K9 Web Protection

User Manual

Blue Coat

Contents

Chapter 1

K9 Web Protection Overview

Blue Coat® K9 Web Protection is a content filtering solution for your home computer. It implements the same enterprise-class web filtering technology used by Fortune 500 companies around the world, wrapped in a simple, friendly, and reliable user experience.

Blue Coat's unique web filtering technology divides Internet content into more than 55 distinct categories. These categories—and their associated websites—are stored in the Blue Coat database, which maintains and updates almost 15 million website ratings and domains. A website will fall into one or more of these categories, based on the content of the site. To meet your particular needs and preferences, you can configure the software to block or allow specific categories.

K9 Web Protection offers:

- **Service-based filtering—**Blue Coat's filtering database operates as a service. It receives and rates over 50 million requests every day, making it the most accurate content filtering database available and ensuring that you are protected against the ever-growing number of inappropriate websites. Plus, with no database to download, K9 Web Protection won't slow down your computer.

- **Dynamic Real-Time Rating™ (DRTR)**—Blue Coat's patent-pending DRTR technology automatically determines the category of an unrated web page without human intervention. Using a method of statistical analysis and artificial intelligence to rate new or previously unrated web pages, DRTR only provides a rating when it is confident that it has reached an accurate conclusion. Unlike other filtering solutions, K9 Web Protection ensures the highest level of protection by building the most relevant ratings database available. Its effective coverage reaches more than a billion web pages.

- **Automatic updating**—Automatic updates of the K9 Web Protection application ensure that you are always protected by the latest features.

- **Efficient caching**—K9 Web Protection uses Blue Coat's unique caching technology, so your Internet experience is always as fast as possible.

System Requirements

Operating System:	Microsoft Windows XP or Windows 2000
Processor:	233 MHz or higher Pentium-compatible CPU
Memory:	At least 64 megabytes (MB) of RAM
Hard Disk:	25 MB free space
Other:	Internet connection

Chapter 2

Getting Started with K9 Web Protection

Before you begin the installation process, please make sure your system meets the requirements listed on page 5 of this manual.

Downloading and Installing K9 Web Protection from the Internet

1. Point your web browser to www.k9webprotection.com

2. Click on the [Get K9 Now] link.

3. Fill out the simple form to complete the license request and click [Request License].

4. Your K9 Web Protection license will be emailed to you shortly. You will need this key to install the K9 software.

*Note: Your email account (and/or your Internet Service Provider) may be set to disregard unwanted email (known as "spam"). **To ensure that you get your K9 license email**, configure your mail account **to accept messages from k9support@bluecoat.com**. If you do not see the K9 license email shortly after requesting your license, check your email account anti-spam settings, and check your "junk" or "anti-spam" folders to see if the K9 license email was routed there.*

5. Navigate to the **Download Software** page to begin downloading the software. You can also use the download link in the e-mail containing your license key.

6. You will be asked whether you want to run or save the file `k9-webprotection.exe`. Click [Save] to save the file to your hard drive. K9 is a small file and downloads almost instantly for most users.

Note: Make sure you write down the path and folder name as you will need it later.

7. Once the file download is complete, open the folder where you saved the file. Double-click on `k9-webprotection.exe` to continue the installation process.

8. The Setup Wizard will launch, guiding you through the installation process.

9. You will be prompted to accept the K9 Web Protection license agreement. If you agreed and would like to proceed, Click [I Agree].

10. You will then be prompted for the install location. K9 Web Protection defaults to `C:\Program Files`. (If you want to install the software in a folder other than this one, please type it in now.)

11. Copy your K9 Web Protection license from the email and paste it into the **License** box. Then click [Next].
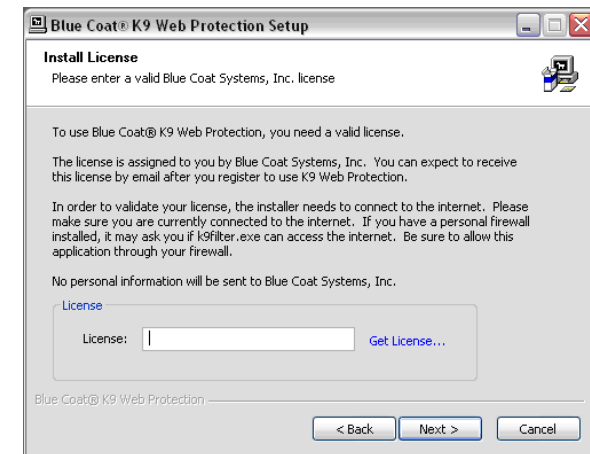
12. You will then be prompted to create an administrator password. This password will allow you to modify your Internet Filtering Settings, view Reports and override blocked pages. It is alos recquired to uninstall the program.

*Note: The password must be 15 characters or less and can only include alpha-numeric characters (e.g., A-Z and 0-9) as well as !, @, #, $, %, ^, *, (,), {, and }.*

13. After you enter and verify your password, you will be asked to place application shortcuts. Choose which shortcuts you want by checking the appropriate boxes, then click [Install].

14. **You will need to restart your computer in order to begin protecting your system.**

15. Congratulations! K9 Web Protection is now installed and protecting your system.

Once you restart your computer, K9 Web Protection will begin protecting your system with the **Default** Internet Protection Level. To change the Internet Protection Level, you will need to log into K9 Web Protection administration interface and go to the **Set Up K9** tab.

Installing K9 Web Protection from CD

1. Put the K9 Web Protection installation CD in your computer's CD drive.

2. The Setup Wizard should automatically launch, guiding you through the installation process. If it does not, double click on your CD drive, then double-click on [k9-webprotection.exe].

3. You will be prompted to accept the K9 Web Protection license agreement. Click [I Agree].

4. You will then be prompted for the install location. K9 Web Protection defaults to `C:\Program Files`. (If you want to install the software in a folder other than this one, please type it in now.) Click [Next]

5. Now you need to obtain your K9 Web Protection License.

   CA eTrust ISS users: If you have a valid CA eTrust Internet Security Suite license, you are automatically entitled to a one-year license for K9 Web Protection.

   a. To obtain this one-year license, **you must have already installed the eTrust Internet Security Suite** on your computer and rebooted before starting your K9 installation.

Note: See Appendix B for some important configuration rules you'll need to set inside of eTrust Internet Security Suite to ensure smooth operation with K9.
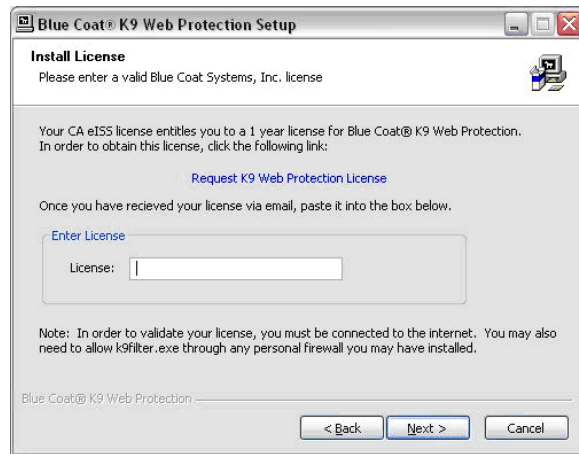

   b. Click the "Request K9 Web Protection License" link when the installer displays the dialog box shown below. It will take you to the K9 Web Protection website.

   c. Fill out the simple form on the K9 website to complete the license request and click "Request License".

   d. Your K9 Web Protection license will be emailed to you shortly.

Remember to review Appendix B to ensure smooth operation between eTrust ISS and K9 Web Protection.

All other users installing from CD: You must obtain a license from the K9 Web Protection website.

   a. Point your web browser to www.k9webprotection.com or click [Get license...] in the K9 Installer program screen shown below.
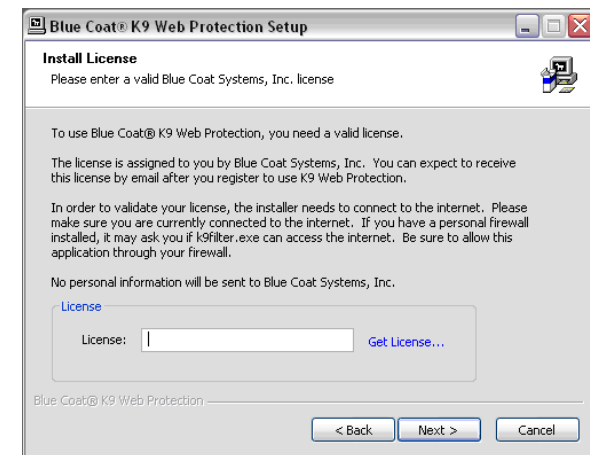
   b. Click on the [Get K9 Now] link.

   c. Fill out the simple form to complete the license request and click [Request License].

   d. Your license key will be emailed to you shortly.

All Users:

*Note: Your email account (and/or your Internet Service Provider) may be set to disregard unwanted email (known as "spam"). **To ensure that you get your K9 license email**, configure your mail account to **accept messages from k9support@bluecoat.com**. If you do not see the K9 license email shortly after requesting your license, check your email account anti-spam settings, and check your "junk" folder to see if the K9 license email was routed there.*

6. Copy your K9 license from your email message and paste into the "Enter License" box and click [Next].

7. You will then be prompted to create an administrator password. This password will enable you to access the K9 Web Protection administration interface, configure the Web filtering rules according to your needs, and override blocked pages. **It is also required to uninstall the application**.

