



User Manual

COPYRIGHT® 2011 BSECURE® TECHNOLOGIES, INC ALL RIGHTS RESERVED.

Copyright in these pages and the material contained herein and their arrangement are owned by Bsecure® Technologies, Inc. and/or its affiliates, unless otherwise indicated.

In addition, the materials contained herein may be Bsecure® Proprietary and/or Trade Secret information and may not be copied, compiled, or distributed without the prior written consent of Bsecure.

PERMITTED USE:

Any person is hereby authorized to view this information for informational purposes only. However, the text and images resident herein may not otherwise be copied, modified, distributed, reproduced, or reused without the express written permission of Bsecure® Technologies, Inc.

Please direct any inquiries related to the use of this material to:

**Bsecure Technologies, Inc.
PO Box 1149
Fort Walton Beach, FL 32549-1149**

TABLE OF CONTENTS

SECTION A - GETTING STARTED	1
Thanks for choosing Bsecure Online	2
Ultimate Online Family Protection	2
Internet Filter for Windows	2
Internet Filter plus McAfee Anti-Virus.....	2
Major Features and Advantages.....	3
Installation	6
Control Panel	8
Services Tabs.....	9
Profile Management.....	9
Feature Tabs	13
Configuration Window	15
Whole Home Filtering.....	15
SECTION B - ACTIVITY MONITORING	18
Activity Monitoring.....	19
Summary Report.....	20
All Sites	21
Social Sites	23
Searches.....	25
Instant Messages	26
Programs.....	26
Alert Log.....	27

SECTION C - PARENTAL CONTROLS	29
Parental Controls	30
Categories	31
Media	42
Block Sites	46
Allow Sites	48
Options	49
Block / Warn / Monitor	50
Password Override	52
Secondary Password	53
Safe Search	53
Safety Lock Option	55
File Extension Blocking	57
iCat (Intelligent Contextual Analysis Technology)	58
Access Times	60
Alerts	61
Programs	64
SECTION D – SECURITY	67
Security	68
Manual Scan	70
Scheduled Scan	71
Scan History	73
Options - Definition Updates	74

Automatic Definition Updates	74
Manual Definition Updates.....	75
Threat Library	76
SECTION E - HOW TO	78
How to add a profile	79
How to add a site to the allow sites list.....	80
How to add a site to the block sites list.....	81
How to allow media using ratings	82
How to apply changes to all profiles	83
How to assign a profile	84
How to block access to select programs on your PC.....	85
How to block explicit music (iTunes only)	86
How to block media using ratings	87
How to block uncategorized websites.....	88
How to create a secondary password	89
How to create a limited user account	90
How to create a white list.....	91
How to delete a computer.....	92
How to edit a profile.....	93
How to edit a scheduled scan.....	94
How to restrict Internet access times.....	95
How to manually update anti-virus files.....	96
How to monitor a profile in silent mode	97

How to perform a manual virus scan	98
How to remove a profile.....	99
How to remove a scheduled scan.....	100
How to remove a site from the allow sites list.....	101
How to remove a site from the block sites list	102
How to schedule an automatic virus scan.....	103
How to setup email alerts.....	104
How to setup text (SMS) alerts.....	105
How to turn off activity monitoring.....	106
How to turn off the iCat feature.....	107
How to turn on the safe search feature	108
How to turn off the safe search feature	109
How to turn off social site reporting	110
How to assign a profile for Whole Home Filtering (WHF).....	111
How to manually setup your router for Bsecure Online WHF Services	112
How to restrict Whole Home Filtering (WHF) Internet access times	113
How to setup Whole Home Filtering (WHF) text (SMS) alerts	114
How to setup Whole Home Filtering (WHF) email alerts	115
How to turn on Whole Home Filtering (WHF)	116

SECTION A

GETTING STARTED

THANKS FOR CHOOSING BSECURE ONLINE

Ultimate Online Family Protection

Since 2001, Bsecure[®] Online has been the most endorsed and trusted provider of Internet protection software for the family. More than just an advanced technology provider, we are parents too and understand what it takes to protect your loved ones in this complex world.

Bsecure Online's new version 6.1 offers a host of new innovative and patented safety features to go with our simple installation and easiest-to-use software on the market today. Our new browser based control panel and “in the cloud” managed services keep you automatically updated with the latest protection features.

Internet Filter for Windows

As a cloud-based solution, Bsecure CloudCare helps take the load off your computers, which results in extremely fast response times not seen with traditional parental controls. Bsecure CloudCare offers accuracy and flexibility with an industry leading 61 categories that are automatically selected based on the age appropriate group.

Internet Filter plus McAfee Anti-Virus

This manual also supports customers who have chosen the optional McAfee[®] Anti-Virus upgrade. Bsecure CloudCare 6.1 integrates the advanced McAfee[®] VirusScan[®] engine into its parental controls system interface - for much less than the cost of stand-alone security.

Major Features and Advantages

- **Internet Web Filtering** – With continuous and automatic updates, Bsecure CloudCare 6.1 uses a database of 62 million URLs representing hundreds of millions of Web pages. Our servers are updated with an average of 20,000 URLs, programs, keywords and acronyms daily to provide comprehensive protection that keeps pace with the dynamic nature of the Internet. An industry leading 61 categories provide unprecedented ability to custom tailor settings to your needs. Text and email alerts notify parents when pages are blocked at home. Our reporting module allows easy monitoring of online activity for Web, search, Social Networking, PC applications and IM chats remotely.
- **SafeSearch Feature** – Filters search inquiries for major search engines Bing, Google, Yahoo and YouTube. Includes image and video searches and works with all browsers.
- **SafeSurf Protection** – Bsecure CloudCare blocks access to dangerous sites containing Malware, Spam and Phishing applications. These applications can infect your computers and steal your family's personal and financial information.
- **Ease-of-Use** – Bsecure CloudCare installs in less than 10 minutes with out-of-the-box protection. Our new setup wizard makes it easy to set up age appropriate templates for all members of the family.
- **Graphical “Cloud” Interface** – Maps users and devices with a flexible and intuitive user interface. Parents can easily customize all settings from anywhere using the new browser based control center. Easily change default options, add and delete custom URLs, programs, time schedules and much more...
- **New 6.1 Social Network Safety** – Provides a clear window into your child's social networking world. Bsecure CloudCare has the most comprehensive parental monitoring for Facebook, Twitter, MySpace, Bebo and 75 other sites including web based chat, Instant Messaging and other types of social sites.

Text and email alerts give parents a warning on potential trouble, then allows the parent to automatically view the child social accounts without needing to know usernames and passwords.

- **New 6.1 Whole Home Filtering** – Exclusive Whole Home option for routers filters any device that enters your home, without the need to install software. Devices like Wii's, smartphones, laptops, Apple and others with browsers are all filtered for search and web sites.
- **Improved 6.1 Online Video Filtering** – Bsecure CloudCare offers the most wide-ranging and accurate filtering of online TV shows and movies based on industry MPAA ratings. Includes coverage for most major online media sites as well as iTunes music filtering. Also restricts iTunes explicit music.



- **Web Game Filtering** – Online gaming sites are automatically filtered for mature content by age group using industry standard ESRB ratings.



- **Block, Warn, or Monitor Options** – This new option allows the administrator to select how to manage and control access to blocked sites. Choose from blocking entirely, posting a warning but allowing access, or simply recording surf history without block pages, Bsecure CloudCare also includes an option for in-page password override.
- **Tamper-Resistance** – Bsecure CloudCare plugs secret workarounds used by tech savvy teens. For example, our exclusive “3 strikes and out” feature that locks the PC if your child tried multiple attempts to visit prohibited sites.
- **Program/Application Blocking** – Bsecure CloudCare lets you easily see and control which programs your family is using. Includes popular email programs, peer-to-peer applications, VPN clients, instant messaging, PC games, proxies and file-sharing software.

- **Time Management** – Parents can easily set time schedules for individual children or across the entire group with our graphical 24 x 7 calendar.
- **Compatibility** – Bsecure CloudCare works from anywhere in the world with any existing Internet connection (dial-up, DSL, cable, satellite).
- **Security** – For less than half the cost of stand-alone security, Bsecure integrates industry-leading McAfee[®] VirusScan[®] Anti-Virus and Spyware Protection into our CloudCare interface. With continuous and automatic updates, McAfee[®] ensures that you're running the most current security to combat thousands of new daily threats on the Internet.
- **Convenience** – Automated-server-side updates along with the Web-based control center makes managing the Bsecure Services a snap.
- **Accuracy** – Our multiple threat database libraries are developed with patent-pending technology and also include human review to reduce false positives.
- **Advanced Reporting** – Bsecure CloudCare offers powerful graphical reporting that is tamper proof and easy to access from any browser, even when on the road. Also, suspicious activities on web, search and social networking sites are flagged by parental alerts using text messages or email.
- **Mobile Device Protection** – FREE web filtering protection for the Apple iPad / iPhone / iTouch devices. Wherever your child travels, the filter app is automatically updated with extensive site lists on cloud servers. When used with a paid account, can be synchronized and managed from the Bsecure Web-based control center.
- **Adult Accountability Option** – Bsecure CloudCare's Accountability option is designed for the many adults who don't want to be tempted or have already struggled with Internet temptations. This option provides online transparency – alerts, reports and administrator rights are sent to the accountability partner of choice.

Installation

1. Purchase the Filter from the Bsecure Web site, www.bsecure.com.
2. **Print this page** (Figure A.1) - it contains valuable information that you will need for future reference.
3. Click the Install Now button.

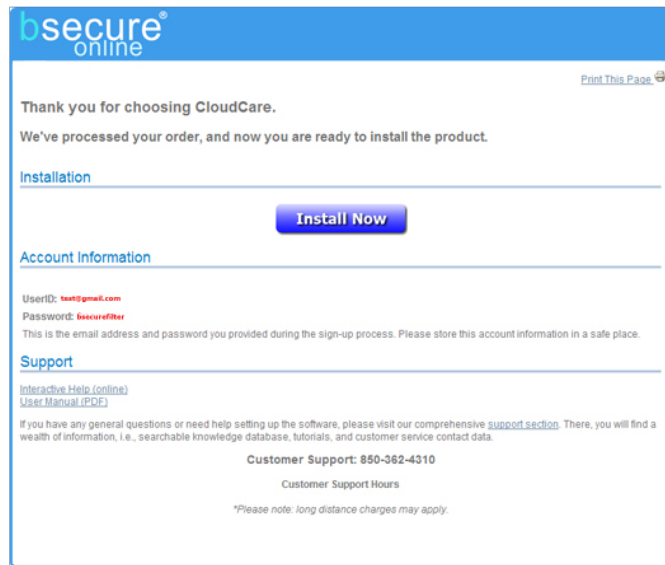


Figure A.1: Installation Print Page 1

4. Choose the level of filtering protection that you would like:
Fully customizable filtering - This option makes you the administrator with a password and complete flexibility to customize settings, to uninstall, and to override the filter.
Accountability Option - This option is for purchasers, who for various reasons do not want the ability themselves to customize, bypass, or “get around” the filter.
Note: We give you the choice to use a trusted friend, spouse or counselor as an accountability partner (recommended), OR we also give you the option to have Bsecure keep the administrative password for you. The **Accountability Option** requires you to contact your accountability partner or Bsecure's support staff to turn off filtering, unblock web sites, or uninstall the product.

5. Choose Configuration Settings:

Default settings (quick setup) - This option will filter all users under one group default profile. This group default is simpler to manage and will automatically be assigned to all Windows users accounts.

Note: You still have the option to set up individual users later if you so desire.

Individual Profiles - This more powerful option will allow the creation of custom profiles for each user individually (Requires Windows user accounts).

Note: This option allows you the most flexibility in setting differing levels of filtering based on users' ages, users' access needs, specifying time of day restrictions. While it requires Windows User Accounts don't let that deter you as we will help you create them automatically.

6. Click Next.

7. **Print this page** (Figure A.2) - instructions for loading the product on additional computers.

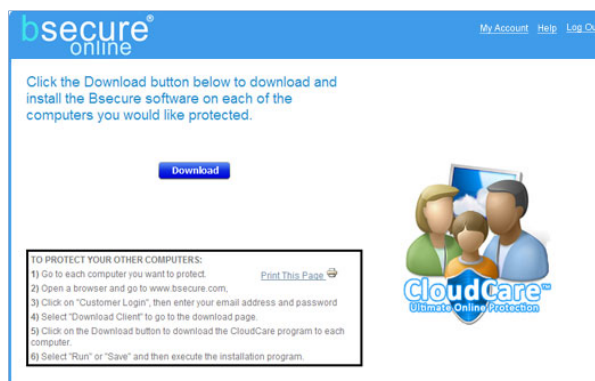


Figure A.2: Installation Print Page 2

8. Click the Download button to begin.



9. After the download and installation, you will need to restart your computer for the changes to take effect.

Note: If you choose to save the Bsecure.exe rather than run it, the file is time-stamped and is only valid for seven days from the download date.

Control Panel

The Internet Protection Control Panel is where you go to customize and configure all your Bsecure Online Internet Protection services. The main page of the Control Panel is the Activity Monitoring Summary Report. The diagram below (Figure A.3) displays the primary areas you will use to customize your Internet Protection Services.

To open the account login page:

1. Double click on either the desktop  or system tray icon  10:06 AM, to open the account login page.
2. Enter your customer login and password and click the login button.
3. Click on the Manage Services link to open the Control Panel.

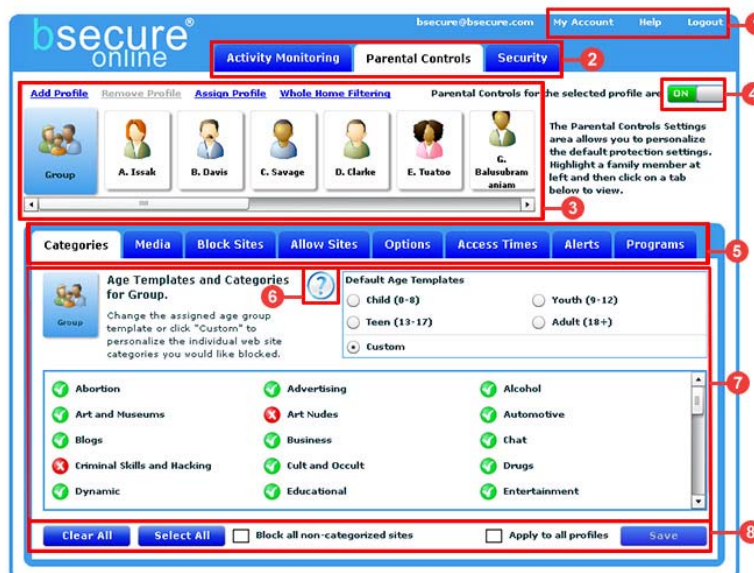


Figure A.3: Control Center Diagram

1. Navigation Panel
2. Service Tabs
3. Profile Management Section
4. Feature on/off switch
5. Feature Tabs
6. Feature Help Button
7. Configuration Window
8. Action Buttons

Services Tabs

The Services Tabs, located at the top of the Control Panel, is where to access and manage the various features for Activity Monitoring, Parental Controls, and Security services.

- Select the **Activity Monitoring tab** to view the activity reports and configure the following Activity Monitoring features: *Summary Report, All Sites, Social Sites, Searches, Instant Messages, Programs, and Alert Log.*
- Select the **Parental Controls tab** to customize and manage the following Parental Control features for each profile: *Categories, Media, Block Sites, Allow sites, Options, Access Times, Alerts and Programs.*
- Select the **Security tab** to manage or view the following security features: *Manual Scan, Scheduled Scan, Scan History, Options, Threat Library.*

Profile Management

The Profile Management section (Figure A.4) is where you create and manage the profiles for your internet protection services. This is also where you setup and modify your **Whole Home Filtering (WHF)** settings. The user setting that is highlighted in blue is the profile that will be affected by any saved changes.

Note: To prevent tampering and for added computer security, Bsecure recommends setting up limited user accounts (see ***How to create a limited user account***) in Windows and assigning them to individual profiles.



Figure A.4: Profile Management


To add a profile:

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **add profile** link, this will open the "create new settings profile" panel (Figure A5).
3. Enter a name for the new profile (**required**).
4. Enter a brief description for the new profile (optional).
5. Select an age group from the **age template initial settings** dropdown menu.
6. Select the icon you would like to use for the new profile. The icons can be displayed by groups, male, female, adult, teens, youth, and child. *For example, you can choose to only view male - teen icons.*
7. Click the **save button** to save your new profile.

Figure A.5: Add a Profile

To remove a profile:

1. Select either the **Activity Monitoring or Parental Controls tab** from the "Services tabs."
2. Select the profile that you would like to remove.

Note: The administrative profile cannot be removed. However, it can be renamed by clicking on the  icon, located in the top left corner of the selected profile.

3. Select the **red X** in the upper right corner of the profile's icon.
4. Click the **Yes button** to confirm the deletion of the selected profile (Figure A.6).

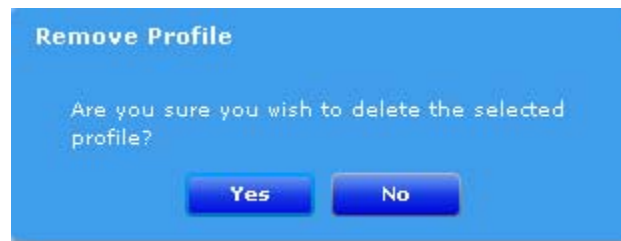




Figure A.6: Remove a profile

To edit a profile:

1. Select either the **Activity Monitoring or Parental Controls tab** from the "Services tabs."
2. Select the profile that you would like to edit.
3. Click the  icon in the upper left corner of the selected profile.
4. Enter a **new name and/or brief description** for the profile (Figure A.7).
5. Click the **save button** to preserve your changes.



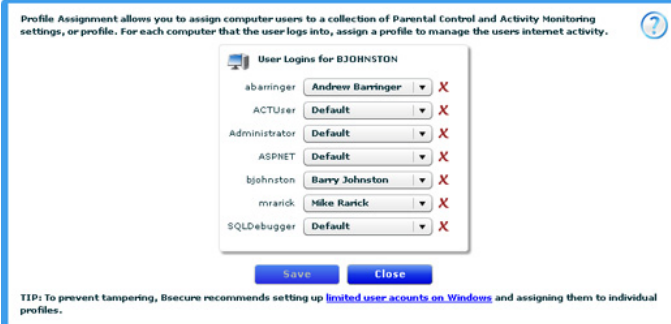
The 'Edit Profile' dialog box contains the following elements:

- Title:** Edit Profile
- Fields:**
 - 'Please enter a name for this settings profile' with a text box containing 'D. Clarke'.
 - 'Please enter a brief description' with an empty text box.
 - 'Please select an icon' with two 'All' dropdown menus.
- Icon Selection:** A horizontal row of 12 user icons, each with a small circular selection button below it.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Figure A.7: Edit a Profile

To assign a profile:

1. Select either the **Activity Monitoring** or **Parental Controls tab** from the "Services tabs."
2. Select the **assign profiles** link.
3. When there are **two or fewer devices**, listed are all the manageable devices and their logins. Click the drop down arrow next to the corresponding system / device login to select & assign one of the established profiles (available profiles will be visible in the profile management section, Figure A8).



The 'Assign Profile' dialog box includes the following information:

- Header:** Profile Assignment allows you to assign computer users to a collection of Parental Control and Activity Monitoring settings, or profile. For each computer that the user logs into, assign a profile to manage the users internet activity.
- Table:**

User Logins for BJOHNSTON		
abarringer	Andrew Barringer	X
ACTUser	Default	X
Administrator	Default	X
ASPNET	Default	X
bjohnston	Barry Johnston	X
mrarick	Mike Rarick	X
SQLDebugger	Default	X
- Buttons:** 'Save' and 'Close' buttons.
- Footer:** TIP: To prevent tampering, Bsecure recommends setting up [limited user accounts on Windows](#) and assigning them to individual profiles.

Figure A.8: Assign a Profile

When there are **three or more devices**, select the device from the list and then select the login to assign a profile, Figure A.9.

