

SecureWeb-*Personal*

User Manual

v3.3

SecureWeb Personal: User Manual

©1999-2006

All rights reserved.

ECS-Secure Ltd.
67 Park Street
Thame
Oxon
OX9 3HT

Main Phone Number:- 0845 127 9892
Support Phone Number:- 0845 127 9894
Fax Number 01844 261751

Email:- support@ecs-secure.com

Every effort has been made to ensure the accuracy of this manual. However, ECS-Secure Ltd. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. ECS-Secure Ltd. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

SecureWeb and ECS-Secure Ltd are trademarks or registered trademarks of ECS-Secure Ltd Incorporated in England and/or in other countries.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Preface

The SecureWeb Personal is a practical method to choose the Internet services and sites that you want to allow access to on your computer. Once installed, it gives you control over how people use the Internet on that computer.

There are two versions of SecureWeb available. SecureWeb Personal is intended for individual Personal Computers for residential use, as well as businesses without a domain server. The Small Business Edition is intended for larger businesses with a domain server.

This document describes the installation and initial configuration of the SecureWeb Personal on a single computer. It also provides some tips on managing Internet access as well as an introductory guide to using SecureWeb Personal for your computer.

About Profiles

SecureWeb uses "Profiles" to control access to the Internet (a profile is a collection of rules defining what can be reached across the internet). You can create a general profile that gives all the users of a computer the same restrictions on accessing the Internet or you can define separate Profiles, one for each user. To simplify the operation of SecureWeb, it is initially configured with a general profile called "Generous"; this restricts the access of all the users on the computer with a standard Profile to prevent anyone reaching negative websites containing Pornography, Gambling, Hate, etc. If you want a more sophisticated solution, you can create and modify Profiles for individual users later, see the "*Managing Profiles*" section of this manual.

With SecureWeb installed and set-up, before anyone can access the Internet, a Profile must be selected. When the computer restarts following the software installation for the first time, it connects automatically to the Internet, where the link between your PC to the SecureWeb Server is completed by entering your Profile Manager User Name and Password, this selects the "Generous" Profile by default. From then on, if you add or change profiles, you must select which Profile you want to be used before the computer is able to surf the net.

Table of Content

Installing the Client Filter	1
Check Before You Install	1
Disabling Firewalls	1
Norton Security Suite 2006.....	2
About Accelerators	2
Installation and Initial Configuration	3
Installation	3
First Time Login	3
Using the Internet with SecureWeb	4
No Profile Selected – You can't access the Internet	4
About the SecureWeb Icon	5
SecureWeb Icon Status:.....	5
Quick Reference Chart	6
About Popup Messages	8
<i>Hide Popup Messages</i>	8
<i>Show Popup Messages</i>	8
Status Page	9
Choose a Profile	10
Deny Page	11
Managing Profiles	12
Getting Started	12
Accessing Profile Manager	12
Using the Control Panel.....	12
<i>Forgotten Password</i>	13
<i>Control Panel Filter Settings</i>	14
Accessing the Profile Manager	15
Modifying Profiles	15
Recommendations	18
Web Categories	18
Instant Messaging	18
File Sharing Applications	18
Email	18
VOIP.....	18
Misc Protocols	18
Streaming Media	18
Advanced Features	19
Accessing the Profile Manager Remotely.....	19
About Mouse-Over Help	19
General Settings Tab of a Profile	20
About Filter Priorities	20
Allowing or Denying All Access	20
Enabling Safe Search	21
Blocking Search Keywords.....	21
Setting Profile Passwords	21
Resetting Profiles	22
Reporting Tab of a Profile	22
Selecting Categories Tab to Block and Unblock	23
Blocking or Unblocking Protocols Tab	24

About the Allow List Tab	25
About the Deny List Tab	26
Setting Time Restrictions Tab	27
Disabling the Filter	27
Preferences Settings	28
Active Profile Settings	28
<i>Retain Profile on restart</i>	28
<i>Exit Profile on restart</i>	28
<i>Use this Profile on restart</i>	29
<i>Allow "Remember my Profile"</i>	29
<i>Exit Profile on screensaver</i>	29
Choosing Profile Settings	29
Deny Page Settings.....	29
<i>Detailed deny page</i>	29
<i>Minimal deny page</i>	29
<i>No deny page</i>	29
<i>Include Quick Allow Access link</i>	30
<i>Include admin email link</i>	30
Profile Logout Settings	30
<i>No password required</i>	30
<i>Require Profile password</i>	30
<i>Require Profile Manager Password</i>	30
<i>Require this password:</i>	30
Submitting Sites for Review	31
Password Changing	32
Appendix: Category Descriptions	33
Adult	33
Alternative Lifestyles	33
Criminal Skills	33
Gambling	33
Extreme	33
Hate Speech	34
Substance Abuse	34
Match Making	34
Occult	34
Pornography	34
Entertainment	34
Arts & Culture	34
Entertainment	35
Games	35
Humor.....	35
Sports	35
Information	35
General News	35
Journals and Blogs	35
Politics	36
Portals.....	36
Religion	36
Self Help.....	36
Sex Education	36
Technology	36
Travel	37

Security	37
Adware	37
Directory	37
Host Is An IP	37
Malformed URL	37
Phishing	37
Proxy Anonymizer	38
Under Construction	38
Miscellaneous.....	38
Investing.....	38
Job Search	38
Sales	38
Search Engine.....	38
Web Chat	38
Web Email	39
Advanced Categories.....	39
General.....	39
Images	39
Network Unavailable	39
Network Timeout.....	39
Intranet Servers.....	39
New URL	40
No Text.....	40
Redirector Page.....	40
Troubleshooting.....	41
1) No Profile Selected - Can't access the Internet.....	41
2) Can't Access the Internet – Anti-Virus blocking it	42
Norton Security Suite 2006.....	42
3) Un-installing SecureWeb	43

Installing the Client Filter

Check Before You Install

During the installation procedure, you will need to restart the computer. The installation takes about a minute. After that, you may want to spend a few moments creating one or more filtering profiles. It takes about one minute to create a Profile.

Please ensure that you and your computer meet the following requirements:

- ◆ You need a Profile Manager Account name and password for SecureWeb Personal. This was sent to you by email, or can be provided by your administrator.
- ◆ Your computer needs to be running Windows XP (recommended) Home or Pro, Windows 2000, or Windows 98, (SecureWeb does work on Windows ME but it is not a preferred configuration). SecureWeb Personal does not operate on Apple Computers.
- ◆ You need about 8.5 MB of disk space on your computer (very little).
- ◆ You need to be logged in to the computer using an account that has Administrator level privileges.
- ◆ Your Windows operating system must be up-to-date with all high-priority security updates. You can do this at <http://update.microsoft.com>

Before you begin the installation procedure, please do the following:

- ◆ Log out of any other user accounts if you have multiple accounts and fast user switching enabled.
- ◆ If you are **not** using Microsoft Internet Explorer as your Internet browser, go to the home site for your browser and install any updates that may be available.
- ◆ Temporarily turn off any anti-virus or anti-spyware programs you may have running. You can turn them on again after you have installed SecureWeb.
- ◆ Save any open files and close any programs that you may have open.
- ◆ Close any Internet messaging applications you may have running, such as MSN Messenger, AOL Instant Messenger, or Yahoo Messenger.
- ◆ Close any file sharing applications, such as Kazaa, BitTorrent, or BearShare.
- ◆ Close any Voice over IP (VOIP) applications, such as Skype or SIP.
- ◆ Turn off Internet Explorer's Content Advisor if you have enabled it previously.

It is recommended that you do not configure your messaging, file sharing, or VOIP applications to automatically start on user login. These applications will not be able to connect to the Internet on restart until the user has chosen a Profile.

Disabling Firewalls

If you have a firewall installed, disable it before installing SecureWeb Personal. After installing, you can enable the firewall again but you need to adjust your firewall settings to always allow the SecureWeb program "nsfx.exe" to access to the Internet and if required open port 3432.

Norton Security Suite 2006

In some cases, Norton Internet Security Suite 2006 may block Internet traffic going through SecureWeb and other legitimate programs.

If you are running Norton Internet Security and try to install secureweb, a Norton Internet Security Message will pop-up telling you that secureweb is trying to access the internet, do you wish to allow it?

DO NOT ACCEPT THE NORTON DEFAULT POPUP OPTION

If you just accept the Norton recommended default option, secureweb will not complete the installation and will get no further than trying to validate the User Name and Password that you have entered. This problem arises because the default that Norton recommends is **"Always Block connections from this Program"** and as you might appreciate, if you accept the default which in most situations you would do, secureweb will be prevented from accessing the internet by Norton and secureweb will become completely non-functional, since it must be able to access the internet to do what it is designed for.

To prevent this problem occurring, during the installation process, when the Norton pop-up security message arises DO NOT accept the default option, but instead click the right-hand drop down option and change it to **"Always Allow connections from this program"**.

SecureWeb uses certain ports to monitor the Internet traffic to your system. The Internet cannot be accessed if these ports are blocked by a firewall application.

To unblock these ports that have been blocked by these firewall applications do the following:

1. Right click on the Norton globe icon in the system tray.
2. Select *Options > Internet Security*.
3. In the Norton Internet Security options dialog, select the *Firewall* tab.
4. In the HTTP port list, select 80 and click *Remove*.
5. Select 8080 and click *Remove*.
6. Select *Ok*.