*Note: The password must be 15 characters or less and can only include alphanumeric characters (e.g., A-Z and 0-9) as well as !, @, #, $, %, ^, *, (,), {, and }.*

8.. After you enter and verify your password, you will be asked to place application shortcuts. Choose which shortcuts you want by checking the appropriate boxes. Click [Install].

9. Congratulations! K9 Web Protection is now installed on your system. You will need to restart your computer in order to begin protecting your system.

Once you restart your computer, K9 Web Protection will begin protecting your system with the **Default** Internet Protection Level. To change the Internet Protection Level, you will need to log into K9 Web Protection administration interface and go to the **Setup** tab.

Introduction to K9 Web Protection

Remember, as soon as you reboot your computer after installing K9, it's actively working. But to configure K9 Web Protection, you'll need to launch K9's Admin application. Find the application in your Start Menu > Program listings. Click on [Blue Coat K9 Web Protection Admin] to run the application. Alternatively, if you chose to place a shortcut to the application on your desktop, launch the software by double-clicking on the shortcut.

The K9 Web Protection Home page will launch in a web browser window:

Note: You are not required to give your password unless you want to access the VIEW INTERNET ACTIVITY or the SETUP pages.

Logging in to K9 Web Protection

In order to access K9 Web Protection's configuration, administration, and reporting functionality, you must log in to the application with the administrator password you selected during the installation process.

1. Find the application in your Start Menu > Program listings. Click on [Blue Coat K9 Web Protection admin] to run the application. Alternatively, if you chose to place a shortcut to the application on your desktop, launch the software by double-clicking on the shortcut.

K9 Web Protection will launch in a Web browser window.
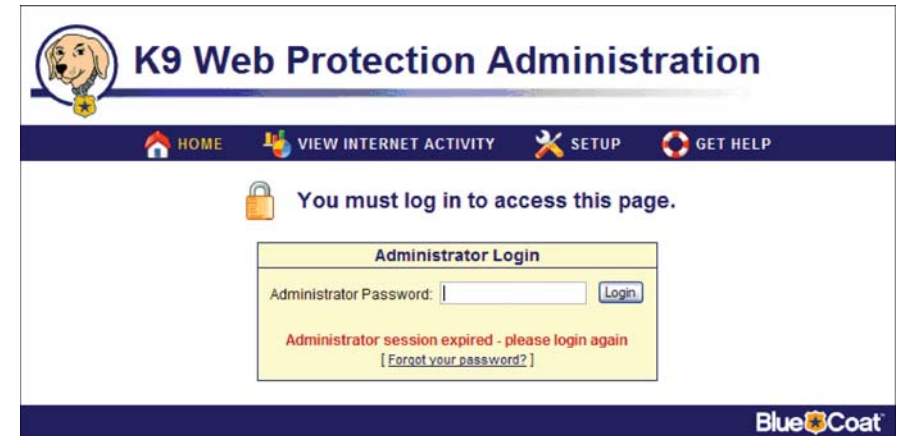
2. Clicking on either [View Internet Activity] or [Setup] brings up the Administrator Login prompt. At the prompt, type in the administrator password that you created during the installation and hit the "Enter" key.

3. You are now logged in as the K9 Web Protection administrator

Note: The administrator login times out in five minutes of non-activity to ensure that, should the administrator fail to log out, other users cannot change filtering or administrative settings.

Forgot your password?

If you forget your password, you can click on the [Forget your password?] link and a temporary password will be sent to the email address you used when you registered your K9 Web Protection application. This temporary password is valid for only 24 hours, so you must change the password after regaining access (see Chapter 3: Configuring K9 Web Protection).

Note: The administrator login times out in five minutes of non-activity to ensure that, should the administrator fail to log out, other users cannot change filtering or administrative settings.

Getting Familiar With the K9 Web Protection User Interface

This section provides a quick overview of the Blue Coat K9 Web Protection user interface. We recommend that you familiarize yourself with the user interface before you configure and use the software.

The Blue Coat K9 Web Protection user interface includes four primary sections:

Home—Default page that allows access to other pages containing K9 Web Protection features.

View Internet Activity—Tracks web browsing activity, including category violations and override requests, and administrative activity, such as changes to program settings and automatic software updates.

Setup—Controls the web filtering rules for your K9 Web Protection application. With this tab, you can create the filtering rules that meet your specific requirements. You can select from five pre-configured Internet Protection Levels or create customized filtering rules using a variety of controls, including the over 55 unique categories in the Blue Coat database.

Get Help—Contains links to "Instant Support" and to frequently asked questions about the product. It also provides a support number for emergencies, a way to check or dispute how a specific website is categorized, and a link for providing feedback.

Configuring K9 Web Protection

Using the **SETUP** tab, you can config-ure K9 Web Protection with the web filtering settings that meet your specific requirements.

Selecting Your Internet Protection Level

1. Click on the **SETUP** tab. If you haven't already logged in you will be prompted for your administrator password:
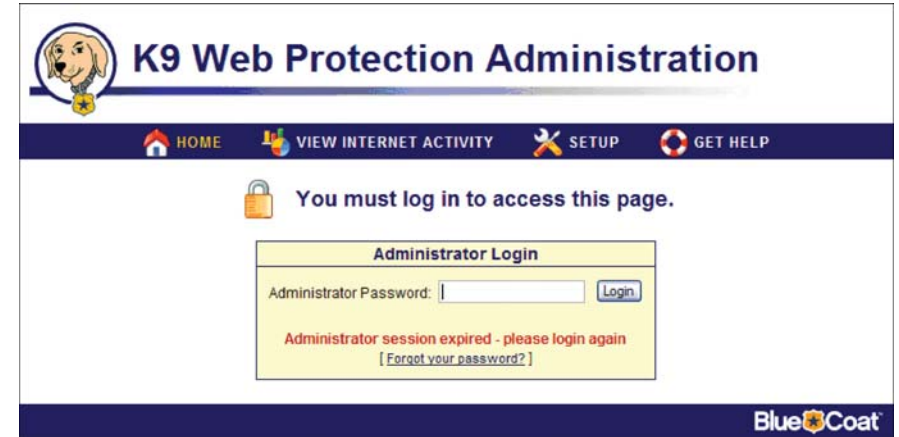
2. Enter your administrator password and click the [Login] button or press the return key:

3. Blue Coat has five pre-configured Internet Protection Levels. These levels range from **Monitor** to **High**. They include different combinations of commonly blocked categories.

When running K9 Web Protection for the first time, the Internet Protection Level is set to **Default**, which blocks the most commonly blocked categories while allowing unrated sites.

4. To change the Internet Protection Level from **Default** to any of the other four levels, click on the radio button associated with the level of desired protection.
5. After selecting the Internet Protection Level that best meets your requirements, click the [Save Changes] button at the bottom of the screen to activate K9 Web Protection level you have specified.

Viewing Category Details

Each of the five pre-configured Internet Protection Levels within K9 Web Protection blocks different categories or combinations of categories. To view more information about the categories blocked by each of the pre-configured Internet Protection Levels, click on the link or links in the level description.

For example, the **Default** and **High** Internet Protection Levels block a collection of 18 categories, which Blue Coat calls the 'Most Commonly Blocked Categories'. To view this list, click on the commonly blocked link in either the **Default** or the **High** Internet Protection Level description.

A window similar to the following will appear within your browser:

If you want to know more about sites included in one of these categories, click the category link. For example, if you want to know more about the category, **Adult/Mature Content**, click the [Adult/Mature Content] link. A window similar to the following will appear, providing a description of the category as well as some examples of sites in the category:

Selecting the **Custom** radio button expands the Web browser to display all the categories identified by the Blue Coat database:
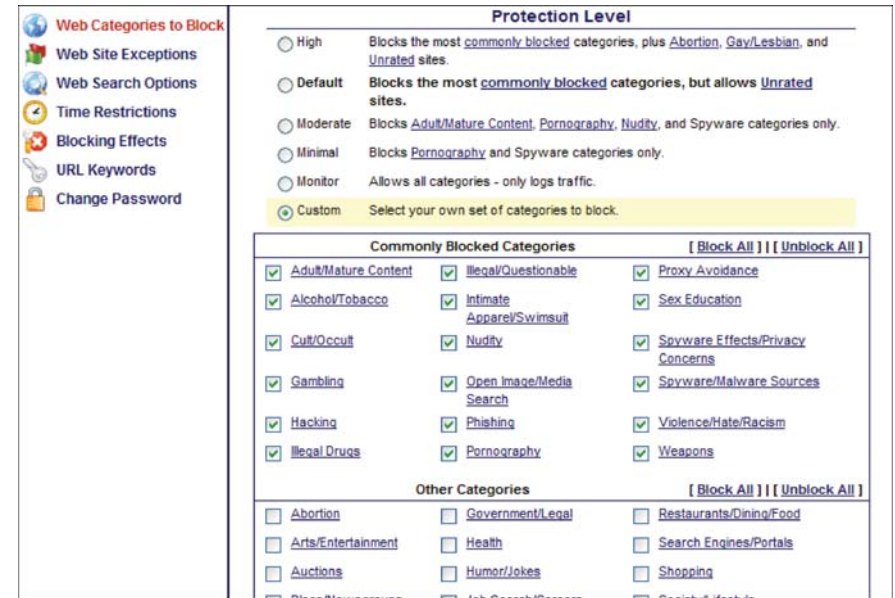
To block any of the categories, simply check the box next to the additional categories. Likewise, you can uncheck any of the categories that are currently blocked to allow access to websites identified as such.

