



# SecureIT Plus

## Parental Controls Module



User's Guide

# Contents

<b>Parental Controls Overview.....</b>	<b>3</b>
<b>Enabling Your Parental Controls.....</b>	<b>3</b>
Running the Setup Wizard .....	4
Adding Users.....	4
Deleting Users .....	4
Setting Passwords.....	4
Changing Passwords .....	5
Setup Access .....	5
Tooltips.....	6
Setup Complete .....	6
<b>Managing User Specific Settings.....</b>	<b>6</b>
General Settings .....	6
Filter Settings .....	7
Time Controls .....	8
White List .....	9
Blocked Sites.....	9
Accessing the Internet.....	10
<b>Reporting / Monitoring.....</b>	<b>11</b>
<b>Automatic Updates.....</b>	<b>14</b>

## Notice to Users

©2007 SecurityCoverage, Inc. All rights reserved. This manual in whole or in part, may not be reproduced, translated, or reduced to any machine readable form without prior written approval.

SECURITYCOVERAGE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL. THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCALIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL. THE SOFTWARE, OR SUCH OTHER INFOMRTION, IN NO EVENT SHALL SECURITYCOVERAGE, INC BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, WHTER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL. THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

SecurityCoverage, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software describes herein is governed by the terms of a separate user license agreement

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions. SecurityCoverage, the SecurityCoverage and SecureIT Services logo are trademarks of SecurityCoverage, Inc. All other trademarks are trademarks of their respective owners.

## **Parental Controls Overview**

The Internet is becoming a routine part of the way we live our lives. Every day it seems we find at least one reason to use it. E-mails, online chatting with friends, banking, shopping, doing research for school, or simply playing an online game; the Internet is an extremely useful tool. However, with its use come inherent dangers – dangers that can also impact every aspect of your life including the safety of your family.

The Parental Controls feature found in SecureIT Plus assists you in managing the amount of time your family can spend on the Internet and helps you protect them from undesirable content that could ultimately prove harmful. This solution provides the following key elements to ensure the protection you need:

- Internet Content Filtering
- Internet Access Controls
- Time Management Controls.
- Monitoring / Reporting
- Automatic Updates

Control of the functions and features found in the Parental Controls Module of SecureIT Plus can be accessed in the Management Console through the SecureIT Controller icon found in your computer's icon tray. During the setup process, you can customize the level of control on a computer or user basis.

Use of this tool will help you monitor the Internet's use in your home and help you teach your family to make the best decisions in terms of accessing inappropriate websites. It is important to note that this technology will provide a level of support, but parental involvement is still the last line of defense in the protection of your family.

## **Enabling Parental Controls**

After installing SecureIT Plus with Parental Controls, the functionality is disabled by default and needs to be enabled. To enable Parental Controls, open the SecureIT Management Console by right-clicking on the gold padlock found in your icon tray. At the Management Console, select the "Parental Controls" button on the left hand navigation bar.

It is required that during setup, the administrator have administrative rights privileges on the computer.

At the Parental Controls page, click the white box entitled "Enable Parental Controls", in order to activate the service and begin setup.

## Running the Setup Wizard

When a user elects to enable Parental Controls, the Setup Wizard is launched. The Setup Wizard walks the user through the initial setup of the Parental Controls features, providing an opportunity to customize the settings or set them at a default level.

## Adding Users

Once Parental Controls are enabled, a username and password must be established for each user profile before being allowed to access the Internet. Profiles associated with the computer running SecureIT Plus are automatically detected and created in the Setup Users view. (See Figure 1).

The administrator can use this area to create new usernames and passwords for specific users that will be saved in the User Profiles section of the program.

