Click Bookmarks for table of contents

AgapeSafeGuard

Desktop Filter: User's Guide

Agape Internet LLC.

16828 Notestine Rd,
New Haven, IN 46774
Phone: (800) 498-1788
Fax: (866) 633-7150

Every effort has been made to ensure the accuracy of this manual. However, Agape SafeGuard Inc. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Agape SafeGuard Inc. 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.

Preface

The Agape SafeGuard Desktop Filter 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 the Agape SafeGuard Desktop Filter available. The Personal Edition is intended for residential use as well as for small businesses not using a domain server. The Professional Edition is intended for larger businesses using a domain server.

This document describes the installation and initial configuration of the Agape SafeGuard Desktop Filter Personal Edition on your computer. It also provides some tips on managing Internet access as well as an introductory guide to using Agape SafeGuard for your computer users.

About Profiles

With the Agape SafeGuard Desktop Filter installed and set up, before anyone using this computer accesses the Internet, they must have a filtering profile selected. The Profile that they choose will determine what restrictions Agape SafeGuard applies and the level of monitoring and reporting.

The Agape SafeGuard Desktop Filter allows the Profile Manager – the administrator – to create one or more Profiles. Several people could use the same Profile or each person could have their own Profile.

The Profile Manager also has several choices with respect to how users select a Profile to use, when (and if) Profiles are automatically disabled, what Profile to use as a default for the computer (if any), and whether a user can choose to have their Profile “remembered” by Windows when they log in.

With this in mind, you may want to decide on what Profiles you want to create before you start the installation. You can get up and running by using the default Profiles that are created during installation. You can add, change, or delete Profiles later.

Table of Contents

1.

1. Installing the Desktop Filter

This chapter describes how to install the Desktop Filter Standard Edition onto your computer. The installation takes about a minute. You will need to restart the computer once installation is complete. After that, you should spend a few minutes creating one or more filtering profiles. It takes about one minute to create a Profile.

Before You Install

Please ensure that your computer meets the following requirements:

- Your computer needs to be running Windows XP (recommended) Home or Professional, Windows Vista, or Windows 2000. The Agape SafeGuard Desktop Filter does not operate on Apple Computers.
- You need about 600 kb 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
- You need a Profile Manager account name and password for the Agape SafeGuard Desktop Filter. This should have been provided by your administrator or Internet provider.

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.
- Clear your Internet browser's cache or delete all temporary Internet files. See *Clearing Your Browser Cache* on page 8.
- 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 Agape SafeGuard.
- 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.

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

1. Using Firewalls

Agape SafeGuard 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.

If you have a firewall installed, disable it before installing the Agape SafeGuard Desktop Filter. After installing, you can enable the firewall again but you need to adjust your firewall settings to always allow the Agape SafeGuard Desktop Filter program "nsfx.exe" to access to the Internet.

1. Norton Security Suite 2006 Users

In some cases, Norton Internet Security Suite 2006 may block Internet traffic going through Agape SafeGuard. To open the ports required for Agape SafeGuard to function and to restore your connection, do the following:

1. Right click on the Norton globe icon in the Windows Notification Area.
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**.

2. Using Internet Accelerators

If you use an Internet connection accelerator, such as SlipStream or Propel, it may be important that the Agape SafeGuard Desktop Filter is installed after the accelerator to ensure the best possible performance of the accelerator.

If you already have an accelerator installed, go ahead and install the Desktop Filter.

If you are adding an accelerator to your connection with the Desktop Filter already installed, we recommend you do the following:

1. Uninstall the Desktop Filter.
2. Install the accelerator.
3. Install the Desktop Filter again.

2. Installation and Initial Configuration

Please note that you need a Profile Manager name and password before you can install the Desktop Filter. Please contact your ISP if you do not have this information. Perform the following steps to install and configure the Agape SafeGuard Desktop Filter:

1. Installation

1. Launch the Agape SafeGuard 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. Agape SafeGuard recommends using the default location.
7. Select **Finish** to restart the computer.

