ContentProtect Pro Suite

Administrator User Manual

Instructions for Installing and Using the Application

ContentProtect EmailProtect PopupProtect

Table of Contents

Welcome to ContentProtect Pro Suite

Congratulations! You now have the most comprehensive—and yet most easily adaptable Internet filtering software available today. However, we realize that not all organizations have the same needs, which is why we have developed **ContentProtect Pro Suite's** unique filtering process, which is customizable for your organization.

Sources of help

The following is a list of help sources for **ContentProtect Pro Suite**.

1. The **ContentProtect Pro Suite** User Guide (PDF format) – Available on-line to Administrators
2. Step-by-step instruction (Quick Start Guide)
3. **ContentProtect Pro Suite** category list with descriptions – Only available to Administrators online by clicking the category link and also listed below.
4. FAQs (Frequently Asked Questions)
5. **ContentProtect Pro Suite** Web-based reporting
6. Prompt, competent, and courteous **Customer Support** by calling **1-800-485-4008** for questions and technical assistance. Customer Support is available Monday through Friday, 8 a.m. to 5 p.m. Mountain Standard Time.
7. You can email your questions any time to info@contentwatch.com.

System Requirements and Key Features

The following list explains the system requirements for **ContentProtect Pro Suite** and the key features.

System Requirements

- PC with Pentium or compatible 133 MHz or faster processor
- Microsoft Windows 98SE/Me/2000/XP
- 64 MB RAM
- 100 MB hard drive space
- Color monitor with a minimum 800x600 resolution
- Internet connection
- Internet Explorer 5.0 or greater, Netscape 6.0 or greater

Key Features

- Online organization management
- Online group management
- Online user management
- User-friendly interface
- Client-based filtering
- Server-based category settings
- Unique and portable user profiles
- Web-based drill-down reports
- Blocked site override option
- Email notifications of inappropriate Internet usage
- Online activity reports on Chat (IM) and Internet activity
- Online URL recategorization

Getting Started

To begin using **ContentProtect Pro Suite**, follow the instructions below:

1. **Set up your organization's account** and create an administrator user account.
2. **Install the Client on each computer** (this step can be accomplished by the system administrator or the user). During the install, if the user account does not already exist, it will be created.

Note: After installation and upon logging into **ContentProtect Pro Suite** (if login is required), each workstation will assume the default Internet settings. Specific user account settings can be set in the online management application by an organization or group administrator.

3. **Log in to the online management application** (https://ce.contentwatch.com/). When prompted, enter your organization account name, administrator username, and password.

With this application you can:

- Add and modify user and group profiles (including Internet settings)
- Assign users to groups
- Re-categorize URLs
- Add Notification Rules to notify you of possible inappropriate activity

You can set up specific Internet settings for:

- Giving other users administrator privileges
- Viewing Internet activity reports from within your organization for the entire organization or by user or group.

Install from the World Wide Web

To install **ContentProtect Pro Suite** from the World Wide Web, follow the instructions below:

1. Access the following Web site:

   https://cemaster.contentwatch.com/CEMaster/

2. Before installing **ContentProtect Pro Suite** on each computer, you will need to create your organization's account. When you purchased the product you received a 16-digit registration number and a link to the online setup. (If the account was set up for you or you already have an account, skip to "Account Setup and

Installation"). The registration number only needs to be entered once to begin the setup process and may not be used again.

3. Enter the 16-digit registration number you received from ContentWatch in an email prior to creating your organization.
4. Enter the appropriate organization information in the respective fields (All fields are required.):

Enter the name of your organization:
This will be used for display purposes in the reporting and online management application.

Create an account name:
This will be needed during the installation of the client application and is designed to identify members within a given organization.
(4-20 alpha-numeric characters)

Create an install password:
This will be used to install **ContentProtect Pro Suite** on individual user machines.
(4-20 alpha-numeric characters)

Create an uninstall password:
This will be needed to uninstall the client application from personal computers. This should be kept confidential and be different from the install password. Anyone with the uninstall password can remove **ContentProtect Pro Suite** from their computer.
(4-20 characters, no dashes or spaces)

5. Click **Next**.

6. Enter the appropriate Organization Administrator information in the respective fields:

First and last name:
This is used to identify you in the Online Management application and reports.

Email address:
Enter the address that you would like notifications of inappropriate Internet activity to be sent to. This address will also be used to send you a confirmation email when the setup process is complete.

Create an Administrator user name and password:
You will need the Administrator user name and password to sign in to the Online Management application, which you would go to in order to add and modify users' profiles, create other Administrators and view reports.
(4-20 alpha-numeric characters)

7. Click **Next.**
8. Verify the information you just entered is correct and print a copy of it for your records, click **Next.**
9. A *What's Next?* screen will display with the following message:

> Congratulations! You've successfully set up your Organization's Account. You can now install the application on personal computers that will be monitored and filtered. An email has been sent to you with a download link and instructions on how to install the client software. The e-mail also contains the Organization Account Name and Install Password, which will be needed. To save time, forward this email to anyone that needs to install this application on his or her computer.
>
> To download the application now, click on the link below:
> http://cemaster.contentwatch.com/CEMaster/download.html

10. Access the following Web site to download the software to your computer:

    http://cemaster.contentwatch.com/CEMaster/download.html

    Click **Download Now**.

11. A download window will display. Select **Save**. Designate where you want to save the file on your computer. Click **OK**.
12. Double-click the downloaded file (wwesetup.exe) on your hard drive and follow the on-screen directions to begin the installation.

Installation from a CD

Note: You must have an Internet connection to install **ContentProtect Pro Suite**. If you have a dial-up connection, you should connect to the Internet and close all applications before installing.

To install the software from a CD, follow the instructions below:

1. Insert the CD into the CD ROM drive (If the CD does not automatically run, go to Start>Run type in "d:Autostart.exe" Replace the D with the letter for your CD-ROM drive.)

2. From the Menu, select Install Software; this will open the Setup Wizard.

3. Click **Next** to start the Setup Wizard.

Setup Wizard

Once the Setup Wizard displays, you are ready to install **ContentProtect Pro Suite**.

1. Click **Next** on the Welcome screen.
2. Choose to accept the license. Click **Next**.
3. Choose the Install directory. Click **Next**.
4. Select the products to install. You must install ContentProtect Professional. Click **Next**.
5. Enter the Organization Account Name and the Install Password. Your administrator should have provided these; contact your administrator if you do not have the account name and password. Click **Next**.
6. Enter all of your user information. The Email field is not required, but it is recommended. Click **Next**.
7. Verify your settings and then click **Install** on the confirmation dialog.
8. Click **Finish** to restart the computer and complete the installation.
9. When the machine restarts, run the Online Updates. You can launch this from any of the products or by selecting it from the right-click menus of the taskbar icons located at the bottom of the screen next to the clock.
10. When the update dialog displays, click **Check For Updates**.
11. If the default settings have not been changed, the new updates will download and install automatically. If the default settings have been modified, follow the prompts to download and install updates. When the process is complete, select the "Click here to restart your computer now" link.
12. Your system should now be fully updated with the newest version of **ContentProtect Pro Suite**.

Signing In as an Administrator

After the **ContentProtect Pro Suite** organization has been created, you need to define the user profiles for the specific groups and/or workstations in your organization. You must first sign in to the online management application as an administrator to modify user profiles. You set up an administrator account during the organization setup, so it is simply a matter of signing in with your organization account name, administrator username and password.

ContentProtect Pro Suite Admin Utility Application

This utility can be used on individual computers to:

1. **Find out which user is currently signed in** on the current PC
2. **Sign users in and out**
3. **Force changes made online to take effect immediately:** There is a wait period of up to an hour for changes made through the online management application to automatically take effect.
4. **Display license information** (This may be needed for customer support.)

This utility can be run from a CD, floppy, network, or hard drive. It does not need to be installed.

Note: This utility is not needed unless the Client User Interface (UI) is hidden except to view license information. If the Client UI is not hidden, you can perform all these tasks within it. We recommend not copying this utility to computers not run by administrators.

To download the utility:

1. Login to the online management application.
2. Click on the **Downloads** link next to Sign Out.
3. Click on the **Download Now** button for the **ContentProtect Pro Suite** Admin Utility application. A dialog box will display asking you where to save the file. Once the utility is downloaded, simply run the utility by double-clicking the icon or filename of the downloaded file. You will need to log in with the administrator user name and password.

User Preferences

To setup your **ContentProtect Pro Suite** preferences, follow the instructions below:

1. Access the following Website:

   https://ce.contentwatch.com/

   The **ContentProtect Pro Suite** login page will display.

2. Enter the login information that you created when you setup your account. Click **Go**. Your specific organization *Management* page will display.

The following preference levels can be set from this page:

- Organization
- Group
- User
- URLs
- Notifications
- Administrators

Organization Overview

All settings made to an organization are inherited by all groups and users. Group or user settings can be made more restrictive, but not less.

From the Organization page you can:

1. **Modify the organization name** (for display purposes only. This is NOT the account name).
2. **Change the install and uninstall passwords** (These are needed to install and uninstall **ContentProtect Pro Suite** on individual computers).
3. **Choose to log Web and Chat (IM) protocols for the entire organization** (Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger).
4. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols for the entire organization (**Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit http://www.gnutella.com/connect/.)
5. **Adjust filter settings in each category to Warn, Block, or Allow** (Next to a category name, select an action (Warn, Block or Allow) for that category by choosing from the drop-down bar. For more information see *Categories)*.

Organization Profile

A profile is made up of names, passwords, protocol settings and filter settings (i.e. whether to warn, block, or allow Web content of specific categories).

Create the Install Password - The password needed to install the **ContentProtect Pro Suite** application on individual computers.

Create the Uninstall Password - The password needed to uninstall the **ContentProtect Pro Suite** application from individual computers.

Web, Chat, Peer-to-Peer, Newsgroups - To allow users access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs. **Note:** User access can be denied through group or user settings.

Logging Users' Activity - To log user activity, check the **Log** box below the Access Allowed box. All user activity will be recorded and displayed in the Reporting section. Only Web and Chat allow logging.

Set Organization Restrictions

1. Click the **Organizations** link. The *Settings* page will display. This screen allows you to set organization-wide filter settings, enable or disable organization protocols and change install passwords.
2. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

    - Allow - allow user access to sites containing content in the category
    - Warn - warn the user the site may contain objectionable material in the category
    - Block - block the user from sites containing content in the category

    For each of the categories set the desired restriction level for the entire organization. Group or User settings can be made more restrictive than the organization settings, but not less.

3. Click the **Apply** button to affect the changes.

Categories

The best way to determine the category of a site is to examine the contents. Once you know the information a site contains you can more easily assign it to a category. Sites in a given category usually contain the same type of links, images, and text.

Note: Some sites will be categorized with multiple categories unless the site is manually recategorized. **ContentProtect Pro Suite** does the examining for you and determines the category of a requested Web page. After the category is determined, filter settings (Allow, Warn, or Block) are then applied.

Note: An administrator of a particular group can set a category action to be more restrictive but not less restrictive than the parent group. (e.g. If the Organization action for Adult/Mature is set to *Block*, no group or user settings within that organization can be set to *Warn* or *Allow*. However, if the Organization action is set to *Warn*, an administrator can change the action for a group or user to *Block* or *Warn* but not *Allow*. If the Organization's action is set to *Allow*, any group or user's action within that organization can be changed to *Warn*, *Block*, or *Allow*.

Category Descriptions

Ads - Advertisements for products, services, etc.

Adult/Mature - Sites or resources that contain subject matter intended for mature audiences, such as obscene or vulgar language and adult Chat rooms. These sites could be considered R-rated.

Chat Site - Sites or resources that contain information on Chat protocols or applications, links to Chat organizations, rings, and rooms.

Drugs/Alcohol - Sites or resources that contain subject matter that deals with the manufacturing, distribution, or obtaining illegal drugs, alcohol, or other controlled substances. Sites that depict drug or alcohol paraphernalia and/or include methods for obtaining or manufacturing them. Does not include sites that provide information on prescription medications except those sites that describe how to illegally obtain them.

Email - Sites or resources that provide access to email services, and applications.

Employment/Career - Sites providing information on employment opportunities and resources for expanding career options.

Family Resources - Sites or resources that provide family counseling, family safety tips, parenting information and tips, and family planning.

Financial/Stocks - Sites or resources that provide information about finances, financial planning, insurance, stock tickers, stock reports, or sites that allow the sell and purchase of stock. Includes banks and credit unions, and credit rating and reporting sites.

Gambling - Sites or resources that allow a person to wager money on online games with the expectation of winning money or prizes. Sites that contain links to other gambling sites or provide information on gambling strategies or tactics.

Games - Sites or resources that provide access to online or downloadable games, or discussions about games. Sites that provide information about game cheats.

