

Securespot User Manual

Table Of Contents

Getting Started.....3

Security Services.....37

Appendix – Backup and Firmware Upgrade.....98

Getting Started

Simplified All-In-One Security

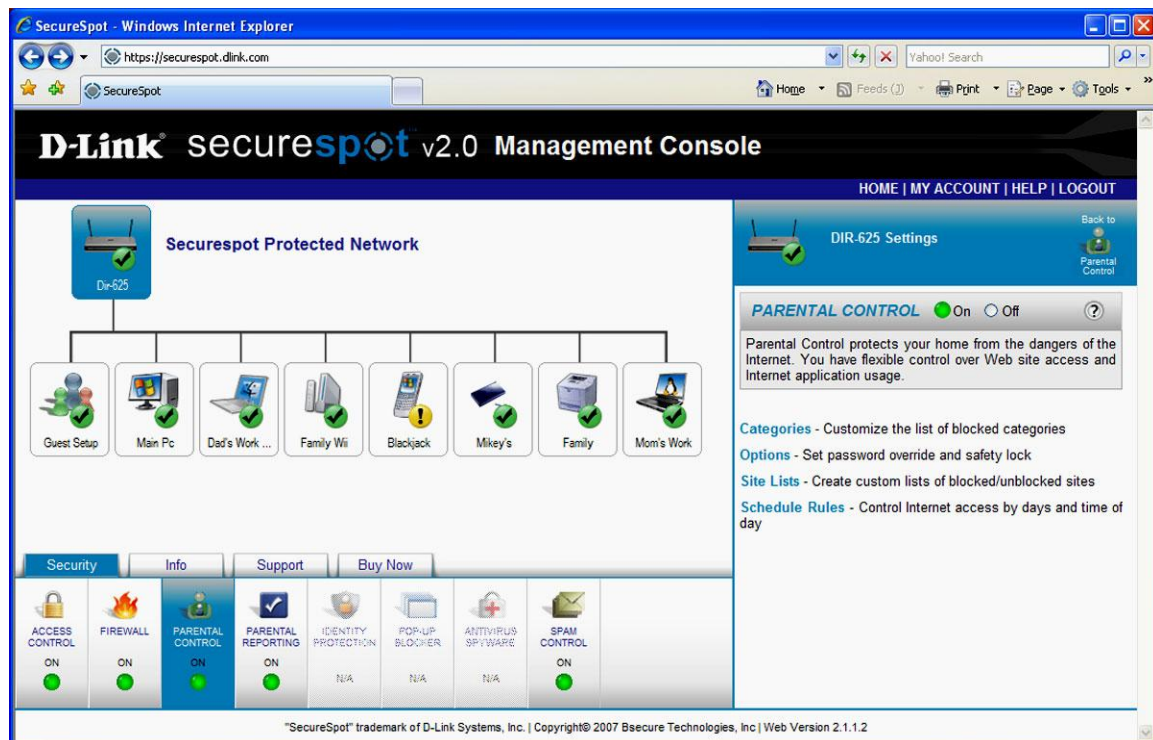
The Securespot 2.0 Services furnished with your D-Link RangeBooster N™ Router offer a complete, all-in-one Internet security solution that provide the easiest and most affordable way to protect your family, computers, data, and personal information from the many dangers and security threats of the Internet.

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, anti-SPAM, 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 thin-client application (25X smaller than leading security suites) that protects PCs and Macs 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. 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 services, even when you're away from home.



Three Layers of Protection

Securespot is the first to provide whole-home protection by utilizing three layers: a managed Web Services Layer outside the home, and the Router and individual Computer layers inside the home. Protection is implemented where it is most efficient and provides the most functionality. For example, by performing the heavy lifting at the back-end Web Services layer instead of on each computer, performance and footprint are greatly improved, and support issues are reduced. Executing the Firewall, Parental Controls and other security features 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 malicious Web sites that can infect your computers or steal your family's personal and financial information. Securespot 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.

Award-Winning 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 the Securespot v2.1.2 services:

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

Registration

Securespot v2.1.2 Security Services are easy to register and setup. After you have installed the D-Link Router to your network, simply follow these steps to begin registration. *(These security services will replace your existing security software and provide total protection for your network, PCs, and your family!)*

1. Open any Web browser.
2. Once you have upgraded your router to the latest version (v3.05), you are directed to the Securespot v2.1.2 Registration page.



3. Click the **Next** button to activate Securespot v2.1.2 security services.
4. Once you click the **Next** button, you are directed to the Registration Information page.

D-Link securespot v2.0 Management Console

HOME | HELP | LOGIN

Registration Information (information collected is secure and strictly adheres to our [Privacy Policy](#).)

First Name: Last Name:

* E-mail Address: Phone:

* New Password: * Confirm Password:

* Required to create account login


☐ I agree to these terms of the Service Agreement and wish to continue [View](#)

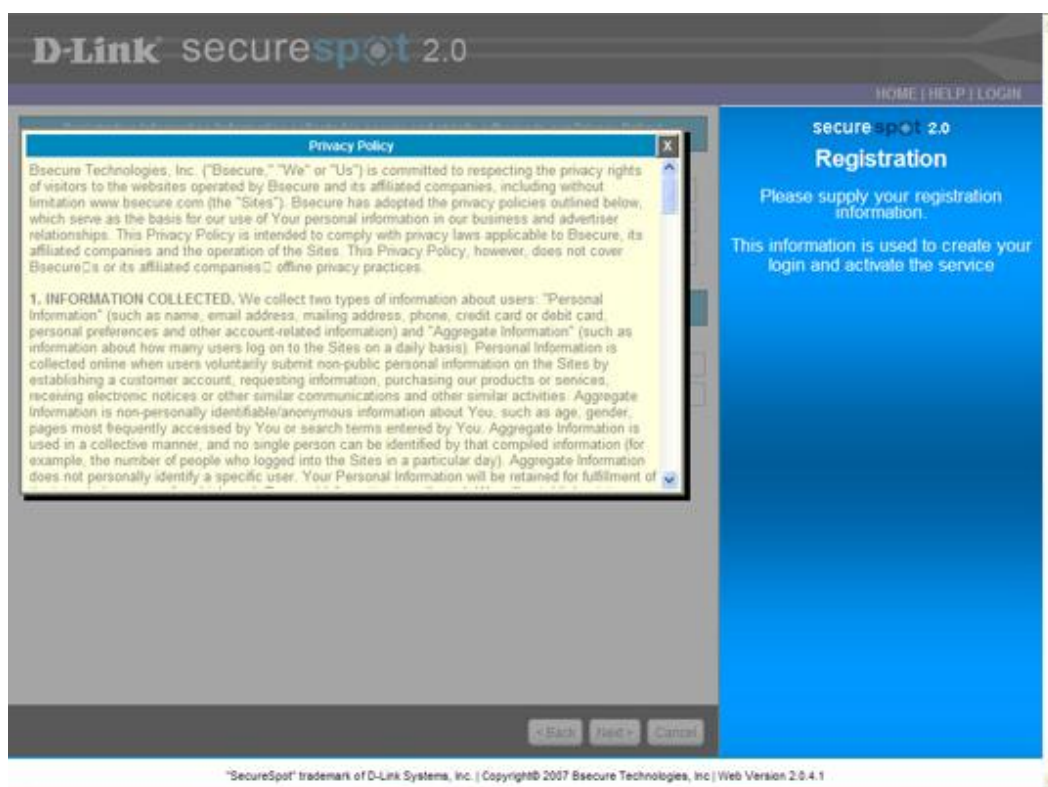
secure spot v2.0
Registration

Please supply your registration information.
This information is used to create your login and activate the service.

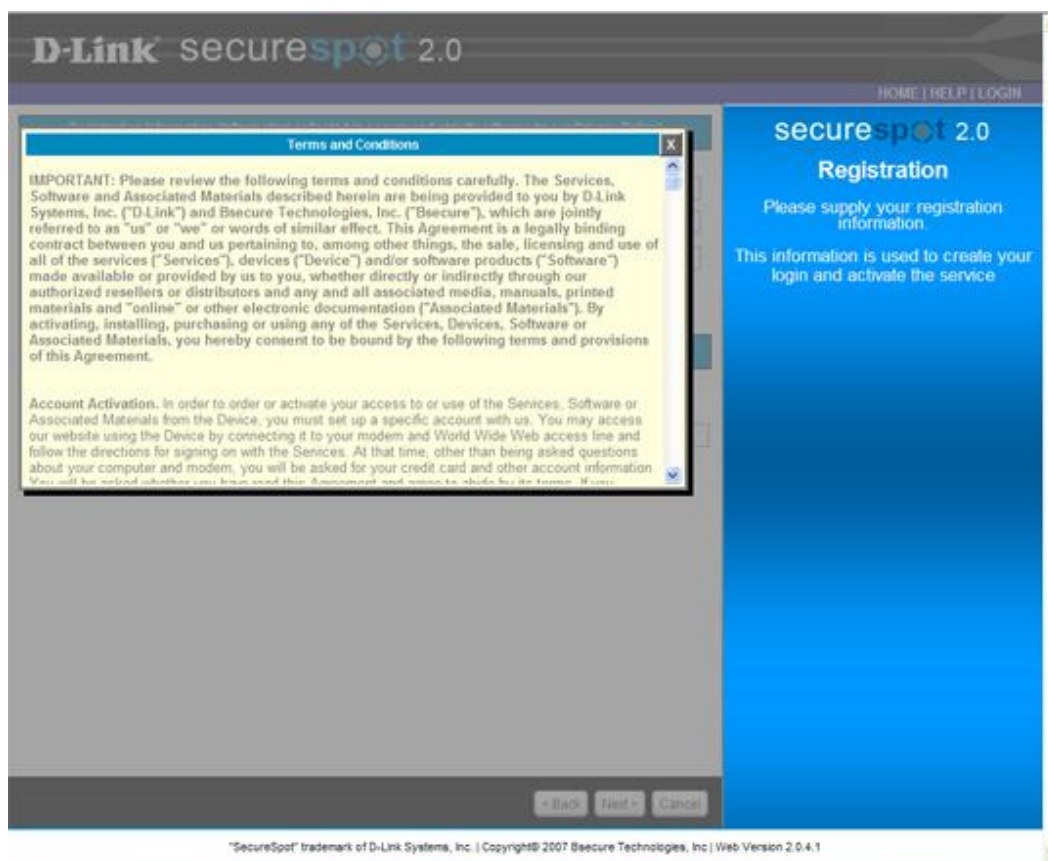
< Back Next > Cancel

"SecureSpot" trademark of D-Link Systems, Inc. | Copyright© 2007 Bsecure Technologies, Inc | Web Version 2.0.4.1

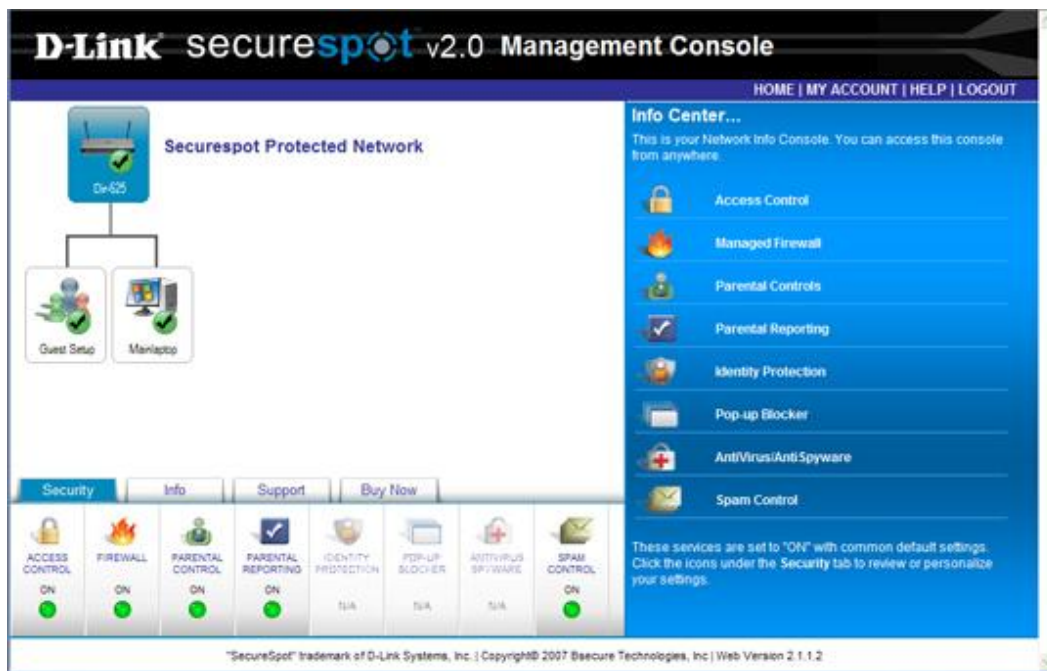
5. Enter the appropriate contact information and select a password, respectively.
6. (Click the **Privacy Policy** link to display the Privacy Policy.) Click the  icon to close the **Privacy Policy** pop-up window.



