SecureSpot 2.0 User Manual

Table of Contents

Table of Contents (Continued)

Chapter 15: Support Function

Chapter 16: Buy Now Function

Chapter 17: Technical Support

Appendices

List of Figures

List of Figures (Continued)

List of Figures (Continued)

List of Figures (Continued)

1. INTRODUCTION

Simplified All-In-One Security

The SECURESPOT 2.0 Services furnished with your D-Link RangeBooster N™ Router offers a complete, all-in-one Internet security solution that provide the easiest and most affordable way to protect your family, computers, data, and personal information from the many dangers and security threats present on the Internet.

Easier to Install and Use

SECURESPOT 2.0 Services install in a fraction of the time that it takes for traditional PC-based security products. The Firewall, Spam control, and Parental Controls are pre-configured on the router to provide automatic, out-of-the-box protection for all connected devices in the home. When a computer is added to the network, SECURESPOT detects it and loads a very small but powerful endpoint security application (25X smaller than leading security suites) that protects personal computers from Viruses, Spyware, ID theft, and pop-ups within the network and while on the road.

Unique, Graphical Remote Management Console

At the heart of the system is an industry first – a Web-based, graphical management console that remotely communicates with the router and protected computers (Figure 1.1). Eliminating the need to physically log in to each and every device in your home, the easy-to-use remote console allows you to view all protected devices, and monitor or configure SECURESPOT 2.0 services, even when you're away from home.
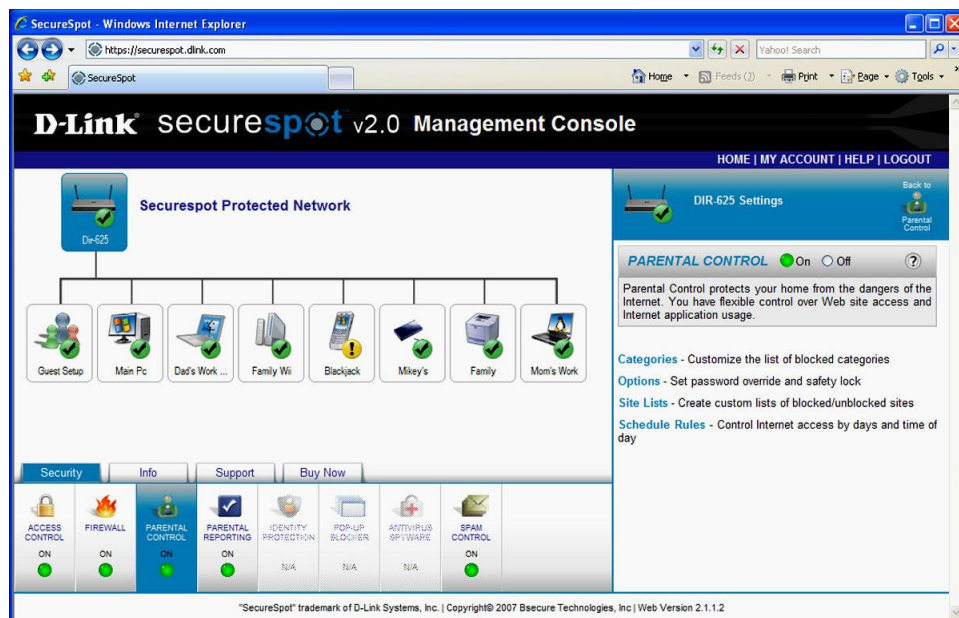
Figure 1.1: Management Console

Layered Security

SECURESPOT is the first to provide whole-home protection by utilizing three layers:

- **In-the-Cloud Security** or that can be managed away from home at the Web level.
- **Perimeter Security (gateway)** overseeing all devices inside the home at the router level.
- **Endpoint (thin client)** managing personal security options inside the home for each computer.

To be effective in an increasingly mobile world, it is crucial that these layers of security work in concert. SECURESPOT 2.0 provides this integrated protection. Layered security also enables SECURESPOT to provide security protection where it is the most efficient and offers the most functionality. For example, by performing the heavy lifting at the back-end security instead of on each computer, performance is greatly improved and support issues are reduced. In addition, executing security features such as firewall, parental controls, and others at the router provides automatic protection, without user intervention, for all devices in the home including game consoles such as the Wii, PSP, and Nintendo DS.

World Class Parental Controls

Safeguarding your entire home with parental controls not only prevents objectionable content from entering, but protects all users from objectionable Web sites that can infect your computers or steal your family's personal and financial information. Additionally, SECURESPOT offers the unique advantage of being able to temporarily safeguard and control computers and other devices belonging to guests who may be utilizing your Internet connection.

SECURESPOT 2.0 utilizes a database of 63 M URLs representing billions of pages, updated daily to provide comprehensive protection that keeps pace with the dynamic nature of the Internet. An industry leading 81 categories provide unprecedented ability to customize the pre-configured settings. Alerts can notify parents via e-mail or text messages when pages are blocked at home. Embedded in the router, SECURESPOT offers tamper-proof, world-class parental controls.

McAfee® VirusScan® Engine

Bsecure Technologies has integrated the McAfee VirusScan 5200 engine into the AntiVirus/Spyware Protection service. The following features are now available with SECURESPOT 2.0 services:

- Enhanced Virus, Spyware, Malware, and Adware definitions
- Improved real-time process, memory, and registry protection
- Automated incremental Virus Definition Updates

2. GETTING STARTED

Purpose

The purpose of this manual is to:

- Guide you step-by-step through the activation and initial set-up of the SECURESPOT 2.0 Services on your D-Link RangeBooster N™ Router

- Describe the services and options provided by SECURESPOT 2.0 Services.

Before You Begin

1. Check the hardware version of your DIR-625 router.

2. SECURESPOT 2.0 will only run on Version C of the DIR-625 router. Please verify the version number of your router by checking the sticker on the back (Figure 2.1). Attempting to upgrade a DIR-625 router that is not H/W Ver. C can damage it.
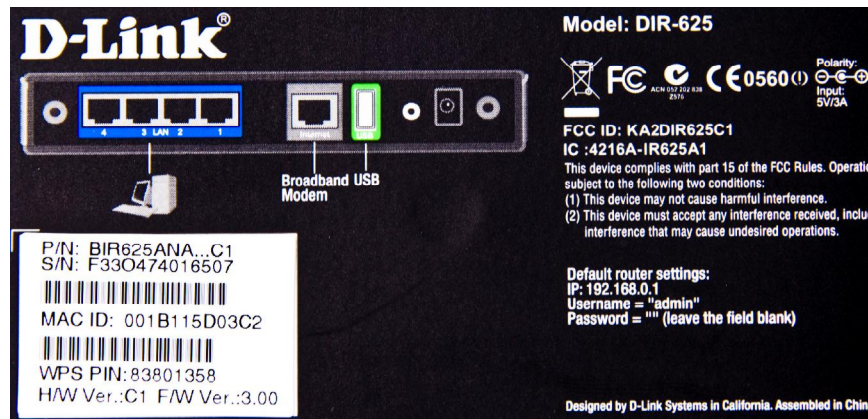
Figure 2.1: Router Setup Page

3. Ensure that you are connected to the router with an Ethernet cable.

4. Do NOT attempt a firmware upgrade from a wireless connection. You could damage your router due to the increased packet loss from a wireless connection. Be sure you are connected to your DIR-625 with an Ethernet cable.

5. Make sure that your router is connected to the Internet.

Installing the Router

1. Install your new DIR-625 RangeBooster N™ Router using its installation CD, and ensure it is operating correctly.

2. SECURESPOT 2.0 services come pre-installed on new DIR-625 Routers (Figure 2.2).

    ▪   Existing DIR-625 users can obtain SECURESPOT 2.0 by upgrading their router firmware. See securespot.dlink.com for firmware and instructions.

    ▪   DIR-625 users can also check this site for firmware that includes SECURESPOT 2.0 services, or to be notified as it becomes available. (See Appendix A for router upgrade instructions.)

3. Ensure your RangeBooster N™ Router is operating correctly and communicating with the internet.

Now that you have installed your router and obtained SECURESPOT 2.0, you are ready to begin. However, before SECURESPOT 2.0 services can start protecting your home, they must first be activated. Activation procedures will be described in the next section of this manual.
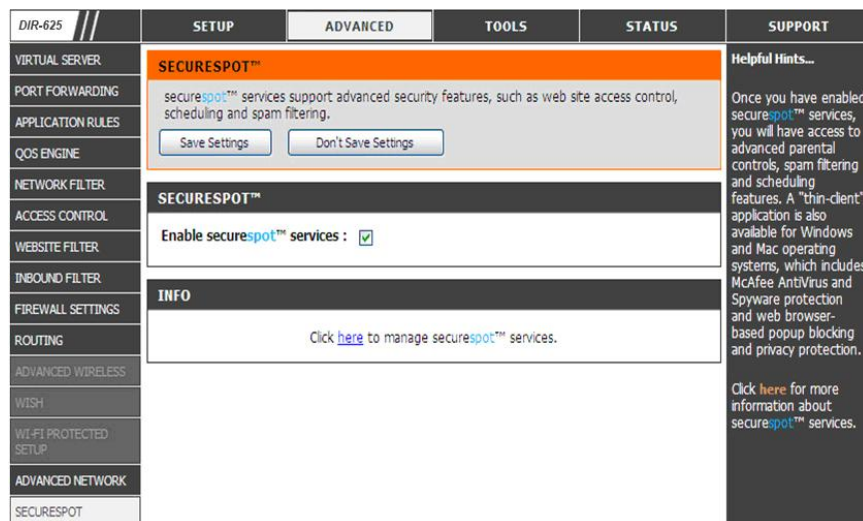
Figure 2.2: Router Setup Page

Activation and Registration

SECURESPOT 2.0 services are easy to activate, register, and configure. Just follow a few simple steps and you will be ready to begin using the services. First you will need to activate the services using the following steps.
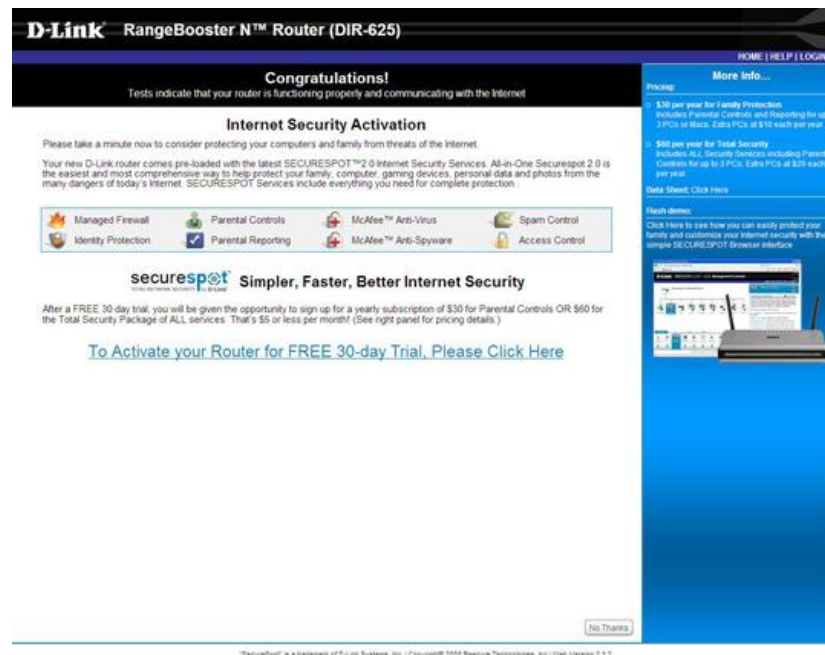
Figure 2.3: Initial Registration Page

Activation Procedure

1. Open a Browser and go to any Web site.

2. You will be redirected to the SECURESPOT 2.0 Services Registration page (Figure 2.3).

3. If you do not see this page, try entering a different Web site since your browser might be displaying a cached page (for example, your browser's home page).

4. Click the **Activate** link to initiate SECURESPOT 2.0 services activation.

5. Once you click the Activate link, you are directed to the Registration Information page (Figure 2.4).

Figure 2.4: Registration Information Page

6. Enter the appropriate contact information, password, and select a security question and answer, respectively.

7. Click the Privacy Policy link located at the top of the Registration Information page to display the Privacy Policy (Figure 2.5). Click the [X] icon to close the Privacy Policy pop-up window*.*

Figure 2.5: Privacy Policy

8. Select the Service Agreement check box to continue registration (Figure 2.4).

9. Click **View** on the Registration Information page to display the Terms and Conditions Agreement (Figure 2.6). Click the X icon to close the Terms and Conditions pop-up window.
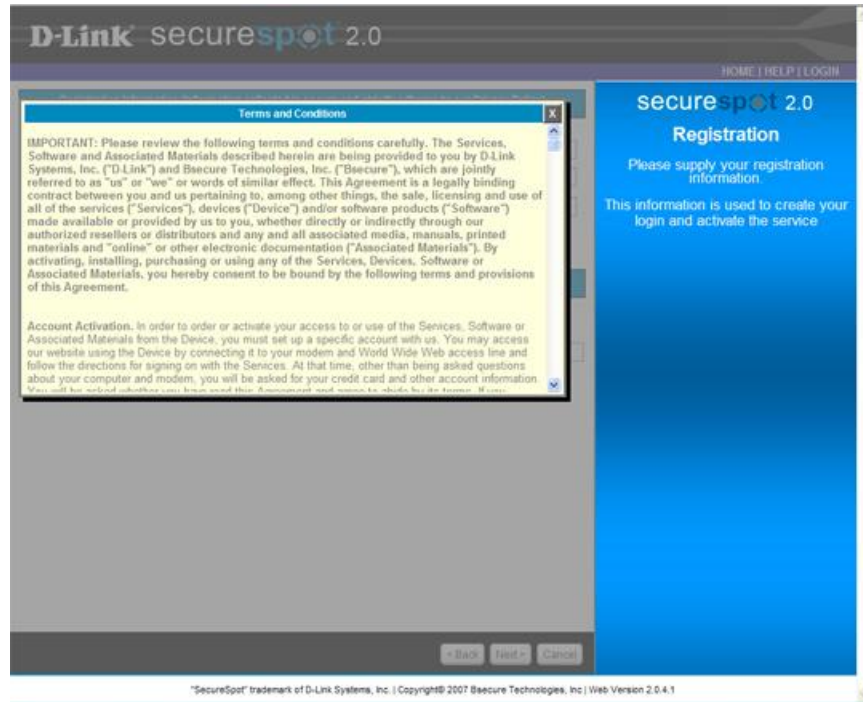
Figure 2.6: Terms and Conditions

10. Click **Next>** on the Registration Information page. (Please wait while the request is being processed.)

11. Once your request has been processed, you will be directed to the SECURESPOT 2.0 Management Console (Figure 2.7) and automatically logged in using the information you supplied on the Registration Information page.

Figure 2.7: SECURESPOT 2.0 Management Console

Congratulations! SECURESPOT 2.0 security services are now activated on your DIR-625 RangeBooster N™ Router, and protecting you and your family with default settings. To customize your configuration and learn how to register additional computers, please continue to the next section.

3. Management Console

The Management Console is a Web-based interface that allows you to review and modify settings for SECURESPOT 2.0 services on the network level, for individual computers and devices, and for the general "Guest Account." The Management Console consists of three sections and a top banner:

- **Network Map** – top left side of screen
- **Tab Bar** – bottom of screen
- **Options and Configuration Section** - right side of screen
- **Navigation Banner** – top right above Options and Configuration Section

Network Map

SECURESPOT 2.0 creates a graphical Network Map of the computers and other devices that share your Internet connection such as game consoles (Figure 3.1). The first time the Network Map appears, you will see DIR Router, Guest Setup, the computer you registered on (primary device, and other known and unknown network devices.

Initially, the Network Map is only populated with the computer you used to activate your SECURESPOT 2.0 services, and a guest computer setup. As new computers and devices in your home connect to the Internet you will be able to register, connect, and integrate them into your SECURESPOT network. This process will be covered in greater detail under Access Control in this user manual.
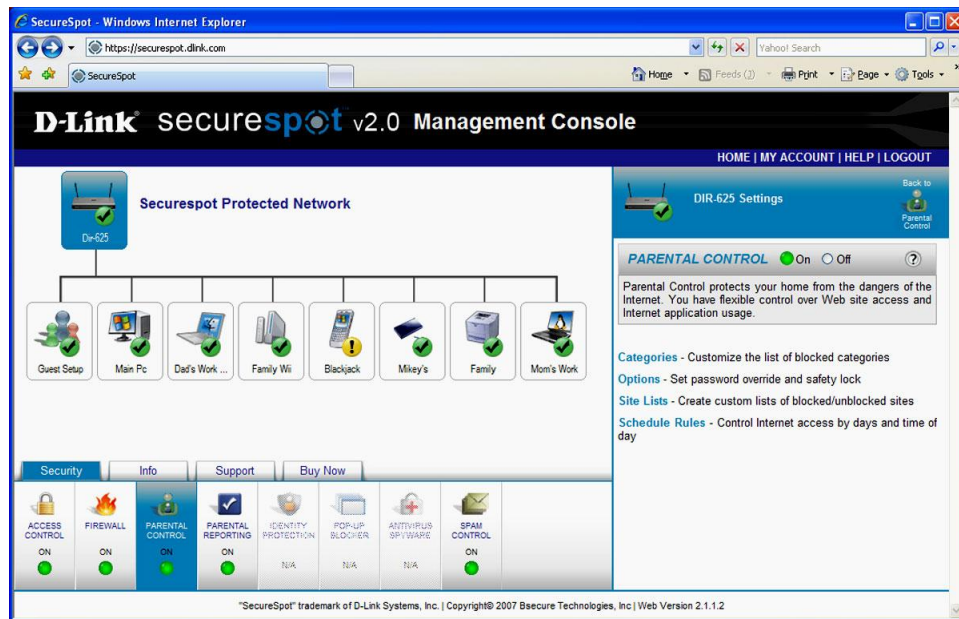
Figure 3.1: Fully Populated Network Map

Tab Bar

The Tab Bar allows you to make changes and verify information concerning the devices on your network quickly and easily. When making a change to an individual computer or device, select the icon representing that device and proceed. You also have the option of making updates that will affect the network as a whole by selecting the router icon located at the top of the Network Map. After you select the device or network, you can make changes by clicking on one of the function tabs. The Tab Bar consists of four functions:

- **Security** – Displays the status for each security service by network device selected.
- **Info –** Provides information about the device you select in the Network Map.
- **Support** – Provides multiple options for accessing technical support.
- **Buy Now** - Displays the SECURESPOT 2.0 Upgrade link.

After you select a function, a bar displaying the function features will appear. Clicking the individual features provides more options. The four functions will be covered in more detail in separate sections of the user manual.

Options and Configuration Section

The Options and Configuration Section of the Management Console provides information on the services you have highlighted on the Network Map and Tab Bar. It is also the area that allows you to make and save updates to your network. When you click a function or service on the Tab Bar, a corresponding panel is displayed on the right hand side of the screen. You then click the options, features, and links to update your network. You may find exploring the different panels displayed in the Options and Configuration Section useful when trying to understand how to manage the numerous services available through SECURESPOT 2.0.

Knowing the following icons will help you perform actions more effectively:

- ⊖ - Hide
- ⊕ - Expand
- ⑦ - Descriptive Information

The Hide and Expand icons allow you to control the amount of information displayed in the panel. Clicking the Descriptive Information icon on the service provides a number of links for further options. The Options and Configuration Section allows you to search through the panels without making unwanted changes to your network. Updates will not be made until you decide to update and save changes. Also, you may return to the functions on the tab bar by clicking the service icon displayed at the top of the section.

NOTE: Clicking the service icon at the top of the section to return to a function area before saving will cancel your actions.

Navigation Banner

The Navigation Banner, located at the top of the Management Console above the Options and Configuration Section, contains links to the SECURESPOT 2.0 Home page, Account Information, Help, and Logout links. Click the individual links for more information.

- **Home** - Click the Home link at the top of any SECURESPOT 2.0 page to return to the SECURESPOT 2.0 Services landing page.

- **My Account** - Click the My Account link at the top of any SECURESPOT 2.0 services page to open the My Account panel. NOTE: This is the same panel found by

clicking the Support function tab and selecting the My Account service. You will learn more about My Account in the Support Function Section of this user manual.

- **Help** - Click the Help link to open the Support tab. The right panel includes all necessary support information.

- **Logout** - Click the Logout link at the top of any SECURESPOT 2.0 Services page to close SECURESPOT. NOTE: You will be redirected to the "My Account" Web Control Center, the SECURESPOT 2.0 Security Login page (Figure 3.2).

Figure 3.2: "My Account" Web Control Center Login Screen

4. Access Control

The Access Control service of SECURESPOT 2.0 prevents computers on your network from accessing the Internet until you have performed a one-time registration using your administrative password. (The administrative password is the one you created to log in to your SECURESPOT account.) This provides an additional layer of security to prevent unauthorized computers from using your Internet connection, even if they are connected to your router via a wireless connection or Ethernet cable.

The Access Control is one of the services found under the Security Function (Figure 4.1). Access Control is turned on by default to provide additional security. As you registered computers and other network devices, they will be automatically added to your Network Map and available for you to configure. To configure a computer or device in your home, you simply click it to highlight, and then select the service you wish to configure.

Should an unregistered computer require Internet access, Access Control provides a temporary 24-hour Guest Account with Parental Control and Parental Reporting services pre-configured. By default, the Guest Account does not require a password, but you have the option to create a separate, easy-to-remember Guest password.

Figure 4.1: Security Function Tab

New Computer Registration

In order for new computers and devices to appear on the Network Map and be available for configuration and customization, they must first be registered so they are recognized by SECURESPOT 2.0 Services. There are two ways to register a device.

1. **Access Control Turned On** (default setting) - When computers access the Internet for the first time, they will be prompted to register using the administrative password. They will also have the option to use the Guest Account, which does not require the administrative password.

2. **Access Control Turned Off** - SECURESPOT 2.0 will detect devices as they connect to the Internet, place them on the Network Map, and allow you to register them from the Management Console.

The next parts will guide you through new computer registration using the above two methods.

Computer Registration (Access Control On)

As you open Web browsers on additional computers in your network, the **Access Control** service prompts you on how you would like to connect to the SECURESPOT 2.0 network.