Government - Sites or resources that are specific to local, state, or federal government organizations or agencies, including political party sites and specific, official political sites. Sites ending in .gov.

Hate/Violence - Sites or resources that promote or depict violence against persons, animals, property, or nations. Sites that single out groups for violence based on race, religion, or creed.

Health/Medicine - Sites or resources that deal with or provide information on mental or physical health issues. Sites that allow the online purchase of prescription medications.

Illegal Activities - Sites or resources that provide information about the manufacture, alteration, or sales of weapons. Sites that promote or depict disorderly conduct, or that provide information on the manufacturing of explosives and explosive devices.

Instructional - Sites or resources that contain instructional material, tutorials, or how-to pages.

Intimate Apparel - Sites or resources that display models wearing underwear, lingerie, or other suggestive or see-through attire, including swimsuits.

Kids - Sites or resources intended for children, including entertainment, education, crisis counseling, and kid-friendly communities.

Music/Entertainment - Sites or resources that provide access to free downloadable or for-pay online music and video files such as MP3, WAV, MPG, and AVI, etc. Sites that sell music or videos, or that are dedicated to the music or entertainment industry. Sites that provide information on TV programs and programming, including movie review sites.

News - Sites or resources that provide live, recorded, or written reports or editorials about current events.

Personals - Sites or resources that contain personal ads, personal info pages, and personal portals.

Pornography - Sites or resources that are meant to sexually arouse the viewer. May show models or real people that are engaged in erotic behavior intended to cause sexual excitement. May describe sexually explicit activities or contain sexually explicit material including images, movies, or text. Sites would be considered X-rated.

Religious - Sites providing information on specific religions or general religious resources.

Schools/Colleges - Sites or resources that contain information dealing with colleges, schools, seminars, or courses. Sites that end with edu.

Search Engines/Portals - Sites or resources that provide mechanisms for searching the Internet by specific words or phrases and that display the results as either links or images. Sites that allow a user to customize the look or content and that are geared to providing a starting place on the Internet.

Shopping - Sites or resources that provide access to online malls, catalogs, or auctions, including classified ads. Department store sites, retail store sites, or sites that have coupons for free or discounted items.

Sports - Sites or resources for sports information including amateur, college, and professional sports.

Travel - Sites or resources that provide travel information ranging from general information to booking reservations.

Work Related - Sites or resources that provide information related to a user's work.

Groups Overview

Using multiple groups is **optional** but makes changing settings and reporting more manageable. For example, you can view reports on a group that will tell you how a specific department in an organization is using the Internet. You can also change Internet settings for all members in a particular group at the same time.

From the group page you can:

1. **Modify the group name** (for display purposes only
2. **Choose to log Web and Chat (IM) protocols for users assigned to this group** Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger. **Note:** If the group's Log checkbox is checked, a user cannot change this setting. Also, if logging is enabled on the organization it cannot be disabled on the Group or User level.

3. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols** Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit http://www.gnutella.com/connect/. **Note:** If the group's **Access Allowed** checkbox is not checked for a particular protocol, no users assigned to this group will be able to access that protocol.
4. **Adjust filter settings in each category to Warn, Block, or Allow** This will affect only members assigned to this group

Note: User settings can be made more restrictive than the organization or group's but not less restrictive.

Group Profiles

A group profile is made up of names, protocol settings and filter settings (i.e. whether to Warn, Block, or Allow Web content of specific categories) that affect all members of the group.

To modify a group's profile, follow the instructions below:

1. Click on the **Groups** button in the navigation menu to view the **Group List**. The groups will display alphabetically.
2. Click on the group name to view and/or modify the profile.

Web, Chat, Peer-to-Peer, Newsgroups - To allow users of this group access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs.

Note: User access can be denied through group or user settings.

Logging Users' Activity - To log user activity within this group, check the **Log** box below the Access Allowed box. All user activity will be recorded and displayed in the Reporting section.

Set Group Restrictions

1. Click the **Groups** link. The *Group Lists* page will display.
2. Click on the name of the group you want to modify. This screen allows you to set group wide filter settings and enable or disable group protocols.
3. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

    - Allow - allow user access to sites containing content in the category

    - Warn - warn the user the site may contain objectionable material in the category

- Block - block the user from sites containing content in the category

For each of the categories set the desired restriction level for the current group. Group or User settings can be made more restrictive than the organization's but not less.

4. To set group level restrictions regarding Chat rooms, Peer- to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
5. Click the **Apply** button to affect the changes.

Create New Groups

1. Click the **Groups** link. The *Group Lists* page will display.
2. Click **Add New Group**. A *Settings* page will display. This screen allows you to set group-wide filter settings and enable or disable group protocols.
3. Enter the name of the group in the **Group Name** field.
4. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

    - Allow - allow user access to sites containing content in the category
    - Warn - warn the user the site may contain objectionable material in the category
    - Block - block the user from sites containing content in the category

    For each of the categories set the desired restriction level for the current group. Group or User settings can be made more restrictive than the organization's but not less.

5. To set group level restrictions regarding Chat rooms, Peer- to- Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
6. Click the **Apply** button to affect the changes.
7. To add additional groups, click the **Groups** link and repeat steps 1 through 6.

Delete a Group

1. Click the **Groups** link. The *Group Lists* page will display
2. Click the **Delete** link located to the right of the group. A *Confirmation* screen will display
3. Click **OK** to confirm the deletion. (Note: The default group cannot be deleted.)

Reassigning Users to Groups

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users names you want to reassign.
3. Select the group you want to assign the users to from the Move selected users to group drop down menu.
4. Click the **Submit** button.

User Overview

User profiles contain settings and information for a specific user. From the users pages you can:

1. **Add and delete users**
2. **Modify user information** (name, email address and password)
3. **Assign user to a specific group**
4. **Disable Internet use** (Internet, Chat (IM), Peer-to-Peer, and Newsgroups)
5. **Allow user to override blocked messages**
6. **Enable automatic login**
7. **Show or hide ContentProtect Pro Suite interface on user's personal computer**
8. **Allow user to request blocked pages to be re-categorized**
9. **Choose to log Web and Chat (IM) protocols** (Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger)
10. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols** (Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit http://www.gnutella.com/connect/)
11. **Adjust filter settings in each category to Warn, Block, or Allow.**

Note: User settings can be made more restrictive than the organization or group but not less restrictive.

User Profiles

To modify a user's profile:

1. Click on the **Users** button in the navigation menu to view the **User List**. Users are listed alphabetically, under the assigned group's heading
2. Click on the user's name to view and/or modify his/her profile.

Status

If **Yes** is checked under **Disable Internet Use**, the user's account will be disabled.

Password

This password is used to:

1. Login to **ContentProtect Pro Suite**
2. Override blocked Web pages (if option is allowed)
3. Log in to the reports and system management (administrators only).

Options

- **Override blocked message:** If **Yes** is checked, the user is able to override any Web page that is blocked by using his or her password. Overridden Web pages are reported if logging is enabled.
- **Auto client login:** If **Yes** is checked, users will be automatically logged in to use the Internet
- **Show client user interface:** If **Yes** is checked, users will be allowed to view their profile and settings on their personal computer. The user will also be able to refresh their profile manually to force changes to take effect immediately.
- **Show Request Recategorize button:** If **Yes** is checked, users will be given the option to request that a blocked site be recategorized by an admin. For more info on Recategorization, click here. (Note: If the client user interface is visible, the user may request URL recategorizations from within it, even if this option is not set to Yes.)

Web, Chat, Peer-to-Peer, Newsgroups - To allow users access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs. **Note:** User access can be denied through organization, group or user settings.

Logging Users' Activity - To log user activity, check the **Log** box below the Access Allowed box. All user activity will be logged and displayed in the Reporting section. Logging is only available for Web and Chat access types.

Import a User's Account to a Specific PC

If a user's account has already been created in the online management application, or by installing **ContentProtect Pro Suite** on another computer, the same settings can be imported to another computer.

1. Begin the **ContentProtect Pro Suite** installation and type in the user name and password you would like to import. The account information and settings will automatically be imported to that computer.

Note: It is not necessary to import a user account if the client software has already been installed. A user that has been previously created by either installing on another computer or by the administrator in the online management application, can simply sign in with his or her username and password. When this is done all of the user's settings are imported. User profiles are fully portable. Once the user profile exists in the online management application the user can sign in on any computer that has the client software installed.

Set User Restrictions

1. Click the **Users** link. The *Users List* page will display.
2. Click on the name of the user you want to modify. The users *Profile* page will display. This screen allows you to modify user information, adjust individual filter settings, enable or disable protocols for an individual, change passwords, and enable override options.
3. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

    - Allow - allow user access to sites containing content in the category
    - Warn - warn the user the site may contain objectionable material in the category
    - Block - block the user from sites containing content in the category

    For each of the categories set the desired restriction level for the current user. User settings can be made more restrictive than the organization and the group, but not less restrictive.

4. The following restrictions and changes can also be set from this screen:

    - Restrict user from the Internet
    - Change user's Password
    - Set user options

    Set the desired options for each of the user settings.

5. To set user level restrictions regarding Chat rooms, Peer-to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
6. Click the **Apply** button to affect the changes.

Create New Users

There are two methods that you can use to create new users.

- The first method (preferred) is through the client installation process. The way this method works is when the user installs the client software on his or her computer the information he or she enters will be compared to the users already in the system. If the account information does not match an account already in the system, the new user will be created. This method does not require any intervention by the administrator. All users created using this method will be placed in the default group as specified by the administrator on the Groups page of the online management application. The administrator can make adjustments to the user profile and/or move it into a different group as needed after the user has completed the client installation.
- The second method requires the administrator to do all of the work that is done automatically by the client installation.

To create a new user in the online management application, follow the instructions below:

1. Click the **Users** link. The *Users List* page will display.
2. Click the **Add New User** link. The *Add New User Profile* page will display.
3. In the Information section add the following information:

    - Username: enter a username in this field. (The username must be unique and if it isn't you will be prompted to enter a different username.)
    - First and Last Name: enter the user's full name in this field

- Email: enter the user's email address in this field (This is the address where notifications will be sent if the user is made an administrator.)

- Group: select the group you want to assign this user to from the drop down menu. (If no group is selected, the user will be placed in the default group, which appears in the dropdown automatically.)

4. Enter the user's password in the **Password** field.
5. Confirm the user's password by reentering it in the **Confirm** field.
6. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

    - Allow - allow user access to sites containing content in the category

    - Warn - warn the user the site may contain objectionable material in the category

    - Block - block the user from sites containing content in the category

    For each of the categories, set the desired restriction level for the current user. You can make the user settings more restrictive than the organization and the group settings, but not less restrictive.

7. The following restrictions and changes can also be set from this screen:

    - Restrict user from the Internet

    - Change user's Password

    - Set user options

    Set the desired options for each of the user settings.

8. To set restrictions regarding Chat rooms, Peer-to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
9. Click the **Apply** button to add the new user. (Note: Clicking on any of the access type tabs will also apply changes. When changes are applied to the user profile, red text will appear under the user's profile name indicating the user profile was updated.)

Delete a User

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users' name.
3. Click the **Delete Selected Users** button. A *Confirmation* screen will display.
4. Click **OK** to confirm the deletion.

Reassigning Users to Groups

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users' names you want to reassign.
3. Select the group you want to assign the users to from the Move selected users to group drop down menu.
4. Click the **Submit** button.

URLs

Just as **ContentProtect Pro Suite** examines each Web page request for category content to determine which category a site belongs to, the administrator(s) can re-categorize any URL. This forces a specific Web site to be categorized as the administrator specifies. Associated Filter Settings (Allow, Warn, or Block) for that category are then applied.

Consider the following example:

CommunityWatch is our community resource section accessible through the ContentWatch Website. Because CommunityWatch contains many educational articles that deal with the problems caused by pornography (and which therefore, contain some adult content) a normal filter (ours included) would block this site as pornography. After going to the site and examining the content, it would be clear that it is not pornography and should be re-categorized. Let's assume you want the URL www.contentwatch.com re-categorized as Family Resources.

To recategorize a URL, follow the instructions below:

1. Click on the **Manage Recategorized URLs** link under the URLs section.
2. Click on the **Add New URL** button.
3. Type in www.contentwatch.com and select Family Resources from the drop down list.
4. Click **Recategorize**. This site will now be compared to the category FAMILY RESOURCES and access will be warned, blocked, or allowed depending on the individual's settings for that category.

Notifications

Notifications are email messages that alert administrators of an organization or group of possible inappropriate Internet usage.

To set up notification rules, follow the instructions below:

1. Click the **Notifications** link. The Notifications page for the currently logged in administrator will display.
2. Click the **Add New Notification** link.
3. Select to whom the notification will apply by clicking the radio button next to Organization (applies to all users in the organization), Group (applies to only users associated with the given group) or User (applies only to a specific user).
4. Select a condition(s) to be notified about.
5. Click the **Add** button.

