the **OK** button to save your settings.

That covers the configuration of the Windows Vista  Web Filter for this user. Press the **OK** button again to get back to the main User Controls screen so we can configure this the time restrictions for this user.

Configuring time restrictions

When you select the **Time Limits** option in the Users Controls you will be brought to a screen where you can specify the hours that the user is allowed to use the computer.

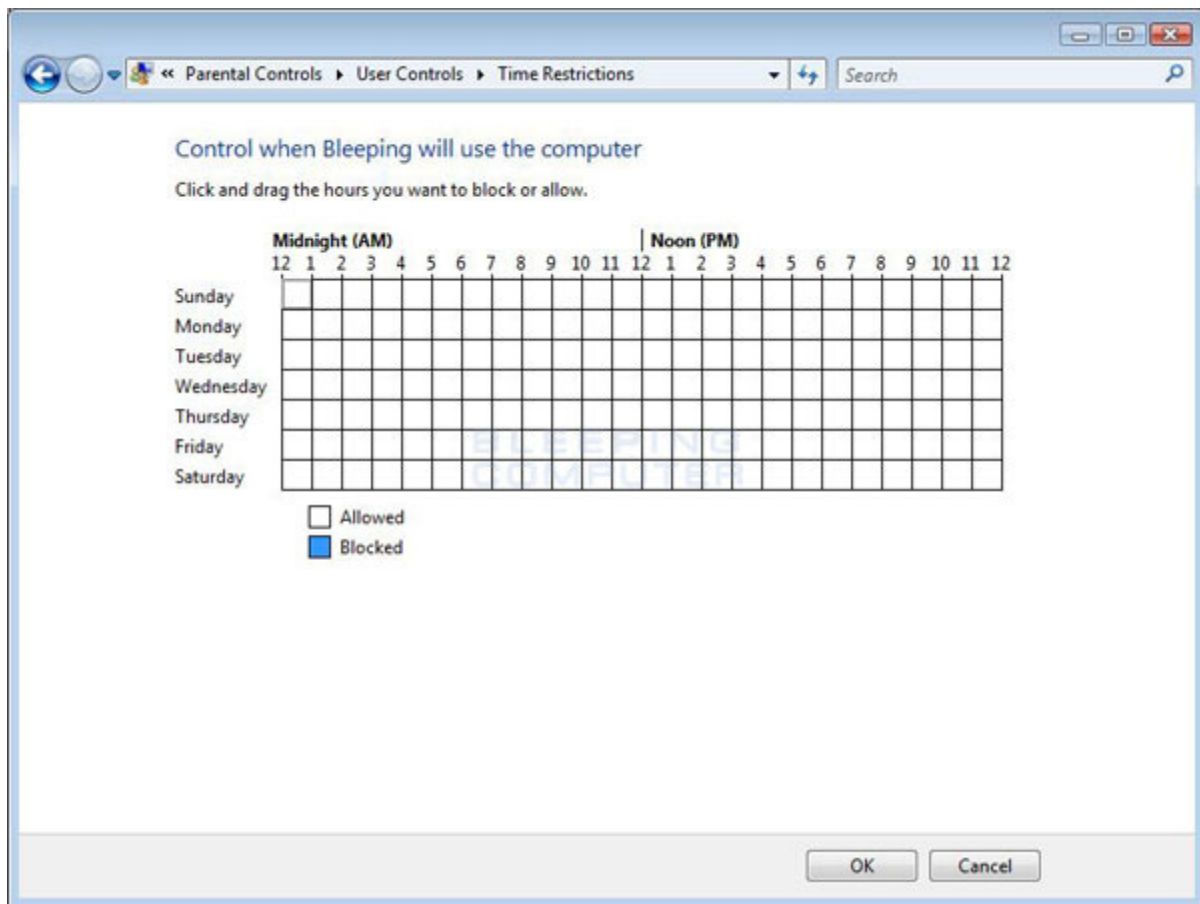


Figure 13. Time Restrictions

By default a user can log on to and use the computer at any time in the day. If you want to limit when they can use the computer you can specify using this screen the specific times they can log on. The hours are represented as individual boxes, where each box represents a specific hour on a specific weekday. If you click on a box, it turns it blue which means the user cannot log on to the computer at that particular time. To remove this restriction you simply need to click once again on the same box so it becomes white. You are also able to select multiple time restrictions at the same time. To do this left click on a box and while holding down the left mouse button, drag the pointer over the time boxes that you would like to restrict. As you highlight each box it will turn blue and block the user from logging on during that time period.