To register a computer with Access Control On

1. When a new device accesses the Internet for the first time, a **New Computer Detected** box (Figure 4.2) appears on your screen. You will have the option to register the computer or use the Guest Account settings.

Figure 4.2: Access Control Page

2. Click **Register This Computer**.
3. NOTE: Game consoles may have browsers that do not work properly with the New Computer Detected page. Should you encounter a problem, it is recommended that you use the second method (Access Control Off) described further in this section to register game consoles.

Figure 4.3: Access Control New Device Registration Page

4. Create a computer name and enter the administrative password (Figure 4.3).

5. Click **Register This Computer** on the New Computer Detected box.

Figure 4.4: Access Control Thin Client (Endpoint Security) Download Page

6. You will be prompted to download the Thin Client (Figure 4.4).

7. Click Download to install and activate Thin Client (Endpoint Security) services, which include AntiVirus/Spyware Protection, Identity Protection, and Pop-up Blocking. (NOTE: This feature is unavailable for Mac users at the present time.)

8. If you do not wish to enable Thin Client, click **No Thanks**.

9. NOTE: You may install the Thin Client at any time in the future by clicking one of the Thin Client (Endpoint Security) required services (AntiVirus/Spyware Protection, Identity Protection, and Pop-up Blocking) found under the **Security** tab on the Management Console.

10. After selecting either **Download** or **No Thanks**, a status bar will appear on the New Computer Detected page. It may take a moment for SECURESPOT 2.0 Services to process your request.

11. If you did not choose to download the Thin Client, you will automatically be redirected to the Access Control Page (Figure 4.2).

12. If you selected to download the Thin Client(Endpoint Security), you will be redirected the Thin Client download page.

13. If Internet Explorer blocks you from downloading the Thin Client application to your computer, click **Download File**.

Figure 4.5: Explorer Download File Page

14. A **File Download** pop-up window appears on your screen (Figure 4.5). Click **Save** to install the Thin Client later, or **Open** to install the Thin Client now. NOTE: Thin Client operation and features will be covered in the next section of the SECURESPOT 2.0 User Manual.

15. Once the download is complete, your Web browser is redirected to the SECURESPOT 2.0 Management Console with the new device added to the Network Map (Figure 4.6).

Figure 4.6: Network Map with New Device Added

Registering Device as Guest Account

The alternative means of connecting a computer to the SECURESPOT 2.0 network is to use the Guest Account settings, which will allow temporary access to the SECURESPOT 2.0 network for 24 hours.

To register a guest account

1. When accessing the Internet with Access Control turned on, a **New Computer Detected** page will appear on your screen.

2. Click **Guest Account**. A status bar will appear – "Please wait while SECURESPOT 2.0 processes your Guest Account request" (Figure 4.7).

Figure 4.7: New Computer Detected Page with Status Bar

3. Once SECURESPOT 2.0 processes your Guest Account request, you will be redirected to the page you were attempting to access.

4. Your new device is now registered and will appear on the Network Map as Guest 1.

Computer Registration (Access Control Off)

If Access Control is turned off, computers and other devices will be automatically detected when they connect to the router by either an Ethernet or Wireless connection. They will first appear on the Network Map as an unknown device. Unknown devices will automatically be protected by the router. However, if you wish to configure unknown devices separately and customize their security services, you will need to register them using the Wizard (Figure 4.7).
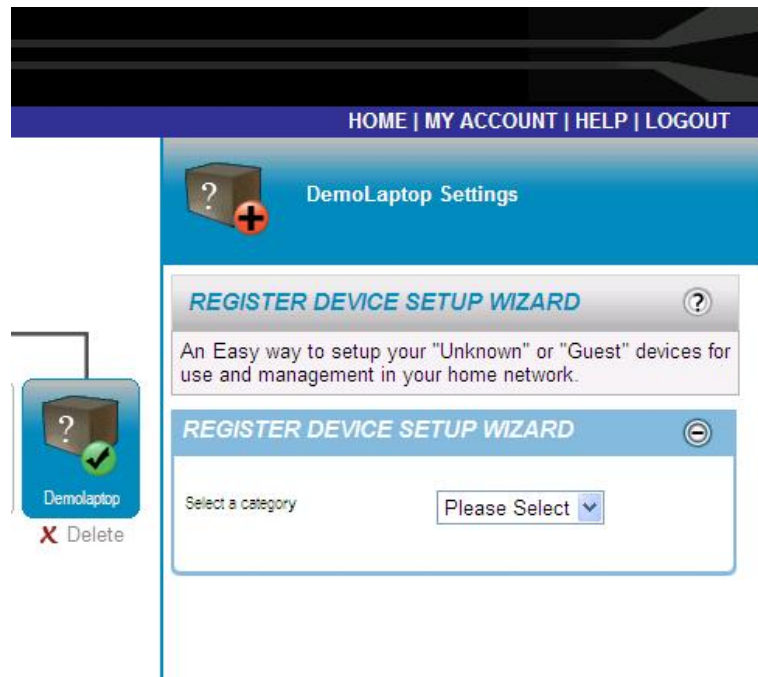
Figure 4.8: Register Device Setup Wizard

Register Device Setup Wizard

The Wizard is a simple way to register unknown or guest devices in your home network.

To register an unknown or guest device

1. Click (highlight) the Unknown or Guest Device. The Register Device Setup Wizard will appear.

2. Select a device in the **Category** drop-down list box (Figure 4.8).

3. Once you select a category, the Install a Network Device panel expands.

4. Select the Type and Operating System from the drop-down menu (Figure 4.9).

5. **Device Name** option allows you to choose a name that will appear on your Network Map.

6. MAC Address and IP Address are automatically populated by the Wizard.

7. Click **Update**.

8. Click **Apply Settings**.
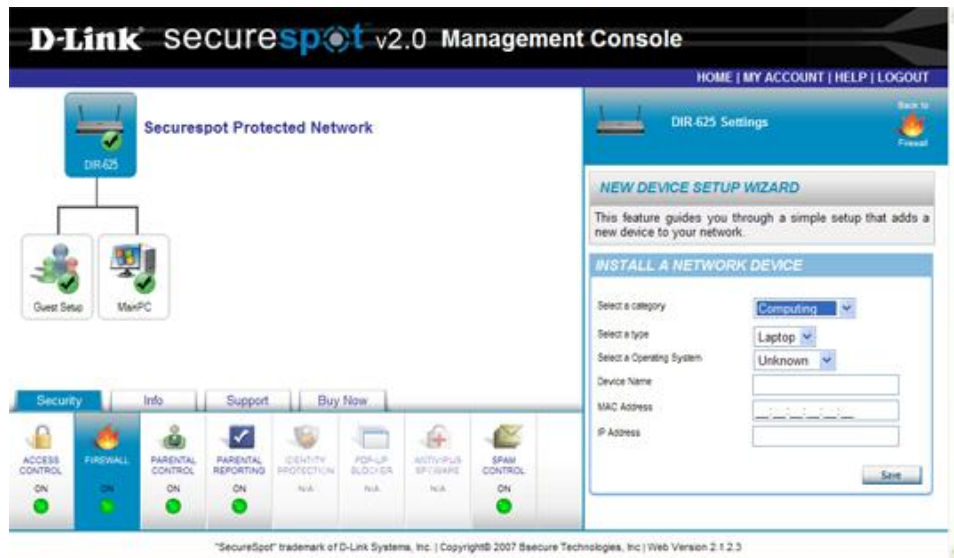
Figure 4.9: Wizard Drop-down Menu

Deleting a Device from the Network Map

There may be times you will want to temporarily or permanently choose to remove a device from your SECURESPOT network (e.g. delete a guest account before the 24 hour, retire a device, etc).

To delete a device from your home network

1. Select a device on the Network Map that you want to delete.

2. Click the X icon (delete) located under the highlighted device.

3. A pop-up window will appear on the screen prompting you for a response.

4. Click **OK** to delete the highlighted device.

5. Once your setting has been saved, the message "**Selected Device deleted**" appears on the Network Map.

5. Thin Client (Endpoint Security) Installation

The SECURESPOT services available through the Thin Client application are:

- Identity Protection
- Pop-up Blocker
- AntiVirus/Spyware Protection

Downloading Thin Client Services

The protection offered by the Thin Client is at the endpoint or PC level. Therefore these services are only available on the individual PCs you actually download and install the Thin Client (Endpoint Security). Although you will be prompted to install the Thin Client application when you register a computer, you may install the service at any time. (NOTE: This application is unavailable for Mac users at the present time.)

To download Thin Client

1. Open a Web browser to the SECURESPOT 2.0 "My Account" Web Control Center login screen (Figure 3.2) on the computer you wish to install the Thin Client and log in.

2. Select the computer on which you wish to install Endpoint Security.

3. Click one of the Thin Client service tabs (ID Protect, Pop-up Blocker, or AntiVirus).

4. Select **Download** in the Options and Configuration Section and follow the onscreen instructions to install the Thin Client. NOTE: It is recommended that you choose **Run** rather than **Save**.

5. Once the installation is complete, you will be forced to restart your computer. As your system restarts, a splash screen appears indicating that the latest virus definition files will be downloaded (Figure 5.1).

Figure 5.1: Thin Client Download Page

6. After the Thin Client has been installed, you will see the SECURESPOT icon on your desktop and in your system tray.

7. You will also see a recommendation to run a full virus scan. (Figure 5.2)

8. NOTE: SECURESPOT 2.0 Endpoint Security **does not** require a full system scan in order for real-time protection to be active.

9. Click Next to take you to the "My Account" Web Control Center login screen with your account E-mail address pre-populated.

Figure 5.2: Download Complete

Accessing and Modifying the Thin Client

The Thin Client application can be accessed and modified two ways:

- **Network Map** - When using the Network Map, you must be physically logged on to the computer you wish to make changes.
- **System Tray** - Right-clicking the SECURESPOT system tray icon on any machine where the Thin Client has been installed will provide you with a pop-up menu that you can use to modify the settings of the machine you are currently using.

The **Open** option will open your default Web browser to the "My Account" Web Control Center Login Screen. As long as the Thin Client is installed and running properly, you should see your account e-mail address automatically populated when you open the Network Map in this manner.

You can also access the Network Map by double-clicking the desktop icon.

Open Intrusion Detection

Open Intrusion Detection opens the Internet Application List, which displays a list of programs that have been previously blocked or allowed (Figure 5.3). The Internet Application List is not shared, but specific to each computer. From here you can:

- Highlight a program or process and change its permission to either **Block** or **Allow** by clicking the options under Permissions.
- Select **Refresh** to see the most recently updated list of blocked and allowed applications.
- Highlight an application and select **Remove** to delete it from the list. NOTE: You must click **Apply** to save your changes.
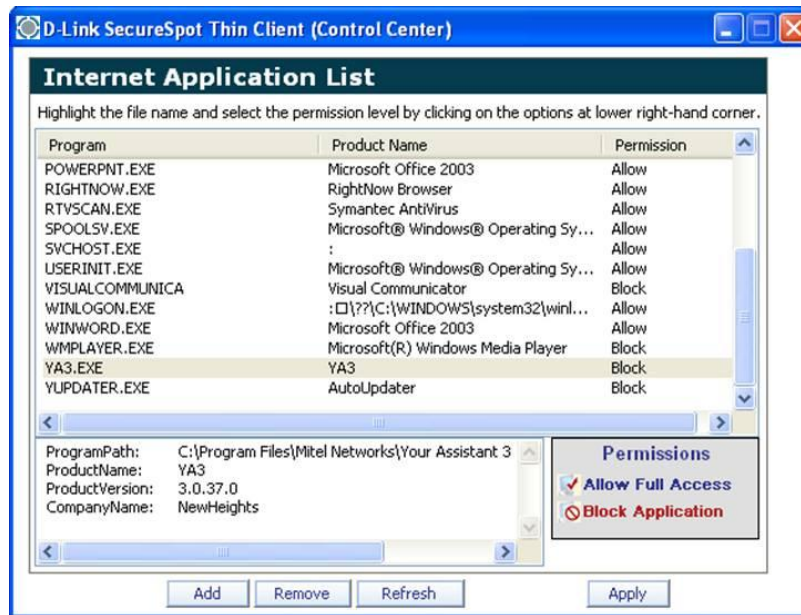
Figure 5.3: Internet Application List

AntiVirus Center

The AntiVirus Center feature gives you access to the AntiVirus/Spyware scanning and scheduling tools.

Scan My Computer - Opens the manual scan interface. Here you have the option to scan all or specific file types as well as what action to take if problems are detected. You have the option to select specific directories to scan, or use the **Scan All** button to run a complete system scan.

Scheduled Scans - Opens the Scheduled Scans interface, where you can add, remove, edit, or run scheduled scans. A default daily scan, which occurs at 12:00 am, is provided when the Thin Client is installed. NOTE: A computer must be turned on at the scheduled time in order for a scan to occur.

Scan History Log - Shows the results of previous scans until you remove individual results, or clear the log.

Download Latest Virus Definitions - Opens the manual update screen. Click **Next** to look for new virus definitions. If there are newer virus definitions available, they will be automatically downloaded. If your definitions are up-to-date, you will be notified that this is the case.

Quarantined Files opens the list of potentially dangerous programs. NOTE: Since the Quarantined File List is specific to each computer, this list is not shared from one computer to another. In order to manage the quarantined files you should:

- Double-click each entry to find detailed information on each file.
- Use the **Remove** button to completely remove the file from your computer.
- Use the **Restore** button to restore the file on your computer.

NOTE: **Real-time Protection** is enabled by default.

Identity Protection

Identity Protection guards against identity theft. You are required to provide the SECURESPOT 2.0 administrative password before being able to view or modify the settings. (NOTE: This service is only available in Internet Explorer.)

Protected Information – Area to add private data that you wish to be protected, such as account IDs, passwords, Social Security numbers, etc.

Trusted Sites – Area for Web sites that require trusted information that would normally be blocked. For example, you may have entered your online banking password in the protected data area, but you can also add your online bank Web address to the trusted sites list so you will not be prompted every time you try to log in.

When you are in **Internet Explorer**, you will see the Identity Protection prompt any time you try to transmit your protected data to a site that isn't on your trusted site list.

Popup Blocker

Pop-up Blocker includes the following:

- The **Settings** option determines how the pop-up blocker notifies you when a pop-up is blocked.
- The **Allowed List** is useful for sites which include login screens that are treated as pop-ups.

Internet Protection Settings

The Settings option support troubleshooting and displays various tools including:

- Service Log
- Offline Help
- Re-Authenticate
- Uninstall

You can also choose to show or hide the desktop icon and startup splash screen.

Thin Client Upgrade

The Upgrade is used to check if you have the latest version. If there is a newer version available, clicking on Thin Client Upgrade will prompt the download process. If you have the latest version available, you will see the "latest client version installed" message.

Reauthenticate

Reauthenticate from the systems tray is used to manually reauthenticate the Thin Client, similar to Reauthenticate in the Settings window. NOTE: You will not see any visual feedback indicating that reauthentication has taken place.

About

This item displays the Thin Client version number.

6. Security Function

Security Function Tab

To customize the individual security services, click the appropriate service icon under the Security function tab. NOTE: Identity Protection, Pop-up Blocker, and AntiVirus/Spyware will not be active unless you have signed up for the Endpoint Security. The services available are:

- – The **Access Control** service allows computers to attach to the network without requiring a Thin-Client installation for AntiVirus and Spyware protection.

- – The **Firewall** service increases PC security by controlling access to incoming and outgoing Internet ports.

- – The **Parental Control** service protects your home from dangers of the Internet, while giving you flexible control over Web sites and Internet application usage.

- – The **Parental Reporting** service creates a historical record of the Web sites that can not be altered or erased. The record is updated daily. Archived reports contain the profile, date, Web site visited, Web site category, number of hits, and age group, and are displayed at any time by the account administrator. Historical information is supplied in a calendar format for up to 2 weeks. Additionally, the Reporting service contains a Parental Notification feature that enables you to receive alerts via e-mail and/or short message service (SMS) whenever a user attempts to access a blocked Web site. NOTE: Currently, the 2.0 release is not enabled to send alerts for all categories. It will only send alerts when a user attempts to access a pornography or R-rated Web site.

- – The **Identity Protection** service encrypts and securely stores your personal identification and financial information, protecting you from malicious applications searching for sensitive information, i.e., credit card numbers and bank account information. NOTE: Service provided only through Endpoint Security (Thin Client).

- – The **Pop-up Blocking** service prevents unwanted and annoying pop-up windows from appearing while you surf the Internet. NOTE: Service provided only through Endpoint Security (Thin Client).

- – The **AntiVirus/Spyware** service protects your computer from viruses that infect your system and spyware that tracks your Web-browsing habits and steals your personal information. NOTE: Service provided only through Endpoint Security (Thin Client).

- – The **Spam Control** service saves time and protects your computers by helping redirect junk, phishing, and pharming e-mails to Spam folders. You may use this area to define a personal tag for unwanted e-mails. This feature uses a series of techniques to tag unwanted e-mails with a user-defined prefix. Suspected junk e-mail contains this prefix in the subject line of your incoming e-mail.

Security Function Navigation

Figure 6.1: Security Function Tab Bar

Access Control – Enable or disable this service, additionally you can set the Guest Password, change the Master Password and change the Master Password retrieval question and answer.

Firewall – Any configuration of the firewall is always done at the router level. If a device is selected and you click on the Firewall service you will be asked to "Click here to view the Router's Firewall Options." This will then selected the router and give you the following options to configure.

- Install Network Device
- Install Network Application
- Virtual Server
- Port Forwarding
- Application Control
- Schedule Rules

Parental Controls – These can either be handled at the network level or the device level. After clicking on the Parental Control icon you will be given the following options

- Site Categories
- Safety Lock
- Password Override
- Custom Block List
- Custom Allow List
- Schedules

Parental Reporting –The services available for configuration for this icon are:

- Parental Notification
- Archived Reports. NOTE: This will show the log for every device on the network regardless of which device is selected when viewing the report.

ID Protection, Popup Blocker, and AntiVirus/Spyware – These services are only available to a device that has the Thin Client installed.

Spam Control – Services can be configured at the Network Level or Device Level

- Tag
- Source List

Access Control Service Navigation

You have already been introduced to the Access Control service when you registered your computer. Access Control is a service under the Security function provided through SECURESPOT 2.0, Following are a number of other procedures available to you with the Access Control service. NOTE: Access Control is managed at the network perimeter. You must have the router highlighted in order to make any changes.

This service detects computers and other devices as they attach to your network. The Access Control service prevents neighbors and hostile devices from attaching to your network. It also allows you to provide temporary access to your network through 24 hour Guest Accounts.

NOTE: As you perform the following procedures, you will be asked to click **Save** to save your new settings. At times you will also be prompted to click **Apply Settings.**

To enable Access Control (Figure 6.2)

1. Select the **DIR-625** icon on the Network Map.

2. Click the **Access Control** service under the **Security** tab.

3. Click ⑦ on the Access Control panel to hide/display descriptive Access Control information.

4. Select the **ON** option (green) button to enable the Access Control service.
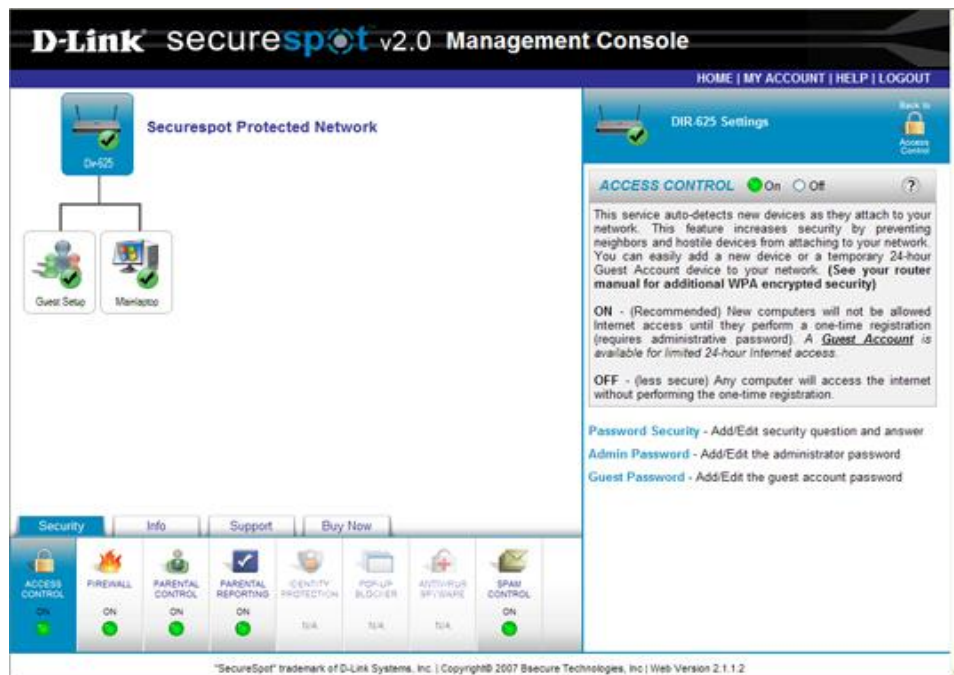
Figure 6.2: Access Control

To view and/or change your Password Information (Figure 6.3)

1. Click the **Password Security** link on the Access Control panel.

2. Type a security question and answer in the provided fields.

3. Click **Save** to save your settings.

4. Once your settings have been saved, the message "**Security Information saved**" appears on the Password Security panel.

Figure 6.3: Password Security

To view and/or change the Master Password (Figure 6.4)

1. Click the **Admin Password** link on the Access Control panel.

   NOTE: The administrative password is the password that you created when registering the SECURESPOT 2.0 services.

2. Type your current password, type a new password, and then confirm the new password.

3. Click **Save** to save your settings.

4. Once your settings have been saved, the message "**Administrative Password saved**" appears on the Admin Password panel.

Figure 6.4: Admin Password

To view and/or change the Guest Account Password (Figure 6.5)

1. Click the **Guest Password** link on the Access Control panel.

2. Type your current password, type a new password, and then confirm the new password.

3. Click **Save** to save your settings.

4. Once your settings have been saved, the message **"Guest Password saved**" appears on the Guest Password panel.

Figure 6.5: Guest Password

7. Firewall Service

The Firewall feature increases network security by controlling access to incoming and outgoing Internet ports. While important services use these ports, they may also be used as entry points by other unwanted services, hackers, and trojan programs.