Scroll down to the bottom of the expanded web page to view two important filtering options:
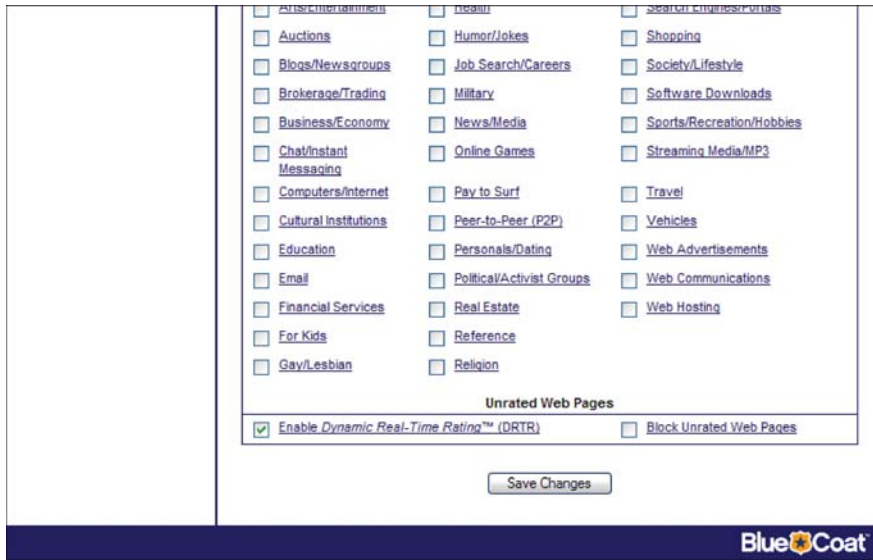
Checking the **Enable Dynamic Real-Time Rating™ (DRTR)** option (on by default) permits K9 Web Protection to try to dynamically match a website to a category in the Blue Coat database. Checking **Block Unrated Web Pages** (off by default) will block any web page that K9 Web Protection cannot match to a specific category. We recommend that you keep the default settings for these two options.

If you make any changes using the Custom option, you must click the [Save Changes] button to activate the desired changes. Subsequent sections describe how to access other useful features on the **SETUP** tab using the left navigation bar.

Web Site Exceptions

K9 Web protection provides a way for you to explicitly block or allow access to specific Websites. To block or allow a Website, click the [Web Site Exceptions] link on the left navigation bar:
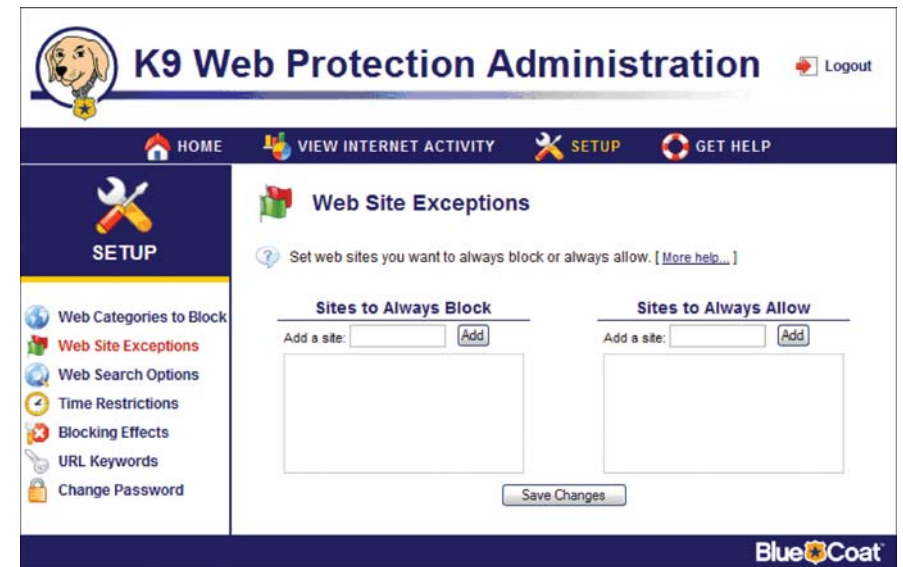
To always block a site, enter the URL in the text field on the left, labeled "Add a site", under Sites to Always Block. You must enter each URL separately. Click the [Add] button or press the Enter key. Each URL will be displayed on a separate line:

Click the [Save Changes] button to activate the new filtering rules.

To allow access to a specific site, enter the URL in the text field on the right, labeled "Add a site", under Sites to Always Allow.   You must enter each URL separately. Click the [Add] button or press the Enter key. Each URL will be displayed on a separate line:
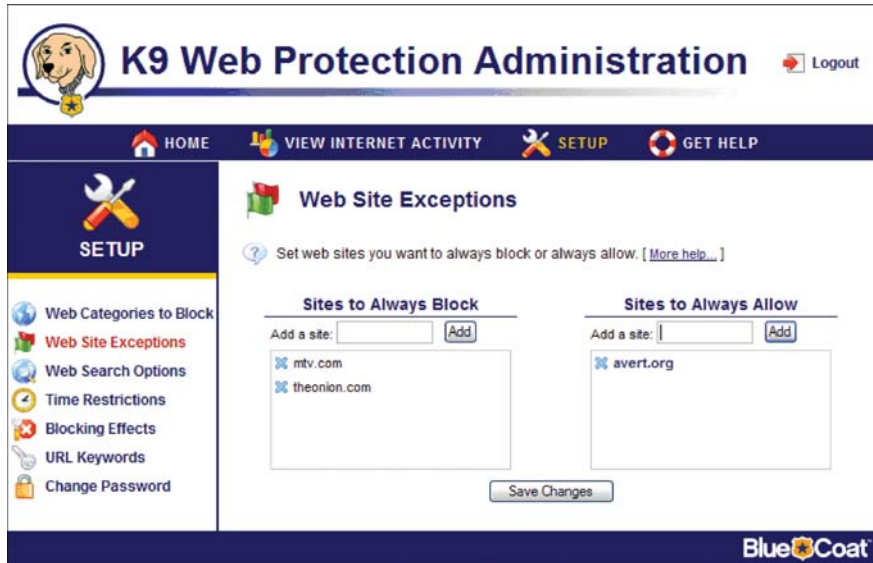
Click the [Save Changes] button to activate the new filtering rules.

At any time you can remove the website from your Sites to Always Allow list by clicking the blue X next to the website. The application will strike through the website as shown:
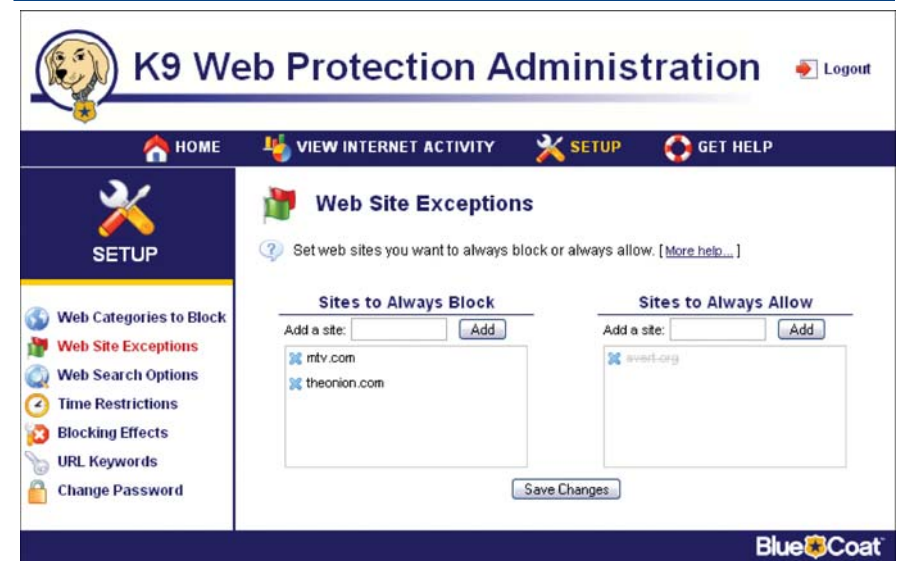
Click the [Save Changes] button to activate your changes.