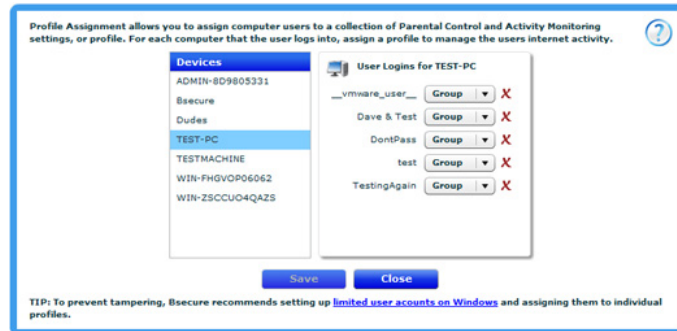


Figure A.9: Assign a Profile, three or more devices

4. Click the **save button** to preserve your changes.

Feature Tabs

The Feature Tabs are located in the middle of the Control Panel. This is where you manage the "features" that are available for each Service.

- The **Activity Monitoring tab** is where to go for the reporting feature of Bsecure Online. The reporting module allows for easy monitoring of online activity for Web, application and IM chats remotely.
 - **Summary Report** - Where to review reports of Web access history.
 - **All Sites** - Where to review Web access history for all sites visited.
 - **Social Sites** - Where to review Web access history for social sites visited.
 - **Searches** - Where to review Web search history.
 - **Instant Messages** - Where to review Instant Message activity.
 - **Programs** - Where to review program access history.
 - **Alert Log** - Where to review alerts history.

- The **Parental Controls tab** is where to go to customize and manage your filter settings.
 - **Categories** - Where to select the list of blocked categories. You may choose a template setting based on age group or customize a list to suit your personal needs.
 - **Media** - Where to manage and restrict a profile's access to media content on the internet.
 - **Block Sites** - Where to create customized lists that enable you to block specific Web sites by URL and helps control content filtering more specifically. Also, where to block all uncategorized Web sites (URL's).
 - **Allow Sites** - Where to create customized lists that enable you to allow specific Web sites by URL and helps control content filtering more specifically. This lets you access a Web site without having to unblock the category it falls under. Also where to create a "white list."
 - **Options** - Where to manage password override, safety lock, block/warn monitor, and file extension filter.
 - **Access Times** - Where to control Internet access for the entire network or individual computer profiles. Web browsing can be controlled by time of day and each day of the week when this feature is enabled.
 - **Alerts** - Where to manage alert delivery.
 - **Programs** - Where to manage access to select programs on your PC.
- The **Security tab** is where to go to manage the McAfee[®] VirusScan[®] service.
 - **Manual Scan** - Where to perform manual Anti-Virus & Anti-Spyware scans.
 - **Scheduled Scan** - Where to manage scheduled Anti-Virus scans.
 - **Scan History** - Where to view scan history.
 - **Options** - Where to manage virus and spyware definition updates.
 - **Threat Library** - Where to access current knowledge about threats from McAfee Avert Labs.

Configuration Window

The Configuration Window, pictured below in Figure A.10, is where you manage your feature settings. These settings can be customized for each profile.

Age Templates and Categories for Group.

Change the assigned age group template or click "Custom" to personalize the individual web site categories you would like blocked.

Default Age Templates

☐ Child (0-8) ☐ Youth (9-12)

☐ Teen (13-17) ☐ Adult (18+)

☒ Custom

<input checked="" type="checkbox"/> Abortion	<input checked="" type="checkbox"/> Advertising	<input checked="" type="checkbox"/> Alcohol
<input checked="" type="checkbox"/> Art and Museums	<input checked="" type="checkbox"/> Art Nudes	<input checked="" type="checkbox"/> Automotive
<input checked="" type="checkbox"/> Blogs	<input checked="" type="checkbox"/> Business	<input checked="" type="checkbox"/> Chat
<input checked="" type="checkbox"/> Criminal Skills and Hacking	<input checked="" type="checkbox"/> Cult and Occult	<input checked="" type="checkbox"/> Drugs
<input checked="" type="checkbox"/> Dynamic	<input checked="" type="checkbox"/> Educational	<input checked="" type="checkbox"/> Entertainment

☐ Block all non-categorized sites ☐ Apply to all profiles

Figure A.10: Configuration Window



Whole Home Filtering

The Bsecure Online Whole Home Filtering (WHF) service provides content filtering of any network device behind a home network router that has been properly configured to interface with the Bsecure Online filtering services. Simply assign a profile to your home network router (Figure A.11), and you are ready to manage the filter services for your whole home network. **WHF includes:** Filtering by Category, Custom Block sites, Custom Allow sites, Access Times per device, Reporting of All Sites visited, and Alerts.



Figure A.11: Whole Home Filtering Panel

To turn on Whole Home Filtering (WHF):

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **Whole Home Filtering** link; this will open the "WHF" panel.
3. Click the red OFF indicator  to display the green ON . The WHF feature is now enabled.
4. Choose the profile setting that you would like to assign to the WHF network. This can be any of the already established profiles or you can create a "new" profile specifically for your WHF. Use the **add profile link** to create a new profile.
5. Enter your username and password for your home network's router.
6. **Click Save** to preserve your settings.

Note: If you change routers, you will need to reestablish your WHF settings.

To setup WHF text (SMS) alerts:

1. Select the **Parental Controls** tab from the "Services tabs."
2. Select the profile that you assigned on the WHF setup panel.
Note: If you have not already done so, you may want to setup an exclusive profile for WHF.
3. Select the **Alerts** tab from the Features tabs.
4. Verify that **Parent Alerts** is **turned on**.

5. **Enter** a mobile phone number in the text box provided under the mobile number section. Be sure to include the area code.
6. **Select** your mobile carrier from the list provided.
7. **Click** the add button to add the number to your mobile number list.

To add an SMS number, type it in here, then click **Add**

<input type="text"/>	7-11 Speakout (US) ▼	Add
----------------------	----------------------	------------

8. **Repeat** steps 5 thru 7 for each mobile number that you would like to setup.
9. Select the "**Send test message**" box in order to verify your SMS alerts setup.
Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.
10. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

<input checked="" type="checkbox"/> Apply to all profiles
--

To setup WHF email alerts:

1. Follow steps 1 – 4 above.
2. **Enter** the email address in the text box provided under the email address section.
3. **Click** the add button to add the email address to your email list.

To add an e-mail address, type it in here, then click **Add**

<input type="text"/>	Add
----------------------	------------

4. **Repeat** steps 2 and 3 for each email address that you would like to have receive alerts.

SECTION B

ACTIVITY MONITORING

Activity Monitoring

The Activity Monitoring service creates historical records, which cannot be altered or erased, of the Web sites accessed. This information is maintained in a calendar format for up to two weeks. Archived reports contain the profile, date, Web site visited (with active link), Web page visited (with active link), Web site category, search terms and number of hits. This information can be viewed by the account administrator at any time by logging in to the Bsecure Online control center, *see Figure B.1*.

Note: Only 2 weeks of report data will be stored on the Bsecure server.

Before you can begin to use the Activity Monitoring feature, make sure you have the feature turned on.

To enable activity monitoring:









1. Double click the Bsecure Online desktop  or system tray  icon.
2. Enter your login information to access the control panel.
3. Select the Activity Monitoring tab from the "Services tabs."
4. Select the **profile** that you would like to view.
5. Click the red OFF  indicator to display the green ON . The Activity Monitoring feature is now enabled for the selected profile.



Figure B.1: Activity Monitoring Features

To disable activity monitoring:

1. Double click the Bsecure Online desktop  or system tray  icon.
2. Enter your login information to access the control panel.
3. Select the Activity Monitoring tab from the "Services tabs."
4. Select the **profile** that you would like to view.
5. Click the green ON  to display the red OFF  indicator. The Activity Monitoring feature is now disabled for the selected profile.

Summary Report

The Summary Report, Figure B.2, displays statistics and links for the most visited Web sites, most visited website categories, blocked categories, and blocked websites for the selected profile.

Note: Only 2 weeks of report data will be stored on the Bsecure server.

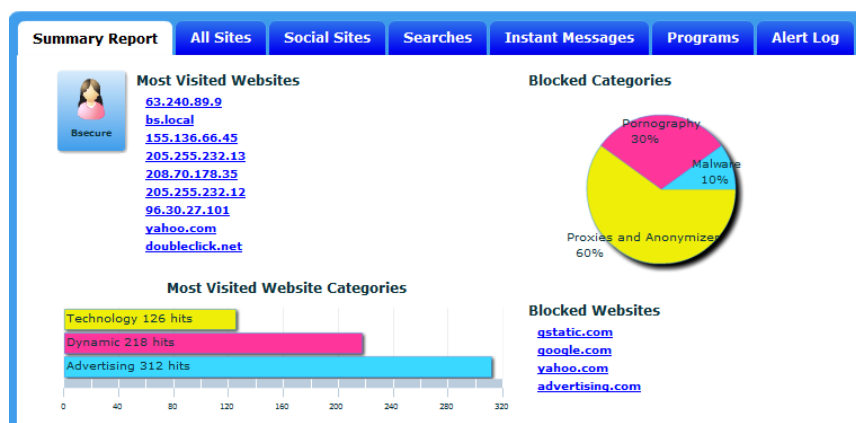


Figure B.2: Summary Report

All Sites

The All Sites section, Figure B.3, is where you can review Web access history for all sites visited by the selected profile. **Two active links will be provided in this reporting section:**

- **Site** - Links to the domain or main Web site address.
- **Page** - Links to the actual page that was visited on the Web site.

Also displayed in this report section are the **Date / Time** the site was visited, the **Category / Reason** the site was block and the number of **Hits** or visits to the site.

Block reasons that may be listed under Category / Reason are:

Category Block

The listed category is blocked for the selected profile. Use the **Categories tab** if adjustments are desired.

Schedule Block

The time schedule for the selected profile prevented internet access. If needed, use the **Access Times tab** to make adjustments.

User Block List

The blocked site is listed on the profile's **Block Sites** list. Use the Block Sites tab to make adjustments.

Uncategorized Block

The blocked site is uncategorized and the **"Block all non-categorized sites"** box is checked. Use the Categories tab to make adjustments. The check box is located on the bottom of the Categories screen.

White List Block

The blocked site is listed on the **Allow Sites** list and the White List or **"Only allow sites listed in the Allow list"** box is checked. The selected profile can only visit sites listed on the Allow Sites list if the White list box is checked. Use the Allow Sites tab to make adjustments (the check box is located at the bottom of this screen).

iCat Block

The blocked site is **uncategorized** and was **iCat** filter evaluated it as offensive. Use the Options tab to manage the iCat setting for the selected profile.

Safety Lock Block

The site was blocked because of the Safety Lock setting for the selected profile. Based on the setting, **Internet access is disabled** once a certain number of sites have been blocked. Use the Options tab to adjust the profile's Safety Lock setting.

Password Override Allow

The blocked site was allowed because the **Password Override** option is turned on and either the administrative or secondary password was provided. Use the Options tab to make adjustments to the Password Override setting.

User Allow List

The site is listed on the profile's **Allow Sites** list. Use the Allow Sites tab to make adjustments.

Filter Disabled Allow

The site was allowed because the filter has been disabled. Use the Parental Controls tab to turn on filtering and make adjustments to the selected profile's settings.






Network Error Allow

The filter server was not available. This could be caused by a firewall. Check your firewall settings.

If there is no Category / Reason listed, the site was not blocked. **To only view blocked sites**, check the box at the bottom left corner of the screen to **"Show Questionable Activity Only."**

☒ Show Questionable Activity Only

To change the time frame of the displayed data:

1. Double click the Bsecure Online desktop  or system tray  icon.
 2. Enter your login information to access the control panel.
 3. Select **Activity Monitoring** from the "Services tabs."
 4. Select the **profile** that you would like to view.
 5. Make sure the Activity Monitoring feature is turned ON .
 6. Select the **All Sites tab**.
 7. Select the desired **From** date and the desired **To** date using the calendar button .
- Click the view button  to see data for the selected range.

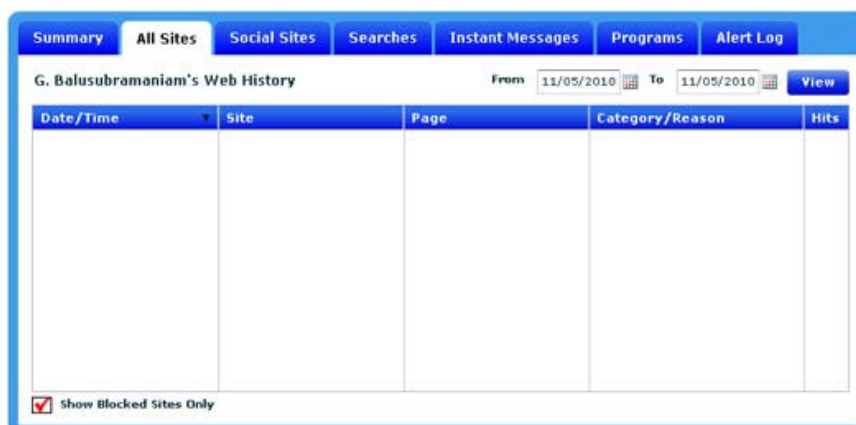


Figure B.3: All Sites History

Social Sites

This powerful reporting feature is not only displays social site access history, but it also is where parents can gain access to the Group's accounts. **Social Networking monitoring is turned off for adult profiles. When you add any teen/child profile, it is defaulted to ON.**

Two active links are provided in this section:

- **Site** - Links to the domain or main Web site address.
- **User Name** – Automatic account login.





Important notice: The social networking feature collects confidential account data and is for enabling parents to monitor their child's safety. **This feature should only be turned on for child profiles and for home computer use.**






Last Login	Site	User Name	Remove
2010/05/24 11:31 AM	www.facebook.com	facebooktest	X

Figure B.4: Social Sites History

To turn off social site filtering:

1. Double click the Bsecure Online desktop  or system tray icon .
2. Enter your login information to access the control panel.
3. Select **Activity Monitoring** from the "Services tabs."
4. Select the **Social Sites tab**.
5. Select the **profile** that you would like to manage.
6. Click the green ON indicator  to display the red OFF . The Social Site reporting feature is now disabled for the selected profile.

To log in to a profiles social site account:

1. Double click the Bsecure Online desktop  or system tray icon .
2. Enter your login information to access the control panel.
3. Select **Activity Monitoring** from the "Services tabs."
4. Select the **Social Sites tab**.
5. Select the **profile** that you would like to view.
6. Verify that the feature is ON .
7. Click the corresponding link under **User Name**, for the site that you would like to access.






Searches

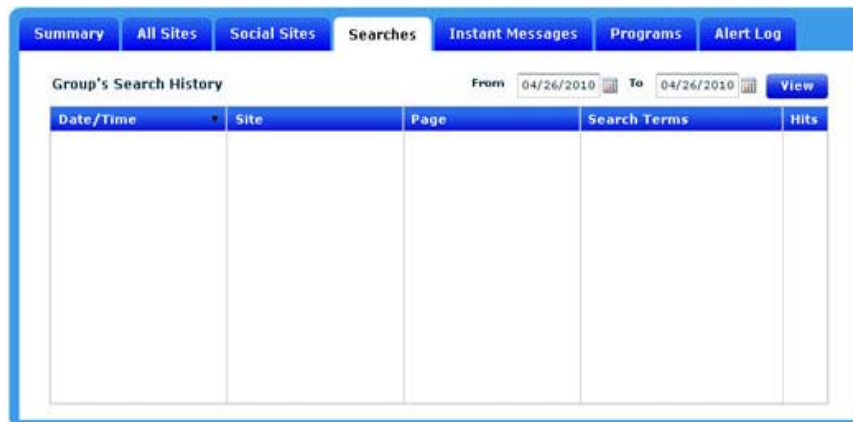
The Searches section, Figure B.5, is where you can review the search detail for Web access history. This feature may be useful in providing an early warning for potentially harmful topics that are being searched by the selected profile. **Two active links will be provided in this reporting section:**

- **Site** - Links to the domain or main Web site address.
- **Page** - Links to the actual page that was visited on the Web site.

Note: Only two weeks of report data will be stored on the Bsecure server.

To change the time frame of the displayed data:

1. Double click the Bsecure Online desktop  or system tray  icon.
 2. Enter your login information to access the control panel.
 3. Select **Activity Monitoring** from the "Services tabs."
 4. Select the **profile** that you would like to view.
 5. Make sure the Activity Monitoring feature is turned ON .
 6. Select the **Searches tab**.
 7. Select the desired **From** date and the desired **To** date using the calendar button .
- Click the view button  to see data for the selected range.



The screenshot shows the Bsecure Online interface with the 'Searches' tab selected. The page title is 'Group's Search History'. Below the title is a date range selector with 'From' and 'To' fields, both set to '04/26/2010', and a 'View' button. The main content area is a table with the following columns: 'Date/Time', 'Site', 'Page', 'Search Terms', and 'Hits'. The table is currently empty.

Date/Time	Site	Page	Search Terms	Hits
-----------	------	------	--------------	------

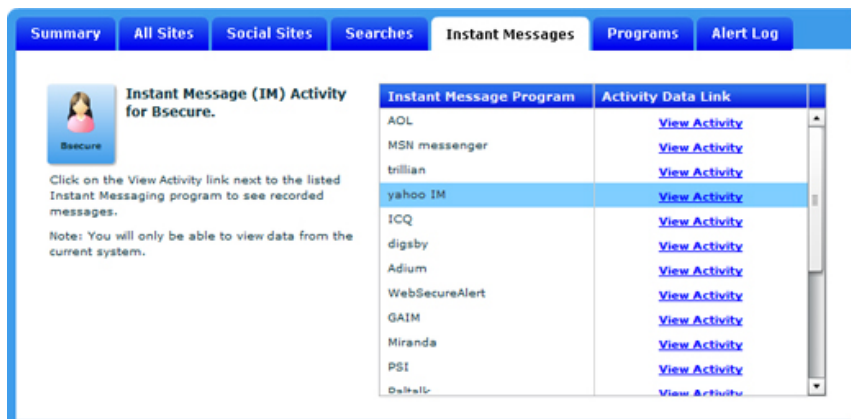
Figure B.5: Search History

Instant Messages

Instant messages are a form of real-time direct text-based communication between two or more people using an instant messaging application such as MSN messenger or yahoo IM. The text is sent using devices that are connected over a network such as the Internet.

The Instant Message activity report provides the recorded messages for various Instant Messaging programs.

Click on the **View Activity** link to see the saved conversation (Figure B.6).




Summary All Sites Social Sites Searches Instant Messages Programs Alert Log						
 Instant Message (IM) Activity for Bsecure. Click on the View Activity link next to the listed Instant Messaging program to see recorded messages. Note: You will only be able to view data from the current system.						
Instant Message Program			Activity Data Link			
AOL			View Activity			
MSN messenger			View Activity			
trillian			View Activity			
yahoo IM			View Activity			
ICQ			View Activity			
digsby			View Activity			
Adium			View Activity			
WebSecureAlert			View Activity			
GAIM			View Activity			
Miranda			View Activity			
PSI			View Activity			
Dialer			View Activity			






Figure B.6: Instant Message History

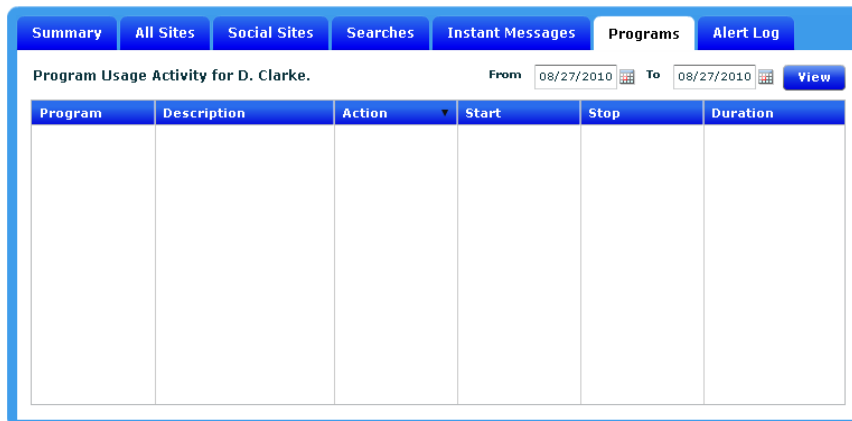
Programs

The Programs section, Figure B.7, is where you can view the program access history for selected profile.