Firewall Navigation

The Firewall service is controlled at the router or perimeter level. You may access the service by clicking Firewall on the Security function tab at the router level or when an individual computer or device is highlighted as discussed below. NOTE: If you access the Firewall service at the router level, you will bypass the panel with the orange banner display.

NOTE: As you perform the following procedures, you will be asked to click **Save** to save your new settings. At times you will also be prompted to click **Apply Settings.**

To enable the Firewall (Figure 7.1)

1. Select a specific PC or device on the Network Map.

2. Select **Firewall** service under the Security tab.

3. Click the **Router Firewall Options** (orange banner) to view and/or change the Router Firewall settings (**ON** is the default). NOTE: Since the Firewall service is controlled at the network perimeter (gateway), this step redirects you to the router.
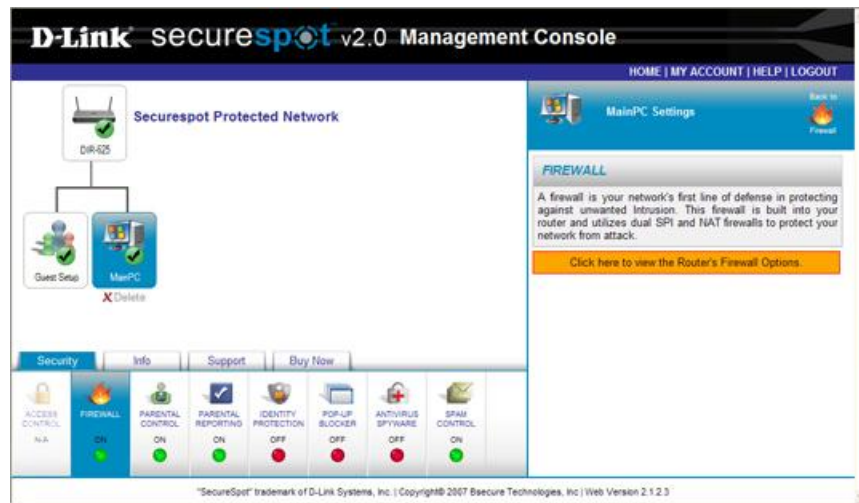
Figure 7.1: Router Firewall Options

To add a network device using the New Device Setup Wizard

1. Click the **Install Network Device** link on the Firewall panel (Figure 7.2).

2. Select a device in the **category** drop-down menu (Figure 7.3).

3. Once you select a category, the Install a Network Device panel expands.

4. Select the type and operating system and enter the appropriate **Device Name**, **MAC Address**, and **IP Address**.

5. Click **Save** to save your settings.
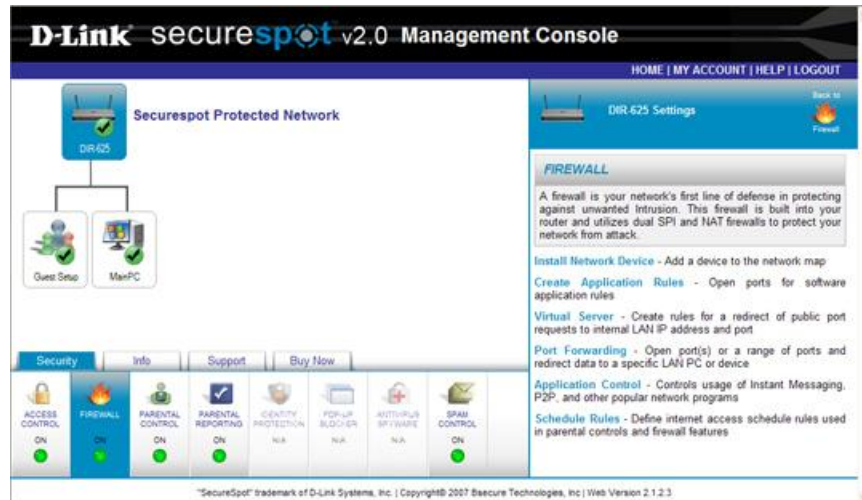
Figure 7.2: Firewall Panel
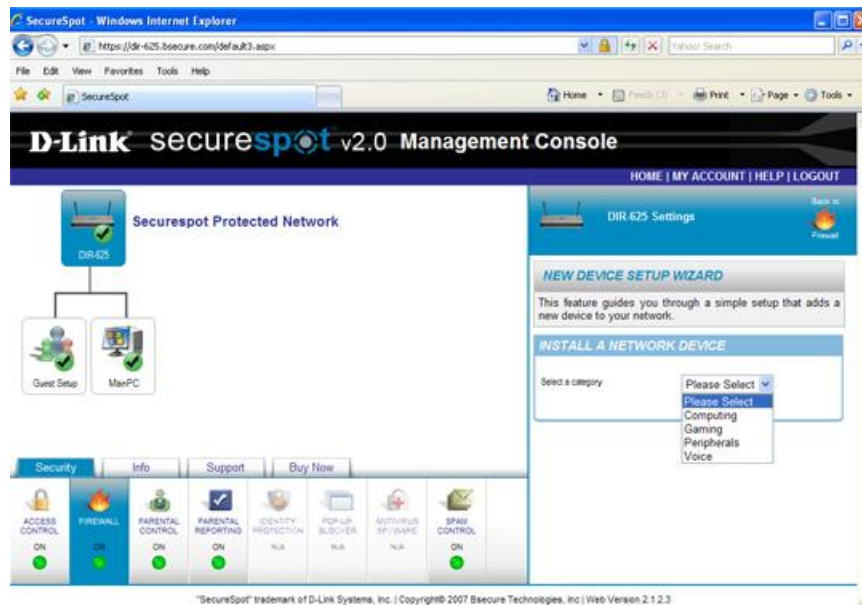
Figure 7.3: New Device Setup Wizard

To add a new application rule to your network (Figure 7.4)

1. Click the **Create Application Rules** link on the Firewall panel.

2. Select an application in the drop-down menu.

3. Select the device in the **Create rule for** drop-down menu that you want to create an Application rule for.

4. Click **Create Rule** to save your settings.

5. Once your settings have been saved, the message "**Application Rule Created**" appears on the Application Setup Wizard panel and the newly created Application Rule is added.

6. Once a rule has been created, you may manage this rule under Port Forwarding or Application Control option. Note that only AIM Talk, Bit Torrent, Calista IP Phone, ICQ, and PalLTalk can be managed from Application Control.

NOTE: To define a single public port on your router for redirection to an internal LAN IP address and private LAN port, click the Virtual Server link on the Firewall panel.

Figure 7.4: Add New Application Rule

To add a Virtual Server Rule (Figure 7.5)

1. In the **Application Name** drop-down menu, select the application and its associated ports and protocol that you want to allow access to your network or device.

2. Select the **«** character to populate the appropriate Name, Ports, and Protocol for the selected application.

OR

1. Enter the Name, Ports, and Protocol to create a new application server setting.

2. In the **Computer Name** drop-down menu, select the appropriate device that you want to allow access.

3. Select the **«** character to populate the appropriate IP Address for the selected device.

OR

1.   Type the IP Address of the device that you want to allow a specific port.

2.   In the **Schedule** drop-down menu, select **Always** or a previously created schedule for which you want to allow Internet access.

3.   In the **Inbound Filter** drop-down menu, select **Allow All** to open a single port in your router and redirect this data through this port to a single device on your network.

4.   Select the **Enabled** check box if you want to enable the Virtual Server Rule on the router also.

5.   Click **Save** to save your settings. Once your settings have been saved, the message "**Virtual Server Rule Created**" appears on the Virtual Server panel.

6.   The newly created Virtual Server Rule is added to the Virtual Servers List.
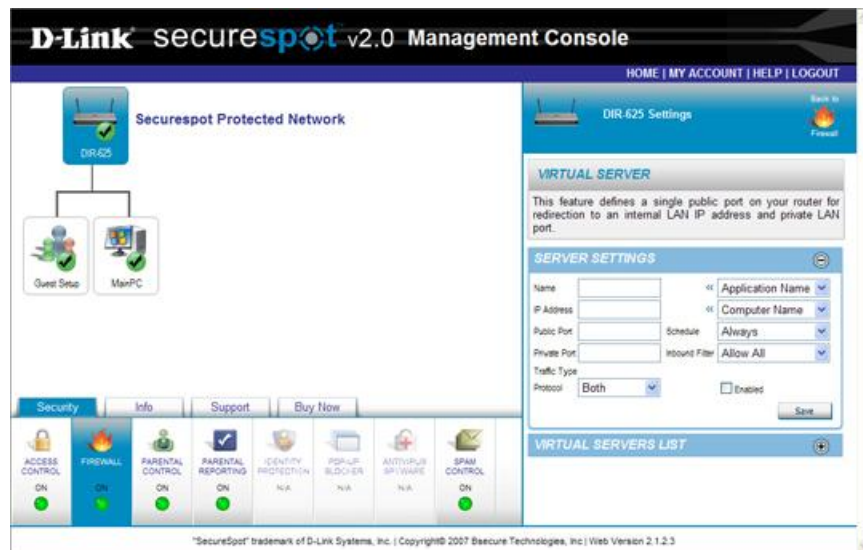
Figure 7.5: Add a Virtual Server Rule

To edit a Virtual Server Rule (Figure 7.6)

1. Click the ⊕ icon to expand the **Virtual Servers List** panel.

2. Select the 📝 icon to edit a Virtual Server Rule. NOTE: The previously-saved Virtual Server Rule input appears in the Server Settings panel.

3. After changes have been made to the Virtual Server Rule, click the **Update** button on the Server Settings panel.

4. The updated Virtual Server Rule is added to the Virtual Servers List.

To delete a Virtual Server Rule

1. Click the ⊕ icon to expand the Virtual Servers List panel.

2. Select the ✗ icon beside the Virtual Server Rule that you want to delete.

3. Once the Virtual Server Rule has been deleted, the message "**Virtual Server Rule Removed**" appears on the Virtual Server panel.

NOTE: To open multiple ports or a port range in your router and redirect data through those ports to a single PC on your network, click the **Port Forwarding** link on the Firewall panel.
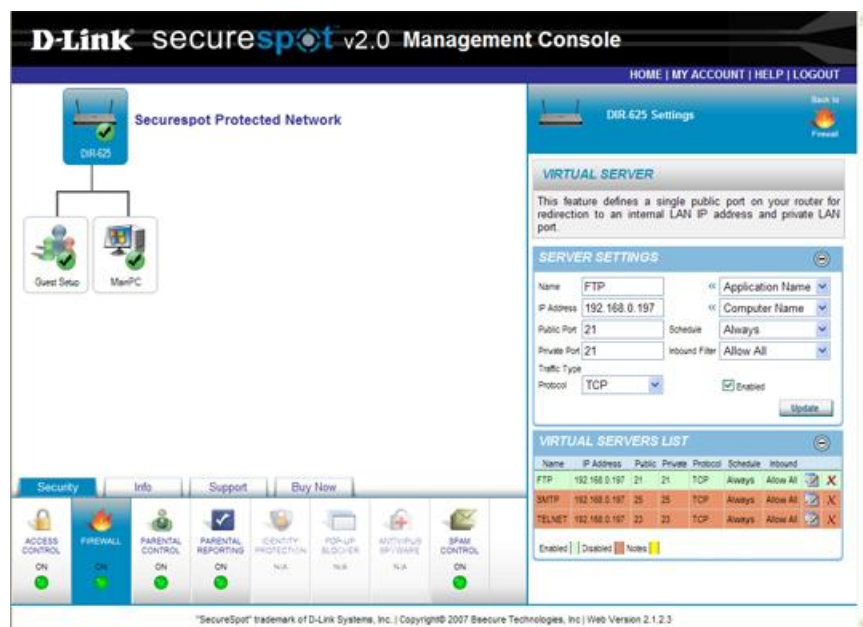
Figure 7.6: Edit a Virtual Server Rule

To allow individual ports, mixed ports, or port ranges (Figure 7.7)

1. In the **Application Name** drop-down menu, select the application and its associated ports that you want to allow access to your network or device.

2. Select the **«** character to populate the appropriate Name, TCP Ports, and UDP Ports for the selected application.

<div align="center">OR</div>

3. Type the Name, TCP Ports, and UDP Ports to create a new application server setting.

4. In the **Computer Name** drop-down menu, select the appropriate device that you want to allow access.

5. Select the **«** character to populate the appropriate IP Address for the selected device.

<div align="center">OR</div>

6. Type the IP Address of the device that you want to allow ports or port ranges.

7. In the **Schedule** drop-down menu, select **Always** or a previously created schedule for which you want to allow Internet access.

8. In the **Inbound Filter** drop-down menu, select **Allow All** to open multiple ports or port range in your router and redirect this data through those ports to a single device on your network.

9. Select the **Enabled** check box if you want to enable the Port Forwarding Rule on the router also.

10. Click **Save** to save your settings.

11. Once your settings have been saved, the message "**Port Forwarding Rule Created**" appears on the Port Forwarding panel and the newly created Port Forwarding Rule is added to the Ports List.

Figure 7.7: Allow Ports

To block individual ports, mixed ports, or port ranges

1. In the **Application Name** drop-down menu, select the application and its associated ports that you want to block access to your network or device.

2. Select the **«** character to populate the appropriate Name, TCP Ports, and UDP Ports for the selected application.

<div align="center">OR</div>

1. Type the Name, TCP Ports, and UDP Ports to create a new application server setting.

2. In the **Computer Name** drop-down menu, select the appropriate device that you want to allow access.

3. Select the **«** character to populate the appropriate IP Address for the selected device.

<div align="center">OR</div>

1. Type the IP Address of the device that you want to allow ports or port ranges.

2. In the **Schedule** drop-down menu, select **Always** or a previously created schedule for which you want to allow Internet access.

3. In the **Inbound Filter** drop-down combo box, select **Deny All** to block multiple ports or port range in your router and deny data through those ports to a single device on your network.

4. Click **Save** to save your settings.

5. Once your settings have been saved, the message "**Port Forwarding Rule Created**" appears on the Application Control panel.

6. The newly created Port Forwarding Rule is added to the Ports List.

7. Select the **Enabled** check box if you want to enable the Port Forwarding Rule on the router also.
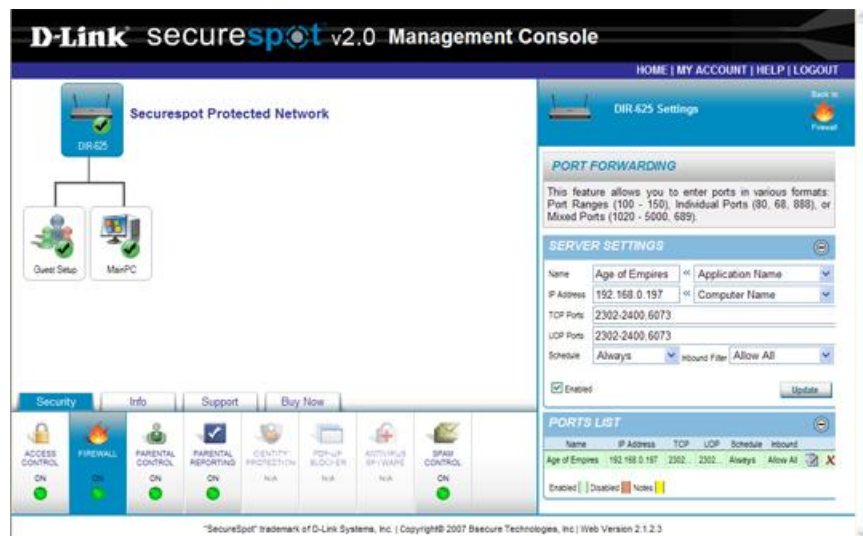
Figure 7.8: Edit Port Lists

To edit a Port Forwarding Rule (Figure 7.8)

1. Click the ⊕ icon to expand the **Ports List** panel.

2. Select the 📝 icon to edit a Port Forwarding Rule. NOTE: The previously-saved Port Forwarding Rule input appears in the Server Settings panel.

3. After changes have been made to the Port Forwarding Rule, click the **Update** button on the Server Settings panel.

4. The updated Port Forwarding Rule is added to the Ports List.

To delete a Port Forwarding Rule

1. Click the ⊕ icon to expand the Ports List panel.

2. Select the ✘ icon beside the Port Forwarding Rule that you want to delete.

3. Once the Port Forwarding Rule has been deleted, the message "**Port Forwarding Rule removed**" appears on the Port Forwarding panel.

NOTE: To control usage of Instant Messaging (IM), Peer-to-Peer (P2P) controls, and other popular network programs, click the **Application Control** link on the Firewall panel.

To allow applications (Figure 7.9)

1. In the **Application Name** drop-down menu, select the application that you want to allow access to your network.

2. Select the **«** character to populate the appropriate Name, Trigger Ports, Firewall Ports, and Traffic Type inputs for the selected application.

<div align="center">OR</div>

1. Type the Name, Trigger Ports, and Firewall Ports, and then select the associated Traffic Types that you want to allow access to your network.

2. In the **Schedule** drop-down combo box, select **Always** or a previously created schedule for which you want to allow this application.

3. Select the **Enabled** check box if you also want to enable the Applications Rule on the router.

4. Click **Save** to save your settings.

5. Once your settings have been saved, the message "**Application Rule Created"** appears on the Application Control panel.

6. The newly created Application Rule is added to the Applications List.
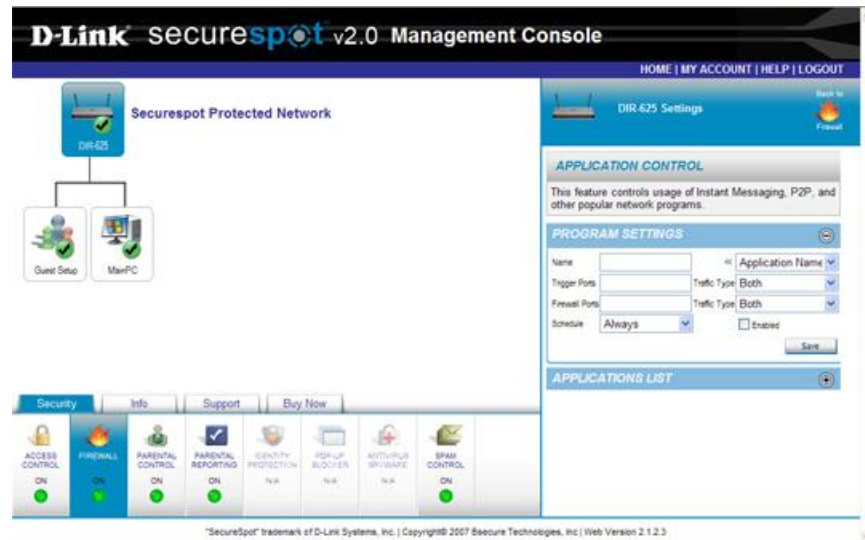
Figure 7.9: Create an Application

To block applications

1. In the **Application Name** drop-down menu, select the application that you want to block access to your network.

2. Select the **«** character to populate the appropriate Name, Trigger Ports, Firewall Ports, and Traffic Type inputs for the selected application.

3. Type the Name, Trigger Ports, and Firewall Ports, and then select the associated Traffic Types that you want to block access to your network.

4. In the **Schedule** drop-down menu, select **Never** to block this application.

5. Select the **Enabled** check box if you also want to enable the Applications Rule on the router.

6. Click **Save** to save your settings.

7. Once your settings have been saved, the message "**Application Rule Created**" appears on the Application Control panel.

8. The newly created Application Rule is added to the Applications List.
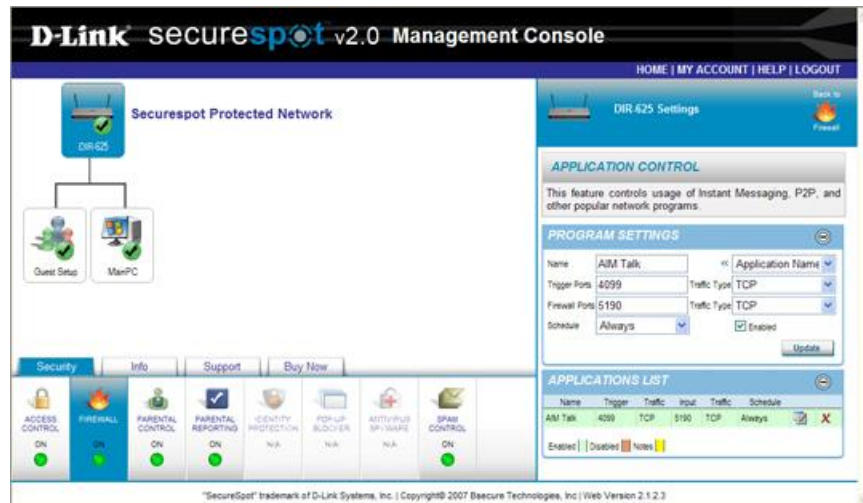
Figure 7.10: Edit an Application

To edit an Application Rule (Figure 7.10)

1. Click the ⊕ icon to expand the **Applications List** panel.

2. Select the 📝 icon to edit an Application Rule. NOTE: The previously-saved Application Rule input appears in the **Program Settings** panel.

3. After changes have been made to the Application Rule, click the **Update** button on the **Program Settings** panel.

4. The updated Application Rule is added to the Applications List.

To delete an Application Rule

1. Click the ⊕ icon to expand the Applications List panel.

2. Select the ✗ icon beside the Application Rule that you want to delete.

3. Once the Application Rule has been deleted, the message "**Application Rule removed**" appears on the Scheduling panel.

NOTE: To control Internet access, click the Schedule Rules link on the Firewall panel. Web browsing can be controlled by time of day and each day of the week.

To create a Schedule (Figure 7.11)

1. In the **Rule Name** text box, type the name of the schedule that you want to create.

2. Select the appropriate options for Days:

   a. All Week NOTE: If the All Week option button is selected, the individual day check boxes collapse (disappear).

   b. Select Day(s)

3. In the **Start** and **End Time** drop-down list boxes:

   a. Select the appropriate time. (Schedule times are hour and minute increments.)

   b. Select the **All Day** check box if you want to block Internet Access for 24 hours. NOTE: If the All Day check box is selected, the Start and End Time drop-down list boxes collapse (disappear).