When a user attempts to log on to the computer when they are restricted they will receive the error shown below.

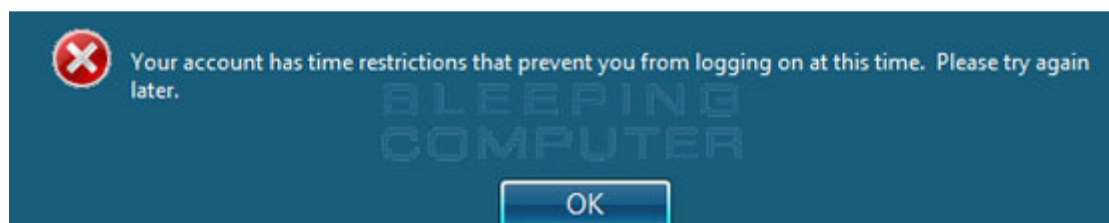


Figure 14. User is restricted from logging on to the computer

Once you have finished configuring the time restrictions for this particular user, you can save these restrictions by clicking on the **OK** button. This will bring you back to the main User Controls screen where we will now configure what types of games the user can play.

Configuring Game Restrictions

When you select the **Games** option in the Users Controls screen you will be brought to the Game Restrictions screen where you can control whether or not the user can play games and what type of games can be played.