Now you should be able to browse the Internet once again.

About Accelerators

If you use an Internet connection accelerator, such as Slipstream or Propel, in some cases it is important that the SecureWeb is installed after the accelerator.

If you already have an accelerator installed, there should be no difficulty installing the Client Filter.

If you are adding an accelerator to your connection and already have the SecureWeb installed, we recommend you do the following:

1. Uninstall the Client Filter.
2. Install the accelerator.
3. Reinstall the Client Filter.

By following these steps, the SecureWeb and accelerator should function together without a problem.

Installation and Initial Configuration

Please note that you need a Profile Manager Name and Password before you can install the Client Filter. Please contact ECS-Secure Ltd if you do not have this information. Perform the following steps to install and configure SecureWeb:

Installation

1. Launch the SecureWeb installation program.
2. If prompted, select the language you wish to use.
3. At the *Welcome* screen, select *Next* to begin the installation.
4. Read the License Agreement. You must accept the agreement to continue.
5. Select *I agree* to accept the agreement.
6. Select *Install* to install the program in the default folder. It is recommended that you use the default location.
7. Select *Finish* to restart the computer.

First Time Login

8. On restart, your Internet browser should start automatically. This may take a moment. Please be patient while SecureWeb communicates with the Policy Server for the first time. If the Internet browser does not start automatically, open the Internet browser and SecureWeb's First Time Login screen displays automatically.
9. Enter your Profile Manager name and password at the SecureWeb *First Time Login* screen and click continue:



You can now Surf the Internet, SecureWeb installs with a basic User Profile called "Generous" which blocks most of the things you would normally want blocked for a family, to modify this profile or add a new on see the section "*Managing Profiles*".

Using the Internet with SecureWeb

No Profile Selected – You can't access the Internet



Before SecureWeb can allow any access to the Internet, a Profile must first be selected (a Profile is a collection of rules defining what can and cannot be reached on the Internet) and hence for security, without a Profile being selected, SecureWeb won't allow any internet access.

On the initial installation, a standard Profile called "**Generous**" is installed which **does not** have a Password.

To select a Profile you need to open the Profile Selection Screen shown below, to reach this you use one of the following methods:-

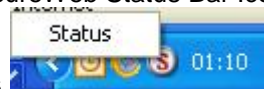
- 1) Double Click with the left mouse button on the SecureWeb Status Bar Icon



in the lower right corner of the screen.

- 2) Right Mouse click on the SecureWeb Status Bar Icon and then left click on

the Status Item that appears



- 3) In the Browser Address bar type <http://filter.secureweb.uk.com>



On this SecureWeb Profile Selection Screen just press "Continue".

About the SecureWeb Icon

Once SecureWeb has been installed on your computer, a red and white SecureWeb icon appears in the Windows System Tray at the bottom right corner of your screen. The icon looks like this:



By double-clicking on this icon, you can view the Status Page (see "*Status Page*"). By right-clicking on this icon, you can also choose to open the Status Page or log out of your current profile

SecureWeb Icon Status:

The SecureWeb Icon changes depending on the Client Filter's status. These animated icons are intended to inform you of what is going on and can help diagnose any problems.



The Internet service you tried to access was denied or redirected to another web site.



SecureWeb is unable to establish a connection with the Policy Server. Please check that your Internet connection is functioning properly.



When this rotating icon appears, SecureWeb is communicating with the Policy Server. SecureWeb is functioning normally and your Internet request will be loaded shortly.

Quick Reference Chart

I'm *not* using a Profile, I want to...

Here's what to do...

Choose a Profile so I can start surfing.

1. Double-click the SecureWeb Icon in the System Tray.
2. Select or enter your Profile name and password.

Go to the Profile Manager.

1. Double-click the SecureWeb Icon in the System Tray.
2. Click the text "Click here to manage Profiles".
3. Enter your Profile manager password and click Continue.

I'm using a Profile, I want to...

Here's what to do...

Surf to a web site.

Use your browser to navigate to a web site as you normally would.

See my Profile Status.

Double-click the SecureWeb Icon in the System Tray.

Change my Profile.

1. Double-click the SecureWeb Icon in the System Tray.
2. Select "Click here to Log Out and Choose a Profile" link.
3. Select or enter your new Profile name (and password).

Leave my Profile and stop surfing

1. Double-click the SecureWeb Icon in the System Tray.
2. Select "Click here to Logout and Choose a Profile" link.
3. Close all browser windows.

About Popup Messages

Popup Messages or Balloon Messages are notes that pop up from the Windows System Tray. They display notices and tips to help you use the Internet. A Protocol Message may tell you what SecureWeb is doing or may tell you how to solve a problem.

For example, if you tried to check your email with an email client (such as Outlook Express or Thunderbird) before you logged in to a Profile, you might see the following message appear at the bottom of your screen



Hide Popup Messages

To stop Popup Messages from appearing on the screen, do the following:

- Double-click on the SecureWeb icon in the Control Panel.
- Enter the Profile Manager password.
- Uncheck "Show Popup Messages" in the Filter Settings screen.

Show Popup Messages

To show Popup Messages after they have been hidden, do the following:

- Double-click on the SecureWeb icon in the Control Panel.
- Key in the Profile Manager password.
- Check "Show Popup Messages" in the Filter Settings screen.

Status Page

The Status Page identifies the name of the Profile you are logged in to as well as the filtering options that are currently enabled for that Profile.

If you are not logged in to a Profile, you must click "Log Out and Choose a Profile", and log into the "Choose a Profile Page".

If you are logged into a Profile, double-click on the SecureWeb icon in the system tray will open the Status Page, as shown below



The Status Page is the default Page that appears often when using SecureWeb and is similar to the Deny Page except the Deny Page contains more information. From this Page you can either "Choose a Profile" or "Manager Profiles".

In the Status Page, you are notified which Profile you are currently logged into and which types of filtering options have been enabled for that Profile. Filters that are currently enabled are marked by the ticks surrounded by green circle and the disabled ones, are the crosses surrounded by red circles. The eight types of filters are...

- Allow All: Temporarily allows unrestricted Internet access.
- Deny All: Temporarily blocks all Internet access.
- Reports: All Internet access is logged and sent to the Web Administrator.
- Web Categories: Certain categories of web sites are blocked.
- Protocols: Certain protocols, such as peer-to-peer networking, Voice-over-IP, or email, are blocked.

- Time Based Controls: Internet access is blocked at certain predefined times during the day.
- Allow List: Specific web pages are marked as allowed or denied.

To log out of your current Profile and choose a new Profile, select "Click here to Log Out and Choose a Profile".

If you are already logged in with a Profile, if you leave the Status Page unattended for 10 Seconds, it will automatically go to www.google.co.uk

Choose a Profile

The *Choose Profile Page* allows you to select the Profile that you will use to access the Internet. After you have logged in using the Choose Profile Page, you can navigate to other web pages in your web browser or use other allowed Internet applications, such as email and instant messaging.

If you are already logged in to a Profile, then you must log out before accessing the *Choose Profile Page*. To log out of your current Profile, double-click on the SecureWeb icon in the system tray and select "Click here to Log Out and Choose a Profile" from the Status Page.

If you are not logged in to a Profile, double-click on the SecureWeb icon in the system tray.

The *Choose Profile Page* should look similar to this:



To log in to your Profile, click on your Profile name and enter your password. If you are inactive at the PC for several minutes, the session may time out. Return to the Choose Profile Page and log in to your Profile to continue.

Deny Page

The Deny Page identifies the name of the Profile you are logged in as, while also giving details of the web page that has been blocked and the Category that SecureWeb has classified it as. For explanations of the list of ticks and crosses see the *Status Page* information.

From the Deny Page you can Click one of the following:-

- **Quick Allow** – To access the blocked website providing you know the password. (see the **Preferences** section of the *Profile Manager*)
- **Request a Review of the Denied URL** - Request that the Page be reviewed to have it's classification amended
- **Request a Review of the Denied Site** - Requests that the Whole Website be reviewed to have it's classification amended
- **Log Out and Choose a Profile** - Select a different profile that will allow you to access the site
- **Manage Profiles** - Change the Settings of the Current Profile to allow access to the web page/site

Alternatively you can press the **Back** button of your browser and return to the last webpage

Managing Profiles

Getting Started

Situations, user needs, and expectations vary widely. SecureWeb uses "Profiles" to control access to the Internet (a profile is a collection of rules defining what can be reached across the internet). You can create a general profile that gives all the users of a computer the same restrictions, which is how SecureWeb is setup initially for you. It has a general profile called "Generous" which restricts the access of all the users to prevent them reaching the negative websites containing Pornography, Gambling, Hate, etc, if you want more sophistication you can create Profiles for each user individually


What you need to decide is are you trying to eliminate certain web sites or applications for all users or is it important to have Profiles tailored to individual users with individual reporting and monitoring? Typically the best strategy is to start with the least filtering (greatest access) appropriate to the users which is what the "Generous Profile" tries to provide.

New Internet applications, technologies, and methods of communicating are being introduced on the Internet daily. When updating an application or adding an application to the computer, SecureWeb may need to be adjusted to work with the application – either allow or deny access to the Internet. In some cases, changes to your local firewall, virus detection, and spyware settings may affect SecureWeb.