4. Click **Save** to save your settings.

5. Once your settings have been saved, the message "**Firewall Schedule Created**" appears on the Scheduling panel.

6. The newly created schedule is added to the Schedules list.
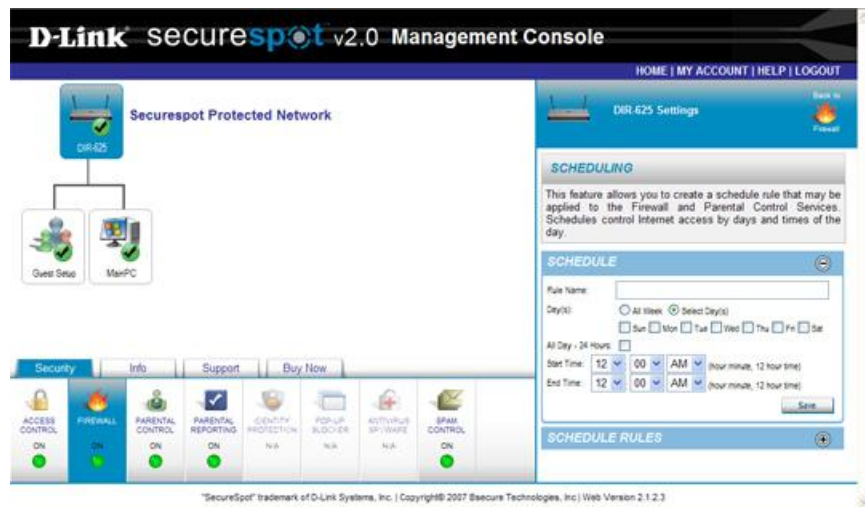
Figure 7.11: Create a Schedule

To edit a Schedule (Figure 7.12)

1. Click the ⊕ icon to expand the **Schedule** panel.

2. Select the 📝 icon to edit a schedule. NOTE: The previously-saved schedule input appears on the Controls panel.

3. After changes have been made to the schedule, click the **Update** button on the Controls panel.

4. The updated schedule is added to the Schedules list.

To delete a Schedule

1. Click the ⊕ icon to expand the Schedule panel.

2. Select the ✗ icon beside the schedule that you want to delete. NOTE: Schedules that are being used can not be deleted.

3. Once the schedule has been deleted, the message "**Firewall Schedule Removed**" appears on the Scheduling panel.
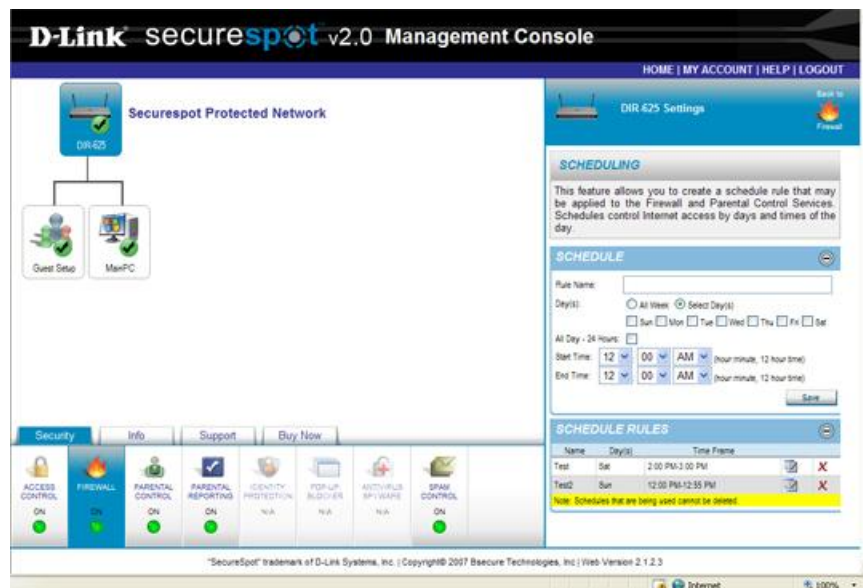
Figure 7.12: Edit a Schedule

8. Parental Control Service

The Parental Control is a service included under the Security function, which protects your home from dangers of the Internet, while giving you flexible control over Web sites and Internet application usage. The flexibility allows for a custom level of filtering sites and protects against dangerous sites infected with spyware or malware.

Parental Control Navigation

The Parental Control panel allows you to customize the list of blocked categories and also control Internet access by days and time. NOTE: Once you set up your schedule rules, you must remember to go back to Categories to enable the schedules.

NOTE: As you perform the following procedures, you will be asked to click **Save,** to save your new settings. At times you will also be prompted to click **Apply Settings.**
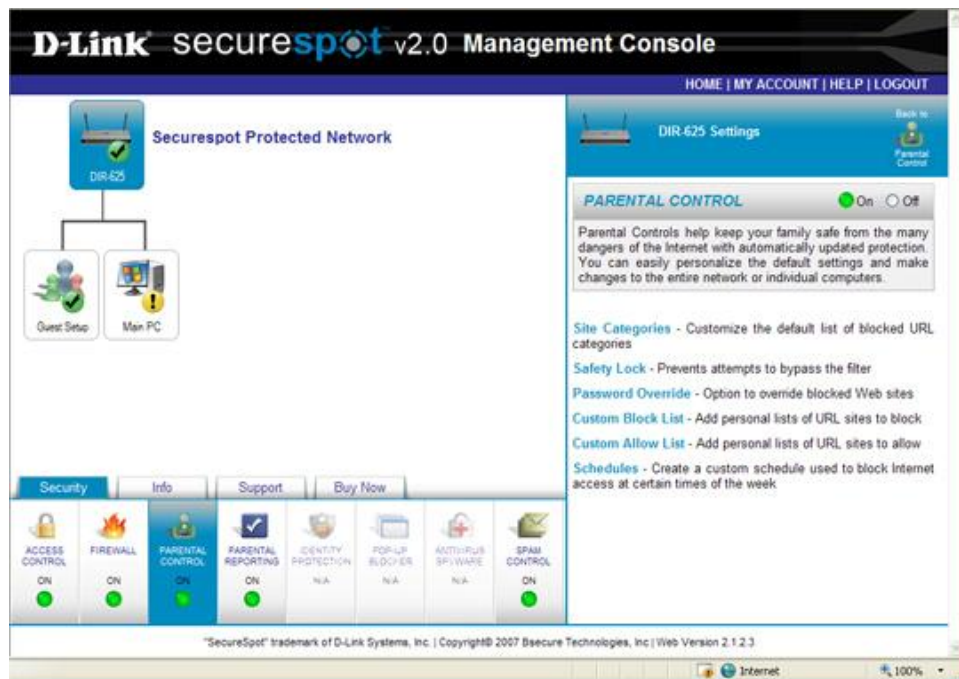
Figure 8.1: Parental Control Panel

To configure Parental Controls (Figure 8.1)

1. Select (highlight) a specific computer or device on the Network Map.
2. Click **Parental Control** under the Security function tab.
3. Select the **ON** option button to enable the Parental Control service. NOTE: **ON** is the default.

To customize the list of default Blocked Categories (Figure 8.2)

1. Click the **Site Categories** link on the **Parental Controls Service** panel. NOTE: This feature facilitates more explicit content filtering through Web site category blocking and unblocking.

2. In the **Select Age Groups** panel, select one of the age groups: NOTE: The Adult Filtering Age Group is selected by default.

   - **Custom**
   - **Child** (0 – 8)
   - **Adolescent** (9 – 12)
   - **Youth** (13 – 17)
   - **Adult** (18+)

3. In the **Schedule** drop-down menu, select one of the schedule options:

   - **Always -** The device will always be allowed Internet access with the filtering categories set above.
   - **Never –** The device will never be allowed Internet access independent of the filtering categories set above.
   - **Newly created schedule**
     1. Select the **Scheduling** link under Parental Control or Firewall panels to create a customized schedule.
     2. Select the listed Web site categories check boxes that you want the filter to block.
     3. Clear any Web sites that you do not want the filter to block.

4. Click **Save** to save your settings. NOTE: Once your settings have been saved, the message "**Parental Control Categories saved**" appears on the categories panel.

Figure 8.2: Categories Panel

Safety Lock Option and Password Override

The Safety Lock option is used to protect against users accessing multiple blocked sites. To customize the Safety Lock, click the **Safety Lock** link on the Parental Control service panel. NOTE: This option prevents attempts to bypass the Content Filter by forcing the user to reboot the router after a specified number of attempts result in blocked pages.

To modify the Safety Lock option (Figure 8.3)

1. Click and hold the slide control button, and then move the button to the desired safety lock setting.

2. Release the slide control button, and then click it one more time. This will set the slide control button. NOTE: The information beneath the slide control will change as you move the button to reveal the current setting.

3. Click **Save** to save your settings.

4. Once your settings have been saved, the message "**Parental Control Options saved**" appears on the Options feature panel.
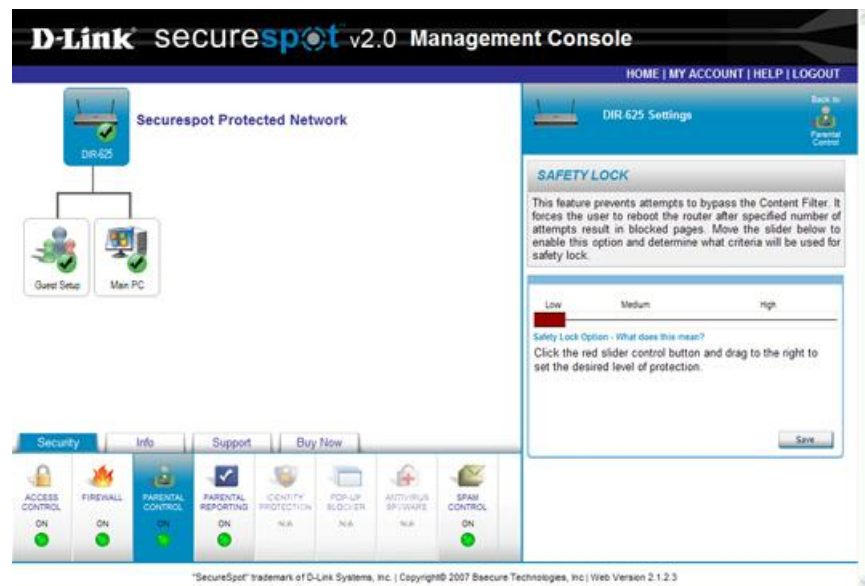
Figure 8.3: Safety Lock Option

When enabled, Password Override allows you to override the existing password with associated individual blocked sites with a new password. To enable or disable password override, click the **Password Override** link on the Parental Controls service panel.

To modify the Status/Password Override option (Figure 8.4)

1. To enable password override, select the **Enable Password Override** check box.

2. Click **Save** to save your settings.

3. Once your settings have been saved, the message "**Parental Control Options saved**" appears on the Options feature panel.

Figure 8.4: Password Overrid**e**

Customized Lists

The ability to create customized lists enables you to block or allow specific Web sites by URL and create White Lists (list of specified "only allow" Web sites) if desired to control content filtering more specifically.

To create Allowed Web Site List (Figure 8.5)

1. In the provided text box, type the URL of a Web site that you want to allow.
2. Click **Add**.
3. The Web site is added to the **Allowed Web Site** List.
4. Repeat the previous two steps (2 and 3) if you want to add additional Web sites to your **Allowed Web Site** List.
5. Once your settings have been saved, the message "**Parental Control Web Site Lists saved**" appears on the Web Sites List panel.

To edit the Allowed Web Site List

- To remove a single entry from a list:
    1. Click (highlight) the **Web Site** entry
    2. Click **Remove**. The Web site is removed from the Allowed Web Site list.
- To remove several entries from a list:
    1. Click (highlight) the **Web Site** entries
    2. Click **Clear**. All entries are removed from the Allowed Web Site list.

Figure 8.5: Allowed Web Sites Panel

To create an "only allow" White List

1. In the **Allowed Web Sites** List, type the URL of the Web site that you want to allow in the text box.

2. Click **Add**.

3. The Web site is added to the **Allowed Web Sites** List.

4. Repeat the previous two steps (2 and 3) to add additional Web sites to your **Allowed Web Sites** List.

5. Select the **Only Allow the Web sites listed** in the Allowed list check box. NOTE: This will block access to all Web sites with the exception of those specified on the Allowed Web Sites List.

6. Click **Save** to save your settings.

7. Once your settings have been saved, the message "**Parental Control Web Site Lists saved**" appears on the Web Sites List panel.

To create Blocked Web Sites List (Figure 8.6)

1. Click the **Custom Block List** link on the Parental Controls service panel.

2. In the provided text box, type the URL of a Web site that you want to block.

3. Click **Add**. The Web site is added to the Blocked Web Sites List.

4. Repeat the previous two steps (2 and 3) to add additional Web sites to your Blocked Web Sites list.

5. Once your settings have been saved, the message "**Parental Control Web Site Lists saved**" appears on the Web Sites List panel.
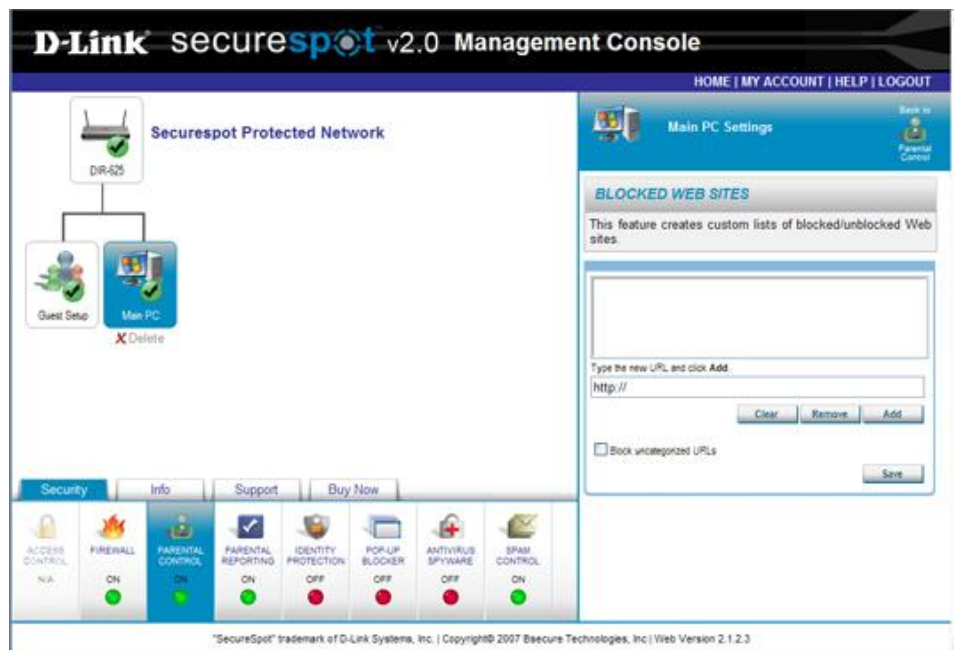
Figure 8.6: Blocked Web Sites

To edit the Blocked Web Site List

- To remove a single entry from a list:
    3. Click (highlight) the **Web Site** entry
    4. Click **Remove**. The Web site is removed from the Blocked Web Site list.
- To remove several entries from a list:
    3. Click (highlight) the **Web Site** entries
    4. Click **Clear**. All entries are removed from the Blocked Web Site list.

Schedules

To control Internet access, click the Schedules link on the Parental Controls service panel. Web browsing can be controlled by time of day and each day of the week.

To create a Schedule (Figure 8.7)

1. In the **Rule Name** text box, type the name of the schedule that you want to create.

2. Select the appropriate options for Days:

    ▪   **All Week**

    NOTE: If the All Week option button is selected, the individual day check boxes collapse (disappear).

    ▪   **Select Day(s)**

3. In the **Start** and **End Time** drop-down list boxes:

    ▪   Select the appropriate time. (Schedule times are hour and minute increments.)
    ▪   Select the All Day check box if you want to block Internet Access for 24 hours.
        NOTE: If the All Day check box is selected, the Start and End Time drop-down list boxes collapse (disappear).

4. Click **Save** to save your settings. Once your settings have been saved, the message "**Firewall Schedule Created**" appears on the Scheduling panel.

5. The newly created schedule is added to the Schedules list.
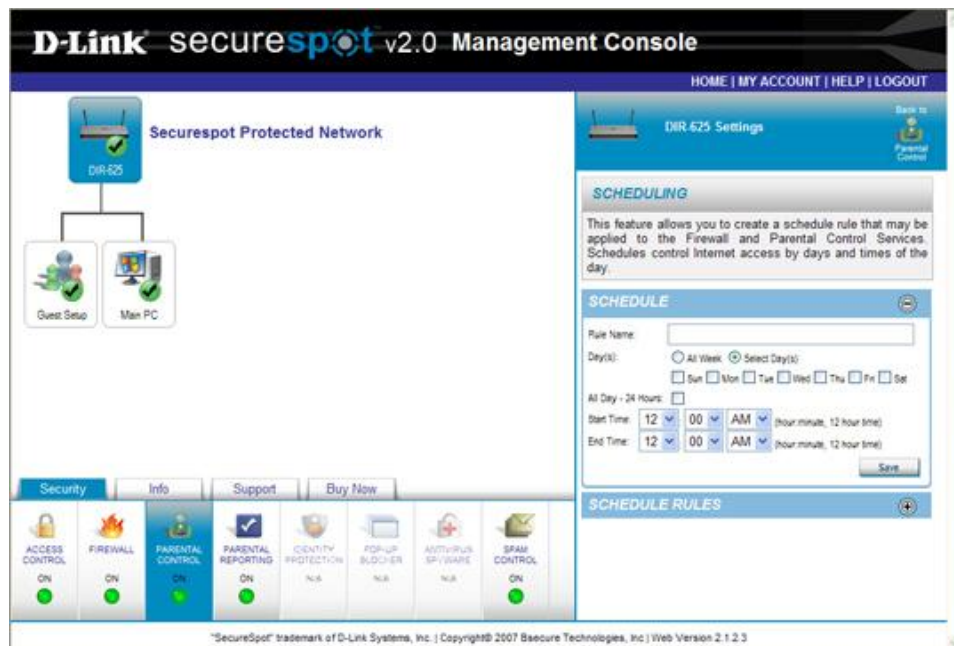
Figure 8.7: Scheduling Setup

To edit a Schedule (Figure 8.8)

1. Click the ⊕ icon to expand the **Schedule Rules** panel.

2. Select the 📝 icon to edit a schedule.

3. The previously-saved schedule input appears in the Schedule panel.

4. After changes have been made to the schedule, click the **Update** button on the Schedule panel.

5. The updated schedule is added to the Schedules Rules list.
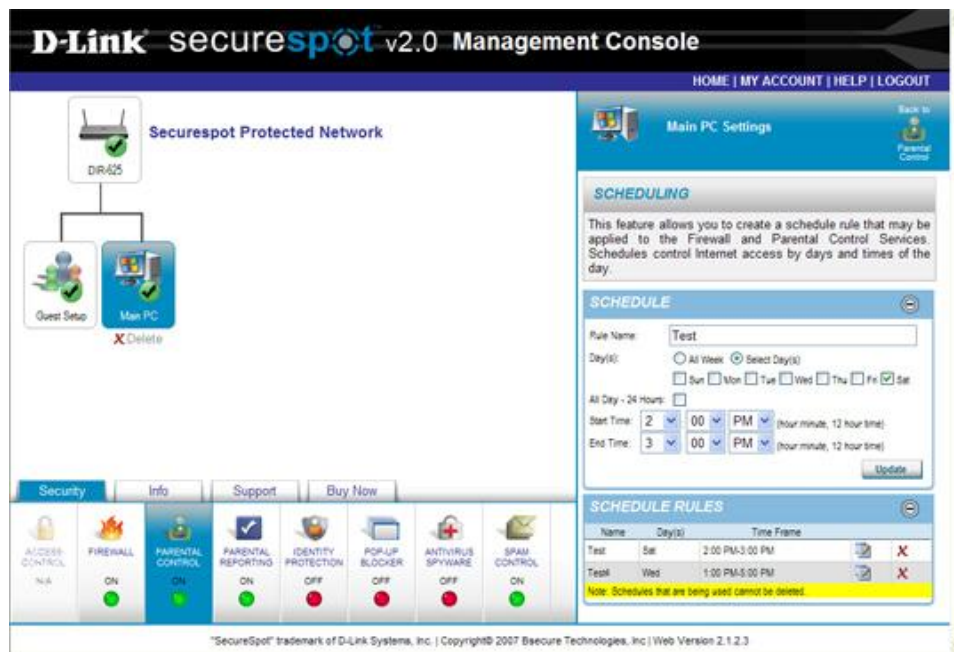
Figure 8.8 Scheduling Editing

To delete a Schedule

1. Click the ⊕ icon to expand the **Schedule** panel.

2. Select the ✗ icon beside the schedule that you want to delete.

    NOTE: Schedules that are currently in use cannot be deleted.

3. Once the schedule has been deleted, the message "**Firewall Schedule removed**" appears on the Scheduling panel.

Custom Security Settings

There may be times when you will want to manage security settings on one PC separate from the other devices in your home network.

To apply customized security settings to a single computer (Figure 8.9)

1. Select any computer on the Network Map that you want to apply customized settings.

2. A pop-up window appears on the screen. Click **Yes**.

3. Click the **Security** tab.

4. Select any service icon.

5. The **Settings managed for this computer** check box will appear on each service panel and the default will be selected.

6. You may now customize any of the Security services and apply these new security settings to a single computer on your network.

Figure 8.9: Customized Security

9. Parental Reporting Service

The Parental Reporting service creates a historical record of the Web sites that cannot be altered or erased. This information is maintained in a calendar format for up to 2 weeks. Archived reports contain the profile, date, Web site visited, Web site category, number of hits, and age group, and are displayed at any time by the account administrator.

The Parental Notification feature enables you to receive alerts via e-mail and/or short message service (SMS) whenever a user attempts to access a blocked Web site. NOTE: This will only send alerts when a user attempts to access a pornography or R-rated Web site.