1. First Time Login

8. On restart, your Internet browser should start automatically. This may take a moment. Please be patient while the Desktop Filter communicates with the Policy Server for the first time. If the Internet browser does not start automatically, open the Internet browser and the Agape SafeGuard First Time Login screen is displayed automatically.

Dial-up Users

If you use a dial-up Internet connection, connect to the Internet now. Once you are connected, refresh your browser. The First Time Login page should now appear.

9. Enter your Profile Manager name and password at the Agape SafeGuard First Time Login screen and click **Continue**.

The First Time Login screen looks like this:

Profiles

One or more default Profiles may be created to allow you to access the Internet immediately after installing the Desktop Filter. These default Profiles typically use the name Child, Parent, Allow list only, Limited, Generous, or Unrestricted. If these Profiles use a password, this password is the same as the Profile Manager password. It is strongly recommended that you change the Profile password or your Profile Manager password if you plan to allow others to use this Profile.

The Desktop Filter is now installed. see *Running Diagnostics* on page 6 for troubleshooting help and *Clearing Your Browser Cache* on page 8 for instructions on removing saved web sites from your hard drive.

You can now create new Profiles or edit existing ones. See *Managing Profiles* on page 11.

3. Running Diagnostics

If you experience any problems after installation or just want to confirm that everything is working, you can run the diagnostics tool. To run the diagnostic tool, do the following:

1. Open your Control Panel from the Windows Start menu.
2. Find and open the **Filter Settings** icon.
3. Enter your Profile Manager password.
4. Select **Diagnostics**.

If everything is working, you should see this message:

Note
The name of your Policy Server may not be the same as above.

If your diagnostic results do not match the example shown (other than the Policy Server name), there may be a problem with your Policy Server, your network, or the computer. Please check for the following error messages or contact your Internet provider (or filtering provider) for assistance:

1. *Corrupt configuration data*
2. *Try reinstalling the client*

There may have been a problem during installation. Try reinstalling the Desktop Filter and running the diagnostics again to see if the problem is resolved. If not, contact your Internet provider.

3. *Unable to start winsock*
4. *Networking may be broken*

The Desktop Filter could not communicate with your network. Contact your network administrator or Internet provider to ensure that your computer has a working network connection.

If your computer is connected to a working network, check to see if there are any other error messages that may be related.

5. *Unable to get Policy Server IP*
6. *DNS is broken*
7. *Not connected to the internet*

The Desktop Filter could not communicate with your Policy Server.

In the Control Panel, remove the check mark from **Enable Filter** to disable the filter. Open a browser and surf to a few web pages to see if you have a working Internet connection. If not, there is a problem with your Internet connection. Contact your Internet provider to resolve this problem.

If your Internet connection is working properly, your firewall may not be configured properly. If you have a firewall, please ensure that it is configured to allow “nsfx.exe” to access the Internet or open port 3432 to both incoming and outgoing traffic.

8. *Policy Server send test failed*
9. *Policy Server port may be blocked*

The Desktop Filter could not send a packet to the Policy Server. Check to make sure that your firewall is configured to allow “nsfx.exe” to access the Internet or open port 3432 to both incoming and outgoing traffic.

10. *Filter provider not installed*
11. *Try re-installing the client*

A component of the Desktop Filter may not have been fully installed. Please try reinstalling the Desktop Filter and run the diagnostics again.

12. *Cannot get the webadmin url*
13. *Try Viewing Status to refresh*

The required registry keys could not be found or may have been modified. Close the diagnostics window and return to the Filter Settings window and click **View Status**. This will refresh the settings and rewrite the registry keys. Run the diagnostics tool again to see if the problem is resolved.

14. *Cannot download from the webadmin url*
15. *Port 8080 may be blocked*

The Desktop Filter could not connect to the Policy Server. Check to make sure that your firewall is configured to allow “nsfx.exe” to access the Internet or open port 8080 to both incoming and outgoing traffic.

4. Clearing Your Browser Cache

When you visit a web page, your browser may save the page, or parts of it, onto your hard drive. This allows it to load the page again later, without having to download all the components again. The result is that after you visit a page once, it may take less time to load the next time you visit it. However, since these pages are already stored on your hard drive, they are not filtered and can be viewed by anybody on the computer.