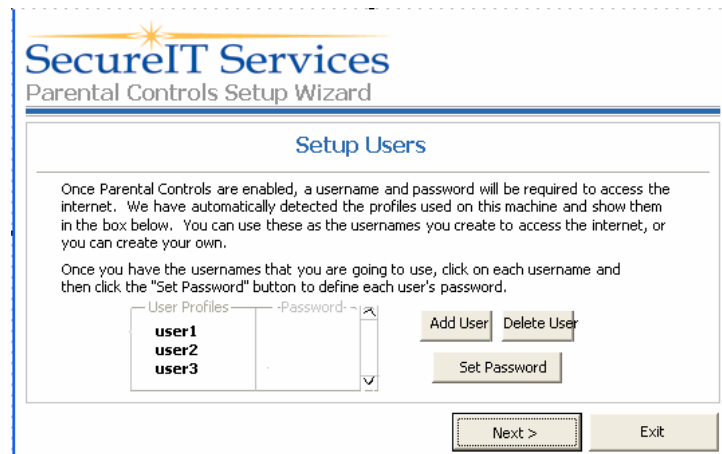


Figure 1

If there are no profiles found, a user profile called “Administrator” will be created. For windows variations prior to Windows 2000, the auto-detect function will not run. The administrator can add new users and passwords by selecting the “Add User” button.

## Deleting Users

If there are user profiles that are no longer used but were auto-detected during setup, or you simply wish to remove a user profile, it can be deleted by selecting the “Delete” button. Once the “Delete” button is clicked, the user disappears from the User Profiles column shown in Figure 1.

## Setting Passwords

In order to set an initial password associated with a valid user, select the appropriate user from the User Profiles list. Next, select the “Set Password” button. Type in a password

and then confirm the password by retyping it in the Confirm box below. If the password is accepted, the box will disappear and the screen shown in Figure 1 will appear.

If a password is not accepted, the user will receive a message stating “Passwords do not match. Please try again”. Select the “OK” button and re-enter the correct password information.

## **Changing Passwords**

To change an existing password for a valid user, access the Parental Controls main administration page. Next, select the “Set Password” button and follow the prompts to make the change.

If there is more than one administrator account set up on an individual machine, each would be allowed to make changes to passwords or settings of standard users. However, one administrator may not make changes to another administrator profile.

## **Setup Access**

The Setup Access page allows the administrator to define the types of sites that a user can see when surfing the internet. There are three levels of access that can be applied:

1. Administrator – This is the default access level for the initial user setup. Its access is unrestricted. There can be more than one account with Administrator access.
2. Default – This is the default access for all non-administrator profiles that are created in the setup wizard. The blocked categories for the Default setting include:
  - Adult/Mature
  - Pornography
  - Drugs/Alcohol
  - Gambling
  - Hate/Violence
  - Illegal Activities
  - Malicious Activity
3. Custom – Any changes from default are considered Custom changes. Custom changes can be made by selecting or unselecting specific categories in the Categories to Block section. When custom changes are made, the User Access column for that user it will automatically change from Default to Custom. (See Figure 2)

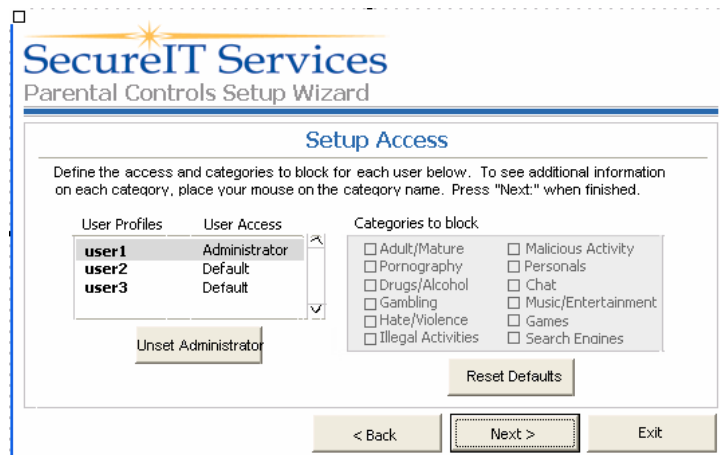


Figure 2

## Tooltips

To better understand the Categories to Block, a Tooltip has been created for each category. Tooltips are a description that explains the category in further detail and can be viewed by placing the cursor over a specific category.