Note: Each administrator can create multiple notifications. This allows the administrator to have specific conditions assigned for specific groups and/or users if desired.

Active **-** To deactivate a notification, follow the instructions below:

1. Deselect the box next to the notification to temporarily disable it.

2. To permanently remove the notification, click the **Delete** link in the same row, last column.

Is Blocked - If this box is checked, a notification will be sent if a covered user is blocked from a specific Web page.

Is Warned - If this box is checked, a notification will be sent if a covered user is warned about a specific Web page.

Overrides a Block - If this box is checked, a notification will be sent if a covered user overrides a blocked Web page.

Continues from a Warning - If this box is checked, a notification will be sent if a covered user continues from a warning message.

Administrators Overview

From the online management application, administrators can:

1. **View Internet activity reports** for the entire organization, group or user (if logging is enabled)
2. **Add and modify user and group profiles** (including Internet settings)
3. **Assign users to groups**
4. **Re-categorize URLs**
5. **Add Notification Rules** to notify them of possible inappropriate Internet use
6. **Give other users administrator privileges**

Adding a New Administrator

The first organization administrator is set up during the organization's account setup.

To create additional administrators, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click the **Add New Administrator** link. The *Administrator* page will display.
3. Select the user you want to give admin rights to from **The following USER:** drop down menu.
4. Put a check in the box to the left of each of the groups you want to give the user admin rights for.
5. Click the **Submit** button.

Note: If the administrator will manage all groups, it is only necessary to click on the organization's name at the top.

Deleting an Administrator

To delete an administrator, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click the **Delete** link located to the right of the administrator. A *Confirmation* screen will display
3. Click **OK** to confirm the deletion.

Note: You cannot delete the original administrator. Also, this will not delete the user from the system; it will only remove the administrator privileges.

Editing Administrator Privileges

To alter the administrator's privileges, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click on the administrator's name.
3. Make changes as desired.
4. Click the **Submit** button.

Reporting Overview

ContentProtect Pro Suite provides comprehensive Web-based reporting that is remotely accessible by any administrator in an organization. The coverage of reports an administrator can view depends upon the groups he or she manages (See Administrators section). Each chart has drill-down capability for transaction detail. Selecting the *Report Coverage, Date Range, Report Selection* (Chat or Web) and *Hourly Wage* will generate charts that report transaction detail.

Note: Logging must be enabled for any reporting to occur. You can enable logging at the user, group or organization level.

Access Reports

To access the reports, follow the instructions below:

1. Login to the Online Management application as an administrator.
2. Click the **Reporting** tab on the top navigation bar.

Report Coverage

Select the organization, group or user from the dropdown list to view reports of Internet activity. (Group administrators will not be able to select coverage for the entire organization. The group administrator will only be able to select coverage for the group(s) or users for which he or she is an administrator.

Date Range

Select a date range from the dropdown list to view Internet activity during that time frame. (If there is a very large amount of data being reported the longer the time period covered, the longer it will take the page to display the data.)

Report Selection - Select the type of reports you would like to view.

Hourly Wage - Some of the graphs use this dollar amount to determine the cost of time spent online. You may adjust this number to the average hourly wage for the organization, groups or specific users.

Note: Discrepancies between the available charts are caused by some Web pages assigned in multiple categories. As a result the charts show an approximation of Web activity and cost.

Customizing Report Defaults

You can customize the default report by clicking the **Customize Defaults** link above the graphs. You can set default options for:

- Report Coverage
- Date Range
- Report Selection
- Hourly Wage
- Time zone
- Graph style

Chat (IM) Reports

Time Spent Online, Chat Messages and *Chat Apps* refer to Instant Messaging applications ONLY, including AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger. *Chat Sites* refer to any Web page that is categorized as having Chat content.

Time Spent in Chat

This is a column chart that represents time spent in Chat within a specified date range.

To observe the **Time Spent in Chat** report graph, follow the instructions below:

1. Resting the mouse pointer over a column marker displays a numeric value of time spent and cost required within a specified date range.

2. Click on a column to drill-down to **Chat Report Detail** (see Chat Report Detail).

Chat Messages

This is a line chart that represents the number of messages sent within a specified date or time range.

To observe the *Chat Messages* report graph, follow the instructions below:

1. Resting the mouse pointer over an intersection between the line and graph displays the number of messages sent within a specified time or date range.
2. Click a specific portion of the line chart to drill-down to **Chat Report Detail** for that time or date.

Chat Apps

This is a pie chart that represents Chat (Instant Messaging, IM) applications used.

To observe the *Chat Apps* report graph, follow the instructions below:

1. Resting your mouse pointer over each pie wedge displays how many messages were sent using that specific Chat application during a specified date range.
2. Click on a pie wedge to drill-down to **Chat Report Detail** for that chat application (see Chat Report Detail).

Chat Sites

This is a bar chart that represents visited Chat-related Websites and the number of times that Chat site was accessed.

To observe the *Chat Sites* report graph, follow the instructions below:

1. Resting your mouse pointer over each bar displays the Chat-related Website visited and the number of times that Chat site was accessed.
2. Click on a bar to drill-down to **Chat Report Detail** for that chat site (see Chat Report Detail).

Chat Report Detail

This is a table that displays an individual user summary listing *Group, User,* the number of messages (*Count), Time Spent* and the average cost to your organization for that time (*Cost*).

To observe the *Chat Report Detail*, follow the instructions below:

1. Click a column heading to sort column data in ascending or descending order.
2. Click a **user name** to drill-down another level to the actual Chat transactions.

Time **-** Time is listed in ascending order and represents the time that the conversation took place.

Screen Name - This column displays the screen names of both the person sending and the person receiving Chat conversation. The user's screen name appears in red text.

Chat Conversation - This column displays the actual conversation text.

Navigation is made easy by following the instructions below:

1. Click any of the page links below the table to display *Next, Previous*, or a specific page of report results.
2. Click the navigation link **Graphs**, located above the table or the *Reporting* tab, to refresh Chat activity and return to reporting.
3. Click **Back** from the *browser's* toolbar to return to reporting. This will not refresh Chat activity.

Web Reports

Web-based reporting on each individual user, group or organization is remotely accessible. Each chart has drill-down capability for Web Report Detail. Selecting a user, date range, and access type (Web) will generate charts that report transaction detail.

Time Spent Online

This is a column chart that represents time spent online within a specified date range.

To observe the *Time Spent Online* report graph, follow the instructions below:

1. Rest the mouse pointer over a column marker to display a numeric value of time spent and cost required within a specified date range.
2. Click a column marker to drill-down to **Detail Report** (See Web Report Detail).

Web Usage

This is a line chart that represents the number of Web requests on an hourly or daily basis.

To observe the *Web Usage* report graph, follow the instructions below:

1. Rest the mouse pointer over an intersection of the line and graph of the line chart to display a numeric value of sites visited and cost associated with the given time frame.
2. Click on a specific portion of the line chart to generate and display **Detail Report** (See Web Report Detail).

Categories Logged

This is a pie chart that represents **ContentProtect Pro Suite** categories that have been browsed during a specified date range.

To observe the *Categories Logged* report graph, follow the instructions below:

1. Rest the mouse pointer over any portion of the pie chart to display a numeric value of Web pages visited in each category.
2. Click on a specific portion of the pie chart to generate and display **Detail Report** (See Web Report Detail).

Filter Actions

This is a bar chart that represents filter responses to Website requests showing if a specific transaction was blocked, warned, continued after warned, overridden, or logged.

To observe the *Filter Actions* report graph, follow the instructions below:

1. Rest the mouse pointer any of the bars to display a numeric value of sites visited and cost associated with each action.
2. Click on any bar in the chart to generate and display **Detail Report** for that action (See Web Report Detail).

Web Report Detail

This is a table that displays an individual user summary listing *Group*, *User*, the number of times the Web page was visited (*Count*), *Time Spent* and the average cost to your organization for that time (*Cost*).

To observe the *Web Report Detail* follow the instructions below:

1. Click a column heading to sort column data in ascending or descending order.
2. Click the **URL** to visit the site or click on the **# of visits** to see specific access times and categories for each URL.

URL - Lists the Universal Resource Locator (URL) or address of a specific Website accessed by a user. Click any URL within this column to open the specific site in a separate window for your review.

Warning: If you are accessing reports from a remote computer that does not have **ContentProtect Pro Suite** installed, all Websites will be fully displayed. Computers that have **ContentProtect Pro Suite** installed will not display blocked Websites unless the administrator uses the override option or allows that specific category.

User - Lists the user account that was used to access the URL. This is the last level of report transaction.

Time - Reports the date and time the Website was accessed. This is the last level of report transaction.

Filter Action - Reports the filter action that was applied. The filter action could be Allow, Warn, Warn Continue, Block Override or Block for each category. This is the last level of report transaction.

Category - Displays the category icon(s) associated with each URL. Resting your mouse pointer over a category icon will display what that category is. Click here for a list of categories and descriptions.

Navigation is made easy by following the instructions below:

1. Click any of the page links below the table to display *Next, Previous*, or a specific page of report results.
2. Click the navigation link **Graphs**, located above the table or the *Reporting* tab, to refresh Web activity and return to reporting.
3. Click **Back** from the *browser's* toolbar to return to reporting. This will not refresh Web activity.

Recategorizing from Second Level Reports

To recategorize from last level report, follow the instructions below:

1. Click **Recategorize** to change the assigned category of the Website (i.e. gambling.com).
2. Select a new category from the drop-down list.
3. Click **Recategorize** to apply the changes.

Note: This will not change the category of Web pages already visited. It will change the category for future visits to the Web page.

Glossary

Administrative Privileges - Assigning a user the same access as an administrator.

Administrator - The person who is responsible for setting up and maintaining a group of users. Duties of the administrator may include uninstalling **ContentProtect Pro Suite**, setting up and managing user profiles, assigning passwords and privileges, viewing reports, etc.

Application - Software, program, or tool used on your computer, such as a word processor, a game, or an email program.

Browser - The application that lets you navigate around and view pages on the Web. Netscape and Internet Explorer are the two most common.

Category - A general term for a whole topic or information type.

Chat – Real time communication. It is typed conversation that is received almost instantly as soon as it is sent. Talking live with one or more people via the Internet. It's like a party line, except you type instead of talk.

Client-Based Filtering - Filtering that is performed from an individual computer. Filtering software and a list of categorized sites are stored on an individual computer that makes filtering more flexible for the user making decisions about acceptable content. Aside from restricting Internet access to certain Websites, many client-based filters also offer controls for other Internet services.

Default Settings - A setting that a program is pre-set to select (usually the recommended settings) if you do not specify other options.

Drill Down - To move from a summary of information to more detailed data. To drill down through a series of reports addressing more detail at each level.

Filtering - Controlling access to a Web page request by analyzing the incoming and outgoing requests and letting them pass or halting them based on settings selected within **ContentProtect Pro Suite**.

Icon - A small picture that represents an object or program.

Instant Messaging (IM)- Instant Messaging is the ability to see if a chosen friend, co-worker, or associate is connected to the Internet and if they are, you are then able to exchange "real time" messages with them. **ContentProtect Pro Suite** currently can block and/or log IM activity from AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger.

Internet - The Internet consists of countless networks of computers that are connected together across the world allowing millions of people to share information. Components of the Internet include: the World Wide Web, Newsgroups, Chat rooms, and e-mail.

Log - A program or system that enters a record into a log file or report file.

Peer-to-Peer - Peer-to-Peer networks exist on the Internet and allow users to have access to other users' files residing on their hard disks. **ContentProtect Pro Suite** is capable of blocking Peer-to-Peer activity only on the Gnutella network.

Portable User Profiles - Allows a user to login on any machine that contains the filtering software and have his or her profile imported instantly.

Remote Management - The capability of accessing files, devices, and other resources not connected directly to your workstation. In the case of **ContentProtect Pro Suite**, reviewing report results and managing user profiles can be performed from any machine with Internet access.

Screen Name - An identifier that consists of a sequence of one or more alpha or numeric characters that uniquely identifies a person.

Server-Based Categorization and Validation - A server that maintains a list of categorized URLs (Universal Resource Locator). The server is updated regularly to ensure that all users are getting the most up to date accurate information. The server does not actually deliver the requested Web page (URL) to the customer but compares the requested URL to the list.

Shortcut Menu - A popup menu that appears by right-clicking an object. When right-clicking the **ContentProtect Pro Suite** icon from the System Tray located in the Taskbar, the shortcut menu is displayed.

System Tray - Located on the Windows Taskbar (usually at the bottom next to the clock) contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more.

Taskbar - A system bar located at the bottom of your screen. The Taskbar is home base for the Start button, system clock, system tray, etc.

Transaction detail - Activity information based on report results.

URL - Universal Resource Locator. An address on the Internet, the URL shows the specific path that locates a site or a document online. The URL for a Web page looks like this:

http://www.domainname/folder name/filename

User - An individual who uses a computer.