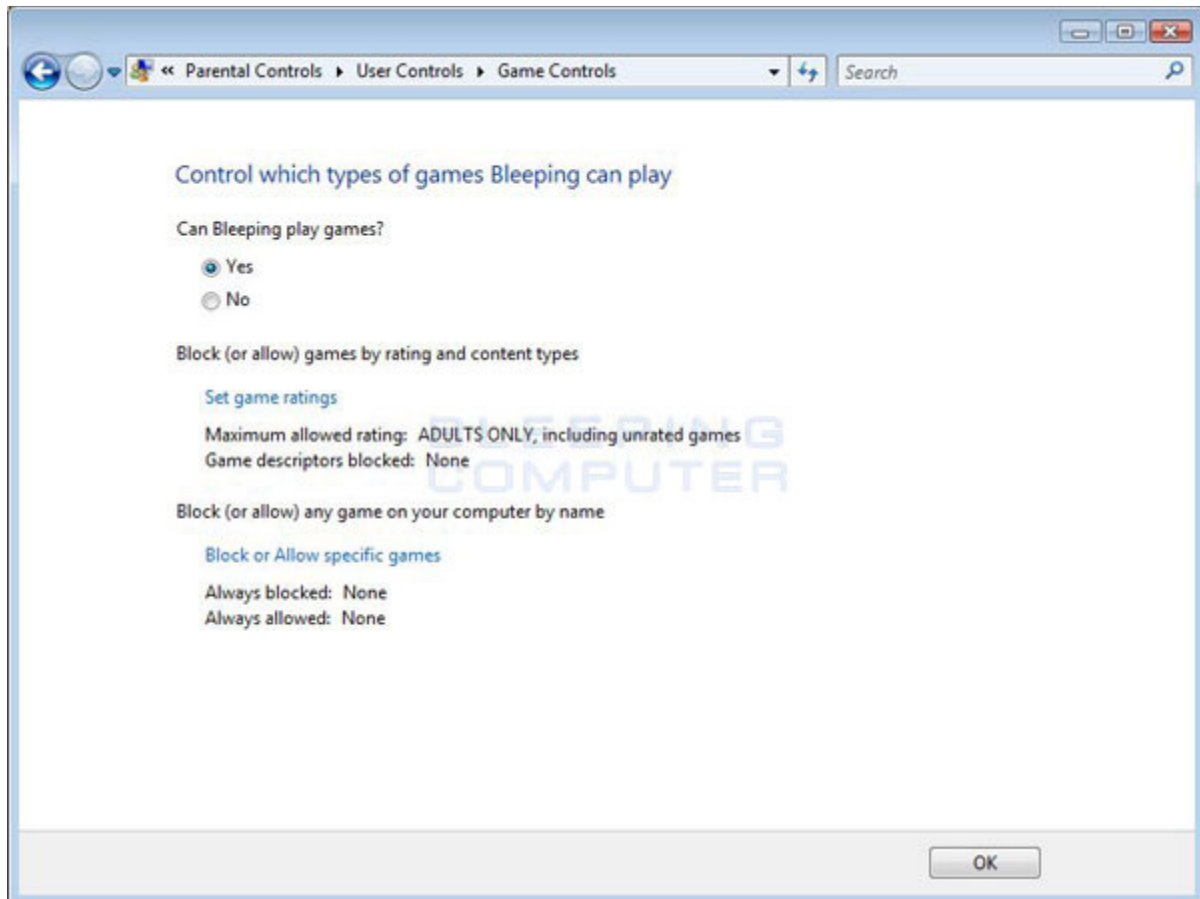


Figure 15. Game Controls Screen

By default all users with Parental Controls can play games of any content level. To disable access to games you can select **No** under the **Can username play games?** category. If you want to allow this user to play games, you can specify the maximum content rating of a game that the user can play, by clicking on the **Set game ratings** option.



Figure 16. Game Restrictions

From this screen you can specify whether or not the user can play games that are not rated as well as specify the maximum content rating of a game that a user can play. When games are created they are given a rating similar to a movie rating so that a parent can determine if the game is appropriate for a child's age. Depending on what you feel is best for your child; select the rating of the games that your child can play. When selecting a rating it is important to remember that the user can play games up to and including the rating you select. Some games, for whatever reason, may not have a rating. If you want to block these types of games from being played you can select the **Block games with no rating** option. If you don't mind that the user will play games with no rating you should instead select the **Allow games with no rating** option.

To further filter games you can also select various game content that you would like a user not to be able to play. Examples of content that you can prohibit are blood, alcohol reference, drug reference, nudity, etc. These settings will override any game ratings that you select, so if you specify that you do not want the user to play games with cursing, but you allow a game rating that allows for that, the games with cursing will still not be allowed. When you are done configuring this section you would click on the **OK** button to save your changes.

You will now be back at the main Game Controls screen. From this screen we will configure the last available setting, which is for allowing or blocking specific games. By clicking on the **Block or Allow specific games** option you will come to the Game Overrides screen.