Web Search Options

K9 Web Protection offers the option of enforcing the use of Google SafeSearch™, which diminishes the amount of adult material that might be returned as a result of an Internet search. This feature is selected by default. Currently, K9 Web Protection only supports the safe search functionality of Google Search Engine. Other search engines will be added in future releases. To enable or disable this feature select Web Search Options from the Left navigation bar:
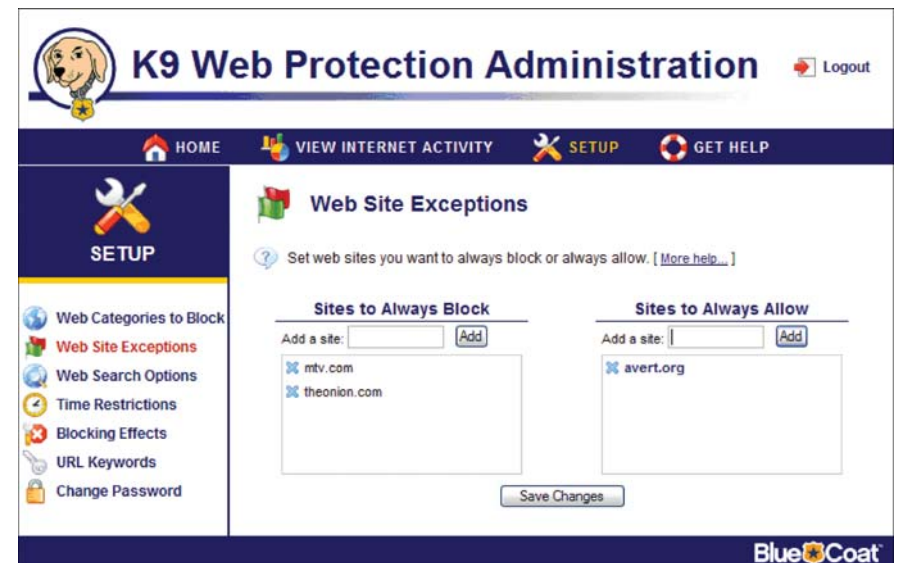
A checked box means Google SafeSearch will always be used. An unchecked box does not enforce this policy. You must click the [Save Changes] button to enable a change in the rule.

Time Restrictions

K9 Web Protection offers the ability to restrict the time of day users can access websites. If there are specific times when you either do or don't want your family accessing the Web, this feature will assist you in enforcing that policy. To access the Time Restrictions page click [Time Restrictions] on the left navigation bar:

Once you have selected a region, you will then be given the ability to allow or deny access to all websites for the region of time you have selected.

The diagram below shows Web access restricted during the night and during the school day, but enabled before school, during the evening, and all day on weekends.

The page contains a seven-day, 24-hour schedule that allows you to explicitly set the times and days users can and can't access web sites.

To configure time restrictions, click any of the 30 minute time blocks. The block will toggle between white/gray and red. Red means access to all websites will be denied during that time. Gray or white means internet access will be allowed.

Note: Even when you Allow access, your other restrictions (for example, restrictions based on categories) are still active. Selecting Deny blocks access to ALL websites.

Alternatively, you can click and drag to select a region consisting of multiple time blocks as shown below.
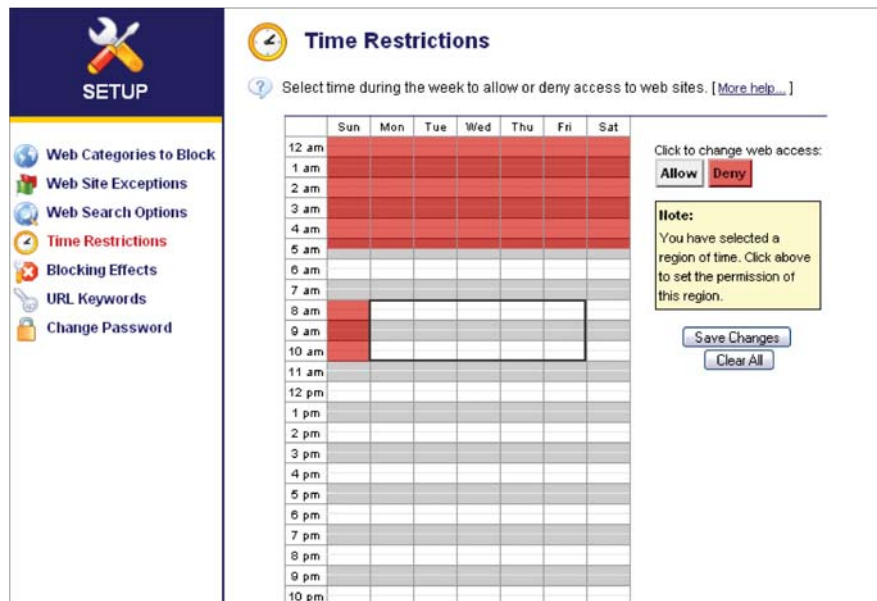
Once you have selected a region, you will then be given the ability to allow or deny access to all websites for the region of time you have selected.

The diagram below shows Web access restricted during the night and during the school day, but enabled before school, during the evening, and all day on weekends.

Blocking Effects

The Blocking Effects page enables you to tailor to your needs what happens when a page is blocked. Clicking the [Blocking Effects] link on the left navigation bar displays the **Blocking Effects** page :
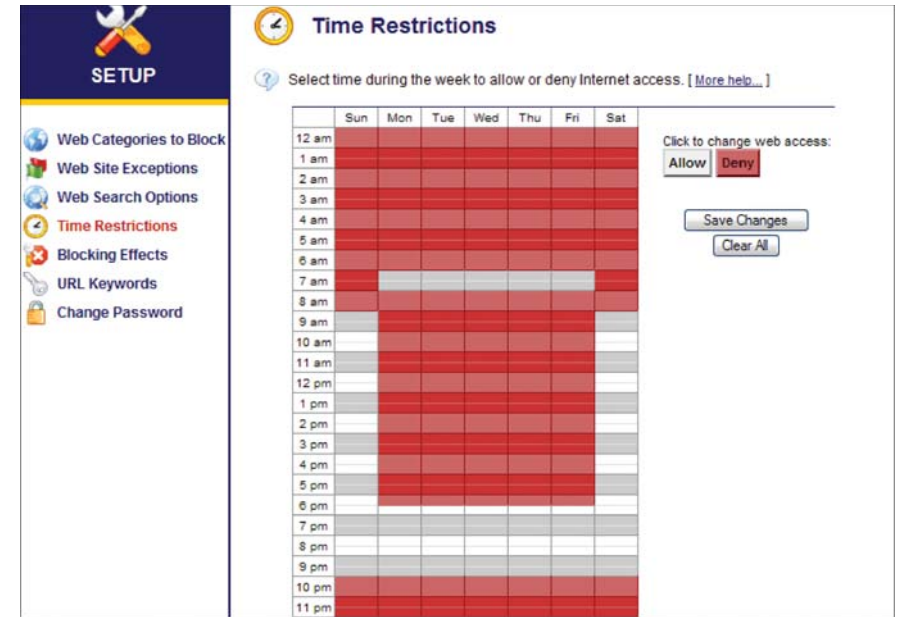
Bark when blocked–K9 Web Protection offers an audible feature in which the application plays a bark when a user attempts to access a blocked site. This feature is useful to alert a parent, teacher, or other care provider that someone under his or her supervision might be stumbling onto offensive or inappropriate content. To enable the bark feature, check [Bark when blocked].

Note: You must have speakers connected to your computer, and the volume control cannot be set to "mute" or you will not hear the bark.

Show admin options on block pages–If a user of your computer attempts to access a Web site that is not allowed by the currently active K9 Web Protection settings, a Filtering Alert block page will appear, indicating that the page violates one of the settings and the reason for the block (see Chapter 6, Understanding Filtering Alerts for full details on these important alerts).

To display and enable administrative options—such as overriding a site that has been blocked or modifying the Web filtering settings—directly from a Filtering Alert block page, check [Show admin options on Block Pages].

Here's an example of a Filtering Alert block page showing Administrative Overrides:
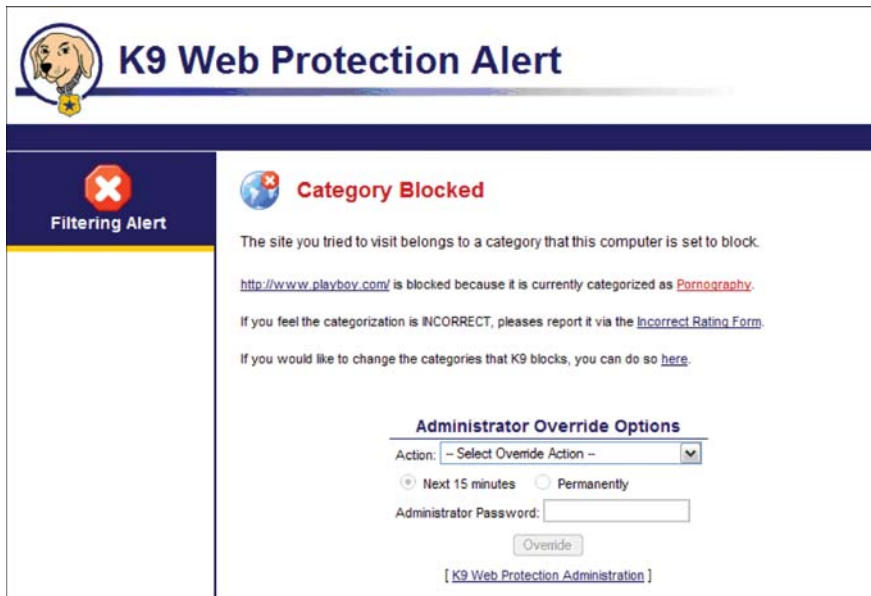
Full details of Filtering Alert block pages are included in Chapter 5.

