



# **ContentBarrier X5**

## **User's Manual**



Intego ContentBarrier X5 for Macintosh  
©2001 - 2009 Intego. All Rights Reserved

Intego  
[www.intego.com](http://www.intego.com)

This manual was written for use with Intego ContentBarrier X5 software for Macintosh. This manual and the Intego ContentBarrier X5 software described in it are copyrighted, with all rights reserved. The Software is owned by Intego, and its structure, organization and code are the valuable trade secrets of Intego. The Software is protected by United States Copyright Law and International Treaty provisions. This manual and the Intego ContentBarrier X5 software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by Intego.



## *Contents*

<b>1- About Intego ContentBarrier X5 .....</b>	<b>5</b>
<b>Protecting Your Children with Intego ContentBarrier X5 .....</b>	<b>6</b>
<b>Intego ContentBarrier X5's Features.....</b>	<b>7</b>
<b>2 - Filtering Internet Content.....</b>	<b>8</b>
<b>The Internet: A Limitless World of Content .....</b>	<b>9</b>
Types of Internet Content.....	9
Filtering Content.....	10
How You can Help your Children Surf Responsibly .....	10
<b>Filtering Content in Businesses .....</b>	<b>11</b>
Optimizing Productivity .....	11
Optimizing Bandwidth .....	11
Protecting Your Company .....	12
<b>3 - Installation.....</b>	<b>13</b>
<b>System Requirements.....</b>	<b>14</b>
<b>Installing ContentBarrier X5 .....</b>	<b>14</b>
<b>4 - Setting Up ContentBarrier X5 .....</b>	<b>15</b>
<b>Using the ContentBarrier X5 Setup Assistant .....</b>	<b>16</b>
Setting an Administrator Password .....	18
Automatic Updates .....	20
User Selection.....	21
Web Filtering Setup.....	23
Chat Filtering Setup.....	25
Recording Setup .....	26
Reporting Setup .....	27
Finishing .....	30
<b>Setting Up Web Administration.....</b>	<b>31</b>
<b>Managing Users .....</b>	<b>33</b>
<b>Changing User Display .....</b>	<b>35</b>
Saving User Profiles .....	36
Editing User Icons .....	37
<b>5 Using ContentBarrierX5 .....</b>	<b>38</b>
<b>Refining ContentBarrier X5 Configurations.....</b>	<b>39</b>
<b>How Content Barrier Filters Internet Content .....</b>	<b>41</b>
<b>Web Filtering .....</b>	<b>41</b>
<b>Chat Filtering .....</b>	<b>47</b>
<b>Using Schedules .....</b>	<b>50</b>
<b>Application Filtering .....</b>	<b>56</b>
<b>Recording Internet Usage.....</b>	<b>59</b>



<b>Other Filtering Options .....</b>	<b>61</b>
E-mail Filtering .....	62
Peer-to-Peer Filtering .....	62
Game Filtering .....	63
Audio/Video Filtering .....	63
Newsgroup Filtering .....	64
FTP Filtering .....	64
SSH Filtering .....	65
Volume Filtering .....	65
<b>Using Logs .....</b>	<b>66</b>
Setting Log Preferences .....	68
Viewing Logs .....	70
Keyboard and Screen Logs .....	74
Exporting Log Reports .....	76
<b>About ContentBarrier X5.....</b>	<b>77</b>
<b><i>5 - Technical Support .....</i></b>	<b><i>78</i></b>



# **1- About Intego ContentBarrier X5**



## Protecting Your Children with Intego ContentBarrier X5

ContentBarrier X5 is a parental control program for the Macintosh, providing functions for parents and businesses. It is designed to filter and block certain Internet content according to the settings you choose. ContentBarrier X5 blocks adult web sites, sites with subjects not fit for children, and blocks chats when predatory language is used. It also blocks certain protocols, or types of Internet communication, that you may not want your children to use, such as peer-to-peer and other file sharing protocols, online games, streaming audio and video, FTP, SSH and more.

ContentBarrier X5 works with multiple users, and interfaces seamlessly with the Mac OS X user accounts on your computer. If you have several children, you can set different limitations corresponding to their age or maturity. You can choose whether they have access to newsgroups, e-mail, or whether they can download files. You can set the program to let them only use the Internet at certain times, and on certain days. You can choose to block or allow specific web sites, allow users only to use selected applications, and block access to specific types of content, such as streaming media or peer-to-peer file transfers. The program can even send you e-mail, automatically, when certain events occur. And you can view logs and manage some of ContentBarrier X5's settings over the Internet, using any web browser.

ContentBarrier X5 sets up a protective wall around your computer. Its pre-defined filters let you choose what you don't want your children to see, and you can create your own custom filters as well. Inappropriate web sites are blocked, shielding your children from content they are too young for. Additional filters block content by program type, such as chats, newsgroups and more.

ContentBarrier X5 keeps a complete log of all web sites visited, whether blocked or not, and records which applications have been blocked, if you choose to block certain programs. You can also record screenshots and keyboard activity, giving you a full record of your children's activities on the Internet. ContentBarrier X5 makes the Internet a safer place for your children.

Intego ContentBarrier X5 is compatible with Mac OS X 10.5 (Leopard) and 10.4 (Tiger), and runs on Macs with either PowerPC or Intel processors.



## Intego ContentBarrier X5's Features

- Blocks and filters all offensive material from the Internet
- Customizable profiles—if you have several children, you can adjust the settings for their age and maturity
- Seamless interface with Mac OS X user accounts
- Setup assistant simplifies user configuration
- Adjustable levels of protection
- Overview screen shows all user settings
- Pre-determined filters for safe and easy content filtering
- Web site blocking—block or allow specific web sites
- Full recording of activity: sites visited, sites blocked, chats, e-mail, applications, screenshots and keystrokes
- Prevents external disks and volumes from mounting
- Remote web administration from any computer
- Quick enabling/disabling of protection for each user
- Add user photos for easy recognition and configuration
- Blocks streaming media, newsgroups and peer-to-peer software
- Blocks chats and e-mail
- Blocks selected applications
- Filters protocols such as FTP/SFTP, SSH, SSL and online games
- Start and stop time limits from the Intego menu
- Instant authorization for blocked sites
- Automatic search engine redirection
- Limits Internet access by day and time
- AntiPredator function to block predatory language in chat sessions
- Detailed logs of each user's Internet usage
- Traffic data recorded for an overview of Internet use
- Only authorized users can change program settings
- Automatic updates with NetUpdate
- Automatic e-mail notification of certain events
- User manual in the Help menu



## 2 - Filtering Internet Content





## **The Internet: A Limitless World of Content**

It's a brave new world out there on the Internet: a world of information, entertainment and fun. You can surf the web for hours, going from news sites to sports sites, from movies to music, but, sooner or later, whether you like it or not, you will come across the dark underbelly of the Internet. For not all is as attractive as it seems. Sometimes you'll look for information in a search engine and come up with a list of links that seem to correspond to your search, when, in reality, some of them are pornographic web sites, others are hate sites, and some are propaganda for cults. More and more purveyors of pornography set up web sites featuring common keywords so search engines take unsuspecting users to them.

You may be convinced that the Internet is the library of the future, and you may want your children to use it for their homework and entertainment, but do you really want them to see everything that's out there? You don't let your children read just anything, do you? When they use the Internet, they can easily stumble on inappropriate material, unless you're there to watch over their shoulders.

The Internet is still young, and, from its earliest days, when it expanded beyond research laboratories and universities, it has been a kind of frontier land where anything goes. While this freedom gives the Internet its strength, it also makes it dangerous for children.

Some people see the Internet as a huge library, newsstand and bookstore all in one. This is actually a good metaphor. But when you think about it, you don't give your children free rein in the library, nor do you let them look at every magazine you find on your local newsstand. The problem with the Internet is that its very nature, that of hypertext links from one site to another, means that content inappropriate for children is often just a mouse-click away.

### **Types of Internet Content**

Children use the Internet for many purposes: to do their homework, to present creative writing, artwork or photos, to do research for school, and to find out more about their favorite singers or movies. Many children have their own web pages, especially on sites like MySpace and Facebook, displaying their interests and hobbies; others participate in chats with peers around the world. More



and more kids set up their own blogs to communicate with their friends, whether they are next door or in other countries.

In most cases, there is nothing dangerous about what they do, but many parents are concerned about the variety of material found on the Internet. Content presenting sexually explicit images, violence, gambling, alcohol advertising, ideological extremism, etc., is easily found, either accidentally or intentionally. While parents consider it normal to protect their children from this content in books and magazines, and count on their local public libraries and schools to do so, there is no such protection on the Internet.

Add to that the complication of the various laws in the many countries accessible via the Internet—while national or local standards may exist in some areas to control such content, other areas may have no legislation at all. Online gambling is legal in many countries, as is pornography; but on the Internet, as we know, there are no borders.

## **Filtering Content**

While adults have the right to free speech, many parents feel that their children should have the right to be protected from material that conflicts with their moral values. While freedom of expression does and should exist, there must be a way to protect children from content that is inappropriate for their age or maturity. This inappropriate content can include web sites, chat rooms, newsgroups and even e-mail. It should be up to parents to decide which of the many Internet resources their children can access.

The best solution to this problem is to filter Internet content with a program such as ContentBarrier X5. This program allows you to choose the specific filters you wish to use and the level of filtering applied. You can also choose to allow your children to only access trusted sites that you add to the program, or only use specific applications, for the highest level of security.

## **How You can Help your Children Surf Responsibly**

The best way to ensure that your children surf responsibly is to stand by their sides and help them choose what is right for them. But not all parents have the time for this, and it is essential to allow



children to have a certain amount of freedom. ContentBarrier X5 helps by offering the possibility of filtering the content you want to protect your children from, or by allowing access only to trusted sites or specific applications. But ContentBarrier X5 also keeps a full log of your children's Internet sessions, so, if you want to give them freedom, you can check up on them afterwards. You can record screen shots of their computer activity, and even record what they type. You can also check up on them using ContentBarrier X5's Web Administration feature, which lets you view detailed logs of their activity both on the Internet and on their Macs, and block or allow web sites.

## **Filtering Content in Businesses**

While parents may want to protect their children by filtering Internet content, business managers may wish to do the same thing to protect their bottom line. The Internet gives their employees access to an endless source of information, but it also gives them plenty of chances to waste time. How many employees do their shopping on the Internet, play network games, send and receive personal e-mail or download MP3 files while at work, reducing productivity and using valuable network bandwidth? ContentBarrier X5 can solve this problem by blocking access to many different types of sites, content and protocols, and contains specific filters for web sites designed for business use.

## **Optimizing Productivity**

The Internet can help improve employee productivity, by providing the latest information and ensuring rapid communication. But this productivity can drop sharply if employees spend their time playing games on the Net, checking sports scores or managing their investment portfolios. Also, your employees might be spending your time looking for a new job, consulting on-line job sites and sending résumés by e-mail. ContentBarrier X5 helps you optimize productivity by blocking the sites you choose, such as shopping, financial or job sites.

## **Optimizing Bandwidth**

Your network bandwidth is valuable. Not only is it expensive, but when you need to send or receive large files, you want that bandwidth to be available. If your employees are wasting your bandwidth by downloading MP3 files, software or movies, you may find your network clogged. ContentBarrier



X5 lets you block access to streaming media and peer-to-peer software, as well as protocols such as FTP, conserving bandwidth and ensuring that your employees are not violating copyrights by downloading content illegally.

## **Protecting Your Company**

If your employees surf sexually explicit sites while at work, this not only reduces productivity, but it may even expose you to liability for sexual harassment. Sending private e-mail over your mail server can also expose you to liability, and even prosecution, since your business is responsible for what circulates on its network. ContentBarrier X5 lets you selectively block access to different web site filters so your employees get down to business, all the time.



# 3 - Installation



## System Requirements

- Any officially-supported Mac OS X compatible computer running a PowerPC or Intel processor
- Mac OS X 10.4 or higher
- 20 MB free hard disk space

Note: ContentBarrier X5 is fully compatible with Mac OS X 10.5 (Leopard) and 10.4 (Tiger).

## Installing ContentBarrier X5

For information on installing and serializing ContentBarrier X5, see the Intego Getting Started manual, included with your copy of the program. If you purchased ContentBarrier X5 by download from the Intego web site, this manual will be in the disk image you downloaded that contains the software. If you purchased ContentBarrier X5 on a CD or a DVD, you'll find this manual on the disc.



## **4 - Setting Up ContentBarrier X5**

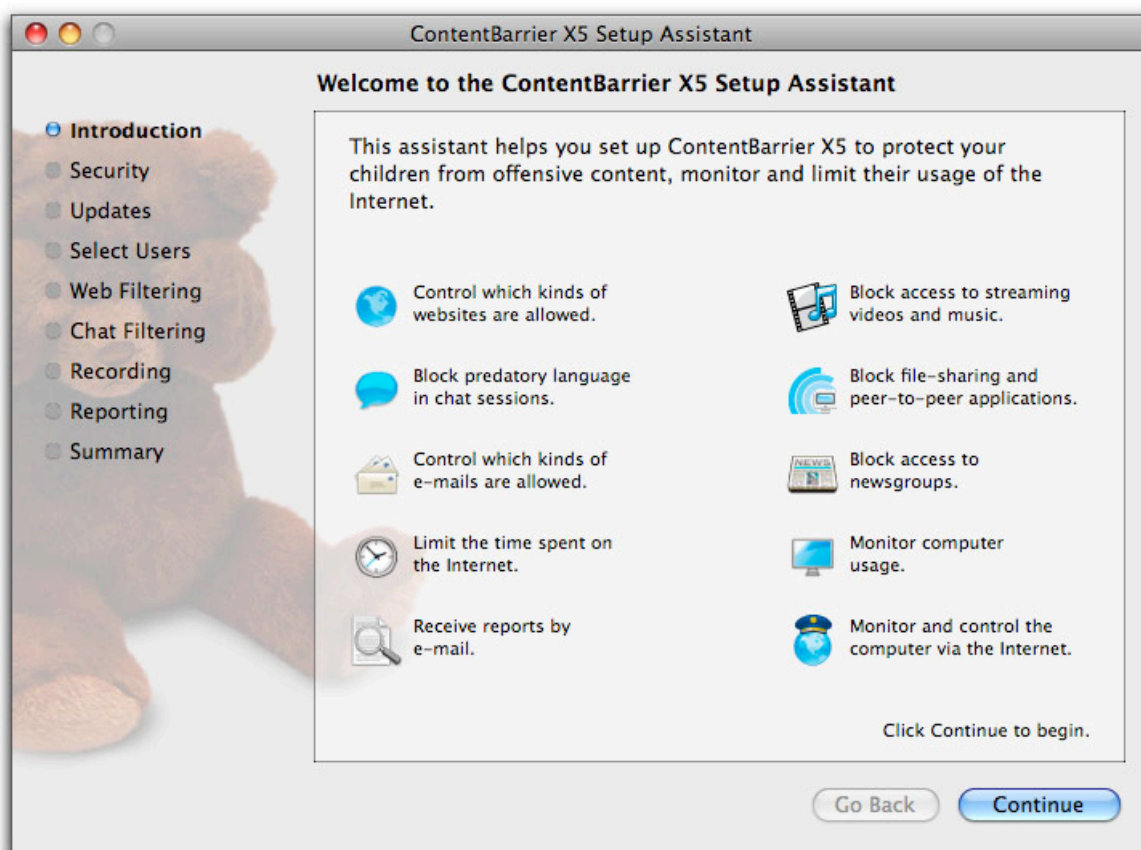


## Using the ContentBarrier X5 Setup Assistant

Intego ContentBarrier X5 is installed in your Macintosh's Applications folder. To open ContentBarrier X5, go to this folder, then double-click the ContentBarrier X5 application icon. You can also launch ContentBarrier X5 by clicking its icon in the Dock.



The first time you launch ContentBarrier X5, the ContentBarrier X5 Setup Assistant displays:



You can also launch the Setup Assistant at any time in ContentBarrier X5 by choosing Window > Setup Assistant while the program is running.





This assistant walks you through the configuration process, and explains the types of content that ContentBarrier X5 filters, and how this filtering is done. Click Continue to start configuring your users. If, at any time, you wish to return to a previous screen, click the Go Back button to do so.



## Setting an Administrator Password

The second screen of the ContentBarrier X5 Assistant asks you to set an administrator password for ContentBarrier X5.



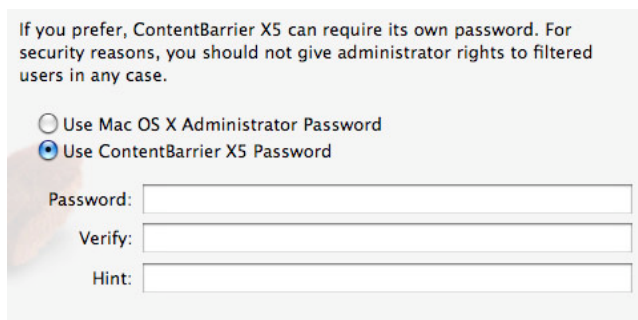
You always need an administrator password to change ContentBarrier X5's settings. This prevents your users from accessing and changing their own settings. ContentBarrier X5 gives you two options: you can use your Mac OS X administrator password, or you can set a special ContentBarrier X5 administrator password.