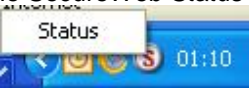
To change or create a new Profile you need to use the "Profile Manager"

Accessing Profile Manager

You access the "Profile Manager" from the SecureWeb "Status Screen". To reach this Status screen you can use one of the following methods:-

1) Double Click with the left mouse button on the SecureWeb Status Bar Icon  in the lower right corner of the screen.

2) Right Mouse click on the SecureWeb Status Bar Icon and then left click on the

Status Item that appears 

3) In the Browser Address bar type <http://filter.secureweb.uk.com>

Any of the above will open the SecureWeb "Status Page" where you just click on the "Click here to manage profile" option and enter your password.

Using the Control Panel

All administrative tools for SecureWeb can also be accessed from the Windows Control Panel. The Control Panel can be found in the Start menu, although its exact location and appearance depend on your version of Windows and your personal settings.

Once you've opened the Control Panel, you are looking for the following icon



Select and Open "Filter Setting" to access the SecureWeb administration. At this point, you need to enter your Profile Manager password and select OK to continue.



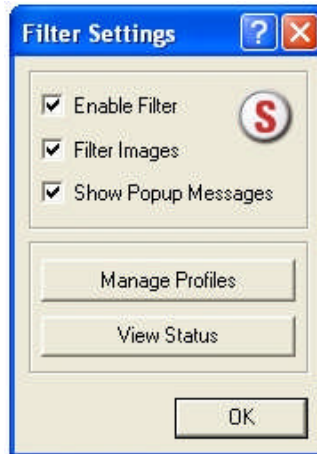
Forgotten Password

If you have forgotten your password and can no longer access the SecureWeb Profile Manager, you can contact ECS-Secure Support, who can either reset your Profile Manager password or if you click on the *Forgot Password* Button, a Security Key number will appear, which if given to the Support Engineer, will enable them to give you a second number to enter into the Override Key box, this will enable you to access the Profile Manager and reconfigure the software.



Control Panel Filter Settings

Once you have logged into the Filter Settings the following screen appears:



From this window, you can choose to Enable/Disable the Client Filter, choose whether images should be scanned as well as text, choose to show/hide Popup Messages, go to the Profile Manager or view the Status Page for the active Profile.



Internet Access Status

You are using the Profile: generous

Allow All	✘
Deny All	✘
Reports	✘
Web Categories	✔
Protocols	✔
Time Based Controls	✘
Allow List	✘
Deny List	✘

Click [here](#) to Log Out and Choose a Profile
Click [here](#) to Manage Profiles



The SecureWeb "Status Page"

Accessing the Profile Manager

All Profile creation and fine tuning can be done using the *Profile Manager*. To access the *Profile Manager* page...

- In the Control Panel , open "Filter Settings":
- Enter your password.
- Select "Manage Profiles".

You can also open the Profile Manager from several of the SecureWeb pages—for example, the Status Page and the Choose Profile Page—by selecting the text "Click here to Manage Profiles" as outlined above.



SecureWeb
Making the Internet a safer place

Profile Manager Login

Profile Manager name: name@email.com

Password:

Continue

Enter Password

Enter a Profile Manager name and password to access Internet-based services.

Click [here](#) to Choose a Profile.



"Profile Manager" Login – just enter the Password that you received.

Modifying Profiles

Profile Manager										
Profiles	Name	Description								
Submit for review	New Profile	Click here to add or copy a profile								
Preferences	generous	This is the	✗	✗	✗	✓	✓	✗	✗	✗
Change Password										
Exit Profile Manager										

- Allow All
- Deny All
- Reports
- Web Categories
- Protocols
- Time Based Controls
- Allow List
- Deny List

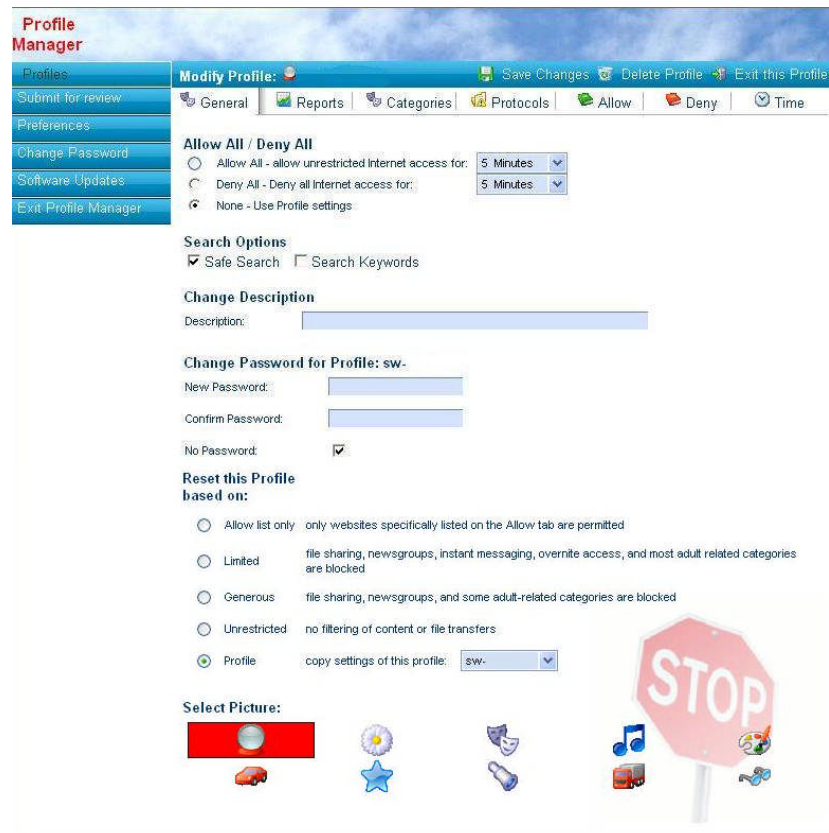
- Enabled
- Disabled

The **"Profile Manager"** Screen

To modify the existing profile "generous" click on the word "generous" and the full "Generous" Profile will appear as shown below.

Once you select a Profile in the Profile Manager, you can...

- ◆ Add profile reporting in the *Reporting* tab.
- ◆ Add filtered categories in the *Categories* tab.
- ◆ Change a Profile's password on the General tab.
- ◆ Add/Remove always-allowed web sites on the Allow tab.
- ◆ Add/Remove always-denied web sites on the Deny tab.
- ◆ Set time restrictions on the Time tab.
- ◆ Try out some of the Advanced Features of the Client Filter.
- ◆ Profile Manager's Quick Reference Chart



The "Generous Profile" settings

Can't wait to get started? Use the following charts to quickly set up your Profiles. Simply log into the Profile Manager account and navigate to the appropriate section.

I want to...	Where to go in the Profile Manager...
Create a new Profile.	Profiles > New Profile
Delete a Profile	Profiles > (select the Trash icon beside the Profile)
Temporarily allow or deny all Internet access for a Profile.	Profiles > (select Profile) > General > Allow All/Deny All
Enable/Disable Safe Search for a Profile or block search engines from searching for certain inappropriate words.	Profiles > (select Profile) > General > Search Options
Change a Profile's password.	Profiles > (select Profile) > General > Change Profile Password
Allow a Profile user to sign in without entering a password.	Profiles > (select Profile) > General > No Password
Change a Profile's picture.	Profiles > (select Profile) > General > Select Picture
View or create Reports.	Profiles > (select Profile) > Reports
Block or unblock a web category for a Profile.	Profiles > (select Profile) > Categories > Web Categories
Block or unblock a file sharing application for a Profile.	Profiles > (select Profile) > Protocols > File Sharing Applications
Block or unblock an Instant Messaging application for a Profile.	Profiles > (select Profile) > Protocols > Instant Messaging (IM)
Block or unblock email protocols.	Profiles > (select Profile) > Protocols > Email
Block or unblock a Voice-over-IP (VOIP) application.	Profiles > (select Profile) > Protocols > Voice Over IP (VOIP)
Block or unblock other Internet protocols (such as FTP, News Groups, or JAP).	Profiles > (select Profile) > Protocols > Misc Protocols
Allow a particular web site (URL) or keyword.	Profiles > (select Profile) > Allow List
Block a particular web site (URL) or keyword.	Profiles > (select Profile) > Deny List
Set time restrictions for a Profile.	Profiles > (select Profile) > Time
Ask SecureWeb to review a web site's category or tell us about an Internet application.	Submit for review
Select when the SecureWeb should automatically select or leave a Profile.	Preferences > Active Profile Settings
Select whether to display Pictures, a drop down menu, or text input on the Choose Profile page.	Preferences > Choose Profile Settings
Choose what information is shown on the Deny Page when users are blocked from a web site.	Preferences > Deny Page Settings
Change my language setting.	Preferences > Language Settings
Change my time zone setting.	Preferences > Timezone Settings
Change my Profile Manager password.	Change Password
Download software updates for the Client Filter.	Software Updates
Leave the Profile Manager and choose a browsing Profile.	Exit Profile Manager

Recommendations

In general, we strongly recommend that you use the default settings unless you have a specific need to change them and you fully understand the consequences of doing so.

Web Categories

In most cases, starting out with too little filtering is a better choice than too much filtering. That is, choose the categories that you are certain you want blocked, test the filtering, and then adjust as necessary. This reduces the likelihood of “over-blocking” (blocking sites that you don’t really want blocked) and preventing users from accessing acceptable content.