Time Out Settings

If a user attempts to visit too many blocked sites in a specified period of time, K9 can completely block access to the Web for a time you specify. To enable this feature click the checkbox next to [Enable Time Out Settings]:
You can now specify how many blocked attempts may occur within a specified period of time before triggering the "Time Out" and how long to block access to the Internet if a "Time Out" occurs.

Click [Save Changes] to activate changes to any Blocking Effects you select.
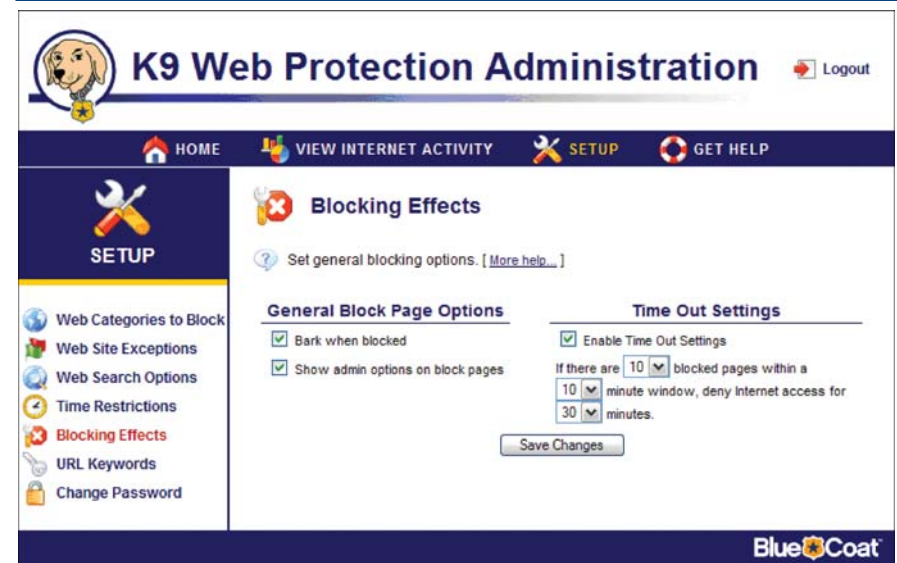
URL Keywords

K9 Web Protection allows you to block access to web pages based on keywords in the web page URL. You can, for example, block any web page that has the word "sex" in the URL. To block specific keywords

1. Click [URL Keywords] on the left navigation bar on the SETUP tab:
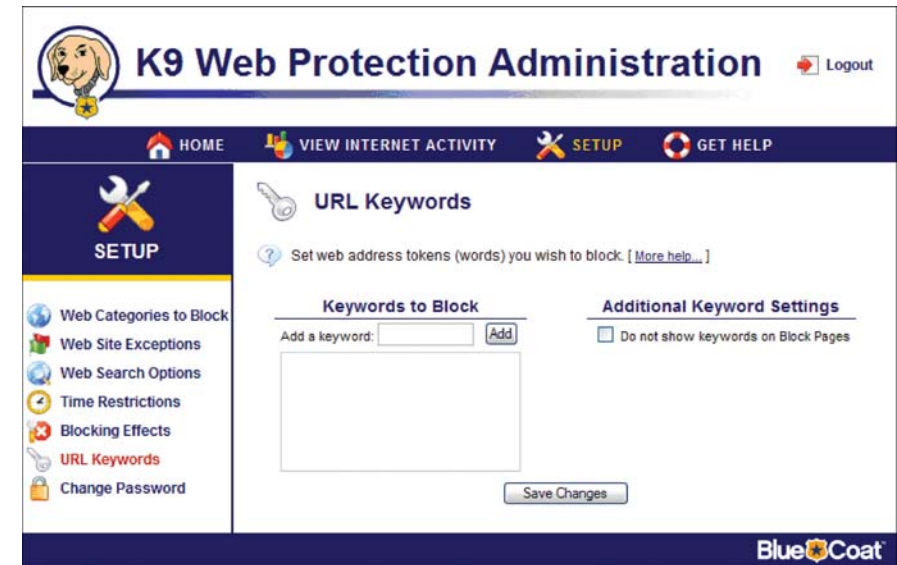
2. Enter the keyword you want to filter in the Add a Keyword text field.

3. Click the [Add] button.

4. Click [Save Changes] to activate your changes.

Note: You can use an asterisk (*) to match portions of the URL. For example, if you enter "sex" as a keyword, it will block www.sex.com, but not www.sexy.com or www.essex.com. If you enter "sex", it will block www.sex.com and www.sexy.com, but not www.essex.com. If you enter "*sex", it will block www.sex.com, and www.essex.com, but not www.sexy.com. Entering "*sex*" will block all of the above examples.*

The keyword will be added to the list of filtering keywords as shown:

When a page is blocked because of banned word in the URL, K9 Web Protection displays a filtering alert that identifies the reason the page was blocked. By default, the message displayed includes a reference to the keyword.

Since these keywords may be offensive, you have the option of not displaying keywords on the filtering alert. To prevent the display of these keywords on the filtering alert, click the checkbox next to [Do Not Show Keywords].

See Chapter 5, Understanding Filtering Alerts, for full details on these important alerts.

To remove the keyword from the filtering list, click the blue x next to the word you want to remove.

Note: Putting "sex" in the URL keywords will NOT block pages that have the word "sex" in the page itself. It will only block pages that have the word "sex" in the URL.

Change Password

At anytime you can change your password from the Change Password page by clicking [Change Password] on the SETUP tab:

To change your password enter the current password in the [Current password] field, and enter the new password in the [New password] and [Re-type new password] fields.

You will want to use this feature any time you request a temporary password. Because your temporary password is only useful for 24 hours, you should use it to log in and immediately navigate to this screen. After logging in with a temporary password, your "Current password" would be the temporary password you used to log in. Enter a new, permanent password, re-type it, and click the [Change Password] button.

Note: The password may include only alphanumeric characters (A-Z and 0-9) and the following symbols: !, @, #, $, %, ^, *, (,), {, and }.

Chapter 4
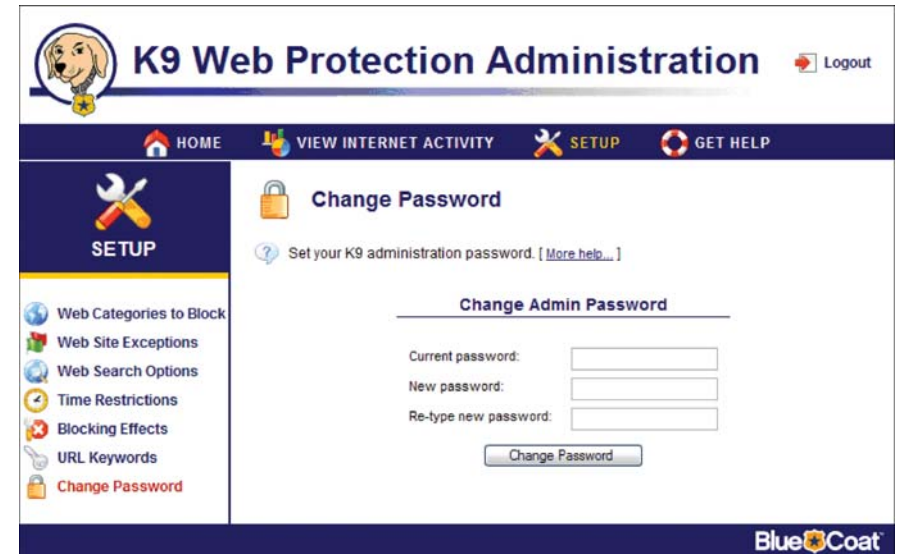
Viewing Internet Activity

The **VIEW INTERNET ACTIVITY** section helps you keep track of web traffic statistics through two types of online activity reports: Summary and Detailed.

Note: The statistics tracked in this window begin upon installation of the software and continue to increment indefinitely. If you would like to purge the log and restart the statistics, click the [Reset All Counters] button at the bottom of the General Overview table.

View Activity Summary

The View Activity Summary link in the left navigation bar has three tables:
-
Category Summary—The Category Summary lists all categories relevant to the active K9 Web Protection rule. Categories shown in green are allowed. Similarly, categories listed in red are blocked by the active policy. Categories in orange have changed status during the reporting period.

The category summary also provides access to statistics about recent Internet activity by category. You can click on a category for a detailed view of website requests in that category. For example, to view a list of which sites within the Pornography category that someone attempted to access, click on the link for Pornography. A detailed report similar to the following will appear:

Notice that you are now in the View Activity Detail in the left navigation bar. To return to the summary report, click on [View Activity Summary]. You can obtain a similar detailed report for any statistic listed on the View Activity Summary page by clicking the statistic's link.