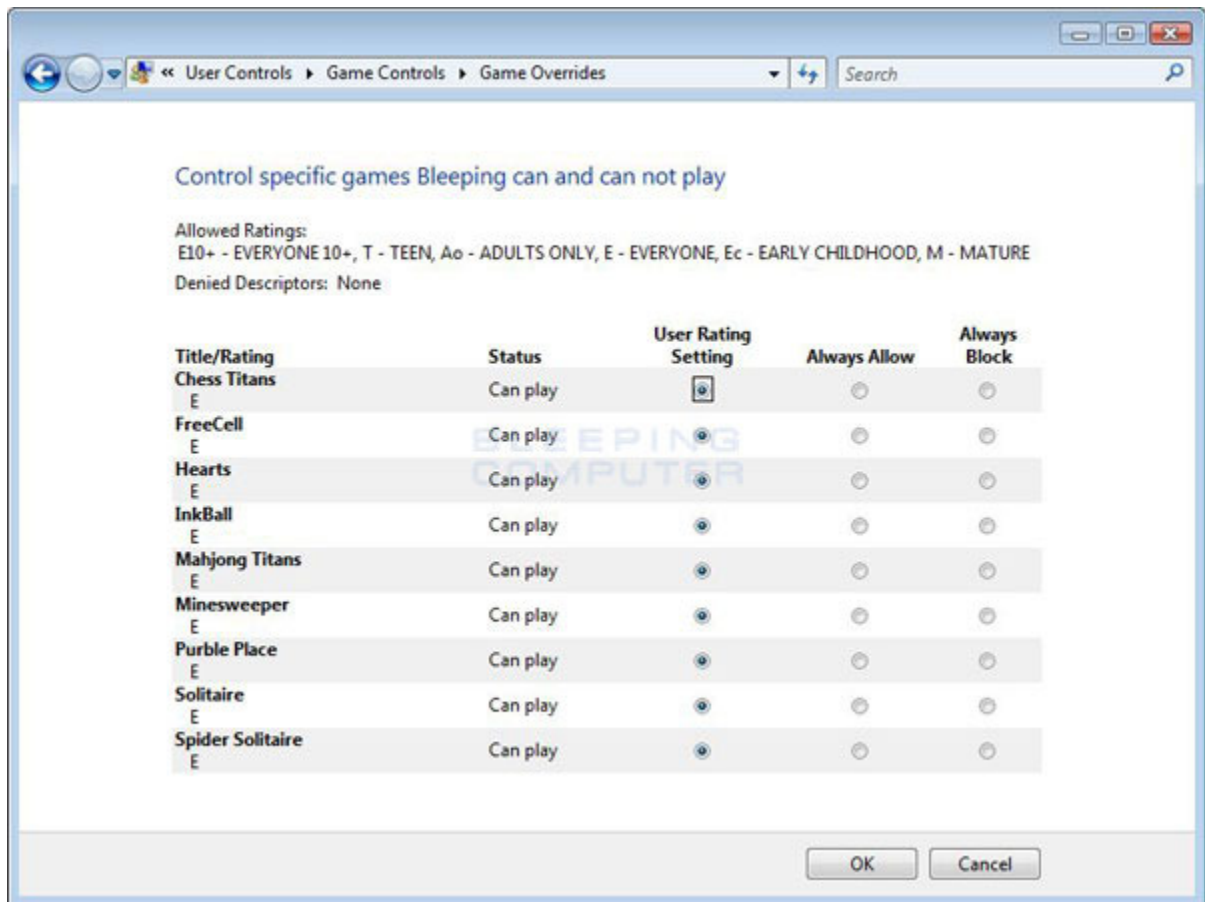


Figure 17. Game Overrides Screen

At this screen you can specify whether or not a game can be played on a per game basis. There are three options next to each game title. The first option is **User Rating Setting**, which will block the game based on the Parental Controls settings previously set. The **Always Allow** or **Always Block** settings will override the other Parental Controls settings and allow access to the game based on the choice in this screen.

When you are done configuring this screen, you can press the **OK** button to save your changes and bring you back to the main Game Controls screen. Now that we are done configuring game settings, we would press the **OK** button again to exit back to the User Controls screen.

Configuring what programs are allowed or are blocked

We are now at the User Controls screen and there is one last section that we have not explored. When you click on the **Allow and Block Specific Programs** option you will be brought to a screen asking if the user can use all programs or only ones that you allow. If you want the user to be able to use all of the programs on the computer you should press the **Cancel** button to exit this screen. Otherwise select the **Username can only use the programs I allow** option and Vista will scan your computer for programs and then display them in a list as shown below.