Parental Reporting Navigation

✔ **NOTE:** As you perform the following procedures, you will be asked to click **Save** to save your new settings. At times you will also be prompted to click **Apply Settings.**
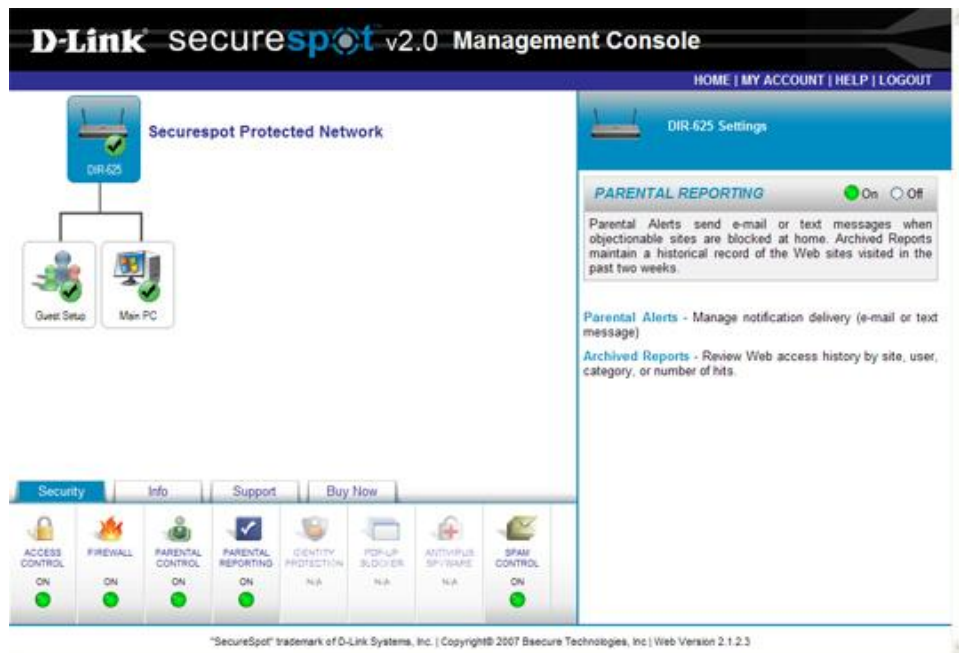
Figure 9.1: Parental Reporting Panel

To enable Reports (Figure 9.1)

1. Select a specific device on the Network Map.
2. Click the **Parental Reporting** service under the Security function tab.
3. Select the **On** option to enable the Parental Reporting service. (NOTE: **ON** is the default)
4. To enable Parental Notification via e-mail and/or SMS notification alerts, click the **Parental Notification** link on the Parental Reporting panel.

To add Parental Notification via E-mail alerts (Figure 9.2)

1. Select **On** option to enable the Parental Notification feature.

2. Enter an e-mail address in the text box and click **Add**.

3. Once your settings have been saved, the message "**Parental Notification settings saved**" appears on the Parental Notification panel.
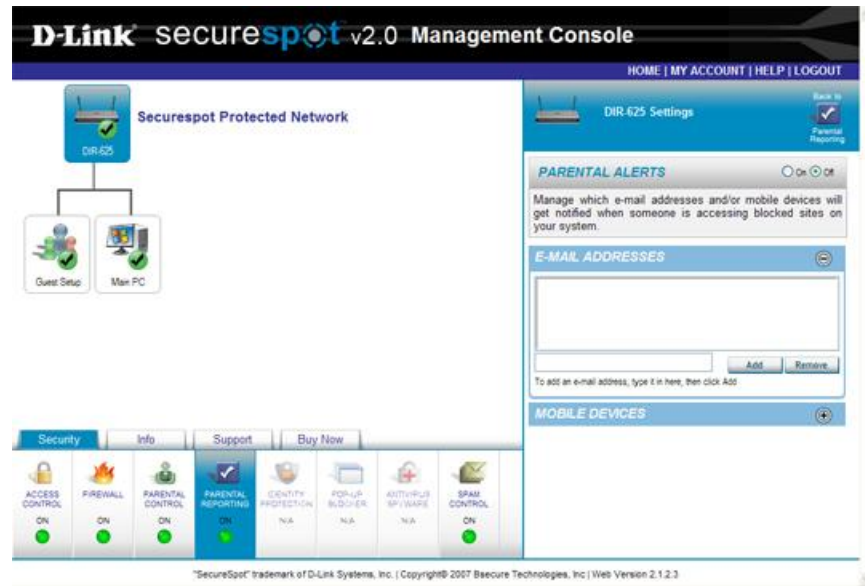
Figure 9.2: E-mail Notification

To stop an E-mail Address from receiving alerts

1. Select the e-mail address in the list that you want to remove, and click **Remove**.

2. Once your settings have been saved, the message "**Parental Notification settings saved**" appears on the Parental Notification panel.

To add Parental Notification via Mobile Device (SMS) alerts (Figure 9.3)

1. Select **On** option to enable the Parental Notification feature.

2. Click ⊕ to expand the Mobile Devices panel.

3. Enter a short message service (SMS) number in the text box and click **Add**.

4. Once your settings have been saved, the message "**Parental Notification settings saved**" appears on the Parental Notification panel.

To stop a SMS number from receiving alerts

1. Select a SMS number in the list, and click **Remove**.

2. Once your settings have been saved, the message "**Parental Notification settings saved**" appears on the Parental Notification panel.
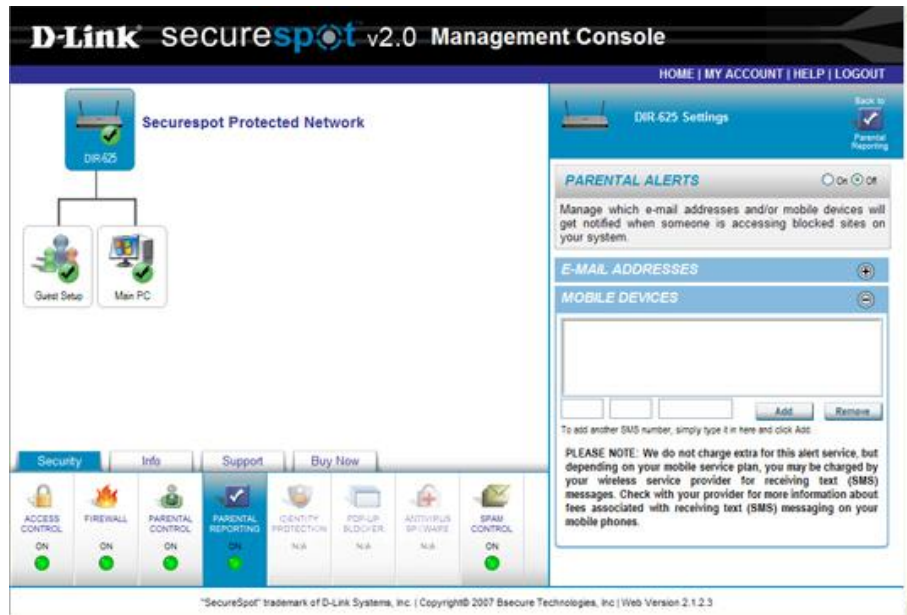
Figure 9.3: Mobile Device Notification

To view a report

1. Click the **Archived Reports** link on the Parental Reporting panel (Figure 9.4).
2. This report includes: Profile, Page, Category, Hits, and Age Group
3. Click any colored block to view that day's detailed history.
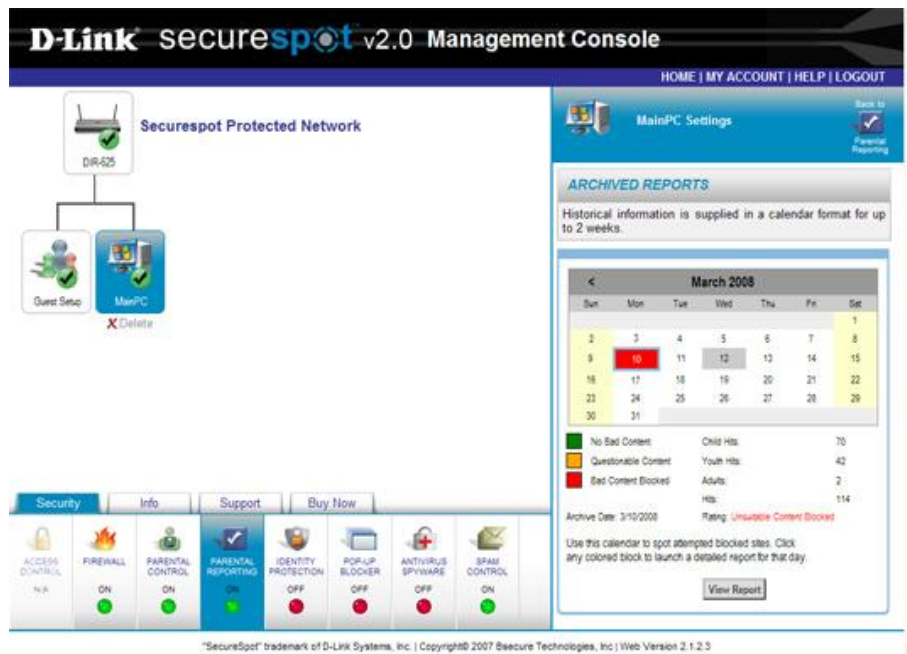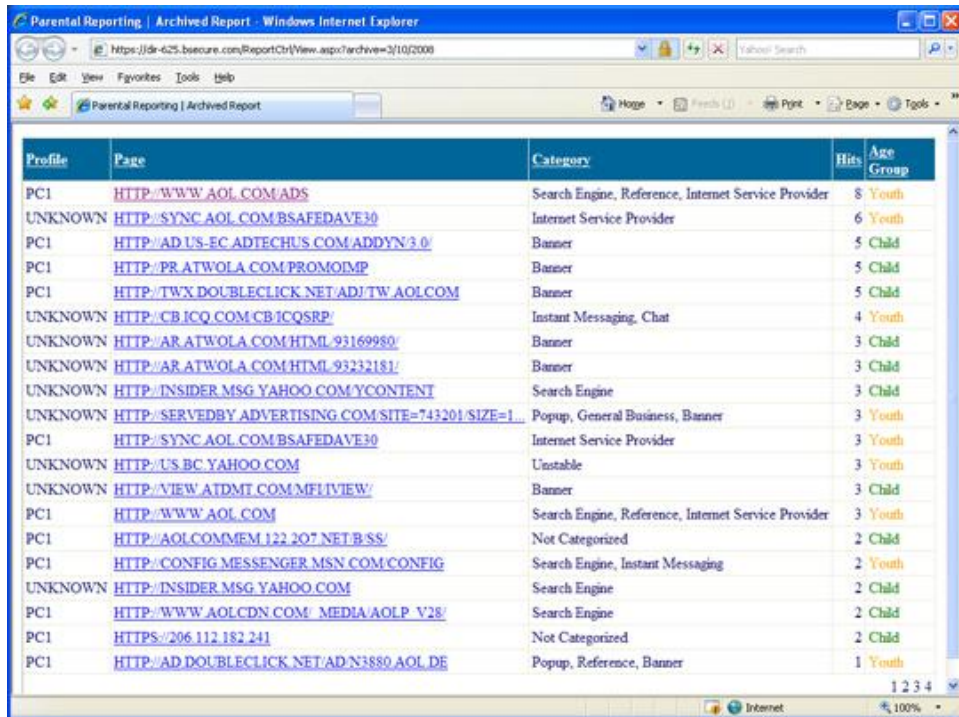
Figure 9.4: Reports

4. Click **View Report** to display a detailed report of the blocked sites (Figure 9.5).

Figure 9.5: Parental Report

10. Identity Protection Service

The Identity Protection Page allows you to enter private information (e.g. Social Security Number (SSN), credit card numbers, bank account numbers, etc.) into online forms and e-mails, while preventing this information from being transmitted from your computer(s) without your permission.

Identity Protection Navigation

Before you can begin to use the Identity Protection service, you will have to make sure you have installed the Thin Client application (End Point Security) on the computer you are on. (Figure 10.1)

NOTE: Thin Client is controlled at the PC level and must be installed on each device separately. Refer to the Thin Client Installation section of this manual to download and install the SECURESPOT 2.0 Thin Client application.
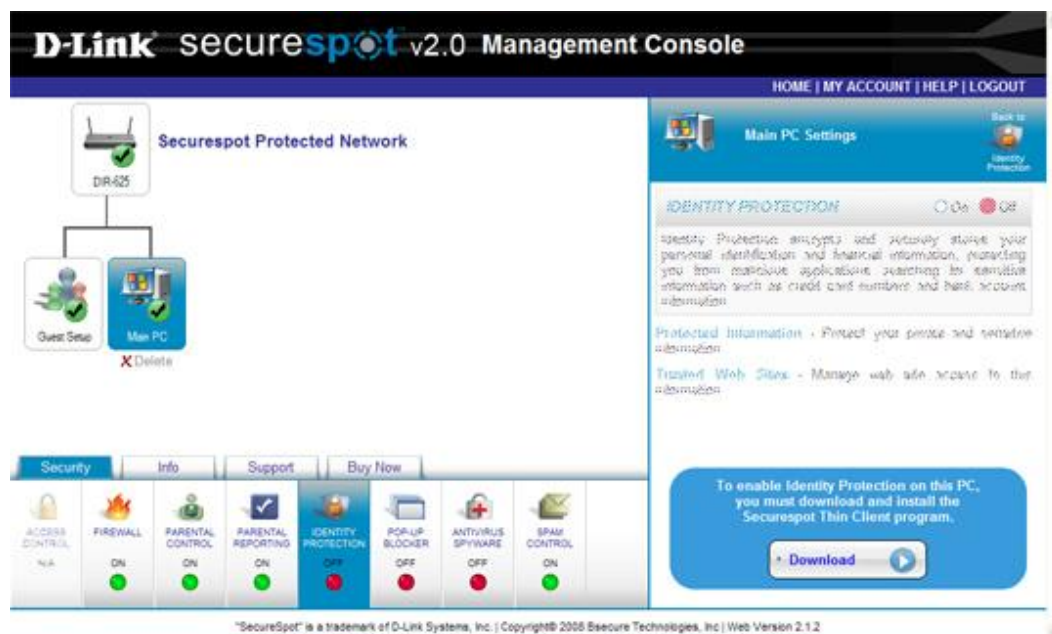
Figure 10.1: Thin Client Download

To activate Identity Protection (Figure 10.2)

1. Log into the Management Console through the "My Account" Web Control Center Login Screen and select a computer on the Network Map.

2. Click **Identity Protection** service under the Security function tab.

3. On the Identification panel, check to see that Identity Protection is **On** (green light). NOTE: If the Identity Protection is **Off** (red light), you must install the Thin Client (Endpoint Security) on your machine and ensure that it is turned on before you can continue.
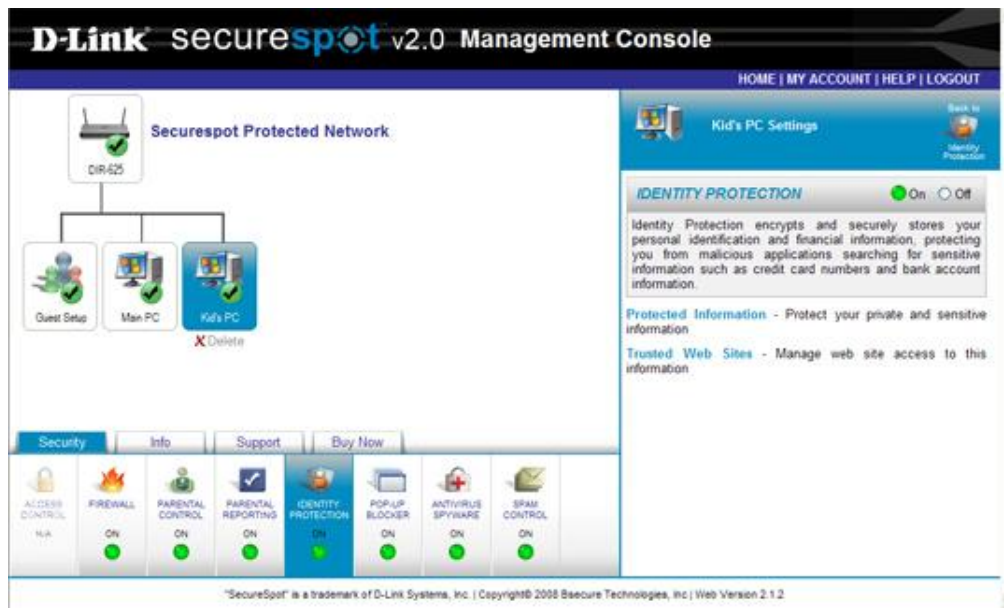
Figure 10.2: Identity Protection Panel
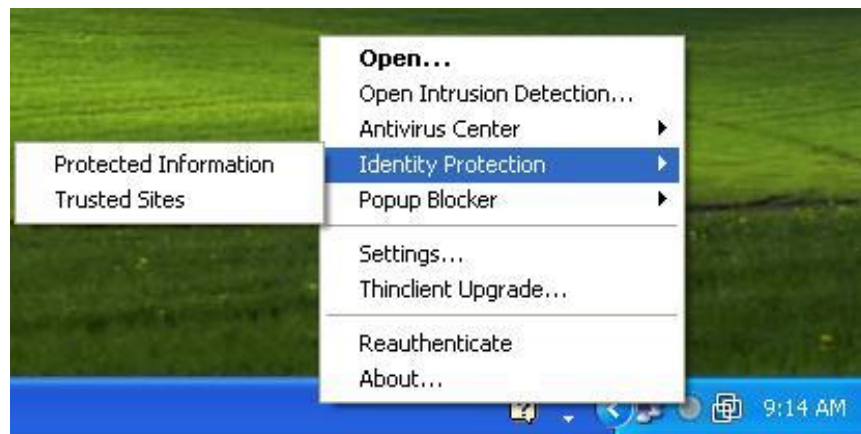
Figure 10.3: Thin Client (End Point Security) Tray

Protected Information

To protect your private information, click the **Protected Information** link on the Identity Protection panel. (Figure 10.2) You may also right click the Thin Client (End Point Security) icon in the Windows tray to choose Identity Protection and Protected Information from the submenu. (Figure 10.3)
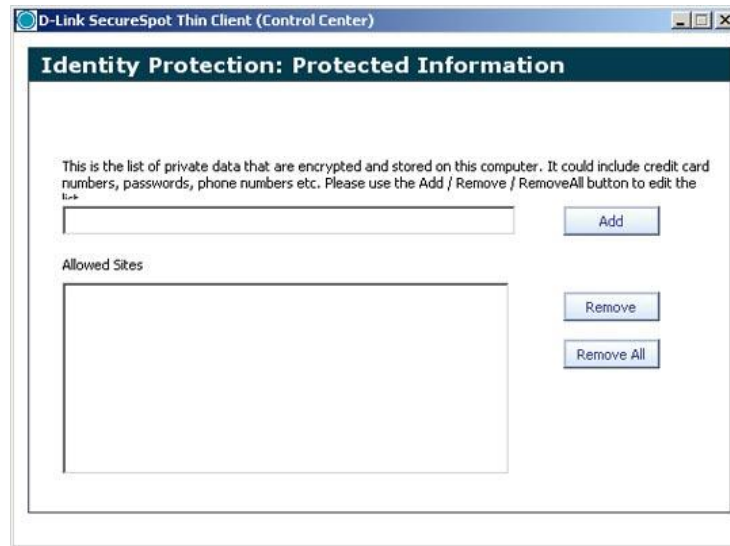
Figure 10.4: Protected Information

To add private information to the Protect List (Figure 10.4)

1. In the provided field, type an item of private data that you want protected.
2. Click **Add**. The information is added to the protect list.

To delete private information from the Protect List (Figure 10.4)

1. In the list of Protected Information, select the data that you want removed from the list.
2. Click **Remove**. The information is removed from the protect list. OR
3. Click **Remove All** to delete ALL private information from the protect list.

Trusted Sites

To view a list of Web sites that are allowed to access the protected data on your computer, click the Trusted Sites link on the identity Protection panel. (Figure 10.2) You may also click the Thin Client icon in the Windows tray to choose Identity Protection and Protected Information from the submenu. (Figure 10.3)

To add a Web site to the Protect list (Figure 10.5)

1. In the provided field, type the address of the Web site that you want to have access to your personal data.
2. Click **Add**. The information is added to the allow list.

To delete a Web site from the Allow list (Figure 10.5)

1. In the allow list, select the address that you want removed from the list.
2. Click **Remove**. The information is removed from the allow list. OR
3. Click **Remove All** to delete ALL Web sites from the allow list.
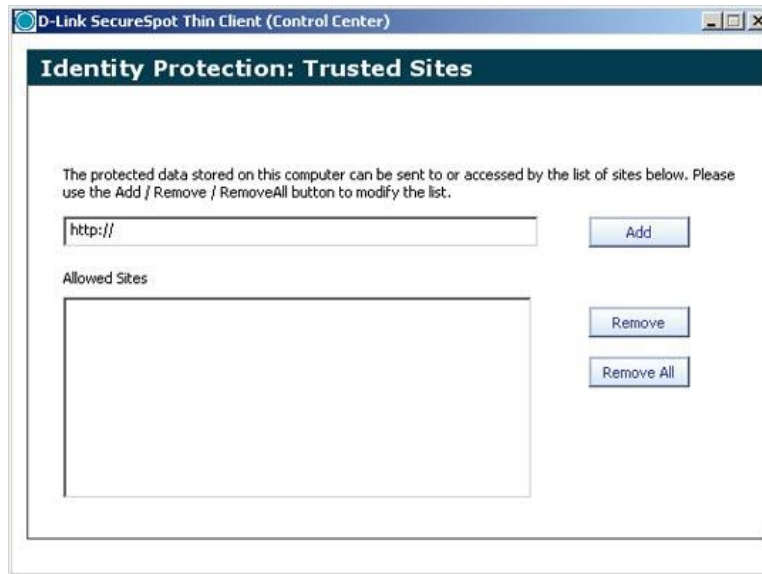
Figure 10.5: Trusted Sites

Example

For example, if you attempt to send an online form containing your SSN, you will receive a prompt alerting you to the fact that your correspondence contains private information and asking you to verify that you want to send this information. (Figure 10.6)

Figure 10.6: Identity Protection Alert

11. Pop-up Blocker Service

This feature blocks annoying pop-up windows that slow down your computer and cover up your desktop, while allowing approved sites to create pop-up windows as needed.