General Overview—The General Overview displays a general breakdown of recent Internet activity, including the number of Web pages visited, requests allowed, and requests blocked.

You can click on any statistic for a detailed view as shown:

Most Recent Admin Events—The Most Recent Admin Events shows recent changes to the web filtering rules (e.g., overrides, keyword blocking additions, and login failures) and other administrative options made using the administrator password. This section is located at the bottom right of the page, below the General Overview section:

Note: Clicking the [Reset All Counters] link does not remove the record of administrative events. This exclusion is by design so that if an unauthorized access to the administrative tool does occur, there will still be a record of the changes that were made during that time.

Clicking the [View full log] displays all administrative events:

View Activity Detail

Clicking [View Activity Detail] in the left navigation bar displays a detailed view of all Internet activity including all Web sites visited and blocked since the last log purge, the category ratings of these sites (if rated), and the actual URL of the site/s visited:

You can view just the activity related to Web surfing in this detailed report, or you can also include administrative events. To include administrative events in the report, click the [Show admin events] link next to the **All requests** title. You will now see all administrative events (e.g., overrides, password changes, failed logins, etc.) as part of the report.

Viewing these administrative events in line with web surfing details can be useful for understanding the behavior of those using your computer. For example, you can see if someone has attempted to break into the system by noting how many failed logins occurred before a recent password change or whether a category was allowed or overridden before a site was visited:

To remove the administrative events from the report, click the link (which will now read [Hide Admin Events]) again.

Chapter 5

Understanding Filtering Alert Pages

If you or anyone else logged into your computer attempts to access a Web site that has been blocked by the currently active K9 Web Protection settings, a Block Page alert will appear. This block page indicates that the page violates one of the settings and the reason for the block.

For example, if the **Default** Internet Protection Level is active on your system and you attempt to access www.playboy.com (categorized as **Pornography** and therefore blocked at the **Default** level), you will receive a Block Page as shown:
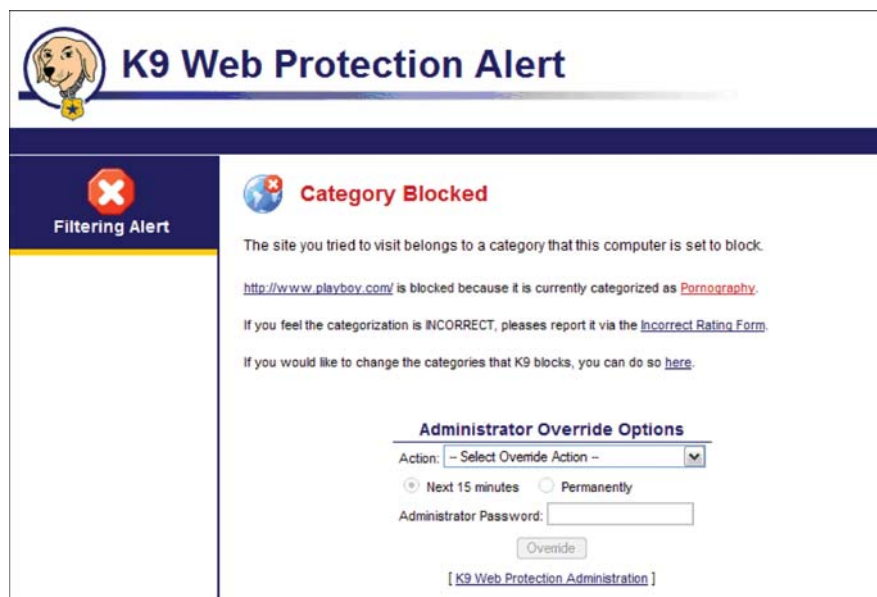
The category that caused the site to be blocked is identified in red. In this case, **Pornography** is the category that caused www.playboy.com to be blocked.

Overrides on Block Pages provide a flexible browsing experience for different users with varying requirements. These override features help provide a browsing environment that matches the dynamic nature of the Internet. There are five different types of Block Page overrides in K9 Web Protection:
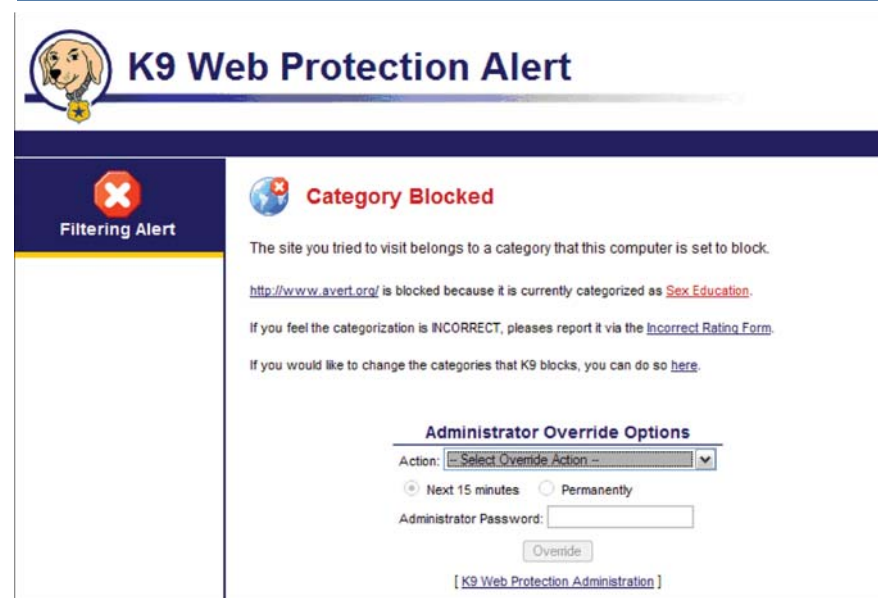
Category Blocks

If the page has been blocked due to the site's inclusion in a particular category, the Block Page alert will look like this:
If you have the administrator password, you will be able to select and submit one of three different override actions in the [--Select Override Action--] pull-down menu:

• Allow all pages on the blocked site

Note: In this case, all pages on www.avert.org, including http://www.avert.org/educate.htm, for example, would be allowed.
-
• Allow all content rated in the blocked category (e.g., Sex Education)
• Allow all categories

Note: This option will allow users to access all Web sites without any protection for 15 minutes. You cannot permanently turn off K9 Web Protection using this option.

To select an override action:
1. Select the desired action in the [-- Select Override Action --] pull-down menu;
2. Choose the timeframe to set the active period of the override;

Note: There are two timeframe options: "Next 15 minutes" or "Permanently"

3. Enter your administrator password;

4. Click the [Override] button.

Note: If you do not enter the administrator password, the selected override will be rejected.

You can also click on the [Incorrect Rating Form] link if you think the displayed category is incorrect. Blue Coat appreciates your feedback!

Any override action you select on a Block Page will be reflected in the appropriate section of the **SETUP** tab. For example, if you override a category from a Block Page (in this case, Sex Education), the override—and its timeframe—will appear in the Web Categories to Block section of the **SETUP** tab, as shown:

In this example, sites in the category, Sex Education, are now permitted due to the override action, with 14 minutes remaining for the override. Alternatively, if you were to override just the site by selecting [Allow all pages on "avert.org"], the Web Site Exception section would reflect the override:

*Note: Even if you select "Permanently" as the timeframe, you can always undo an override later by navigating to the appropriate section of **SETUP** and removing exception or re-checking the category.*

Website Blocks

If the blocked page is a site from your website Exceptions list of sites to always block, , the Block Page will look like this:
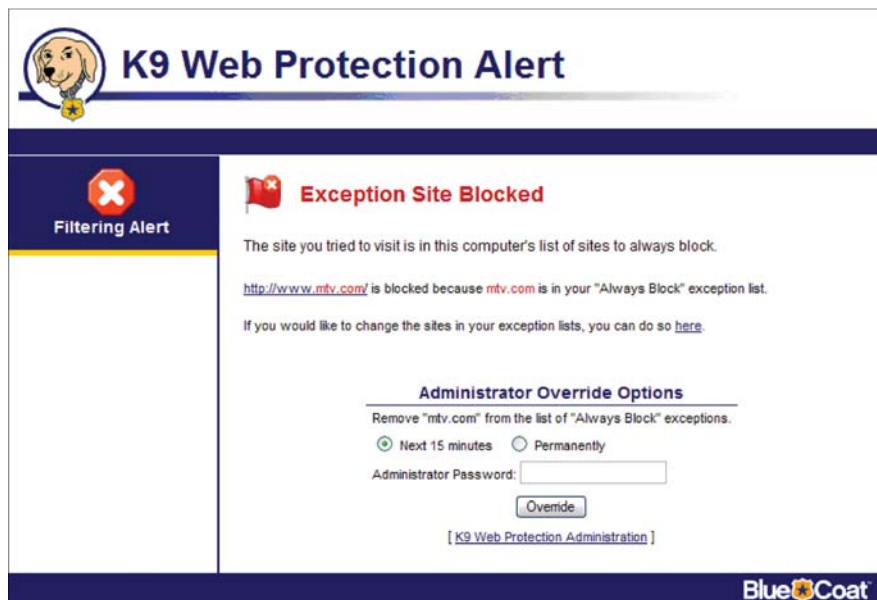

As in the previous example, if you override a site-specific block the exception and its timeframe will be reflected in the Web Site Exceptions section.