Note: Two weeks of programs report data will be stored on the Bsecure server.

To change the time frame of the data being displayed:

1. Double click the Bsecure Online desktop  or system tray  icon.
 2. Enter your login information to access the control panel.
 3. Select Activity Monitoring from the "Services tabs."
 4. Select the **profile** that you would like to view.
 5. Make sure the Activity Monitoring feature is turned ON .
 6. Select the **Programs tab**.
 7. Select the desired **From** date and the desired **To** date using the calendar button .
- Click the view button  to see data for the selected range.



Program	Description	Action	Start	Stop	Duration

Figure B.7: Program Usage History

Alert Log

The Alert Log is where you can view the history of all alerts sent for the selected profile. An alert will be sent when a profile user attempts to access a Web site categorized as pornography and when a keyword or phrase is used on most social sites.

- **Pornographic websites** - when pornographic site access is attempted, an alert will be sent and the alert log will record the following (**Parental Controls** and **Alerts** must be turned on and at least one email address or mobile number must be provided):

- date and time the attempt was made
 - a link to the pornographic site
 - the site category
- **Keywords Filtering** - when any one of the many **keywords or phrases** is used on most Web sites categorized as social sites, and alert will be sent and the alert log will record the following information (**Parental Controls** and **Alerts** must be turned on and at least one email address or mobile number must be provided):
 - date and time the keyword or phrase was used
 - the social site used on
 - the keyword or phrase used
 - the context in which it was used

Note: The email address provided during registration is the default for all alerts.

Date/Time	Site	Category
2010/06/09 02:25 PM	playboy.com/	Pornography
2010/06/09 02:25 PM	playboy.com/	Pornography
2010/06/09 02:20 PM	playboy.com/	Pornography
2010/06/09 02:20 PM	playboy.com/	Pornography
2010/06/09 02:19 PM	playboy.com/	Pornography

Date/Time	Site	Keyword	Used in Context
2010/06/03 03:26 PM	Facebook	crapola	what a piece of crapola
2010/06/03 03:24 PM		crap	what a piece of crap
2010/06/03 03:23 PM		junk	check out this junk, dude

Figure B.8: Alert Log

SECTION C

PARENTAL CONTROLS

Parental Controls

Parental Controls is a service that protects your home from the dangers of the Internet while giving you flexible control over Web sites and Internet application usage. The flexibility allows for a custom level of filtering sites and protects against dangerous sites infected with spyware or malware.

The ability to create customized lists enables you to block or allow specific Web sites by URL and create White Lists (list of specified "only allow" Web sites) if desired to control content filtering more specifically.

Note: While the Bsecure filter is continually being updated, no filter can guarantee 100% effectiveness. In addition, there are a number of Web sites that are uncategorized, or have overlapping categories.

Use the parental controls panel to manage the following filter settings:

- **Categories** - Where to assign age templates or manage the Web site categories that you would like blocked for your profiles.
- **Media** - Where to manage the accessibility of online media content using industry standard ratings.
- **Block Sites** - Where to create and manage a custom list of Web sites that you would like to block for your profiles.
- **Allow Sites** - Where to create and manage a custom list of Web sites that you would like to allow settings for your profiles.
- **Options** - Where to manage key filter settings such as, password override, safety lock, block/warn monitor, and image filter for your profiles.
- **Access Times** - Where to establish and manage Internet access time limit settings for profiles.
- **Alerts** - Where to establish and manage alerts to receive notification via email or text messages when Web pages are blocked.
- **Programs** - Where to manage access to select programs on your PC.






Figure C.1: Parental Controls Features


Categories

Most Web sites are classified in one or more groups or **categories**. The categories identify the topics or interests that are the main focus of the Web site. Our filter gives you the ability to block all URLs (Web sites) that have been identified as being in a particular **category**.

The **Categories** tab is where you go to manage the Web site categories. You can select from a list of blocked categories for more explicit content filtering or you may choose a template setting based on age group.

-  = Categories to be **blocked**
-  = Categories to be **allowed**
-  = Categories **blocked by default**

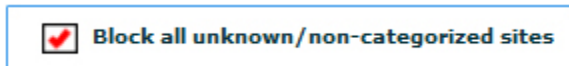
To manage categories:

1. Select **Parental Controls** from the "Services tabs."
2. You should be on the **Categories tab**.
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned On  for the selected profile.
5. Select custom or one of the preset age group templates (**The Adult Filtering Age Group is selected by default**):
 - **Custom** - select this option to choose from all categories.
 - **Child (0-8)*** - select this group to **only allow**:
 - *Arts and Museums*
 - *Automotive*
 - *Business*
 - *Dynamic*
 - *Educational*
 - *Finance and Investing*
 - *Government*
 - *Hobby*
 - *Kids*
 - *Music*
 - *Reference*
 - *Religion*
 - *Science*
 - *Search Engine (protected)*
 - *Sports*
 - *Technology*
 - *Travel*
 - **Youth (9-12)*** - select this group to **only allow**:
 - *Arts & Museums*
 - *Automotive*
 - *Business*
 - *Dynamic*
 - *Educational*
 - *Entertainment*
 - *Finance & Investing*
 - *Games*
 - *Glamour*
 - *Government*
 - *Health & Fitness*
 - *Hobby*
 - *Kids*
 - *Music*

- News
 - Reference
 - Religion
 - Science
 - Search Engine (protected)
 - Shopping
 - Sports
 - Technology
 - Travel
 - Webmail
- **Teen (13-17)*** - select this group to **only block**:
 - Abortion
 - Alcohol
 - Art Nudes
 - Chat
 - Criminal Hacking
 - Cult & Occult
 - Drugs
 - File Sharing
 - Gambling
 - Hate
 - Lifestyles
 - Malware
 - Mature Content R-Rated
 - Movies and TV
 - NNTP News Groups
 - Personals & Dating
 - Pornography
 - Proxies & Anonymizers
 - Search Engine (unprotected)
 - Search Terms
 - Self-Harm
 - Suicide
 - Tobacco
 - Violence & Gore
- **Adult (18+)*** - select this group to **only block**:
 - Malware
 - Mature Content R-Rated
 - Pornography
 - Proxies & Anonymizer
 - Search Terms

6. Select the categories to **block** or **allow** access.

7. To block all unknown and non-categorized sites, **select the check box** located below the categories list. A check mark indicates that this feature is turned on.



8. Click the **Clear All** to allow all categories.
9. Click the **Select All** to block all categories.
10. Select the "Apply to all profiles" box if you would like the changes applied to all of your established profiles. Click Save to save your settings.

Note: Any modification to the categories selected in the predefined Age groups automatically changes your template selection to "Custom".

Listed below are all of the categories that are available.

Abortion

Sites which provide information or arguments related to abortion, describe abortion procedures, or offer advice, help, or testimonials related to abortion.

Advertising

Web sites dealing with pop ups, banner ads, pay per click advertising, etc...

Alcohol

Web sites which sell or contain information relating to the recreational use of alcohol. This includes sites that sell alcohol, sites of alcohol manufacturers, sites containing tips and information on mixing your own drinks, and any other sites dedicated to and promoting the use of alcohol.

Art and Museums

Sites which include art galleries, artists, and museums. All types of visual arts such as performing arts, theater, painting, drawing, sculpture, and photography are included.

Art Nudes

Sites which contain the non-pornographic, tasteful, and artful display of the naked body. The main purpose of these sites is NOT sexual arousal.

Automotive

Web sites which market, discuss, promote, or offer information on all forms of transportation. This would include vehicle maintenance Web sites and car rental sites.

Blogs

Web sites which feature commentary and articles written a long or journal format, generally called blogs. These blogs can be from personal or non-commercial sources.

Business

Web sites which are businesses defined as organizations that provide goods or services for profit.

Chat

Sites which allow chatting without a moderator to monitor for questionable content. In order to avoid this category, the site must require the moderator to be present the entire time the chat is open.

Criminal Skills and Hacking

Web sites which promote illegal or criminal activity such as credit card theft, illegal surveillance, murder, unlawful or questionable tools to gain access to software or hardware, communications equipment, or passwords. This category includes sites that discuss password generation, compiled binaries, hacking tools, cheating, pirated materials, or software piracy. Web sites which contain material of a questionable legal or ethical nature. This category includes sites that promote or distribute products, information, or devices whose use may be deemed unethical or illegal.

Cult and Occult

Web sites which promote non-traditional or unconventional religious activities, and a zealous devotion to a person, idea, object, movement, or work.

Drugs

Web sites which promote the sale or use of illegal drugs and narcotics, including sites offering paraphernalia for use with narcotics, legal supplements for their narcotic effect, or instruction manuals for the production of various narcotics.

Dynamic

Web sites that contain content which is constantly changing and is of a questionable nature, such as group hosting, auction, and stock photography. Known harmful sections will be assigned an appropriate category.

Educational

Web sites for the purpose of education, universities, schools, learning centers, teaching institutions, online classes, workshops, technical institutes, and trade schools. Would also include sites which contain information on teaching aids such as lesson planning guides, teacher supplies, educational games, career development education, and .edu sites.

Entertainment

Web sites which include any general entertainment sites such as theaters, concerts, sporting events, restaurants and clubs, clipart and animated .gifs, amusement parks, and sites offering cell-phone ring tones. Also Web sites which discuss and promote film and television. This category also includes official movie and television sites, and official film and television celebrity sites. Fan Web sites for film, television, or celebrities are also included.

File Sharing

Web sites which offer peer-to-peer file sharing software and transfers.

Finance and Investing

Web sites which are related to the financial trade, and include stock and exchange trading sites, financial news sites, and online banking services.

Forums and Message Boards

Web sites which offer interaction among Internet users with similar interests. They may include message boards, bulletin boards, forums, or any other site that offers its visitors the ability to discuss topics with one another via the Internet. This category applies to downloadable and customizable message board software.

Free Host Sites

Sites which provide individuals or organizations with online systems for storing information, images, video, or any content accessible via the Web such as Free and paid hosting, Dedicated or managed hosting, Virtual private server hosting, Online backup or file storage.

Freeware and Shareware

Web sites that offer the download of software online without requiring purchase.

Gambling

Web sites which encourage gambling, and may include betting, bookmaker odds, lottery, bingo, horse or dog track, or online casinos.

Games

Web sites that offer or promote games. These may include discussion, review, or online gaming sites. This category also applies to sites that offer or are dedicated to promoting board games and electronic games. Sweepstakes and giveaway sites would also fall under this category. This category is not used for gaming sites depicting violence or sex.

Glamour

Web sites which are dedicated to the promotion of fashion and modeling, including discussion boards, portfolio sites and modeling agencies, contests and fashion shows, and any non-commercial Web site dedicated to fashion.

Government

Web sites which include sites with .gov domain, and any other sites for governmental agencies at the national, state, local, or international level. Web sites which promote community involvement, and may include City or local government sites, the Chamber of Commerce, or sites that detail community events or places to see.

Hate

Web sites which contain material related to discrimination based on race, religion, gender, or nationality. This category includes sites that approve of racial superiority, degradation, violence, or the destruction of human life motivated by such discrimination.

Health and Fitness

Web sites which contain information on the practice of medicine, and may include medical practice, hospital, health insurance provider, nursing home, and assisted living sites. This category also includes Web sites that offer or provide information on prescription medicines and over-the-counter treatments, as well as preventative health care. Also Web sites which offer information on alternative medicines and natural healing. These sites may include information on homeopathic medicine, acupuncture and acupressure, chakra alignment, or Feng Shui.

Hobby

Web sites which offer information and support to hobbies, clubs and social organizations. This category includes sites pertaining to horticulture, gardening and yard maintenance, decorating and crafting, and collecting.

Inactive Domains

Web sites where currently unused domain names are redirected to. Often questionable advertising is resident on these pages.

Job Search

Web sites which are geared toward job seekers, and include sites such as job bulletin boards, classified ad sites, services that list or compile resumes and cover letters, and headhunting firms.

Kids

Web sites which provide a safe and interesting Internet experience for children under 12 years old. Includes activities, crafts, and interactive learning.

Lifestyles

Web sites which contain material relative to an individual's personal choices. This category includes sites advocating sexual lifestyles outside of marriage.

Malware

Web sites which contain malware. This includes viruses, spyware, trojans, and adware.

Mature Content R-Rated

Web sites which offer material that is adult in nature without being explicitly pornographic. These sites may contain profanity, information of a mature nature, photographs of women in swimsuits or lingerie, or revealing and sensual photography.

Military

Web sites which include all .mil top-level domains, and any other government-sponsored sites on the various branches of the military. Also Web sites which promote or celebrate the armed services, including individual or regiment sites, and veteran or troop support sites.

Movies and TV

Web sites which include online media, movie and television sites, and major network television sites.

Music

Web sites which discuss or promote music, musicians, or the methods in which they are distributed. This category includes official and fan sites for musical artists.

News

Web sites which distribute news, current events, weather, traffic and headlines. This would also include news commentary, and news blogs.

NNTP (Network News Transfer Protocol) Groups

Is the protocol used by computer clients and servers for managing the notes posted on Usenet newsgroups. NNTP servers manage the global network of collected Usenet newsgroups and include the server at your Internet access provider. An NNTP client is included as part of a Netscape, Internet Explorer, Opera, or other Web browser or you may use a separate client program called a newsreader.

Online Videos

Sites which host streaming media like television, movies, video, radio, or other media.

Personals and Dating

Web sites which facilitate the search for and development of relationships with other people. The purposes of these sites are to bring people together for friendships, dating, or marriage. This category includes sites offering personal ads, dating services, and information.

Politics

Web sites which offer opinions dealing with political issues. These Web sites may include such topics as party platforms, political reform, candidate advocacy, lobbying organizations, campaign sites, or sites offering negative opinions or data regarding a political party member.

Pornography

Web sites that offer video, images, or stories of sexual situations with the intent to encourage prurient interest.

Portal

Web sites that offer a broad array of resources and services, such as email, forums, search engines. Portals often allow access to much material from many various sources/sites not under their control.

Proxies and Anonymizers

Sites which offer anonymous access to Web sites through a PHP or CGI proxy, allowing users to gain access to Web sites blocked by corporate and school proxies as well as parental control filtering solutions.

Reference

Sites which contain personal, professional, or educational references such as online dictionaries, encyclopedias, thesauri, Maps, Language translation sites.

Religion

Web sites which are dedicated to mainstream religious institutions. These sites may include church sites, information regarding service times or location, or church event calendars. This category applies to such religions as Judaism, Mormonism, Christianity, Buddhism, and any other well-established religion. Also Web sites which discuss or advocate religion-based opinions and organizations.

Science

Web sites which provide research materials in the natural and life sciences.

Search Engine (protected)

Web sites which allow you to search the Internet and **DO allow** the enforcement of the "Safe Search" feature. This category would include all sub-URL's under the main site.

Search Engine (unprotected)

Web sites which allow you to either search the Internet and **DO NOT allow** the enforcement of the "Safe Search" feature. This category would include all sub-URL's under the main site.

Search Terms

Provides filtering of search words on sites such as Google, Yahoo, Bing. If you are having issues where your searches are being blocked you may want to uncheck this category.

Self-Harm

Web sites which describe or discuss ways in which to self harm including eating disorders and self injury.

Sexual Education

Web sites which provide a wide range of information on reproduction and sexual development, prevention of sexually transmitted diseases, contraception methods, and sexual orientation issues.

Shopping

Web sites which contain any type of online commerce. Shopping malls, online clothing stores, classifieds, and online trading/auction services.

Social Networking

Sites which offer a variety of tools and mechanisms to enable a group of people to communicate and interact via the Internet such Facebook, MySpace.

Sports

Sites which promote or provide information about spectator sports such as Professional sports teams, leagues, organizations, or association sites; player and fan sites, Collegiate football, basketball, etc.; men's and women's; team, league, and conference sites; player and fan sites, Sites for official Olympic Committees; media Olympic portals , Sports portals and directories - scores, schedules, news, statistics, discussion, etc.; spectator sports link aggregations , Sports event ticket sales for targeted professional or collegiate sports; sports tourism, Online magazines, newsletters, chats and forums for targeted professional and collegiate sports.

Suicide

Sites which describe or promote suicide such as Suggestions on how to kill yourself; newsgroups; chat rooms; message boards, Descriptions/depictions of methods/systems/machines; instructions, Personal stories; suicide diaries; blogs; forums, Famous suicides/details of famous suicides, Famous suicide spots, Glorification or worshipful attitude to suicide.

Technology

Sites which provide information pertaining to computers, the Internet as well as telecommunication such as Software solutions and services, Computer and telecommunication hardware, devices and gadgets, Internet and phone access services, Technology news.

Tobacco

Sites which encourage, promote, offer for sale or otherwise encourage the consumption of tobacco such as Retailers, Manufacturers/tobacco industry, Tobacco products and paraphernalia, Smoking is good/glamorous/cool etc. , How to smoke/smoking lessons.

Travel

Sites which promote or provide opportunity for travel planning in a general sense, particularly finding and making travel reservations such as Travel portals, packages, and information (includes tours, travel clubs and associations, and travel information for specific demographic groups), Air travel (air carriers: tickets/reservations/charters).

Violence and Gore

Sites which advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence, such as Explosives and bombs: how to manufacture, obtain materials, transport, or seed an area, including but not limited to making explosives using common household items, Pranks, destructive mischief, "revenge," teenage anarchy including but not limited to dangerous chemistry, Descriptions or instructions for killing people.

Weapons

Sites which describe or offer for sale weapons including guns, ammunition, firearm accessories, knives and martial arts such as Online sales of firearms, ammunition, accessories, knives, etc. Descriptions, reviews, specifications or weapons, Weapons retailers, manufacturers, auctions, trading centers, Instructions for manufacture of weapons.

Webmail

Web sites which offer free Web-based email services.

Media

Bsecure Online now provides a means to further manage parental controls by controlling the accessibility of online media content. The Media panel is where you can restrict a profile's access to online media such as movies, TV shows, and games. Using industry standard ratings, the most popular media web sites (*ABC, NBC, CBS, FOX, TLC, MTV, BET, TNT, FX, Hulu, Fancast, Comedy Central & Netflix*) are individually filtered, giving you the ability to control a profile's media access by the assigned media rating.

Note: For safety reasons, less popular sites will be blocked.

❌ = Media to be **blocked**

✅ = Media to be **allowed**

Online Media Settings for Group							
Movies (MPAA Ratings)							
G	PG	PG-13	R	NC-17			
✅	✅	✅	✅	❌			
TV Shows (FCC Ratings)							
TV-Y	TV-Y7	TV-Y7...	TV-G	TV-PG	TV-14	TV-MA	
✅	✅	✅	✅	✅	❌	❌	
Games (ESRB Ratings)							
EC	E	E+	T	M	AO	RP	
✅	✅	✅	✅	❌	❌	❌	
Music (iTunes only)							
Explicit							
❌							

Figure C.2: Block Sites list

Movies (MPAA Ratings)

G (General Audiences)

means material is appropriate for all ages.

PG (Parental Guidance Suggested)

means that parental guidance is recommended and some material may be unsuitable for children.

PG-13 (Parents Strongly Cautioned)

means some material may be inappropriate for children under 13.

R (Restricted)

means some material may be inappropriate for children under 17, and, if shown in a movie theater, requires accompanying parent or adult guardian.

NC-17 (No One 17 and Under Admitted)

means movie contains material that most parents would consider patently inappropriate for children 17 and under, and, if shown in a movie theater, no one 17 and under would be admitted.

TV Shows (FCC Ratings)

TV-Y

(All Children) Whether animated or live-action, the themes and elements in this program are specifically designed for a very young audience, including children from ages 2–6. These programs are not expected to frighten younger children. Examples of programs issued this rating include Sesame Street, Barney & Friends, Dora the Explorer, Go, Diego, Go! and The Backyardigans.

TV-Y7

(Directed to children 7 and older) These shows may or may not be appropriate for some children under the age of 7. This rating may include crude, suggestive humor, mild fantasy violence, or content considered too scary or controversial to be shown to children under seven. Examples include Foster's Home for Imaginary Friends, Johnny Test, and SpongeBob SquarePants.