7. Select the Service Agreement check box to continue registration. (Click **View** on the Registration Information page to display the Terms and Conditions Agreement.)



8. Click the **X** icon to close the **Terms and Conditions** pop-up window.
9. Click **Next>** on the Registration Information page. (*Please wait while the request is being processed.*)
10. Once your request has been processed, you are directed to a Securepot v2.1.2 Management Console page. (*The Securespot v2.1.2 Services are now activated.*)



Navigation Buttons

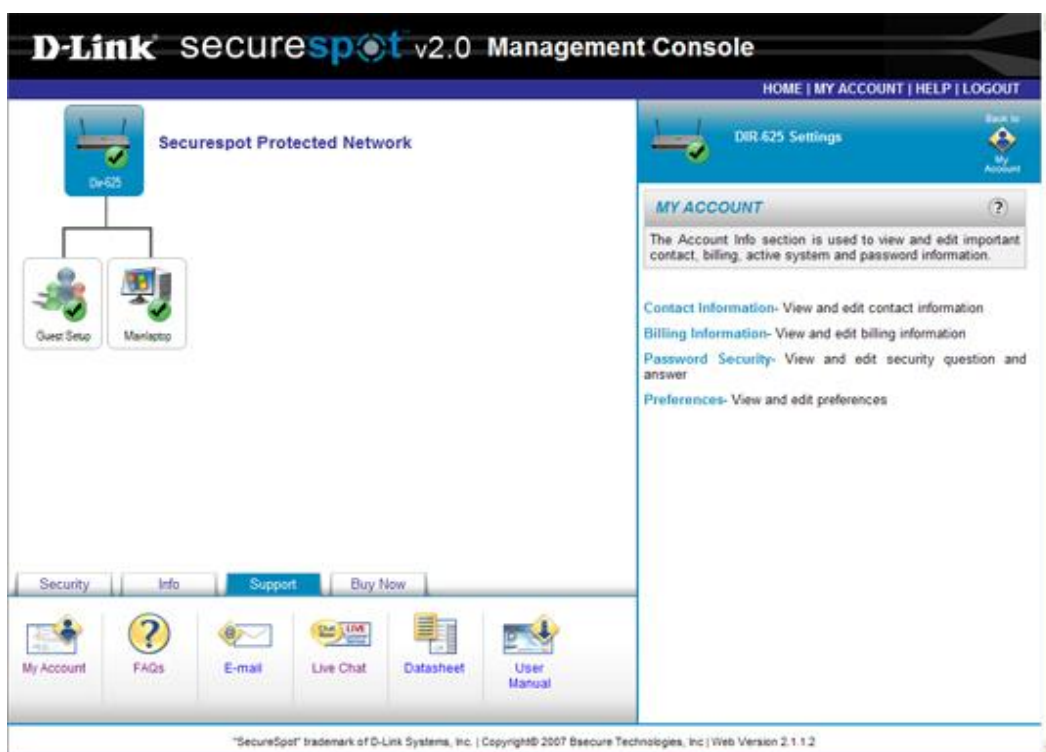
These buttons display the Securespot Landing Page, Account Information, Help, and Logout links. Click the individual links for more information.

Buttons


Home – Click the Home link at the top of any Securespot v2.1.2 Security Services page to return to the Securespot v2.0 Services landing page.

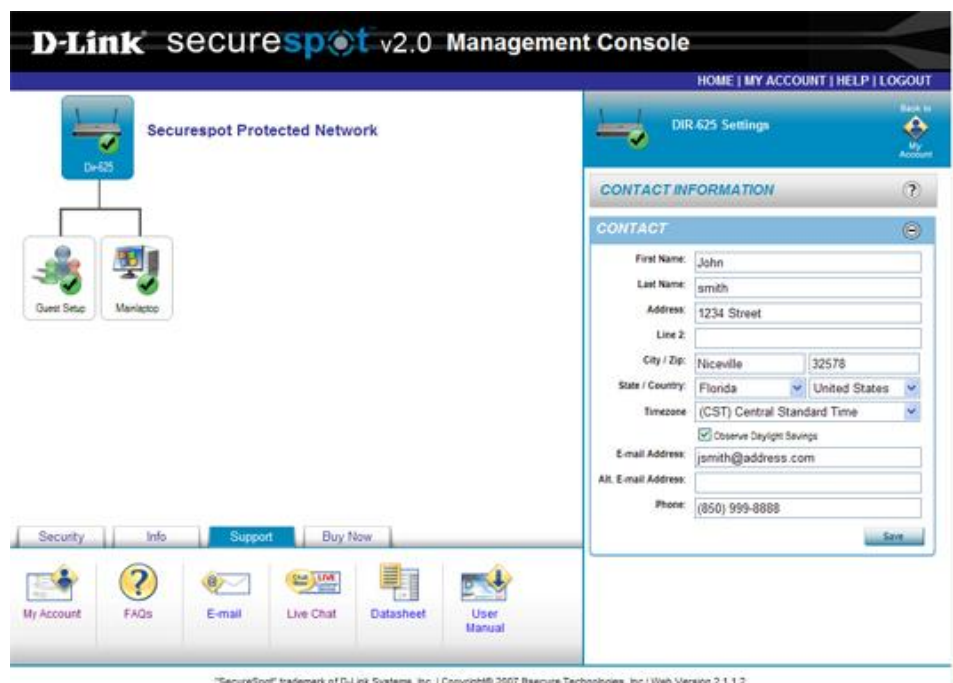


My Account – Click the My Account link at the top of any Securespot v2.1.2 Security Services page to open the My Account panel under the **Support** tab.





To view and/or edit contact information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Contact Information** link on the My Account panel.




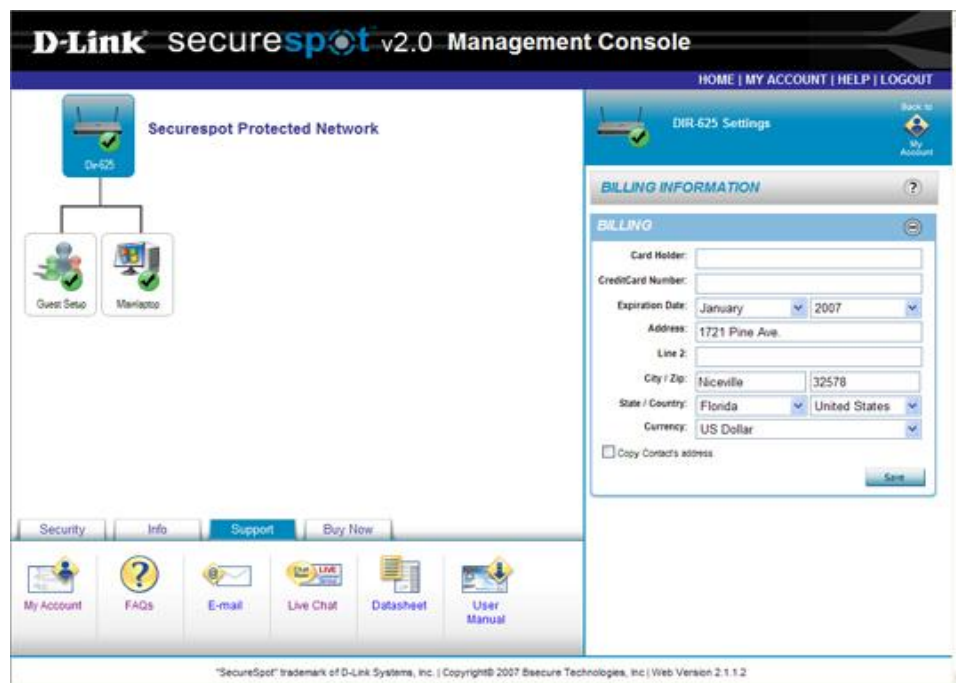
- Select or enter the appropriate data into the drop-down list or text boxes, respectively.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Contact Information saved" appears on the Contact Information Feature panel.)

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Contact Information details, click the  icon.

To view and/or edit billing information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Billing Information** link on the My Account panel.





- Select or enter the appropriate data into the drop-down list or text boxes, respectively.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Billing Information saved" appears on the Billing Information Feature panel.)

OR

- Click the  icon to return to the My Account Service panel without saving changes.

- To hide Billing Information details, click the  icon.



To view and/or edit your password information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the  icon to expand the **Password Security** panel.




- Type a security question and answer in the provided fields.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Security Information saved" appears on the Password Security panel.)

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Password Security details, click the  icon.



To view and/or change your preferences:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Preferences** link on the My Account panel.



- Select the appropriate check box to turn OFF some of the initial Securespot Landing page preferences.
- Click **Save** to save your settings. (*Once your settings have been saved, the message "The preferences have been saved" appears on the Preferences panel.*)

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Preferences details, click the  icon.

Help – Click the Help link to open D-Link Customer Services support.

D-Link

ANSWERS | ASK A QUESTION | LOGIN | HELP

SUPPORT

Category: Search Text (optional): Search:

Product: Search By: Sort By:

ANSWERS FOUND

210 Answers Found Page: of 11

ID	Summary	%
1	610 Is the SecureSpot compatible with Windows Vista?	100
2	625 I receive a Runtime Error when downloading the Thin Client (Windows Vista).	100
3	238 What criteria does the SecureSpot use to block sites?	100
4	93 How do I uninstall the Internet Protection Services?	100
5	261 Do I need to download/install any software once the device is connected to my network?	100
6	392 How much does the SecureSpot cost and what does the price cover?	100
7	279 Will the SecureSpot Internet Protection Services slow down my connection speed?	100
8	208 How many computers can I protect on my home network using the SecureSpot?	100
9	406 I've set up my SecureSpot and now our Xbox can no longer connect to online games.	100
10	118 Will the SecureSpot work with Macintosh Operating Systems?	100
11	262 What does the SecureSpot Download Client License do?	100
12	266 How do I add a computer to my SecureSpot Internet Protection Service?	100
13	315 How do I log in to the SecureSpot device admin site?	100

Logout – Click the Logout link at the top of any Securespot v2.0 Security Services page to close the Securespot v2.1.2 Security Services. (You will be redirected to the Securespot v2.0 Security Services Login page.)

D-Link securespot v2.0 Management Console

HOME | HELP | LOGIN



"My Account" Web Control Center.

D-Link customers that have already registered their SecureSpot™ Internet Security v2.0 Services, should use this page to change their settings. (You may access this page and make changes from anywhere on the Internet.)

E-mail Address: Password:

[Click here if you forgot your password](#)

Network Map

Securespot Security v2.1.2 Services creates a graphical network map of the computers and/or devices that share your Internet connection. The Network Map is automatically updated when a change occurs or new device is added to the Network Map area.