User ID - An identifier that identifies a specific user in a program.

User Profile - Program settings that are specific to an individual user.

WWW - World Wide Web - The Web is the visual component of the Internet. Created with HTML language, Web pages can include text, pictures, sound clips, video, links for downloading software, and much more. The Web is only one component of the Internet, although the terms are often (and mistakenly) interchanged.

Web-Based Reporting - Reports that have compiled Web and Chat activity for a **ContentProtect Pro Suite** organization and are accessible from any computer with Internet access.

Frequently Asked Questions

How do I create a new user?
See Create New Users.

What is recategorization?
Just as **ContentProtect Pro Suite** examines each Web page request for category content to determine which category a site belongs to, the administrator(s) can recategorize any URL to force a specific Web site to be categorized as he/she chooses. Associated Filter Settings (Allow, Warn, or Block) for that category are then applied. For more info see URLs (Recategorization).

I made changes online to the Internet settings. Why isn't it working?
There is a wait period of up to an hour for changes made through the online management application to automatically take effect. To force changes made to take effect immediately, use the Admin Utility application. Or, if the Client UI is available for individual users, click **Refresh Profile** from the menu.

Why can't I see the report graphs?
Macromedia Flash free browser plugin is required to view the graphs. If you don't have this installed, you may get it by going to:
http://www.macromedia.com/shockwave/download/download.cgi
?P1_Prod_Version=ShockwaveFlash

How does ContentWatch define the categories?
See Category Descriptions.

Why don't I see reports on a specific user or group?
Make sure you have privileges to view reports or modify profiles for that group or user. Also verify that logging is enabled. For more information see Administrators.

Why don't I see reports of all Chat activity?
ContentProtect Pro Suite currently is capable of blocking and/or logging IM activity from AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger.

EmailProtect Welcome

Congratulations! You now have the most easily adaptable email filtering software application available today. EmailProtect comes pre-set to protect you from objectionable and inappropriate content. However, we realize that not all users are alike. Each has unique values and needs, which is why we have developed EmailProtect to be flexible enough to work for you. Several help resources have been produced to specifically provide easy-to-follow instructions for using EmailProtect. ContentWatch wants you to feel confident and fully satisfied in using this program. Your choice to help reduce risk and increase privacy for your family is an important one.

Sources of help

- The EmailProtect User Guide (PDF format) -- available from the Help menu within EmailProtect:
- Step-by-step instruction
- A category list with descriptions
- Glossary
- Comprehensive, always current, detailed help with step-by-step instruction -- available from the Help menu within EmailProtect and available from our Product Documentation site.
- You can receive prompt and courteous Customer Support by calling 1-800-485-4008 for questions and technical assistance. Customer Support is available Monday through Friday -- 8 a.m. to 5 p.m. Mountain Standard Time.
- You can also email any time to info@contentwatch.com.

Key Features

- Provides pre-set protection against pornography
- Dozens of filtering categories available
- Protects multiple email accounts automatically
- Supports POP email software
- Sends unwanted email to Quarantine instead of your Inbox
- Creates unlimited custom filters
- Downloads filter updates automatically
- Easily adds your friends to a Safe List
- No complicated account names or server names to type
- Saves settings for convenient backups for use at work and home

System Requirements

- PC with Pentium or compatible 133 MHz or faster processor
- Microsoft Windows 98SE/Me/2000/XP
- 64 MB RAM
- 100 MB hard drive space
- Color monitor with a minimum 800x600 resolution
- Internet connection
- Internet Explorer 5.0 or greater, Netscape 6.0 or greater

Installation from a CD

1. Insert the CD into the CD ROM drive (If the CD does not automatically run, go to Start>Run type in "d:Autostart.exe" Replace the D with the letter for your CD-ROM drive.)
2. From the Menu, select Install Software; this will open the Setup Wizard.
3. Click **Next** to start the Setup Wizard.
4. Click **Next** on the Welcome screen.
5. Choose to accept the license. Click **Next**.
6. Choose the Install directory. Click **Next**.
7. Select the products to install. (You must install ContentProtect Professional.) Click **Next**.
8. Enter the Organization Account Name and the Install Password. Your administrator should have provided these; contact your administrator if you do not have the account name and password. Click **Next**.
9. Enter all of your user information. The Email field is not required, but it is recommended. Click **Next**.
10. Verify your settings and then click **Install** on the confirmation dialog.
11. Click **Finish** to restart the computer and complete the installation.
12. When the machine restarts, run the Online Updates. You can launch this from any of the products or by selecting it from the right-click menus of the taskbar icons located at the bottom of the screen next to the clock.
13. When the update dialog displays, click **Check For Updates**.
14. If the default settings have not been changed, the new updates will download and install automatically. If the default settings have been modified, follow the prompts to download and install updates. When the process is complete, select the "Click here to restart your computer now" link.

Your system should now be fully updated with the newest version of **ContentProtect Pro Suite**.

How to Open, Close, Disable, Enable, and Exit

EmailProtect starts up with Windows by default. This provides email protection all the time, in the background, regardless of the email client (program) you use. Because EmailProtect works silently, the only indication that it is running is the active EmailProtect icon from the system tray. The system tray is located at the bottom-right of your screen next to your system clock.

Opening EmailProtect

There are three options for opening EmailProtect.

Opening Option 1

1. Right-click EmailProtect from the system tray and select **Open Quarantine** from the menu.

Note: When EmailProtect opens, a list of email items will appear in a window called Quarantine. This is a list of email items that have been blocked from your Inbox due to a filter. Clicking each column header will sort email in ascending or descending order with each click. All EmailProtect features are available from the toolbar or menu bar.

Opening Option 2

5. Double-click EmailProtect from the system tray.

Opening Option 3

5. Click **Open Quarantine** from the floating toolbar.

Note: To display the floating toolbar, right-click EmailProtect from the system tray and select **Show Floating Toolbar**.

Closing EmailProtect

There are two options for closing EmailProtect.

Closing Option 1

1. Click the **x** at the upper right-hand corner of the window. This will close the window but continue to run program protection.

Note: When the EmailProtect window is closed, protection is still running in the background. There may be times when you will want to temporarily disable EmailProtect or stop it from running completely.

Closing Option 2

1. Select **File > Close** from the menu bar. This will close the window but continue to run program protection.

Disabling EmailProtect

1. Right-click EmailProtect from the system tray.
2. Select **Disable EmailProtect** from the menu.

Enabling EmailProtect

1. Right-click EmailProtect from the system tray.
2. Select **Enable EmailProtect** from the menu.

Exiting EmailProtect

There are two options for exiting EmailProtect.

Exiting Option 1

EmailProtect will no longer be accessible from the system tray but will still run full filtering protection.

1. Right-click EmailProtect from the system tray.
2. Select **Exit** from the menu.

Exiting Option 2

1. If the EmailProtect window is open and displayed on your screen, select **File > Exit** from the menu bar.

Disabling and Exiting EmailProtect

To completely disable EmailProtect and remove accessibility from the system tray, you must follow the steps below in the given order.

1. Right-click EmailProtect from the system tray.
2. Select **Disable EmailProtect** from the menu.
3. Right-click EmailProtect from the system tray.
4. Select **Exit** from the menu.

Important: Protection will no longer be provided. Disabling and Exiting EmailProtect will completely stop program protection and remove the EmailProtect icon from the system tray. You will have to select Start > Programs > EmailProtect > EmailProtect to start program protection and display the EmailProtect icon in the system tray.

The EmailProtect Window

Title Bar -- Where the application name resides.

Minimize, Maximize/Restore, and Close -- Clicking Minimize closes the EmailProtect window. Clicking Maximize sizes the window to full screen, clicking Restore (the maximize button changed to two small squares) returns the window to the previous size, and Close will close the program window but keep EmailProtect running protection in the background.

Menu Bar -- The menu bar contains menus (File, Edit, Actions, View, and Help) with different options and actions.

Toolbar -- Action buttons that perform a specific action or will display a window with options or settings.

Banner -- Contains the window name and the option to Show Email Images.

Quarantine List -- Quarantine is a list of email items that have been blocked as a result of filtering.
Status Bar -- Displays program information, such as the number of items in the Quarantine list.

Quarantine Overview

Quarantine is a list of email items that have been blocked as a result of filtering. These items are not deleted automatically to prevent losing email items that may be wanted, but were blocked by a filter rule. You will always have the ability to evaluate an email. Please check your quarantine frequently to review email that may be wanted or added to the safe list or moved to your Inbox.

Viewing Quarantined Email

One of the most unpleasant experiences of some email is the display of objectionable images. EmailProtect allows you to view HTML-type email safely, without the images. To view these images, simply check Show Email Images from the Quarantine window.

To view quarantined email, use the following steps:

1. Double-click EmailProtect from the system tray to open Quarantine if necessary.

Choose one of the following options for viewing:

- Double-click the email you want to view.
- Select an email item and choose Actions > View Email from the menu bar.
- Right-click the email item to view and select View Email from the shortcut menu.

Note: You can now inspect any viewed email item to Delete, Add to Block List, Add to Safe List, add new filter rules, or send email items to your Inbox.

Viewing Quarantined Email Images

There may be times when you need to view images within a Quarantined email. This can be done from the Quarantine window or from an open Quarantined email. Follow the steps below:

Viewing Quarantined Email Images Option 1

1. Double-click EmailProtect from the system tray.
2. Check the box Show Email Images.
3. Double-click the email message to review email content and images.

Viewing Quarantined Email Images Option 2

1. Double-click **EmailProtect** from the system tray.
2. Double-click the email message to review from the Quarantine list.
3. Check the box **Show Email Images**.

Note: To no longer view email images, uncheck **Show Email Images** while an email message is open or from the Quarantine window.

Viewing Quarantined Email Images Option 3

1. Double-click EmailProtect from the system tray.
2. Click **Preferences** from the toolbar.
3. Check **Show email images**.
4. Click **OK** to always view email images.

Note: To no longer view email images, uncheck Show email images from the Preferences window.

Deleting Quarantined Email

One advantage of EmailProtect is the ability to delete Quarantined email manually or automatically. Autodelete is a Preference setting.

Manual delete

1. Double-click **EmailProtect** from the system tray.
2. Select the email message to delete.
3. Click **Delete** from the toolbar or press Delete on your keyboard. You can also select **Actions > Delete Email** from the menu bar.

Note: You can select all email items to be deleted by selecting Edit > Select All from the menu bar, or select and deselect individual email items by pressing Ctrl and selecting each email as needed. You can also select a group by selecting the first email in a group and while pressing Shift, select the last email in a group, then click **Delete**.

Autodelete

1. Double-click EmailProtect from the system tray.
2. Click **Preferences** from the toolbar or select **Tools > Preferences** from the menu bar.
3. Observe the Preferences window. The default for Autodelete is to automatically delete Quarantined email after 31 days. You can change the number of days by selecting and typing the number of days you want to allow or by using the arrows to increase or decrease the number of days for email to stay in Quarantine. The highest number of days allowed is 31. All Quarantined email will be deleted automatically in the number of days specified from the date it was received. It is not recommended to set Autodelete to zero, as this will continually delete all quarantined email.
4. Click **OK** to save changes and close the window.

Note: Clicking Apply will save changes but keep the window open. Clicking Cancel will close the window, but will not save changes.

Block List Overview

This feature is very valuable to a new user. The two tabs from this window enable you to add an address, word, or phrase to the Block List. The Block List has filter rules that are applied to increase your protection. There is not a limit on the number of rules you are allowed to create. Items on your Safe List always override items on your Block List. The two tabs within the Add to Block List window are Addresses and Words. Let's review each tab.

Reviewing the Addresses Tab

The first portion of the Addresses tab, located at the top of the window, is a recent list of email that has made it past EmailProtect to your Inbox. If you select one or more email items from this list, you can create a new rule for multiple items at once. No typing is necessary.

Important: If someone wants to block an email address, but they do not have any email from that address, they can type the address under the Words tab. For example: to block sam@mysite.com, go to the word section, check Sender Name, Contains from the drop-down list, and then type the address (sam@mysite.com) in the text box provided. The same is true when typing addresses under the Addresses tab. If you don't have anything selected in Quarantine and click **Add to Block List**, select the Addresses tab and type the address in manually.

Filter Levels

Address -- Blocking an email address is done on an individual account level, such as sam@mysite.com is the most common type of address.

Domain -- Blocking an email domain is done on a site level, which will block many more addresses. For example: The bold part of (sam@mysite.com) is showing the domain of the address. All addresses from mysite.com would be blocked. This is useful if a particular site sends email repeatedly where the address account name keeps changing. For example: If the email addresses were offer37@mysite.com or offer415@mysite.com, both would be blocked.