To prevent the browser from displaying web pages that were stored before the Desktop Filter was installed, it is recommended that you clear your browser's cache now. The following are instructions for three of the most common browsers: Internet Explorer 6, Firefox, and Netscape 7. If your browser is not listed here, please consult the browser's help option, website, or customer support.

1. *Internet Explorer 6*

Internet Explorer uses the term Temporary Internet Filter for the cache. To delete your Temporary Internet Files, do the following:

1. Open an Internet Explorer browser window.
2. Select **Tools**.
3. Select **Internet Options**
4. In the **General** tab, click **Delete Files**.
5. Select **Delete all offline content**.
6. Click **OK**.
7. Close all windows.

2. *Netscape 7*

To clear your cache in Netscape 7, do the following:

1. Open a Netscape browser window.
2. Select **View**.
3. Select **Preferences**.
4. Select **Advanced** from the menu on the left.
5. Select **Cache** from the menu under **Advanced**.
6. Click **Clear Cache.**
7. Close all windows.

3. Firefox

To clear your cache in Firefox, do the following:

1. Open a Firefox browser window.
2. Select **Tools**.
3. Select **Clear Private Data**.
4. Select **Cache** if it is not already selected.
5. If you do not want any other personal data removed (such as saved passwords or browsing history) or do not know what these options are, remove the checkmarks from these options. Generally, it is safe to remove all private data, unless your browser has stored important passwords for you that you don't remember.
6. Select **Clear Private Data Now**.
7. Close the browser window.

2. Managing Profiles

Situations, user needs, and expectations vary widely. Are you trying to just 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.

Also bear in mind that the Agape SafeGuard Desktop Filter is quite configurable. You can use the default settings or modify Profiles to meet individual needs. Tune the Profiles to achieve the filtering you desire with the least disruption. Whether you currently use a different filtering method or this is new, the users will learn what is allowed and denied and conform over time.

This chapter describes how to configure and fine tune your Desktop Filter to meet your needs.

1. Getting Started

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, Agape SafeGuard 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 the Agape SafeGuard Desktop Filter.

1. Accessing the Control Panel

All administrative tools for the Desktop Filter can 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:

Open the **Filter Settings** icon to access the Desktop Filter administration. At this point, you must enter your Profile Manager password and select OK to continue. The following screen appears:

From this window, you can choose to Enable/Disable the Desktop 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.

2. Accessing the Profile Manager

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

1. In the Control Panel, open **Filter Settings.**
2. Enter your password.
3. Select **Manage Profiles**.

You can also open the Profile Manager from several of the Agape SafeGuard pages (for example, the Status page and the Choose Profile page) by selecting the text **Click here to Manage Profiles**.

The Profile Manager screen appears with the Profiles tab selected:

1. Creating a Profile

1. Open the Windows Control Panel from the Start menu.
2. Locate and open **Filter Settings** from the Control Panel.
3. Enter your Profile Manager password and select **OK**.
4. Select **Manage Profiles**.
5. Select **New Profile**.
6. Enter a name for the new Profile.
7. Enter a description for this Profile, this is optional.
8. Enter a password and re-enter it to confirm. Passwords are case sensitive (lower case “a” is not the same as upper case “A”) and may contain both letters and numbers. If you want to allow anyone to use this Profile without entering a password, select “No password” instead.
9. Select the basic filter settings you want for this Profile. You can adjust or reset these settings later.

10. Choose the picture you want to associate with this Profile. This picture is only used when Icons are selected in Preferences.
11. Select **Add Profile**.

4. Modifying Profiles

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 or login settings 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.
- Test out some of the other Advanced Features of the Desktop Filter.

2. Profile Manager's Quick Reference Chart

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 Agape SafeGuard to review a web site's category or tell us about an Internet application.	Submit for review
Select when the Desktop Filter 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 Desktop Filter.	Software Updates
Leave the Profile Manager and choose a browsing Profile.	Exit Profile Manager

3. 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.

1. 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.

2. 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** group.

3. 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.