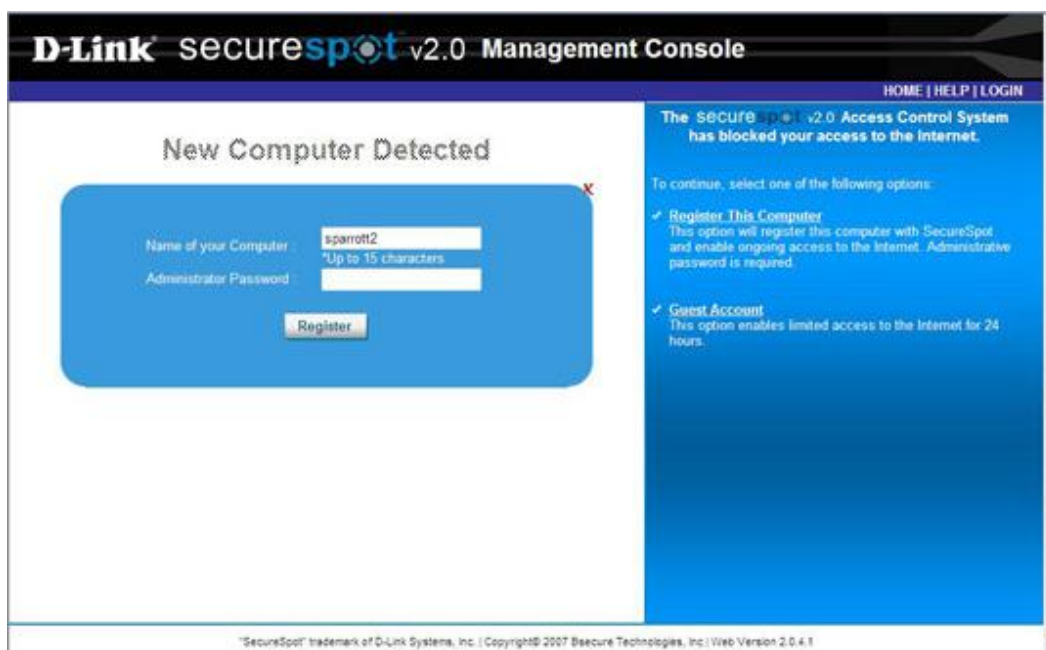
Securespot v2.1.2 Security Services include a Guest Account Setup that can be used to provide anonymous users with Internet access for a 24-hour time frame. Once the Guest Account has been set up, then Parental Control and Parental Reporting services are temporarily available for the Guest Account. *(Once the 24-hour time period has lapsed, the Guest Account is deleted from the Network Map.)*

To add a device:

1. A New Computer Detected page appears on your screen.



2. Click **Register This Computer**.
3. Create a computer name and enter the administrative password.
4. Click **Register** on the New Computer Detected page.



5. To enable Virus/Spyware Protection, Identity Protection, and Pop-up Blocking, click the **Download** button to install the Thin-Client application.

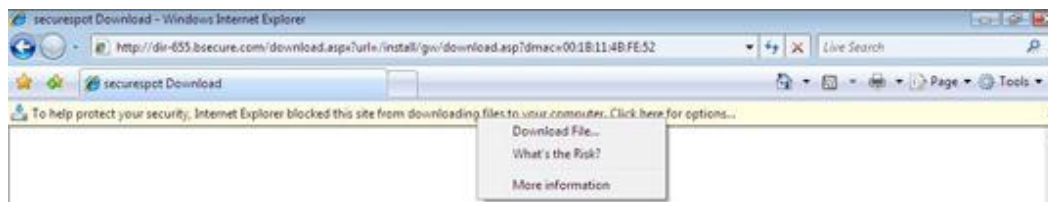


6. A status bar appears on the New Computer Detected page. (*Please wait while Securespot Security v2.1.2 Services processes your request.*)



7. Once Securespot Security v2.1.2 Services processes your request, you will be redirected to the Securespot download page in your Web browser.

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



9. A **File Download** pop-up window appears on your screen. Click **Save**.

10. Once the download is complete, your Web browser is redirected to the Securespot Security v2.1.2 Services landing page with the new device added to the Network Map.



OR

11. Click **No Thanks** if you do not want to download the Thin-Client Application. (You will be redirected to the default page in your Web browser.)



To add a Guest Account:

1. A New Computer Detected page appears on your screen.



2. Click **Guest Account**.

3. A status bar appears on the New Computer Detected page. (*Please wait while Securespot Security v2.1.2 Services processes your Guest Account request.*)



4. Once Securespot Security v2.1.2 Services processes your Guest Account request, you will be redirected to the default page in your Web browser.

To delete a device:

1. Select a device on the network map that you want to delete.

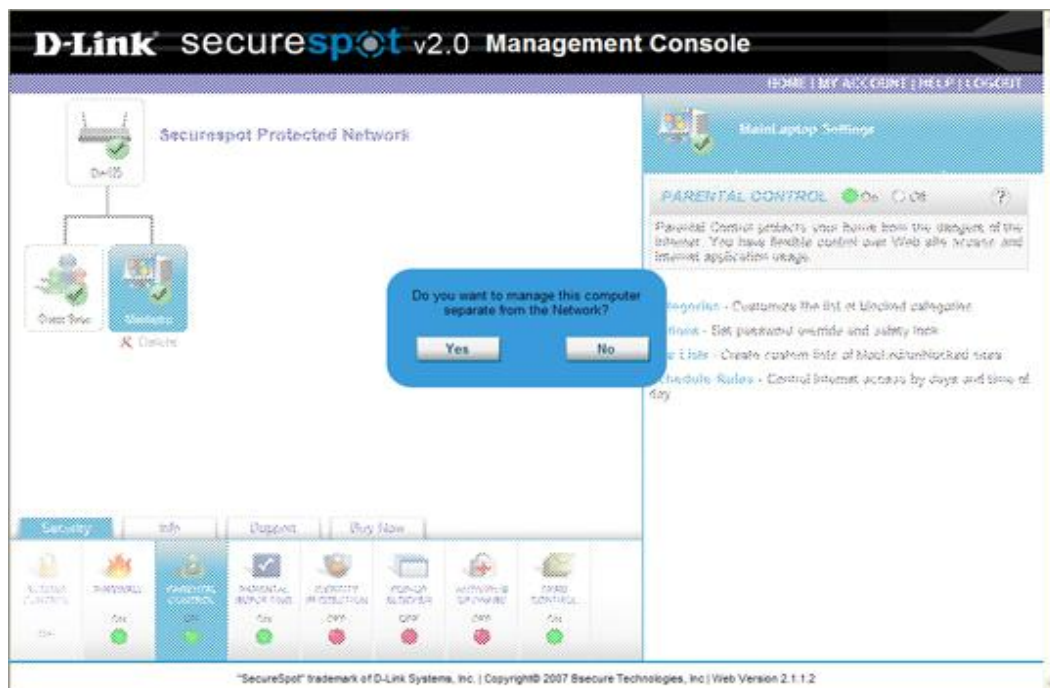
2. Click **Delete** under the highlighted device.
3. A pop-up window will appear on the screen prompting you for a response.
4. Click **OK** to delete the highlighted device.
5. Once your setting has been saved, the message “Selected Device deleted” appears on the Network Map.

OR

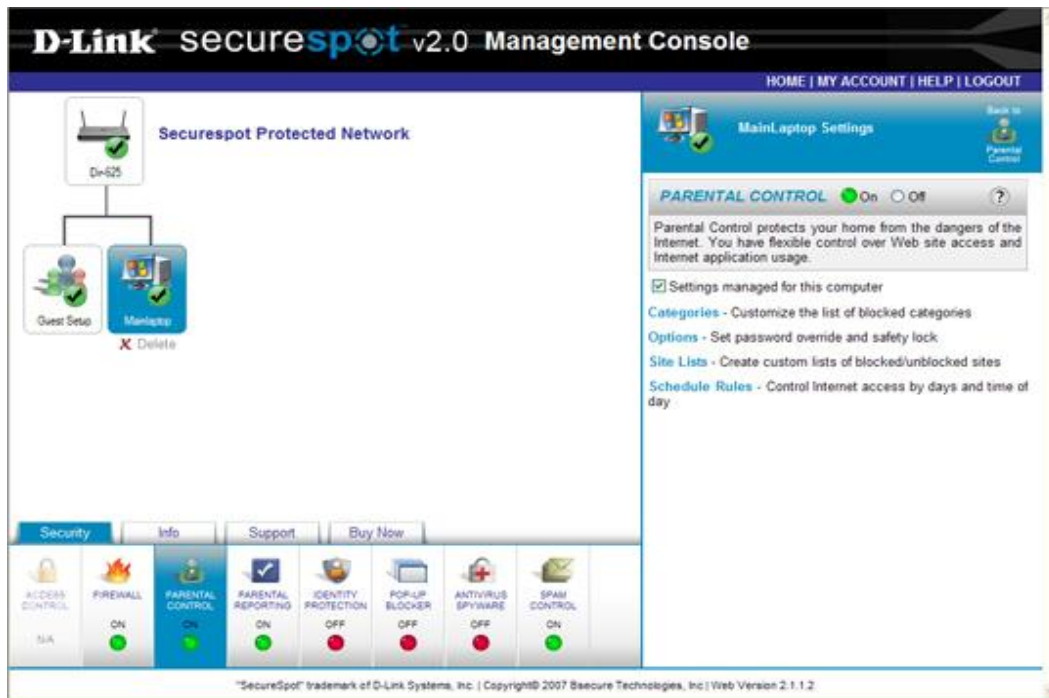
6. Click **Cancel** to return to the Network Map without deleting any device.

To apply customized security settings to a single computer:

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.

Tabs

Security Tab

This tab displays the status for each security service. To customize the individual security services, click the appropriate service icon under the **Security** tab.

Security Services

-  – The **Access Control** feature allows computers to attach to the network without requiring a Thin-Client installation for AntiVirus and Spyware protection.
-  – The **Firewall** feature increases PC security by controlling access to incoming and outgoing Internet ports.
-  – The **Parental Control** feature protects your home from dangers of the Internet, while giving you flexible control over Web sites and Internet application usage.
-  – The **Parental Reporting** feature creates a historical record of the Web sites that can not be altered or erased. 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 calender 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. Currently, the v2.1.2 release is not enabled to send alerts for all categories. *(Note that it will only send alerts when a user attempts to access a pornography or R-rated Web site.)*
-  – The **Identity Protection** feature 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.
-  – The **Pop-up Blocking** feature prevents unwanted and annoying pop-up windows from appearing while you surf the Internet.
-  – The **AntiVirus/Spyware** feature protects your computer from viruses that infect your system and spyware that tracks your Web-browsing habits and steals your personal information.
-  – The **Spam Control** feature 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.

Info Tab

(Note that the selected device in the Network Map will determine what information is displayed under the Info tab.)

This tab displays the following device information:

- **Device Category** – This drop-down list box 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 list box is used to select a specific device type, i.e., PC, XBox360, Skype, etc.
- **Operating System** – This drop-down list box 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 per device.
- **Firmware Version** – This text box displays the latest Firmware version per network device.