TV-Y7-FV

(Directed to children 7 and older [fantasy violence]) When a show has noticeably more fantasy violence, it is assigned the TV-Y7-FV rating. Action-adventure shows such as Digimon, the Pokémon series (after being transferred to Cartoon Network, where on Kids' WB it was formerly rated TV-Y) and Sonic X series are assigned a TV-Y7-FV rating.

TV-G

(General audience) Although this rating does not signify a program designed specifically for children, most parents may let younger children watch this program unattended. It contains little or no violence, no strong language and little or no sexual dialogue or situation. Networks that air informational, how-to content or generally inoffensive content (such as the Food Network and HGTV) usually apply a blanket TV-G rating to all of their shows (unless otherwise noted). Shows directed to preteen and teens on Nickelodeon and Disney Channel are rated TV-G.

TV-PG

(Parental guidance suggested) This rating signifies that the program may be unsuitable for younger children without the guidance of a parent. Many parents may want to watch it with their younger children. Various game shows and most reality shows are rated TV-PG for their suggestive dialog, suggestive humor, and/or coarse language. Some prime-time sitcoms such as Everybody Loves Raymond, Fresh Prince of Bel-Air, The Simpsons, Futurama (on Fox and adult swim airings), and Seinfeld usually air with a TV-PG rating.

TV-14

(May be unsuitable for children under 14 years of age) Parents are strongly urged to exercise greater care in monitoring this program and are cautioned against letting children of any age watch unattended.

TV-MA

(Mature audience — may be unsuitable for children under 17) The program may contain extreme graphic violence, strong profanity, overtly sexual dialogue, very coarse language, nudity and/or strong sexual content. Although not a very large number of shows carry this rating, The Sopranos is a popular example.

Games (ESRB Ratings)

EC (Early Childhood)

May be suitable for ages 3 and older. Contains no material that parents would find inappropriate.

E (Everyone)

May be suitable for ages 6 and older. Titles in this category may contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language.

E10+ (Everyone 10 and older)

May be suitable for ages 10 and older. Titles in this category may contain more cartoon, fantasy or mild violence, mild language, and/or minimal suggestive themes.

T (Teen)

May be suitable for persons ages 13 and older. Titles in this category may contain violence, suggestive themes, crude humor, minimal blood, simulated gambling, and/or infrequent use of strong language.

M (Mature)

May be suitable for persons ages 17 and older. Titles in this category may contain intense violence, blood and gore, sexual content, and/or strong language.



AO (Adults Only)

Should only be played by persons 18 years and older. Titles in this category may include prolonged scenes of intense violence and/or graphic sexual content and nudity.

RP (Rating Pending)

Title has been submitted to the ESRB and is awaiting final rating. (This symbol appears only in advertising prior to a game's release).

To allow media:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Media tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify Parental Controls is turned ON**  for the selected profile.
5. Select the highest rating to be allowed . The selected rating and all ratings "below" (to the left of) the selection will automatically be included or allowed.

Additionally, all ratings above (to the right of) the selection will be excluded or blocked. For example, if you elect to allow R rated movies, all the ratings listed to the left of "R" (i.e. PG-13, PG, and G) are automatically allowed as well.

6. Select the "Apply to all profiles" box if you would like the changes applied to all of your established profiles. Click Save to save your settings.

To block media:


1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Media tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Select the rating to be blocked. The selected rating and all ratings "above" (to the right of) the selection will automatically be included or blocked. For example, if you choose to block PG-13 movies, all ratings to the right of PG-13 (R & NC-17) will automatically be blocked as well.
5. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Block Sites

The Block Sites list, Figure C.2, is useful for blocking specific Web sites that may not fall under any of the Bsecure categories. For example, you may have discovered that your child has been browsing a certain Web site that, although not necessarily obscene, find very distasteful. The filter has not blocked it, but you may do so by adding that Web address to the Block you Sites list.

To create a block sites list:

1. Select **Parental Controls** from the "Services tabs."
2. Select **Block Sites** from the "Features tabs."
3. Select the **profile** that you would like to manage.

4. **Verify** that **Parental Controls** is turned **ON**  for the selected profile.
5. In the provided text box, **type the URL** of a Web site that you want to block.
6. **Click Add**. The Web site is added to the Blocked Web sites List.
7. **Repeat steps 5 and 6** to add additional Web sites to your Block Sites list.
8. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*

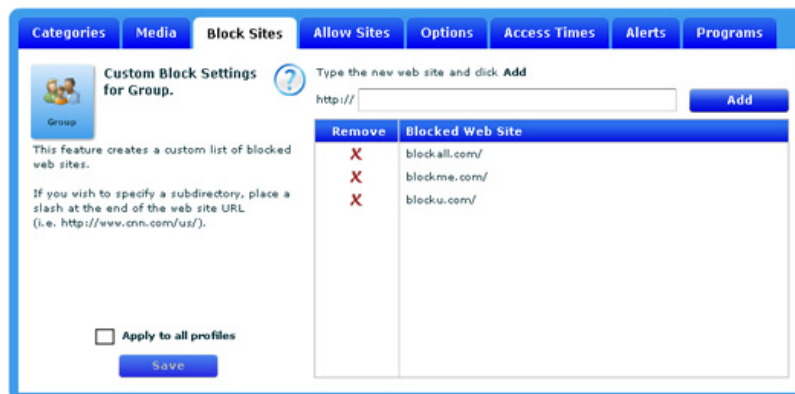



Figure C.2: Block Sites list

To remove an entry from the block sites list:


1. Select **Parental Controls** from the "Services tabs."
2. Select **Block Sites** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. Click on the **red X** next to the Web site entry.
6. **Repeat** for every Web site entry to be deleted.
7. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Allow Sites

The ability to create customized lists enables you to allow specific Web sites by URL and create White Lists (an approved list of Web sites to be allowed to display) if desired to control content filtering more specifically.

Note: If there are no addresses listed in this window and the **"Only allow..."** box is checked, **NO sites at all will be accessible except the hard-coded Bsecure Web sites**. If you are unable to access the Internet, it is helpful to make sure "Only allow the Web sites listed in the Allowed list" box is not checked.

To create an allowed sites list:

1. Select **Parental Controls** from the "Services tabs."
2. Select **Allow Sites** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify Parental Controls turned ON**  for the selected profile.
5. In the provided **text box**, type the URL of a Web site that you want to allow.
6. **Click Add**. The Web site is added to the Allow Sites List.
7. **Repeat** the steps 5 and 6 to add additional Web sites to your Allow Sites list.
8. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

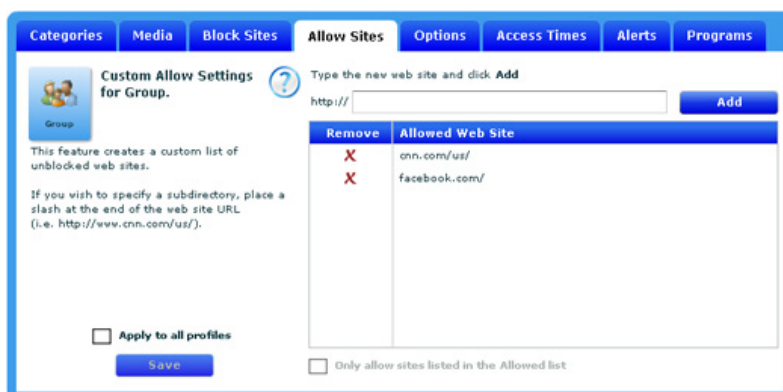



Figure C.3: Allow Sites list

To remove an entry from the allow sites list:

1. Select **Parental Controls** from the "Services tabs."
2. Select **Allow Sites** on the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Click on the **red X** next to the Web site entry.
5. **Repeat** step 4 for every Web site entry to be deleted.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

A **white list** is a list of Web sites that are authorized to display. If this option is selected, the selected user profile *will only be able to navigate to the Web sites on the Allowed Web sites list*.

To create a white list:

1. Select **Parental Controls** from the "Services tabs."
2. Select **Allow Sites** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify Parental Controls turned ON**  for the selected profile.
5. **Select the box** below the Allowed Web sites list (Figure C.4). A check mark indicates that the "white list" feature is turned on.

Note: The **"Block Sites" feature on the Options Tab** must be turned on in order for this feature to be active. **The selected profile will only be able to navigate to web sites on this list.**

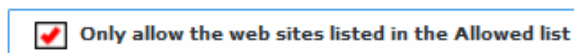


Figure C.4: Allow Sites list

Options

In the Options (Figure C.5) section you can manage the following key filter settings for your profiles:

- **Block / Warn / Monitor Option** - Where to establish the internet permissions level for your profiles.
- **Password Override** - Where to temporarily unblock Web sites or add them to your "Allow Sites" list by providing your administrative or secondary password.
- **Secondary Password** – Where to create a secondary password for non-administrative users.
- **Safe Search** - Where to manage the built-in safe search feature of the Google, Yahoo, and Bing search engines for each of your profiles.
- **Safety Lock** - Where to disable Internet access after a certain number of sites have been blocked.
- **File Extension Blocking** - Where to block Web pictures and various media files that display on good sites but are linked to objectionable sites.
- **iCat** - Where to activate the filters second line of defense against uncategorized sites.

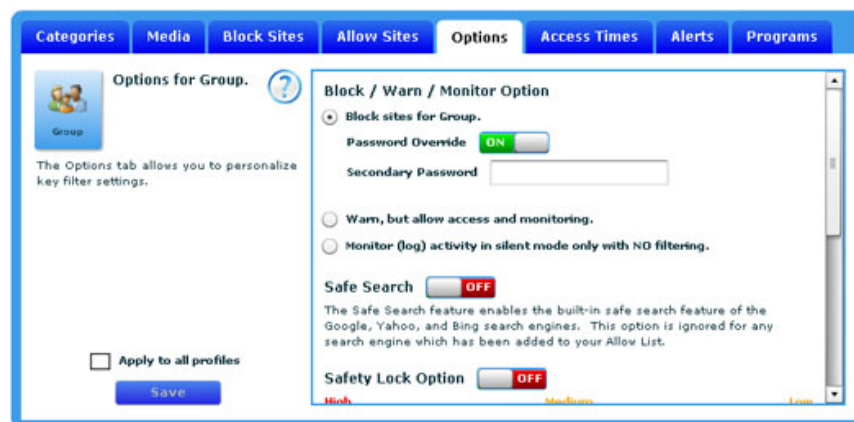


Figure C.5: Parental Controls Options Panel

Block / Warn / Monitor

Use the **Block / Warn / Monitor** feature (Figure C.6) to manage and control access to blocked sites for your profiles. The following permission levels are available:

- **Block sites** - This is the strictest setting. The user will have restricted internet access based on filter settings such as, Categories, Allow Sites, Block Sites, etc. A **Block page** will allow **password override** if the override feature is turned on. Password override will allow the user to open the blocked Web site by entering either the administrative or secondary password.

Note: Verify that the Parental Controls feature is turned ON .

- **Warn, but allow access and monitoring** - the "selected profile" will have unrestricted internet access, but will receive a **warn page** before navigation to Web sites in blocked categories. The warn page, will give the option to go "**back**" or "**continue**" on to display potentially unwanted content.

Note: The Warn option will still block Web sites in the **Block Sites** list. Verify that the Parental Controls feature is turned ON .

- **Monitor (log) activity in silent mode only with NO filtering** - the "selected profile" will have unrestricted internet access and will not receive block or warn pages.

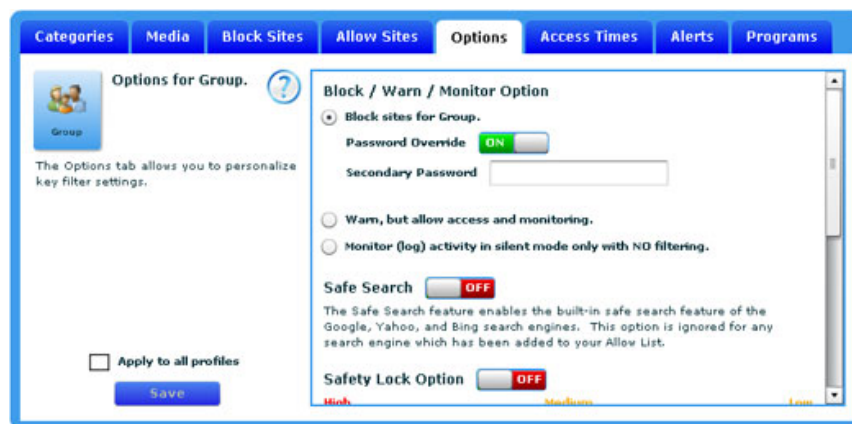


Figure C.6: Block / Warn / Monitor selection




Password Override

With Password Override enabled, you have two additional options to further manage internet sword override access for your User Settings:

- **Option 1:** When the Block page comes up for any URL, the Password Override feature allows you to grant access to the blocked URL by entering the administrative or secondary password. Access will be granted to the URL until the next time the computer is restarted.
- **Option 2:** When the Block page comes up for any URL, the Password Override feature also allows you to add the URL to your allow list. Select the check box located to the right of the password entry box.






To turn **ON** the Password Override feature:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "Password" option in the window provided. The default setting for this feature is OFF. Click the red OFF indicator  to display the green ON . The Password Override feature is now enabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Secondary Password

The Secondary Password option allows you to create an alternate password for your established profiles to use for overriding blocked Web content. This feature can be used to give your profiles temporary access to blocked content without compromising the administrative password. The administrator is able to create a different secondary password for each profile and it can be changed as often as is desired.

To create a Secondary Password:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "Password" option in the window provided. The default setting for this feature is OFF. Click the red OFF indicator  to display the green ON . The Password Override feature is now enabled.
6. Enter a secondary password in the text box provided.
7. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*

Safe Search




The Safe Search (Figure C.7) feature allows you to manage the built-in safe search feature of the Google, Yahoo, and Bing search engines. The search engine's safe search is designed to filter out explicit, adult-oriented content from the engines' search

results. The listed search engines have three settings for their safe search options **(These settings must initially be set in the individual search engines)**:

- **Strict** – Filters out adult **text, images, and videos** from your search results.
- **Moderate** – Filters adult **images and videos** but not text from your search results.
- **Off** – no filtering of the search results.

Note: The Safe Search option is ignored for any search engine which has been added to your Allow List.

To turn on the safe search feature:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Verify that Parental Controls is turned ON  for the selected profile.
3. Select the **Options tab** from the "Features tabs."
4. **Drag the scroll bar** to show the "Safe Search" option in the window provided. The default setting for this feature is ON. Click the red OFF indicator  to display the green ON . The Safe Search feature is now enabled.
5. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

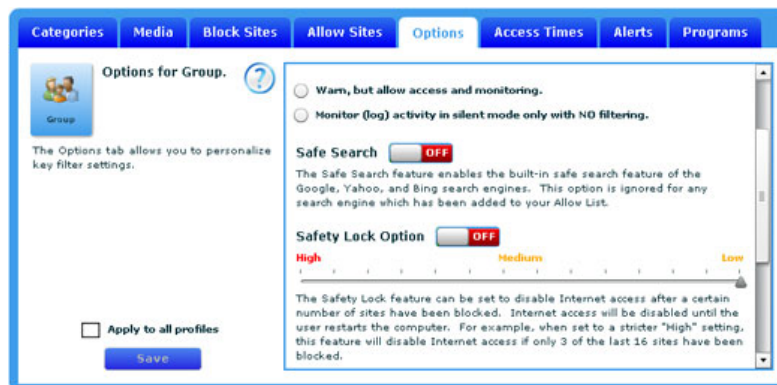





Figure C.7: Safe Search

To turn off the safe search feature:

1. Select the **profile** that you would like to manage.
2. Select the **Parental Controls tab** from the "Services tabs."

3. Verify that Parental Controls is turned ON  for the selected profile.
4. Select the **Options tab** from the "Features tabs."
5. **Drag the scroll bar** to show the "Safe Search" option in the window provided. The default setting for this feature is ON. Click the green ON indicator  to display the red OFF . The Safe Search feature is now disabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

Safety Lock Option

The Safety Lock feature (Figure C.8) is used to protect against users accessing multiple blocked sites. This feature prevents attempts to bypass the Content Filter by forcing the user to restart the computer after a specified number of attempts result in blocked pages. For example, when set to a stricter "High" setting, this feature will disable Internet access if only 3 of the last 16 sites have been blocked. The number displayed as the slider is moved indicates the number of sites blocked before internet access is disabled.

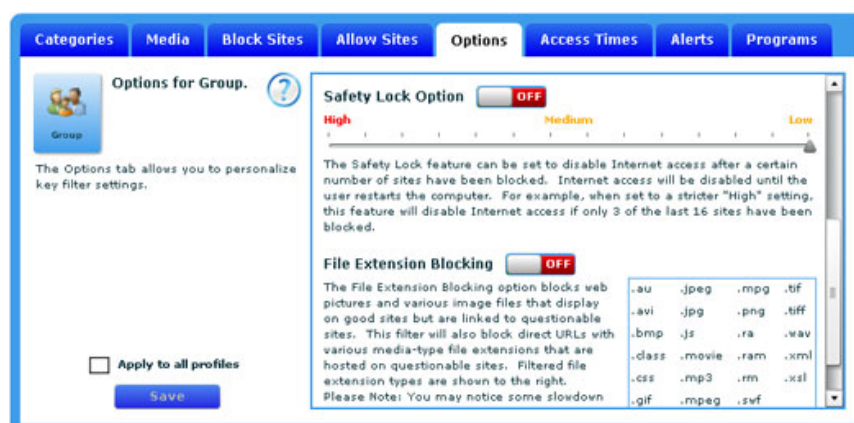








Figure C.8: Safety Lock

To turn on and adjust the safety lock feature:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "Safety Lock" option in the window provided. The default setting for this feature is "Low" or OFF. Click the red OFF indicator  to display the green ON . The Safety Lock feature is now enabled.
6. **Click and slide** (Figure C.9) the marker sideways to adjust the setting. Sliding the marker to the left increases the setting for a stricter setting.
7. **Click Save** to preserve your settings.

**Figure C.9: Safety Lock adjustment****To turn off the safety lock feature:**

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that parental controls are turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "Safety Lock" option in the window provided. The Safety Lock feature is on when a green ON  indicator is displayed. Click ON to change the indicator to a red OFF . The Safety Lock feature is now disabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

7. **Note:** If you navigate away from this section before saving your changes, the **Save Changes** message appears.

File Extension Blocking

The **File Extension Blocking** (Figure C.10) feature **blocks Web pictures and various media files** that display on good sites but are linked to objectionable sites. This filter will also block direct URLs with various media-type file extensions that are hosted on objectionable sites. **The filtered file extensions are:**

.au	.avi	.bmp	.class
.css	.gif	.jpeg	.jpg
.js	.movie	.mp3	.mpeg
.mpg	.png	.ra	.ram
.rm	.swf	.tif	.tiff
.wav	.xml	.xsl	

Note: When turned on, File Extension Blocking will block **all** of the listed extensions. You may notice some slowdown in Web browsing when utilizing File Extension Blocking.

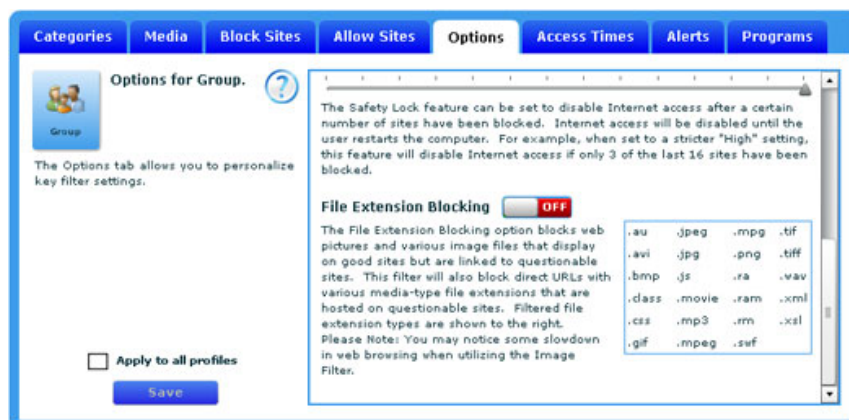





Figure C.10: File Extension Blocking

To turn on file extension blocking:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify that Parental Controls is turned ON**  for the selected profile.
5. **Drag** the scroll bar to show the "File Extension Blocking" option in the window provided.
6. The default setting for this feature is OFF. **Click** the red OFF indicator  to display the green ON . File Extension Blocking is now enabled.
7. **Click Save** to preserve your settings.

iCat (Intelligent Contextual Analysis Technology)

Bsecure's patent pending iCat feature provides a second line of defense to further protect our users from the dangers of the web. On the rare occasion when a web page is not categorized in our databases, the iCat capability will evaluate the web page, its content and its links to make sure it is not a threat. The feature is turned on by default and can be disabled easily by switching it to off, Figure C.11.