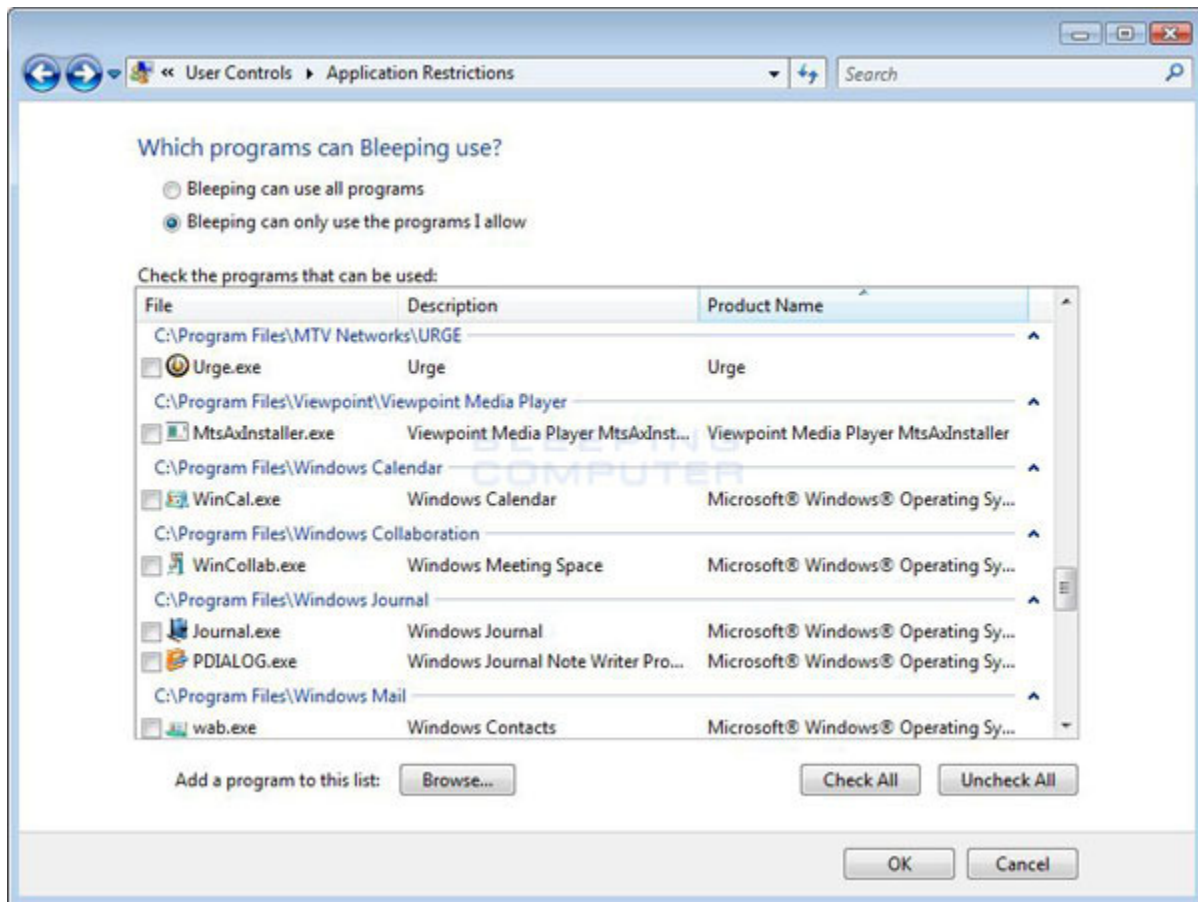


Figure 18. Application Restrictions

You can now pick and choose the specific programs that you wish to allow the user to use. To allow a program to be used, simply put a checkmark in the checkbox next to the programs name. If there is a program that is missing from the list, and you would like the user to have access to it, you can click on the **Browse** button and browse to the executable. When the executable is added it will automatically be checked. You can also select the **Check All** button to allow all the programs or the **Uncheck All** button to disallow all of the listed programs. When you are done selecting the programs you want to permit access to, click on the **OK** button to save these settings and bring you back to the User Controls screen.

Congratulations! You have now completed setting up Parental Controls for this user. As this was the last group of settings to configure for this user, you can now press the **OK** button to get back to the main Parental Controls welcome screen. You can now configure Parental Controls for any other users on your computer, or close the screen to finish this process. In the next sections we will go over some advanced material about Parental Controls. If you have no need for this material, then you can skip to the conclusion.

How to create a custom Web Allow Block Lists file (FOR ADVANCED COMPUTER USERS ONLY)

The Windows Vista Web Filter allows you to export and import lists of sites that you would like to allow or block for a particular user. These lists of sites are stored in a file called a **Web Allow Block Lists** file. These files are text files that have the extension of **.WebAllowBlockList** and contain a list of URLs. The URLs are formatted in a particular way so that the Vista Web Filter knows whether or not they should be added to the Allow or Block lists. Below we describe the format of the file so that you can make your own Web Allow Block Lists files.

The contents of all Web Allow Block Lists files start with the tag and end with the tag. In between these two tags are URL statements using the following syntax:

```
<URL AllowBlock="X">http://example.com</URL>
```

The value of the AllowBlock variable, represented by X, can either be the number **1** or the number **2**. If you specify the value of AllowBlock to be **1** then the Web Filter will add that URL into the Allow list. On the other hand if you specify the value of the AllowBlock to be **2** then the Web Filter will add that URL into the Block list.

It is also important to note that when you add URLs to the list, you can only add URLs that start with http://
Below are some example URL statements:

<URL AllowBlock="1">http://www.example.com</URL> would allow all pages that start with www.example.com/ to be accessible.

<URL AllowBlock="2">http://www.example.com/badurl/</URL> would block access to the specific URL http://www.example.com/badurl/

You can list as many URL statements as you wish as long as you use the syntax shown above and as long as they are in between the opening and the closing tags. An example Web Allow Block Lists file can be found below so that you can see the format used.

```
<WebAddresses>
<URL AllowBlock="1">http://apple.test.com/</URL>
<URL AllowBlock="1">http://test.com/test</URL>
<URL AllowBlock="2">http://mac.test.com/</URL>
<URL AllowBlock="2">http://test.com/</URL>
<URL AllowBlock="2">http://test.com/blocked</URL>
```