The advantage to using a Mac OS X administrator password is that any user with administrator access to the protected Mac will be able to make changes to ContentBarrier X5's settings. Since you can have several user accounts with administrator access under Mac OS X, this allows you to



ensure that, in certain environments such as schools, an administrator who can access and change ContentBarrier X5's settings is always available.

If you are using ContentBarrier X5 on a home computer, you may only have one administrator. In this case you can also use the Mac OS X administrator password. However, if you want extra security, or if you want to limit the ability to make changes to ContentBarrier X5's settings to specific administrators, you can set a special ContentBarrier X5 password. To do this, check Use ContentBarrier X5 Password and fill in the fields that appear: first, enter a password, then enter it again in the Verify field, then enter a hint that will remind you of the password, in case you forget it, in the Hint field.



If you prefer, ContentBarrier X5 can require its own password. For security reasons, you should not give administrator rights to filtered users in any case.

☐ Use Mac OS X Administrator Password  
☒ Use ContentBarrier X5 Password

Password:

Verify:

Hint:

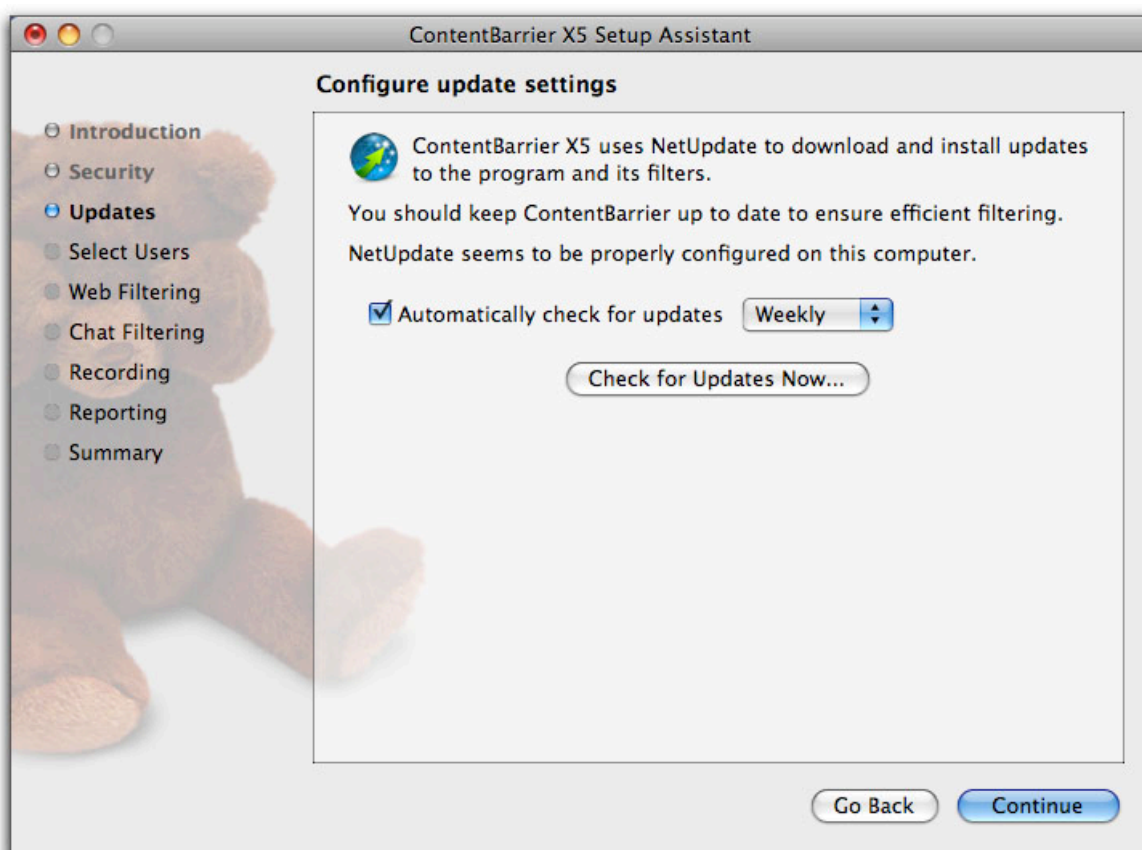
Click Continue to go to the next screen, or click Go Back to return to the previous screen.

You can change this password at any time in the Password pane of the Preferences window. To access it, choose ContentBarrier X5 > Preferences....



## Automatic Updates

The next screen lets you define whether ContentBarrier X5 will check to see whether it needs to update itself and its filters, and, if so, how often. By default the process will happen once a week, but you can increase the frequency by changing the popup menu to Daily, or decrease it by changing the menu to Monthly. You can also turn off this feature by unchecking the “Automatically check for updates” box, or force ContentBarrier X5 to check immediately by clicking “Check for Updates Now...”, which will launch NetUpdate. (For more information about Intego NetUpdate, see the Intego Getting Started Manual.

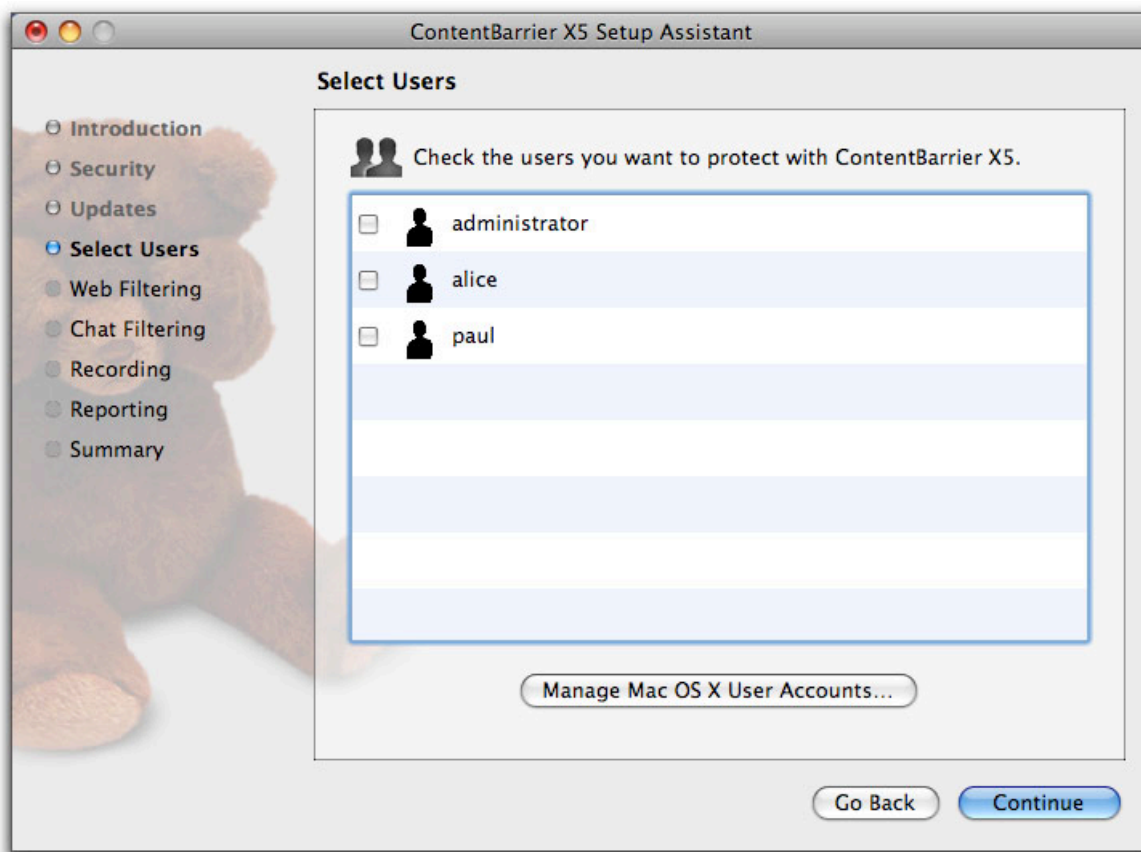


After you’ve confirmed the settings you want, click Continue to go to the next screen.



## User Selection

The next screen of the assistant lets you select which user you wish to configure. This screen shows all the users you have on your Mac (including certain types of non-human users created by Mac OS X or other software, such as the Guest account).



There are two types of user accounts: administrators and standard users. Administrators are permitted to make system-level changes to your computer to, for example, install software or prevent programs from launching. If you attempt to protect an Administrator's account with ContentBarrier X5, you'll get a warning saying, "For security reasons, filtered users should not have administrator rights." ContentBarrier X5 will still let you set up protection for such users, although they might be able to use their administrator privileges to change or remove your settings.



But if you've set a special ContentBarrier X5 password, even users who are administrators will not be able to make changes to ContentBarrier X5's settings. While the ContentBarrier X5 password prevents administrators from changing the program's settings, any user who is an administrator will be able to uninstall the program. Therefore, if you have not set a special ContentBarrier X5 password, it is best to use standard accounts for users for whom you wish to filter content.

If you need to make changes to any user accounts, such as adding or removing administrator privileges, or if you wish to add, edit or remove any user accounts, click Manage Mac OS X User Accounts; this opens the Accounts preference pane. For more on managing user accounts, see the Mac OS X help.

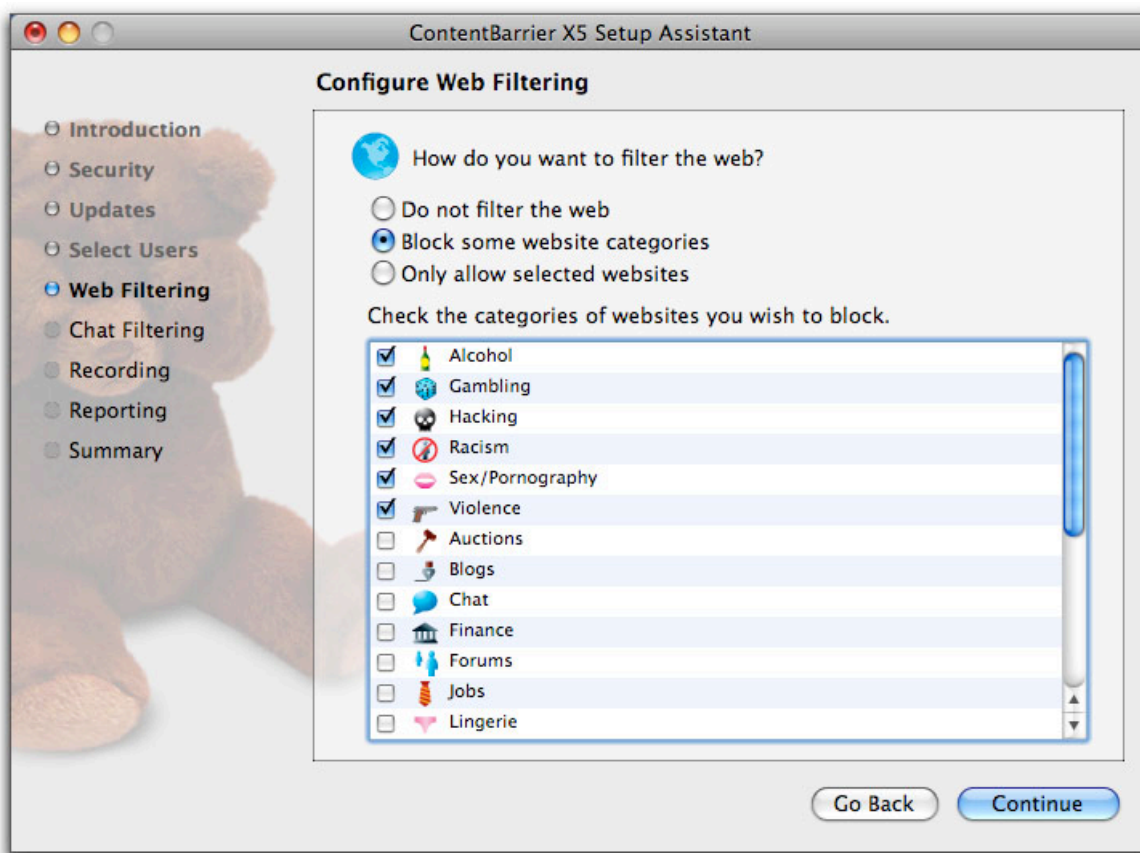
To configure users, check the boxes next to their names, then click Continue. In the assistant screens that follow, the same protection will be set for all users you select here. However, you'll be able to customize the settings for each person later. If you wish to use the Setup Assistant to configure settings for one user, you can do so, then run it again (by choosing Window > Setup Assistant) for another user.



## Web Filtering Setup

ContentBarrier X5 next presents you with three options for preventing the selected users from accessing certain web sites. They are:

- Do not filter the web, which allows the user to access all web sites;
- Block some website categories, which lets you block websites containing content belonging to a basic set of categories; and,
- Only allow selected websites, which gives you the opportunity to restrict the user's web use to only those "whitelisted" sites you specify.

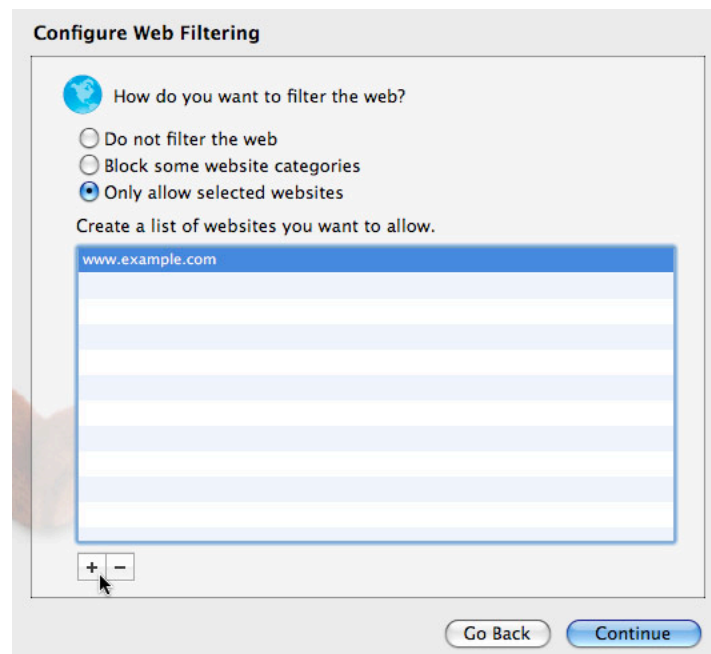


The default setting blocks web sites in the Alcohol, Gambling, Hacking, Racism, Sex/Pornography, and Violence categories, and you can add or remove categories by checking and unchecking their



boxes. Intego constantly updates its lists of suspect websites, so you don't have to surf the web to determine which sites fall in these categories; these updates are available in the ContentBarrier X5 filters that you can download and install using NetUpdate.

If you choose to only allow selected websites, your user(s) will be unable to access *any* website until you create a list of permitted sites. You add sites to the list by clicking the plus sign at the bottom of the screen, which puts "www.example.com" into the list.



To change this to the site of your choice, double-click on that line and type the site you want to allow. Note that all subdomains will be allowed, so allowed google.com also allows www.google.com, maps.google.com, and news.google.com. However, the opposite isn't true: if you allow only www.google.com, the user will be unable to reach google.com (without the www.)

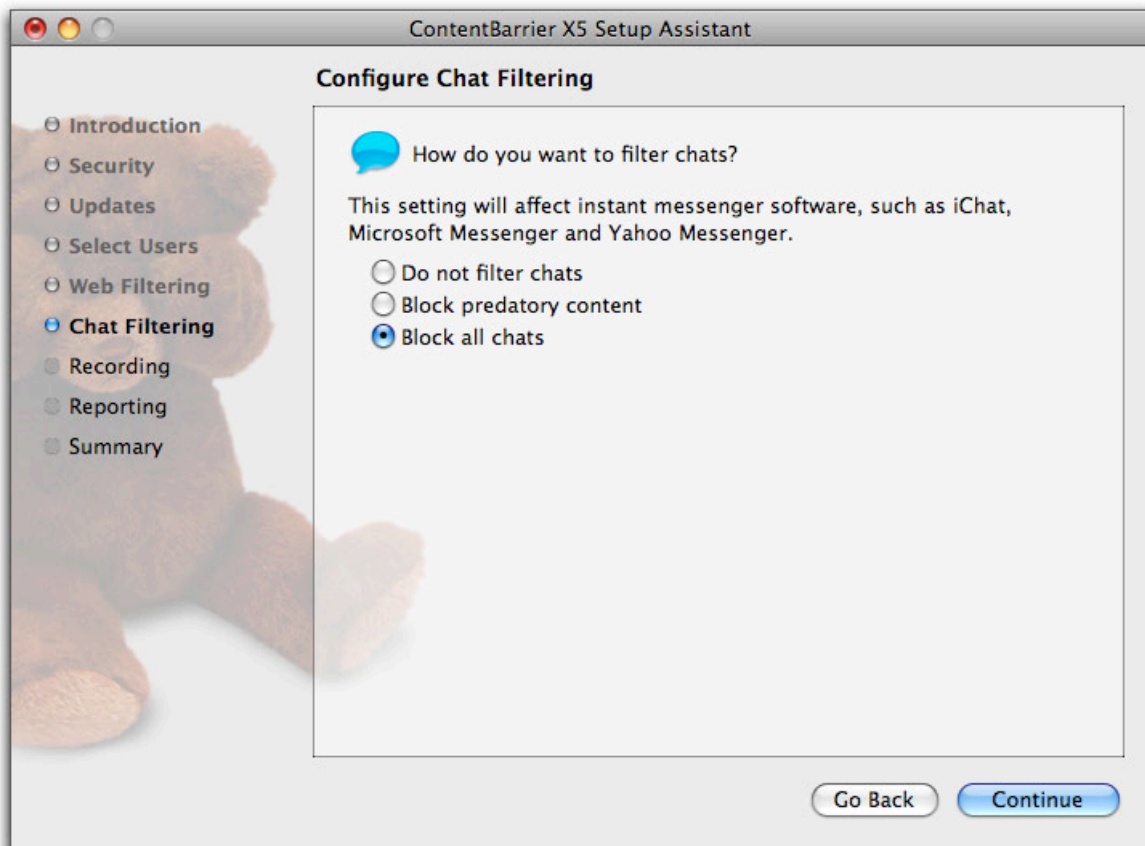
After you've confirmed the settings you want, click Continue to go to the next screen.