Instant Messaging

Instant messaging applications, such as Windows Messenger, allow users to chat between computers. There are many ways to set up messaging between computers and the most popular methods are listed on the *Protocols* tab. This category does not include web based chat sites and forums. If you also want to block these sites, select Web Chat/Forums from the *Web Categories*.

File Sharing Applications

File sharing applications often involve methods to download or access music, video, software, or other files. As with Instant Messaging, there are many methods to share files; the most popular are listed on the *Protocols* tab under *File Sharing Applications*.

Email

Email (or electronic mail) allows users to send messages and files using special mail protocols. Select the email protocols you want to block and all mail of that type is blocked. If you are not sure what these protocols mean, simply select all them if you don’t want to block email access or select none of them if you want to allow email access. If you want to block web-based email, such as Hotmail or G-mail, you must select Web E-mail from the *Web Categories*.

VOIP

Voice Over Internet Protocol (VOIP) allows users to talk to each other over the Internet, much like a telephone. If you have a VOIP application that you want certain users blocked from using, select it and all messages under that protocol are blocked. Select the VOIP application from the applications listed on the *Protocols* tab under **VOIP**.

Misc Protocols

This section contains miscellaneous protocols that do not fit under any of the other category groups. For example if File Transfer is selected then all FTP protocols (used for the transfer of files over the Internet) are blocked.

Streaming Media

This section contains media applications that are used to play live audio and video like Real Player and Winamp.

Advanced Features

After your SecureWeb is up and running, the features described in this section are used to tune SecureWeb to your needs.

Accessing the Profile Manager Remotely

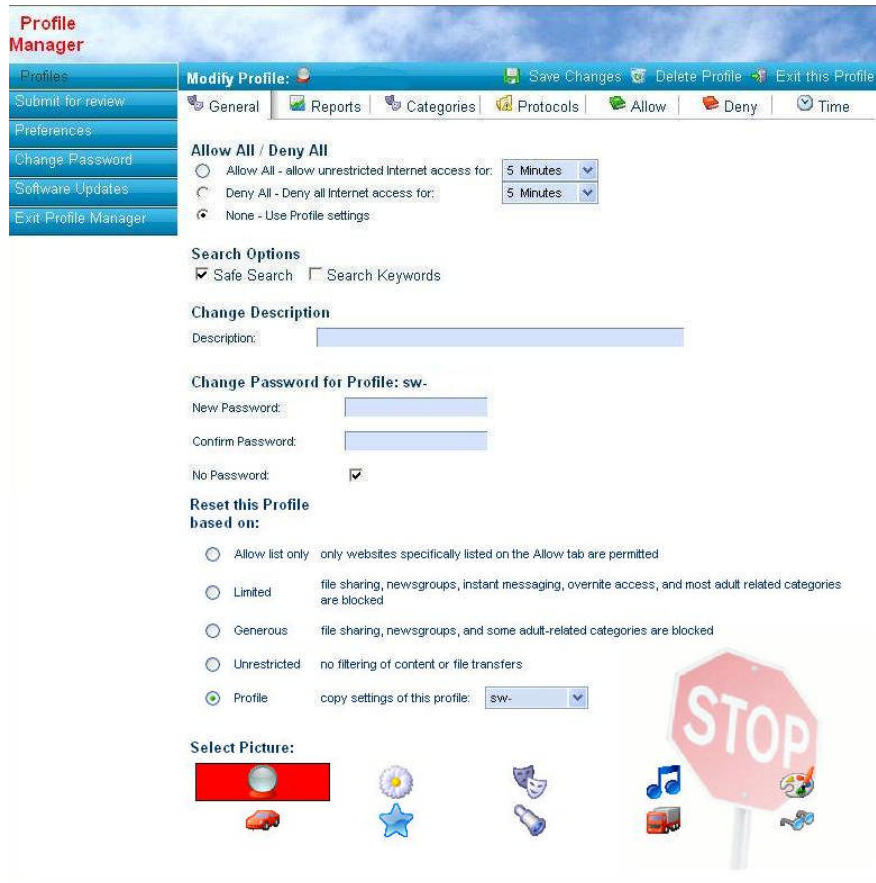
There may be times when you need to use the Profile Manager, but do not have physical access to your computer. SecureWeb allows you to access your Profiles using remote web-based login. Using a computer with Internet access, but without SecureWeb installed, enter your Remote Login URL into your web browser to access the Profile Manager. Your Remote Login URL is:
<http://filter.secureweb.uk.com>

The URL string for the Choose Profile Page, the Status Page and the Deny Page also begin with the same information. If you can not access a computer with the client installed, contact your ISP or have one of your users check this for you.

About Mouse-Over Help

Most items in the Profile Manager interface have helpful "mouse-over" tips and descriptions associated with them. To view a mouse-over tip, place your mouse cursor over the item. For example, you can view a description of each of the Categories by pointing your mouse cursor over the category. The description appears in the text box at the bottom left of your screen.

General Settings Tab of a Profile



About Filter Priorities

As the filter operates, there is a certain sequence that is followed to determine whether to allow or deny. The filtering process can be divided in to four stages:

Allow All or Deny All setting

Time restriction setting

Allow List and Deny List settings

Category, Protocol, and Safe Search settings

When the user tries to go to a web site, the filter first determines if either the Allow all or Deny all override is set. If not, the time restrictions are checked. If the time restrictions do not apply, the Allow and Deny lists are checked for the requested site. If there is no match there, the filter looks at the category and protocol settings.

Allowing or Denying All Access

To temporarily allow unfiltered access to the Internet (Allow All) or to block all access (Deny All), do the following:

Open the Profile Manager.

Select the Profile you want to modify.

Go to the General tab.

Select either "Allow All" or "Deny All" and choose a time period

Click Save Changes.

These settings override all other filter settings. However, activity is logged and reports can still be generated during this time.

Enabling Safe Search

The Safe Search option can be accessed by clicking on the General tab after selecting a Profile. Enabling Safe Search effectively blocks most sexual content from appearing in search results when using certain search engines. The currently supported search engines are:

Google

Yahoo

MetaCrawler

Excite

Lycos

If the Search Engine category is blocked, no search engines are allowed, regardless of whether this category is selected or not. Search engines must be allowed for Safe Search to work.

Note

Turning on Allow All overrides the Safe Search function.

Blocking Search Keywords

On the Policy Server, administrators have the ability to define a list of words or phrases as keywords that may be considered objectionable. If you select Search Keywords in the General tab, sites detected as Search Engines are checked for a match with the keywords. If there is a match, the URL is denied.

For example, if "dirty word" is in the Search Keyword list and a Profile user searches for the phrase "This is a dirty word" in a search engine, such as Google or Yahoo, the search results are blocked

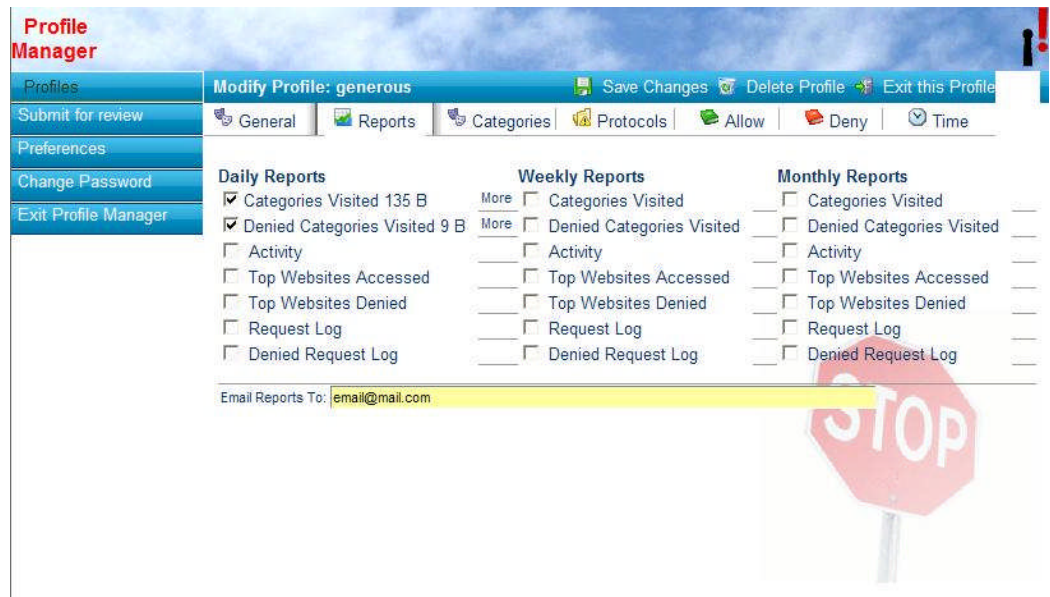
Setting Profile Passwords

Each profile has the option of a Password, if there are multiple profiles specific to individuals, it is best to create a password for each user to ensure that only that user can access the Internet with that Profile. In the Preferences (*see Preferences below*) section it is possible to select which Profile is chosen when the computer is restarted. If there is just one profile for the computer it may be best to tick the No Password Box so that everyone can use the internet on the computer without having to constantly re-enter a password.

Resetting Profiles

At the bottom of the General Page is the option of Resetting a Profile to a predefined security profile, which is useful when creating a new Profile.