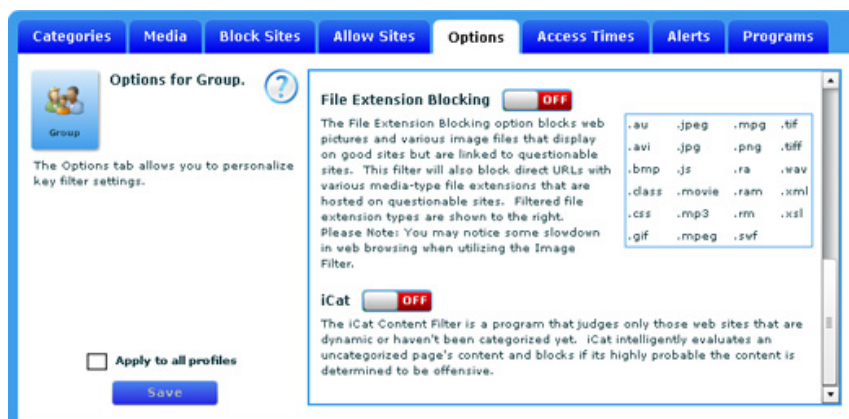





Figure C.11: iCat on/off switch




To turn on the iCat feature:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "iCat" on / off switch in the window provided. The default setting for this feature is ON. If it has been turned off, click the red OFF indicator  to display the green ON . The iCat feature is now enabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the Save Changes message appears.

**All changes made will be applied to the highlighted profile only.*


To turn off the iCat feature:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "iCat" on / off switch in the window provided. The iCat feature is on when the green ON  indicator is displayed. Click the ON switch to change the indicator to a red OFF . The iCat feature is now disabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Access Times

This feature allows you to set time limits for your profiles by blocking access to Web surfing and Internet games during certain times of the day for each day of the week.

To restrict Internet access times:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Access Times tab** from the "Features tabs."
3. **Verify Parental Controls is turned ON**  for the selected profile.
4. ***Important:** Select your time zone from the drop down list (Figure C.12).

The schedule uses a server based clock to avoid tampering with the PC clock. Please make sure your time zone below is correct.

Central Time (US & Canada) ▼

Figure C.12: Time Zone drop down list

5. **Click** the time block to change the color. **Green** blocks indicate times that are **allowed** and **red** blocks indicate times that are **blocked**. To select multiple time blocks (Figure C.13), click in the initial time block and drag your mouse across the desired blocks.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

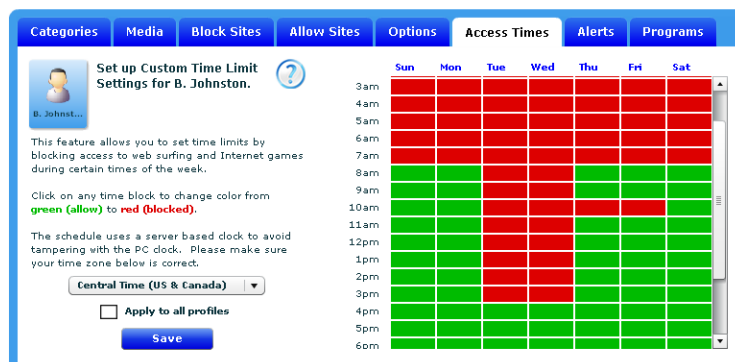


Figure C.13: Access Times selection

Alerts



Using the Alerts feature, parents can receive alerts via e-mail and/or text messaging (SMS) whenever a user attempts to access a Web site categorized as **pornography** or when **keywords or phrases** are used on a Web site categorized as a **social site**. **Social Networks alerts** are turned **on by default** while **Blocked Sites** alerts are defaulted to **off**.

Note: If no email address or mobile number is provided, Alerts may be viewed by accessing the Activity Monitoring / Alert Log tab.

Mobile Number	Carrier	Remove	Email Address	Remove
(850) 324-1256	Alltel Wireless	X	pholmes@gmail.com	X

Figure C.14: Alerts Panel


To turn Blocked Sites alerts off:

1. Select the **Parental Controls** tab from the "Services tabs."
2. Select the **Alerts** tab from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. The default setting for this feature is ON. **Click** the **"Blocked Sites"** green ON indicator  to display the red OFF . The "Blocked Sites" Alerts feature is now disabled.

Note: There are two On/Off switches for Alerts: one to manage **Blocked Sites** (pornography only) alerts and one to manage **Social Network** alerts.


To turn Social Networks alerts off:

1. Select the **Parental Controls** tab from the "Services tabs."

2. Select the **Alerts tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. The default setting for this feature is ON. **Click** the "**Social Networks**" green ON indicator  to display the red OFF . The "Social Networks" Alerts feature is now disabled.

Note: There are two On/Off switches for Alerts: one to manage **Blocked Sites** (pornography only) alerts and one to manage **Social Network** alerts.

To setup text (SMS) alerts:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the profile that you would like to setup.
3. Select the **Alerts tab** from the "Features tabs."
4. **Verify** that **both Parental Controls** and **Alerts** (Blocked Sites and/or Social Networks) are turned ON  for the selected profile.
5. **Enter** a mobile phone number in the text box (Figure C.14) provided under the mobile number section. Be sure to include the area code.
6. **Select** your mobile carrier from the list provided.
7. **Click** the add button to add the number to your mobile number list.

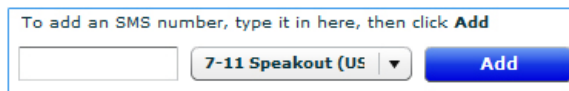
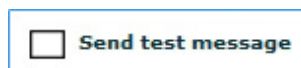


Figure C.15: Alert setup - mobile number entry

8. **Repeat** steps 4 thru 6 for each mobile number that you would like to setup.
 9. Select the "**Send test message**" box in order to verify your SMS alerts setup.
- Note:** SMS alerts are sent out in one minute intervals. Please allow at least one minute between each test.




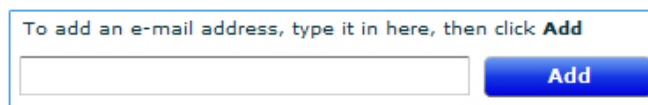
10. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*

To setup email alerts:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Alerts tab** from the "Features tabs."
3. **Verify** that **both Parental Controls** and **Alerts** (Blocked Sites and/or Social Networks) are turned **ON**  for the selected profile.
4. **Enter** the email address in the text box (Figure C.16) provided under the email address section.
5. **Click** the add button to add the email address to your email list.



To add an e-mail address, type it in here, then click **Add**

Figure C.16: Alert setup - email entry

6. **Repeat** steps 4 and 5 for each email address that you would like to setup.
7. Select the "**Send test message**" box in order to verify your email alerts setup.

Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.

8. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*

Programs

The **Programs** panel (Figure C.17) is where you manage access to certain programs on your PC. By selecting from a predefined list, you can determine whether to block or allow the programs.

- **Email programs** - programs used to manage email client applications. **Email programs that can be blocked are:** *Alphine, DreamMail, Eudora, Foxmail, i.scribe, Incredimail, Mozilla Thunderbird, Mulberry, Opera, Outlook, Outlook Express, Pegasus Mail, Sylpheed, Windows Live Mail and Windows Mail.*
- **Games** - electronic games that involve interaction with a user interface to generate visual feedback. **Games that can be blocked are:** *Call of Duty Modern Warfare, Company of Heroes, Company of Heroes: Tales of Valor, Company of Heroes: Opposing Forces, Counter Strike, Guild Wars, Half Life, Left4Dead, Quake, Quake 4, Team Fortress and World of Warcraft.*
- **IM Programs** - programs that make possible a form of real-time communication between two or more people by way of typed text. The text is conveyed via devices connected over a network such as the Internet. **IM Programs that can be blocked are:** *Adium, AOL, Bopup Messenger, Chat Anywhere, Chat Watch, digsby, GAIM, Google Talk, ICQ, iOL Messenger, Miranda, MSN messenger, Paltalk, PSI, Skype, Smiley Central, Trillian, WebSecureAlert, yahoo IM and Zovine Messenger.*
- **Malware** - programs designed to infiltrate a computer system without the owner's informed consent **Malware programs that can be blocked are:** *Bypass, Bypass Proxy Client, Claria, Offsurf Firewall Bypass Unblocker Professional, Proxifier and Unrest.*
Note: All of these Malware programs are blocked by default.
- **Media programs** - programs for playing back multimedia files. **Media programs that can be blocked are:** *alt.binz 0.25.0, Forte Agent 6.0, Grabit, iTunes, Mimo, News Rover, Newsbin Pro, Newsgroup Commander Pro 9.05, Newsleecher, NomadNews v2.10, Omea Reader 2.2, Real Player, SABnzbd, slrn, Songbird, Unzbin, VLC Player, Winamp, Windows Media Player, xnews, XPN 1.2.6 and YeahReader.*

- **P2P Programs/ Torrent Programs** - programs that allow groups of computer users to connect for the purpose of file sharing and software distribution. **P2P Programs/Torrent Programs that can be blocked are:** *Ares, Avarice, Azureus, Bearflicx, Bearshare, Bitche, BitComet, BitTornado, Bittyrant, Calria, Code Red, Dashbar, DateManager, eMule, Error Check System (Facebook), Frostwire, Gizmo, GotSmiley, Grokster, Hermes, iMesh, Kazaa, LanOnInternet, Limewire, Meebo, Memoryup, Morpheus, MS Blaster, MySpace Messaging, Peer guardian, Pidgin, QQ, Shareaza, Sharetastic, Small.DAM, Tribler, Vuze, uTorrent and Zultrax.*

Note: All of these P2P/Torrent programs are blocked by default.

- **Proxy / Bypass** - programs manage traffic between your network and servers on the internet, and determines of information is allow. **Proxy/Bypass programs that can be blocked are:** *ActivePerl-5.8.3.809-MSWin32-x86.msi, Barracuda Proxy 1.0, Bypass Proxy and bypass firewall 3.0 (surfnolimit), Bypass Proxy Client 0.75, Circumventer setup exe, Customyspace 1.0, Cyclope Internet Filtering Proxy 2.9, Elite Proxy Switcher 1.07D, Facebook Circumventor, Firefox Setup 4.0 Beta 7, Gpass 4.1, hopster 1.0.16, JonDo_Portable.paf.exe, ProxyTunnel 1.1, Proxyway 5.0, ProxyWay.rar.torrent, UltraSurf 9.4-9.6, UltraSurf v90, WinsockxpFix, Your Freedom 20040119-01 and Your freedom 20091203-01.*

Note: All of these Proxy/Bypass programs are blocked by default.

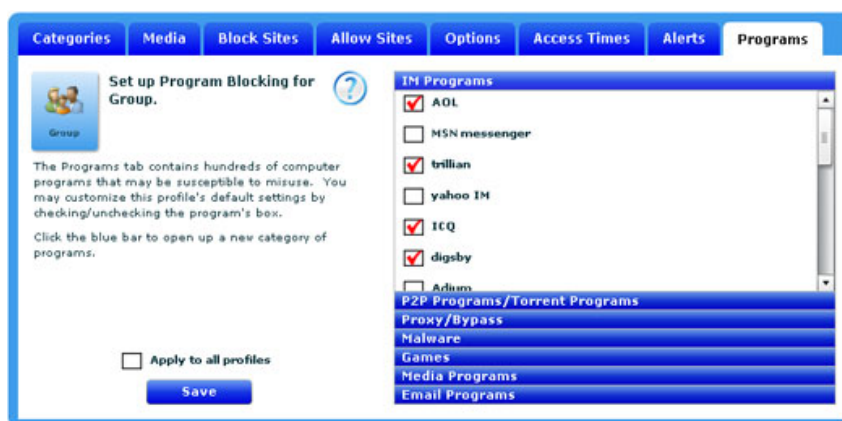



Figure C.17: Programs panel – Parental Controls

To block access to select programs on your PC:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Programs tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. Click the **blue bar** to open the listed program category.
6. Click the **box** next to the program you would like to block. A checked box indicates active blocking of the listed program for the current user setting.
7. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: Blocking one of these applications prevents the application from running, connecting to the Internet and sending out sensitive or other data from your computer. It **does not** prevent the download or install of the application.

SECTION D

SECURITY

Security

The Anti-Virus/Anti-Spyware service protects your computer from viruses that can infect your system and spyware that has the potential to steal your personal information and track your Web-browsing habits. Utilizing McAfee[®] VirusScan[®] protection your Bsecure Online Internet Protection Service provides you with round-the-clock, world-wide monitoring and automatic updates that respond to the latest virus, Trojan, and spyware threats in an integrated service.

Note: We recommend that you scan your computer for viruses on a regular basis. Scheduling or performing manual scans ensures that nothing gets past even on friendly channels.

Before you can begin to use the McAfee[®] VirusScan[®] services, make sure you have them turned on (Figure D.1).

To enable anti-virus / anti-spyware:





1. Select the **Security tab** from the "Services tabs".
2. **Click** the red OFF indicator  to display the green ON . The anti-virus / anti-spyware service is now enabled for the selected device.



Figure D.1: Security Panel

To disable anti-virus / anti-spyware:

1. Select the **Security tab** from the "Services tabs."
2. **Click** the green ON  to display the red OFF indicator . The anti-virus / anti-spyware service is now enabled for the selected device.

To delete a computer:

1. Select the **Security tab** from the "Services tabs."
2. Select the computer to be deleted.
3. Select the red **X** in the upper right corner of the computer's icon.
4. Click the **Yes button** to confirm the deletion of the selected computer (Figure D.2).

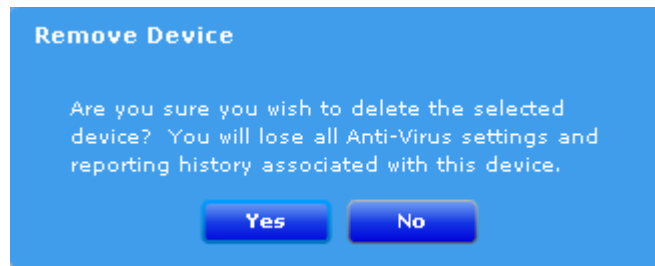


Figure D.2: Security Panel

Manual Scan

Although it is recommended that you schedule scans on a regular basis, you can manually scan for viruses at any time.

To perform a manual virus/spyware scan:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Manual Scan tab** (Figure D.3) from the "Features tabs."
3. Click the **Scan Type** drop down menu and select the type of scan desired.

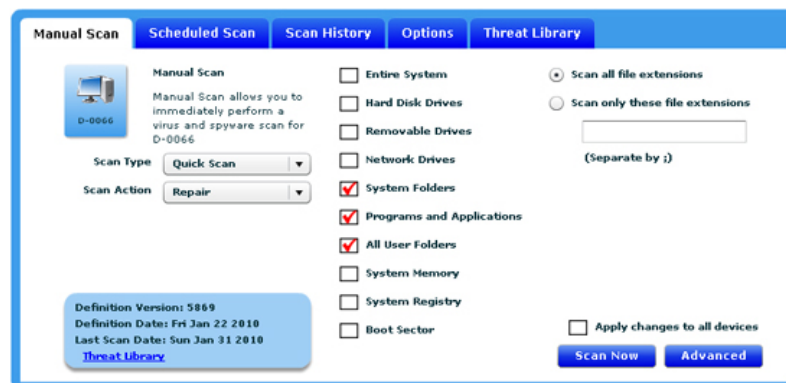


Figure D.3: Manual Scan

4. Click the **Scan Action drop down** menu and select the scan action desired.
5. To scan all files - **Select** the button next to "**Scan all file extensions**" or

6. To scan specific files - **Select** the button next to "**Scan files with supplied extensions.**" With this option selected, you must enter at least one file extension in the text box provided. Use a ";" to separate multiple entries (exe; doc).
7. Select the box for **at least one location** to be scanned. You can choose to scan the entire system or scan multiple locations.
8. To scan all recognized devices with this manual scan, **select** the box to "**apply changes to all devices.**"
9. Click the **Advanced** button (Figure D.4) to **select directories** to scan.
10. Click the **Scan Now** button to begin the manual scan.

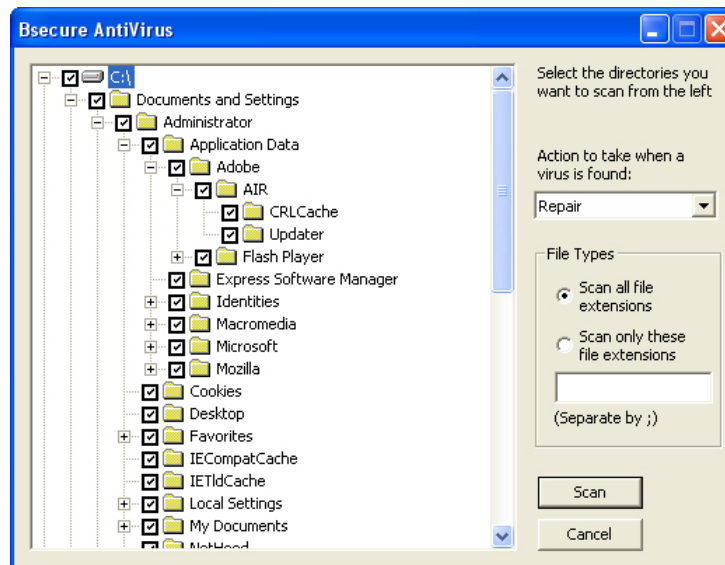


Figure D.4: Advanced Scan – select directories

Scheduled Scan

Your Internet Protection Service lets you set up one or more Scheduled Scans.

To Schedule an automatic virus/spyware scan:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."

- Click the **Add button** (Figure D.5) located in the bottom right corner of the window.

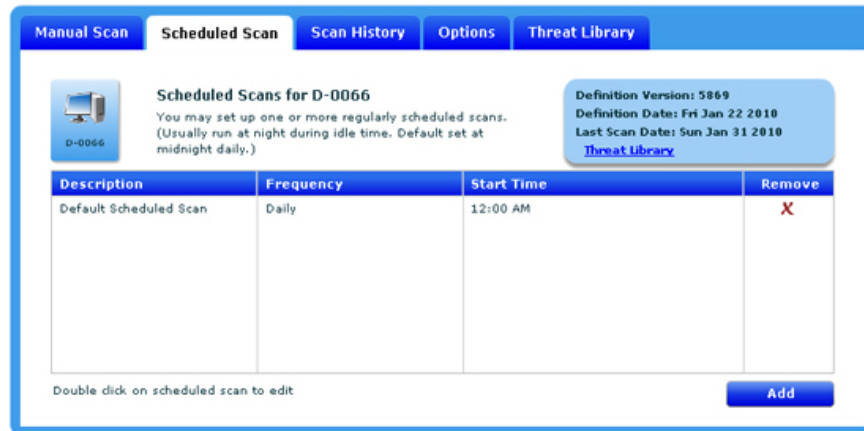


Figure D.5: Scheduled Scan

- Type a name** (Figure D.6) for the scheduled scan in the box next to Scan Name.
- Click the **Scan Type drop down** menu and select the type of scan desired.
- Click the **Scan Action drop down** menu and select the scan action desired.
- Click the **Every drop down** menu and select the day of week desired.
- Click the **Start Time drop down** menu and select the time desired.
- To scan all files - **Select** the button next to **Scan all file extensions** *or*
- To scan specific files - **Select** the button next to **Scan files with supplied extensions**.
With this option selected, you must enter at least one file extension in the text box provided. Use a ";" to separate multiple entries (exe; doc).
- Select the box for at least one **location** to be scanned. You can choose to scan the entire system or scan multiple locations.
- To scan all recognized devices with this scheduled scan, **select** the box to "**apply changes to all devices.**"
- Click the **Save** button to preserve your settings.