## Chat Filtering Setup

This screen lets you decide which chat filter settings you wish to use.



You have three options:

- **Do not filter chats:** This lets users chat with no restrictions.
- **Block predatory content:** This lets users chat, but enables ContentBarrier X5's AntiPredator function, which filters language deemed predatory in chat sessions. (We'll show you how to see and manage the list of "predatory" phrases in the later section, "Chat Filtering".)
- **Block all chats:** This prevents users from accessing any chat applications.

After you've confirmed the settings you want, click Continue to go to the next screen.



## Recording Setup

This screen lets you keep an eye on your user's activity, recording screenshots and keyboard activity to ContentBarrier X5's logs.



By clicking the first checkbox, you make ContentBarrier X5 take a screenshot of either the Main Window—that is, the frontmost one—or of everything visible on the computer, including additional monitors, if any, if you select All Screens from the popup menu. You can also decide how often these screenshots will be created, from one per minute to one per 999 hours.

If you click the Record Keyboard Activity checkbox, you keep track of all typing done by the user, in all applications. You can see these graphics and text files by looking at ContentBarrier X5's log, as is described in the section, “Using Logs”.

After you've confirmed the settings you want, click Continue to go to the next screen.



## Reporting Setup

This screen lets you determine how ContentBarrier X5 reports users' activities to you via e-mail or the web. Regardless of what you set on this screen, you can always monitor user activity by viewing ContentBarrier X5's log, as is described in the section, "Using Logs".



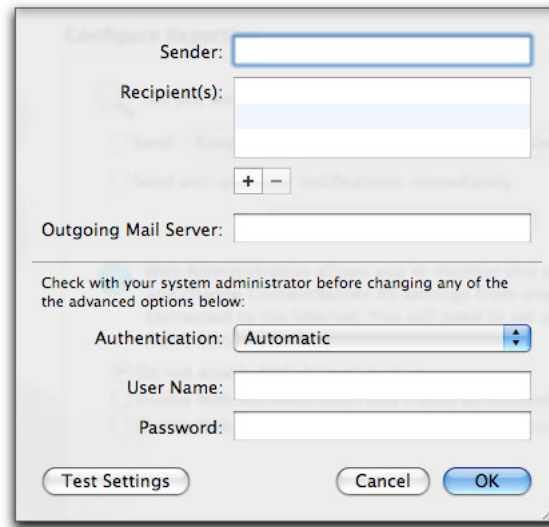
If you check the first checkbox, you'll receive reports of user activity by e-mail. Depending on what you choose in the first popup menu, your reports will be shown as "Simplified", "Complete", or "Compressed Complete". For details on these formats, see the section "Exporting Log Reports".

You can choose to receive these reports either daily (at the time at which you set up this option) or weekly (at the same time and day at which you set up this option).

If you check the second checkbox, ContentBarrier X5 will send you an e-mail whenever it detects predatory activity, according to its rules regarding text content.



But before ContentBarrier can send you any e-mail notifications, you must tell it what e-mail server to use, who should receive the alerts, and where they should come from. To create these settings, click Configure E-mail Settings....



In the Sender box, type the e-mail address you'd like these reports to appear to come from. In the next box, add recipients by clicking the plus sign, then typing an e-mail address. To delete any e-mail addresses, select them and click –.

In the rest of this window, you define how e-mails will be sent: the server, user name, password, and authentication scheme. You can probably find this information by checking the settings in your e-mail program; if not, ask your ISP or your computer's administrator.

Click OK to save these e-mail settings, which will return you to the window to configure Web Administration settings. If you haven't already created a free Intego Web Administration account, select "Enable Web Administration and create an account". You'll then be prompted to give an e-mail address to identify yourself, a password for the account, and verification of that password. (If you already have an account, select "Enable Web Administration using an existing account"; if you don't want to use Web Administration, select "Do not enable Web Administration".)



Web Administration allows you to monitor this computer's usage and change ContentBarrier X5 settings from any computer connected to the Internet. You will need to set up a free Web Administration account to use this feature.

☐ Do not enable Web Administration

☒ Enable Web Administration and create an account

☐ Enable Web Administration using an existing account

Email:

Password:

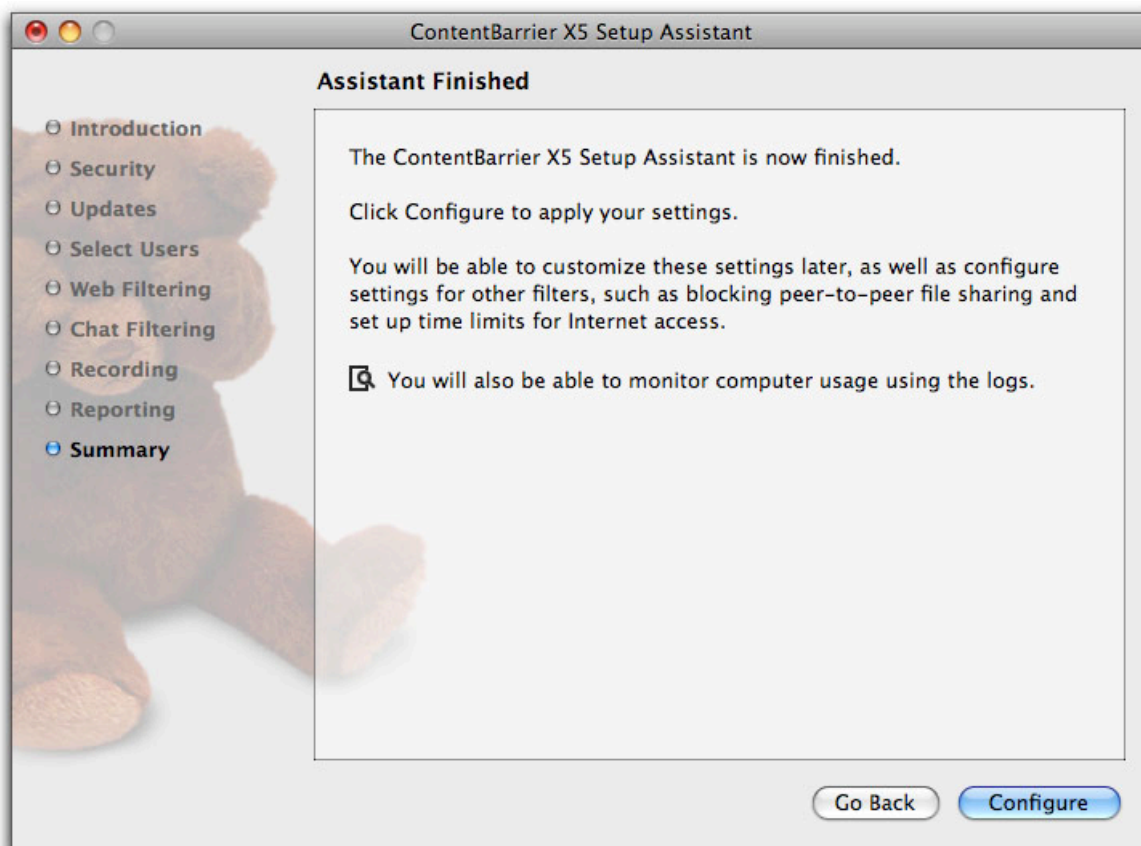
Verify:

When you click Configure, you'll get a brief message that the account is being set up. After you've configured reporting preferences to your liking, click Continue to finish the setup process.



## Finishing

You've now reached the end of the setup process, and will see a confirmation screen. Click **Configure** to apply the changes you specified and go to ContentBarrier X5's main screen.

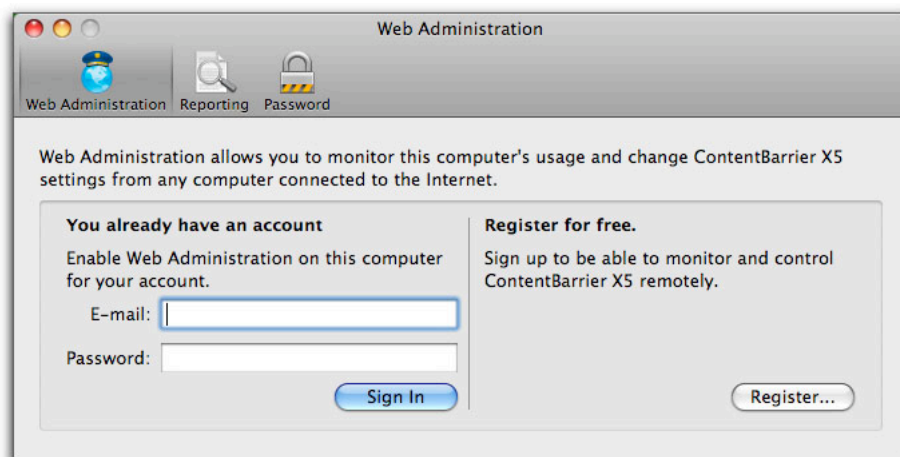


Congratulations! You've successfully told ContentBarrier X5 how to block users' access to parts of the Internet. If you wish to reconfigure your users, or configure new users by using the Assistant, you can do so at any time by choosing **Window > Setup Assistant** while ContentBarrier X5 is running.



## Setting Up Web Administration

ContentBarrier X5 includes a way to monitor Internet use on your computer even when you're far away, through a Web Administration interface that you can view from any web browser. First, you must set up a free account: if you haven't already set up an account in the ContentBarrier X5 Setup Assistant, choose ContentBarrier X5 > Preferences..., then click the Web Administration icon.



To set up your ContentBarrier X5 Web Administration account, click Register.... In the sheet that displays, enter your e-mail address, your password, then confirm your password. Click Create to create your account. If you have an account and need to sign in, enter your e-mail address and password, then click Sign In.

In either case, you'll see a screen telling you that web reporting is enabled, and offering you the opportunity to disable it, if you wish. To connect to your ContentBarrier X5 Web Administration web page, click Open Web Administration. Your web browser will take you to a login page, where you must enter the e-mail address and password you used to set up your account.

After logging into your Web Administration page, you'll see a log page, which displays information about your users and their activity. For more information about using online Web Administration



for ContentBarrier X5, click the Help button on that web page; you'll be taken to an online help page.

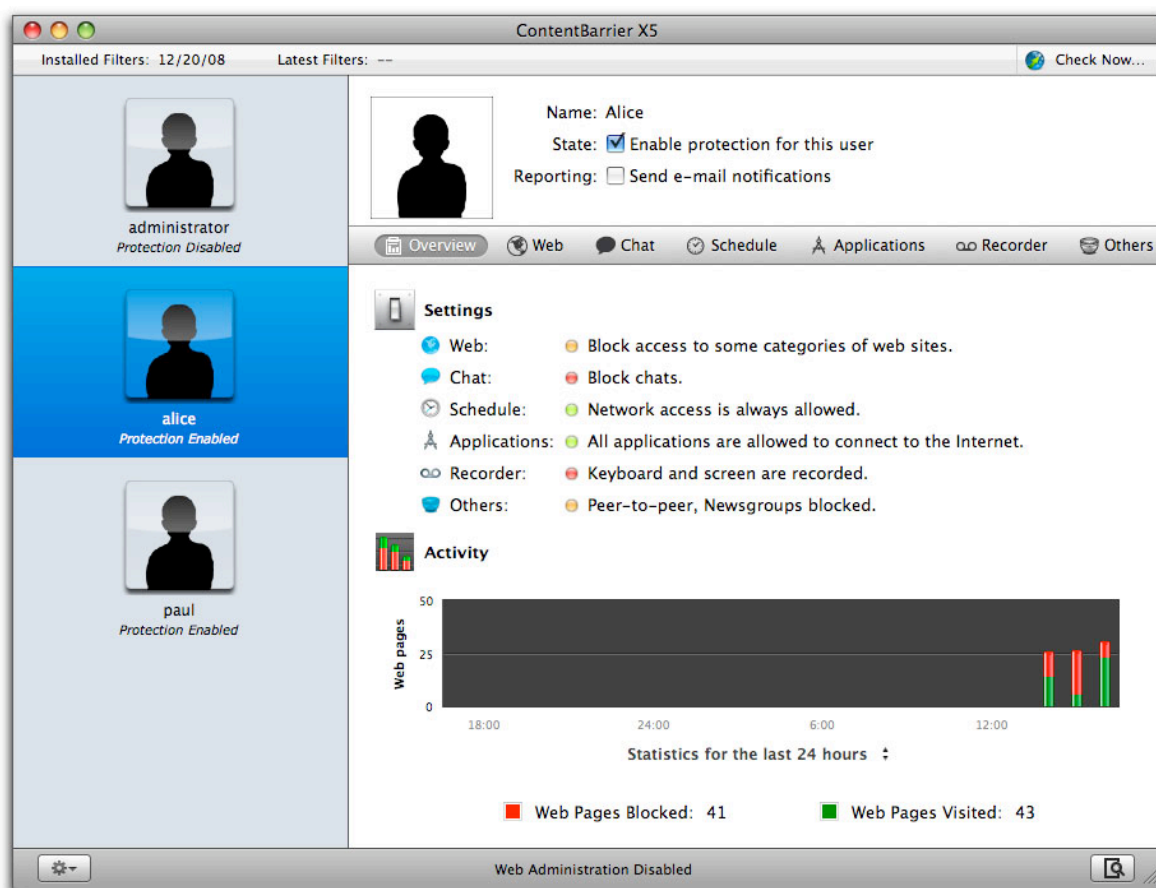




## Managing Users

When you set up ContentBarrier X5, you are its *administrator*, with access to all the controls that limit or grant permission to access the Internet. The people you are overseeing—whether children or employees—are called *users*. This section shows you how to create and delete users, and control how you and other administrators see users.

When you've finished running the Setup Assistant, and every time you launch ContentBarrier X5 thereafter, you'll see its main window.



At the left is a list of your users. If you click a user, the right-hand pane shows you which settings are applied to that user. Two checkboxes next to the user's icon give you quick access to frequently



used functions: the “Enable protection for this user” checkbox lets you turn ContentBarrier X5’s filtering on and off, while the “Send e-mail notifications” checkbox informs you of certain access attempts. (For more information about how to change which e-mail notifications you get, see the section, “Setting Log Preferences”.)

Mac OS X 10.5 (Leopard) and later offer a “Guest” account that you can configure in Mac OS X’s Accounts preference pane. If you activate the Guest account, any user can log in temporarily; they have standard access to your Mac, but when they log out, their user folder is deleted. This is great for when you have visitors who want to use your Mac temporarily.

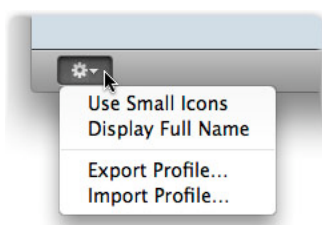
If you enable the Guest account in the Account preferences, ContentBarrier X5 will display this user in its Users list. You can apply settings to the Guest account, which will then apply each time someone logs in as Guest. If your children have friends who may use their Mac, you might want to use the same protection on the Guest account as on your children’s accounts.



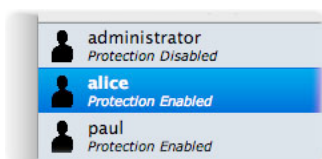
## Changing User Display

ContentBarrier X5 displays users by default as silhouettes with large icons in the left-hand column of the program's window. You can change this display, customizing each user's image, name and more.

If you click the Action button at the bottom of the user list, you can choose to display small user icons and/or full names. Choose either of these options to change the display.



Choosing small user icons is practical if you have many users, and using full names is helpful if you have several users with the same first name.

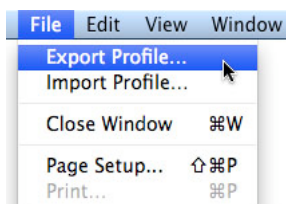


You can also make these changes from the View menu: choose View, then choose Use Small Icons or Show Full Name.