To modify device data:

1. Select a specific device on the network map.
2. Click the **Info** tab.



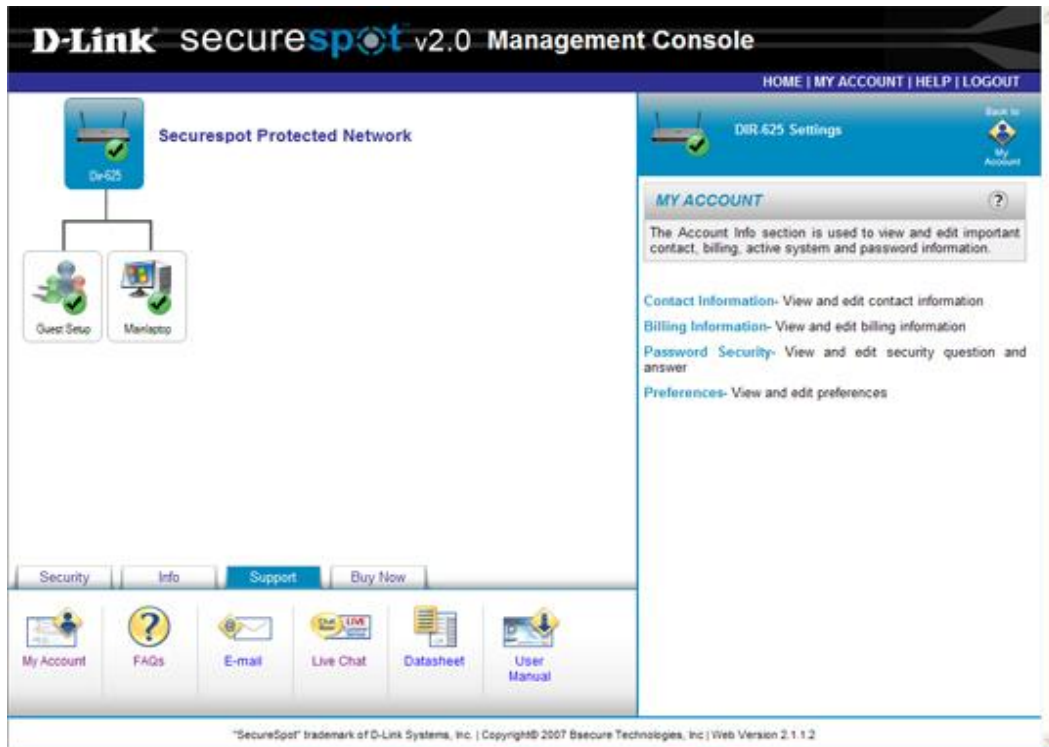
3. Select or enter the appropriate data into the drop-down list or text boxes, respectively.
4. Click **Update**.

Support Tab


This tab displays the Account Information, FAQs, E-mail, Live Chat, Securespot Datasheet, and User Manual links. Click the individual icons for more support information.

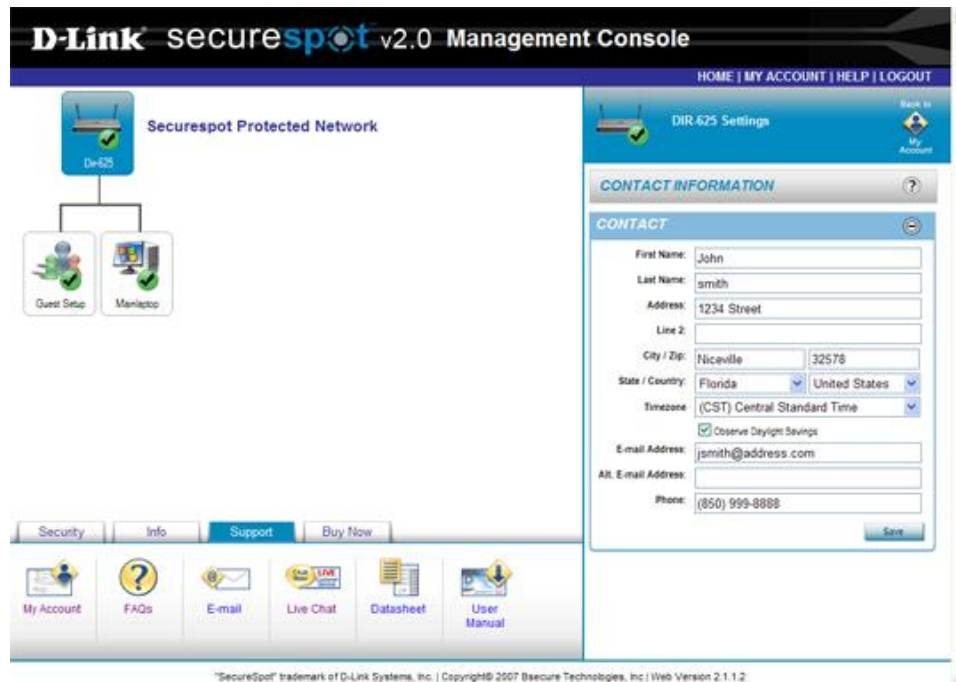
Support Icons

My Account – Click this icon to view and edit contact, billing, password, and preference information.





To view and/or edit contact information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Contact Information** link on the My Account panel.




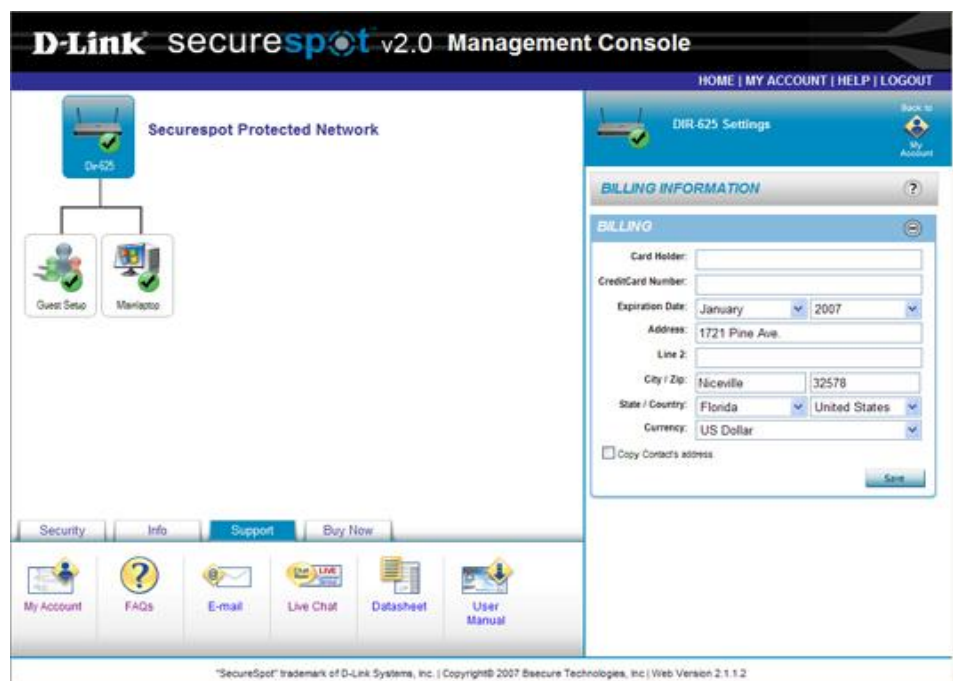
- Select or enter the appropriate data into the drop-down list or text boxes, respectively.
- Click **Save** to save your settings. (*Once your settings have been saved, the message "Contact Information saved" appears on the Contact Information Feature panel.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Contact Information details, click the  icon.



To view and/or edit billing information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Billing Information** link on the My Account panel.





- Select or enter the appropriate data into the drop-down list or text boxes, respectively.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Billing Information saved" appears on the Billing Information Feature panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Billing Information details, click the  icon.



To view and/or edit your password information:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the  icon to expand the **Password Security** panel.




- Type a security question and answer in the provided fields.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Security Information saved" appears on the Password Security panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Password Security details, click the  icon.



To view and/or change your preferences:

- Select a specific device on the network map.
- Click the **Support** tab and the  icon, respectively.
- Click the **Preferences** link on the My Account panel.



- Select the appropriate check box to turn OFF some of the initial Securespot Landing page preferences.
- Click **Save** to save your settings. (*Once your settings have been saved, the message “The preferences have been saved” appears on the Preferences panel.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the My Account Service panel without saving changes.
- To hide Preferences details, click the  icon.

FAQs – Click this icon to launch the D-Link Securespot FAQ page.

D-Link

ANSWERS | ASK A QUESTION | LOGIN | HELP

SUPPORT

Category: Search Text (optional): Search:

Product: Search By: Sort By:

ANSWERS FOUND

210 Answers Found Page: of 11

ID	Summary	%
1	610 Is the SecureSpot compatible with Windows Vista?	100
2	625 I receive a Runtime Error when downloading the Thin Client (Windows Vista).	100
3	238 What criteria does the SecureSpot use to block sites?	100
4	93 How do I uninstall the Internet Protection Services?	100
5	261 Do I need to download/install any software once the device is connected to my network?	100
6	392 How much does the SecureSpot cost and what does the price cover?	100
7	279 Will the SecureSpot Internet Protection Services slow down my connection speed?	100
8	208 How many computers can I protect on my home network using the SecureSpot?	100
9	406 I've set up my SecureSpot and now our Xbox can no longer connect to online games.	100
10	118 Will the SecureSpot work with Macintosh Operating Systems?	100
11	262 What does the SecureSpot Download Client License do?	100
12	266 How do I add a computer to my SecureSpot Internet Protection Service?	100
13	315 How do I log in to the SecureSpot device admin site?	100

E-mail – Click this icon to submit an e-mail form to Securespot Customer Services support. (Once you filled out the e-mail form, click the **Submit** button.)

D-Link securespot v2.0 Management Console

HOME | MY ACCOUNT | HELP | LOGOUT

SecureSpot Protected Network

DIR-625 Settings

E-MAIL SUPPORT

Use this form to obtain more product and/or technical information from our Customer Support staff.

Note: After pressing the Submit Form button, please wait until you receive a "Thank You" screen confirming your request has been sent. Clicking on the button multiple times will result in duplicate messages arriving in our mailbox.

E-MAIL FORM

Name:

Type of Question: ☒ Billing ☐ Support

E-mail Address:

Phone Number: where you can be reached for further information

Question / Comment:

(If a technical problem, please provide as much information as possible about your system and any errors you may be seeing.)

Security | Info | **Support**

My Account | FAQs | E-mail | Live Chat | Datasheet | User Manual

"SecureSpot" trademark of D-Link Systems, Inc. | Copyright© 2007 Baocore Technologies, Inc | Web Version 2.1.2.3

Live Chat – Click this icon to launch Live Chat and speak with a Support Agent.