While there are hundreds of file sharing applications available, they generally use one of several common protocols. For example, Morpheus and Limewire currently use the Gnutella protocol. If you have a file sharing application you want to block but don't see it in the list, try searching the web for information about the application and what protocol it uses. Chances are it can be blocked by selecting one of the protocols in the **Protocols** tab.

4. 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 want to allow email access or don’t select any protocols 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**.

5. 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*.***

6. 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.

7. Streaming Media

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

4. Reports

When the Desktop Filter is installed, all Internet activity is recorded. Reports can be generated from this information to help you review the websites and Internet services that are being requested by each Profile.

Reports can be created daily, weekly, or monthly and are usually generated at midnight at the end of the report period. When you first create a report, a report for the previous day, month, or year is generated right away. You can view reports from the **Reports** tab in the Profile Manager, or you can have the reports emailed to you.

1. Report Descriptions

In the **Reports** tab, there are up to seven different types of reports available to help you review your user's Internet use.

Note
Some of the reports may not be available for all Profile Managers.

1. Internet Request Activity

This is a chart that shows the total number of requests, the requests that were allowed, and the requests that were denied. A request is any attempt to access the Internet, including attempts to check email, send instant messages, downloads files through peer-to-peer networks, and access other Internet-based protocols; not just view web sites.

2. Categories Visited

This is a pie chart and table of the number of times each category was assigned to a requested web page. A page can be assigned to one or more categories, so the Total Pages indicates the total number of categories assigned, not the number of pages that were categorized. For this reason, the Total Pages in this report may be higher than the number of pages shown in other reports.

3. Denied Categories Visited

This is a pie chart and table showing the categories that were denied. Again, a page request can be assigned to one or more categories so the total indicates all the denied categories that were assigned, not the number of pages that were categorized.

4. Top Websites Accessed

This is a table of the top 10 web sites that were requested – all requests over the top ten are grouped together under “other”. This report shows all web sites requested, including allowed and denied sites. This report does not include non-HTTP requests, such as email or instant messaging.

This report lists the top web sites, not the individual web pages. A web site is a collection of web pages that share the same host and port address. For example, there are many web pages (such as http://www.Agape SafeGuard.com/ISP and http://www.Agape SafeGuard.com/Products) at Agape SafeGuard's web site (http://www.Agape SafeGuard.com). The Total Pages column counts the total numbers of requests to any pages at that site.

5. Top Websites Denied

This is a table of the top 10 web sites (not web pages) that were requested and denied—all requests over the top ten are grouped together under “other”. This report shows all web pages requested, including allowed and denied pages. This report does not include non-web site requests, such as email or file sharing.

6. Request Log

This is a table that lists all Internet requests. A request includes any attempt to access the Internet. This includes email, instant messaging, file sharing, and any other Internet-based protocol; not just web sites. The table lists the time and date of the request, the URI of the request, the category (or categories) assigned, and a flag indicating whether the request was denied. **On** means the request was denied. **Off** means it was allowed.

7. Denied Request Log

This is a table that lists all the Internet requests that were denied. A request includes any attempt to access the Internet. The table includes the time and date of each request, the URI of the request and the category assigned to the denied request.

2. Creating Reports

To have one of the reports generated, do the following:

1. In the Profiles menu tab, select the Profile you want a report for.
2. Select the **Reports** tab.
3. Click the check box beside the Report you want to create.
4. If you want the reports sent to you by email, enter your email address in the **Email Reports to:** field. You can send the reports to more than email address by entering multiple addresses separated by a comma (,) and no spaces. For example:

   example1@Agape SafeGuard.com,example2@Agape SafeGuard.com

5. Select **Save**. A report for the last report period is now generated.
6. After a couple seconds, refresh (or reload) your browser and the report should be ready for viewing. If the report does not appear after refreshing your browser, the Reporter may be busy. Please wait a few minutes and try again. Reports that have no data may not emailed, depending on your server's settings.
7. Click **More** and select the report you want to view. If you are not emailing your reports, this is where you will go to view reports in the future.

If you want to send a test email through the Profile Manager to make sure that your reports can be sent properly, click on the **Test** button on the **Reports** tab.