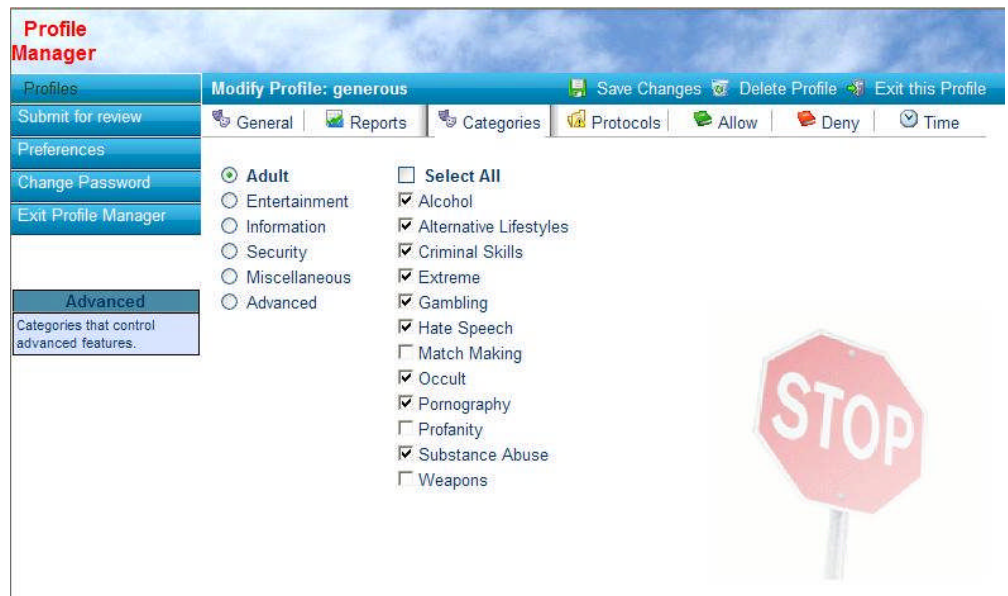
Reporting Tab of a Profile



Within the Reporting Tab you can select Daily, Weekly and Monthly Reports, to see examples of these, visit:-

<http://www.cleaned-internet.com/reporting.htm>

Selecting Categories Tab to Block and Unblock

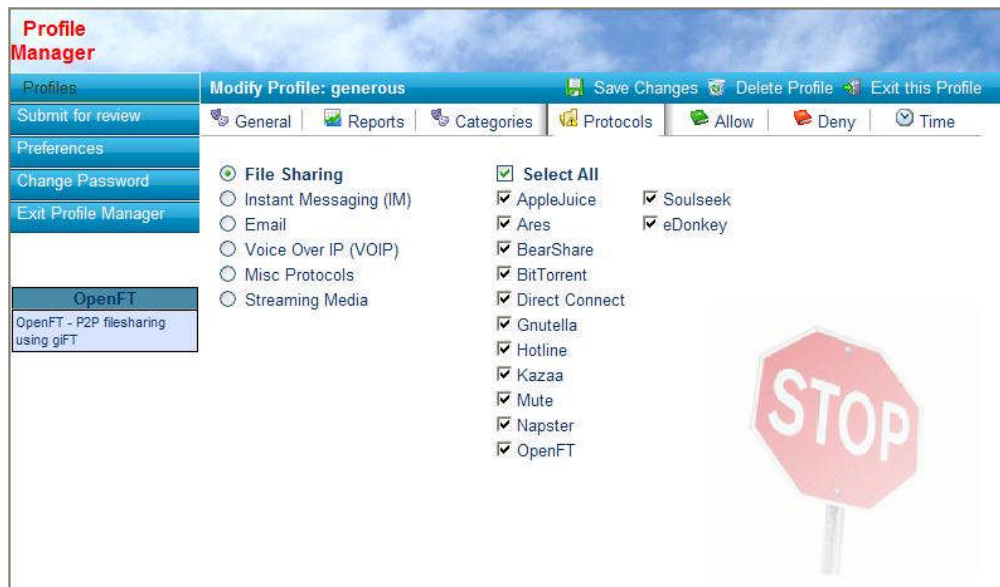


To block certain categories of web content, do the following:

In the Profiles menu tab, select the Profile you wish to modify.

- Go to the Categories tab.
- Click a radio button on the left to select which type of web categories to modify e.g. Adult, Entertainment, Information etc.
- Click on a check box to block that category. Boxes that already have a check mark are currently blocked. To unblock a category, click on the box to remove the check mark.

Blocking or Unblocking Protocols Tab



In general, we recommend that you accept the default settings for these protocols. However, you may want to change the Instant Messaging (Windows Messenger) and Email selections, depending on your preferences.

Instant messaging applications, such as Windows Messenger, allow users to chat between computers. This category does not include web based chat sites and forums. If you also want to block web based chat, select Web Chat/Forums from the Categories tab. Email (or electronic mail) allows users to send messages and files. If you want to block web-based email, such as Hotmail or G-mail, you must select Web E-mail from the Web Categories.

To block or unblock a protocol, do the following:

In the Profiles menu tab, select the Profile you wish to modify.

- Go to the Protocols tab.
- Click a radio button on the left to select which group of protocols to modify.
- Click on a check box to block that protocol. Boxes that already have a check mark are currently blocked. To unblock a protocol, click on the box to remove the check mark.

About the Allow List Tab

The screenshot shows the 'Profile Manager' interface. On the left is a navigation menu with options: Profiles, Submit for review, Preferences, Change Password, and Exit Profile Manager. The top bar shows 'Modify Profile: generous' and buttons for 'Save Changes', 'Delete Profile', and 'Exit this Profile'. Below the top bar are tabs for 'General', 'Reports', 'Categories', 'Protocols', 'Allow', 'Deny', and 'Time'. The 'Allow' tab is active, showing an 'Allow:' input field with 'http://', a 'Comment:' input field, and an 'Add' button. Below this is a table with columns 'URL/Keyword' and 'Comment'. The table contains three entries: 'http://myspace.com', 'http://bebo.com', and 'http://cleaned-internet.com', each with a 'Delete' link to its right. A large red octagonal 'STOP' sign is overlaid on the bottom right of the screenshot.

Each Profile has an Allow List in the Profile Manager. The Allow tab allows you to enter the URL of a web site that you want to be allowed for a Profile—even if it's in a blocked category. You can allow one particular page, an entire domain, or any page with a certain keyword present in the URL string.

If you want to allow one particular page of a web site, copy the URL string of the page into the Allow List along with a description of why you want to allow it.

Example: <http://www.example.com/path/example.html>

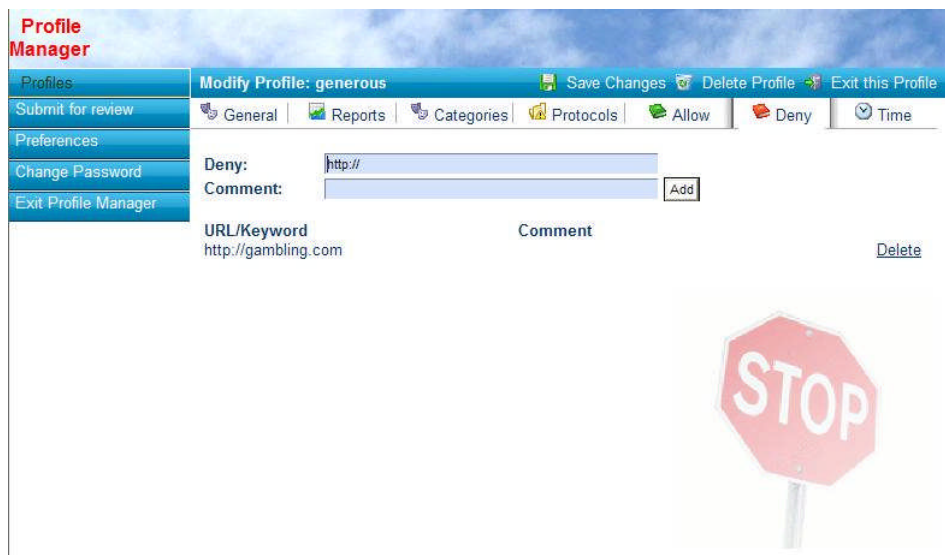
However, this can be tedious if you want to block all the pages at a particular web site. If you want to allow every page at the example.com web site, remove the "www" to allow the entire domain.

Example: <http://example.com>

If you want to allow a keyword, simply enter any word without http:// at the beginning. Be careful when choosing keywords. Allowing the word "ex" also allows any site with the word "sex" in the URL.

Once you click Save Changes, the allowed site's name and your reason for allowing are displayed.

About the Deny List Tab



Each Profile has a Deny List in the Profile Manager. The Deny tab enables you to enter the URL of a web site that you want to be denied (or blocked) for a Profile – even if it’s in an allowed category. You can deny one particular page, an entire domain, or any page with a certain keyword present in the URL string.

If you want to block one particular page of a web site, copy the URL string of the page into the Deny List along with a description of why you want to deny it.

Example: <http://www.example.com/path/example.html>

If you want to deny every page at the example.com web site, remove the “www” and the path to deny the entire domain.

Example: <http://example.com>

If you want to block a keyword, simply enter any word without http:// at the beginning. As with the Allow List, use caution when choosing keywords. For example, blocking the word “sex” also blocks the word “Sussex”.