Live Assistance

Answers
Ask a Question
Live Help
My Support
Login
Help

Chat with a Support Agent

*First Name:

*Last Name:

*Email Address:

Product: All

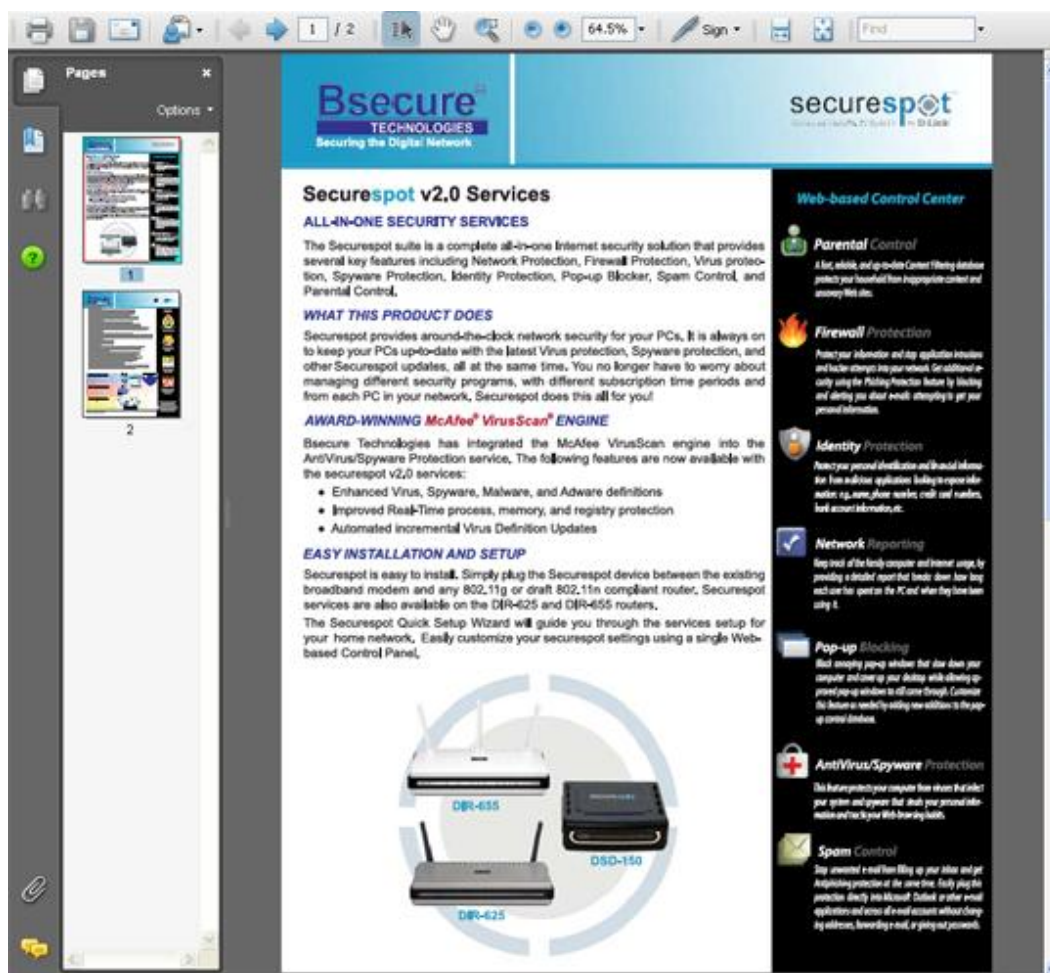
* Denotes a required field.

Please Note:

- Chat support is available:
 - MondayAM - 07:00 - 11:00
 - Sunday: PM CDT
- It is currently
 - Thursday, Aug. 23, 2007 05:18 PM CDT

Copyright © 2004-2006 D-Link Systems, Inc.

Datasheet – Click this icon to open the Securespot v2.0 Services datasheet.



User Manual – Click this icon to open the Securespot v2.1.2 Services User Manual.

Buy Now Tab

This tab displays the Securespot Services Upgrade link. Click this icon to display the Securespot Services upgrades panel and shopping cart.

D-Link securespot v2.0 Management Console

HOME | MY ACCOUNT | HELP | LOGOUT

DIR-625 Settings

Please specify the level of protection for each computer.

Computer Name	Family Package	Total Package	Price
MainLaptop	<input checked="" type="radio"/>	<input type="radio"/>	\$15.00
Additional Licenses	<input type="text" value="0"/>	<input type="text" value="0"/>	\$0.00
TOTAL			\$15.00

[Buy Now](#)

Security | Info | Support | **Buy Now**

Service Upgrade

SERVICE UPGRADE (?)

Family Protection Package
(Only \$15 per computer or \$30 for 2)

- ✓ Comprehensive, whole home protection with
- ✓ Parental Controls web filtering and Time Scheduling
- ✓ Web Usage Reporting options
- ✓ (Includes "No Charge" Security Services above)

Total Home Security Package
(Only \$30 per computer or \$60 for 2)

- ✓ Includes Package above PLUS;
- ✓ **McAfee** Anti-Virus and Anti-Spyware protection
- ✓ Anti-Spam Controls
- ✓ Pop-up Blocker
- ✓ Identity Theft Protection
- ✓ Intrusion Detection

"SecureSpot" trademark of D-Link Systems, Inc. | Copyright© 2007 Securo Technologies, Inc. | Web Version 2.1.1.2

To select the Family Protection Package:

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

- Select the Family Package option button for each existing computer on your network.
- When you are done, click the **Buy Now** button.
- A **Payment Information** pop-up window will appear in the Network Map region.

The screenshot shows the D-Link SecureSpot v2.0 Management Console. The main area is a blue box titled "Payment Information" with a close button (X) in the top right corner. It contains a form with the following fields:

- Cardholder: Required Field Card Holder Name is required
- Card Number: Required Field Credit Card Number is required
- Expiration Date: January 2007
- Card Address: 1721 Pine Ave.
- Line 2:
- City: Niceville
- State: Florida
- Zip/Postal Code: 32578
- Country: United States

At the bottom of the form is a "Buy Now" button. To the right of the form is a "SERVICE UPGRADE" section with two options:

- Family Protection Package** (Only \$15 per computer or \$30 for 3):
 - Comprehensive, whole home protection with
 - Parental Controls web filtering and Time Scheduling
 - Web Usage Reporting options
 - (Includes "No Charge" Security Services above)
- Total Home Security Package** (Only \$30 per computer or \$60 for 3):
 - Includes Package above PLUS:
 - McAfee Anti-Virus and Anti-Spyware protection
 - Anti-Spam Controls
 - Pop-up Blocker
 - Identity Theft Protection
 - Intrusion Detection

At the bottom of the console, there is a navigation bar with links: Security, Info, Support, and Buy Now. Below the navigation bar is a "SecureSpot" logo and a copyright notice: "SecureSpot" trademark of D-Link Systems, Inc. | Copyright© 2007 Secure Technologies, Inc. | Web Version 2.1.1.2

- Enter your payment information.
- Click the **Buy Now** button. (After information has been processed, you will be redirected to the Securespot Security Services home page.)

To select the Total Home Security Package:

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

- Select the Total Home Security Package option button for each existing computer on your network.
- When you are done, click the **Buy Now** button.
- A **Payment Information** pop-up window will appear in the Network Map region.
- Enter your payment information.
- Click the **Buy Now** button. (After information has been processed, you will be redirected to the Securespot Security Services home page.)

To remove a PC from the shopping cart:

- Select the **X** icon next to computer that you want to remove from the shopping cart.
- You will be prompted with a pop-up window.

- Click **OK** if you want to delete this device from the shopping cart.

OR

- Click **Cancel** to return to the shopping cart.

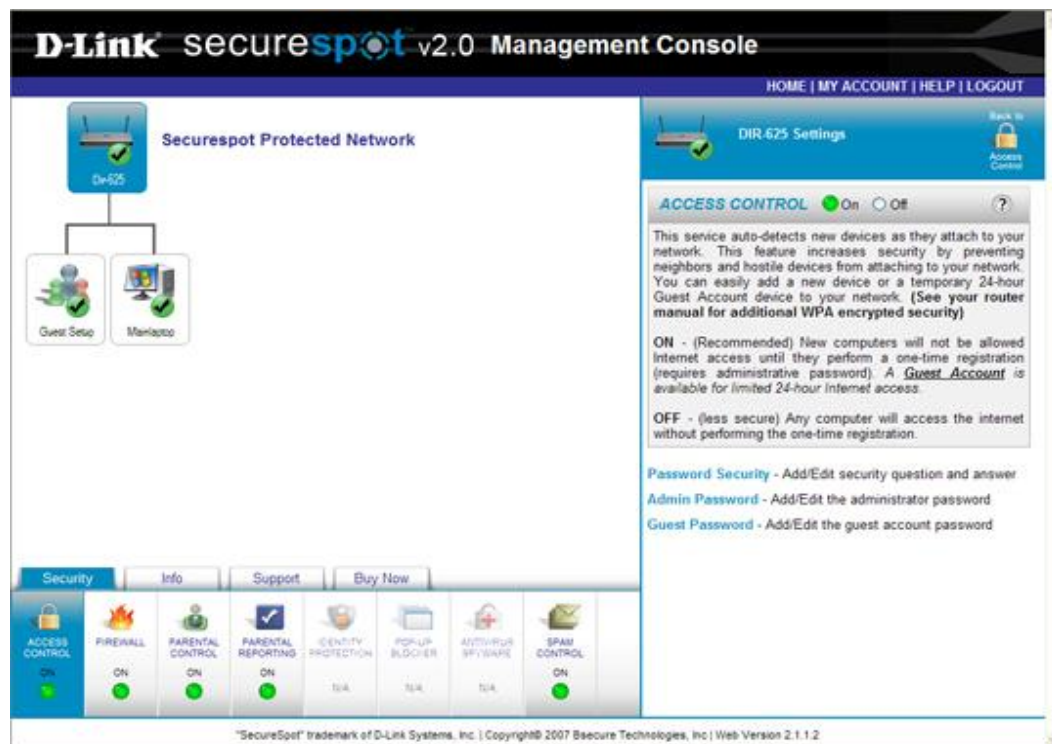
Security Services


Access Control Service

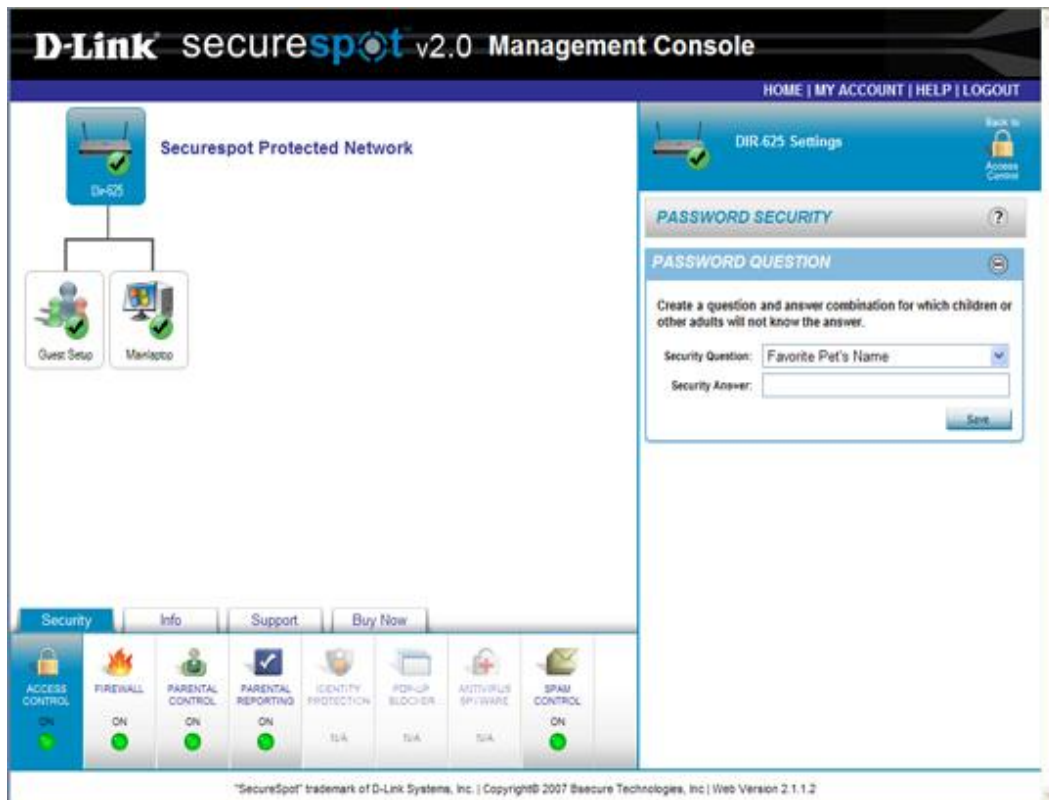
This feature allows networked computers and guest accounts access to the Internet without requiring a Thin-Client Installation.