Pop-up Blocker Navigation

Before you can begin to use the Pop-up Blocker service, you will have to make sure you have installed and activated the Thin Client (Figure 11.1).

NOTE: Thin Client (End Point Security) is controlled at the PC level and must be installed on each device separately. Refer to the Thin Client Installation section of this manual to download and install the SECURESPOT 2.0 Thin Client application.
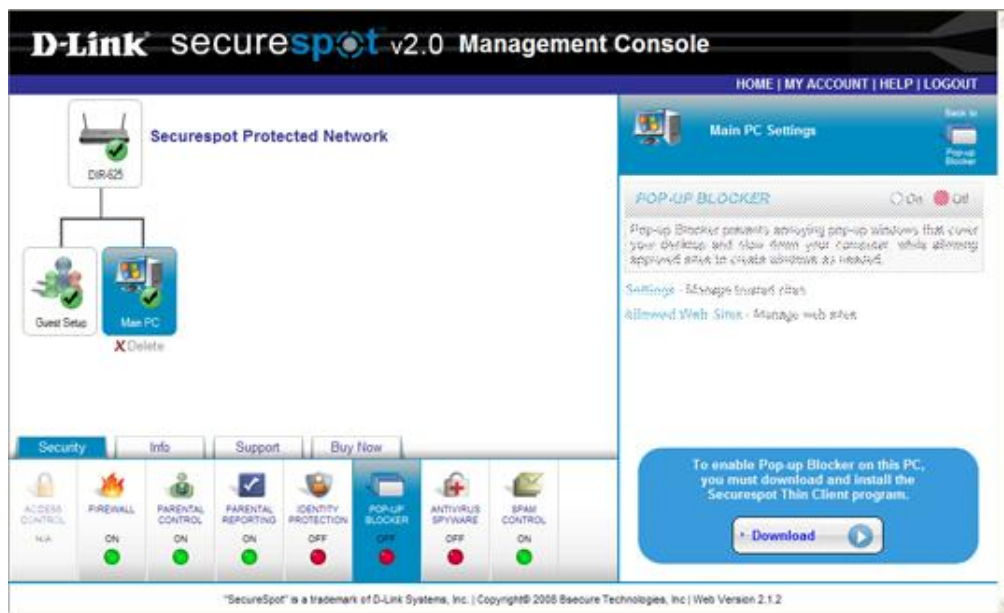
Figure 11.1: Thin Client (End Point Security) Download

To enable the Pop-up Blocker (Figure 11.2)

1. Log into the Management Console through the "My Account" Web Control Center Login Screen and select a computer on the Network Map.

2. Click the **Pop-up Blocker** service under the Security function tab.

3. On the Pop-up Protection panel, check to see that Pop-up Blocker is **On** (green light). NOTE: If the Pop-up Blocker is **Off** (red light), you must install the Endpoint Security (Thin Client) on your machine and/or turn the Thin Client on before you can continue.

4. To control pop-up settings, click the **Settings** link on the Pop-up Blocker panel.

Figure 11. 2: Pop-up Blocker Panel

Figure 11.3: Pop-up Blocker Settings

To adjust Pop-up Notification Settings (Figure 11.3)

1. Check the box next to the notification features you want to activate.

2. Click **Apply**, and then **OK** to save your settings. This will return you to the Pop-up Blocker panel.

NOTE: To create a list of Web sites from which you want to allow pop-up windows, click the **Allow List** link on the Pop-up Blocker panel. This feature allows you to unblock pop-up windows from Web sites that may use pop-up windows to help you conduct personal business, (e.g. Internet banking Web site, mortgage company Web site, 401 Benefits, etc.)
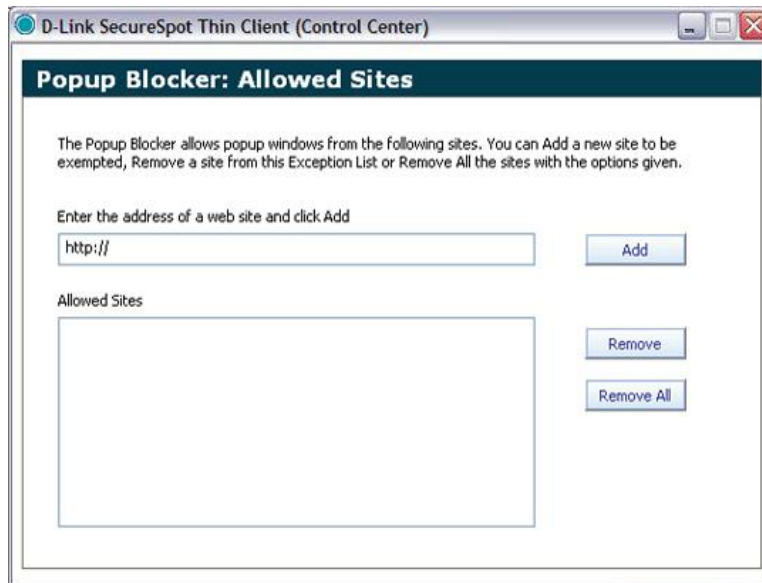
Figure 11.4: Pop-up Blocker Allowed Sites

To add a Web site address to the Pop-up Windows Allow List

1. In the provided field, type the Web site address that you want to allow pop-up windows.

2. Click **Add**. The Web site address has been added to the Allowed Sites list.

To remove a Web site address from the Pop-up Windows Allow List

1. From the Allowed Sites list, select the Web site address that you want to remove from the Allowed List.

2. Click **Remove**. OR

3. Click **Remove All** to remove all the Web site addresses from the Allowed List.

12. AntiVirus/Spyware Service

The AntiVirus/Spyware service protects your computer from viruses that can infect your system and spyware that has the potential to steal your personal information and track your Web-browsing habits. Utilizing McAfee AntiVirus and McAfee Spyware protection SECURESPOT 2.0 provides you with round the clock (24/7) world-wide monitoring and automatic updates that respond to the latest virus, trojan, and spyware threats in an integrated service.

NOTE: We recommend that you scan your computer for viruses on a regular basis. Scheduling or performing manual scans ensures that nothing gets past even on friendly channels.

AntiVirus/Spyware Navigation

Before you can begin to use the AntiVirus/Spyware services, you will have to make sure you have enabled the Thin Client (End Point Security) application. (Figure 12.1) If you do not have AntiVirus/Spyware installed, the right panel will give you the option to download the Thin Client program at this time.

NOTE: Thin Client (End Point Security) is controlled at the PC level and must be installed on each device separately. Refer to the Thin Client Installation section of this manual to download and install the SECURESPOT 2.0 Thin Client application.

Figure 12.1: Thin Client (End Point Security) Download

To enable AntiVirus/Spyware

1. Log into the Management Console through the "My Account" Web Control Center Login Screen and select a computer on the Network Map (Figure 12.2).

2. Click the **AntiVirus/Spyware** service under the Security function tab.

3. On the AntiVirus/Spyware panel, Check to see that AntiVirus/Spyware is **On** (green light). NOTE: If the AntiVirus/Spyware is **Off** (red light), you must install the Thin Client (End Point Security) on your machine or turn the Thin Client on before you can continue.
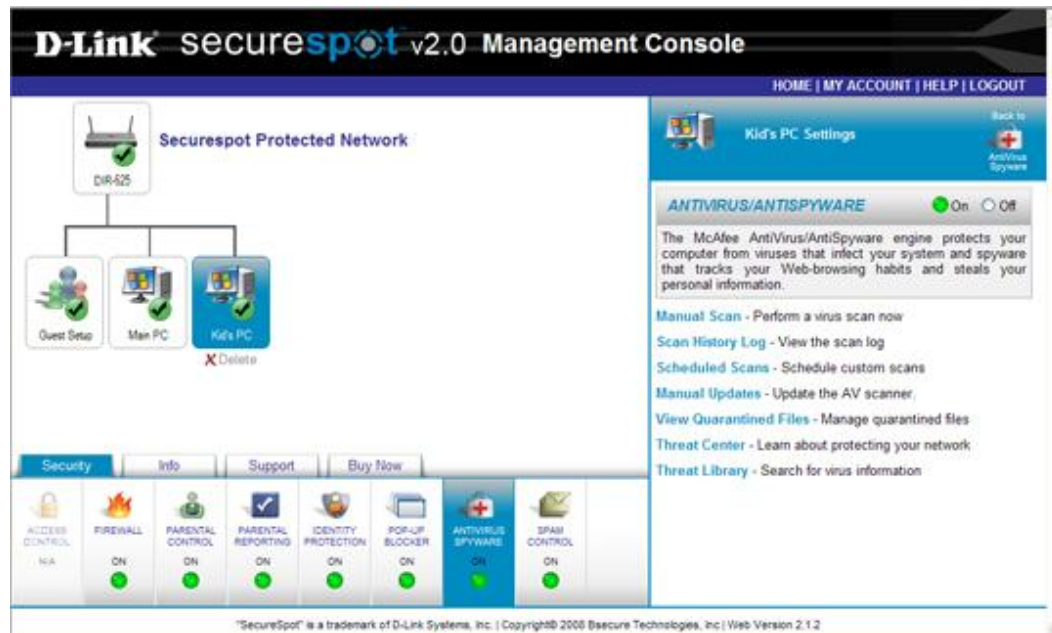
Figure 12.2: AntiVirus/Spyware Panel

Manual Scan

Although it is recommended that you schedule scans on a regular basis, you can manually scan for viruses at any time.

To perform a manual virus scan (Figure 12.3)

Click the **Manual Scan** link on the AntiVirus/Spyware panel.

- To choose a specific folder to scan:
  - Select the check box next to the folder that you wish to scan. (You can view deeper subfolders by clicking the expand icon to the left of the check boxes.)
  - To pick a particular type of file to scan based on file extension (e.g. doc) click the **Supplied Extensions** option in the Scan Options dialog box.
- To scan all files:
  - Select the **All** option in the Scan Options dialog box.

- To scan the selected file types in all of the system folders and drives, click **Scan All.**

▪ To scan the selected file types in designated folders and drives:

1. Click **Scan.**
2. A Scan Progress pop-up window will open and the scanning process begins.
3. When the scan is finished, **Scan complete** is displayed at the top of the pop-up window. Any infected files will be displayed in the pop-up window.

Figure 12.3: Scan My Computer Dialog Box

Scan History Log

To view your virus scan history

Click the **Scan History Log** link on the AntiVirus/Spyware panel. (Figure 12.4)

▪ To view the results of a scan performed after this pop-up window is opened, click **Refresh** to repopulate the list to include the most recent scan.

▪ To remove a scan from the AntiVirus history log, select the scan within the displayed list and click **Remove**. The scan record is removed from the list.

▪ To delete all scan records, click **Clear Log**. When you receive a verification prompt, click **Yes**.
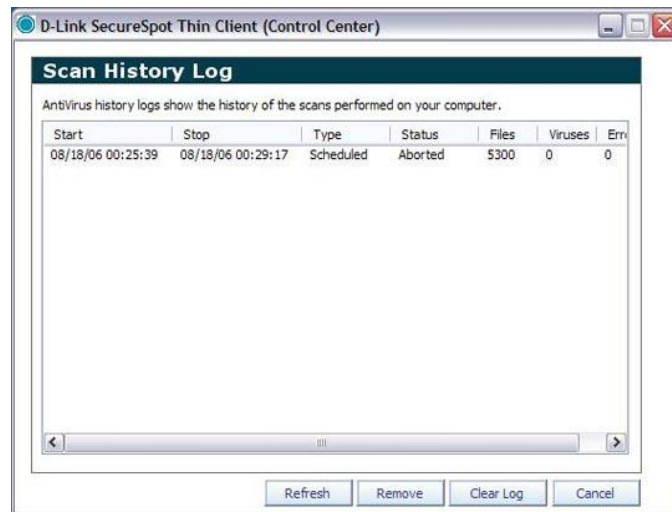
Figure 12.4: Scan History Log

Scheduled Scans

To schedule an automatic virus scan

1. Click the Scheduled Scans link.

2. Click **Add**. The **Schedule a scan** pop-up window appears. (Figure 12.5)

3. Type a name and description for the scheduled scan, and then click **OK**.

4. Click the **Files** tab. Check the boxes next to the folders or drives you want scanned, and then click **OK**.

5. Click the **Options** tab. Select the **All** option button to scan all file types, or select the **Supplied Extensions** options button to specify which types of files you want scanned. In the **Action** drop-down menu, select what action you want performed when detection of an infected file has occurred:

   - **Disinfect the file** – Cleans infected files automatically when they are found.
   - **Warn me before taking action** – Lets you choose what to do with each infected file when it is found.
   - **Delete infected file** – Deletes infected files automatically when there are found.

6. Click **OK**.

7. Click the **Time** tab. Select the option button for the desired automatic scan frequency: **Daily**, **Weekly**, or **Monthly**.

8. If you choose a monthly scan, select a number from the **Day** drop-down menu. For Weekly, select the day from the **Every** drop-down menu.

9. Click **OK**.

10. Click **Scan now** to start a scheduled scan.
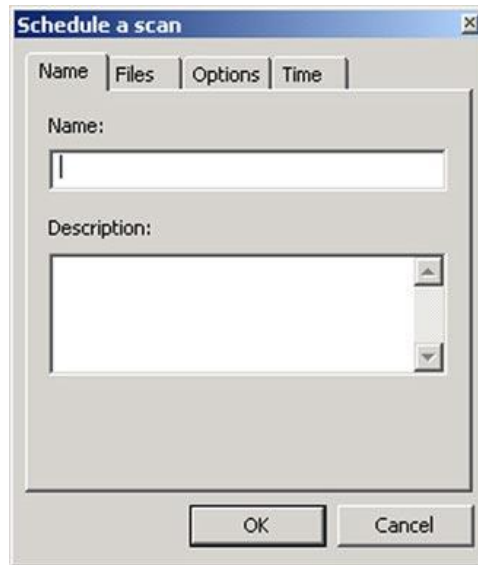
Figure 12.5: Schedule a Scan Pop-up

To delete a scheduled virus scan

1. Select the scan that you want to cancel.

2. Click **Remove**. The scan is permanently removed from the schedule.

To edit a scheduled virus scan

1. Select the scan that you want to edit.

2. Follow the steps under **Scheduling an Automatic Scan** to edit the details of your scheduled scan.

Manual Update

You can manually check for updates at any time. You can also make sure you have not missed an update or catch up if you cancelled an update notification.

To update your virus definition file updates (Figure 12.6)

1. Click the **Manual Updates** link on the AntiVirus/Spyware panel.

2. Click **Next** to check for updates. NOTE: The SECURESPOT Client Control Center will be closed during this operation.

3. An update pop-up window will appear when the virus definition files have been updated.

4. Click **Close**.
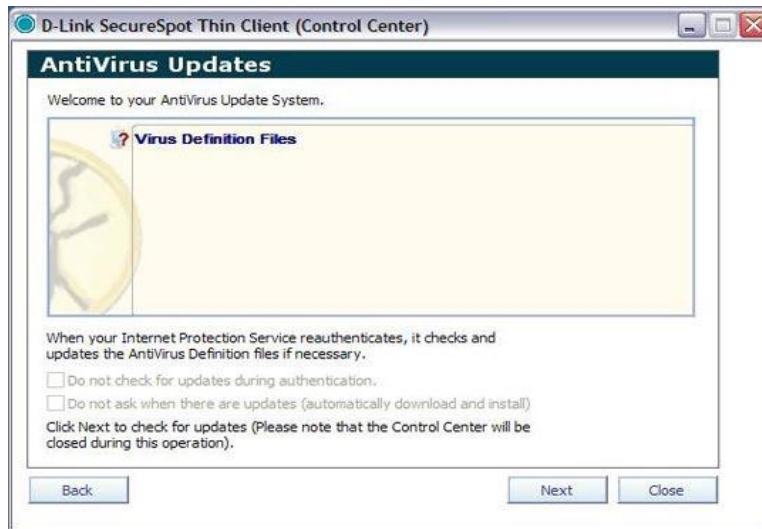
Figure 12.6: AntiVirus Updates

View Quarantined Files

To view quarantined potentially unwanted program (PUP) files or viruses found during a manual, automated, or real-time virus scan

Figure 12.7: PUP Warning

1. If there is a potential threat during a scan or while you are downloading a program, a Bsecure AntiVirus services pop-up window will appear on the screen and display the PUP file and Program Name. (Figure 12.7)

2. Click the McAfee link at the bottom of the pop-up window for detailed threat information.

3. Click **Allow** if you want to permit system access to the file. NOTE: If the same PUP file is detected again, it will be silently allowed.

4. Click **Quarantine** to repair the buffer/object/file.

5. If repair fails, the filename is added to a quarantined list and file access is denied

6. From the SECURESPOT tray icon, click the Quarantined Files submenu under AntiVirus Center (Figure 12.8).

7. A Quarantined File List dialog box will appear on the screen with a list of quarantined files (Figure 12.9).

8. If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file (Figure 12.10).

9. Double-click the object/file to launch the McAfee Web site.

10. Click **Restore** to repair and release the file/object from the quarantined list.

11. Click **Remove** to delete the file/object permanently.
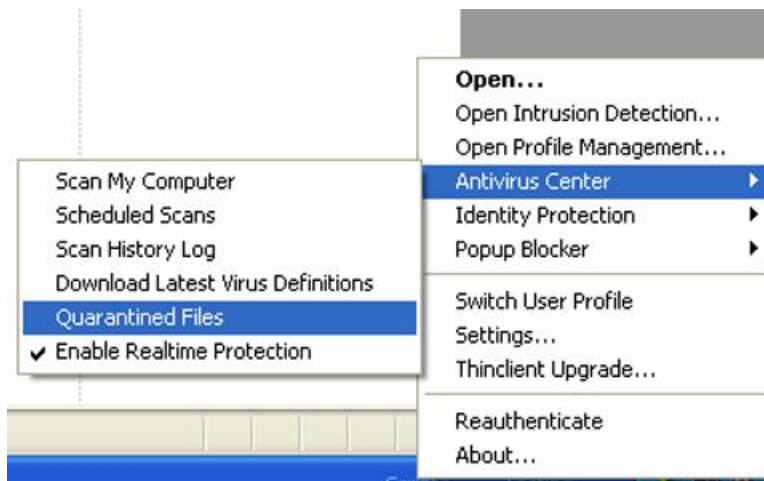
Figure 12.8: AntiVirus Center Menu
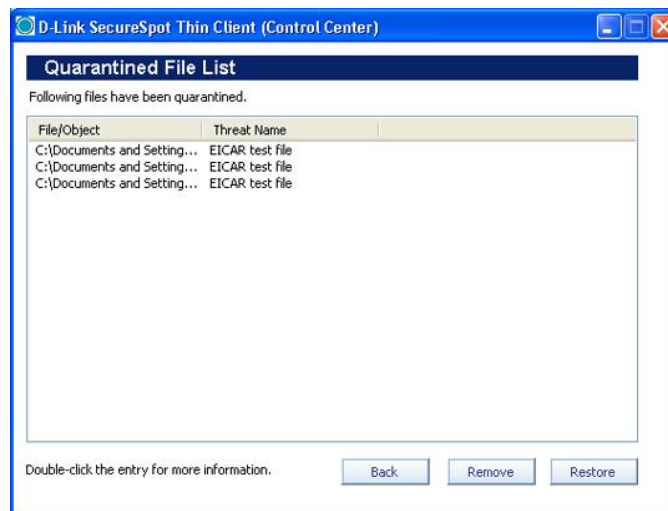
Figure 12.9: Quarantine File List

To view viruses found during a manual, automated, or real-time virus scan

1. A **Bsecure pop-up window** will appear on the screen and display the Virus file and Threat Name if a virus has been detected while you are conducting a scan or downloading a program.

2. For more threat information, double-click the file/object to launch the McAfee Web site.

3. Close the pop-up window.

4. From the SECURESPOT tray icon, click the **Quarantined Files** submenu under AntiVirus Center.

5. A **Quarantined File List** dialog box will appear on the screen with a list of quarantined files.

6. If the potential threat has been quarantined, but is not listed, the AntiVirus Services have successfully repaired the file.

7. Double-click the object/file to launch the McAfee Web site.

8. Click **Restore** to repair and release the file/object from the quarantined list.

9. Click **Remove** to delete the file/object permanently.
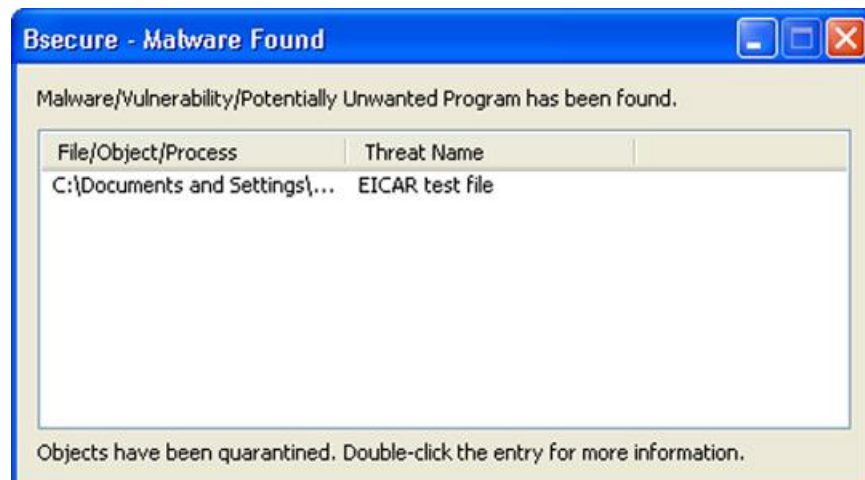
Figure 12.10: Virus File
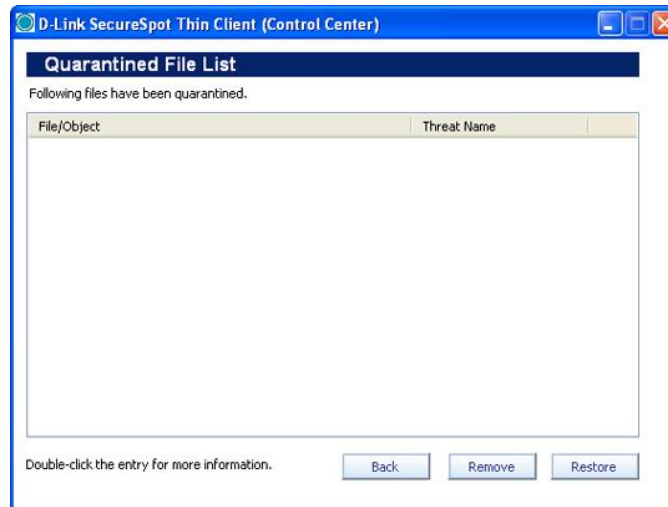
Figure 12.11: Empty Quarantined File List

Threat Center

To learn more about protecting your computer from potential threats, launch the McAfee® Threat Center by clicking the Threat Center link on the AntiVirus/Spyware Service panel.