Manual Scan Scheduled Scan Scan History Options Threat Library

D-0066
Add an Automatic Scan for D-0066

Scan Name:
Scan Type: Custom
Scan Action: Repair
Every: Sunday
Start Time: 12:00 AM

☒ Scan all file extensions
☐ Scan only these file extensions

(Separate by ;)

☐ Apply changes to all devices

☐ Entire System
☐ Hard Disk Drives
☐ Removable Drives
☐ Network Drives
☐ System Folders
☐ Programs and Applications
☐ All User Folders
☐ System Memory
☐ System Registry
☐ Boot Sector

Save Cancel

Figure D.6: Add Scheduled Scan

To edit a Scheduled Scan:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."
3. Double Click on the Scheduled Scan to open the entry.
4. After making the desired changes, click the **Save** button.
5. **Repeat** for every Scheduled Scan entry to be edited.

To remove a Scheduled Scan:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."
3. Click on the **red X** next to the Scheduled Scan.
4. **Repeat** for every Scheduled Scan entry to be deleted.

Scan History

Shows history (Figure D.7) of virus scans performed on your computer.

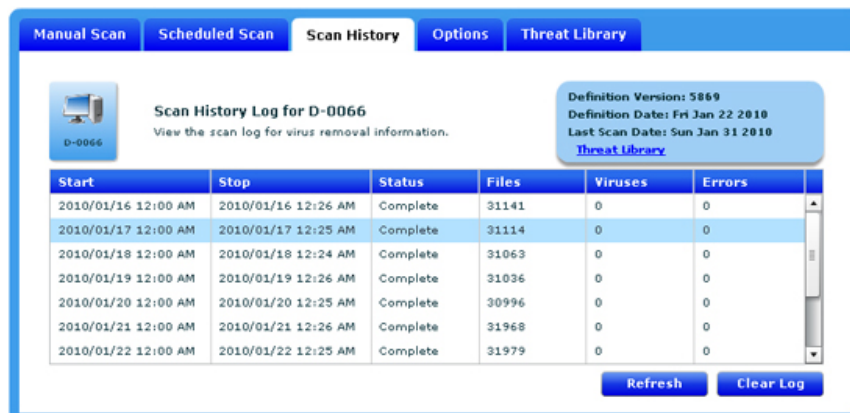


Figure D.7: Scan History

Options - Definition Updates

Your Bsecure service is set by default to automatically update itself with the latest virus and spyware definition files. This option allows you to stop these updates or change their frequency. You can also perform manual definition updates anytime.

Automatic Definition Updates

Controls for setting Automatic Anti-Virus Definition updates (e.g., check for new virus definitions when the filter authenticates, automatically update virus definitions, Figure D.8).

To modify automatic definition updates:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Click the **Auto Update drop down** menu and select the frequency desired.
4. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted device only.*

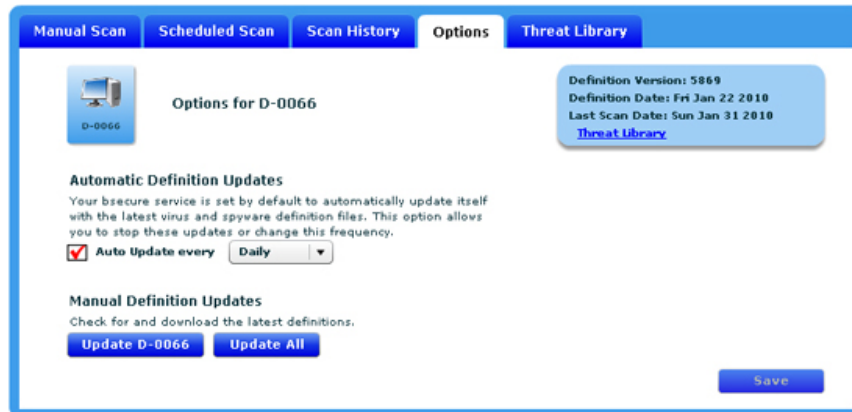


Figure D.8: Options – Definition Updates

To stop automatic definition updates:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Click the **Auto Update Box** to "deselect" it.
4. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the Save Changes message appears.

**All changes made will be applied to the highlighted device only.*

Manual Definition Updates

Controls for performing **manual** Anti-Virus Definition updates (Figure D.9).

To perform manual definition updates:

1. Select the **Security tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Click the **Update (device name)** button for a single device *or*
4. Click the **Update All** button to check updates for all recognized devices.

5. Click **Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted device only.*

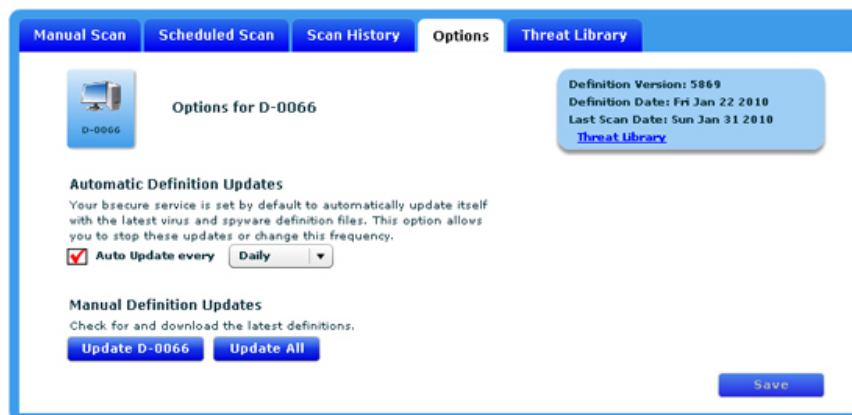


Figure D.9: Manual Definition Updates

Threat Library

The Threat Library (Figure D.10) allows you to search for information on known viruses and other threats.

To launch the McAfee[®] Threat Library:

1. Select the **Security tab** from the "Services tabs."
2. Click the **Threat Library** link located on the following tabs: Manual Scan, Scan History, Options and Threat Library.

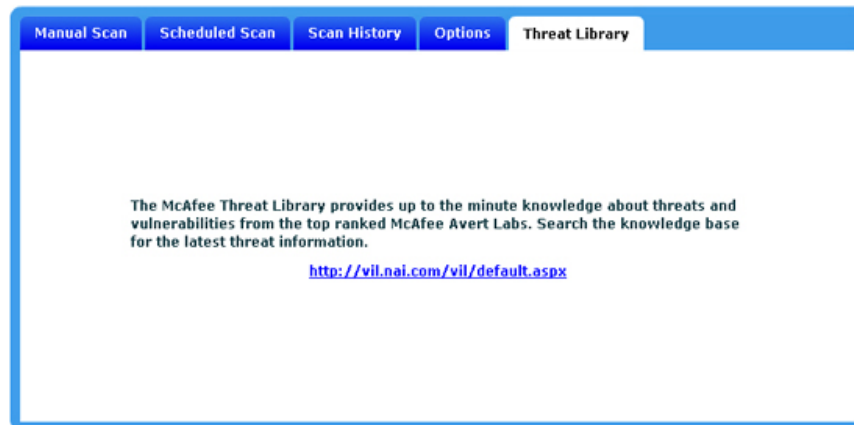


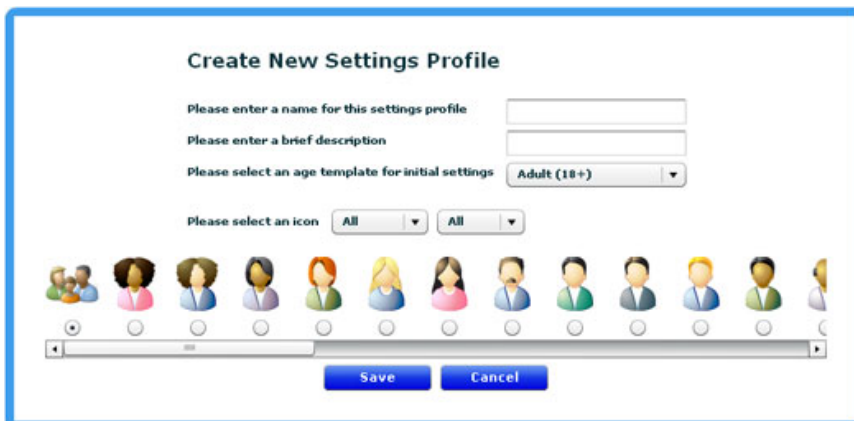
Figure D.10: Threat Library

SECTION E

HOW TO

How to add a profile


1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **Add Profile** link; this will open the "create new settings profile" panel.
3. Enter a name for the new profile (**required**).
4. Enter a brief description for the new profile (optional).
5. Select an age group from the **age template initial settings** dropdown menu.
6. Select the icon you would like to use for the new profile. The icons can be displayed by groups, male, female, adult, teens, youth, and child. For example, you can choose to only view male - teen icons.
7. Click the save button to save your new profile.



The screenshot shows a web form titled "Create New Settings Profile". It contains the following fields and controls:

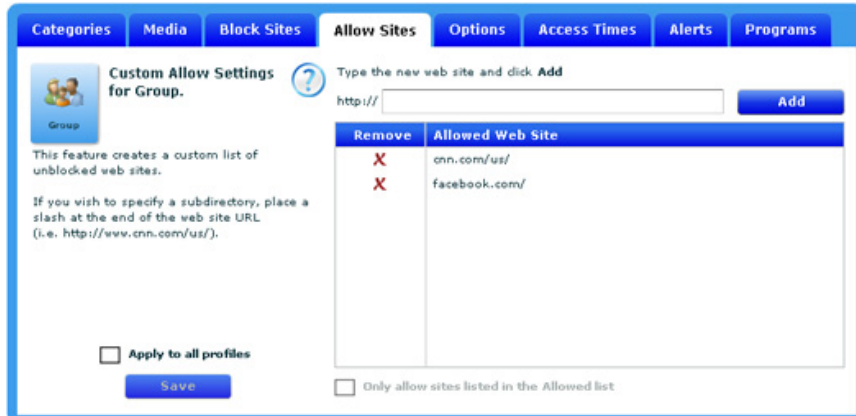
- A text input field for "Please enter a name for this settings profile".
- A text input field for "Please enter a brief description".
- A dropdown menu for "Please select an age template for initial settings" with "Adult (18+)" selected.
- Two dropdown menus for "Please select an icon", both set to "All".
- A horizontal scrollable list of 12 profile icons (male and female avatars of various ages).
- At the bottom, there are "Save" and "Cancel" buttons.

How to add a site to the allow sites list

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Allow Sites tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. In the provided **text box**, type the URL of a Web site that you want to allow.
6. **Click Add**. The Web site is added to the Allowed Web sites List.
7. **Repeat** the steps 5 and 6 to add additional Web sites to your Allow Sites list.
8. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.


Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*



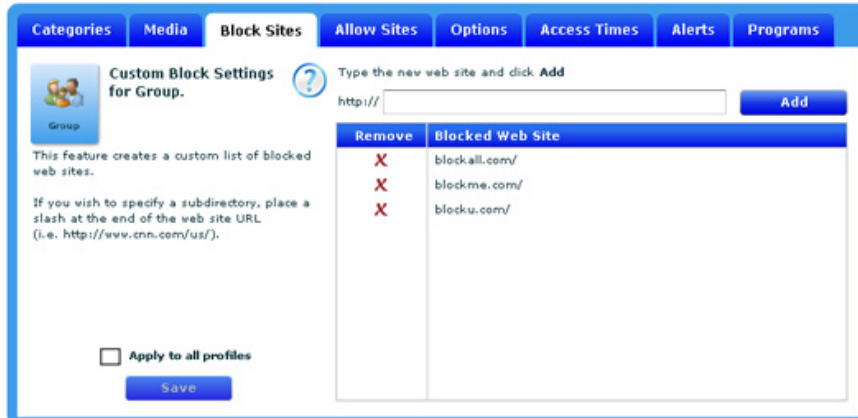
Remove	Allowed Web Site
X	cnn.com/us/
X	facebook.com/

How to add a site to the block sites list

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Block Sites tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. In the provided **text box**, type the URL of a Web site that you want to block .
6. **Click Add**. The Web site is added to the Allowed Web sites List.
7. **Repeat the steps 5 and 6** to add additional Web sites to your Allow Sites list.
8. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.



Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*




Remove	Blocked Web Site
X	blockall.com/
X	blockme.com/
X	blocku.com/


How to allow media using ratings

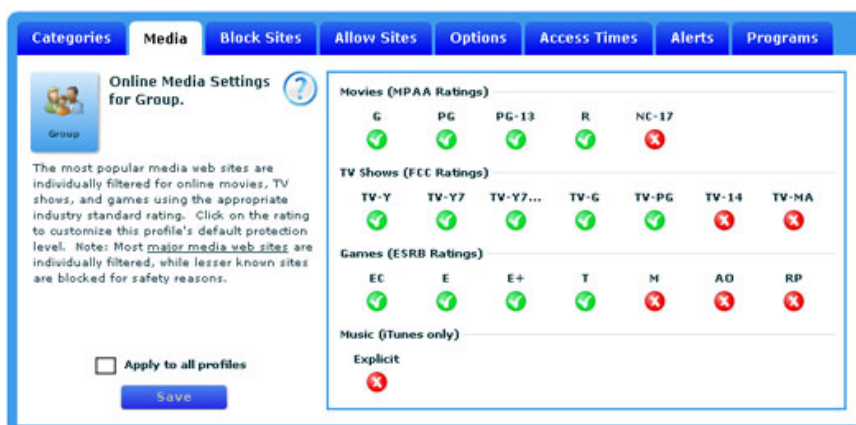
1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Media tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. Select the highest rating to be allowed . The selected rating and all ratings "below" (to the left of) the selection will automatically be included or allowed. Additionally, all ratings above (to the right of) the selection will be excluded or blocked. For example, if you elect to allow R rated movies, all the ratings listed to the left of "R" (i.e. PG-13, PG, and G) will automatically be allowed as well.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only unless "apply to all profiles" is selected.*

 = Media to be **blocked**

 = Media to be **allowed**



The screenshot shows the "Media" tab in the bsecure online interface. It displays settings for "Online Media Settings for Group". The settings are organized into sections: Movies (MPAA Ratings), TV Shows (FCC Ratings), Games (ESRB Ratings), and Music (iTunes only). Each section has a grid of ratings with green checkmarks indicating allowed content and red X's indicating blocked content.

Category	Rating	Status
Movies (MPAA Ratings)	G	Allowed
	PG	Allowed
	PG-13	Allowed
	R	Allowed
	NC-17	Blocked
TV Shows (FCC Ratings)	TV-Y	Allowed
	TV-Y7	Allowed
	TV-Y7...	Allowed
	TV-G	Allowed
	TV-PG	Allowed
	TV-14	Blocked
	TV-MA	Blocked
Games (ESRB Ratings)	EC	Allowed
	E	Allowed
	E+	Allowed
	T	Allowed
	M	Blocked
	AO	Blocked
	RP	Blocked
Music (iTunes only)	Explicit	Blocked

At the bottom left, there is a checkbox labeled "Apply to all profiles" which is currently unchecked, and a "Save" button.

How to apply changes to all profiles

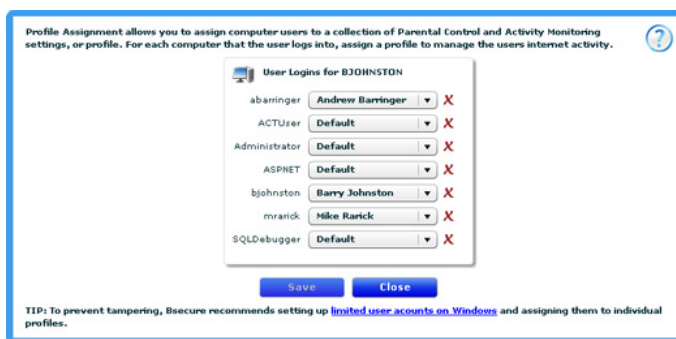
1. Select either the **Parental Controls tab** from the "Services tabs."
2. Select the "Feature tab" to modify (i.e. Categories, Media, Block Sites, Allow Sites, Options, Access Times, Alerts or Programs).
3. Select the profile that you would like to manage.
4. Make the desired changes to the profile's settings.
5. Select the "**apply to all profiles**" **check box** located on each of the Parental Control "Feature Tabs."
6. Click **Save** to preserve your changes.
7. Click **"Yes"** to confirm.

Note: Using the "apply to all" option **will overwrite the previous settings for every profile**. For example, if you add a site to a profile's allow sites list and you elect to "apply to all," this option does not just add the change to other profiles, **the entire** allow list settings will be applied and will replace the existing allow list settings for every profiles.

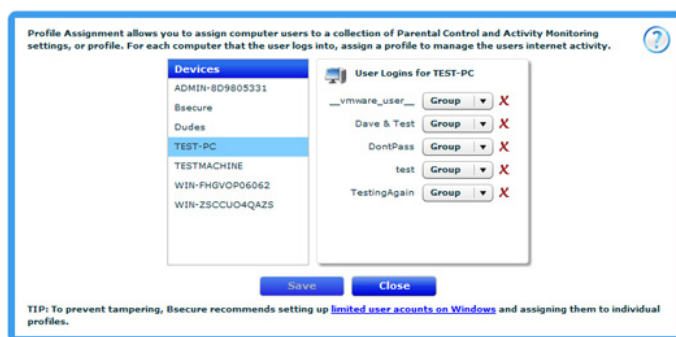


How to assign a profile

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **Assign Profile** link.
3. When there are **two or fewer devices**, listed are all the manageable devices and their logins. Click the drop down arrow next to the corresponding system / device login to select & assign one of the established profiles (available profiles will be visible in the profile management section).




When there are **three or more devices**, select the device from the list and then select the login to assign a profile.



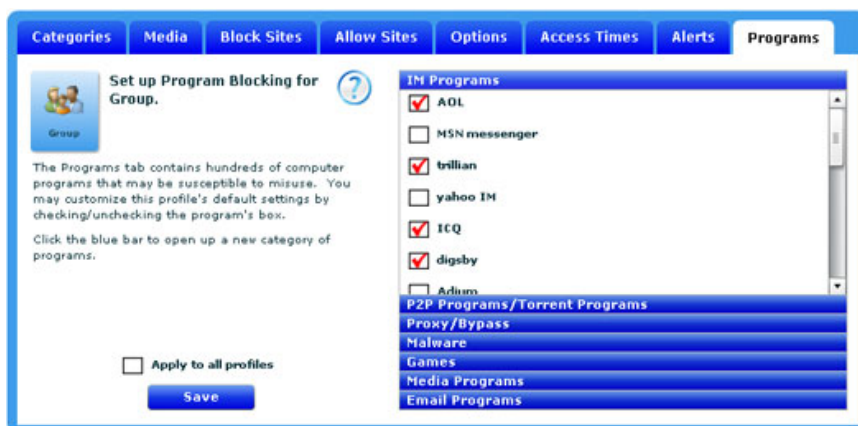
4. Click the **save button** to preserve your changes.

Note: To prevent tampering, Bsecure recommends setting up **limited user accounts** in Windows and assigning them to individual profiles.





How to block access to select programs on your PC

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Programs tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. Click the **blue bar** to open the listed program category.
6. Click the **box** next to the program you would like to block. A checked box indicates active blocking of the listed program for the current user setting.
7. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: Blocking one of these applications prevents the application from running, connecting to the Internet and sending out sensitive or other data from your computer. It **does not** prevent the download or install of the application.