5. Advanced Features

Once your Desktop Filter is up and running, there are many options available to the Profile Manager to tune the Desktop Filter to your needs. This section describes those features and how to use them.

1. Opening 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. Agape SafeGuard allows you to connect to the Profile Manager from anywhere over the Internet. Using a computer with Internet access, but without the Desktop Filter installed, enter your Remote Login URL into your web broswer to access the Profile Manager. Your Remote Login URL depends on the name of your Policy Server. The URL typically starts with "http://", followed by the name of your Policy Server, and ends with "/webadmin/clientlogin/".

Example: http://example.Agape SafeGuard.com/webadmin/clientlogin/

The URL string for the Choose Profile page*,* the Status page and the Deny page also contain the name of your Policy Server. If you can not access a computer with the client installed, contact your ISP or have one of your users check this for you.

2. 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.

3. Blocking or Allowing Categories

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

1. In the Profiles menu tab, select the Profile you wish to modify.
2. Go to the **Categories** tab.
3. Click an option button on the left to select which type of web categories to modify.
4. Click on a check box to block the category. Boxes that already have a check mark are currently blocked. To unblock a category, click on the box to remove the check mark.

4. Blocking or Allowing Protocols

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 Gmail, you must select Web E-mail from the *Web Categories*.

To block or unblock a protocol, do the following:

1. In the Profiles menu tab, select the Profile you wish to modify.
2. Go to the **Protocols** tab.

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

While there are hundreds of file sharing applications available, they generally all use one of the protocols listed. For example, Morpheus and Limewire currently use the Gnutella protocol. If you have a file sharing application you want to block but don't see it in the list, try searching the web for information about the application and what protocol it uses. Chances are it can be blocked by selecting one of the protocols in the **Protocols** tab.

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:

1. Open the Profile Manager.
2. Select the Profile you want to modify.
3. Go to the **General** tab.
4. Select either **Allow All** or **Deny All** and choose a time period
5. Click **Save Changes**.

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

5. About the Allow List

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” and the path 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.

6. About the Deny List

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 keyword “sex” also blocks any site with the word “Sussex” in the URL string.

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

7. 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:

1. Allow All or Deny All setting
2. Time restriction setting
3. Allow List and Deny List settings
4. 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.

8. 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
- Live
- Excite
- Lycos

If the Search Engine category is blocked, no search engines are allowed, regardless of whether this category is selected or not. The Search Engines category must be allowed(or specific engines placed in the allow list) for Safe Search to work.

Note

Turning on **Allow All** overrides the Safe Search function.

1. Setting Time Restrictions

2. The Desktop Filter 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. Click on a grid for a particular day and time to block all access to the Internet during that period.

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 “What are some dirty words” in a search engine, such as Google or Yahoo, the search results are blocked.

9. Disabling the Filter

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

1. Open the Windows Control Panel from the Start menu.
2. Locate and open **Filter Settings**.
3. Enter your Profile Manager password and select **OK**.
4. Click to remove the check mark in the **Enable Filter** check box.
5. Select **OK**.

Your Desktop Filter is now disabled. Once you are ready to turn the Desktop Filter back on, repeat these steps and replace the check mark in the **Enable Filter** check box.

10. Saving Active Profile Settings

In the Preferences menu tab, you can select whether the Desktop Filter 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 can not 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 the Desktop Filter log out when the computer has been idle long enough to activate the screensaver by selecting **Exit Profile on screensaver**.

1. 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.

2. 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.

3. 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.

4. 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.

5. *Exit Profile on screensaver*

If your computer sits idle for several minutes, your screensaver may appear or you may enter "Suspend" mode, depending on your system and your Control Panel settings. If this option is enabled, users are logged out of their Profile when the screensaver appears or the computer enters the suspend mode. Users must choose their Profile again if this occurs.

11. Restricting Profile Logout

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:

1. *No password required*

Users do not need to enter a password to log out of their current Profile. Generally, this option is

2. *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.

3. *Require Profile Manager password*

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

4. *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.

12. Customizing the Deny Page

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 a web site that is not allowed by their Profile.

1. *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.