## Setup Complete

Once all selections have been made, the user will receive a message entitled "Setup Complete". Select "Finish" to return to the Parental Controls section of the Management Console.

## Managing User Specific Settings

At the Management Console, select the "Settings" button to access various user specific settings options. These settings include:

- General Settings
- Filter Settings
- Time Controls
- White List
- Blocked Sites

## General Settings

The General Settings tab of Parental Controls allows user-level customization of specific applications, such as instant messaging, file sharing, and web browsing. This section has specific settings for:

- Instant Messaging blocking
- Peer-to-peer blocking (P2P)

- FTP Blocking
- Blocking of file downloads
- Inactivity timeout settings

These controls allow protection from outside users, files, and activity from harming your PC or family. (See Figure 3)

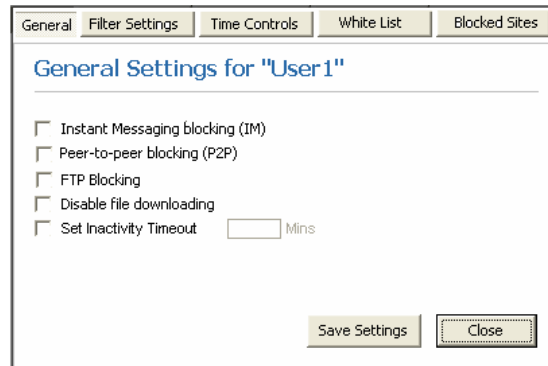


Figure 3

## Filter Settings

The Filter Settings Tab allows specific categories to be blocked based on User Profile. The library of these sites is maintained and updated on the program through the automatic updates feature. (See Figure 4)

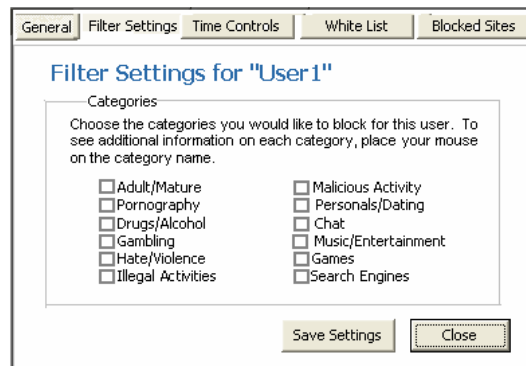


Figure 4

The following is a list of categories or activities that can be blocked:

- File Transfer (FTP) Blocking
- Adult/Mature – When selected, will block sites containing adult content, art nudes, sexuality, and naturism.
- Pornography – When selected, will block sites containing pornographic material.
- Drugs/Alcohol – When selected, will block sites containing drug and alcohol related content.

- Gambling – When selected, will block sites containing content gambling or related content.
- Hate/Violence – When selected, will block sites containing content related to aggression, violence, and weapons.
- Illegal Activities – When selected, will block sites containing content related to hacking, phishing, and warez.
- Malicious Activity – When selected, will block sites containing content related to ads, proxy, spyware, anti-spyware, update sites, virus infections, and dialers.
- Personals/Dating – When selected, will block sites containing content related to personal advertisements or dating.
- Chat – When selected, will block sites and content related to chat and instant messaging.
- Music/Entertainment – When selected, will block sites containing content related to music and entertainment.
- Games – When selected, will block sites containing content related to online games.
- Search Engines – When selected, will limit browser search engine results to items on an approved list of sites and activities for your children to enjoy.