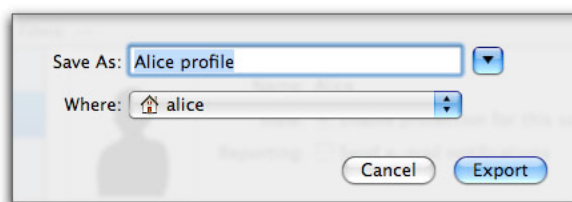


## Exporting User Profiles

After you create a profile for one of your users, you may want to apply the same profile to others. To do this, apply all the settings and filters you want to a user. Make sure you have selected that user in the ContentBarrier X5 Users list, then select Export Profile... under either the File menu or in the Action menu at the bottom of the window.



Give the profile a name and save it wherever you want.

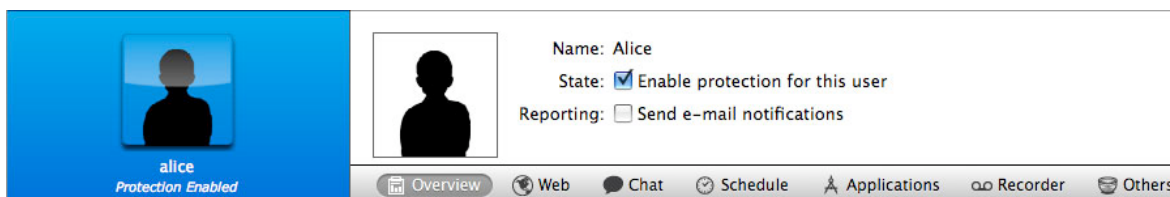


If you wish to apply this profile to another user, click that user's name, then select Import Profile... from either the File menu or in the Action menu at the bottom of the window. Locate the saved profile in the Open dialog that displays, then click OK. All the settings contained in this profile will be applied to the selected user. You can make changes to this user's settings, modifying the settings you imported from the saved profile, but these changes will not affect the saved profile. In this way, you can set up a standard profile for many users, then apply it to others. You can also set up a number of profiles based on the ages and maturity of your users, and using the import/export function, apply them to new users as needed.

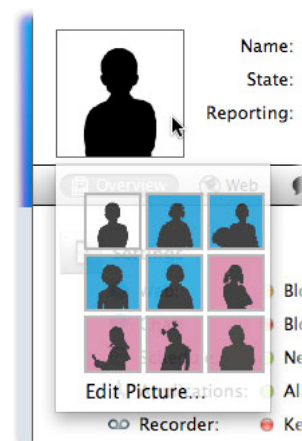


## Editing User Icons

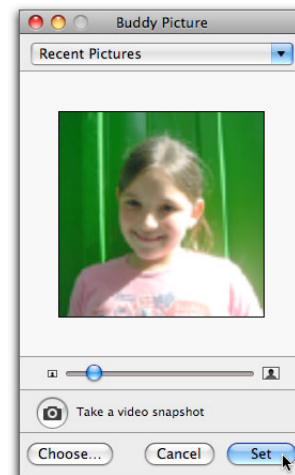
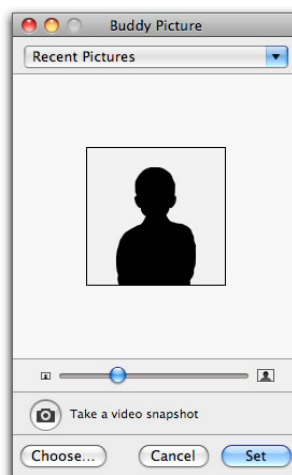
ContentBarrier X5 allows you to change the icons associated with your users, even letting you add their photos. To do so, click on a user in the Users list. The top section of the ContentBarrier X5 window shows you information about this user.



To change the user's icon, click it. Choose one of the default silhouettes, or choose Edit Picture to add a photo of the user.



Drag an image file to the image well, or click Choose to browse and find a photo. If your Mac has a built-in camera or you have an external camera, you can take a video snapshot. When you have added your picture, click Set to apply it, then click Save to save the changes you have made to your user's information.

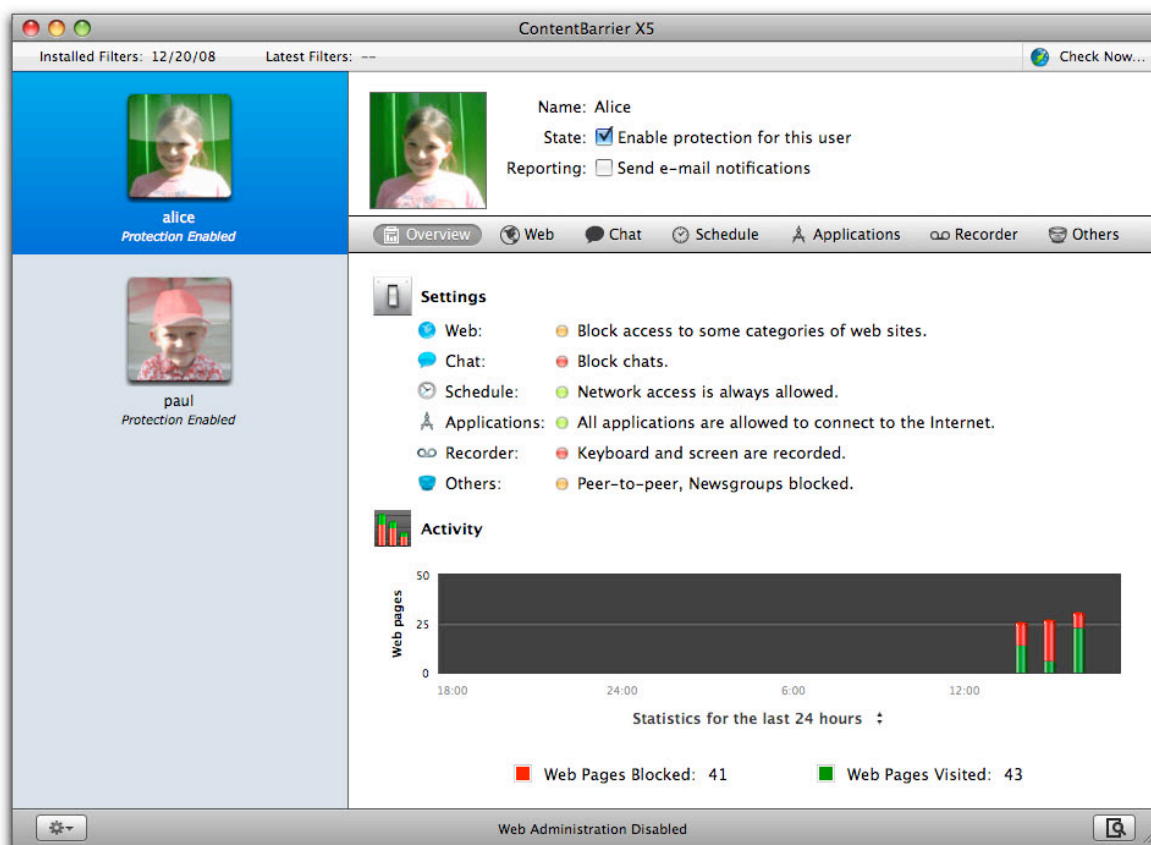


# **5 - Using ContentBarrier X5**



## Refining ContentBarrier X5 Configurations

You've seen how to use the ContentBarrier X5 Setup Assistant to create and configure your users, in the section "Setting Up ContentBarrier X5". You can also make changes to these configurations from ContentBarrier X5's main window, which provides access to more detailed configuration options, as well as an overview of your users' settings and a summary of their past activities.



The above screen displays whenever you launch ContentBarrier X5, and its contents correspond to the user selected in the Users list. It shows you the following:

- **User information:** At the top of the screen, you see the user's name, whether that user's Internet access is being filtered, and whether you're receiving reports on that person's Internet usage. You also see a silhouette for the user, or a photo, if you have set one.
- **Filter settings:** The middle section shows the current settings for each of ContentBarrier X5's filters. A colored dot next to each one gives you information about the type of filtering: green means there are no restrictions or monitoring, orange means there are some restrictions, and red means access is being blocked or tracked. Texts next to each filter icon give you more information about the filter and its settings.
- **Usage report:** The bottom section shows a usage report for the user, such as how many web pages they have visited and how many have been blocked. By default, the chart shows statistics from the past 24 hours, but by clicking on the text "Statistics for the last 24 hours" you can change it to 7 or 30 days. Note that the number of web pages displayed is usually more than the actual number of pages visited, because most web pages are made up of multiple elements, each of which comprises a request to a web server. Each request is counted.

You can also access the log for the selected user by clicking the Log button, which looks like this:



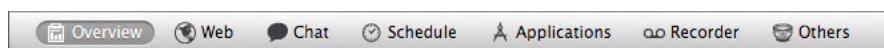
For more on logs, see "Using Logs" later in this manual.





## How Content Barrier Filters Internet Content

ContentBarrier separates its filtering functions into four categories: Web, Chat, Applications, and Other. In addition it has the ability to record users' actions without their knowledge ("Recorder"), and you can limit Internet access entirely according to a schedule that you set ("Schedule"). Each of these six tools is represented by a button underneath the user's information in ContentBarrier's main window.



Next, we'll discuss each of these tools in detail. You can return to the Overview screen at any time by clicking the Overview button.

## Web Filtering

As discussed in the "Web Filter Setup" section earlier in this manual, ContentBarrier X5 gives you three options to prevent the selected users from accessing certain web sites. They are: Allow access to all web sites, Block selected categories of web sites, and Only allow selected web sites. Each has its own screen of configuration options that resembles the screens you saw during the setup process, except with more options.

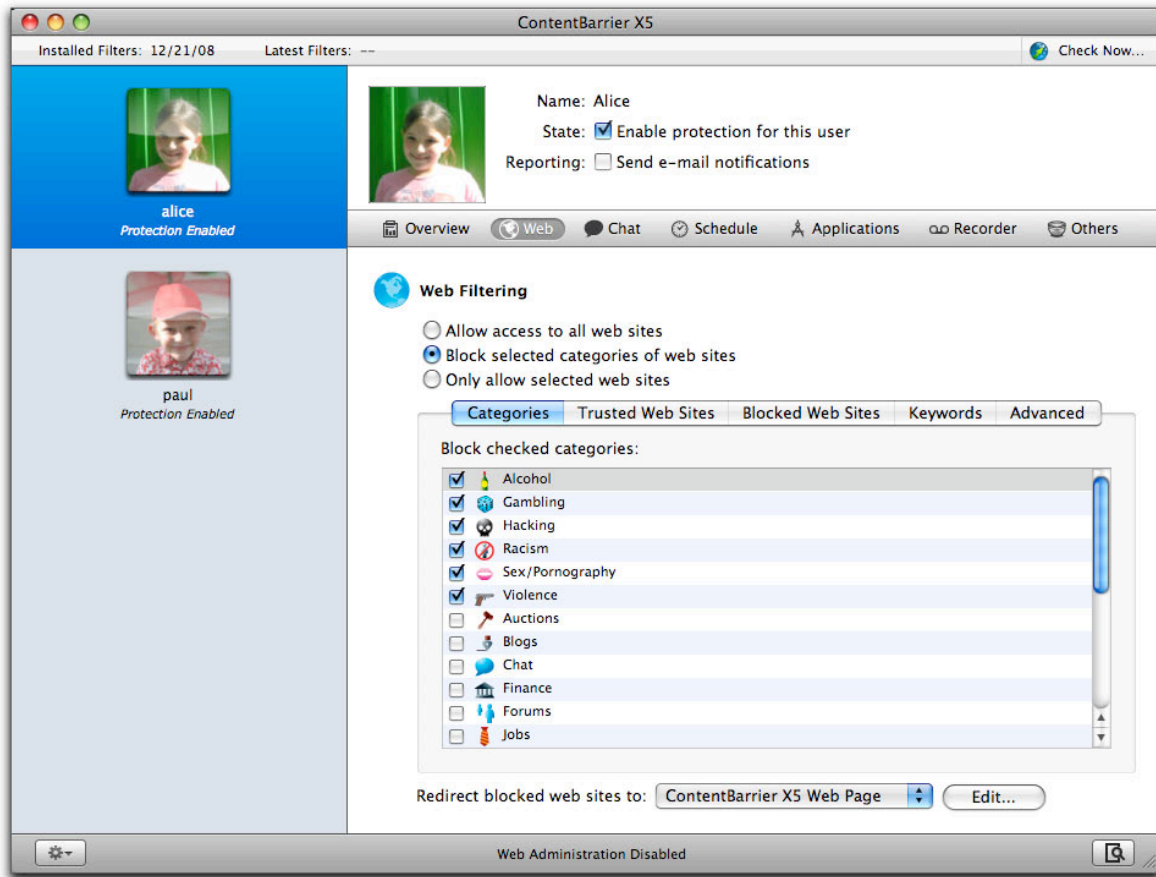
The **Allow access to all web sites** option is the simplest, as there are no settings: if you select this radio button, no web sites will be held back from the selected user.

The **Block selected categories of web sites** choice is ContentBarrier X5's default. It provides the most options, divided into five tabs: Categories, Trusted Web Sites, Blocked Web Sites, Keywords, and Advanced.

When you select this radio button, the Categories tab is selected and you see a list of web site categories with the Alcohol, Gambling, Hacking, Racism, Sex/Pornography, and Violence

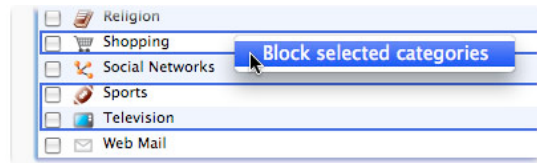


categories turned on—that is, blocked from this user. To prevent this user from browsing web sites in other categories, check their boxes; to allow access to categories, uncheck their boxes. (Filtering is done by analyzing keywords in web pages, as well as by a list of web sites maintained by Intego and updated regularly via NetUpdate.)



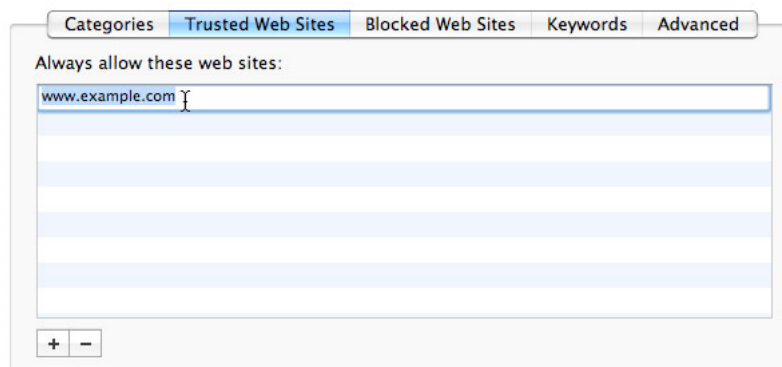
You can also change whether a category is blocked for this user by clicking a category while holding down the Control key, then choosing “Block selected categories” or “Allow selected categories” from the contextual menu. By clicking multiple categories while holding down the Shift or Command key, you can block or allow multiple categories at once.





Next, you can choose to allow your user to access certain web sites regardless of whether they fall into a forbidden category, by clicking on the Trusted Web Sites tab. To add a web site to this list, click the plus sign at the bottom of the screen, which puts “www.example.com” into the list. This is just a placeholder: to change it to the site of your choice, double-click that line and type the site for which you want to allow access.

Note that all subdomains will be allowed, so allowing google.com also allows www.google.com, maps.google.com, and news.google.com. However, the opposite isn’t true: If you allow only www.google.com, the user will be unable to reach google.com (without the www).



To remove a site from the list, click it and either press the Delete key or click the minus sign at the bottom left of the list.

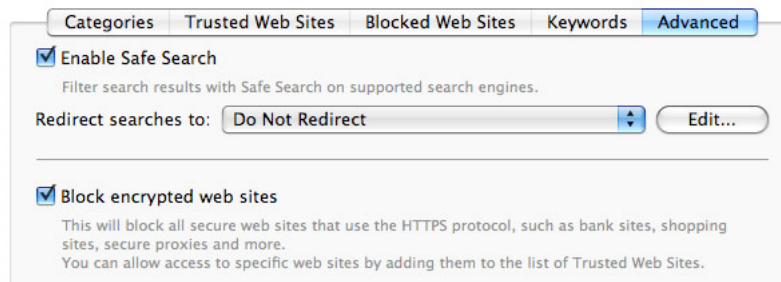
You set up Blocked Web Sites and Keywords in exactly the same way as you set up Categories, after clicking on the appropriate tab. They function as their names suggest:

- Users can never reach a site that you’ve listed on their “Blocked Web Sites”, even if it doesn’t fall into any forbidden categories.
- If you’ve created any entries in a user’s “Keywords” list, that user can’t reach any site on which that word appears.



In the event of a conflict—if you’ve listed the same web site listed in both the Trusted Web Sites and Blocked Web Sites lists, for example—ContentBarrier X5 will block the site.

Last on the “Block selected categories of web sites” method is the Advanced tab.