2. *Minimal deny page*

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

3. *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 Agape SafeGuard logo or information about why they were blocked. Note that you can not enable Include **Quick Allow Access link** or **Include admin email link** when this option is selected.

4. 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. Anyone 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 can 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”. This is expected since the page is trying to load more than just the site you've allowed. Sites that redirect you to another web site will be denied again.

5. 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 the address you provide 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.

13. Submitting Sites for Review

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

If you have a web application or protocol that is not listed in the **Protocols** tab, you can also submit the name of the application or a web site associated with the application.

3. Using the Internet With Agape SafeGuard

This section is designed to teach you how to use the Internet with the Desktop Filter installed. Each user, or group of users, should receive a Profile name and a password from their administrator.

With the Desktop Filter installed, anyone using the computer must be using a Profile to access the Internet. You can log into a Profile using the Choose Profile page. The Agape SafeGuard Icon, Popup Messages, and the Status page are some other useful tools that help you use Agape SafeGuard simply and easily.

About the Agape SafeGuard Icon

Once the Agape SafeGuard Desktop Filter has been installed on your computer, a blue and yellow Agape SafeGuard icon appears in the Windows notification area (also called the 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. By right-clicking on this icon, you can also choose to open the Status page or log out of your current profile

1. Agape SafeGuard Icon Status

The Agape SafeGuard Icon changes depending on the Desktop 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.

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

When this rotating icon appears, the Desktop Filter is connecting to the Policy Server. The Desktop Filter is working and your Internet request will load shortly.

2. Internet User's 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 Agape SafeGuard Icon in the notification area (system tray). 2. Select or enter your Profile name and password.
Open the Profile Manager to manage Profiles.	1. Double-click the Agape SafeGuard Icon in the notification area. 2. Click the text **Click here to manage Profiles**. 3. Enter your Profile manager password and click **Continue**.

I am 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 Agape SafeGuard Icon in the notification area.
Change my Profile.	1. Double-click the Agape SafeGuard Icon in the notification area. 2. Select the **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 Agape SafeGuard Icon in the notification area. 2. Select the **Click here to Logout and Choose a Profile** link. 3. Close all browser windows.

3. Popup Messages

Popup Messages or Balloon Messages are notes that pop up from the Windows Notification Area. They display notices and tips to help you use the Internet. A Protocol Message may tell you what the Desktop Filter 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:

1. Hide Popup Messages

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

1. Open the Windows Control Panel from the Start menu.
2. Locate and open the **Filter Settings** icon in the Control Panel.
3. Enter the Profile Manager password.
4. Uncheck **Show Popup Messages** in the Filter Settings screen.

2. Show Popup Messages

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

1. Open the Windows Control Panel from the Start menu.
2. Locate and open the **Filter Settings** icon in the Control Panel.
3. Enter the Profile Manager password.
4. Check **Show Popup Messages** in the Filter Settings screen.

4. The Choose Profile Page

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 Agape SafeGuard icon in the Notification Area and select **Click here to Log Out and Choose a Profile**.

If you are not logged in to a Profile, double-click on the Agape SafeGuard icon in the Notification Area.

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 PIC for several minutes, the session may time out. Return to the Choose Profile page and log in to your Profile to continue.

5. The 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. You can not access the Status page until you log in to a Profile.

If you are not logged in to a Profile, you must return to the Choose Profile page, by double-clicking the Agape SafeGuard icon, and log in to a Profile before you can access the Status page.

If you are logged in to a Profile, double-click on the Agape SafeGuard icon in the Notification Area to open the Status page. The Status page should look similar to this:

In the *Status page*, you are notified which Profile you are currently logged in to and which types filtering options have been enabled for that Profile. Filters that are currently enabled are marked by with check mark surrounded by green circle. 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”.

4. Category Descriptions

This list identifies and describes the Agape SafeGuard categories that are visible in the Profile Manager. There are also a number of internal categories that are generally not visible to the user/administrator that are used to manage error conditions or internal processing.

The Agape SafeGuard categories can be considered “black list” categories—that is, when you choose a category, users will be blocked from going to or seeing any URL that has been determined to belong to that category. For example, when you select the Sports category, users are not allowed to go to URLs that are determined to be sports sites.