## Time Controls

The Time Controls tab allows the administrator to set the number of hours per year, hours per month, hours per week and hours per day that a user can have access to the Internet. (See Figure 5)

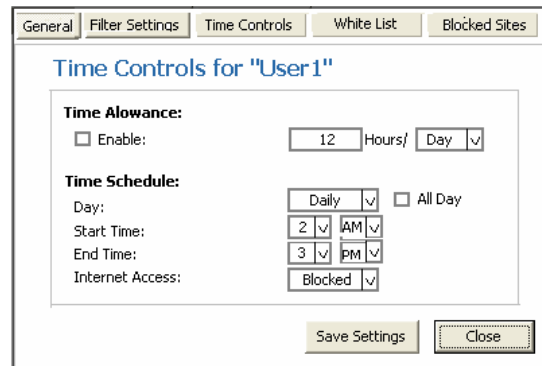


Figure 5

Additionally, controls can be placed on days of the week, and specific time periods. If attempts are made to access the Internet during the times that are not allowed, the user will receive a message indicating that the internet is not available to them at this time and to consult the administrator of the machine. (See Figure 6)

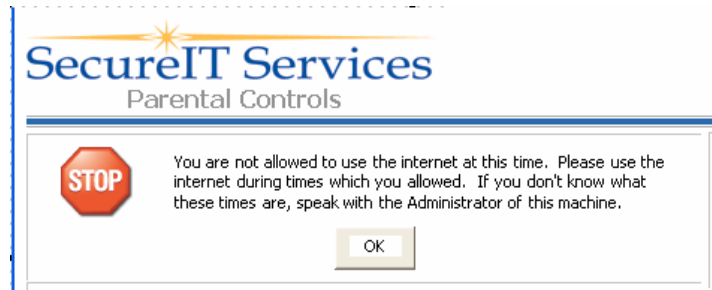


Figure 6

## White List

The White List tab allows the administrator to create a list of approved websites that a user can access regardless of their inclusion in a filtered or blocked group. (See Figure 7).

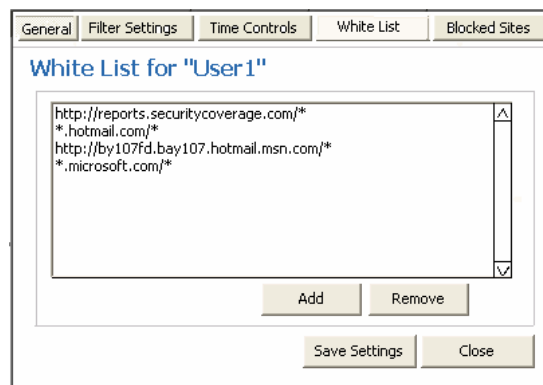


Figure 7

This feature allows the administrator to add a single site to the White List so that it can be accessed by a user who may not have access to other sites in a related category. Any sites on the White List will over-ride attempts to block access to it. The administrator can select the "Add" or "Remove" button to manage the sites on the White List.

## Blocked Sites

The Blocked Sites tab allows the administrator to create a list of blocked websites that even though they are excluded from a filtered or blocked group. (See Figure 8)

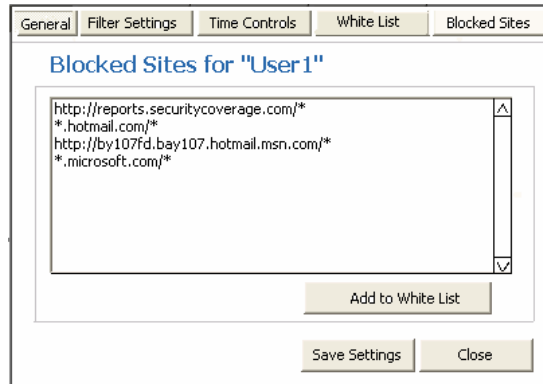


Figure 8

Although not part of a filtered or blocked category, sites appearing on the Blocked Sites tab will not be accessible to the user. The administrator can select the “Add” or “Remove” button to manage the sites on the Blocked Sites list.