Once you click Save Changes, the denied site's name and your reason for denying it will be displayed.

Setting Time Restrictions Tab

The screenshot shows the Profile Manager interface. The 'Time' tab is selected, displaying a grid for setting time restrictions. The grid has columns for hours (12 AM to 11 PM) and rows for days of the week (Sunday to Saturday). A legend indicates that red squares represent 'Block All Access' and blue squares represent 'Filtering Active'. A red stop sign graphic is overlaid on the bottom right of the grid.

SecureWeb also allows you to block a Profile user's Internet access at certain times of the day. To do so, select the Time tab after selecting a Profile. Clicking on a grid for a particular day and time, turns the square **red** and blocks all access to the Internet during that period.

Disabling the Filter

If you need to temporarily disable the Client Filter, you can do so through the Control Panel. You must have the Profile Manager password to disable the Client Filter. Password protection ensures that unauthorized users cannot bypass the SecureWeb monitoring and filtering service. To disable the Client Filter...

- Open the Windows Control Panel. (Start > Settings > Control Panel)
- Select Filter Settings.
- Enter your Profile Manager password and select OK.
- Click to remove the check mark in the Enable Filter checkbox.
- Select OK.

Your SecureWeb is will remain disabled until you re-check this box to.

Once you are ready to turn the SecureWeb back on, repeat these steps and replace the check mark in the Enable Filter checkbox.

Preferences Settings

The screenshot shows the 'Account Preferences' page in SecureWeb. On the left is a navigation menu with options like 'Profiles', 'Submit for review', 'Preferences', 'Change Password', 'Software Updates', and 'Exit Profile Manager'. The main content area is titled 'Account Preferences' and includes several sections: 'Active Profile Settings' (with 'Use this Profile on restart' selected and circled in red), 'Choose Profile Settings' (with 'Picture' selected), 'Deny Page Settings' (with 'Show detailed deny page' selected), 'Profile Logout Settings' (with 'No password required' selected), 'Language Settings (all Profiles)' (with 'English' selected), and 'Timezone Settings (all Profiles)' (with 'Europe/London' selected). There are also fields for 'Password' and 'Email' (phill@philtratton.com). A red arrow points to the selected option with the text 'a. Select This option'. A 'STOP' sign graphic is visible in the bottom right corner of the form area.

In the Preferences menu tab, you can select whether SecureWeb will automatically choose a Profile when you turn on your computer. When choosing your settings, keep in mind that users should not have access to any Profile but their own. Otherwise, their activity cannot be logged correctly for reports and they may be able to access objectionable content by using a Profile with fewer restrictions.

You can choose one of the following four options: Retain Profile on restart, Exit Profile on restart, Use this Profile on restart, or Allow "Remember my Profile".

You can also choose to have SecureWeb log out when the computer has been idle long enough to activate the screensaver by selecting "Exit Profile on screensaver activation".

Active Profile Settings

Retain Profile on restart

When this option is selected, the computer keeps the Profile settings that were in use during shutdown. That is, if a Profile was in use, the computer automatically logs into that Profile again. If no Profile was in use, users must choose a Profile to access the Internet.

Exit Profile on restart

After starting the computer, each user must choose a Profile before accessing the Internet. This is the recommended option for systems with multiple users.

Use this Profile on restart

The selected Profile in the dropdown menu is used when the computer is started. Use the menu to change the selected Profile. For example, you may want to create a safe Profile for anyone to use on startup.

Allow “Remember my Profile”

When this option is enabled, users have the option to select “Remember my Profile” when choosing a Profile. The computer then associates that Profile with the current Windows user name. The next time that user logs in to their Windows account, the computer automatically chooses the same Profile.

Exit Profile on screensaver

If your computer sits idle for several minutes, it may enter “Suspend” mode, depending on your Control Panel settings. If this option is enabled, users are logged out of their Profile when the computer enters the suspend mode. Users must choose their Profile again if this occurs.

Choosing Profile Settings

This option enables the selection of the way that a Profile list is displayed when choosing a profile from SecureWeb’s Status Page where it says “Click here to choose a profile”

The Choose Profile options can appear in three ways:-

- **A Picture** – A list of icons appear representing each Profile
- **Dropdown** – A dropdown list appears to choose the profile from
- **Input** – No list appears this option requires the entry of a valid Profile

Deny Page Settings

In the Preferences menu tab, you can choose how much information should be displayed to users when they are denied access to a web site. The deny page is used to notify the user that they have tried to access content that is not allowed by their Profile. You can choose to show a detailed deny page, a minimal deny page, or no deny page at all. There are also two additional links that can be shown on either the minimal or detailed pages called “*Include Quick Allow Access link*” and “*Include admin email link*”.

Detailed deny page

If you select “Detailed deny page”, the user is shown all relevant information, including the Profile name, the URL address of the web site, the web site’s category, and the Status screen information.

Minimal deny page

If you select “Minimal deny page”, only the Profile name, and the web site category are displayed to the user.

No deny page

If you select “No deny page”, the user will be shown an unauthorized access error by the browser. The user does not see any SecureWeb logo or information about why they were blocked.

Include Quick Allow Access link

If you select this option and enter a password, users are shown a "Click here to Quick Allow this URL" link after being denied access to a page. Users can then select this link, enter the Quick Allow Access password that you chose, and view the content on the page. If you view the page and decide that users should always have access to it, you should enter it into the Allow List.

Note that any page that loads other files or sites or may not be fully displayed or may appear "broken". Sites that redirect you to another web site may be denied again.

Include admin email link

If you select this option and enter your email, users are shown a "Click here to Request a Review of the Denied Url" link. If the user selects this link, an email will be sent to you requesting a review of the web site. This allows you to review the web site and if necessary, adjust the Profile settings to allow future access to this web site

Profile Logout Settings

In the Preferences menu tab, you can choose to restrict users from logging out of their Profile. In most cases, requiring a password to log into a Profile provides strong enough security. However, these options can increase or decrease security, should you require it. There are four options available:

No password required

Users do not need to enter a password to log out of their current Profile.

Require Profile password

To log out of a Profile, users or their administrators must enter the same password that was used to log in. Note that if a Profile has the "No password" option enabled in the General tab, they do not need a password to log out even if "Require Profile Password" is selected.

Require Profile Manager Password

With this option enabled, users must have their administrator enter the Profile Manager password each time they logout.

Require this password:

To choose a custom logout password that is different from both the Profile password and the Profile Manager password, select this option and enter the custom password. Users must enter this password before they can log out of a Profile.

Submitting Sites for Review

Profile Manager

Profiles | Submit the following information for review. | Send | Clear Changes


Submit for review | Preferences | Change Password | Exit Profile Manager

Website

Messenger Application

File Sharing Application

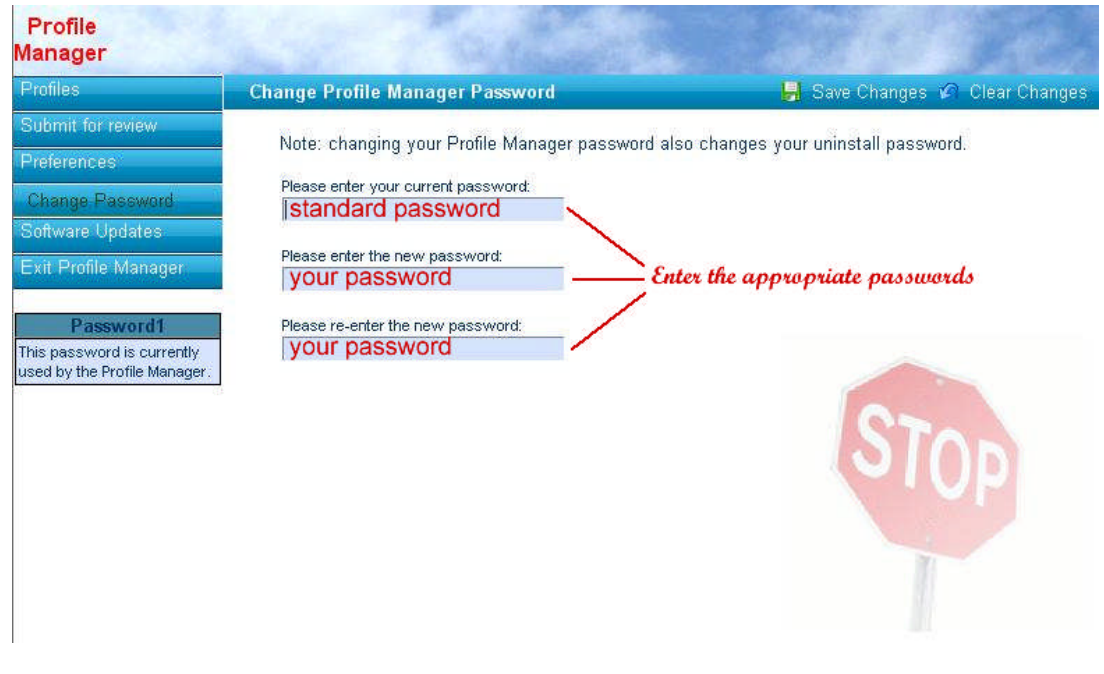
Comment (optional)



If you believe a web site has been categorized incorrectly, you can submit it to the SecureWeb Central Server to have it reviewed by our Content Review team. Web sites that require a category change are uploaded to the Central Server within 24 hours of being reviewed.