It has two settings:

- “Enable Safe Search”, which prevents the user from seeing questionable sites in the search results of several popular search engines, such as Google and Yahoo, which offer a Safe Search feature. You can go one step further and prevent your user from performing any kinds of searches on these sites by selecting a web page listed on the “Redirect searches to:” popup menu. (You can add your own web page—or a local file on your computer—to that popup menu by clicking Edit....)
- “Block encrypted web sites” prevents the user from reaching any site that uses the HTTPS protocol, as is common in sites where money or confidential information changes hands. Checking this box will effectively stop nearly all online shopping, although it will also block other sites.

The third option for controlling access to web sites is **Only allow selected web sites**, which has two tabs:

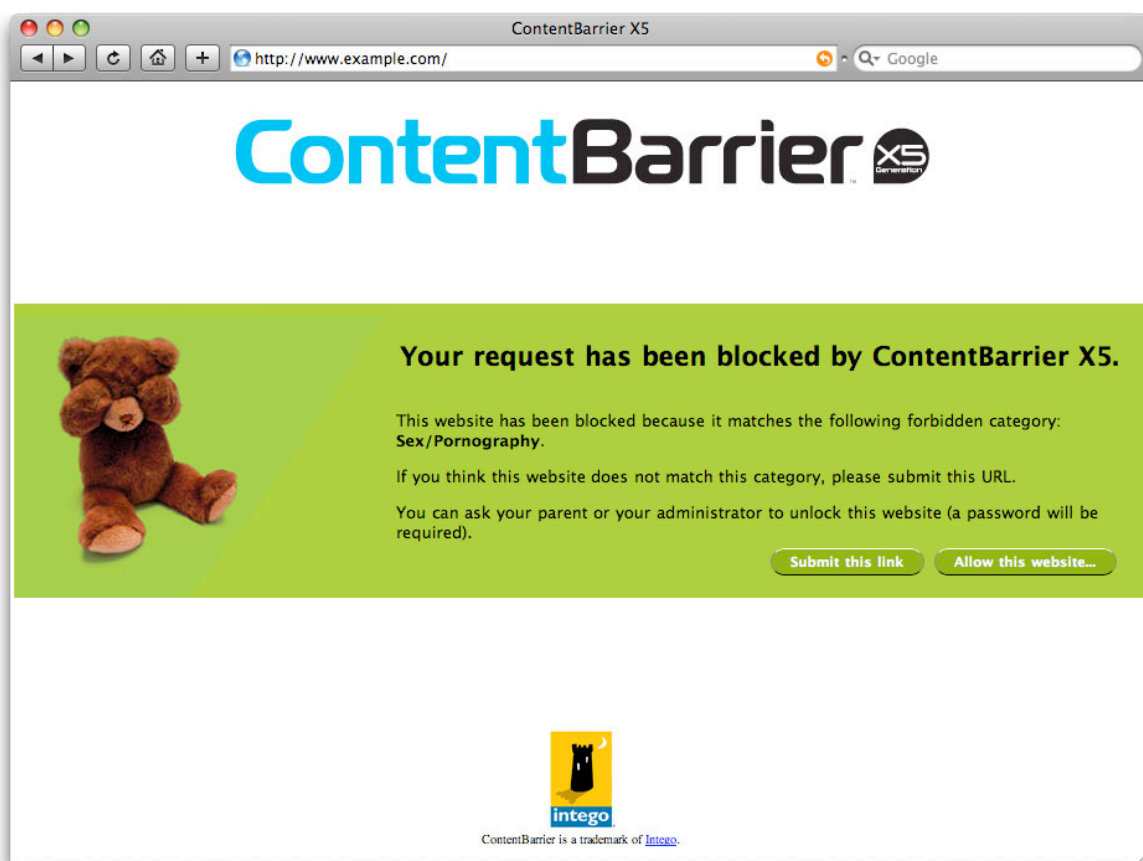
- A White List tab, which works in exactly the same way as the Trusted Web Sites list described above; and,
- A Searches tab, which lets you filter with Safe Search enabled, as described above, on search engines that offer this feature.



Regardless of how you decide to block (and allow) access to sites, the popup menu at the bottom of this window gives you a choice of what happens when your user attempts to reach a blocked site.

Redirect blocked web sites to:

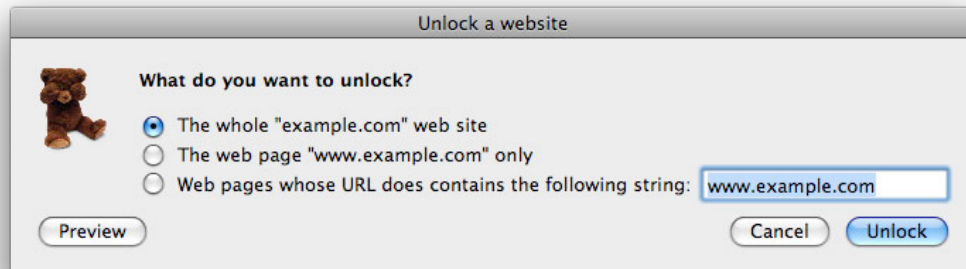
By default users will be sent to a web page that tells them why ContentBarrier X5 has blocked their access.



To give this user access to the page—if it was incorrectly blocked, for example—click the “Allow this web site...” button at the bottom of the page. A dialog box comes up with options to give access



to the entire domain (example.com in this case), just the specific web page the user attempted to access, or any web page containing a specified text.



Clicking either Preview or Unlock requires you to enter an administrator's password, preventing ordinary users from unlocking sites without permission. (The only thing a non-administrative user can do from here is click Cancel, leaving the site blocked.)

If you click Preview, a window appears that displays the requested page so you can check to see if it's safe; you'll see the choices given above. Unlock provides access to the page, site, or pages containing the specified text, depending on which of these you have checked.

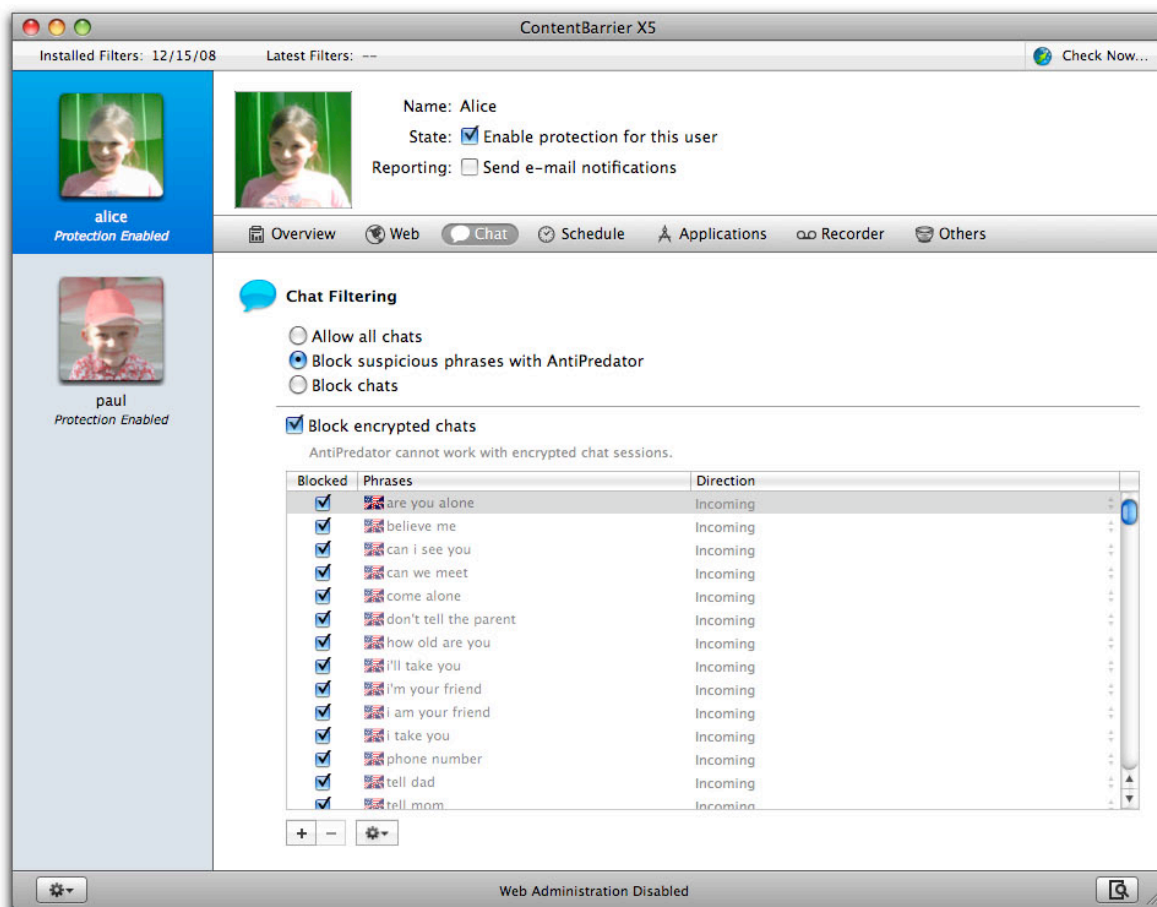
If you feel a web site was blocked unjustly, you can click [Submit this link](#), which will send a report to Intego. Intego will examine the page and see if we feel it should not be blocked.



## Chat Filtering

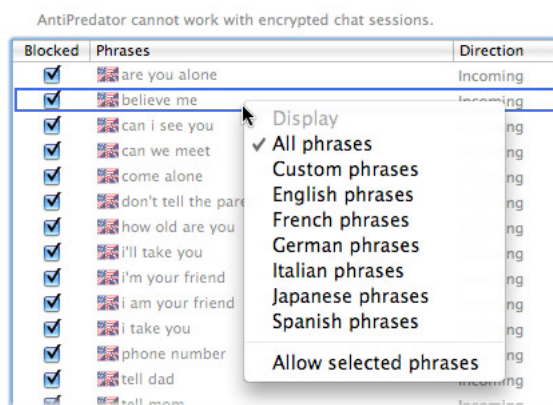
ContentBarrier X5 lets you filter or block chat sessions, and offers a powerful function to protect your children when using chat programs such as iChat, ICQ or AIM instant messaging software. The AntiPredator function filters chat texts for predatory language—that is, language asking for personal information about the user. This includes such questions, among others, as “are you home alone?” and “what is your phone number?”.

To enable chat filtering, select the user you wish to control in the left column, then click the Chat button. As with web filtering, you have three options: Allow all chats and Block all chats (which need no explanation), and Block suspicious phrases with AntiPredator, which we’ll examine.



ContentBarrier X5's AntiPredator comes with a set of basic text strings as filters for incoming data, and several languages are available. You can choose to display all filters, filters in a specific language, or just custom filters that you add to the list either by:

- Pressing your keyboard's Control key while clicking on a phrase, or,
- Clicking the Action menu (with a gear depicted on it) below the list of phrases.



By default, all the AntiPredator phrases are active when you turn on chat filtering. You can disable any of them if you wish by unchecking them; by selecting them and clicking the Action menu and choosing Allow selected phrases; or by clicking them while pressing your keyboard's Control key and choosing Allow selected phrases.

While ContentBarrier X5 contains an extensive list of text strings to be filtered, you can also add your own words and phrases. You could add, for example, your address or phone number, as well as any other personal information you feel should be protected.

To add a filter for either Incoming or Outgoing data, click the + button. A new line displays at the top of the filter list. Enter the word, phrase or sentence you wish to filter, and enable it if desired by checking the box to its left.

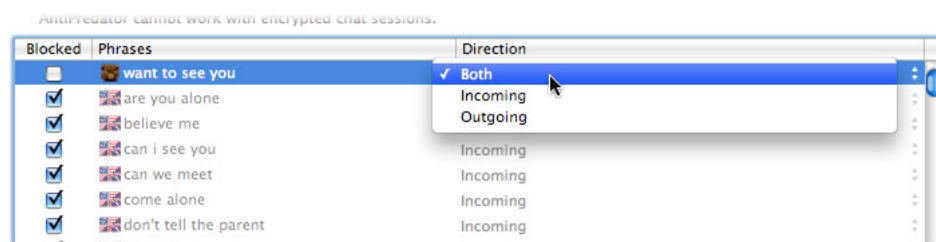




AntiPredator cannot work with encrypted chat sessions.

Blocked	Phrases	Direction
<input type="checkbox"/>	want to see you	Both
<input checked="" type="checkbox"/>	are you alone	Incoming
<input checked="" type="checkbox"/>	believe me	Incoming
<input checked="" type="checkbox"/>	can i see you	Incoming
<input checked="" type="checkbox"/>	can we meet	Incoming
<input checked="" type="checkbox"/>	come alone	Incoming
<input checked="" type="checkbox"/>	don't tell the parent	Incoming

Click the menu in the Kind column and select whether you want this text to be filtered for incoming chats, outgoing chats or both.

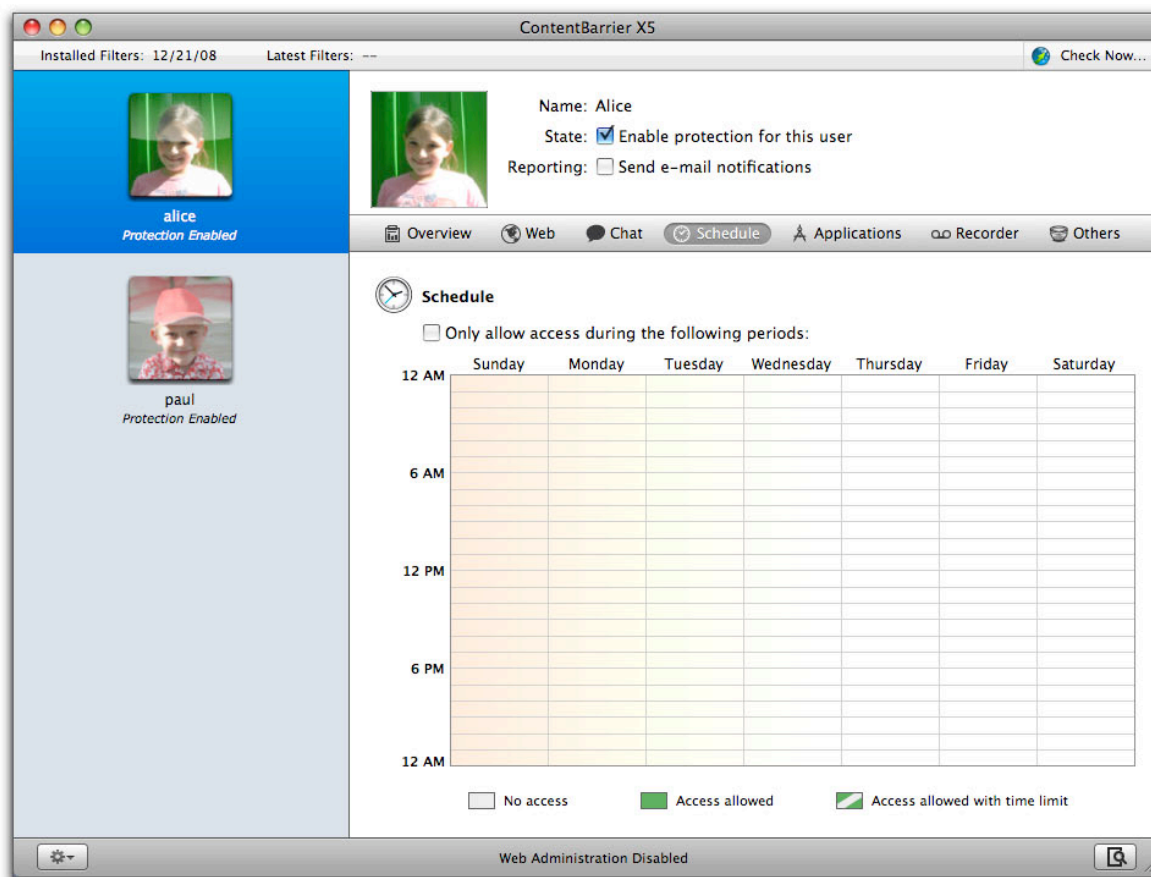


It is best to filter the shortest possible texts. ContentBarrier X5 looks for the **exact** text you have entered in the filter, and, if the user types it differently, it will not be blocked. For example, rather than enter “my phone number is 555-1999”, it is best to enter just the phone number.



## Using Schedules

ContentBarrier X5 lets you set a schedule for each of your users that allows them to access the Internet only on certain days and for a certain length of time. To access schedule settings, click the Schedule button in the ContentBarrier X5 button bar.

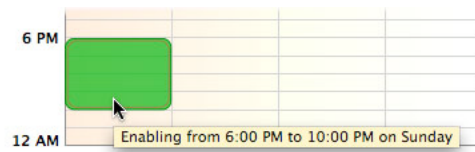


By default, all users are granted Internet access at all times. To restrict access to times you'll specify, click "Only allow access during the following periods:".

When you first see the timetable, all the cells are blank, representing that the selected user is not allowed to access the Internet at any time. To grant Internet access at given times, click the time

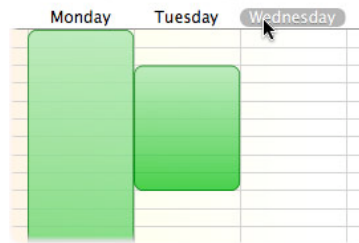


cells in the timetable—each cell represents one hour. You can click individual cells, or you can click and drag to cover longer periods.