### **Accessing the Internet**

After parental controls are configured and enabled, a user must log in with an appropriate username and password in order to access the Internet. (See Figure 9)



Figure 9

If the user uses the incorrect username and/or password and clicks the “Login” button, a box will come up and state “Login incorrect. Please type in the correct username and password.” Access to the Internet will not be granted until a valid username and password have been entered.

### **Attempts to Access a Filtered or Blocked Site**

Each time an attempt is made to access a filtered or blocked website, access to the site is denied and a message is sent to the browser window on the computer informing the user that access for that website is blocked. Reporting information is also logged and added to the reporting section on the Online Reports site.

## Overriding a Filtered or Blocked Site

If a site is filtered or blocked, a message will be displayed to the user with two buttons; “Back” and “Override”. (See Figure 10)

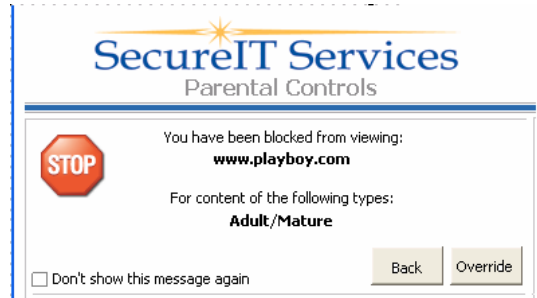


Figure 10

If the “Back” button is selected, it will return the user to their browser window, but will redirect to the page [www.securitycoverage.com](http://www.securitycoverage.com).

If the “Override” button is selected, it will prompt the user for a username and password. If a user who has Administrator access enters a correct username and password, it will allow this site to be accessed and will temporarily add the site to the White List.

## Reporting and Monitoring

In order to access the online reporting, a user must right-click on the gold padlock and select “Open SecureIT Online Reports”. (See Figure 11)

On this site, a user can see statistics including:

- Summary View
- Websites Accessed
- Chat Activity
- Security Violations



Figure 11



The Websites Accessed information can be filtered by:

- Today
- Yesterday
- 2 days ago
- Last week
- Two weeks ago
- Last month.

The information is available for each user profile associated with that machine.

## Chat Activity

The Chat Activity tab allows the users to see statistics related to chat activity. (See Figure 14) The categories include:

- Dates and times used
- Client used
- Amount of time spent on each session



Figure 14

The Chat Activity information can be filtered by:

- Today
- Yesterday
- 2 days ago
- Last week
- Two weeks ago
- Last month.

The information is available for each user profile associated with that machine.

## Security Violations

The Security Violations tab identifies the number of attempts made to access the Internet using an invalid username or Password.

The Security Violations information can be filtered by:

- Today
- Yesterday
- 2 days ago
- Last week
- Two weeks ago
- Last month.

The information is available for each user profile associated with that machine.

## Monitoring

Once a user initially logs on to the computer running SecureIT Plus with Parental Controls, the Internet history is recorded in a file on the users PC. This file is located in C:\Program Files\SecurityCoverage Help and Support Center\web\_[username].txt

Entries in the file are identified by day, time and website address. For example:

```
2006-07-21 15:36:00 – www.securitycoverage.com
2006-07-21 18:36:00 – www.website2.com
2006-07-22 04:36:00 – www.yahoo.com
2006-07-23 11:36:00 – www.securitycoverage.com
```

A similar file is also created that will keep track of all attempts made to blocked sites. This file is located in C:\Program Files\SecurityCoverage Help and Support Center\blocked\_[username].txt

These two log files would be reported on a daily basis and be used in showing the statistics shown in Figure 11

## Automatic Updates

As with all aspects of SecureIT Services, updates to the service are done automatically and without any user intervention. The user can control the specific time at which SecureIT Services will check for and apply any updates to the information used to operate the Parental Controls module.

To set this time, begin by selecting “Set Component Schedule” in the Management Console. Next, select Parental Controls to set the desired time to manage any updates. (See Figure 15)



Figure 15