One frustrating issue when making a Block Lists file is that certain legitimate types of http:// URLs are not permissible in a Web Allow Block Lists file which makes it difficult to automate the conversion of existing lists of unwanted sites to this new format. The first is that you cannot use a &, ampersand, in an URL. So an URL that looks like the following is not allowed:

http://www.example.com/test.html?test=1&bad=1

When trying to import urls that contain an &, you will get an error message stating the import failed. One last caveat, which is not necessarily a problem, is that the import process will strip off the first GET variable in an URL so that it is only the specific page, without arguments, that gets added to the lists. Let's look at the following URLs list as an example:

http://www.example.com/index.php
http://www.example.com/index.php?type=.html

Both URLs are legitimate and both may perform differently when you visit them, but when you import this list, you will be notified that the URLs are redundant, the importer will strip off the arguments, and you will only be left with the single URL, **http://www.example.com/index.php**, in your block list. I understand that they are doing this so that you have a more general URL to block, but I find it strange that the import process is fine with the first variable designated by a ?, but has problems with further arguments specified with the symbol &.

Advanced Information

In this section we will touch on some advanced information as to the inner workings of Parental Controls. The configuration settings for the Parental Controls are stored in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls

Under that key are a variety of global settings, exemption lists, and the per user settings. For each user that has Parental Controls there is a subkey named for their SID, or Security Identifier, under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\Users

Under the SID subkey you will find all the settings that were configured for the user. An interesting subkey is the Web\Overrides subkey, which contains the Web Filter overrides.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\Users\S-1-5-21-2583266263-1766765975-3327590656-1004\Web\Overrides

Each value name is the particular URL in our block or allow list and the data of that value is either the number **1** or **2**, with 1 meaning the URL is allowed and 2 meaning it is blocked. These settings are obviously only accessible by an Administrator so we do not have to worry about malware running under a standard user's account modifying this information.

There are four different exclusion lists, in two categories, for Parental Controls. These lists contain URLs and programs that are white listed so that they cannot be blocked or filtered. The first category of white lists are for entries added to the list by programs so that they can update themselves, retrieve help information, or activate their products. These program writable lists are the **HttpExemptionList** and the **UrlExemptionList**. They are found at the following Registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\HTTPExemptions

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\URLExemptions

HTTPExemptions are a list of programs that are can't be blocked from accessing the HTTP protocol and URLExemptions are urls that can't be blocked by the Vista Web Filter. Below are default exemptions for a Vista Ultimate installation.

HTTPExemptions

C:\Program Files\Windows Media Player\Wmprph.exe
C:\Program Files\Windows Media Player\Wmpnscfg.exe
C:\Program Files\Windows Media Player\Wmlaunch.exe
C:\Program Files\Windows Media Player\Wmpenc.exe
C:\Program Files\Windows Media Player\wmpplayer.exe
C:\Program Files\Windows Media Player\Wmpsideshowgadget.exe
C:\Program Files\Windows Media Player\Wmpnetwk.exe
C:\Program Files\Windows Media Player\Wmpshare.exe
C:\Program Files\Windows Media Player\Wmpconfig.exe

URLExemptions

<http://services.wmdrm.windowsmedia.com>
<http://preview.services.wmdrm.windowsmedia.com>
<http://drmlicense.one.microsoft.com>

The second type of white list is read-only and is a list of Windows programs and URLs that are required for proper Windows functionality. These entries cannot be added or removed by standard means and will most likely only be altered via future Windows updates. The Registry keys associated with these white lists are:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\WinHTTPExemptions

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\WinURLExemptions

WinHTTPExemptions are a list of programs that are can't be blocked from accessing the HTTP protocol and WinURLExemptions are urls that can't be blocked by the Vista Web Filter. Below are default exemptions for a Vista Ultimate installation.

WinHTTPExemptions

C:\\Windows\ehome\ehrec.exe
C:\\Windows\HelpPane.exe
C:\\Windows\ehome\McUpdate.exe

WinURLExemptions

http://www.microsoft.com/windowsvista/images/lockedout_uncompressed48.png
<http://wer.microsoft.com>
<http://oca.microsoft.com>
<http://www.microsoft.com/library/media/1033/windowsvista/images/shield.png>
<http://images.metaservices.microsoft.com>
<http://games.metaservices.microsoft.com>
<http://go.microsoft.com/fwlink/>

Conclusion

Now that you understand how to use Vista's Window Parental Controls, it is possible to create a safe and productive environment for the children in your household. It is particularly comforting knowing that the Windows Parental Controls team envisioned that what one parent may find offensive, another may not, and thus provided us a set of tools that we can customize to fit our own requirements.