To enable Access Control

1. Select the DIR-625 icon on the network map.
2. Click the **Access Control** service under the **Security** tab.





3. Click the  icon to hide/display descriptive Access Control information.
4. Select the **ON** option button to enable the Access Control service. (*The default is OFF.*)
5. To view and/or change your password information, click the Password Security link on the Access Control Service panel

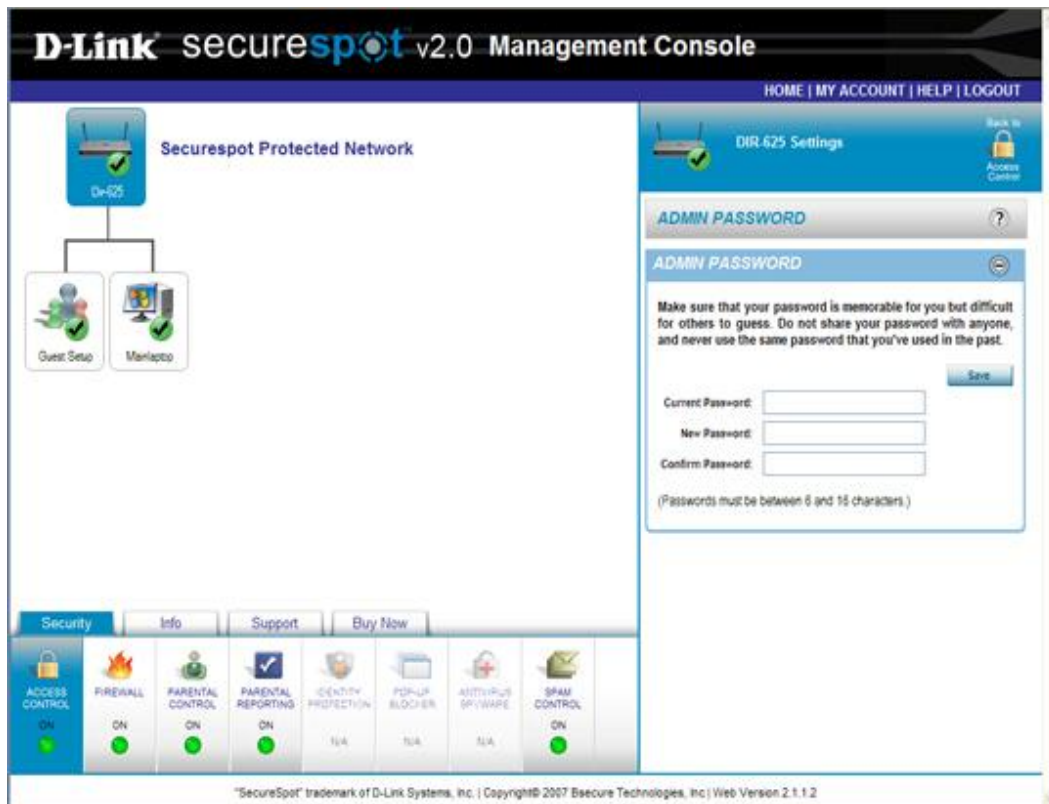


- Type a security question and answer in the provided fields.
- Click **Save** to save your settings. (*Once your settings have been saved, the message “Security Information saved” appears on the Password Security panel.*)
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Access Control Service panel without saving changes.
- To hide Password Security details, click the  icon.

6. To view and/or change your master password, click the Admin Password link on the Access Control Service panel. (*The administrative password is the password that you created when registering the Securespot Services.*)



- Type your current password, type a new password, and then confirm the new password.
- Click **Save** to save your settings. (Once your settings have been saved, the message “Administrative Password saved” appears on the Admin Password panel.)
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Access Control Service panel without saving changes.
- To hide Admin Password details, click the  icon.

7. To view and/or change your guess account password, click the Guest Password link on the Access Control Service panel.



- Type your current password, type a new password, and then confirm the new password.
- Click **Save** to save your settings. (*Once your settings have been saved, the message "Guest Password saved" appears on the Guest Password panel.*)

OR

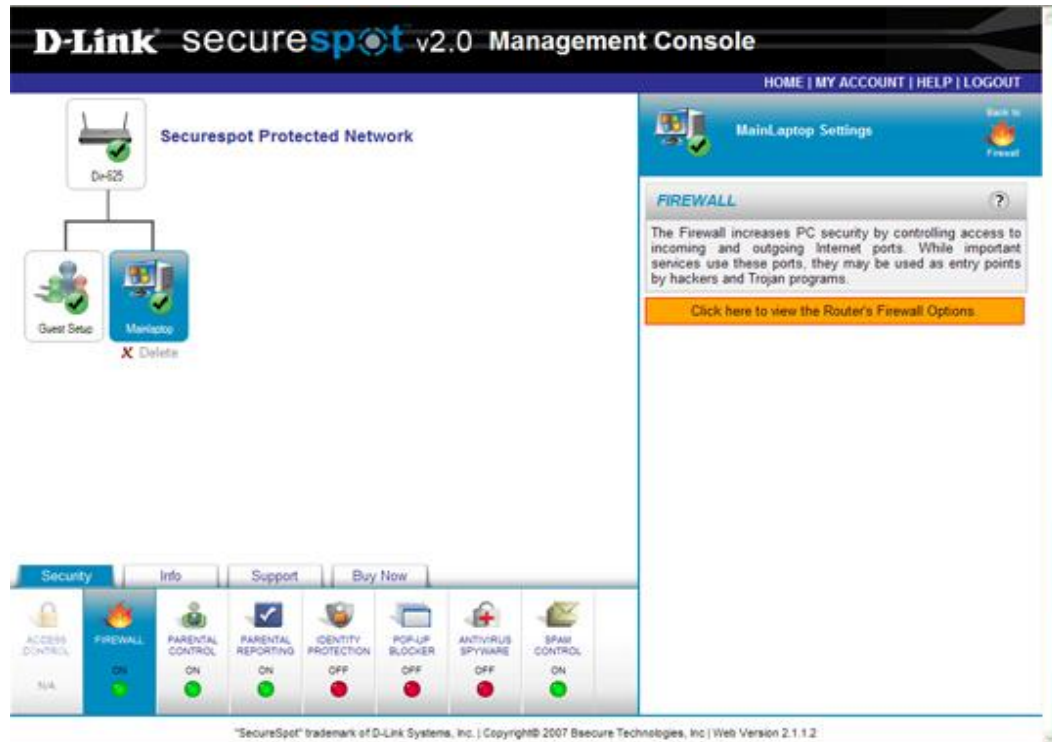
- Click the  icon to return to the Access Control Service panel without saving changes.
- To hide Guest Password details, click the  icon.


Firewall Page

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

To enable the Firewall:

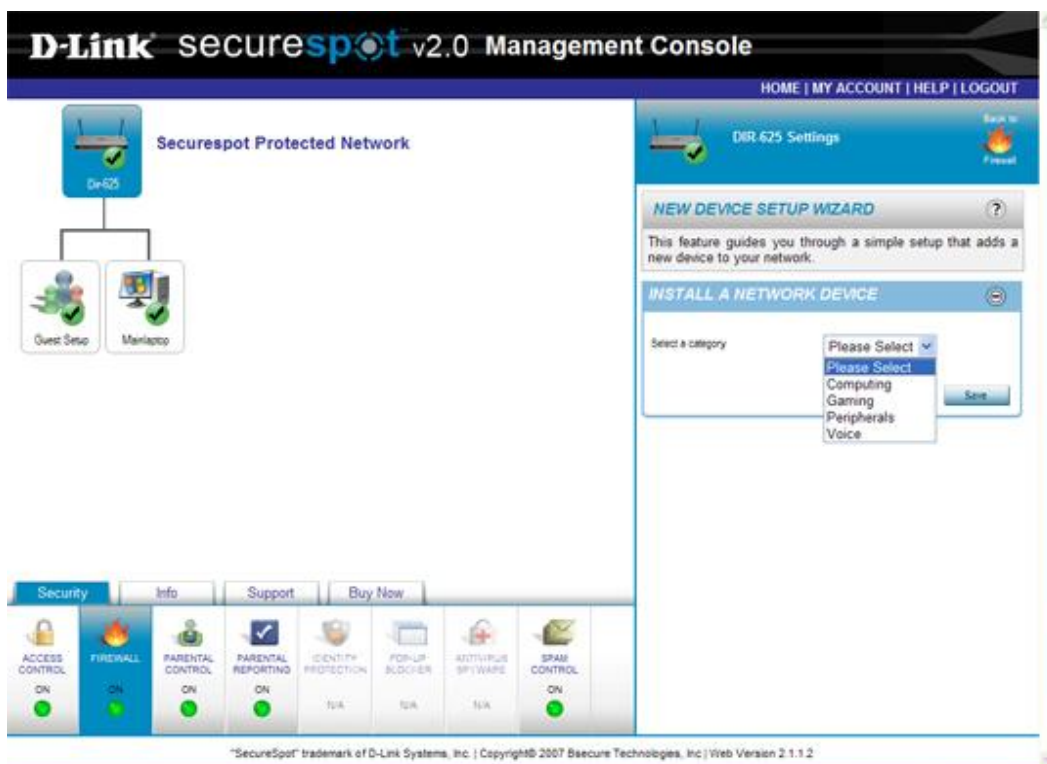
1. Select a specific device on the network map.
2. Click the **Firewall** service under the **Security** tab.



3. Click the  icon to hide/display descriptive Firewall information.
4. Click the **Router Firewall Options** orange button to view and/or change the **Router Firewall settings**. (The default is ON.)





5. To add a network device using the Device Setup Wizard, click the Install Network Device link on the Firewall Service panel.



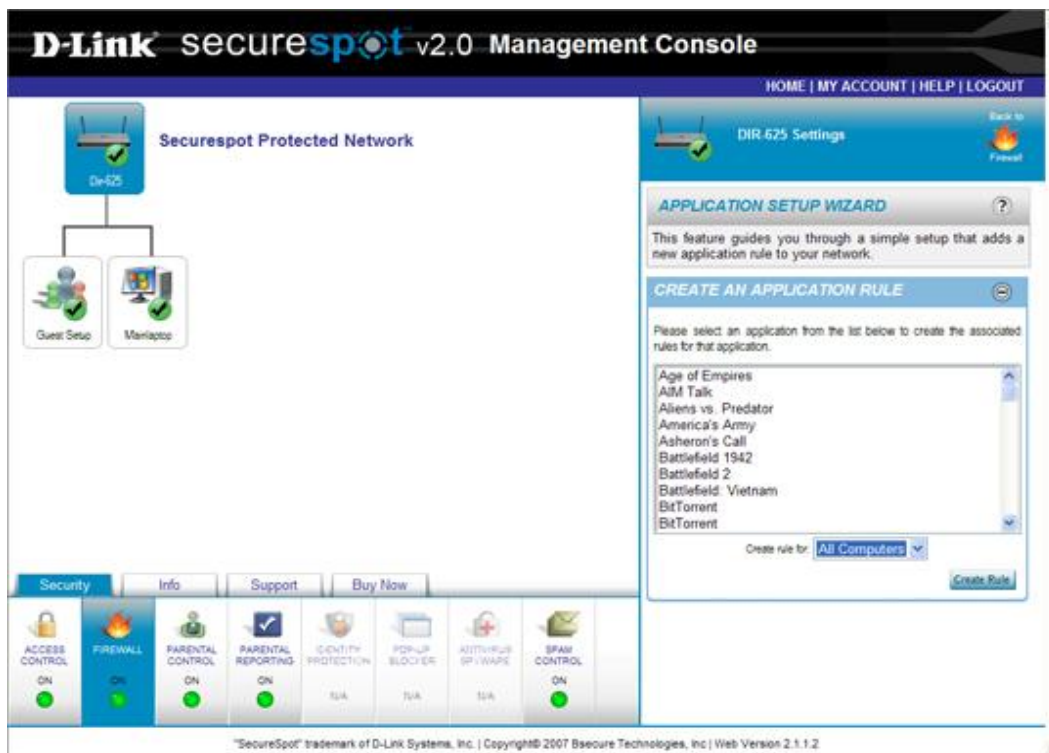
- Select a device in the **category** drop-down list box.