How to block explicit music (iTunes only)

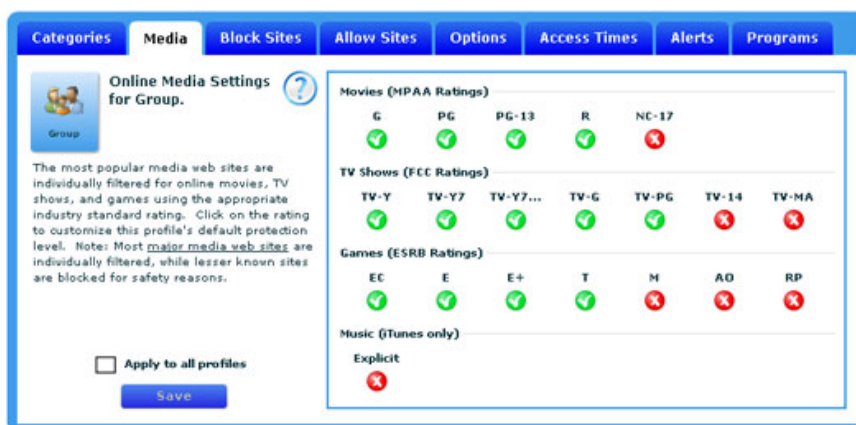
1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Media tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. Under Music, select the green check mark  to change it to . Explicit music will now be blocked for the selected profile, **in iTunes only**. The default setting for this feature is ON .
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.



**All changes made will be applied to the highlighted profile only unless "apply to all profiles" is selected.*

 = Media to be **blocked**

 = Media to be **allowed**




How to block media using ratings

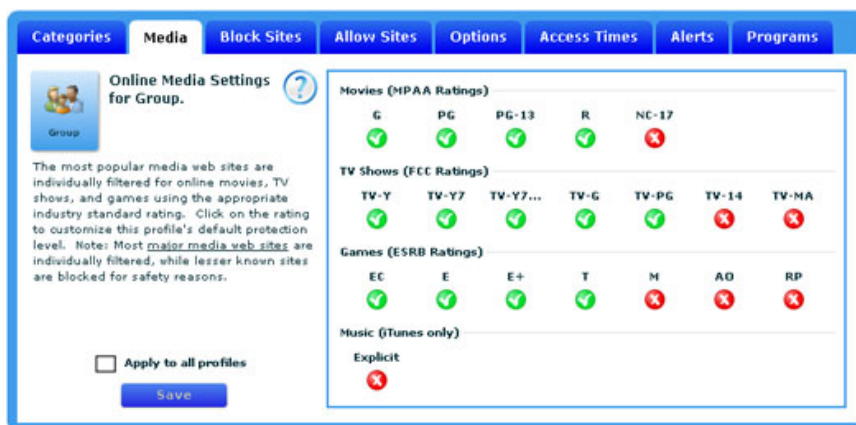
1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Media tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. Select the rating to be blocked . The selected rating and all ratings "above" (to the right of) the selection will automatically be included or blocked. For example, if you choose to block PG-13 movies, all ratings to the right of PG-13 (R & NC-17) will automatically be blocked as well.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only unless "apply to all profiles" is selected.*

 = Media to be **blocked**

 = Media to be **allowed**



Online Media Settings for Group.

The most popular media web sites are individually filtered for online movies, TV shows, and games using the appropriate industry standard rating. Click on the rating to customize this profile's default protection level. Note: Most major media web sites are individually filtered, while lesser known sites are blocked for safety reasons.

☒ Apply to all profiles

Save


Movies (MPAA Ratings)				
G	PG	PG-13	R	NC-17

TV Shows (FCC Ratings)						
TV-Y	TV-Y7	TV-Y7...	TV-G	TV-PG	TV-14	TV-MA

Games (ESRB Ratings)						
EC	E	E+	T	M	AO	RP

Music (iTunes only)
Explicit




How to block uncategorized websites

1. Select **Parental Controls** from the "Services tabs."
2. Select the **Categories tab** (if it is not already selected).
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. To block all unknown and non-categorized sites, **select the check box** located below the categories list. A check mark indicates that this feature is turned on.



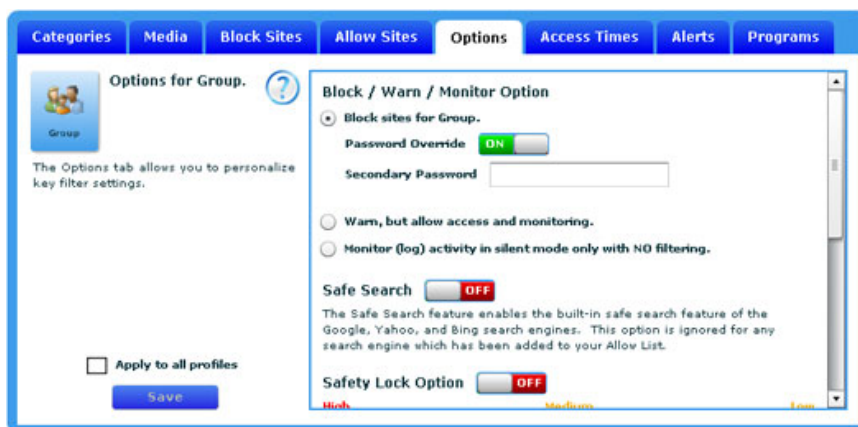
6. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

How to create a secondary password

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "Password" option in the window provided. The default setting for this feature is or OFF. Click the red OFF indicator  to display the green ON . The Password Override feature is now enabled.
6. Enter a secondary password in the text box provided.
7. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

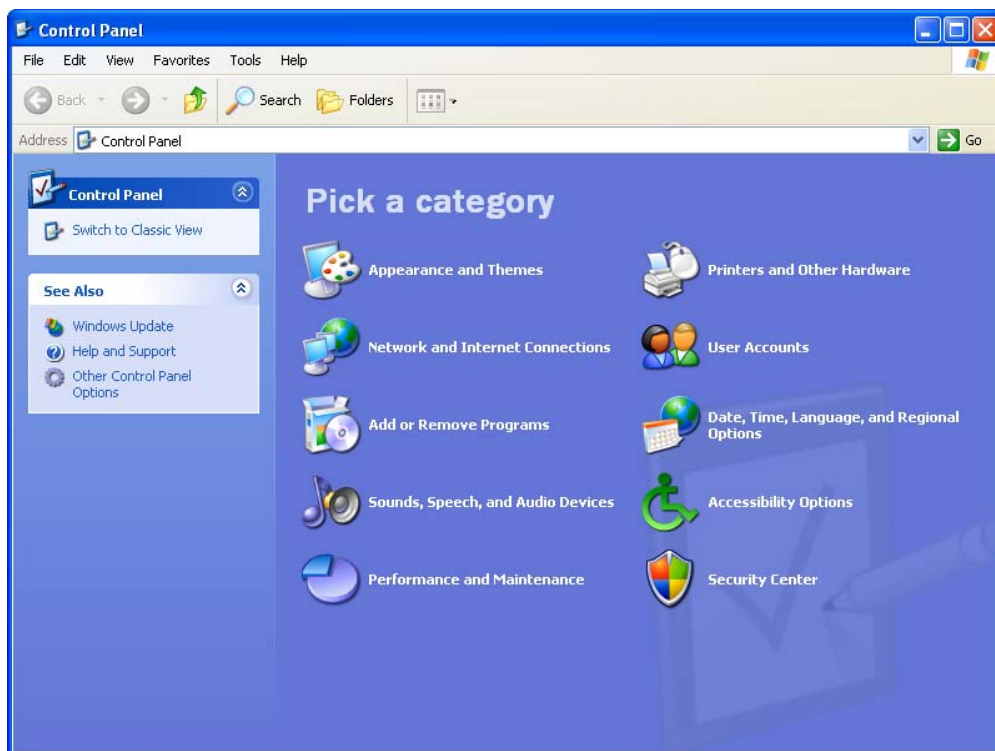
Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*




How to create a limited user account

1. Login to Windows as an **administrator**.
2. **Click Start** and then select the control panel.
3. Click on **user accounts**.
4. Depending on the version of Windows running on your machine, **select pick a task/create new account or the add button**.
5. **Type in the username** and click next.
6. Select **limited or restricted user**.
7. Click on **create account or finish**.



How to create a white list

1. Select **Parental Controls** from the "Services tabs."
2. Select **Allow Sites** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. **Select the box** below the Allowed Web sites list. A check mark indicates that the "white list" feature is turned on.

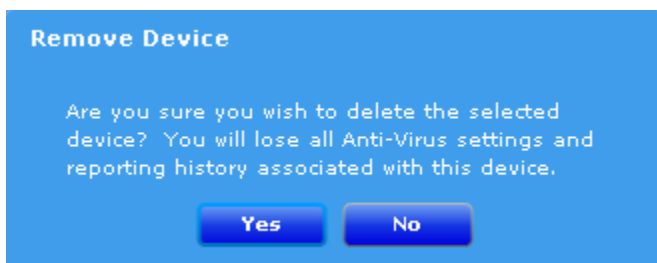
Note: **Block Sites** feature on the **Options Tab** must be **turned on** in order for this feature to be active. **The selected profile will only be able to navigate to web sites on this list.**




Only allow the web sites listed in the Allowed list

How to delete a computer

1. Select the **Security tab** from the "Services tabs."
2. Select the computer to be deleted.
3. Select the **red X** in the upper right corner of the computer's icon.
4. Click the **Yes button** to confirm the deletion of the selected computer.



How to edit a profile

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the profile that you would like to edit.
3. Click the  icon in the upper left corner of the selected profile.
4. Enter a **new name and/or brief description** for the profile.
5. Click the **save button** to preserve your changes.



Edit Profile

Please enter a name for this settings profile:

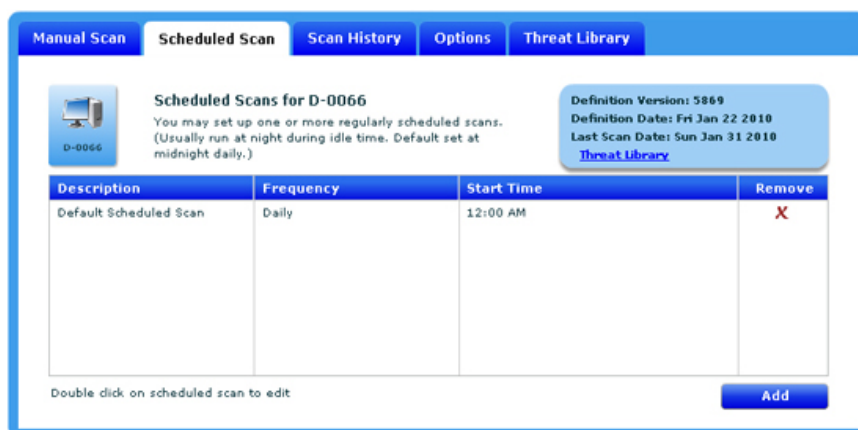
Please enter a brief description:

Please select an icon:


12 icons in a scrollable row

How to edit a scheduled scan

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."
3. Double Click on the Scheduled Scan to open the entry.
4. After making the desired changes, click the **Save** button.
5. **Repeat** for every Scheduled Scan entry to be edited.



How to restrict Internet access times

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Access Times tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. Verify that Parental Controls is turned ON  for the selected profile.
5. **Important:** Select your time zone from the drop down list.

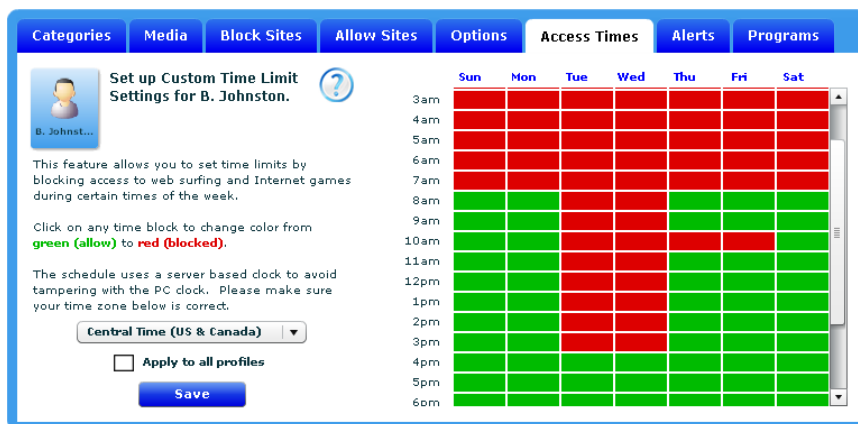
The schedule uses a server based clock to avoid tampering with the PC clock. Please make sure your time zone below is correct.

Central Time (US & Canada) ▼

6. **Click** the time block to change the color. **Green** blocks indicate times that are **allowed** and **red** blocks indicate times that are **blocked**. To select multiple time blocks, click in the initial time block and drag your mouse across the desired blocks.
7. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted profile only.*



The screenshot shows the 'Access Times' configuration page. On the left, there is a sidebar with a user profile icon and name 'B. Johnston...'. Below the name, it says 'Set up Custom Time Limit Settings for B. Johnston.' and provides instructions: 'This feature allows you to set time limits by blocking access to web surfing and Internet games during certain times of the week. Click on any time block to change color from green (allow) to red (blocked). The schedule uses a server based clock to avoid tampering with the PC clock. Please make sure your time zone below is correct.' Below this text is a dropdown menu set to 'Central Time (US & Canada)', a checkbox for 'Apply to all profiles', and a 'Save' button.

The main area displays a grid for the week of the month. The columns are labeled Sun, Mon, Tue, Wed, Thu, Fri, Sat. The rows are labeled with times from 3am to 6pm. The grid shows a schedule where access is blocked (red) from 3am to 7am on all days, and from 12pm to 1pm on Tuesday, Wednesday, and Thursday. Access is allowed (green) for all other times.

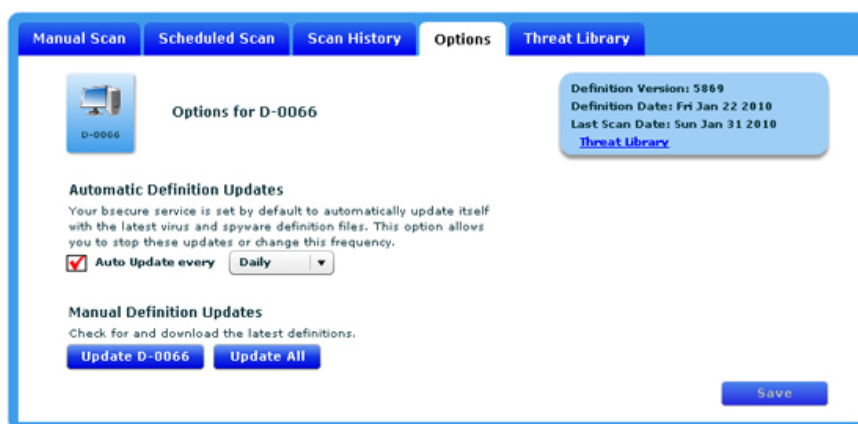
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
3am	Red	Red	Red	Red	Red	Red	Red
4am	Red	Red	Red	Red	Red	Red	Red
5am	Red	Red	Red	Red	Red	Red	Red
6am	Red	Red	Red	Red	Red	Red	Red
7am	Red	Red	Red	Red	Red	Red	Red
8am	Green	Green	Red	Red	Green	Green	Green
9am	Green	Green	Red	Red	Green	Green	Green
10am	Green	Green	Red	Red	Green	Green	Green
11am	Green	Green	Red	Red	Green	Green	Green
12pm	Green	Green	Red	Red	Green	Green	Green
1pm	Green	Green	Red	Red	Green	Green	Green
2pm	Green	Green	Red	Red	Green	Green	Green
3pm	Green	Green	Red	Red	Green	Green	Green
4pm	Green	Green	Red	Red	Green	Green	Green
5pm	Green	Green	Red	Red	Green	Green	Green
6pm	Green	Green	Red	Red	Green	Green	Green

How to manually update anti-virus files

1. Select the **Security tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Click the **Update (device name)** button for a single device *or*
4. Click the **Update All** button to check updates for all recognized devices.
5. **Click Save** to preserve your settings.


Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

**All changes made will be applied to the highlighted device only.*



How to monitor a profile in silent mode

Use the **Block / Warn / Monitor** feature to establish the internet permission level for your profiles. The following permission levels are available:

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. From the **Block / Warn / Monitor Option** section, select the *"Monitor (log) activity in silent mode only with NO filtering."*
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

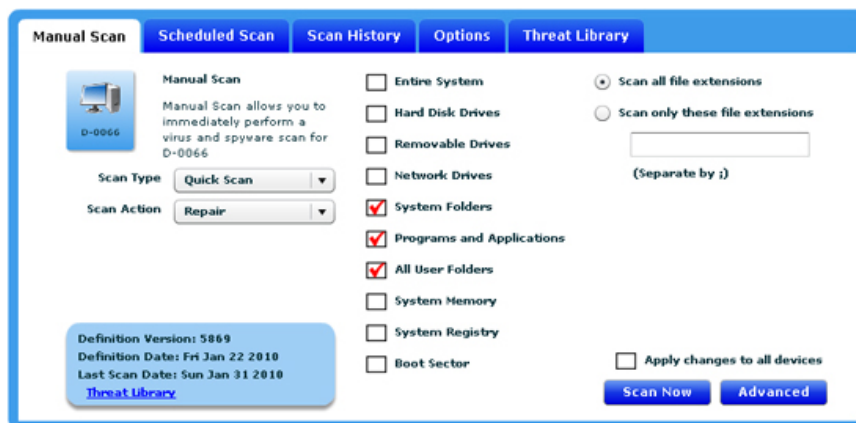
**All changes made will be applied to the highlighted profile only unless "apply to all profiles" is selected.*

The selected profile will have unrestricted internet access and will not receive block or warn pages.



How to perform a manual virus scan


1. Select the **Security tab** from the "Services tabs."
2. Select the **Manual Scan tab** from the "Features tabs."
3. Click the **Scan Type** drop down menu and select the type of scan desired.



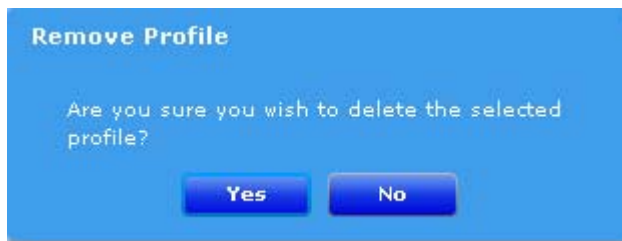
4. Click the **Scan Action drop down** menu and select the scan action desired.
5. To scan all files - **Select** the button next to "**Scan all file extensions**" or
6. To scan specific files - **Select** the button next to "**Scan files with supplied extensions.**" With this option selected, you must enter at least one file extension in the text box provided. Use a ":" to separate multiple entries (exe; doc).
7. Select the box for **at least one location** to be scanned. You can choose to scan the entire system or scan multiple locations.
8. To scan all recognized devices with this manual scan, **select** the box to "**apply changes to all devices.**"
9. Click the **Advanced** button to **select directories** to scan.
10. Click the Scan Now button to begin the manual scan.

How to remove a profile

1. Select either the **Activity Monitoring or Parental Controls tab** from the "Services tabs."
2. Select the profile that you would like to remove.

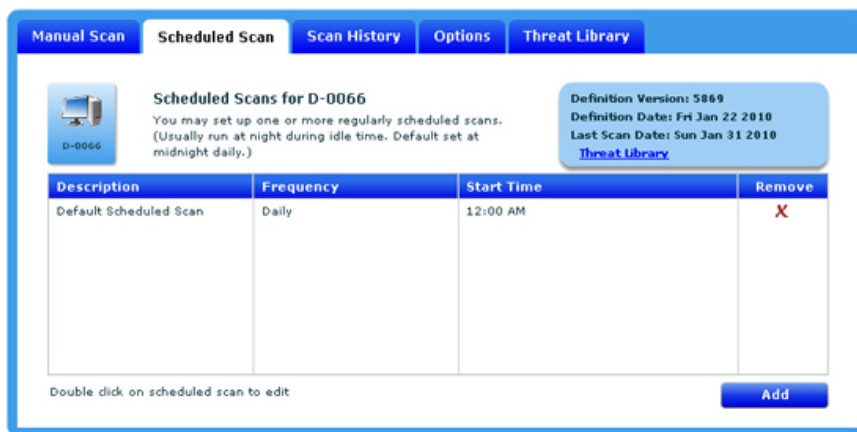
Note: The **administrative profile cannot be removed**. However, it can be renamed by clicking on the  icon, located in the top left corner of the selected profile.

3. Select the **red X** in the upper right corner of the profile's icon.
4. Click the **Yes button** to confirm the deletion of the selected profile.