Server -- Clicking Advanced will allow you to block an email server on a web server level. This is even broader. A web server, usually described by its IP address (10.5.10.2), can easily hold dozens of websites. Because some of those sites may be places you do want email from, this option should only be used with great care. This level of filtering is most helpful when blocking pornography, because web hosts tend to place adult sites on different servers than non-adult sites.

Reviewing the Words Tab

This tab allows any words or phrases to be entered as a rule to divert email to Quarantine. By checking an item such as Subject, Body and Attachments, Sender Name, or All, and typing in specific text, EmailProtect will look for those specific conditions and if those conditions are found, the email is sent to Quarantine. The text box has a 256-character limit for each rule. There is no restriction on the number of rules created. Conditions available from the drop-down list are:

Contains -- If the Subject, Body and Attachments, Sender Name, or All of an email contains the text you have typed in. Contains is the default setting.

Starts With -- If the Subject, Body and Attachments, Sender Name, or All of an email start with the text you have typed in.

Ends With -- If the Subject, Body and Attachments, Sender Name, or All of an email end with the text you have typed in.

Equals -- If the Subject, Body and Attachments, Sender Name, or All of an email are equal to the text you have typed in.

Adding to the Block List from Quarantine

1. Double-click **EmailProtect** from the system tray.
2. Select an email entry from the Quarantine list.
3. Click **Add to Block List** from the toolbar.
4. Select either the tab for Addresses or Words.
5. Check and enter options as needed under the appropriate tabs. Under the Addresses tab, Address is checked by default. **Note:** You can click Help for web assistance within each tab to find help on which option to choose and why, or refer to the Overview above. You can check and select options under both tabs to apply rules as needed.
6. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but keep the window open. Clicking Cancel will close the window, but will not save changes.

Adding to the Block List on the Fly

1. Double-click **EmailProtect** from the system tray.
2. Click **Add to Block List** from the toolbar, or click **Add to Block List** from the floating toolbar. **Note:** There is no need to have EmailProtect open when you are using the floating toolbar.
3. Check and enter options as needed under the Addresses and/or Words tabs. For your convenience, the selected address is displayed so there is no need for typing. Under the Addresses tab, select Address. **Note:** Refer to the Overview above to help you decide which option is best and why. You can check and select options under both tabs to apply rules for both as needed.
4. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes.

Adding to the Safe List

This works exactly the same as Adding to Block List, except EmailProtect NEVER blocks email items on your Safe List. For example: You may always want to receive email items from your boss or your friends. There is not a limit on the number of rules you are allowed to create. If an email has both a safe rule AND a block rule applied, the Safe rule wins.

Filtering Levels

Important: If someone wants to block an email address, but they do not have any email from that address, they can type the address under the Words tab. For example: to block sam@mysite.com, go to the word section, check Sender Name, Contains from the drop-down list, and then type the address (sam@mysite.com) in the text box provided. The same is true when typing addresses under the Addresses tab. If you don't have anything selected in Quarantine and Add to Block List, select the Addresses tab and enter the address manually.

Address -- Allowing an email address is done on an individual account level, such as sam@mysite.com is the most common type of address.
Domain -- Allowing an email domain is done on a site level, which will allow many more addresses. For example: The bold part of (sam@mysite.com) is showing the domain of the address. All addresses from mysite.com would be allowed. This is useful if a particular site sends email repeatedly where the address account name keeps changing. For example: If the email addresses were offer37@mysite.com or offer415@mysite.com, both would be allowed.

Server -- Clicking Advanced will allow you to allow an email server on a web server level. This is even broader. A web server, usually described by its IP address (10.5.10.2), can easily hold dozens of websites. Because some of those sites may be places you do want email from, this option should only be used with great care. This level of filtering could allow more than is actually wanted. Web hosts tend to place adult sites on different servers than non-adult sites.

Adding to the Safe List from Quarantine

1. Double-click EmailProtect from the system tray.
2. Select an email item from the Quarantine list.
3. Click **Add to Safe List** from the toolbar.
4. Check and enter options as needed under the Addresses and/or Words tabs. **Note:** You can click **Help** for web assistance within each tab to find help on which option to choose and why, or refer to the Overview above. You can check and select options under both tabs to apply rules as needed.
5. Click **OK** to save changes and close the window.

Note: Clicking Apply will save changes but will keep the window open. Clicking Cancel will close the window, but will not save changes.

Adding to the Safe List on the Fly

1. Double-click EmailProtect from the system tray.
2. Click Add to Safe List from the toolbar, or click **Add to Safe List** from the floating toolbar. **Note:** There is no need to have EmailProtect open when you are using the floating toolbar.
3. Select the email item to allow from the list under Unblocked Address List.
4. Check and enter options as needed under the Addresses and/or Words tabs. **Note:** You can click Help for web assistance within each tab to find help on which option to choose and why, or refer to the Overview above. You can check and select options under both tabs to apply rules as needed.
5. Click **OK** to save changes and close the window.

Note: Clicking Apply will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes.

Sending to the Inbox

There may be a time that an email will be filtered and sent to Quarantine, but you want to keep it anyway. You can send this email to its original destination (your Inbox), without having to change filter rules. Be sure to review your Quarantine list from time to time for email items you may possibly want to keep.

1. Double-click **EmailProtect** from the system tray.
2. Select an email item from the Quarantine list.
3. Click **Send** to Inbox from the toolbar to move the email item from Quarantine to your Inbox.

Note: If you send a Quarantined email to the Inbox, it will appear in the Recent Email list if you choose to Add to Block List or Add to Safe List.

The Floating Toolbar

By default, the Floating Toolbar is not displayed. The buttons on this toolbar look and function just the same as the buttons do in the EmailProtect window. You can turn the toolbar on and off by right-clicking EmailProtect from the system tray and selecting **Show Floating Toolbar**. The shortcut menu from the system tray contains many of the menu commands from the Quarantine window.

Toolbar buttons are described below from left to right:

Add to Block List -- On the fly access to the Block List, no need to have EmailProtect open. Simply click **Add to Block List** from the EmailProtect toolbar, select the email item, the desired address and word rules, and click **OK**.

Add to Safe List -- On the fly access to the Safe List, no need to have EmailProtect open. Simply click **Add to Safe List** from the EmailProtect toolbar, select the email item, the desired address and word rules, and click **OK**.

My Filter Settings -- On the fly access to categories of content to be filtered. As you come across different types of content in your email, you can change the filter settings as needed.

Open Quarantine -- Opens EmailProtect directly to the Quarantine list.

EmailProtect -- This toolbar button is a direct link to the ContentWatch website for easy access to other protection products and other valuable information about protecting you and your family.

Close -- Clicking the **x** in the upper right-hand corner of the toolbar will close it. To view the toolbar again, right click EmailProtect from the system tray and select **Show Floating Toolbar**.

Changing Default Filter Settings

This is a list of pre-defined filters based on a number of categories representing email content. By default, Adult/Mature, Financial/Stocks, and Pornography categories are checked to be filtered by EmailProtect.

To filter and therefore block a category, simply check it. To allow a category, uncheck it. These categories will automatically update themselves through your Internet connection. Click here for a complete list of categories and definitions.

1. Double-click EmailProtect from the system tray.
2. Click **My Filter Settings** from the Quarantine toolbar, or simply click **My Filter Settings** from the floating toolbar.
3. The Default Filters tab will be displayed.
4. Check all categories of content you would like filtered and therefore blocked. You can return to Default Filters to change which categories are filtered or unfiltered. Simply check or uncheck categories as needed. Remember, Adult/Mature, Financial/Stocks, and Pornography are checked by default.
5. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Clicking **Restore Defaults** will return categories filtered to Adult/Mature, Financial/Stocks, and Pornography. No other settings or lists will be affected such as My Blocked or My Safe Addresses and Words.

My Blocked Addresses

Each time you add an Address rule in the Add to Block List feature, that rule is added to a list in My Blocked Addresses. There is no limit to the number of rules that can be added so it is possible for this list to get quite large. Any rule you create can be temporarily disabled by deselecting it. You can also Add, Edit, or Delete address rules from this tab. Addresses in My Safe Addresses will always override items in My Blocked Addresses.

1. Double-click EmailProtect from the system tray.
2. Click **My Filter Settings** from the Quarantine toolbar, or simply click **My Filter Settings** from the floating toolbar.
3. Select the **My Blocked Addresses** tab.
4. Deselect the check boxes next to each address you want to disable or click **Uncheck All** from the toolbar to disable them all at once. You can activate the rules again by checking the boxes or clicking **Check All** from the toolbar.
5. You can choose from other options on the toolbar such as:
    - **Add Address** -- Clicking **Add Address** from the toolbar will display the Add to Block List window and Addresses tab. Just select the email item and select **Address** or **Domain**. Continue to Step 6.
    - **Edit Address** -- Clicking **Edit Address** from the toolbar will allow you to edit an address directly from this list. Continue to Step 6.
    - **Delete Address** -- Clicking **Delete Address** from the toolbar will delete the selected address and rule from the list. Deleting is permanent and cannot be undone. Continue to Step 6.
6. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Restore Defaults is grayed out and is not available for this window.

My Blocked Words

Each time you add a Word rule in the Add to Block List feature, that rule is added to a list in My Blocked Words. There is no limit to the number of rules that can be added so it is possible for this list to get quite large. Any rule you create can be temporarily disabled by deselecting it. You can also Add, Edit, or Delete word rules from this tab. Words in My Safe Words will always override words in My Blocked Words.

1. Double-click EmailProtect from the system tray.
2. Click **My Filter Settings** from the Quarantine toolbar, or simply click **My Filter Settings** from the floating toolbar.
3. Select the **My Blocked Words** tab.
4. Uncheck the check boxes next to each word you want to disable or click **Uncheck All** from the toolbar to disable them all at once. You can activate the rules again by checking the boxes or clicking **Check All** from the toolbar.
5. You can choose other options from the toolbar such as:
    - **Add Words** -- Clicking **Add Words** from the toolbar will display the Add to Block List window and Words tab, just check the desired options and type the address or words in the text box provided. Continue to Step 6.
    - **Edit Words** -- Clicking **Edit Words** from the toolbar will allow you to edit an address or word directly from this list. Continue to Step 6.
    - **Delete Words** -- Clicking **Delete Words** from the toolbar will delete the selected item and rule from the list. Deleting is permanent and cannot be undone. You will have to create the rule again. Continue to Step 6.
7. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Restore Defaults is grayed out and is not available for this window.

My Safe Addresses

Each time you add an Address rule in the Add to Safe List feature, that rule is added to a list in My Safe Addresses. There is no limit to the number of rules that can be added so it is possible for this list to get quite large. Any rule you create can be temporarily disabled by deselecting it. You can also Add, Edit, or Delete address rules from this tab. Addresses in My Safe Addresses will always override addresses in My Blocked Addresses.

1. Double-click EmailProtect from the system tray.
2. Click **My Filter Settings** from the Quarantine toolbar, or simply click **My Filter Settings** from the floating toolbar.
3. Select the **My Safe Addresses** tab.

4. Uncheck the check boxes next to each address you want to disable or click **Uncheck All** from the toolbar to disable them all at once. You can activate the rules again by checking the boxes or clicking **Check All** from the toolbar.
5. You can choose from other options on the toolbar such as:
    - **Add Address** -- Clicking **Add Address** from the toolbar will display the Add to Safe List window and Addresses tab. Just select the email item and select **Address** or **Domain**. Continue to Step 6.
    - **Edit Address** -- Clicking Edit Address from the toolbar will allow you to edit an address directly from this list. Continue to Step 6.
    - **Delete Address** -- Clicking **Delete Address** from the toolbar will delete the selected address and rule from the list. Deleting is permanent and cannot be undone. Continue to Step 6.
6. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Restore Defaults is grayed out and is not available for this window.

My Safe Words

Each time you add a Word rule in the Add to Safe List feature, that rule is added to a list in My Safe Words. There is no limit to the number of rules that can be added so it is possible for this list to get quite large. To temporarily disable any rule you create, simply deselect it. You can also Add, Edit, or Delete address rules from this tab. Words in My Safe Words will always override words in My Blocked Words.

1. Double-click EmailProtect from the system tray.
2. Click **My Filter Settings** from the Quarantine toolbar, or simply click **My Filter Settings** from the Floating toolbar.
3. Select the **My Safe Words** tab.
4. Uncheck the check boxes next to each word you want to disable or click Uncheck All from the toolbar to disable them all at once. You can activate the rules again by checking the boxes or clicking Check All from the toolbar.
5. You can choose other options from the toolbar such as:
    - **Add Words** -- Clicking Add Words from the toolbar will display the Add to Safe List window and Words tab. Just check the desired options and type the address or words in the text box provided. Continue to Step 6.
    - **Edit Words** -- Clicking Edit Words from the toolbar will allow you to edit an address or word directly from this list. Continue to Step 6.
    - **Delete Words** -- Clicking Delete Words from the toolbar will delete the selected item and rule from the list. Deleting is permanent and cannot be undone. You will have to create the rule again. Continue to Step 6.
6. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Restore Defaults is grayed out and is not available for this window.