Note: If you select "Permanently" as the timeframe, you can undo the override later by navigating to the Web Site Exceptions section of the **SETUP** *tab and removing the site from "Sites to Always Allow" or adding it again to "Sites to Always Block" .*

URL Keyword Blocks

If the page has been blocked due to a keyword, the Block Page alert will look like this:
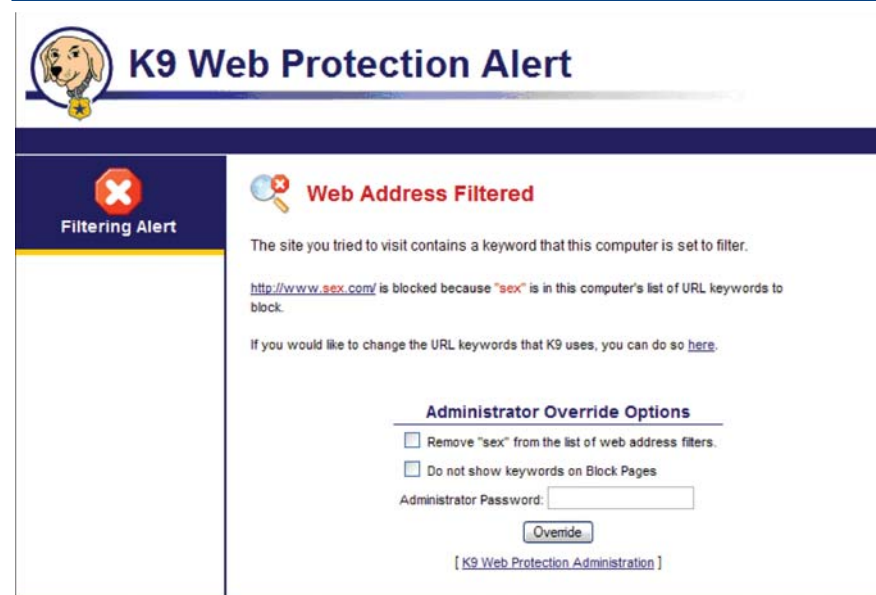
In the screenshot above, the page was blocked based on the appearance of the keyword "sex" in the URL. If you have the administrator password for the K9 Web Protection software, you can select one or both of the following over-ride options:

• Remove the keyword from the keyword list
• Only match complete words
• Do not show keywords outside admin interface

To select one or more of these override options:

1. Check the box associated with the action/s;

2. Enter your administrator password; and

3. Click the [Override] button

Time Restriction Blocks

If website access is blocked because you have disallowed access at a specific time, the Block Page alert will look like the following:
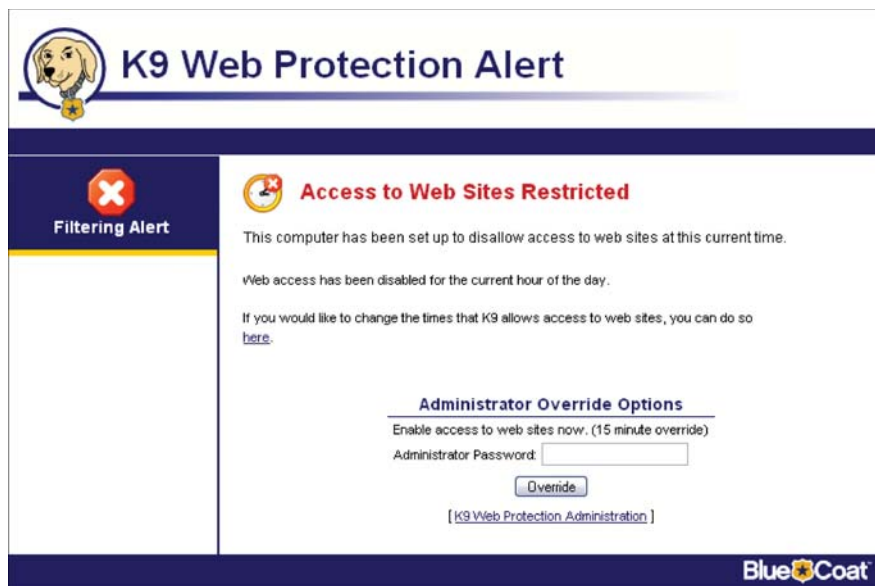
You have the option of overriding time-restricted access for 15 minutes by entering your password in the Administrator Password and pushing the Override button.

NOTE: All other access controls are still in place. For example, if you have the category Pornography blocked, and you decide to override time restrictions, access to pornography sites will remain blocked.

Timeout Blocks

If a user attempts to access a blocked website or category too many times within a period of time you have specified, K9 Web Protection will suspend access to websites as shown:
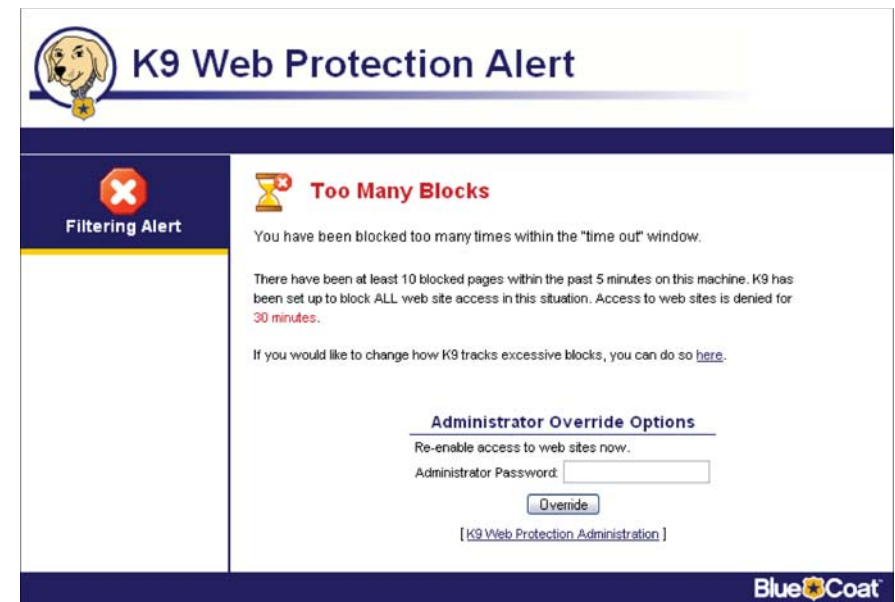
You have the option of re-enabling web access by entering your administrator password and clicking the [Override] button.

Chapter 6

Get Help

Through the **GET HELP** menu, you—or anyone using your computer—can communicate directly with Blue Coat. No administrator password is required to access these tabs.

Note: If you are using K9 as a part of CA eTrust® Internet Security Suite, you need to contact CA for support. Go to http://www.my-etrust.com/Support/.

The GET HELP section enables you to access support and provide feedback to Blue Coat. Get Help also has a link to the Frequently Asked Questions section on the K9 website.
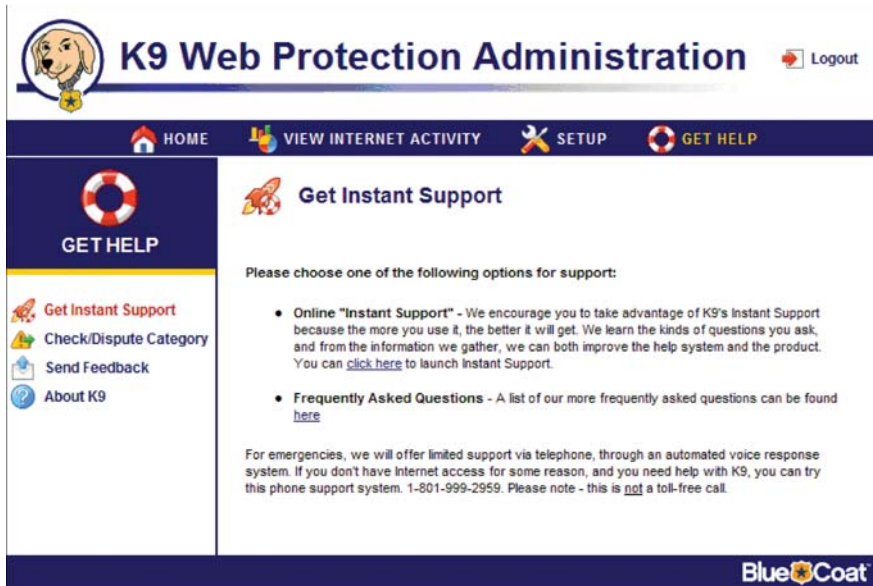
Clicking the [click here] link in the **Get Instant Support** section displays the K9 Web Protection online support web page:
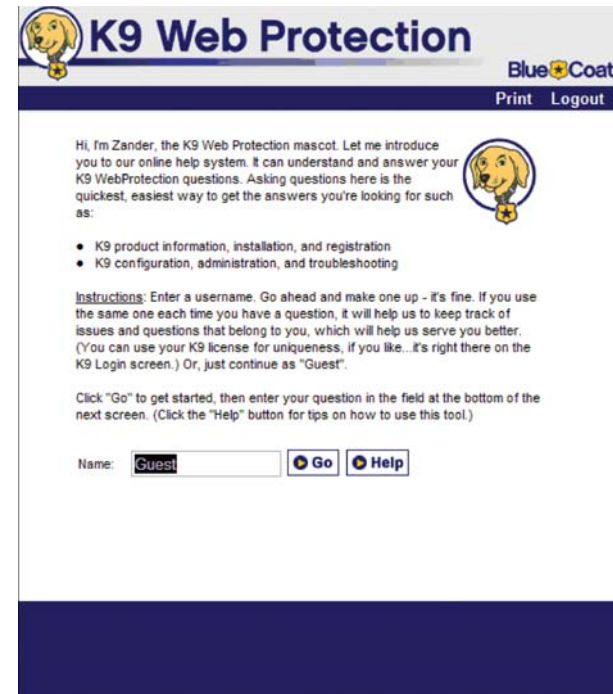
From here you can access the support you need online, by simply typing in a guest name and clicking [Go] button:

Type a question in the Question text field and click the [Go] button:

The Get Help page also has a link to **Frequently Asked Questions** in the support section of the K9 Web Protection website. The FAQ's answer a variety of general support questions about K9.