How to remove a scheduled scan

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."
3. Click on the **red X** next to the Scheduled Scan.
4. **Repeat** for every Scheduled Scan entry to be deleted.



How to remove a site from the allow sites list

1. Select **Parental Controls** from the "Services tabs."
2. Select **Allow Sites** from the "Features tabs."
3. Select the profile that you would like to manage.
4. Click on the **red X** next to the Web site entry.
5. **Repeat** for every Web site entry to be deleted.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Categories **Media** **Block Sites** **Allow Sites** **Options** **Access Times** **Alerts** **Programs**

Custom Allow Settings for Group.

This feature creates a custom list of unblocked web sites.

If you wish to specify a subdirectory, place a slash at the end of the web site URL (i.e. <http://www.cnn.com/us/>).

☐ **Apply to all profiles**

Save

Type the new web site and click **Add**

<http://> **Add**

Remove	Allowed Web Site
X	cnn.com/us/
X	facebook.com/

☐ Only allow sites listed in the Allowed list

How to remove a site from the block sites list

1. Select **Parental Controls** from the "Services tabs."
2. Select **Block Sites** from the "Features tabs."
3. Select the profile that you would like to manage.
4. Click on the **red X** next to the Web site entry.
5. **Repeat** for every Web site entry to be deleted.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Custom Block Settings for Group.

This feature creates a custom list of blocked web sites.

If you wish to specify a subdirectory, place a slash at the end of the web site URL (i.e. <http://www.cnn.com/us/>).

☐ Apply to all profiles

Save

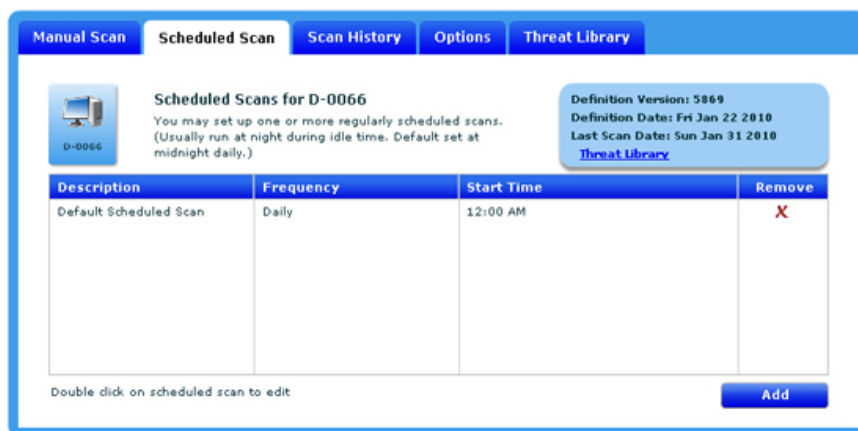
Type the new web site and click **Add**

<http://> **Add**

Remove	Blocked Web Site
X	blockall.com/
X	blockme.com/
X	blocku.com/


How to schedule an automatic virus scan

1. Select the **Security tab** from the "Services tabs."
2. Select the **Scheduled Scan tab** from the "Features tabs."
3. Click the **Add button** located in the bottom right corner of the window.



4. **Type a name** for the scheduled scan in the box next to Scan Name.
5. Click the **Scan Type drop down** menu and select the type of scan desired.
6. Click the **Scan Action drop down** menu and select the scan action desired.
7. Click the **Every drop down** menu and select the day of week desired.
8. Click the **Start Time drop down** menu and select the time desired.
9. To scan all files - **Select** the button next to "**Scan all file extensions**" **or**
10. To scan specific files - **Select** the button next to "**Scan only these file extensions.**"
With this option selected, you must enter at least one file extension in the text box provided. Use a ";" to separate multiple entries (exe; doc).
11. Select the box for at least one **location** to be scanned. You can choose to scan the entire system or scan multiple locations.
12. To scan all recognized devices with this scheduled scan, **select** the box to "**apply changes to all devices.**"
13. Click the **Save** button to preserve your settings.

How to setup email alerts

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Alerts tab** from the "Features tabs."
3. Verify that both **Parental Controls** and **Parent Alerts** are **turned on**  for the selected profile.



4. **Enter** the email address in the text box provided under the email address section.
5. **Click** the add button to add the email address to your email list.

To add an e-mail address, type it in here, then click **Add**

Add

6. **Repeat** steps 4 and 5 for each email address that you would like to setup.
7. **Select** the "**Send test message**" box in order to verify your email alerts setup.


Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.

☐ **Send test message**

8. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

How to setup text (SMS) alerts


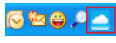



1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the profile that you would like to setup.
3. Select the **Alerts tab** from the "Features tabs."
4. Verify that both **Parental Controls** and **Alerts** are **turned on** .



5. **Enter** a mobile phone number in the text box provided under the mobile number section. Be sure to include the area code.
6. **Select** your mobile carrier from the list provided.
7. **Click** the add button to add the number to your mobile number list.

8. **Repeat** steps 5 thru 7 for each mobile number that you would like to setup.
9. Select the "**Send test message**" box in order to verify your SMS alerts setup.
Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.
10. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.




How to turn off activity monitoring

1. Double click the Bsecure Online desktop  or system tray icon .
2. Enter your login information to access the control panel.
3. Select the **Activity Monitoring** tab from the "Services tabs."
4. Select the **profile** that you would like to manage.
5. The default setting for this feature is ON .
6. **Click** the green ON  to display the red OFF  indicator located in the top right corner of the console.

Note: The Activity Monitoring feature is now disabled for the **selected profile only**.

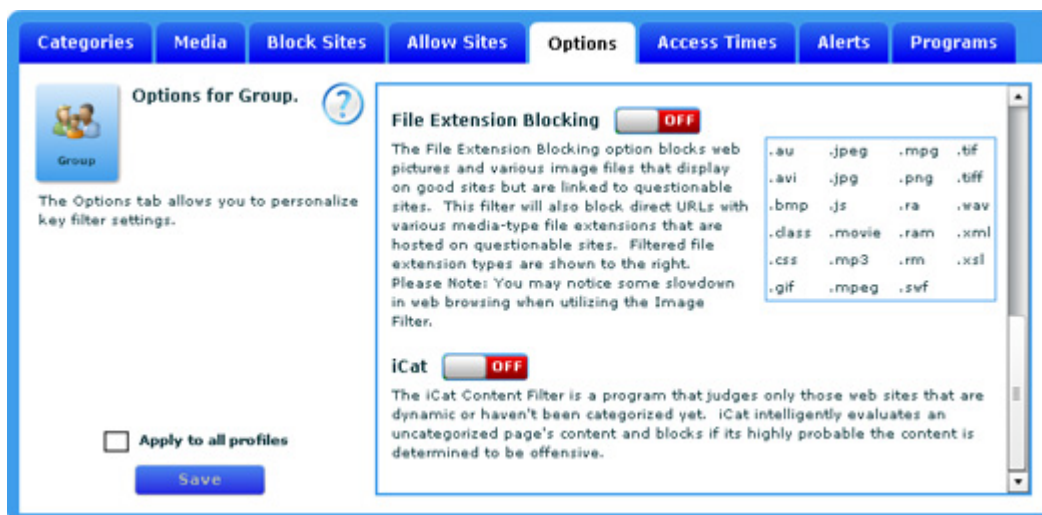


How to turn off the iCat feature



1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Verify** that Parental Controls is turned ON  for the selected profile.
5. **Drag the scroll bar** to show the "iCat" on / off switch in the window provided. The iCat feature is on when the green ON  indicator is displayed. Click the ON switch to change the indicator to a red OFF . The iCat feature is now disabled.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the Save Changes message appears.

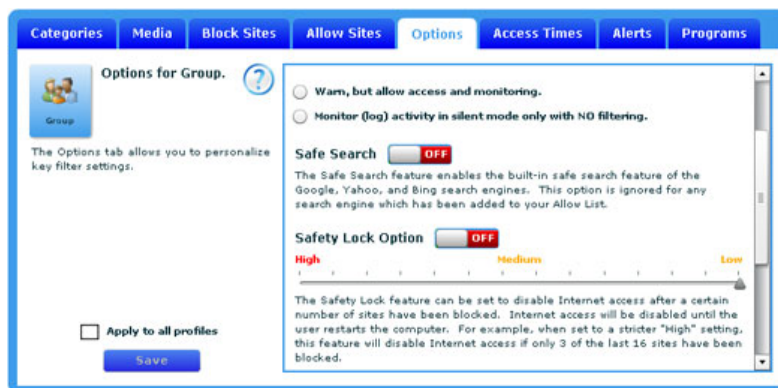
**All changes made will be applied to the highlighted profile only.*






How to turn on the safe search feature

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the **Options tab** from the "Features tabs."
3. Select the **profile** that you would like to manage.
4. **Drag the scroll bar** to show the "Safe Search" option in the window provided. The default setting for this feature is ON. Click the red OFF indicator  to display the green ON . The Safe Search feature is now enabled.
5. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

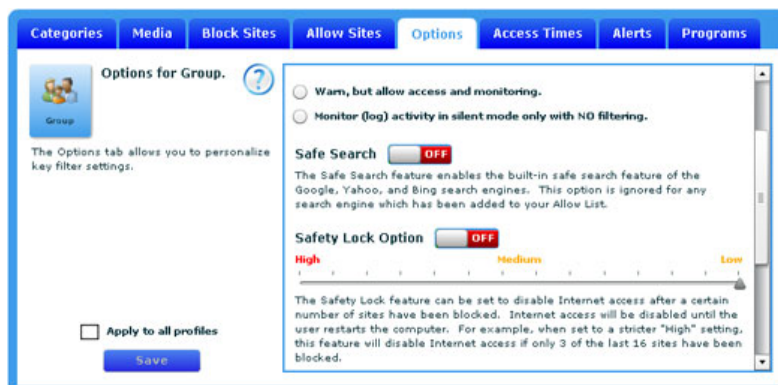
Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.







How to turn off the safe search feature

1. Select the **profile** that you would like to manage.
2. Select the **Parental Controls tab** from the "Services tabs."
3. Verify that Parental Controls is turned ON  for the selected profile.
4. Select the **Options tab** from the "Features tabs."
5. **Drag the scroll bar** to show the "Safe Search" option in the window provided. The default setting for this feature is ON. Click the green ON indicator  to display the red OFF .
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to preserve your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.





How to turn off social site reporting

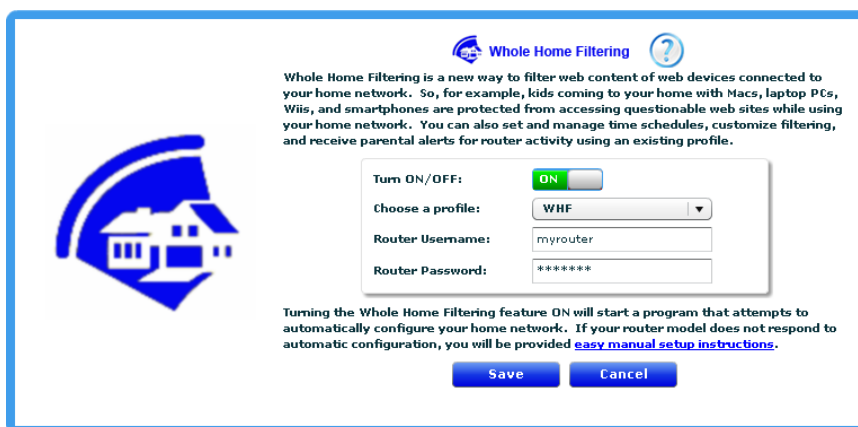
1. Double click the Bsecure Online desktop  or system tray icon .
2. Enter your login information to access the control panel.
3. Select **Activity Monitoring** from the "Services tabs".
4. Select the **Social Sites** tab.
5. Select the **profile** to be managed.
6. Click the green ON indicator  to display the red OFF . The Social Site reporting featured is now disabled for the selected profile.



How to assign a profile for Whole Home Filtering (WHF)

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **Whole Home Filtering** link; this will open the "Whole Home Filtering" panel.
3. Click the red OFF indicator  to display the green ON . The WHF feature is now enabled.
4. Choose the profile setting that you would like to assign to the WHF network. This can be any of the already established profiles or you can create a "new" profile specifically for your WHF (see the how to add a profile section).
5. Enter your username and password for your home network's router.
6. **Click Save** to preserve your settings.

Note: It is recommended that you create an exclusive WHF profile for managing your network's filter settings. If you change routers, you will need to reestablish your WHF settings.



Whole Home Filtering ?

Whole Home Filtering is a new way to filter web content of web devices connected to your home network. So, for example, kids coming to your home with Macs, laptop PCs, Wiis, and smartphones are protected from accessing questionable web sites while using your home network. You can also set and manage time schedules, customize filtering, and receive parental alerts for router activity using an existing profile.

Turn ON/OFF: ☒ ON ☐ OFF

Choose a profile:

Router Username:

Router Password:

Turning the Whole Home Filtering feature ON will start a program that attempts to automatically configure your home network. If your router model does not respond to automatic configuration, you will be provided [easy manual setup instructions](#).

How to manually setup your router for Bsecure Online WHF Services

1. Open the preferences for your router.

Note: Only do this when connected to the Internet through your home network router.

- a. Often, the preferences are set in your web browser, via a URL with the routers IP address which is represented by numbers (example: http://192.168.0.1). You may need to enter a password.

Note: If you set the router password long ago and cannot remember it now, you can often reset the password to the manufacturer default by pressing a button on the router itself.

- b. Or preferences may be set via specific application for your router, which you installed on your computer when you added the router.

2. **Find** the DNS server settings.

- a. Scan for the letters DNS next to a field which allows two or three sets of numbers, each broken into four groups of one to three numbers. It might look like this:

64	.	158	.	219	.	100
64	.	158	.	219	.	200

3. **Write down your current settings** before entering the Bsecure Online DNS addresses, just in case you should ever want to change them back.
4. **Enter** the following Bsecure Online **DNS server addresses** as your DNS server settings:

165	.	193	.	49	.	62
174	.	78	.	110	.	62

5. **Select** save or apply.

How to restrict Whole Home Filtering (WHF) Internet access times

1. Select the **Parental Controls tab** from the "Services tabs".
2. Select the **Access Times tab** from the "Features tabs".
3. Select the profile that you assigned on the WHF setup panel.

Note: If you have not already done so, you may want to setup an exclusive profile for WHF.

4. **Important:** Select your time zone from the drop down list.

The schedule uses a server based clock to avoid tampering with the PC clock. Please make sure your time zone below is correct.

Central Time (US & Canada) ▼

5. **Click** the time block to change the color. **Green** blocks indicate times that are **allowed** and **red** blocks indicate times that are **blocked**. To select multiple time blocks, click in the initial time block and drag your mouse across the desired blocks.
6. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

Categories Media Block Sites Allow Sites Options **Access Times** Alerts Programs

Set up Custom Time Limit Settings for Group. ?

Group

This feature allows you to set time limits by blocking access to web surfing and Internet games during certain times of the week.

Click on any time block to change color from **green (allow)** to **red (blocked)**.

The schedule uses a server based clock to avoid tampering with the PC clock. Please make sure your time zone below is correct.

Central Time (US & Canada) ▼

☐ Apply to all profiles

Save

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12am	Red	Red	Red	Red	Red	Red	Red
1am	Red	Red	Red	Red	Red	Red	Red
2am	Red	Red	Red	Red	Red	Red	Red
3am	Red	Red	Red	Red	Red	Red	Red
4am	Green	Green	Red	Red	Red	Red	Green
5am	Green	Green	Red	Red	Red	Red	Green
6am	Green	Green	Red	Red	Red	Red	Green
7am	Green	Green	Red	Red	Red	Red	Green
8am	Green	Green	Red	Red	Red	Red	Green
9am	Green	Green	Red	Red	Red	Red	Green
10am	Green	Green	Red	Red	Red	Red	Green
11am	Green	Green	Red	Red	Red	Red	Green
12pm	Green	Green	Red	Red	Red	Red	Green
1pm	Green	Green	Red	Red	Red	Red	Green
2pm	Green	Green	Red	Red	Red	Red	Green
3pm	Green	Green	Red	Red	Red	Red	Green

How to setup Whole Home Filtering (WHF) text (SMS) alerts

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the profile that you assigned on the WHF setup panel.
Note: If you have not already done so, you may want to setup an exclusive profile for WHF.
3. Select the **Alerts tab** from the Features tabs.
4. Verify that **Parent Alerts** is **turned on**.



5. **Enter** a mobile phone number in the text box provided under the mobile number section. Be sure to include the area code.
6. **Select** your mobile carrier from the list provided.
7. **Click** the add button to add the number to your mobile number list.

8. **Repeat** steps 5 thru 7 for each mobile number that you would like to setup.
9. Select the **"Send test message"** box in order to verify your SMS alerts setup.
Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.
10. Select the **"Apply to all profiles"** box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.

How to setup Whole Home Filtering (WHF) email alerts

1. Select the **Parental Controls tab** from the "Services tabs."
2. Select the profile that you assigned on the WHF setup panel.
Note: If you have not already done so, you may want to setup an exclusive profile for WHF.
3. Select the **Alerts tab** from the Features tabs.
4. Verify that **Parent Alerts** is **turned on**.





5. **Enter** the email address in the text box provided under the email address section.
6. **Click** the add button to add the email address to your email list.

To add an e-mail address, type it in here, then click **Add**

Add

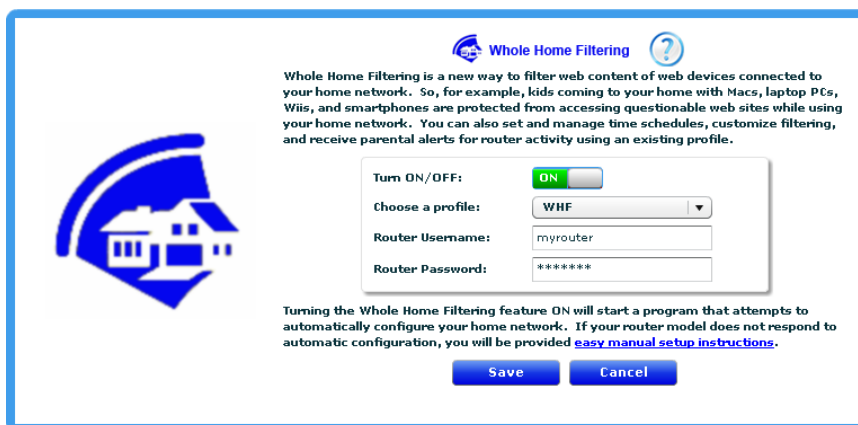
7. **Repeat** steps 5 and 6 for each email address that you would like to setup.
8. Select the "**Send test message**" box in order to verify your email alerts setup.
Note: Alerts are sent out in one minute intervals. Please allow at least one minute between each test.
9. Select the "**Apply to all profiles**" box if you would like the changes applied to all of your established profiles. **Click Save** to save your settings.
Note: If you navigate away from this section before saving your changes, the **Save Changes** message appears.

How to turn on Whole Home Filtering (WHF)

1. Select either the **Activity Monitoring** or **Parental Controls** tab from the "Services tabs."
2. Select the **Whole Home Filtering** link; this will open the "Whole Home Filtering" panel.
3. Click the red OFF indicator  to display the green ON . The WHF feature is now enabled.
4. Choose the profile setting that you would like to assign to the WHF network. This can be any of the already established profiles or you can create a "new" profile specifically for your WHF (see the how to add a profile section).
5. Enter your username and password for your home network's router.
6. **Click Save** to preserve your settings.


Note: It is recommended that you create an **exclusive WHF profile** for managing your network's filter settings.

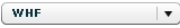
If you change routers, you will need to reestablish your WHF settings.



Whole Home Filtering ?

Whole Home Filtering is a new way to filter web content of web devices connected to your home network. So, for example, kids coming to your home with Macs, laptop PCs, Wiis, and smartphones are protected from accessing questionable web sites while using your home network. You can also set and manage time schedules, customize filtering, and receive parental alerts for router activity using an existing profile.

Turn ON/OFF: 

Choose a profile: 

Router Username:

Router Password:

Turning the Whole Home Filtering feature ON will start a program that attempts to automatically configure your home network. If your router model does not respond to automatic configuration, you will be provided [easy manual setup instructions](#).

Save **Cancel**