Preference Features

Preference features can be changed by the click of a button. Checking and deselecting the options shown below will customize EmailProtect for you and your family. Each option is defined below.

Features

Show email images -- There may be a need to review possible images within an email in Quarantine. Checking Show email images will set all email items in Quarantine to display images when opened. The default is not to Show email images.

Run this program when Windows starts -- Each time you start your computer, EmailProtect will launch automatically for you for worry-free protection.

Show notification of new email in Quarantine -- A small notification will pop up at the bottom right-hand corner of your screen for a few seconds when new email has been added to Quarantine.

Show Splash at program start -- A program image that flashes when your computer first starts up to remind you that EmailProtect is enabled and running.

Autodelete

Automatically delete email 31 days after receipt -- The default setting for Autodelete is 31 days, which means that each time an email turns 31 days old, it is deleted from Quarantine. You can turn this option on and off just by deselecting and checking the check box next to Automatically delete email after. It is not recommended to set this option to zero days, Quarantined email would then be continually deleted without the option of review or creating rules.

Show notification before automatically deleting email -- A prompt will be displayed asking if you would like to delete email from Quarantine. Clicking **Yes** will complete this action.

Delete email from the Recent Email list after applying a rule -- When a rule is made from this list, the email entry is automatically deleted from the list, as most email generally creates just one new rule. If you expect to create more than one rule based on the same email, this option should be disabled. Instead, a red icon will appear to the left of the email entry, indicating that a Block Rule was made on the email. A green icon will indicate a Safe Rule was made from the email. The icon is based on the last rule made.

Password Protection

Password Required -- Requires a password when accessing Quarantine or Preferences. A password would also be required in order to disable EmailProtect. Passwords are case sensitive, with a maximum of 40 alphanumeric characters.

Accessing and changing Preference features:

1. Double-click EmailProtect from the system tray.
2. Click **Preferences** from the Quarantine toolbar.
3. Check or uncheck **Preference Features** accordingly.
4. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Clicking **Restore Defaults** will return preferences to the checked features you see in the above Preferences window diagram.

Autodelete

Autodelete is a revolving feature. For example, the default setting for Autodelete is 31 days, which means that each time an email turns 31 days old, it is deleted from Quarantine. You can turn this option on and off just by deselecting and checking the check box next to Automatically delete email after. It is not recommended to set this option to zero days, Quarantined email would then be continually deleted without the option of review or creating rules.

1. Double-click EmailProtect from the system tray.
2. Click **Preferences** from the toolbar or select **Tools > Preferences** from the menu bar.
3. Observe the Autodelete section of the Preferences window.
4. The default setting for Autodelete is set to 31 days. You can change the number of days as shown in the diagram above by selecting and typing the number of days you want email to stay in Quarantine. All Quarantined email will be deleted automatically after the number of days specified from the date it was received. The maximum number of days allowed for Autodelete is 31 days.

5. You have the option to automatically delete the email entry in the Recent Email list once you create a rule on it. Not selecting this option will leave the email entry in the list, with a corresponding icon.
6. Click **OK** to save changes and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Clicking **Restore Defaults** will return preferences to the original checked features in the Preferences window.

Password Protection

Passwords are used to restrict access to EmailProtect settings. However, all users can add to the Block List or the Safe List, without requiring a password. If a password is entered once, EmailProtect will not request it again unless you log off, shut down, or reboot your computer. Passwords are case-sensitive and have a 40-alphanumeric character limit. The default for EmailProtect is not to require a password. Requiring a password will also prevent others from disabling EmailProtect.

For password protection, follow the steps below:

1. Double-click EmailProtect from your system tray.
2. Click **Preferences** from the Quarantine toolbar.
3. Observe the Password section of the Preferences window.
4. Check **Password Required**.
5. Observe the Change Password window.
6. Enter a password in the text box under Enter new password:
7. Press tab and type the same password in the text box under Re-enter new password:
8. Click **OK** to save the password and close the window.

To change a password, follow the instructions below:

1. Double-click EmailProtect from your system tray.
2. Click **Preferences** from the Quarantine toolbar.
3. Click **Change Password**.
4. Observe the Change Password window.
5. Enter a password in the text box under Enter new password:
6. Press tab and type the same password in the text box under Re-enter new password:
7. Click **OK** to save the password and close the window.

Note: Clicking **Apply** will save changes but will keep the window open. Clicking **Cancel** will close the window, but will not save changes. Clicking **Restore Defaults** will return preferences to the original checked features in the Preferences window.

Saving and Importing Settings

There are several features involving saving and importing settings.

Saving EmailProtect Settings

It is possible to save EmailProtect settings as an external file. This allows you to make a backup of EmailProtect settings just in case your computer breaks down or for some other reason. Typically, these files will easily fit onto a floppy disc. EmailProtect setting files can be emailed, shared, or transferred if you buy a new computer. You can save settings anywhere on your hard drive, zip drive, etc. and even update them for use at work and home.

To save EmailProtect settings for backup, follow the instructions below:

1. Double-click **EmailProtect** from the system tray to open Quarantine.
2. Insert a 3-1/2 Floppy disk into drive (A:).
3. Select **File > Save Settings** from the menu bar.
4. Navigate to (A:). The file name is EPSettings. No need to change it. The file type is Filter Setting File. No need to change it.
5. Click **Save** or press **Enter**. Your EmailProtect settings are now saved on disc for backup.

Note: You can even email a copy of your EmailProtect settings to yourself or to another email address for safekeeping.

Importing EmailProtect Settings

Importing EmailProtect settings from backup:

1. Double-click **EmailProtect** from the system tray to open Quarantine.
2. Make sure the backup floppy disc containing your EmailProtect settings is inserted into (A:).
3. Select **File > Import Settings** from the menu bar.
4. Navigate to (A:).
5. Double-click **EPSettings.dat.**
6. Select to **Append** or **Replace** your current settings
7. The file will be copied to the common directory for EmailProtect.

Note: Append allows you to add new rules to your existing ones, and does not change your Preferences. Replace will overwrite all your rules and Preferences.

Exporting Address Books

First, you have to export your address book from the email program you are currently using in order to Import your address book into EmailProtect. EmailProtect has included some of the more familiar programs with step-by-step instructions below. Locate the email program you are currently using and follow the Export instructions. After exporting your email address book successfully, you will be ready to Import.

Exporting using Eudora 5.1

1. Open Eudora and select **Tools > Address Book** from the menu bar.
2. Select **File > Save As** from the menu bar.
3. Select the location and directory you would like to save the file to.
4. Enter a file name such as My Address Book.
5. Select **CSV Files (*.csv)** as the file type.
6. Click **Save**. You are now ready to Import.

Exporting using Netscape

1. Open Netscape and select **Window > Address Book** from the menu bar.
2. Select the Address Book you want to export.
3. Select **Tools > Export** from the menu bar.
4. Select the location and directory you would like to save the file to.
5. Enter a file name such as My Address Book.csv. Be sure to include the .csv file extension.
6. Select **CSV Files (*.csv)** as the file type.
7. Click **Save**. You are now ready to Import.

Exporting using Outlook 2002

1. Open Outlook 2002 and select **File > Import and Export** from the menu bar.
2. From the Import and Export Wizard, select **Export to a file**, and click **Next**.
3. Under Create a file of type: select **Comma Separated Values (DOS)**, and click **Next**.
4. Under Select folder to export from: select **Contacts**, and click **Next**.
5. Select the location and directory you would like to save the file to.
6. Enter a file name such as My Address Book and click **Next**.
7. Click **Finish**. You are now ready to Import.

Exporting using Outlook Express 6

1. Open Outlook Express and select **Tools > Address Book** from the menu bar.
2. Observe the Address Book window. Select **File > Export > Other Address Book** from the menu bar.
3. Observe the Address Book Export Tool window. Select **Text File** (Comma Separated Values) and click **Export**.
4. Select the location and directory you would like to save the file to.
5. Enter a file name such as My Address Book and click **Next**.
6. From the Select the fields you wish to export window, check the items you would like exported. Name and Email Address are the minimum recommended.
7. Click **Finish**. You are now ready to Import.

Exporting using Pegasus 4-02

1. Select **Addresses > Address books**.
2. Select the address book you want to export from the Address books and distribution list.
3. Leave this window open.
4. Select **Addressbook > Export** to tab-delimited file from the menu bar.
5. Select all addresses to import (select the first address in your list and then while pressing the Shift key, select the last address in your list).
6. Browse to the location you would like to save your address book file from Export to which file?
7. Type a file name such as My Address Book.tab (make sure to add a .tab file extension). Without the .tab extension, the import cannot be read.
8. Click **Save**. You are now ready to Import.

Importing Address Books

First, you have to Export your address book from the email program you are currently using in order to Import your address book into EmailProtect. If you have not Exported your address book, please do so now. Click here for step-by-step instructions on Exporting. You are now ready to Import.

Importing

1. Double-click EmailProtect from the system tray to open Quarantine.
2. Select **File > Import Address Book** from the menu bar.
3. Locate and double-click the **CSV Files (*.csv)** file you created when Exporting your Address Book.
4. You will receive a prompt that Importing has been completed successfully. Your Address Book addresses have been saved in My Filter Settings under My Safe Addresses.
5. Click **Close**.

Checking your Import

1. Right-click EmailProtect from the system tray and select My Filter Settings.
2. Select the **My Safe Addresses** tab.
3. Scroll to observe your Address Book addresses saved to the list.

EmailProtect and Your Email Client Compatibility

EmailProtect is automatically compatible with any POP-based email software. Features, such as the floating toolbar, have been designed to be independent of your email software. Although integration is often desired, it can be at the cost of instability and incompatibility with various versions of software. EmailProtect is widely compatible with most popular email software. In most cases, EmailProtect should still continue its protection normally, even if your email software is upgraded.

Setting up a POP account

- Webmail Clients -- POP accounts can be created in some Webmail Clients such as: Yahoo!. Please refer to the Yahoo website and perform a search on Setting up a Yahoo email account.
- Email Clients -- POP accounts can be created in some Email Clients
- Earthlink
- Eudora
- Netscape
- Outlook
- Outlook Express
- Pegasus

What to expect

All EmailProtect commands are available by right-clicking EmailProtect from the system tray. The first time you receive an email that is diverted to Quarantine, you will see two things:

1. A Popup Alert Notification (optional)
2. An email with an alert and reason for Quarantine

While many users want to know that EmailProtect is working in the background, some users may not want to see an email with an alert. This email includes a link to Product Documentation and step-by-step instructions for popular POP-based email software which shows how to create a local rule to filter out these email alerts.

Setting up a POP account with Earthlink

Before you begin, you will need the following information:

- Names of the incoming and outgoing servers (can be the same)
- User name
- Your email address
- Your password

To setup the account, follow the instructions below:

1. Select **Tools > Settings** from the menu bar
2. Click the **Accounts** tab.
3. Your Earthlink POP account should already be listed. If not continue on.
4. Select **New**.
5. Enter Account name, etc.:
6. Make sure the incoming mail server is set to POP3.
7. Enter your Incoming mail server (pop.earthlink.net).
8. Enter your Outgoing mail server (smtp.earthlink.net).
9. Click **OK**.
10. Click **OK** again.

To set a rule for Earthlink to delete EmailProtect alert messages, follow the instructions below:

1. Select **Tools > Edit Filters** from the menu bar.
2. Click **Add**.
3. Make sure If the From field contains the following text is checked, and that EmailProtect Alert is displayed.
4. Click **Next**.
5. Click **Close**.

Setting up a POP account with Eudora 5.1

Before you begin, you will need the following information:

1. Names of the incoming and outgoing servers (can be the same)
2. User name
3. Your email address
4. Your password

To setup the account, follow the instructions below:

1. Select the Personality tab and click **Personalities** (the one with profile faces) at the left side of the window, about two-thirds of the way down.
2. Right-click in the window and select **New** from the shortcut menu.
3. From the New Account Wizard, select **Create** a brand new email account. Click **Next**.
4. Enter your Personality Name. Click **Next**.
5. Enter Your Name. Click **Next**.
6. Enter your Email Address. Click **Next**.
7. Enter your Login Name. Click **Next**.
8. Enter the name of your Incoming Server.
9. Make sure that the POP server type is selected. Click **Next**.
10. Enter the name of your Outgoing Server. Click **Next**.
11. Click **Finish**.

To set a rule for Eudora to delete EmailProtect alert messages, follow the instructions below:

1. Right-click the message you want to base a rule on (in this case, the email from Quarantine).
2. Select **Make Filter** from the shortcut menu.
3. From the Make Filter window, make sure that conditions Incoming and Manual are checked, and that From is selected. Quarantine should appear in the Contains field.
4. Under the Action section, select **Delete Message** (Transfer to Trash).
5. Click **Create Filter**.