There are three other sections on the **GET HELP** section that are available from the left navigation bar:

Check/Dispute Category

This screen provides a quick and easy way for you to check a website's current rating and submit the site to Blue Coat for review. This screen is especially useful when you think a site's rating is incorrect.

Entering a website URL and clicking the [Submit] button displays the category according to the Blue Coat database:

If you believe the categories listed are incorrect, you can suggest a more appropriate category as well as provide additional comments and a description of the site by checking the "Please send results of the Site Review via email" box and selecting your category suggestions from the pull down menus.. Your comments will aid Blue Coat in the review process.

Send Feedback

This screen enables you to provide feedback to Blue Coat about your experience with the application:

If you want to provide feedback, simply enter your comments in the text field and click the [Submit Feedback] button.

NOTE: DO NOT USE the Send Feedback screen to request support from Blue Coat. Use Instant Support instead.

About K9

Provides information about the application such as version number user license:

You can view details about your K9 Web Protection installation and filtering statistics by clicking the [Show Advanced Information] link at the bottom of the page:

If you need additional technical support, please visit www.k9webprotection.com and click on [SUPPORT].

You can find additional information about Blue Coat and K9 at our websites: www.bluecoat.com and www.k9webprotection.com

Common Error Pages

K9 Web Protection users have occasionally experienced problems using K9. Usually these are because of Internet connection or desktop firewall issues.

K9 Not Connected

Symptom
You are getting the following picture:

Cause
   •User is not connected to the internet
   •A firewall is blocking K9 from validating license
   •User is forced to access the internet through a proxy

Solution
   •Connect to the internet and try again
   •Configure your firewall to always allow k9filter.exe access to the internet

Note: This error may occur if you are installing K9 on a computer that sits behind a device known as a proxy server. Currently K9 does not support proxy configurations.

Appendix B

K9 Not Responding

CA's eTrust Internet Security Suite Users

Symptom

You are getting the following picture:

CA eTrust ISS users may experience problems when setting up K9 Web Protection. This section lists the most common problems and how to resolve them.

Note:For users who acquired K9 Web Protection as part of their eTrust Internet Security Suite, K9 Web Protection will not install without CA's eTrust ISS being installed first; this is by design. Please first install the CA Internet Security Suite, then install K9 Web Protection.

Symptoms

You cannot "stay logged in" to the K9 administration page with the password you set or a temporary password. You also have installed one of the following:

1. CA Internet Security Suite
2. CA Firewall
3. Zone Alarm Internet Security Suite
4. Zone Alarm Firewall

Cause

A setting in the CA / Zone Alarm firewall is preventing you from logging into K9 Web Protection.

Cause

• Somebody may have tried to disable K9 Web Protection
• The K9 filter has crashed
• The K9 installation has become corrupt
• A software firewall has crashed on the system, causing K9 to stop functioning.

Solution

• Uninstall any program you suspect might be causing the crash.
• Try re-installing K9 again on top of the existing version. You can obtain the latest version at:

http://www.k9webprotection.com/download/k9-webprotection.exe

After you reinstall K9, please reboot your computer.

• If you receive a message that K9 has been updated, and rebooting does not solve the problem, please contact K9 support.

Solution

Please follow these instructions to change your firewall settings:

1. Download the latest version of K9 Web Protection from this link: http://www.k9webprotection.com/download/k9-webprotection.exe

Install this file right on top of the existing version. You should receive a message that K9 was successfully updated.

2. Reboot your computer.
3. Open your firewall settings, click the **Privacy** section on the left, and click the **Site List** tab at the top. If you cannot see the title **Private Header** at the top of the chart, expand the box until you see it.
4. Find the entries **Loopback** and **license.cwfservice.net** and make sure there is a green check-mark under the **Private Header** column.
5. If there is not a green check-mark, select **license.cwfservice.net** and click the **Options** button.
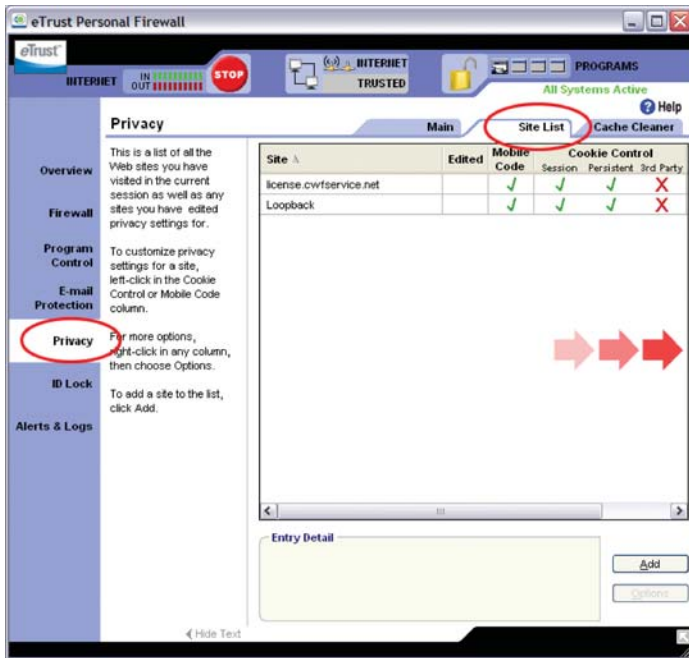
6. In the new window that opens, un-check the box next to **Remove private header** information.

7. Repeat steps 5 and 6 for the entry **Loopback**. If this entry does not exist

• Click **Add** and type **Loopback** in the box that pops up to add this entry.

• Again click **Add** and type **127.0.0.1** in the box that pops up.

8. After following these steps, your settings should look like the picture in step 5 with an additional line for 127.0.0.1. Each of these entries should show a green check-mark under the Private Header column. You may also have other entries in this list, but these should not affect K9.
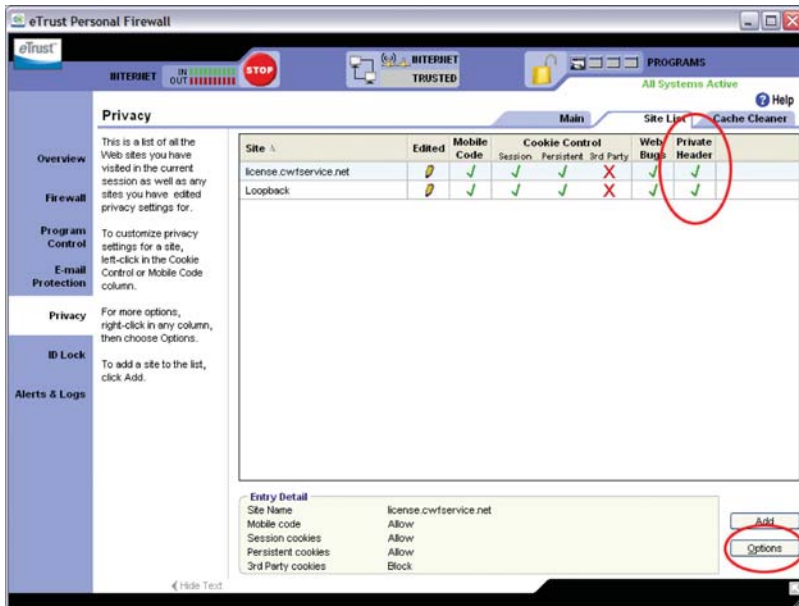
Your original password or temporary password should now log you in to K9. Please note that a temporary password will only work for 24 hours. If it has expired (and you forgot your original one), please request a new one by clicking on the [Forgot your password?] link below the password box when you try to log in to K9. Once you are logged in to K9 you can change your password by clicking Setup, then clicking [Change Password] in the far left column. Enter the temporary password for your current password.

If the above instructions do not solve the problem, you may email K9 Support at k9support@bluecoat.com. Please provide as much detail as possible so that we can solve the problem quickly.

Blue✪Coat®

Part Number 231-02796-01