If you have a web application or protocol that SecureWeb does not provide management for and is not listed in the Protocols tab, you can submit the name of the new Application like a Messenger Application or File Sharing Application with a quick description, the new program will then be reviewed with the potential of it being included in the next release of the software.

Password Changing



The Change Password option allows the main Profile Manager Password to be changed from the standard one that you receive at registration and choose a password which is more appropriate for you to remember.

Appendix: Category Descriptions

Categories Titled in **Red** are those which are set by the initial "Generous Profile"

Adult

Alternative Lifestyles

Alternative Lifestyles are habits or behaviours related to social relations, dress, or recreation. These behaviours are typically important enough to significantly influence the lives of a sector of the population and hence can be used as a basis of social classification.

Sites assigned to this category are not pornographic but may deal with lifestyle choices that are sexual in nature.

Criminal Skills

Criminal Skills includes instructions or methods that promote, encourage, or provide the skills to do anything that is generally considered to be illegal, criminal, harmful to the general public, and/or that are forbidden by laws. This category does not necessarily reflect the laws of any particular region or country.

This category includes sites that promote academic cheating or software hacking/key breaking. It typically excludes any site that deals with the prevention of criminal activity.

Gambling

Gambling (or betting) includes any URLs that involve the wagering or risk of money or valuables on the outcome of a game, contest, or other event in which the outcome is partially or completely dependent upon chance or on one's abilities.

This category includes sites that directly provide that ability to place a bet or to determine the outcome of a bet as well as sites that promote or facilitate gambling. Also includes sites that range from purely factual to strategic to cheating. Includes sites related to lotteries or looking up winning numbers.

Excludes sites that are clearly support sites for gambling addiction.

Extreme

Extreme web sites contain things that are far from the norm. These URLs are categorized as such for their degree of intensity. The pages are usually violent or disturbing and are often related to pornography, bodily functions, obscenity, or perverse activities.

This category does not include widely accepted "extreme" activities, such as extreme rock climbing, skiing, or other achievements.

Hate Speech

Hate Speech is the portrayal (written, verbal, illustrated) of views that are intentionally overwhelmingly critical or offensive to a person. It is intended to degrade, intimidate, or incite violent or prejudicial actions against someone based on race, ethnic affiliation, nationality, gender, sexual orientation, religion, disability, or profession. Any description of one of these groups or group members that uses strong or crude language, explicit sexual references, or obscene gestures is considered Hate Speech.

Substance Abuse

Substance Abuse contains URLs that provide information on illegal drugs used for recreational rather than medical purposes.

This category includes sites that promote the use of any substance that produces a hallucinated effect on self or others. It excludes informational sites that are clearly intended to provide description of drugs and substances, their negative effects, and addiction potential.

Match Making

Match Making is the process of introducing people for the purpose of dating, mating, and friendship. It includes topics related to dating services, dating advice and tips, relationships, listings or personal advertisements, and on-line dating services.

Occult

Occult contain sites involving the study of secret or hidden knowledge and includes any URLs about cults, supernatural forces and events, occult lore, vampires, astrology, witchcraft, mysterious symbols, and other phenomena beyond ordinary understanding. It includes sites about these topics that are historical or factual in nature and/or promote such practices.

Pornography

This category contains URLs that reference, discuss, or show pornography, pictures, videos, or sexually oriented material. This category includes nudity, soft and hard-core pornography, sadomasochism, bestiality, child porn, fetishes, stories, adult magazines, toys, or any sexual related purchase. This category excludes sex education sites.

Entertainment

Arts & Culture

Art is a product of human creativity. It is the creation of meaningful things; yet it does not need to be innovative to be good. Culture refers to human activity. Varying definitions of culture reflects the different theories for understanding and valuing human activity.

Art that includes the human body with an erotic intent is typically included in this category and the pornography category.

Entertainment

Entertainment contains all things pertaining to music, recreation, amusements, fan clubs, gossip, celebrities, movies, or any other form of casual diversion. This category also includes personal sites devoted to movies and television shows.

Sites overwhelmingly critical of an entertainer or group are categorized as Hate Speech.

Games

Gaming contains games or information about games—electronic games, computer games, card games, board games, Internet games, and so on. This category also includes strategies, cheats, and any sites that promote game makers, sites, or sellers.

Humor

Humour contains URLs that are intended to entertain or make people laugh and feel happy. It includes jokes, funny pictures, comic pages, and comedy clubs.

Sports

This category includes any physical activity for the recreational purpose of competition or self enjoyment. Sports typically involve side by side competition and a scoring system. This category includes athletics, racing, hunting, baseball, football, basketball, soccer, hockey, and so on.

Information

General News

General News contains various forms of journalism. It involves the reporting of current events by local, regional or mass media in the form of newspapers, television, radio programs, and sites on the World Wide Web. Most news is investigated and written or broadcast by journalists (or reporters) and often distributed via news agencies.

This category includes any mainstream newspaper, television stations, and radio station site.

Journals and Blogs

Journal and Blogs (or web logs) are electronic diaries or personal chronicles, intended for open communication and sharing of thoughts, knowledge, and opinion. This category ranges from personal and medical to literary and culturally oriented publications.

This category typically does not include electronic forms of mainstream magazines and newspapers. Also does not include personal/family web pages unless there is a diary or blog component.

Politics

Politics is the process and method of decision making for groups of human beings. Although it is generally applied to governments and politics, is also observed in all human group interactions including corporate, academic, and religious. This category contains sites related to the structure or affairs of government, politics, or the state.

Portals

Portals are web-based applications that provide a single starting point to retrieve information from multiple sources. For example, the content of a portal could include web searching, news, free-email, discussion groups, online shopping, references, and other services.

Religion

Religion is any specific system of belief, worship, or conduct that prescribes certain responses to the existence of a God or Gods. This category contains URLs related to or dealing with religious beliefs, practices, faith, churches, worship, and so on.

Self Help

Self Help pages provide the information or support for an individual or a group to better themselves economically, intellectually, physically, or emotionally. This category ranges from therapy methods to support groups.

Sex Education

Sex Education is the study of human reproduction, sexual intercourse, and other aspects of human sexual behaviour. Sites in this category usually describe the various stages of reproduction including the conception, the embryo, the foetus, and the birth of the baby. It also includes topics such as sexually transmitted diseases, abortions, contraception, abstinence and sex advice.

Technology

Technology is the development and application of tools, machines, materials, and processes that help to solve human problems. This category includes sites that pertain to technology related content. It also includes sites that offer a software download, either for free as a trial or for purchase.

Travel

Travel is the transport of people on a trip or journey, primarily for vacation, tourism, or family outings. This category includes discussions of favourite travel destinations, discounts for travellers, special events in different cities, travel guides, vacations, accommodation, transportation, regulations, and bookings. It also includes sites directed towards business travel.

Security

Adware

This category contains URLs that are advertisements or contain Malware/Spyware. Blocking this will improve your computers security, many portal pages may however appear broken with “Stop Signs” appearing in the place of Adverts– what is actually happening is that the advertisements are being blocked because the site has Adware, while the main content is still displayed.

Most frequently visited web pages are actually composed dynamically, drawing on data from several sources at once. Each portion of a page that is drawn in from a unique location is categorized and filtered separately. This may result in a page that appears “broken”, with some portions appearing correctly and some blocked.

Directory

The Directory category contains URLs that produce a directory listing instead of a default html page. This page is generated by the remote web server if no default html page is available and directory browsing is enabled. These directory files can be images, movies, applications, or any other type of file. Each individual file within the listing will be assigned a category once requested. Generally, Directory site pages should not be blocked.

Host Is An IP

Host Is An IP identifies a request that is the form of an IP address. This means the DNS or host name was not used. It is possible that allowing this type of request could in some circumstances override normal content filtering settings. Generally, pages accessed by IP should be blocked.

Malformed URL

Malformed URL is used when a URL is not valid (for example the following URL with a semicolon instead of a colon: `http;\\www.google.ca`). Generally, malformed URL pages should be blocked.

Phishing

This category contains URLs that are known or suspected Phishing sites – typically financial fraud or identity theft. Blocking this category does not guarantee that ALL fraud or Phishing sites will be blocked. Generally, Phishing pages should be blocked.

Proxy Anonymizer

This category contains URLs that allow a user to mask their identity online. Generally, anonymizer pages should be blocked.

Under Construction

This category indicates a site that has been identified by the owner as being incomplete – under construction. Generally, Under Construction pages pose little threat and need not be blocked.

Miscellaneous

Investing

Investing includes Internet banking systems that allow users to invest online, view their equity portfolio, and ask the bank to buy shares or bonds on their behalf. This includes URLs about stocks and quotes, money management, online publications, banks, discount brokerage services, mutual funds, and portfolio management.

Job Search

Job Search sites allow people to search and apply for employment positions. This category includes resume writing and interviewing skills, career information, classified advertising, job databases, and job application pages.

Sales

The Sales category includes any site or page offering consumers the ability to purchase products or services online. In some cases, it may include sites that provide a catalogue of products that are offered for sale off-line.

Search Engine

A Search Engine is a tool that helps web users to search the Internet using keywords. Some Search Engines work by automatically searching the contents of other systems and creating a database of the results, and other Search Engines contain only material manually approved for inclusion in a database. Some combine the two approaches.