- Once you select a category, the Install a Network Device panel expands.
- Select the type and operating system and enter the appropriate **Device Name**, **MAC Address**, and **IP Address**.
- Click **Save** to save your settings.
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Network Device Install details, click the  icon.

6. To add a new application rule to your network, click the Install Network Application link on the Firewall Service panel.



- Select an application in the drop-down list box.
- Select a device in the **Create rule for** drop-down combo box that you want to create an Application rule.
- Click **Create Rule** to save your settings. (*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.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Application Rule details, click the  icon.

7. 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 Service panel.



To add a Virtual Server Rule:

- In the **Application Name** drop-down combo box, select the application and its associated ports and protocol that you want to allow access to your network or device.
- Select the « character to populate the appropriate Name, Ports, and Protocol for the selected application.

OR



- Enter the Name, Ports, and Protocol to create a new application server setting.
- In the **Computer Name** drop-down combo box, select the appropriate device that you want to allow access.
- Select the « character to populate the appropriate IP Address for the selected device.

OR


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

- In the **Schedule** drop-down combo box, select **Always** or a previously created schedule for which you want to allow Internet access.
- In the **Inbound Filter** drop-down combo box, 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.
- Select the **Enabled** check box if you want to enable the Virtual Server Rule on the router too.
- Click **Save** to save your settings. (*Once your settings have been saved, the message “Virtual Server Rule Created” appears on the Virtual Server panel, and the newly created Virtual Server Rule is added to the Virtual Servers List.*)
- If you changed the settings, click **Apply Settings**.


OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Server Settings or Virtual Servers List details, click the  icon.

To edit a Virtual Server Rule:



- Click the  icon to expand the **Virtual Servers List** panel.





- Select the  icon to edit a Virtual Server Rule. (*The previously-saved Virtual Server Rule input appears in the Server Settings panel.*)

- After changes have been made to the Virtual Server Rule, click the **Update** button on the Server Settings panel. (*The updated Virtual Server Rule is added to the Virtual Servers List.*)



OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Server Settings or Virtual Servers List details, click the  icon.

To delete a Virtual Server Rule:

- Click the  icon to expand the Virtual Servers List panel.
- Select the  icon beside the Virtual Server Rule that you want to delete.
- Once the Virtual Server Rule has been deleted, the message “Virtual Server Rule Removed” appears on the Virtual Server panel.
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Server Settings or Virtual Servers List details, click the  icon.

8. 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 Service panel.



To allow individual ports, mixed ports, or port ranges:

- In the **Application Name** drop-down combo box, select the application and its associated ports that you want to allow access to your network or device.
- Select the « character to populate the appropriate Name, TCP Ports, and UDP Ports for the selected application.

OR



- Type the Name, TCP Ports, and UDP Ports to create a new application server setting.
- In the **Computer Name** drop-down combo box, select the appropriate device that you want to allow access.
- Select the « character to populate the appropriate IP Address for the selected device.

OR

- Type the IP Address of the device that you want to allow ports or port ranges.
- In the **Schedule** drop-down combo box, select **Always** or a previously created schedule for which you want to allow Internet access.
- In the **Inbound Filter** drop-down combo box, 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.

- Select the **Enabled** check box if you want to enable the Port Forwarding Rule on the router too.
- Click **Save** to save your settings. (*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.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Server Settings or Ports List details, click the  icon.

To block individual ports, mixed ports, or port ranges:

- In the **Application Name** drop-down combo box, select the application and its associated ports that you want to block access to your network or device.
- Select the « character to populate the appropriate Name, TCP Ports, and UDP Ports for the selected application.

OR

- Type the Name, TCP Ports, and UDP Ports to create a new application server setting.
- In the **Computer Name** drop-down combo box, select the appropriate device that you want to allow access.
- Select the « character to populate the appropriate IP Address for the selected device.

OR

- Type the IP Address of the device that you want to allow ports or port ranges.
- In the **Schedule** drop-down combo box, select **Always** or a previously created schedule for which you want to allow Internet access.
- 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.
- Click **Save** to save your settings. (*Once your settings have been saved, the message “Port Forwarding Rule Created” appears on the Application Control panel, and the newly created Port Forwarding Rule is added to the Ports List.*)
- Select the **Enabled** check box if you want to enable the Port Forwarding Rule on the router too.

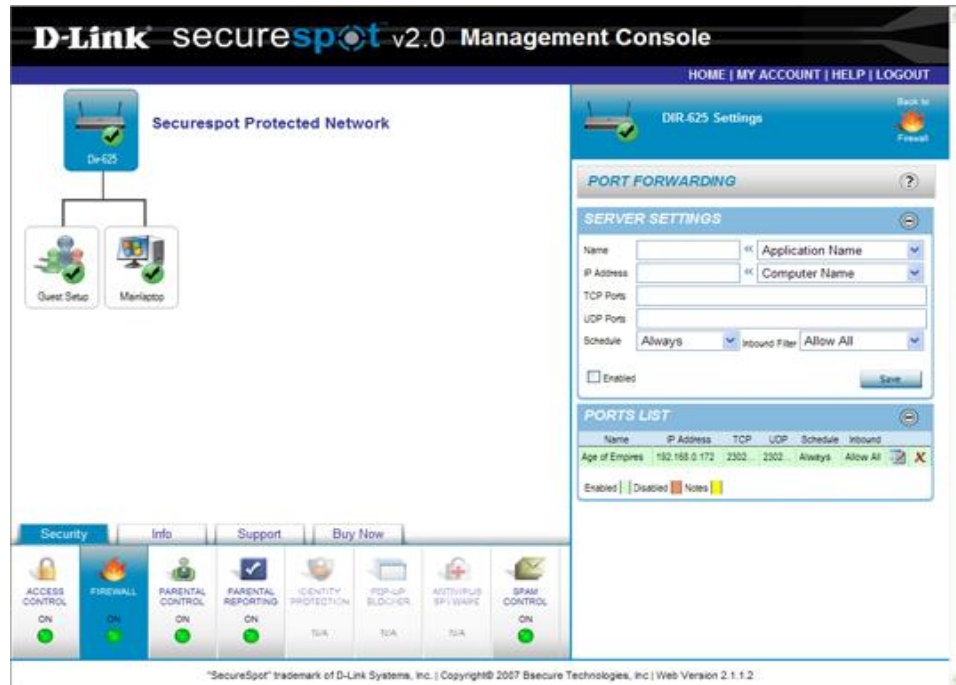
OR


- Click the  icon to return to the Firewall Service panel without saving any changes.

- To hide Server Settings or Ports List details, click the  icon.



To edit a Port Forwarding Rule:

- Click the  icon to expand the **Ports List** panel.





- Select the  icon to edit a Port Forwarding Rule. *(The previously-saved Port Forwarding Rule input appears in the Server Settings panel.)*
- After changes have been made to the Port Forwarding Rule, click the **Update** button on the Server Settings panel. *(The updated Port Forwarding Rule is added to the Ports List.)*



OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Applications List details, click the  icon.

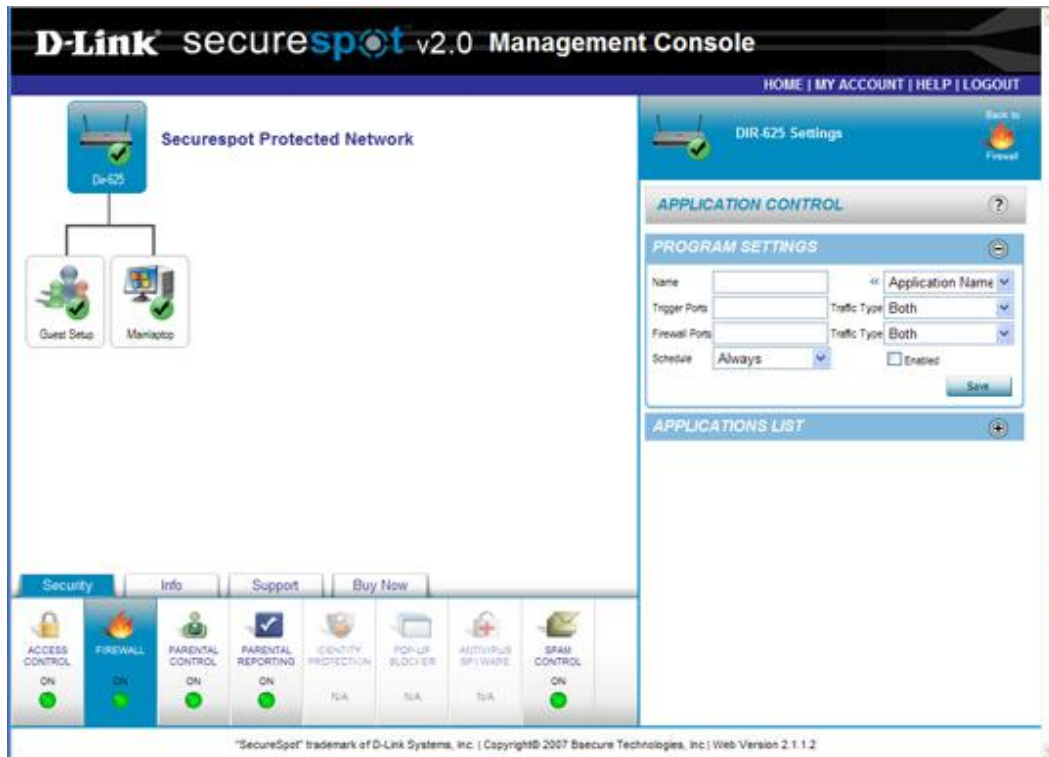
To delete a Port Forwarding Rule:

- Click the  icon to expand the Ports List panel.
- Select the  icon beside the Port Forwarding Rule that you want to delete.
- Once the Port Forwarding Rule has been deleted, the message “Port Forwarding Rule removed” appears on the Port Forwarding panel.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Server Settings or Ports List details, click the  icon.

9. 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 Service panel.



To allow applications:



- In the **Application Name** drop-down combo box, select the application that you want to allow access to your network.
- Select the « character to populate the appropriate Name, Trigger Ports, Firewall Ports, and Traffic Type inputs for the selected application.

OR

- Type the Name, Trigger Ports, and Firewall Ports, and then select the associated Traffic Types that you want to allow access to your network.
- In the **Schedule** drop-down combo box, select **Always** or a previously created schedule for which you want to allow this application.
- Select the **Enabled** check box if you want to enable the Applications Rule on the router too.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Application Rule Created" appears on the Application Control panel, and the newly created Application Rule is added to the Applications List.)

- If you changed the settings, click **Apply Settings**.



OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Program Settings or Application List details, click the  icon.

To block applications:

- In the **Application Name** drop-down combo box, select the application that you want to block access to your network.
- Select the « character to populate the appropriate Name, Trigger Ports, Firewall Ports, and Traffic Type inputs for the selected application.
- Type the Name, Trigger Ports, and Firewall Ports, and then select the associated Traffic Types that you want to block access to your network.
- In the **Schedule** drop-down combo box, select **Never** to block this application.
- Select the **Enabled** check box if you want to enable the Applications Rule on the router too.
- Click **Save** to save your settings. *(Once your settings have been saved, the message “Application Rule Created” appears on the Application Control panel, and the newly created Application Rule is added to the Applications List.)*
- If you changed the settings, click **Apply Settings**.


OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Program Settings or Application List details, click the  icon.



To edit an Application Rule:

- Click the  icon to expand the **Applications List** panel.





- Select the  icon to edit an Application Rule. (The previously-saved Application Rule input appears in the **Program Settings** panel.)
- After changes have been made to the Application Rule, click the **Update** button on the **Program Settings** panel. (The updated Application Rule is added to the Applications List.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Applications List details, click the  icon.