It is possible for a URL to belong to more than one category.

1. Adult Categories

1. Alcohol (Blocked by Agape)

This category contains information related to alcohol, including wine, spirits, beer, cocktail recipes, homemade alcohol, or any other alcoholic drink. It also includes information about bars, pubs, nightclubs, bartending, liquor sales, and hangovers and other side effects of alcohol.

2. Alternative Lifestyles (Blocked by Agape)

Alternative Lifestyles are habits or behaviors related to social relations, dress, or recreation. These behaviors 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.

3. Criminal Skills (Blocked by Agape)

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.

4. Gambling (Blocked by Agape)

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.

5. Extreme (Blocked by Agape)

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.

6. Hate Speech (Blocked by Agape)

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.

7. Substance Abuse (Blocked by Agape)

Substance Abuse contains URLs that provide information on illegal drugs used for recreational rather than medical purposes, or URLs that promote the abuse of legal drugs. 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.

8. Match Making (Blocked by Agape)

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.

9. Occult (Blocked by Agape)

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.

10. Pornography (Blocked by Agape)

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.

11. Profanity (Blocked by Agape)

This category contains words that are generally considered obscene, vulgar, or derogatory. This includes the use of so-called "four letter words", racist or sexist terms, and objectionable sexual references.

12. Weapons (Optional to User)

This category contains information related to the promotion, sale, or discussion of weapons. Weapons are any form of device used in combat that can injure or kill, such as guns, knives, or swords. Information on how to build weapons or bombs is included in Criminal Skills.

2. Entertainment Categories

1. Arts & Culture (Optional to User)

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.

2. Entertainment (Optional to User)

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.

3. Games (Optional to User)

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.

4. Humor (Optional to User)

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

5. Sports (Optional to User)

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.

3. Information Categories

1. General News (Optional to User)

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.

2. Journals and Blogs (Optional to User)

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.

3. Politics (Optional to User)

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.

4. Portals (Optional to User)

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.

5. Religion (Optional to User)

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.

6. Self Help (Optional to User)

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.

7. Sex Education (Optional to User)

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

8. Technology (Optional to User)

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.

9. Travel (Optional to User)

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

Security Categories

1. Adware (Blocked by Agape)

Adware contains intrusive advertising, such as banners ads and pop-up ads that may be used to track your activity and display ads based on your surfing patterns. These ads are typically drawn from an ad server at a different site. When this category is blocked, portions of some pages may appear broken – what is actually happening is that the advertisements are being blocked while the main content is displayed. Each portion of a page drawn from a unique location is categorized and filtered separately. Generally, this category should be blocked.

2. Directory (Blocked by Agape)

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.

3. Host Is An IP (Blocked by Agape)

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.

4. Malformed URL (Blocked by Agape)

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.

5. Phishing (Blocked by Agape)

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.

6. Proxy Anonymizer (Blocked by Agape)

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

7. Under Construction (Optional to User)

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.

5. Miscellaneous Categories

1. Investing (Optional to User)

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.

2. Job Search (Optional to User)

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.

3. Sales (Optional to User)

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.

4. Search Engine (Optional to User)

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.

5. Web Chat (Optional to User)

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.

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

6. Web Email (Optional to User)

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.

6. 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 Desktop 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.

1. General **(Optional to User)**

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.

2. Images **(Optional to User)**

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

3. Network Unavailable **(Blocked by Agape)**

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.

4. Network Timeout **(Blocked by Agape)**

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.

5. Intranet Servers **(Optional to User)**

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

6. New URL **(Blocked by Agape)**

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). If you block New URL you are failing closed (deny) on any new URL; if you do not block New URL you are failing open (allow) on any new URL.

7. No Text **(Optional to User)**

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, No Text pages should not be blocked.

8. Redirector Page **(Optional to User)**

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.

We are here to help.

You can reach us at:

****Preferred – Change request form on the website**

Phone – (800) 498-1788

Fax (866) 633-7140

After Hours Emergency Number – (260) 433-3144