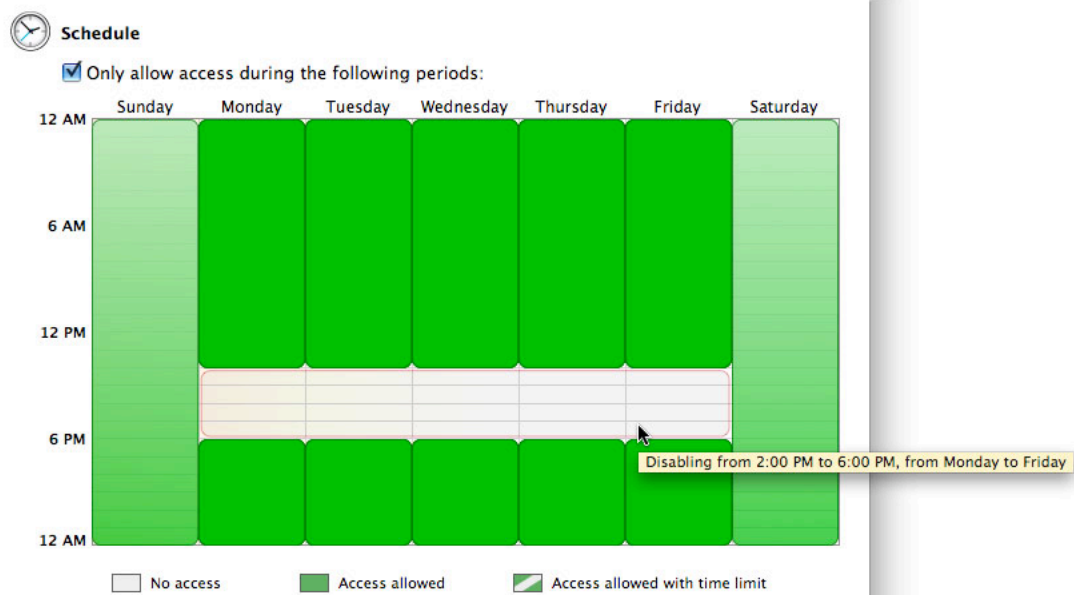


As you click cells, tooltips display showing the periods that you are enabling or disabling. You can allow or block access for any hour-long period on any day of the week in this manner.

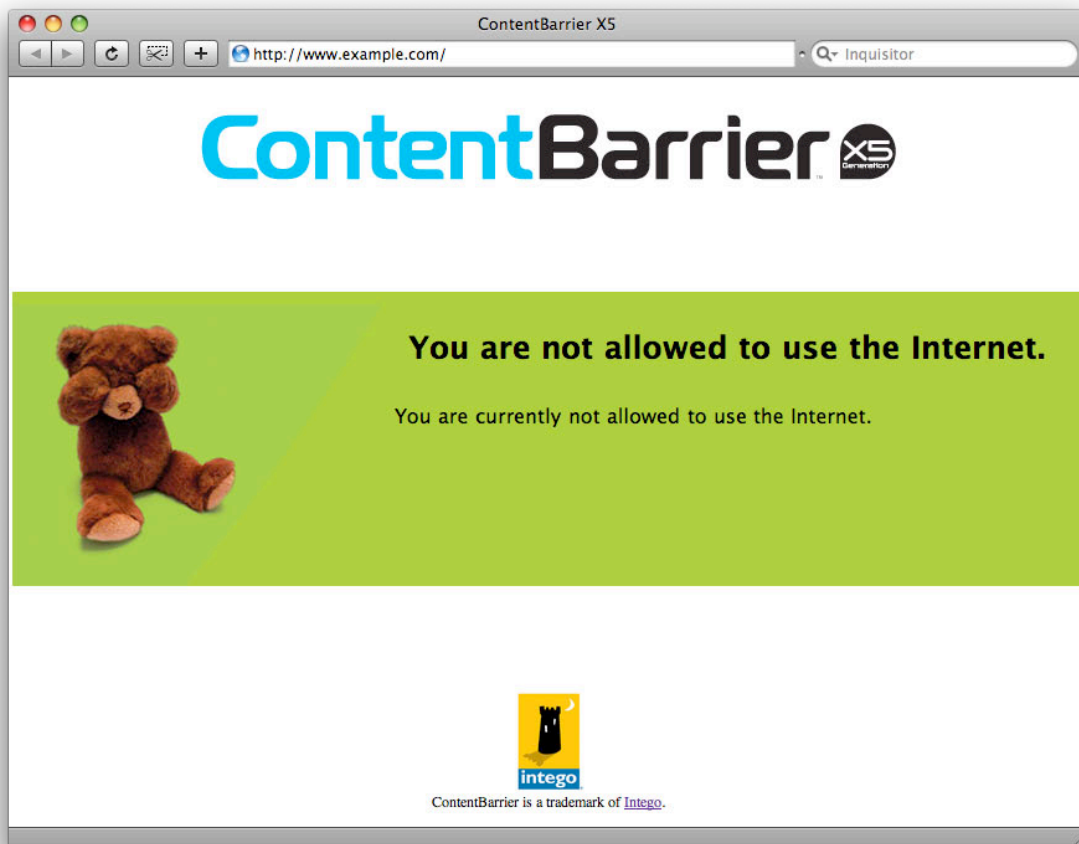
If you wish to allow or block access to an entire day, or if you simply want to reset access for a day to change settings from scratch, you can click the name of a day. This resets the entire day to green, allowing access for that day. Click again to block access for that day.



You can also click and drag in any direction to change cells. If, for example, you want to block access when a child comes home from school until suppertime, you would first enable all times, and then drag from 2pm on Monday to 6pm on Friday to disable those times.



A user attempting to connect to the Internet using a web browser during a forbidden period will see an alert:

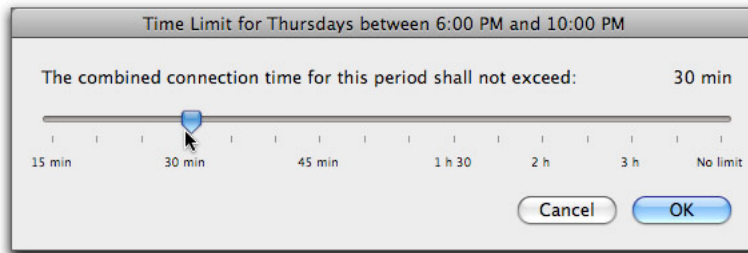


However, attempts to connect to the Internet with other applications might not cause an alert to be displayed; in some cases, access will simply be blocked. Some applications will display their own alerts, saying that they could not connect to the Internet.

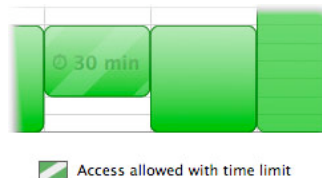
You can also allow Internet access for a limited period of time in between specific hours—for example, half an hour between 6pm and 9pm. To do so, first enable that time period by clicking and dragging to create a green access block; then, press the Control key while clicking that time period, and choose “Add Time Limit...”.



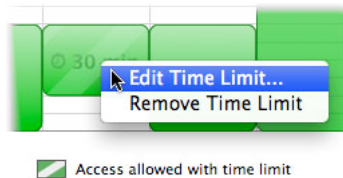
A dialog will appear, allowing you to set the amount of combined Internet access permitted during that period.



Drag the slider to the time limit you want to allow. After you click OK, your choice will appear as a striped green area on the time chart, specifying the amount of time allowed.



To change the amount of time available in a time limit, move the cursor over one of the sections with a time limit, hold down the Control key, and click. Choose “Edit Time Limit...” from the menu.

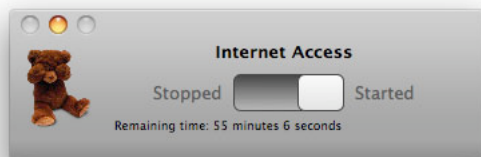


The time limit dialog displays again. Change the time limit by dragging the slider, then click OK to save your changes; alternately, click Cancel to keep the previous time limit.

To remove a time limit, move the cursor over one of the sections with a time limit, hold down the Control key, and click. Select Remove Time Limit from the menu. The time limit is removed.



When a user has a time limit, ContentBarrier automatically displays a small controller allowing them to start and stop their Internet access period. Since you may want your children to be able to use their Mac, but not the Internet, this allows them to control the periods when they can access the Internet. The controller looks like this:



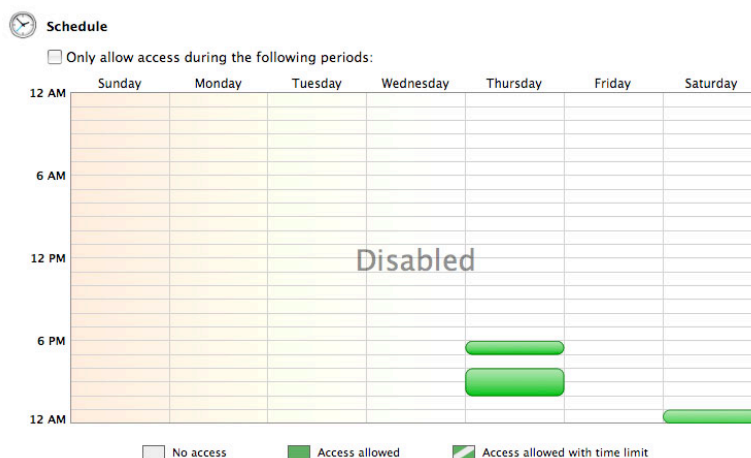
To start or stop a session, just drag the slider to Started or Stopped. Below the slider is the remaining time.

To remove the controller from the screen, you can click the yellow button; the controller is then minimized into the Dock:



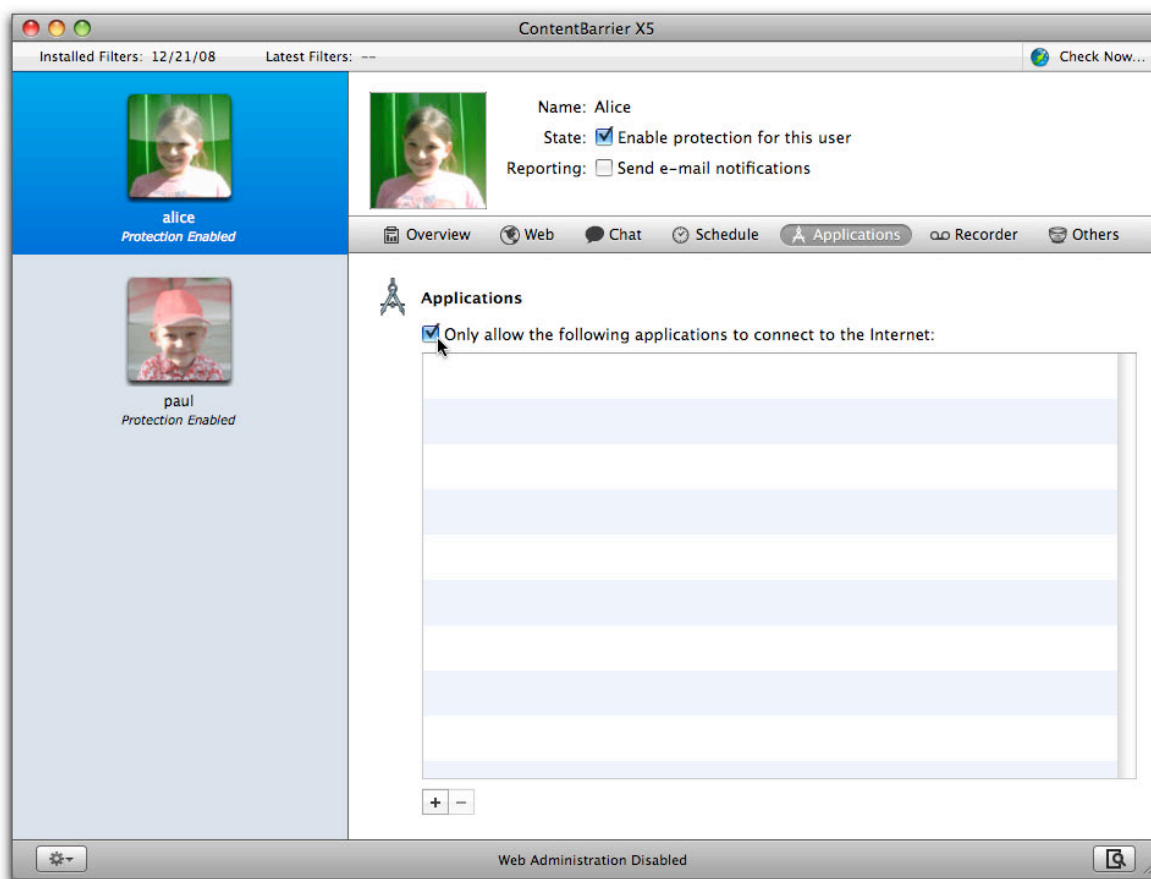
Clicking the controller's icon returns it to the screen so the user can start or stop their Internet access period.

To turn off all schedules and therefore allow Internet access at all times—with all of ContentBarrier X5's other filters in place, of course—uncheck the “Only allow access during the following periods:” box. If you've set any schedules, the word “Disabled” will appear in the middle of the time grid as a warning that those schedules won't be in effect.



## Application Filtering

ContentBarrier X5 gives you the option of only allowing users to access the Internet with specific applications. Rather than filter web access by category, for example, you can prevent a user from using any web browser. You can choose which applications can access the Internet; all other applications are blocked. To set up application filtering, click the Applications button on the ContentBarrier X5 button bar, then check “Only allow the following applications to connect to the Internet.”.



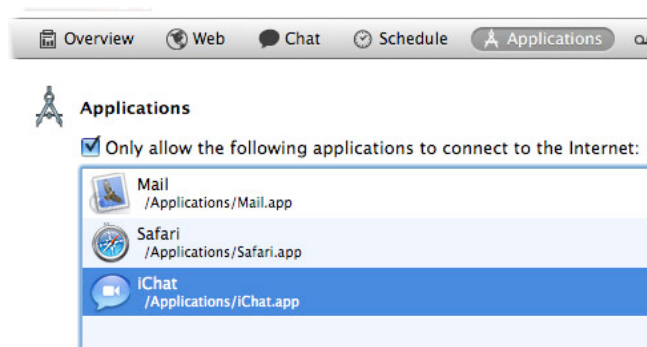
Application filtering will supersede all other ContentBarrier X5 filtering rules. If, for example, you do not add a web browser to the application list, then web filtering will have no effect: all web sites will be inaccessible, as no program that accesses them is available. However, ContentBarrier X5's other filtering rules apply to all applications added to this list. So if you choose to allow a user to





access the Internet with a web browser, then ContentBarrier X5's active web filtering categories will filter web sites visited.

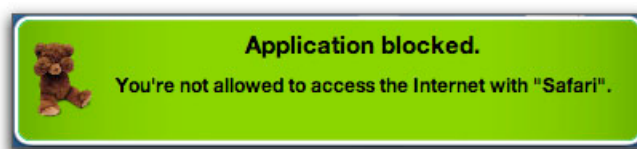
To add applications to the list, click the + button and navigate to your Applications folder. You can also drag applications from a Finder window into this list. As you add applications, they display in the list.



To remove an application from the list, click it to select it, then either click the – button or press the Delete key.

If, at any time, you want to stop using application filtering for a given user, simply click their name in the Users list, click the Applications button, then uncheck “Only allow the following applications to connect to the Internet:”.

When ContentBarrier blocks an attempt to access the Internet by a non-approved application, it displays a warning. You can change this behavior in the Reporting preferences, as is described in the section, “Setting Log Preferences”.