Setting up a POP account with Netscape 7

Before you begin, you will need the following information:

- Names of incoming and outgoing servers (can be the same)
- User name
- Your email Address
- Your password

To setup the account, follow the instructions below:

1. Select Edit > Mail & Newsgroups Account Settings from the menu bar.
2. Click **Add Account**.
3. Select Email account. Click **Next**.
4. Type your name in the text box for Your Name.
5. Type your email address in the text box for Email Address. Click **Next**.
6. Select **POP** as the Incoming Server.
7. Type your Incoming POP server name in the text box for Incoming Server.
8. Type your Outgoing POP server name in the text box for Outgoing SMTP server. Click **Next**.
9. Type your email address in the text box User Name. Click **Next**.
10. Type your email address in the text box Account Name. Click **Next**.
11. Click **Finish**.

To set a rule for Netscape to delete EmailProtect alert messages, follow the instructions below:

1. Select the message from a specific sender (in this case, the email from Quarantine).
2. Select **Message > Create Filter From Message** from the menu bar.
3. Type Quarantine for the filter name in the Filter Rules window.
4. Make sure Match any of the following is selected, and that Sender is Quarantine is displayed.
5. Under Perform this action, change the selection from Move to folder to Delete the message.
6. Click **OK**.
7. Click **OK** again.

Setting up a POP account with Outlook 2002

Before you begin, you will need the following information:

- Name of incoming and outgoing servers (can be the same)
- User name
- Your email address
- Your password

To setup the account, follow the instructions below:

1. Select **Tools > Email Accounts** from the menu bar.
2. Select **Add a new e-mail account**. Click **Next**.
3. Select **POP3** as the email server. Click **Next**.
4. Enter the following information:
    - Your name: Your full name
    - E-mail Address: you @yourdomain.com
    - User Name: Identifying you the user

- Password: Your password
- Incoming mail server (POP3): mail.yourdomain.com
- Outgoing mail server (SMTP): smtp.yourisp.com
- Unless your ISP has indicated that your service uses Secure Password Authentication (SPA), do not check Log on using Secure Password Authentication (SPA).

5. Click **Test Account Settings** to make sure your settings are valid. Click **Next**.
6. Click **Finish**.

To set a rule for Outlook to delete EmailProtect alert messages, follow the instructions below:

1. Right-click the message you want to base a rule on (in this case, the email from Quarantine).
2. Select **Create Rule** from the shortcut menu.
3. Select a condition from Quarantine. Click **Next**.
4. Under What do you want to do with the message?, select **Delete it**. Click **Next**.
5. Click **Next** from Add any exceptions (if necessary) page.
6. Edit the name of the rule for the Quarantine message.
7. Make sure **Turn** on this rule is checked.
8. Click **Finish**.

Setting up a POP account with Outlook Express 6

Before you begin you will need the following information:

- Name of incoming and outgoing servers (can be the same)
- User name
- Your email address
- Your password

To setup the account, follow the instructions below:

1. Select **Tools > Accounts** from the menu bar.
2. Click **Add** located on the right.
3. Select **Mail** from the menu.
4. Enter Display name. Click **Next**.
5. Enter your Email address. Click **Next**.
6. Make sure the incoming mail server is set to POP3.
7. Enter your Incoming mail server (mail.yourdomain.com).
8. Enter your Outgoing mail server (smtp.yourisp.com). Click **Next**.
9. Enter your Account name and Password.
10. Unless your ISP has indicated that your service uses Secure Password Authentication (SPA), do not check Log on using Secure Password Authentication (SPA). Click **Next**.
11. Click **Finish**.

To set a rule for Outlook Express 6 to delete EmailProtect alert messages, follow the instructions below:

1. Select the message you want to base a rule on (in this case, the email from Quarantine).
2. Select **Message > Create Rule From Message** from the menu bar.
3. Under number 1, select the conditions for your rule:, make sure Where the From line contains people is checked.
4. Under number 2, select the Actions for your rule:, check **Delete**.
5. Number 3 is a description of your rule. No need to make changes.
6. Under number 4, Name of the rule, select and type a rule name.
7. Click **OK**.

Setting up a POP account with Pegasus 4.02

Before you begin, you will need the following information:

- Name of incoming and outgoing servers (can be the same)
- User name
- Your email address
- Your password

To setup the account, follow the instructions below:

1. Select **File > Network** configuration from the menu bar.
2. Select the General tab and complete the following information.
    - My Internet e-mail address is: you@yourdomain.com
    - Receiving (POP3): General settings for receiving via POP3
    - POP3 host: mail.yourdomain.com
    - User name: you
    - Password: your password
    - Sending (SMTP): General settings for sending mail via SMTP
    - SMTP host: smtp.yourisp.com
    - Connect to SMTP server on TCP/IP port: 25
3. Click **OK**.

To set a rule for Pegasus to delete EmailProtect alert messages, follow the instructions below:

1. Select the message you want to base a rule on (in this case, the email from Quarantine).
2. Select **Tools > Mail filtering rules > Edit new mail filtering rules > Rules** applied when folder is opened.
3. Click **Add Rule**.
4. Select **Headers**.
5. For *If any of these headers*, check **Subject**.
6. For *Contains this text*, type Quarantine
7. For *Then do this Action:* select **Delete**. Click **OK**.
8. Click **Save**.
9. Close the window.

Online Updates

Revisions to the categories listed in Default Filters are updated automatically, because the updates are extremely small in size and do not take any time at all to download. However, an update for EmailProtect may be required in the future. Software updates for EmailProtect may be larger in size. You can check for EmailProtect Updates anytime by clicking on the Online Updates button on the Quarantine Toolbar. EmailProtect will automatically open the ContentWatch Updater utility. If there is an update available, select the product name and click the Download Updates button. Once the update has been downloaded, click the **Install Updates** button.

After the update has been installed, you will be asked to restart your computer for the changes to take effect.

Updater Preferences

You may also change the preferences of the updater so it will automatically look for and install updates when they are available.

1. Select **Preferences > Change Preferences** from the menu bar.
2. Make any changes and click **OK** or **Apply** to save the changes or **Cancel** to close the window without saving any changes. When an update is automatically installed, it will display a notification window above the system tray. Restart the computer for the changes to take effect.

Using Help

To access the help files, follow the instructions below:

1. Double-click EmailProtect from the system tray to open Quarantine.
2. Select **Help > HTML Help** from the menu bar.
3. HTML help files are accessed and opened from the ContentWatch Product Documentation site.
4. Locate and double-click EmailProtect Help.
5. Double-click a topic from the Contents tab, or select a topic from the Contents tab and click **Display** for step-by-step help.

Using the Index Tab

To access the Index tab, follow the instructions below:

1. Select the **Index** tab from the EmailProtect Help window.
2. Enter a keyword.
3. Select a topic from the alphabetical list.
4. Click **Display** or just double-click the desired topic.

Using the Search Tab

To access the Search feature, follow the instructions below:

1. Select the **Search** tab from the EmailProtect Help window.
2. Type in a keyword that will generate a list of possible uses and spellings of that keyword.
3. Click **List Topics**.
4. Select a topic under Select Topic to display:
5. Click **Display** or double-click the topic to display help.

Frequently Asked Questions

What is the Quarantine area?
Quarantine is a “safe area” where you can view the sender and subject lines of flagged messages. If you wish to view the email in Quarantine, you can choose to view it with or without images. This protects you from unintentionally viewing explicit images in your email.

Will EmailProtect work with my email client?
EmailProtect works with most POP3 email clients, including Outlook, Outlook Express, Eudora, Pegasus, IncrediMail, PocoMail, Netscape Communicator, Earthlink and others. Even better—a single copy of EmailProtect protects ALL supported email clients on the same computer.

Does EmailProtect support AOL, Juno or other Webmail?
Sorry, but AOL and Juno use private, proprietary systems. Webmail is based on standard HTML. For example, if an AOL software change occurred, unknown to us, then EmailProtect would simply stop working for our customers using these services. This is why we support POP3, as it is an open, standard protocol.

What do you mean when you say EmailProtect supports “unlimited accounts?”
This means that we filter all POP accounts and users on the one computer where EmailProtect is installed. One user license covers all email traffic on that computer. Some of our competitors have a limit in their software. They can only handle so many POP accounts per computer, because they log into your account. EmailProtect doesn't log into any accounts, so there is no limit.

Will EmailProtect work with my Exchange Server?
EmailProtect does not install on Exchange Server itself, but works with email client software that connects to it, like Outlook. Microsoft Exchange addresses can be configured for POP3 access, with clear text logins allowed. Check with your system administrator.

Can I install EmailProtect on my email server, so it can work with all the clients?
Sorry, EmailProtect is designed for the client only, so the individual user can decide what email is desired. In order to support many clients with similar rules, purchase a license for each client. Set up the desired rules for the first installation, and export the settings file. For each installation, simply import the saved settings file to that client.

Is EmailProtect available for the Mac?

Sorry, no. Our software does not support the MAC.

Does EmailProtect support IMAP?
Sorry, not currently. However, this support is planned for our next version.

EmailProtect – Setup FAQs

How do I set up my Yahoo account to work with EmailProtect?
You can signup for a POP mail account through Yahoo and access your Yahoo mail through a POP3 mail client. This will allow you to use EmailProtect with a Yahoo email account. For more information, visit: http://help.yahoo.com/help/us/mail/pop/.

Does EmailProtect allow me to block anyone who is NOT in my email address book or that I have not sent a message to?
Yes, you can block everyone unknown. Import your address book, which will place everyone you know in the Safe List. Then go to Add to Block List, Address tab, and press the Advanced button. Add an IP address of 0.0.0.0, then choose OK. Go to My Filter Settings, Blocked Addresses tab, and find the rule for 0.0.0.0. Choose edit, and change this entry to an asterisk '*'. This blocks all servers, all email. Since the Safe List always overrides the Block List, any email from someone you know will always get through to your Inbox.

Troubleshooting

I created a Block rule, but it didn't work. Why did EmailProtect let the email through to my Inbox?
First, check your Safe List. Remember, Safe rules ALWAYS override Block rules.
I have selected a category to Block, but it doesn't always work. What happened?
Although EmailProtect tries to get all unwanted email, it is very difficult to get 100%. This problem is similar to anti-virus software. As filtering technology improves, there are those that will try to find new ways to get past it. This will always be an ongoing issue, which is one reason why we will have periodic updates available. Until the next update, create a quick Block rule on the address or word to be blocked. In addition, remember that Safe rules ALWAYS override Block rules.

Why do I not receive any emails at all?
While we have tested with the major POP3 email servers, yours could be a little different. Also, if you have firewall or ant-virus software, you may have settings that might need changing. Please call Customer Service at 1.800.485.4008, so that we can help you.

Why do I have words and buttons cut off on the screen?
This can occur when using large fonts. Please change to normal fonts from the Windows Control Panel.
When EmailProtect traps an email that I want to keep, clicking on Send to Inbox just causes it to disappear from Quarantine. It does not appear in my Inbox. Where is it?
When you click Send to Inbox, the email is marked for delivery to your Inbox. Simply click Send/Receive from your email client, and the email will appear in your Inbox.

Why can't I import my address book?
We support all the major POP3 email clients, but yours may not be compatible with EmailProtect. Export your address book as a CSV or comma-delimited type.

I get an error with Outlook Express "MSIMN.Exe - Application error." Why is that?
This is a Microsoft problem with Outlook Express. It happens to many people who have never used EmailProtect. Microsoft recommends that you update to the latest fixes of Internet Explorer. This should fix the problem.

Glossary

Application -- A program or tool used on your computer, such as a word processor, a game, or an email program.

Blocked -- To keep from appearing, displaying, accessing, etc.

Browser -- The application that lets you navigate around and view pages on the Web. Netscape and Internet Explorer are the two most common.

Category -- A general term for a whole topic or information type.

Default Settings -- A setting that a program automatically selects (usually the recommended settings) if you do not specify a substitute.

Filtering -- Controlling access to category content by analyzing the incoming and outgoing requests and letting them pass or diverting them based on settings selected within EmailProtect.

Help -- Online documentation. Many programs come with the instructional manual, or a portion of the manual, integrated into the program. If you encounter a problem or forget a command while running the program, you can access help documentation by selecting Help from the menu bar and clicking a topic for help documentation.

Icon -- A small picture that represents an object or program.

Internet -- The Internet consists of countless networks of computers that are connected together across the world allowing millions of people to share information. Components of the Internet include: the World Wide Web, newsgroups, chat rooms, and email.

Override -- To neutralize an action or automatic control with a desired but intermittent control.

Preferences -- Program settings that can be customized to meet your needs.

Rule -- Restrictions or program instructions that are applied according to options you select. You can decide whether or not to have rules applied to addresses or words.