Figure 12.12: Threat Center

Threat Library

The Threat Library allows you to search for information on known viruses and other threats. To launch the McAfee® Threat Library, click the Threat Library link on the AntiVirus/Spyware Service panel.

Figure 12.13: Threat Library

13. Spam Control Service

This service stops unwanted e-mail from filling up your inbox while preventing e-mail scams and providing Phishing protection at the same time. You will have the ability to flag and quarantine unwanted e-mail. An advantage of SECURESPOT 2.0 Spam Control service is that you may add this protection directly into Microsoft Outlook or other e-mail accounts without changing addresses, forwarding e-mail, or giving out passwords.

Spam Control Navigation

After you access Spam Control, two links will appear on the Spam Control panel.

Tag – Allows you to create a personal tag for unwanted e-mails that appears in the subject line of incoming unwanted e-mails. Once you set up a rule in your e-mail account, (e.g. Outlook, Outlook Express) e-mail that has been tagged will be sent directly to a spam folder.

Source Lists – This feature allows you to customize your blocked and allowed lists of approved domains and e-mail addresses.

NOTE: As you perform the following procedures, you will be asked to click **Save** to save your new settings. At times you will also be prompted to click **Apply Settings.**
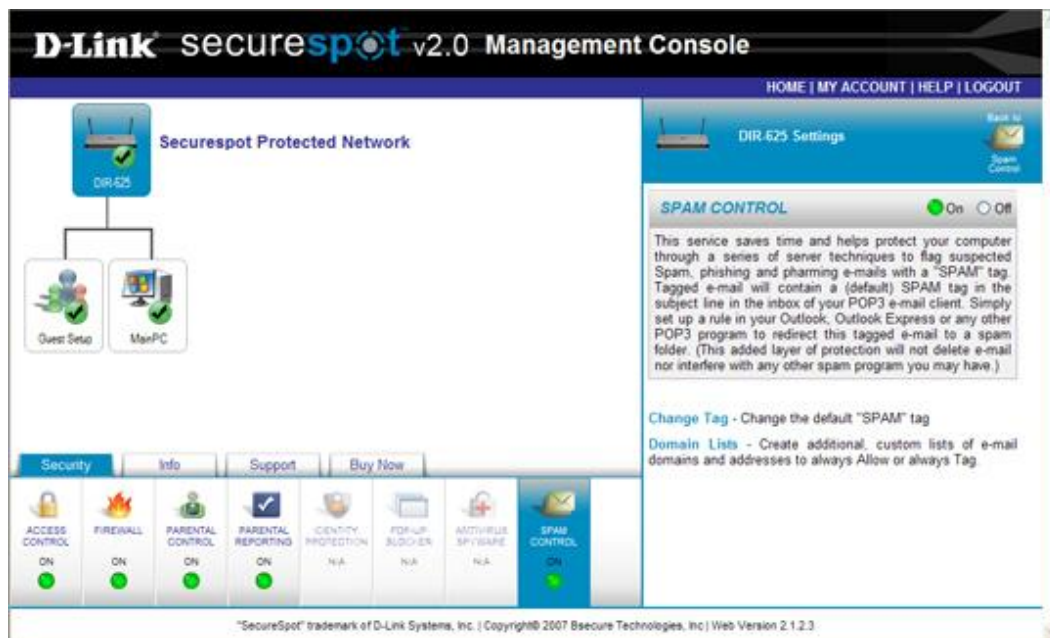
Figure 13.1: Spam Control Panel

To enable Spam Control

1. Select a specific device on the Network Map.

2. Click **Spam Control** service under the Security function tab.

3. Select the **ON** option to enable the Spam Control service. (NOTE: **ON** is the Default)
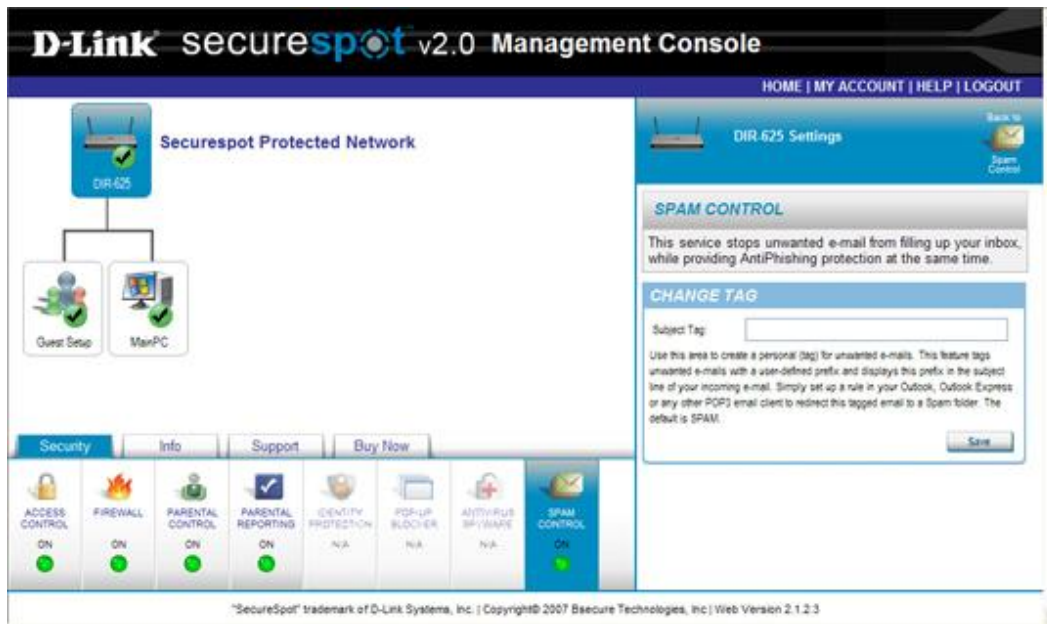
Figure 13.2: Tag Link

To define a Personal Tag to an unwanted e-mail (Figure 13.2)

1. Click the **Change Tag** link on the Spam Control panel.

2. Type the prefix in the **Subject Tag** text box. (NOTE: **Spam** is the default)

3. Click **Save** to save your settings.

4. Once your settings have been saved, the message "**Spam settings updated**" appears on the Spam Control panel.
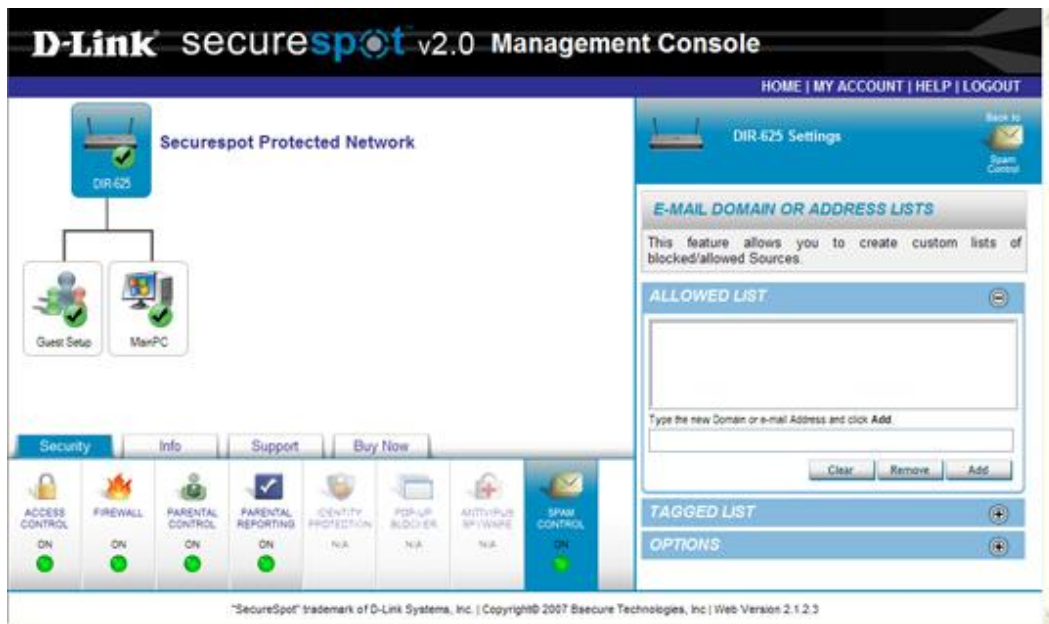
Figure 13.3: Allowed Sources Panel

To create an Allowed Sources List (Figure 13.3)

1. In the provided text box, type the Domain and/or e-mail address that you want to allow.

2. Click **Add**. The Domain and/or e-mail address is added to the Allowed Sources List.

3. Repeat the previous two steps if you want to add additional Domain and/or e-mail addresses to your Allowed Sources List.

4. Once your settings have been saved, the message "**Spam Lists saved**" appears on the Approved Sources List panel.

5. To hide Allowed Sources List details, click the ⊖ icon.
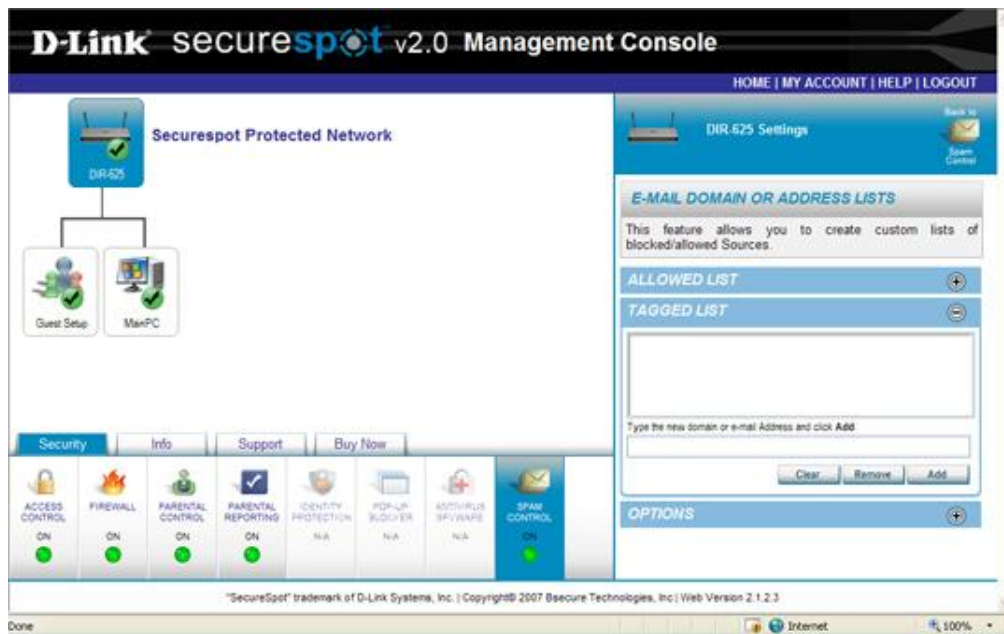
Figure 13.4: Blocked Sources Panel

To create a Blocked Source List (Figure 13.4)

1. Click the **Source Lists** link on the Spam Control panel.

2. Click the ⊕ icon to expand the Blocked Sources List panel.

3. In the provided text box, type the Domain and/or e-mail address that you want to block.

4. Click **Add**. The Domain and/or e-mail address is added to the Blocked Sources List.

5. Repeat the previous two steps to add additional Domain and/or e-mail addresses to your Blocked Sources List.

6. Once your settings have been saved, the message "**Spam Lists saved**" appears on the Blocked Sources List panel.

7. To hide Blocked Sources List details, click the ⊖ icon.

To edit the Allowed and Blocked Source Lists

1. Click the ⊕ icon to expand the list that you want to edit: **Allowed Domain List** (Figure 13.3) or **Blocked Domain List** (Figure 13.4).

2. To remove a single entry from a list, click (highlight) the Domain and/or e-mail address entry and click **Remove**.

3. The Domain and/or e-mail address is removed from the appropriate list. OR

4. To remove several entries from a list, click (highlight) the Website entries and click **Clear.** (All entries are removed from the appropriate list.)
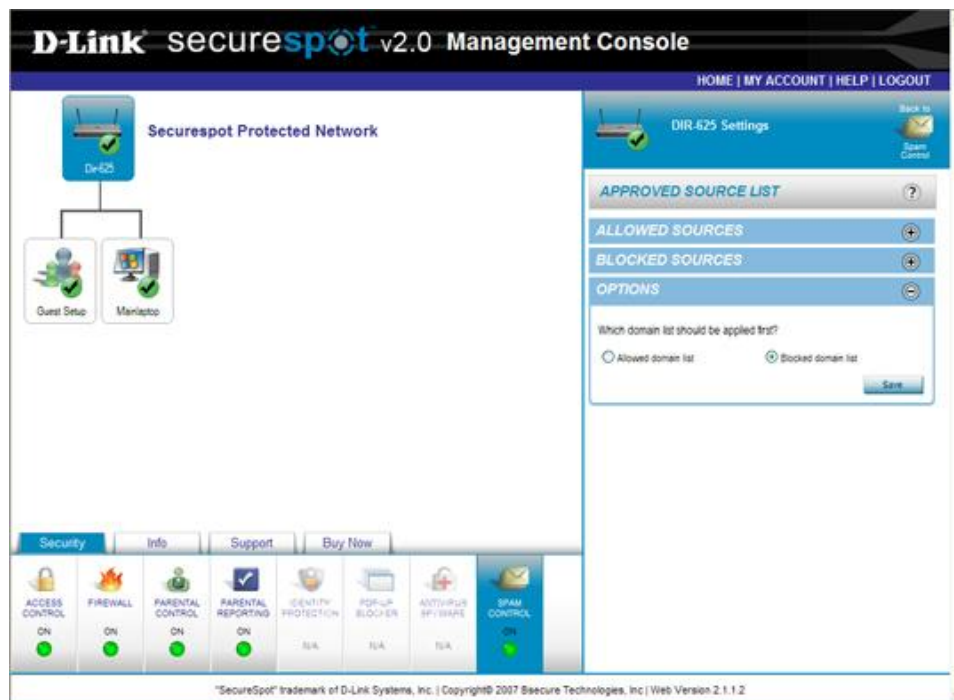
Figure13. 5: Options Panel

To create a Source List Rule (Figure 13.5)

1. Once you have created Allowed and/or Blocked Source Lists, you may create a Source List rule.

2. Click the ⊕ icon to expand the **Options** panel.

3. Select the Source list that you want applied first (**Allow** or **Blocked**).

4. Click **Save,** to save your settings.

5. Once your settings have been saved, the message "**Spam Lists saved**" appears on the Approved Source List panel.

14. Info Function

Info Function Tab

To access the services, you must select (highlight) one of the computers or network devices shown on the Network Map and then click the Info Function tab. NOTE: The selected device will appear with a dark blue background. The information displayed when a device is selected includes:

- **Device Category –** This drop-down menu is used to select a specific device category, i.e., Computing, Gaming, Peripherals, Voice, etc.

- **Device Name** – This text box is used to create a user-defined computer and/or device name.

- **Device Type** – This drop-down menu is used to select a specific device type, i.e., PC, XBox360, Skype, etc.

- **Operating System** – This drop-down menu is used to select an operating system.

- **Media Access Control (MAC) Address** – This text box displays a unique number that is attached to the device network adapter.

- **Internet Protocol (IP) Address** – This text box displays the IP address that has been assigned to an individual computer or network device.

- **Client Version** – This text box displays the latest Thin Client version for the device.

- **Firmware Version** – This text box displays the latest Firmware version for the network.
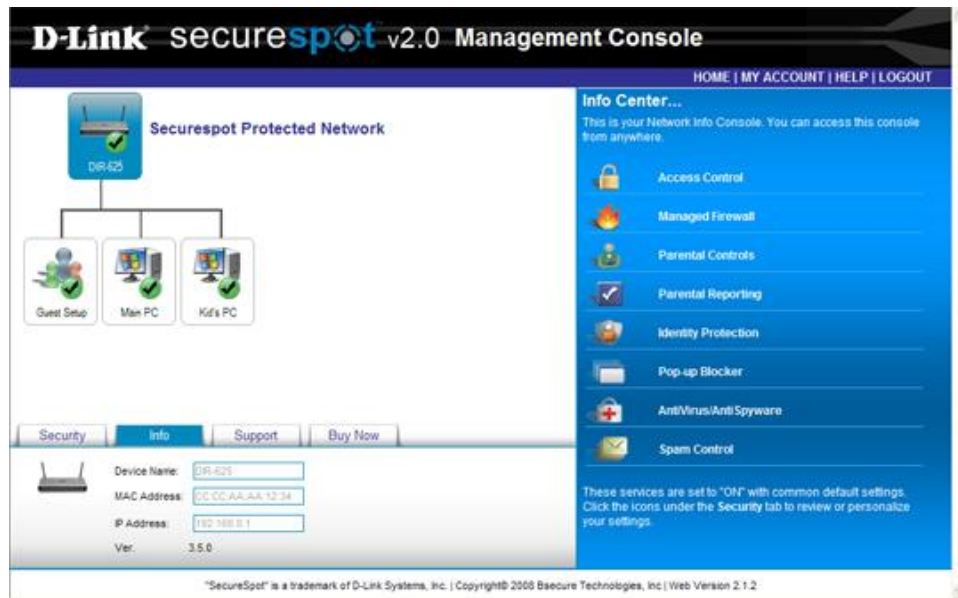
Figure 14. 1: Device Data

To modify/update individual device data

1. Select a specific device on the Network Map.
2. Click the **Info** function tab.
3. Select or enter the appropriate data into the drop-down menu or text boxes, respectively.
4. Click **Update.**

15. Support Function

The Support Function provides technical support including: Account Information, FAQs, E-mail, Live Chat, SECURESPOT Datasheet, and User Manual links that can be accessed by clicking the Support Function tab and then the individual services. Additional options will appear as panels in the Options and Configuration Section on the right side of the screen.

1. **My Account** – This service allows you to view and edit contact, billing, password, and preference information (Figure 15.1).
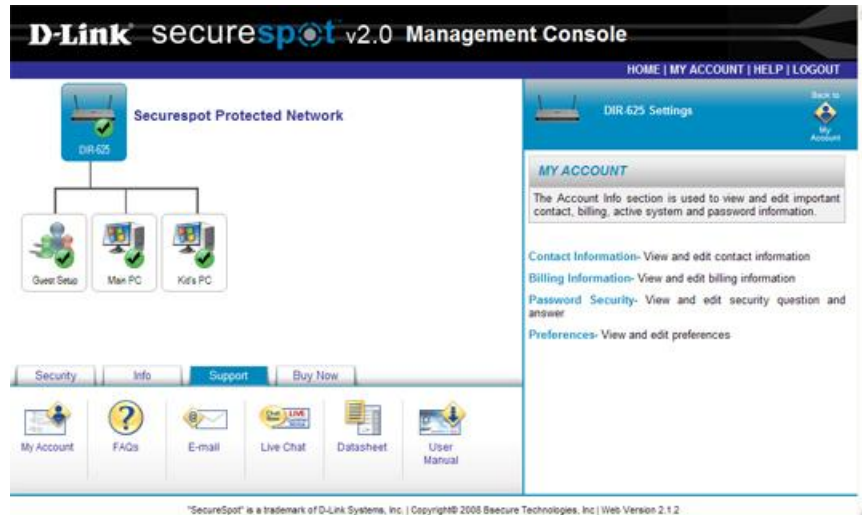
Figure 15.1: My Account Feature

2. **FAQs** – Click this service to launch the D-Link SECURESPOT FAQ page (Figure 15.2).
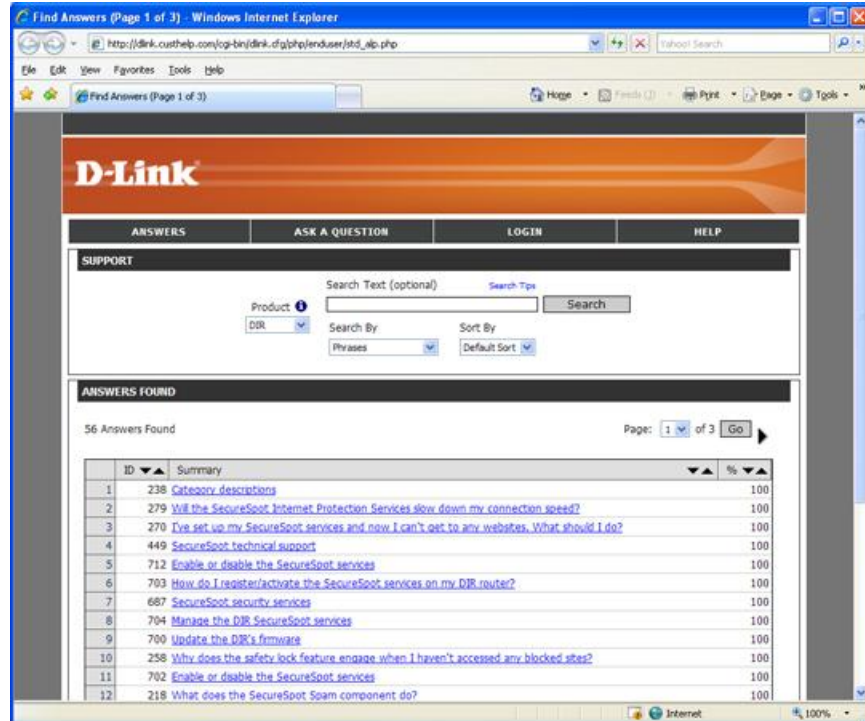
Figure 15.2: D-Link Frequently Asked Questions
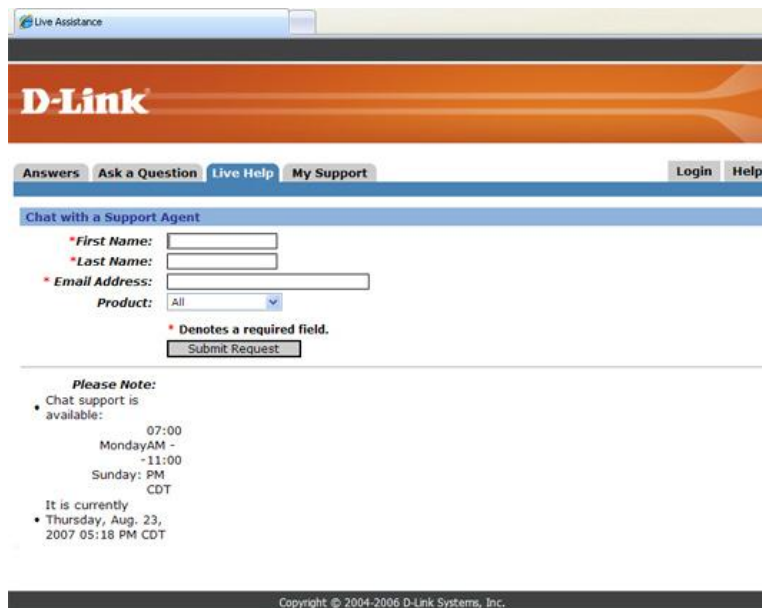
3. **E-mail** – This service allows you to send e-mails to SECURESPOT Customer Services (Figure 15.3). NOTE: You must click **Submit** to complete the transaction.