Many Internet pages offer some form of search function. Blocking Search Engines blocks only sites or pages whose sole purpose is Internet search.

Web Chat

Web Chat sites contain computer programs that enable two-way communication between users within an active browser window. This category includes any type of instant messaging and forums that talk about current events, debate, and share common interests and My Space. We suggest that you allow specific sites for your family to use rather than removing this category from the blocking list.

This category does not block instant messaging applications that are run outside a browser, such as MSN, AIM, or Yahoo Messenger.

Web Email

The Web Email category includes web pages that permit users to send and receive text, HTML, images, and other data files to each other.

This category does not block email client applications that run outside a browser, such as Outlook, Thunderbird, or Eudora.

Advanced Categories

The advanced categories are ones that generally should not be changed from the default setting without fully understanding the overall impact and a period of testing. Advanced categories are intended to be changed by an experienced administrator only. Some of these categories are not made available to the Profile Manager administrator for the Client Filter.

We strongly recommend that you use the default settings for the Security and Advanced categories unless you have a specific need to change them and you fully understand the consequences of doing so.

General

This category contains URLs that do not belong to any other category. The majority of the Internet is assigned to this category. Do not block this category unless you are filtering in an “allow list only” mode.

Images

The Images category contains URLs for an image file, determined by file name extension (example: www.netsweeper.com/images/logo.jpg). Generally, Images should not be blocked.

Network Unavailable

Network Unavailable is a system category indicating there is no connection to the Distribution Servers. This means that there is a networking problem between the Policy Server and the Distribution Server.

Network Timeout

Network Timeout is a system category that identifies a connection delay to the Distribution Server—it can not respond fast enough to the Policy Server’s requests so the Policy Server times out and returns this category.

Intranet Servers

Intranet Server is a system category used to identify servers that are not publicly accessible from outside your local area network.

New URL

New URL is a temporary category assigned to a URL that has not been categorized before or whose categorization has expired.

Blocking the New URL blocks any URL that has not already been categorized or whose categorization has timed out. Normally, revisiting a URL immediately after being denied as New URL will return the appropriate category for the URL (it takes about one second to categorize a URL).

No Text

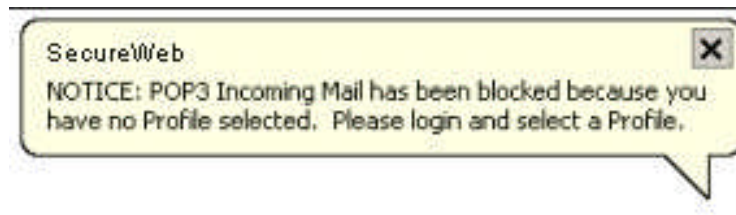
No Text is used when the file extension of this page is not recognizable by the Categorization Engine. Blocking is entirely based on the file extension. Generally this option, “No Text” pages should not be blocked.

Redirector Page

This category indicates a URL that redirects the user to another page. Do not block this category unless you are filtering in an “allow list only” mode.


Troubleshooting

1) No Profile Selected - Can't access the Internet

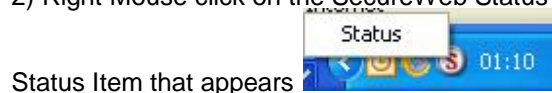


Before SecureWeb can allow any access to the Internet, a Profile must first be selected (a Profile is a list of rules defining what can and cannot be reached on the Internet). On the initial installation, a standard profile called "**Generous**" is installed which **does not** have a Password.

To select a Profile you need to open the Profile Selection Screen shown below, to reach this you use one of the following methods:-

1) Double Click with the left mouse button on the SecureWeb Status Bar Icon  in the lower right corner of the screen.

2) Right Mouse click on the SecureWeb Status Bar Icon and then left click on the



Status Item that appears

3) In the Browser Address bar type <http://filter.secureweb.uk.com>



SecureWeb
Making the Internet a safer place

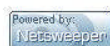
Choose Profile

Name:

Password:

Enter a Profile name and password to access Internet-based services.

Click [here](#) to Manage Profiles



SecureWeb Profile Selection Screen

2) Can't Access the Internet – Anti-Virus blocking it

Norton Security Suite 2006

In some cases, Norton Internet Security Suite 2006 may block Internet traffic going through SecureWeb and other legitimate programs.

If you are running Norton Internet Security and try to install secureweb, a Norton Internet Security Message will pop-up telling you that secureweb is trying to access the internet, do you wish to allow it?

DO NOT ACCEPT THE NORTON DEFAULT POPUP OPTION

If you just accept the Norton recommended default option, secureweb will not complete the installation and will get no further than trying to validate the User Name and Password that you have entered. This problem arises because the default that Norton recommends is **"Always Block connections from this Program"** and as you might appreciate, if you accept the default which in most situations you would do, secureweb will be prevented from accessing the internet by Norton and secureweb will become completely non-functional, since it must be able to access the internet to do what it is designed for.

To prevent this problem occurring, during the installation process, when the Norton pop-up security message arises DO NOT accept the default option, but instead click the right-hand drop down option and change it to **"Always Allow connections from this program"**.

SecureWeb uses certain ports to monitor the Internet traffic to your system. The Internet cannot be accessed if these ports are blocked by a firewall application.

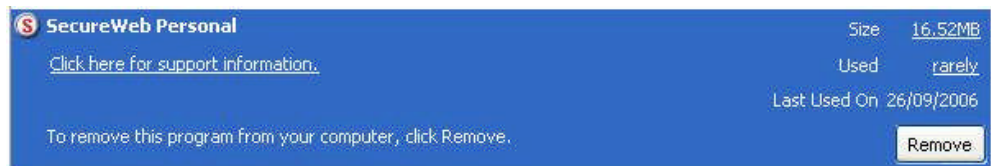
To unblock these ports that have been blocked by these firewall applications do the following:

- Right click on the Norton globe icon in the system tray.
- Select *Options > Internet Security*.
- In the Norton Internet Security options dialog, select the *Firewall* tab.
- In the HTTP port list, select 80 and click *Remove*.
- Select 8080 and click *Remove*.
- Select *Ok*.

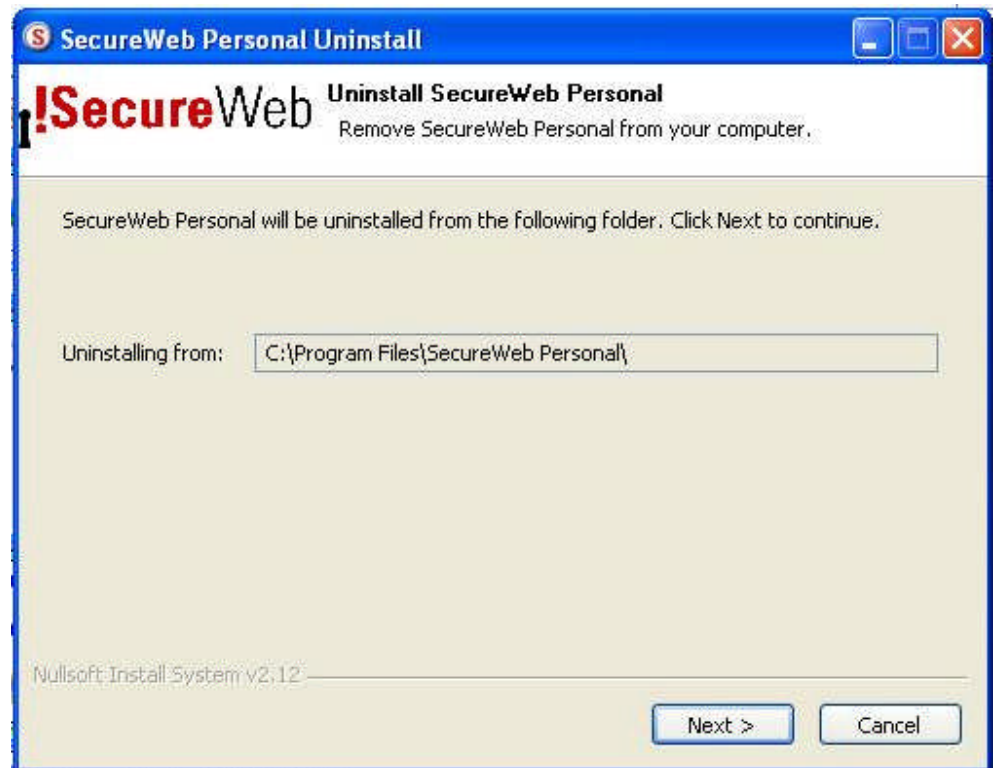
Now you should be able to browse the Internet once again.

3) Un-installing SecureWeb

To un-install SecureWeb you open the Control Panel of your computer and find the "Add/Remove Programs" Icon. Double Click the "Add/Remove Programs" icon with your left mouse button, to open the installed programs list. From the list of installed programs find SecureWeb Personal program and click on it with you left mouse button once to expand the item, then click on the "Remove" Button to the right of the screen, as shown below.



When you have pressed the "Remove" button the Un-Install Process (shown below) will start, continue by pressing the "Next" button as each option appears.



To complete the un-install process, you will need the Profile Manager Password, which if you have not changed it, is the one which you received by email when you first installed the software. On completion of the un-install process the computer must be allowed to restart to ensure that all the SecureWeb functions are deactivated.