System Tray -- Located on the Windows taskbar, usually at the bottom of your screen and next to the clock. The system tray contains miniature icons for easy access to system functions such as fax, printer, modem, etc., and programs.

Customer Support

For questions and technical assistance, call 1-800-485-4008 for prompt, competent, and courteous customer support, Monday through Friday, 8 A.M. to 5 P.M. Mountain Standard Time.

Also, you can email questions at any time to info@contentwatch.com

Categories

Categories are representative of content. ContentWatch keeps an up-to-date list which is automatically passed on to you through your Internet connection. The best way to determine which categories you would like to allow and which categories you would like to have filtered, examine the category definitions below to aid you in your decisions. EmailProtect does the examining for you and determines which category a Quarantined email belongs to.

Defining Categories

Ads - Advertisements for products, services, etc.

Adult/Mature - Sites or resources that contain subject matter intended for mature audiences, such as obscene or vulgar language and adult Chat rooms. These sites could be considered R-rated.

Chat Site - Sites or resources that contain information on Chat protocols or applications, links to Chat organizations, rings, and rooms.

Drugs/Alcohol - Sites or resources that contain subject matter that deals with the manufacturing, distribution, or obtaining illegal drugs, alcohol, or other controlled substances. Sites that depict drug or alcohol paraphernalia and/or include methods for obtaining or manufacturing them. Does not include sites that provide information on prescription medications except those sites that describe how to illegally obtain them.

Email - Sites or resources that provide access to email services, and applications.

Employment/Career - Sites providing information on employment opportunities and resources for expanding career options.

Family Resources - Sites or resources that provide family counseling, family safety tips, parenting information and tips, and family planning.

Financial/Stocks - Sites or resources that provide information about finances, financial planning, insurance, stock tickers, stock reports, or sites that allow the sell and purchase of stock. Includes banks and credit unions, and credit rating and reporting sites.

Gambling - Sites or resources that allow a person to wager money on online games with the expectation of winning money or prizes. Sites that contain links to other gambling sites or provide information on gambling strategies or tactics.

Games - Sites or resources that provide access to online or downloadable games, or discussions about games. Sites that provide information about game cheats.

Government - Sites or resources that are specific to local, state, or federal government organizations or agencies, including political party sites and specific, official political sites. Sites ending in .gov.

Hate/Violence - Sites or resources that promote or depict violence against persons, animals, property, or nations. Sites that single out groups for violence based on race, religion, or creed.

Health/Medicine - Sites or resources that deal with or provide information on mental or physical health issues. Sites that allow the online purchase of prescription medications.

Illegal Activities - Sites or resources that provide information about the manufacture, alteration, or sales of weapons. Sites that promote or depict disorderly conduct, or that provide information on the manufacturing of explosives and explosive devices.

Instructional - Sites or resources that contain instructional material, tutorials, or how-to pages.

Intimate Apparel - Sites or resources that display models wearing underwear, lingerie, or other suggestive or see-through attire, including swimsuits.

Kids - Sites or resources intended for children, including entertainment, education, crisis counseling, and kid-friendly communities.

Music/Entertainment - Sites or resources that provide access to free downloadable or for-pay online music and video files such as MP3, WAV, MPG, and AVI, etc. Sites that sell music or videos, or that are dedicated to the music or entertainment industry. Sites that provide information on TV programs and programming, including movie review sites.

News - Sites or resources that provide live, recorded, or written reports or editorials about current events.

Personals - Sites or resources that contain personal ads, personal info pages, and personal portals.

Pornography - Sites or resources that are meant to sexually arouse the viewer. May show models or real people that are engaged in erotic behavior intended to cause sexual excitement. May describe sexually explicit activities or contain sexually explicit material including images, movies, or text. Sites would be considered X-rated.

Religious - Sites providing information on specific religions or general religious resources.

Schools/Colleges - Sites or resources that contain information dealing with colleges, schools, seminars, or courses. Sites that end in .edu.

Search Engines/Portals - Sites or resources that provide mechanisms for searching the Internet by specific words or phrases and that display the results as either links or images. Sites that allow a user to customize the look or content and that are geared to providing a starting place on the Internet.

Shopping - Sites or resources that provide access to online malls, catalogs, or auctions, including classified ads. Department store sites, retail store sites, or sites that have coupons for free or discounted items.

Sports - Sites or resources for sports information including amateur, college, and professional sports.

Travel - Sites or resources that provide travel information ranging from general information to booking reservations.

Work Related - Sites or resources that provide information related to a user's work.

PopupProtect Welcome

Congratulations on your choice of PopupProtect. You now have the power to block those annoying popup and popunder windows from invading your computer and the cookies that result. Now that PopupProtect has been installed, popup advertisements are a thing of the past. Even though you can eliminate all popup and popunder advertisements and windows, you may want to have the flexibility to decide which popup and popunder windows you would like displayed. You can add any website to an Allow List which overrides PopupProtect from blocking popups from a specific website.

PopupProtect is designed for your ease of use with access to a 7-day history, capabilities to add and remove websites from an Allow List, apply advanced options, etc.

Features and Benefits

- Blocks all popups, popunders, mousepops, etc.
- Turn on and off with a single click
- Interactive Rule Assistant to log and allow sites for popups
- Compatible with all browsers (IE, Opera, Netscape, AOL, etc.)
- Works with all types of Internet connections
- Works with any ISP (AOL, EarthLink, local, etc.)
- Compatible with Windows 98SE, Me, 2000, XP
- System tray access from the taskbar
- Customizable Allow List to override automatically when necessary
- Simple alert system that is optional with elective sound when popups are blocked
- Keeps a complete history log of all allowed or blocked popups
- Stops window spawning
- Free Online Updates and Customer Support
- Designed for the nontechnical user

System Requirements

- PC with Pentium or compatible 133 MHz or faster processor
- Microsoft Windows 98SE/Me/2000/XP
- 64 MB RAM
- 100 MB hard drive space
- Color monitor with a minimum 800x600 resolution
- Internet connection
- Internet Explorer 5.0 or greater, Netscape 6.0 or greater

Installation from a CD

1. Insert the CD into the CD ROM drive (If the CD does not automatically run, go to Start>Run type in "d:Autostart.exe" Replace the D with the letter for your CD-ROM drive.)
2. From the Menu, select Install Software; this will open the Setup Wizard.
3. Click **Next** to start the Setup Wizard.
4. Click **Next** on the Welcome screen.
5. Choose to accept the license. Click **Next**.
6. Choose the Install directory. Click **Next**.
7. Select the products to install. (You must install ContentProtect Professional.) Click **Next**.
8. Enter the Organization Account Name and the Install Password. Your administrator should have provided these; contact your administrator if you do not have the account name and password. Click **Next**.
9. Enter all of your user information. The Email field is not required, but it is recommended. Click **Next**.
10. Verify your settings and then click **Install** on the confirmation dialog.
11. Click **Finish** to restart the computer and complete the installation.
12. When the machine restarts, run the Online Updates. You can launch this from any of the products or by selecting it from the right-click menus of the taskbar icons located at the bottom of the screen next to the clock.
13. When the update dialog displays, click **Check For Updates**.
14. If the default settings have not been changed, the new updates will download and install automatically. If the default settings have been modified, follow the prompts to download and install updates. When the process is complete, select the "Click here to restart your computer now" link.

Your system should now be fully updated with the newest version of **ContentProtect Pro Suite**.

Disabling and Enabling PopupProtect

After installing PopupProtect, you can disable or enable PopupProtect. If you disable PopupProtect, popups will no longer be blocked while browsing the Internet.

PopupProtect is enabled by default after installation.

Disabling and Enabling Option 1:

3. Right-click PopupProtect from the system tray.
4. Select **Enabled** from the menu to remove the check mark.
3. The system tray icon for PopupProtect will have a diagonal line through it meaning it is disabled.

5. To enable PopupProtect again, right-click **PopupProtect** and select **Enabled** from the menu.

The PopupProtect Window

Let's look at PopupProtect Window components:

1. Double-click **PopupProtect** from the system tray located at the bottom right of your screen.
2. Observe the PopupProtect application window. Review the labeled components below and their definitions.

Title Bar – Where the application name resides.

Minimize and Close – The minimize and close buttons both hide the application window but will keep PopupProtect running to provide protection against popup and popunder windows.

Menu Bar – The menu bar contains menus (File, Tools, Help) with different options and actions.

Toolbar – Action buttons that perform an action or provide a window with options when you click them.

History List – A table of information of website or Internet address that have had popup or popunder windows blocked or allowed. Table information consists of Date/Time (the date and time the popup was blocked or allowed), Source (where the popup originated), Blocked? (yes or no appears appropriately), and Location (the actual domain address). You must have Internet activity for a history to accumulate.

Action Buttons - Help displays context sensitive instruction for that topic, the Hide button will hide the application window just as Minimize and Close, but keeps PopupProtect running in the background, you can also select File>Hide from the menu bar. Clicking **Delete Selected** will delete the selected entry from the History List.

Opening and Exiting PopupProtect

Note: To perform different tasks such as adding Addresses, checking the History, editing the Allow List, etc. you will want to open PopupProtect by following the steps below:

Opening PopupProtect

1. Double-click **PopupProtect** from the system tray, or
2. Right-click PopupProtect and select **Show** from the menu, or
3. Click **Start** and select Programs>PopupProtect>PopupProtect to open the application.

Note: You can keep PopupProtect running and hide the program window by clicking the minimize or close buttons (click here to view PopupProtect window components) and then restore as needed by double-clicking the PopupProtect icon from the system tray.

Exiting PopupProtect

Exiting PopupProtect is different from minimizing the application. Minimizing maintains the last window you navigated to in the application and are then able to restore the application.

1. If the PopupProtect application window is displayed on your screen, select **File>Exit** from the menu bar, or right-click the PopupProtect icon from the system tray and select **Exit** from the menu.
2. A message is displayed asking if you are sure you want to exit. Popups will no longer be blocked.

Important: PopupProtect will no longer be available from the system tray. You will have to click **Start** from the taskbar and select Programs>PopupProtect>PopupProtect from the menu to open the program and display the PopupProtect icon in the system tray.

Adding to the Allow List

1. Observe the Add to Allow List window. The selected address appears in the Address text box. If this is the domain in which you would like to allow popups, simply select one of the following options:
    - Allow ALL popups while at this address
    - Allow only popups pertaining to this address while at this address
2. Click **OK** to save changes.

Editing the Allow List

There are several ways to edit the Allow list.

Disabling an address rule

Rules are restrictions or program instructions that are applied according to options you select. You can decide whether or not to have popups appear for any website address. Addresses that have been added to the Allow List can be disabled without deleting the entry altogether. That way, you can enable and disable the rule for an address as needed without having to repeatedly add and delete website addresses.

1. Double-click **PopupProtect** from the system tray.
2. Click **Edit Allow List** from the toolbar, or select **Tools>Edit Allow List** from the menu bar.
3. Click the check box to the left of the address to disable the address rule and remove the check mark. To enable the address rule, simply click the same check box again.
4. Click **OK** to save changes.

Note: You can quickly check and uncheck all address entries from the Allow List by clicking **Check All** or **Uncheck All** from the toolbar.

Deleting an address

Addresses that are no longer needed can be removed from the Allow List.

1. Double-click **PopupProtect** from the system tray.
2. Click **Edit Allow List** from the toolbar.
3. Select the address to delete and click **Delete Address**.
4. Click **OK** to save changes.

Editing an address

If you notice that the popups for a specific address are not being allowed or blocked properly, you might want to check the address for accuracy. Typing a comma instead of a period will make an address invalid so accuracy is critical. Copying and pasting the address is the most accurate method. Editing an address is quick and easy. You may want to change the rule for an address, i.e. changing the rule from Allow ALL popups while at this address to Allow only popups pertaining to this location while browsing this address.

1. Double-click **PopupProtect** from the system tray.
2. Click **Edit Allow List** from the toolbar.
3. Select the address to edit and click **Edit Address** from the toolbar.
4. The Add to Allow List window is displayed. Make changes as needed to the address in the address text box. This is where you can change the rule for an address when necessary such as Allow all popups while at this address or Allow only popups pertaining to this address while browsing this address.
5. Click **OK** to save changes.

PopupProtect History

1. Double-click **PopupProtect** from the system tray.
2. Observe the Popup History window. A complete list of all allowed and blocked popups are logged for your review. Items can be sorted in ascending or descending order by clicking a column header such as **Date/Time**, **Source**, or **Location**. All column widths can be adjusted by dragging the separation lines between columns.
3. To add a logged entry to the Allow List, select an entry item from the history list, click **Add to Allow List** from the toolbar.
4. Select one of the following options:
    - Allow ALL popups while at this address
    - Allow only popups pertaining to this location while browsing this address
5. Click **OK** to save changes.