Figure 15.3: E-mail Support

4. **Live Chat** – Click this service to launch Live Chat and speak with a Tech Support Agent (Figure 15.4).

Figure 15.4: Live Chat Support

5. **Datasheet** – Click this service to open the SECURESPOT 2.0 Services Datasheet (Figure 15.5).

Figure 15.5: Data Sheet

6. **User Manual** – Click this icon to access the SECURESPOT 2.0 User Manual

My Account Navigation

NOTE: If you click located at the top right of the screen in the Options and Configuration section before you click **Save**, you will be returned to My Account without changing the information you entered

To view and/or edit Contact Information (Figure 15.6)

1. Select a specific device on the Network Map.

2. Click **Support** and then **My Account**.

3. Click the **Contact Information** link on the My Account panel.

4. Select or enter the appropriate data into the drop-down list or text boxes.

5. Click **Save** to save your settings.

6. Once your settings have been saved, the message "**Contact Information saved**" appears on the Contact Information panel.

Figure 15.6: Contact Information

To view and/or edit Billing Information (Figure 15.7)

1. Select a specific device on the Network Map.

2. Click **Support** and then **My Account**.

3. Click the **Billing Information** link on the My Account panel.

4. Click **Save** to save your settings.

5. Once your settings have been saved, the message "**Billing Information saved**" appears on the Billing Information panel.

Figure 15.7: Billing Information

To view and/or edit Password Information (Figure 15.8)

1. Select a specific device on the Network Map.

2. Click **Support** and then **My Account**.

3. Click ⊕ to expand the **Password Security** panel.

4. Type a security question and answer in the provided fields.

5. Click **Save** to save your settings.

6. Once your settings have been saved, the message "**Security Information saved**" appears on the Password Security panel.

Figure 15.8: Password Security

To view and/or change Preferences (Figure 15.9)

1. Select a specific device on the Network Map.

2. Click **Support** and then **My Account**.

3. Click the **Preferences** link on the My Account panel.

4. Select the appropriate check box to turn **OFF** some of the initial SECURESPOT Preferences.

5. Click **Save**. Once your settings have been saved, the message "**the preferences have been saved**" appears on the Preferences panel.
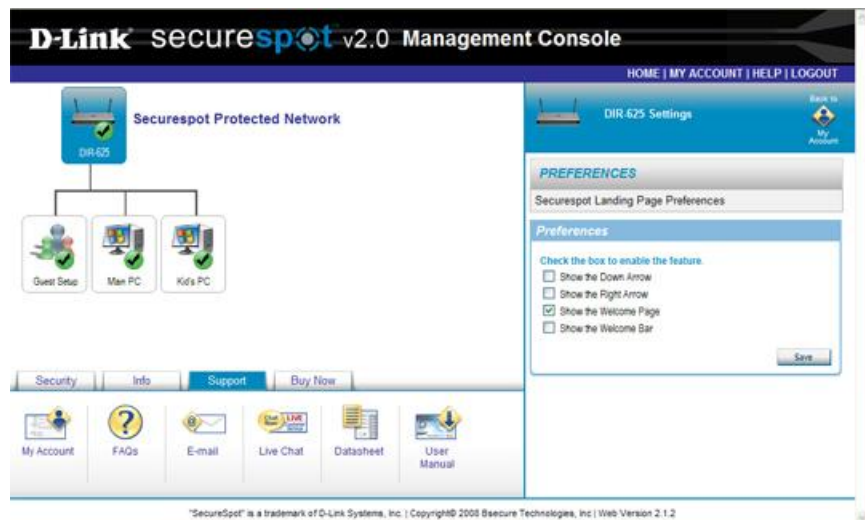
Figure 15.9: Preferences

16. Buy Now Function

Buy Now Navigation

The Buy Now Function tab displays the SECURESPOT 2.0 Services Upgrade link. Click this icon to display the SECURESPOT Services upgrades panel and shopping cart.
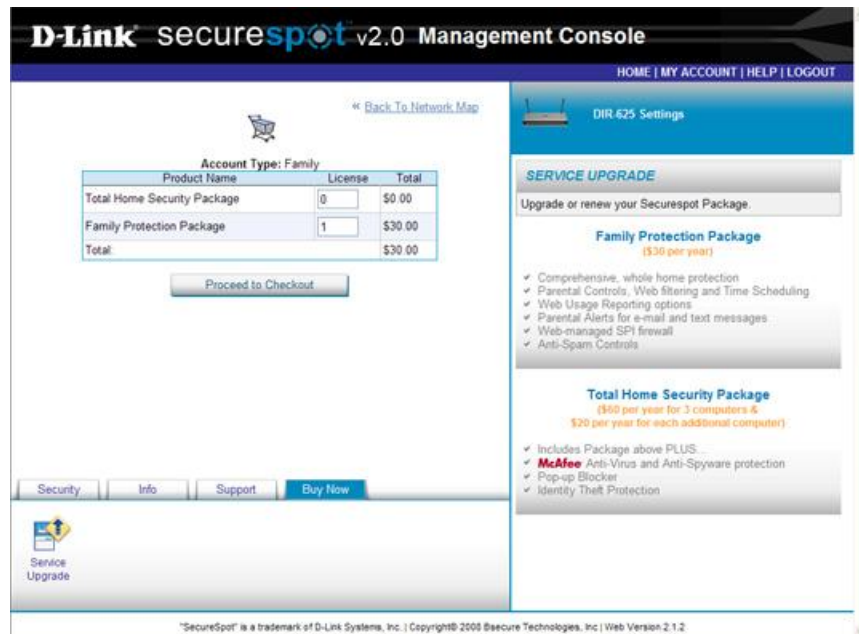
Figure 16.1: Shopping cart

Family Protection Package

Select this package if you want to protect your household from inappropriate content and objectionable Web sites and track Internet usage.

1. Enter the number of licenses that you would like to purchase in the text box next to **Family Protection Package** in the shopping cart area (Figure 16.1).
2. Once you have decided how many Family Protection Packages you would like to purchase, click the **Proceed to Checkout** button.
3. A Payment Information pop-up window will appear (Figure 16.2).
4. Enter your payment information.
5. Click the **Complete Order** button (Figure 16.3).
6. Click the **OK** button to close the Shopping Cart and return to the Securespot 2.0 Management Console page.

Figure 16.2: Payment Information Window

Figure 16.3: Thank you Box

Total Home Security Package

Select this package if you want to protect your household from inappropriate content and objectionable Web sites, track Internet usage, and provide McAfee AntiVirus/Spyware protection, Spam Controls, Pop-up Blocking, Identity Theft Protection, and Intrusion Detection.

1. Enter the number of licenses that you would like to purchase in the text box next to **Total Home Security Package** in the shopping cart area.
2. Once you have decided how many Total Home Security Packages you would like to purchase, click the **Proceed to Checkout** button.
3. A Payment Information pop-up window will appear (Figure 16.2).
4. Enter your payment information.
5. Click the **Complete Order** button. Follow the steps in the blue box (Figure 16.3).
6. Click the **OK** button to close the Shopping Cart and return to the Securespot 2.0 Management Console page.

To remove a PC from the shopping cart

1. Select the ✘ icon (delete) next to computer that you want to remove from the shopping cart.
2. You will be prompted with a pop-up window.
3. Click **OK** if you want to delete this device from the shopping cart.

17. Technical Support

How to Get Support

For SECURESPOT Services Functionality Issues – Contact SECURESPOT Service

- Support Hours: 7am – 12 pm Midnight CST (Central Standard Time)
- 7 Days a Week
- E-mail or Chat links
    - NOTE: Refer to e-mail and chat features listed under the Support tab on the SECURESPOT Management Console. (Support Function section of the SECURESPOT 2.0 User Manual)
- Call: 1-866-837-8908

For Basic Router Functionality Issues – Contact D-Link Technical Support

- Hours: 24x7
- Call: 1-877-453-5465
- **http://support.dlink.com/contact/**

Appendix A – Upgrading Router Firmware

Firmware Upgrade

To install Securespot 2.0 Security Services to your DIR-625 router, you must upgrade the Router Firmware to v3.06. NOTE: Firmware v3.03 or above must uploaded on your D-Link Router before you can upload firmware v3.06.

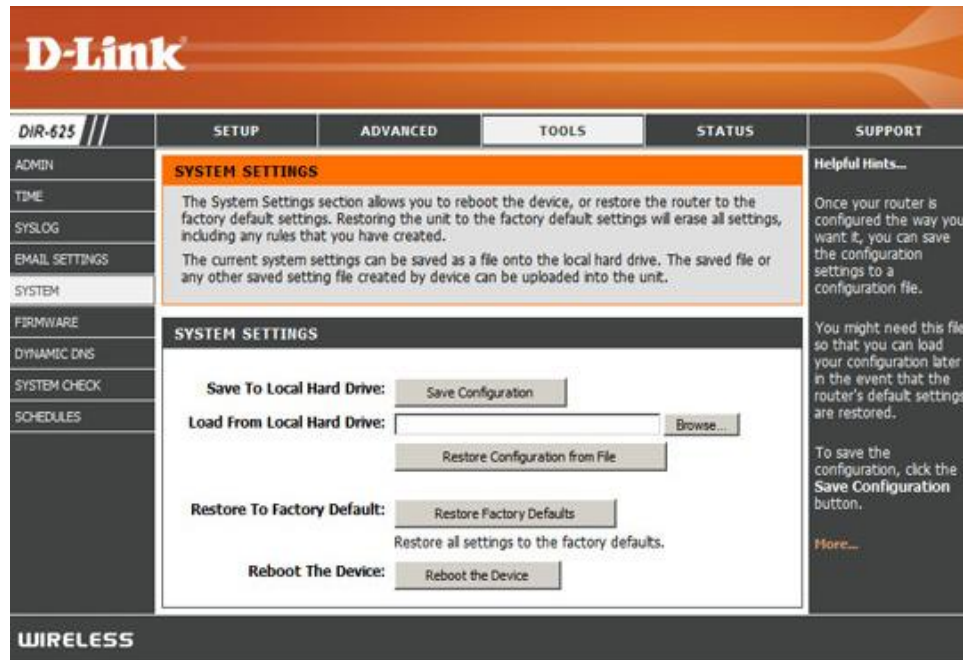**Figure A.1:** Router Tools Menu

Figure A.2: Systems Setting Page

To Upgrade your Firmware

1. Ensure your PC has a wired connection to the router.

2. Open any Web browser and log into the D-Link DIR-625 Product Login page (http://192.168.0.1).

3. Select your router username, enter your password, and then click the Log In button.

4. Select the **Tools** menu. (Figure A.1)

5. Select the **System** link on the **Tools** menu. (Figure A.2)

6. Click the **Save Configuration** button. (NOTE: To retain your existing Router configuration settings, you must manually save these settings before upgrading the Router firmware.)

7. A **File Download** pop-up window will appear on your screen. Click the **Save** button.

8. A **Save As** pop-up window will appear on your screen. You may rename the file something easy to remember, or save it as the default file name, gateway_settings.gws.

9. Click the **Save** button to save this file to your desktop.
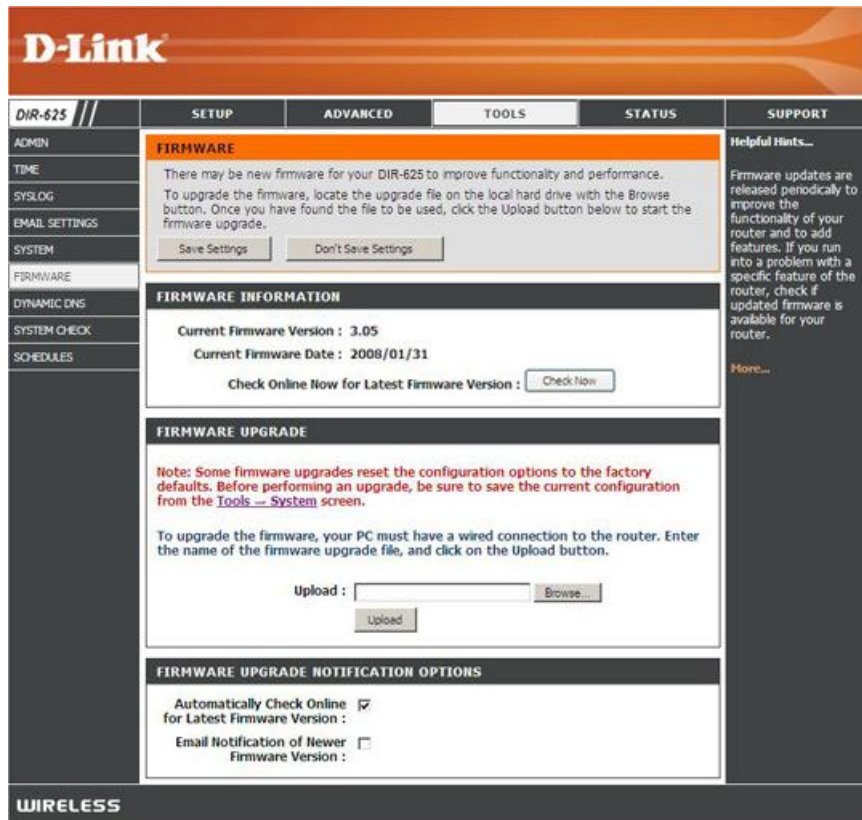
Figure A.3: Firmware Information Section

10. Select the **Firmware** link on the **Tools** menu. Verify the version in the Firmware Information section. (Figure A.3)

11. Click the **Browse** button in the Firmware Upgrade section. A Choose File pop-up window will appear on your screen

12. Select the appropriate firmware file (*.bin), and click **Open**. (Figure A.4)

13. Click the **Upload** button in the Firmware Upgrade section. NOTE: It may take up to 90 seconds to complete the upgrade.

14. A pop-up window appears on the screen warning you about your configuration options. Click **OK**.

15. A second pop-up window appears verifying the firmware file. Click **OK**.
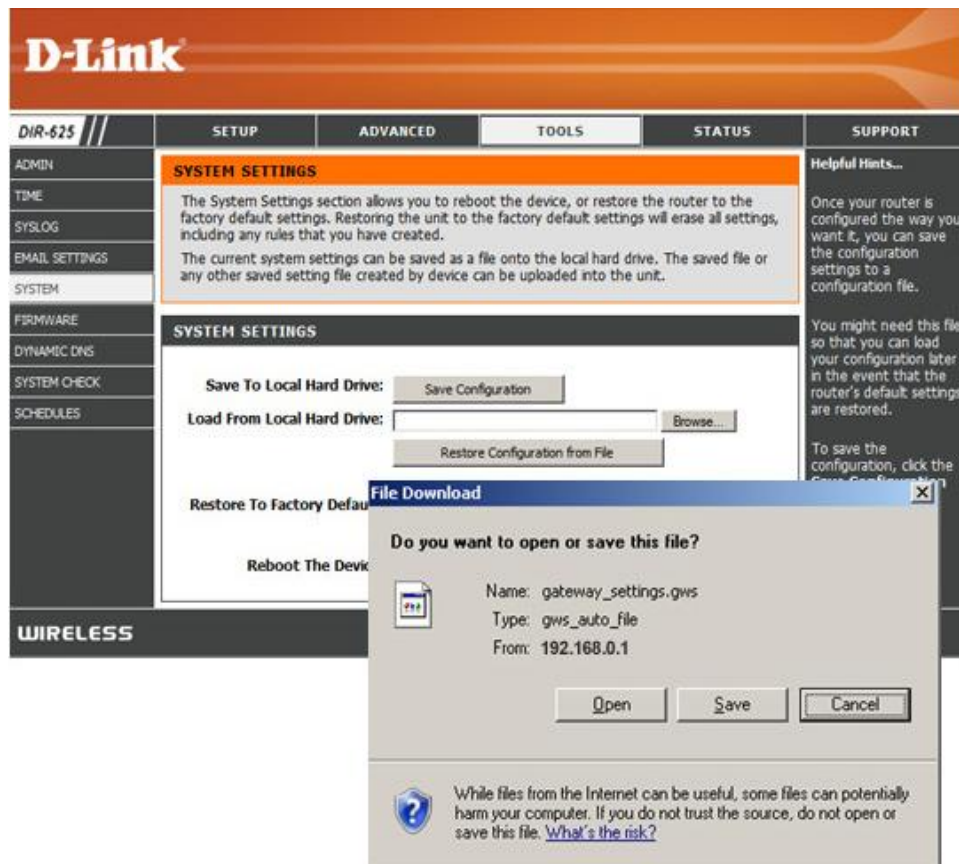
Figure A.4: Open File

Figure A.5: Upload Success

16. When firmware upgrade is complete, an **Upload Succeeded** pop-up window will appear on your screen. (Figure A.5)

17. After the process is complete you will be redirected back to the D-Link DIR-625 Product Login page.

Appendix B – Restoring Configuration Settings

Restore Configuration Settings

This option restores all configuration settings back to the settings that were in effect for your previous version of firmware. This will save you from having to manually reconfigure your settings after upgrading your Firmware.

Figure B.1: Administrator Settings

Use the following procedure to Restore previous Configuration Settings

1. Click the **Tools** menu. (Figure B.1)

2. Select the **System** link on the **Tools** menu. (Figure B.2)

3. Click the **Browse** button in the System Settings section.

4. A **Choose File** pop-up window appears on your screen.

5. Select the appropriate configuration file (e.g. gateway_settings.gws) and click **Open**.

6. Click **Restore Configuration from File** on the System Settings page. (NOTE: Please wait while the configuration is being restored.)

7. When Restore Configuration is done, a **Restore Succeeded** pop-window will appear on your screen. (Figure B.3)

8. You must reboot your router before the restored settings will take effect. Click the **Reboot Now** or **Reboot Later** button.
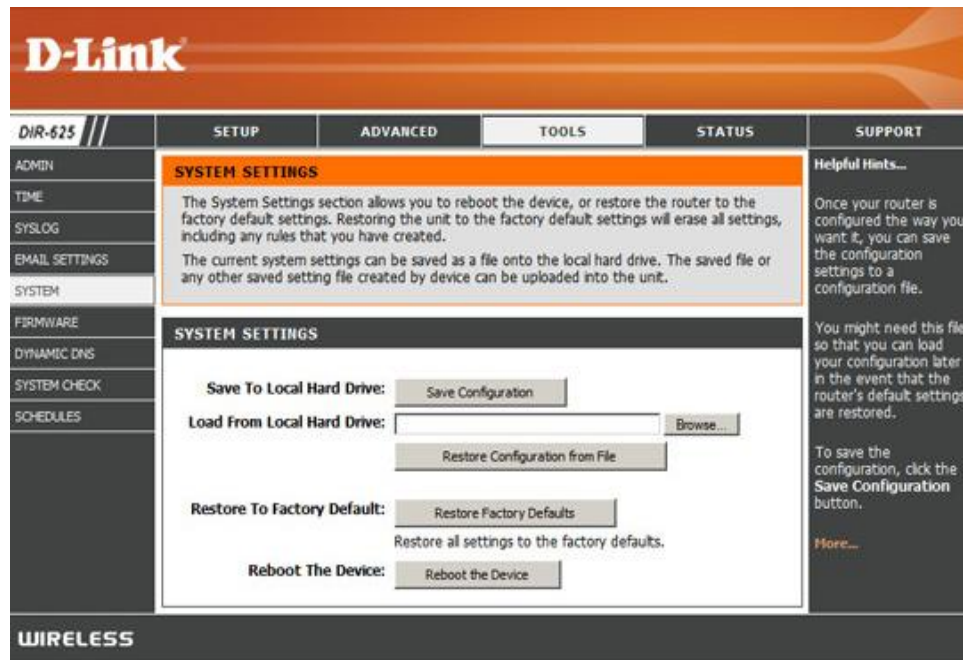

Figure B.2: System Settings

Figure B.3: Restore Success

Appendix C – How Icons Differ and Why

Registered Device – Any device that accesses the WAN side of the router and progresses through the Access Control registration.

Registered Devices (non-PC based) – Many other devices are automatically added to the Web UI after accessing the WAN side of the router.

Unknown Devices – These devices have not gone through the Access Control registration process but have attempted to access the WAN side of the router.

Guest Icons – These icons are only created when Access Control is enabled and the user chooses Guest account instead of registering the device. A guest account only lasts for 24 hours before the user must choose again to register or continue to be a guest on the network.

Caution Icon – Any device will display a "caution" yellow icon if any of the services have been disabled. This is only to alert the customer that something is turned off not that there is a potential problem with that particular computer on their network.

Guest Setup – This is where all configuration for Guest Accounts are set. Anything relating to guest accounts is setup in this section including Guest account passwords.

Selected Device - To configure any device for SecureSpot services that device must be selected. The background color for the device is blue (as show to the left) when the device is the selected