Note: some applications may use “helper” applications when they connect to the Internet. One example is Apple's iChat, which requires that iChatAgent access the Internet. If you add iChat to



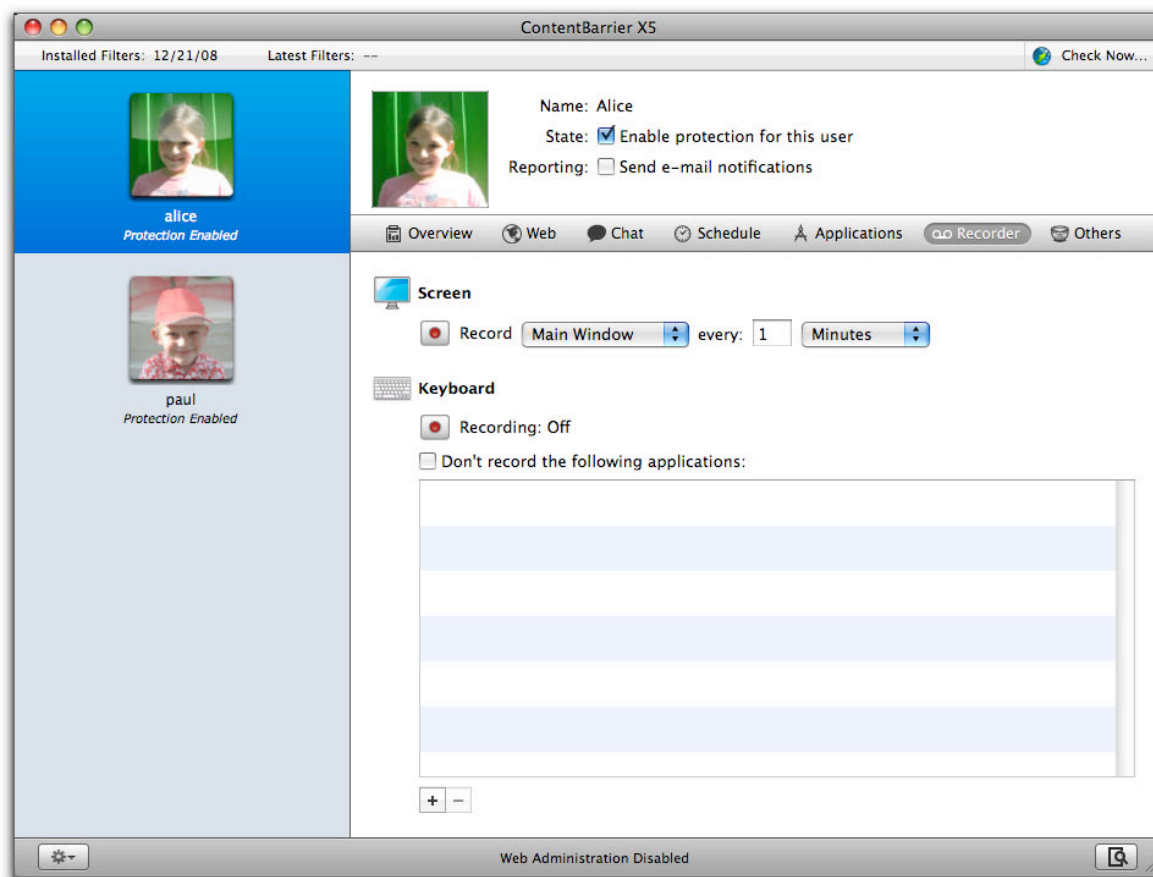
the list of allowed applications, this will not add iChatAgent. To add the latter helper application, go to your user's log, click Applications, then find which applications have been blocked. (There may be others.) Click the disclosure triangle next to an application or helper application you want to allow, then hold down the Control key and click on its name. A contextual menu displays with one option: Allow Application. Choose this and the application in question will be added to the list of allowed applications.

You may also want to check the logs from time to time; many applications that you might not expect need to connect to the Internet. Apple's Address Book, for example, makes an Internet connection, as does Help Viewer, the application that provides Mac OS X help. Your users will probably tell you which applications are blocked, but you can always see them, then allow them, from the log.



## Recording Internet Usage

ContentBarrier X5 lets you keep track of what your users have been doing by secretly taking pictures of what's on their screens, and recording what they type into a hidden log. To access the Recording controls, click the Recorder button in ContentBarrier X5's button bar.



To turn on screen recording, click the Record button underneath “Screen”. ContentBarrier X5 will then take a screenshot of either the Main Window that is, the frontmost one—or of everything on the computer, including a second monitor, if one is connected, if you select All Screens from the popup menu. You can also decide how often these screenshots will be created, from one per minute to one per 999 hours. (One reason to direct ContentBarrier X5 to take less-frequent screenshots is that a large number of graphics can take up a lot of hard disk space.)



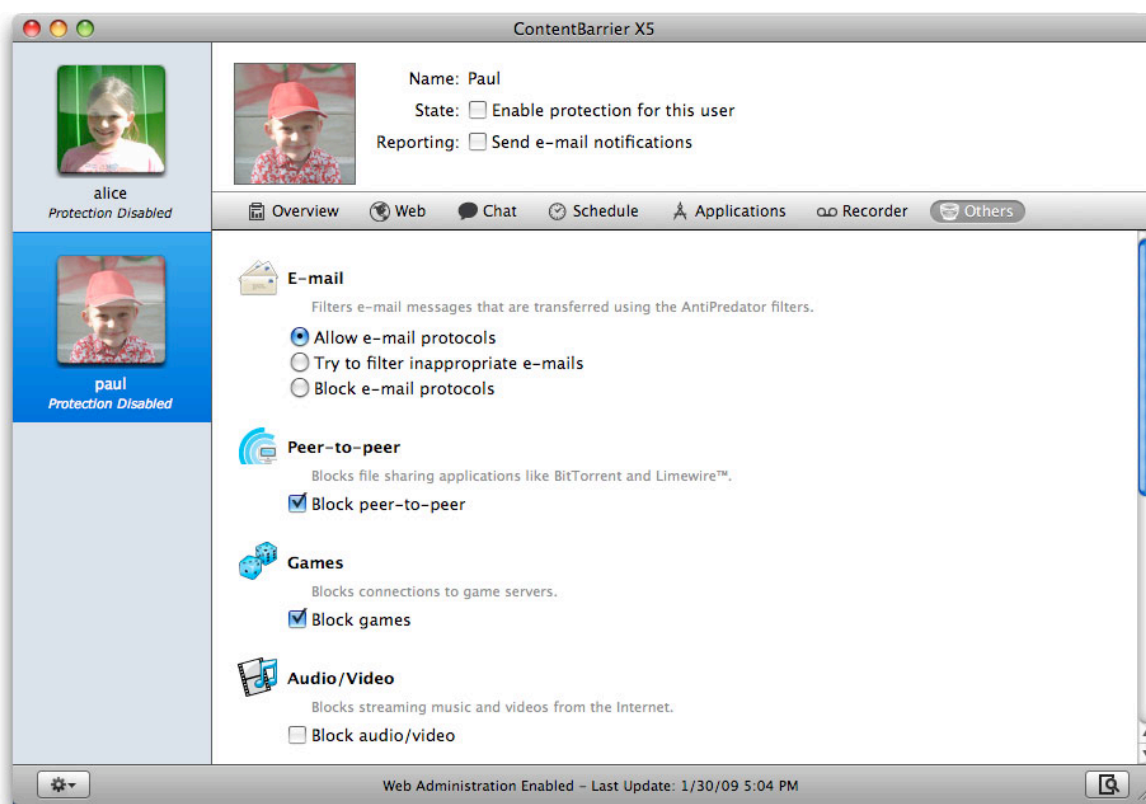
To record all typing done by the selected user, click the Record button underneath “Keyboard”. You can then exempt the keyboard from being recorded in certain applications by checking the “Don’t record the following applications:” box and adding those applications to the list by either clicking the + button and navigating to them via the Mac OS X dialog box, or dragging and dropping the application from the Finder into the list. (Note that all text typed is recorded, with the exception of passwords typed into a standard password text field.)

You can see these graphics and text files created by these recordings by looking at ContentBarrier X5’s log, as is described in the section, “Using Logs”.



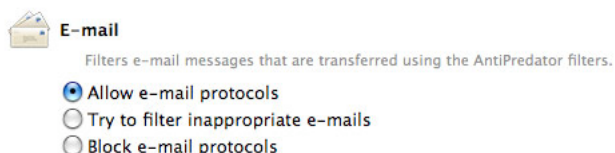
## Other Filtering Options

While chatting and web browsing are two of the most popular Internet activities, ContentBarrier X5 also provides filtering for other types of Internet accesses. To adjust setting for these, click the Others button.



## E-mail Filtering

ContentBarrier X5 allows you to apply its built-in content filters to e-mail messages that are transferred through any e-mail program.

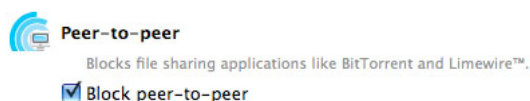


Your three options for e-mail filtering are:

- Allow e-mail protocols: all e-mail will be allowed through.
- Try to filter inappropriate e-mails: ContentBarrier X5 will scrutinize the contents of incoming and outgoing e-mail and block those that it believes are dangerous. ContentBarrier X5 uses the entire list of AntiPredator phrases for this filtering; even if you have only activated certain phrases in the Chat Filtering preferences, those choices do not affect e-mail filtering.
- Block e-mail protocols: forbids all e-mail from coming through standard e-mail programs. Note, however, that this setting will not affect messages delivered in other ways, for example on message boards or web sites.

## Peer-to-Peer Filtering

ContentBarrier X5 can filter peer-to-peer software, which is often used to share files over the Internet. To activate peer-to-peer filtering for a selected user, check the “Block peer-to-peer” box.



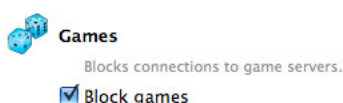
There are no options for peer-to-peer filtering; It is either active or inactive.



## Game Filtering

ContentBarrier X5 can filter common protocols used by online games such as World of Warcraft and Quake. To activate game filtering for the selected user, check the “Block games” box.

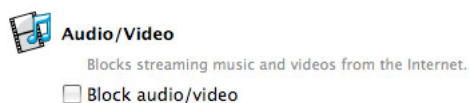
This setting will only block those games that access a server in a way that ContentBarrier X5 can identify: standalone games and those played within a web page probably will not be affected.



There are no options for game filtering; It is either active or inactive.

## Audio/Video Filtering

ContentBarrier X5 can filter streaming audio and video, which is audio or video content that is played back live, rather than after downloading. To activate streaming filtering for a selected user, check the “Block audio/video” box.



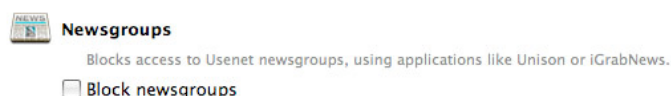
There are no options for audio/video filtering; it is either active or inactive.



## Newsgroup Filtering

ContentBarrier X5 can filter Usenet newsgroups, which offer discussion forums using a specific protocol and software. To activate newsgroup filtering for a selected user, check the “Block newsgroups” box.

This setting will only block newsgroups that are accessed through such software, and will not affect those that are displayed on a web page. However, you can block those web sites by checking the “Newsgroups” category in the Web filtering screen. (For more information, see the section, “Web Filtering”.)

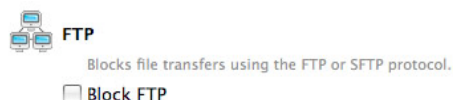


There are no options for newsgroup filtering; it is either active or inactive.

## FTP Filtering

ContentBarrier X5 can filter incoming or outgoing “file transfer protocol”, or FTP, which is commonly used for exchanging files among computers. To activate FTP filtering for a selected user, check the “Block FTP” box.

This setting will only block file transfers that take place using FTP’s default port 21 and SFTP’s default port 22, either through an FTP program or through a web browser pointed at URLs that begin with “ftp://”. It will not stop files transferred using other methods, such as HTTP download or peer-to-peer programs.



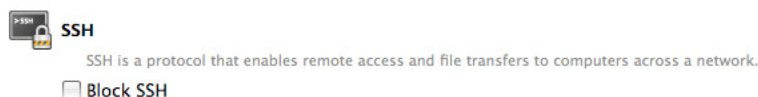
There are no options for FTP filtering; it is either active or inactive.





## SSH Filtering

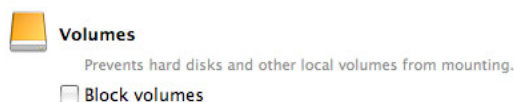
ContentBarrier X5 can filter incoming or outgoing “secure shell”, or SSH, which is commonly used for logging into remote computers. To activate SSH filtering for a selected user, check the “Block SSH” box. This setting will block communications that take place using SSH’s default port 22.



There are no options for SSH filtering; it is either active or inactive.

## Volume Filtering

ContentBarrier X5 can stop your users from mounting external hard drives, iPods, USB thumb drives, CDs, DVDs or other volumes, thereby preventing them from introducing new software or content onto the computer via hardware that’s directly connected to it. To activate Volume filtering for a selected user, check the “Block volumes” box.



There are no options for Volume filtering; it is either active or inactive.



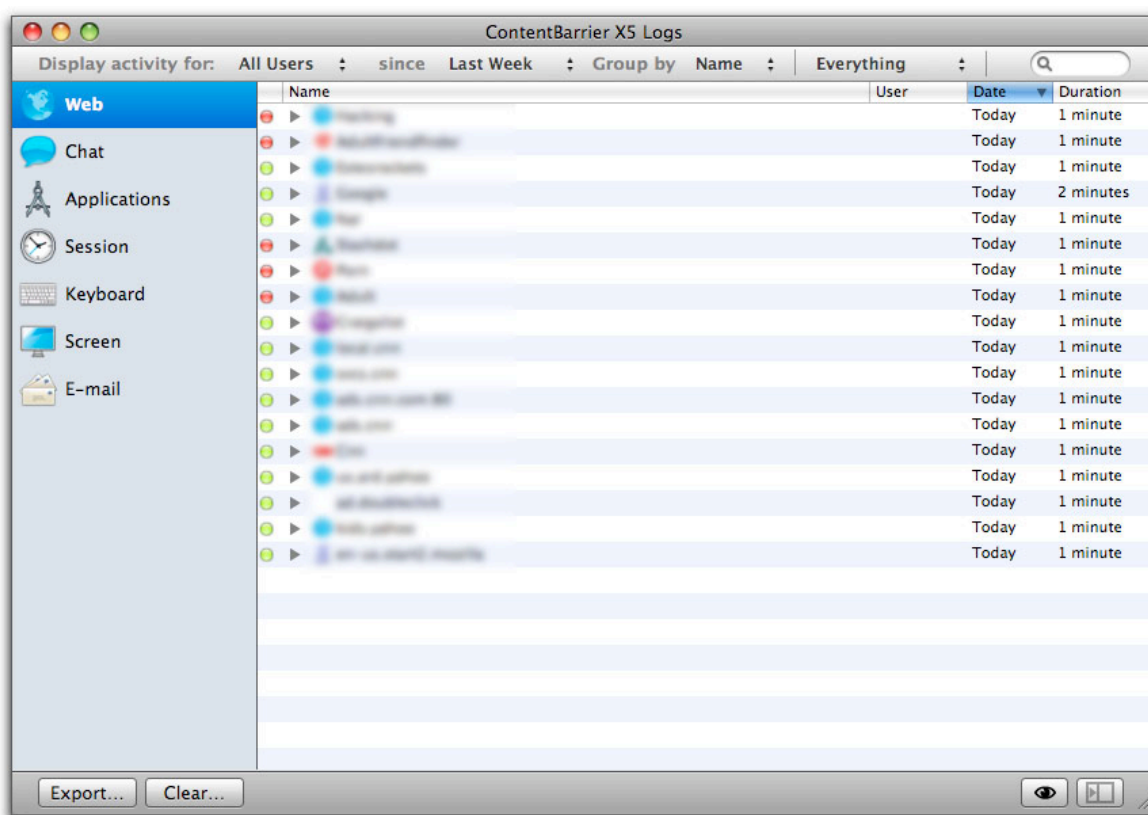
## Using Logs

ContentBarrier X5 provides a complete log of all Internet activity for each user. To view the log, either:

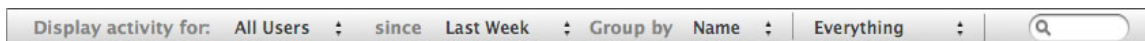
- Choose Window > Log;
- Press Option-Command-L; or,
- Click the Logs button at the bottom-right of the main screen.



When you first open it, the Log shows a record of all users' Web access attempts for the past week.



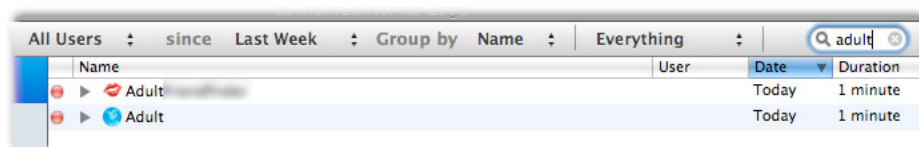
You can filter log entries by clicking the popup menus in the bar at the top of the window.



Criteria are:

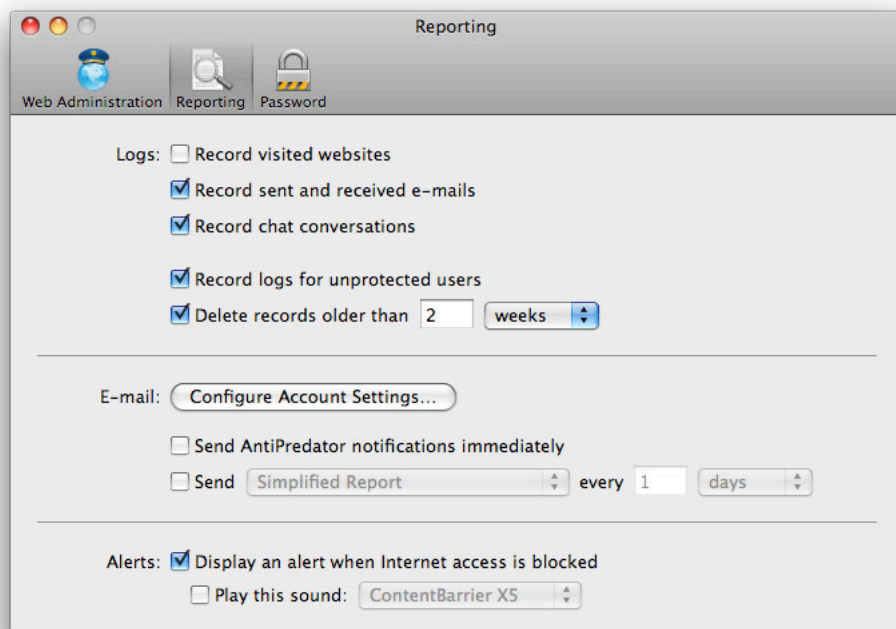
- “Display activity for”: Select the name of a specific user, or leave it on the default setting, “All Users”.
- “since”: Choose from Last Week, Last Month, or Forever.
- “Group by”: Makes ContentBarrier X5 reorganize list entries according to user name or the date of attempted Internet access.
- Whether to show all Internet accesses or only those that ContentBarrier X5 has blocked.

You can also search for specific log entries by typing the desired text in the search box at the top of the window; as you type, all entries disappear except for those matching your search. To show all log entries again, click the “X” next to the search string.



## Setting Log Preferences

Some of ContentBarrier X5's logging behavior is determined by settings in its preferences, which you access by choosing ContentBarrier X5 > Preferences..., or by pressing Command-, and then by clicking the Reporting icon.



The options are:

- Record visited websites: if this is checked, ContentBarrier X5 keeps a list of all visited websites in its log. Otherwise, ContentBarrier X5 only records those websites that are blocked or filtered.
- Record sent and received e-mails: records all e-mails sent and received by users.
- Record chat conversations: records all chats and instant message conversations.
- Record logs for unprotected users: keeps track of Internet usage by users whose access isn't restricted in any way. By default this is turned off.
- Delete records older than...: allows you to throw away logs beyond a certain age to preserve hard drive space or improve security. By default, logs are kept for two weeks.
- E-mail: the "Configure Account Settings..." button brings up a window in which you specify where you'd like e-mailed reports to be sent. Details on how to fill in this window are in the "Reporting Setup" section earlier in this manual.

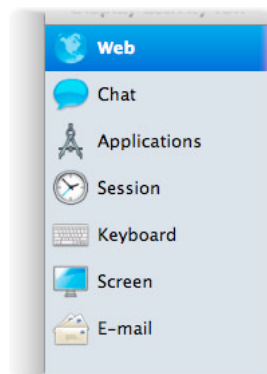


- Send AntiPredator notifications immediately: if you check this, ContentBarrier X5 will send you an e-mail whenever it detects “predatory” text strings in chat. (To learn how to manage the list of “predatory” phrases, see the section, “Chat Filtering”.)
- Send reports: when checked, you’ll receive a report of the type specified periodically, with the frequency you specify.
- Alerts: these two checkboxes let you determine whether users are alerted of blocked access with a floating alert, a sound, or both. (Users are also alerted to ContentBarrier X5’s activity by being redirected when they attempt to access a forbidden web site. For details on how to change this setting, see the section, “Web Filtering”.)



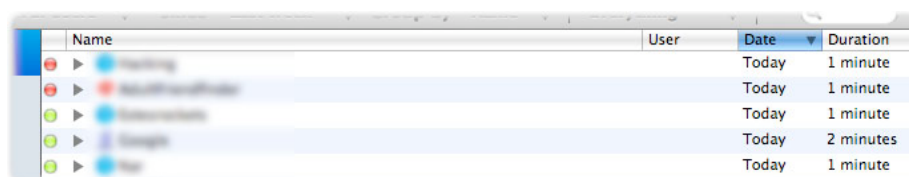
## Viewing Logs

The Log window's left-hand column lists types of log entries: Web, Chat, Applications, Session, Keyboard, Screen, and E-mail.



Clicking any of these log types displays only those entries. For example, clicking “Session” tells you of times when your user attempted to use the Internet, while Applications tells you which programs attempted to connect to the Internet.

Each line in the Log contains five different pieces of information: a colored icon, a disclosure triangle, the Name of the site attempted, the User who attempted to access that site, the Date of the attempted access, and how long the user spent on that site.

A screenshot of a log window showing a table of entries. The table has five columns: Name, User, Date, and Duration. The first column contains colored icons and disclosure triangles. The entries are as follows:

	Name	User	Date	Duration
Red icon, right-pointing triangle	facebook		Today	1 minute
Red icon, right-pointing triangle	facebook		Today	1 minute
Green icon, right-pointing triangle	facebook		Today	1 minute
Green icon, right-pointing triangle	Google		Today	2 minutes
Green icon, right-pointing triangle	Web		Today	1 minute

- **Icons** are either green (showing successful Internet access attempts) or red (showing attempts that were blocked). Red icons do not necessarily indicate that an entire page was blocked; they may display when parts of a page were blocked.



Name	User	Date	Duration
http://www.google.com		Today	6 minutes
http://www.google.com/development/	alice	Today	54 seconds
http://www.google.com/development/	alice	Today	54 seconds
http://www.google.com/development/	alice	Today	1 minute
http://www.google.com/development/	alice	Today	1 minute
http://www.google.com/development/	alice	Today	4 minutes
http://www.google.com/development/	alice	Today	1 minute

- **Name** refers to the domain of the site attempted (for web sites), without anything after the first “/”. To the left of the name is a **disclosure triangle** that you click to expose the specific pages on a given domain that one of your users attempted to reach. For example, if a user tried to reach both <http://www.example.com/index.html> and <http://www.example.com/games/shootemup>, both pages will appear grouped under example.com. These individual items are called Log entries.
- **User** shows who attempted to access the Internet. User names display after you click a disclosure triangle to display the different parts of a web site that were accessed or blocked.
- **Date** shows the date, relative to today, that the most-recent attempt occurred.
- **Duration**: Shows how long this Internet access attempt lasted.

By default, log entries are sorted according to the last attempted access. You can re-sort the log according to any of the five criteria by clicking the appropriate header at the top of the column. Click again, and the column re-sorts in the opposite order.

Name	User	Date	Duration
ad.doubleclick		Today	1 minute
ads.cnn		Today	1 minute
ads.cnn.com:80		Today	1 minute
Adult		Today	1 minute

You can preview log entry in several ways.

- Double-click a log entry;
- Choose a log entry by clicking it once, then press the space bar; or,
- Choose a log entry, then click the Quick Look button at the Log window’s bottom right.



ContentBarrier X5 will connect to the Internet to show you what the web page looks like. This preview is “live”—that is, you see the page as it exists right now.



It is possible, at times, that a web site might not be available; if so, double-clicking will not display the site. Also, some of the elements of a web page are merely parts of a page, and will display as such.

The icons at the bottom of this window control how you see these previews. They are:

- Left arrow: Go to the previous entry.
- Right arrow: Go to the next entry.
- Vertical line: A visual separator—does nothing.
- Diagonal arrow in a box: View the entry as a full-screen image. (Press the Escape key to dismiss the full-screen image.)
- Right arrow in a box: Export the image or text to a file.

You can dismiss this window at any time by either clicking the “X” in its upper-left corner, or by pressing the Escape key.



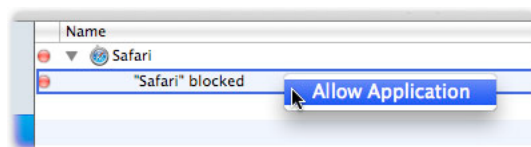


Clicking a disclosure triangle next to an application's name lets you view specific, individual entries in a popup window as described above, and with the same controls.

When viewing log entries for web sites, you can quickly allow or block web sites that are listed in the log by holding down the Control key and clicking a log entry. Select Trust Web Page or Block Web Page from the contextual menu that displays, and ContentBarrier X5 adds that site to the list of allowed or blocked sites.

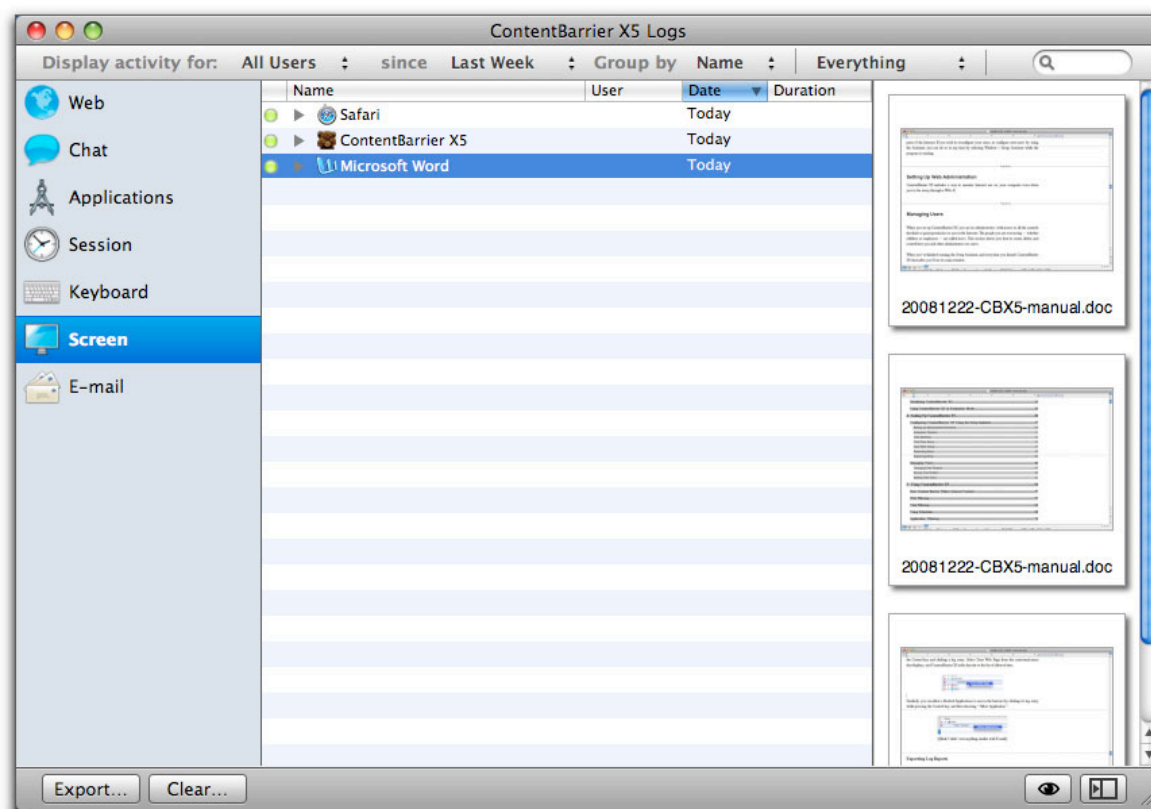


Similarly, you can allow a blocked application to access the Internet by clicking its log entry while pressing the Control key, and then choosing “Allow Application”.



## Keyboard and Screen Logs

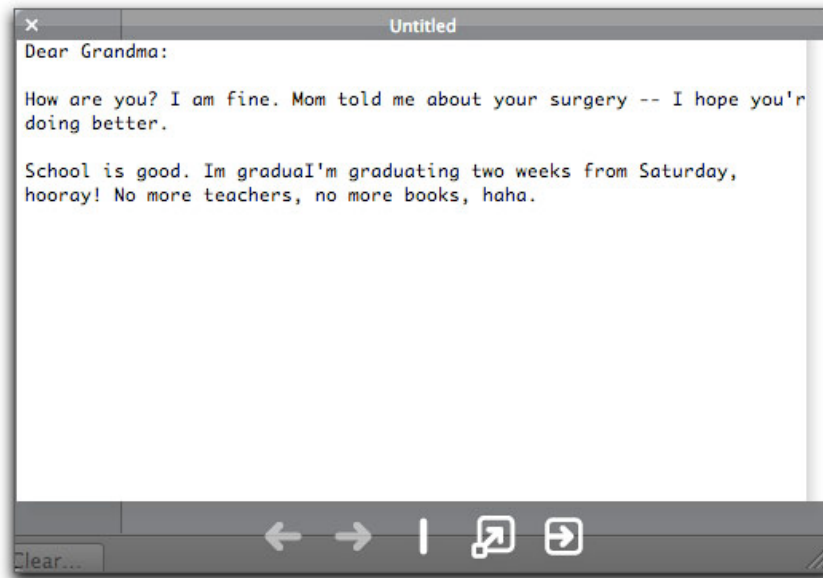
Two of the Log entry types—Keyboard and Screen—have extra information to help you see how your users have accessed the Internet. For the Log to track such entries, you must first turn on screen and/or keyboard recording: See the section, “Recording Internet Usage” for further information. (Note that all text typed is recorded, with the exception of passwords typed into a standard password text field.)



Keyboard and Screen Log entries are grouped according to the application being used so, for example, all text typed into Microsoft Word appears under a “Microsoft Word” listing. Clicking the name of any application shows you all the activity that occurred while that application was being used in the right column. You can hide this column at any time by clicking the bottom-right button.

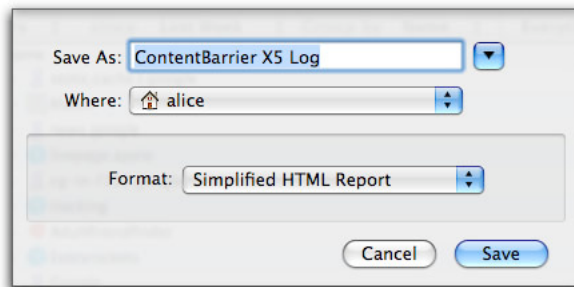


As with other log entries, you can see a visual snapshot of the user's actions by double-clicking an application, or selecting it and then clicking the Quick Look icon in the bottom right corner. A quick look window appears, letting you page through all screen shots or keyboard captures made while that application was being used.



## Exporting Log Reports

You can export ContentBarrier X5 logs as HTML files to view them later in a web browser, or as text files. To do so, select one or several log categories (Web, Chat, Applications, etc.), then click the Export... button at the bottom left of the Log window. A sheet displays where you choose a name for the log, a location to save the file, and the format.

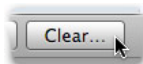


ContentBarrier X5 lets you choose from three types of reports when you export logs. They are:

- **Simplified HTML Report:** Shows global elements from the selected categories; what you see before clicking a disclosure triangle. For example, for web sites, only the name of the site is shown, not the actual URLs of pages visited or blocked. For keystroke recording, only the name of the application is shown, and not the actual text recorded.
- **Complete HTML Report:** Shows all ContentBarrier X5 activity in detail. All selected categories show all activity.
- **Complete Plain Text Report:** Shows the same information as the Complete HTML Report, but in a format that's useful for further analysis (in, for example, a spreadsheet or custom-programmed application).

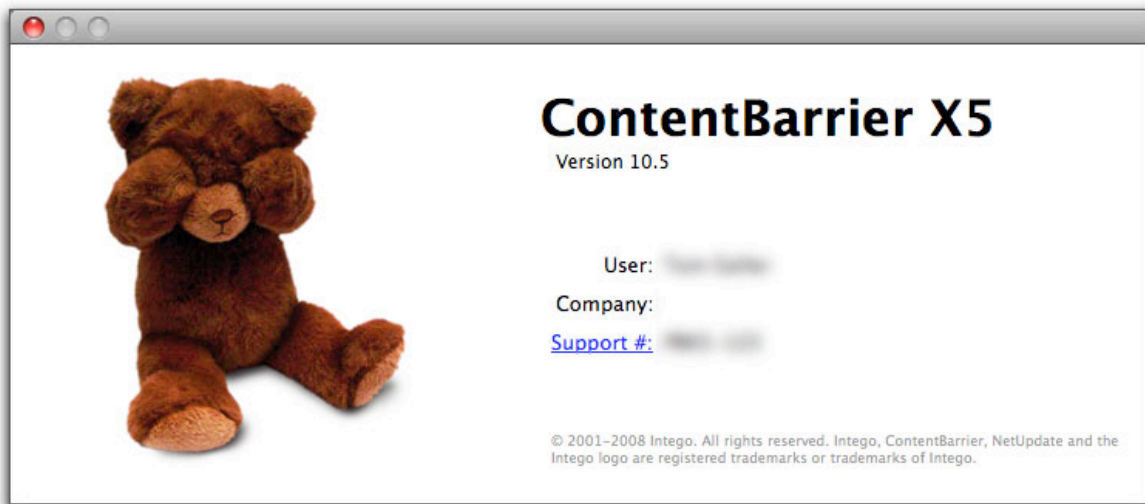
Click Save to export the log in the selected format.

To erase all information stored in the log for all users, click the Clear... button at the bottom of the Log window.



## About ContentBarrier X5

If you select About ContentBarrier X5 from the ContentBarrier X5 menu, the About... window gives information about ContentBarrier X5, such as the version number, your support number (a number you need for technical support), and a clickable link that creates an e-mail message to Intego's technical support.



# 5 - Technical Support



Technical support is available for registered purchasers of Intego ContentBarrier X5.

***By e-mail***

support@intego.com: North and South America

eurosupport@intego.com: Europe, Middle East, Africa

supportfr@intego.com: France

supportjp@intego.com: Japan

***From the Intego web site***

[www.intego.com](http://www.intego.com)