To delete an Application Rule:

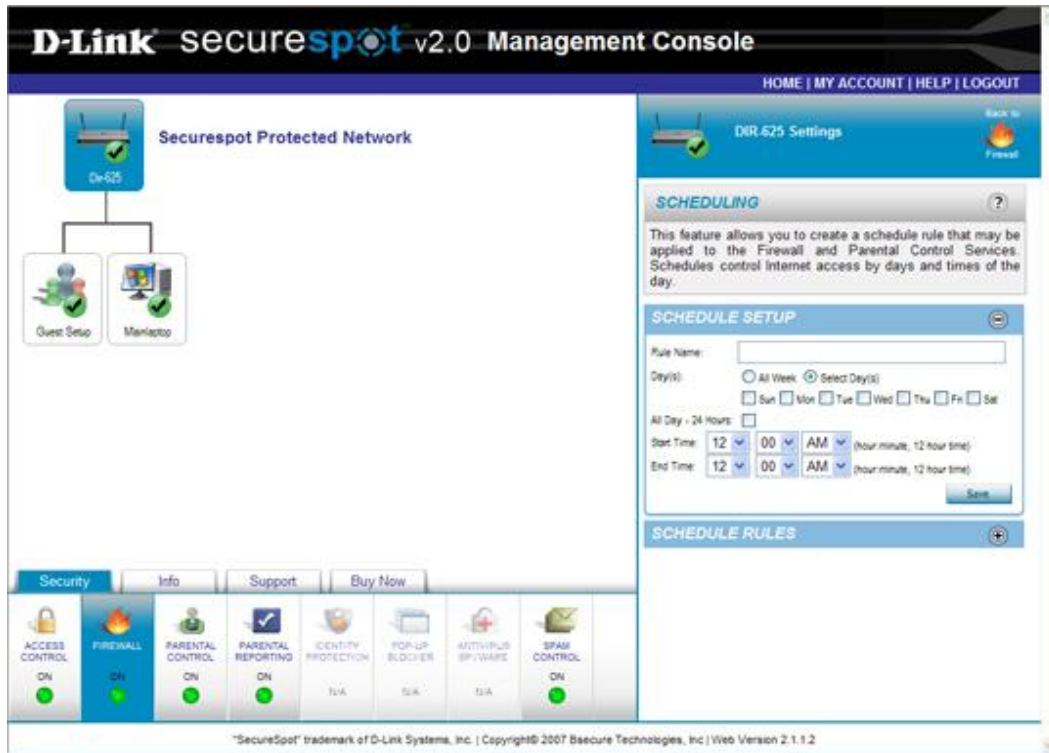
- Click the  icon to expand the Applications List panel.
- Select the  icon beside the Application Rule that you want to delete.
- Once the Application Rule has been deleted, the message “Application Rule removed” appears on the Scheduling panel.
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Firewall Service panel without saving any changes.

- To hide Program Settings or Application List details, click the  icon.

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





To create a Schedule:

- In the **RuleName** text box, type the name of the schedule that you want to create.
- Select the appropriate options for Days: **All Week** or **Select Day(s)**. *[If the **All Week** option button is selected, the individual day check boxes collapse (disappear).]*
- In the **Start** and **End Time** drop-down list boxes, select the appropriate time. *(Schedule times are hour and minute increments.)*

OR

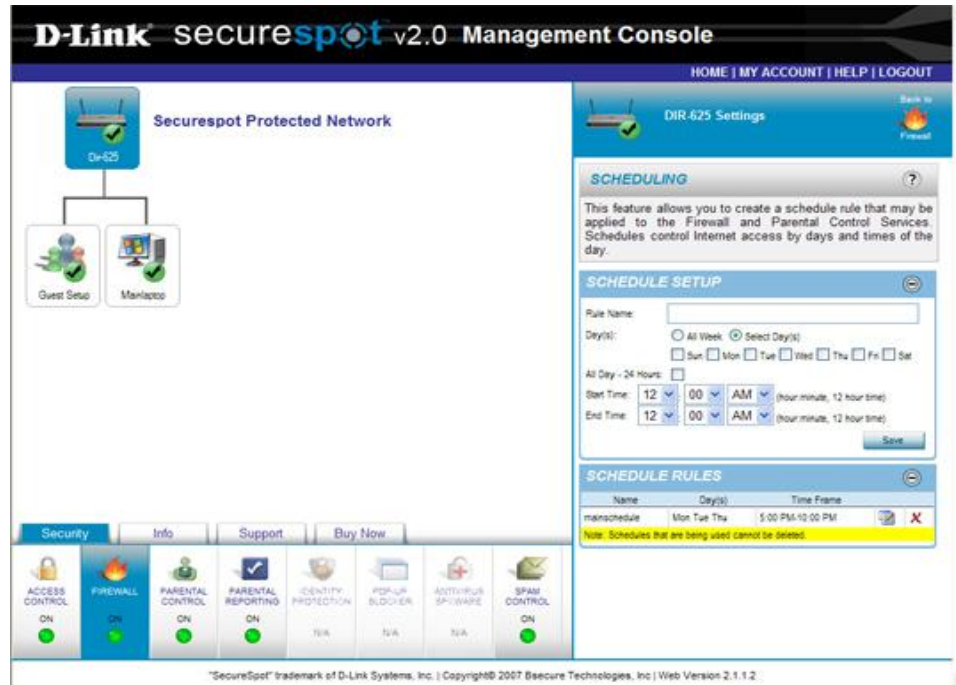
- Select the **All Day** check box if you want to block Internet Access for 24 hours. *[If the **All Day** check box is selected, the **Start** and **End Time** drop-down list boxes collapse (disappear).]*
- Click **Save** to save your settings. *(Once your settings have been saved, the message "Firewall Schedule Created" appears on the Scheduling panel, and the newly created schedule is added to the Schedules list.)*
- If you changed the settings, click **Apply Settings**.


OR

- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Controls details, click the  icon.

To edit a Schedule:

- Click the  icon to expand the **Schedule** panel.





- Select the  icon to edit a schedule. (*The previously-saved schedule input appears in the Controls panel.*)
- After changes have been made to the schedule, click the **Update** button on the Controls panel. (*The updated schedule is added to the Schedules list.*)
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Schedules details, click the  icon.

To delete a Schedule:

- Click the  icon to expand the Schedule panel.
- Select the  icon beside the schedule that you want to delete. (*Note that Schedules that are being used can not be deleted.*)

- Once the schedule has been deleted, the message “Firewall Schedule removed” appears on the Scheduling panel.
- If you changed the settings, click **Apply Settings**.

OR

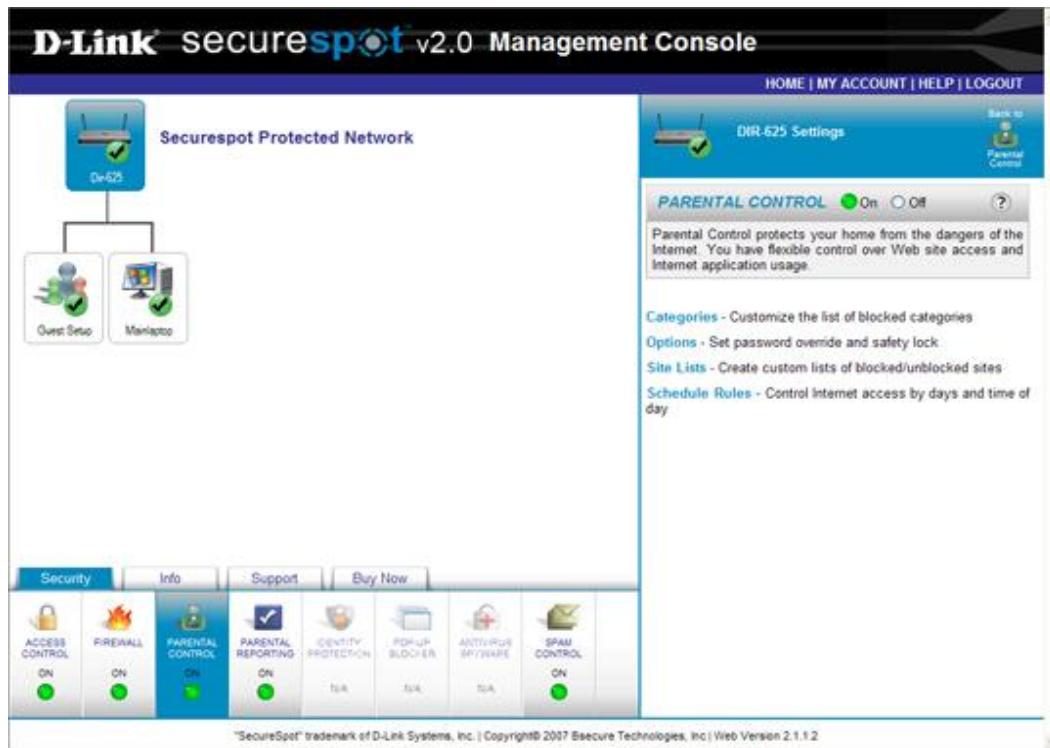
- Click the  icon to return to the Firewall Service panel without saving any changes.
- To hide Schedules details, click the  icon.


Parental Control Service

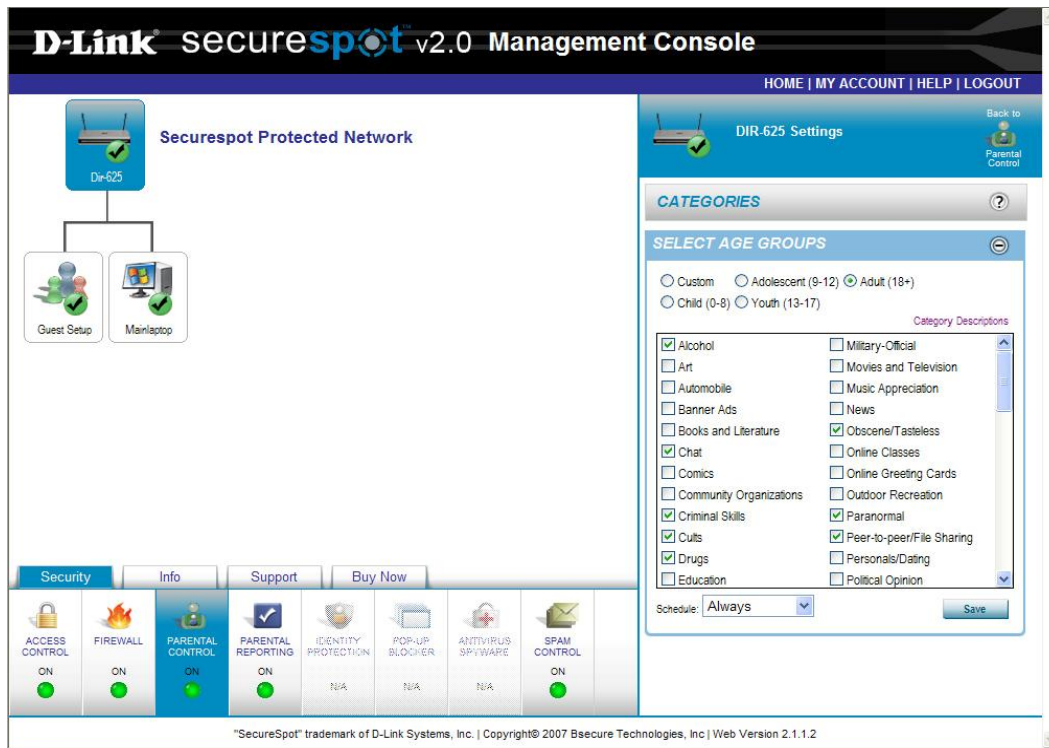
This feature protects your home from dangers of the Internet, while giving you flexible control over Web sites and Internet application usage.



To adjust parental controls:

1. Select a specific device on the network map.
2. Click the **Parental Control** service under the **Security** tab.

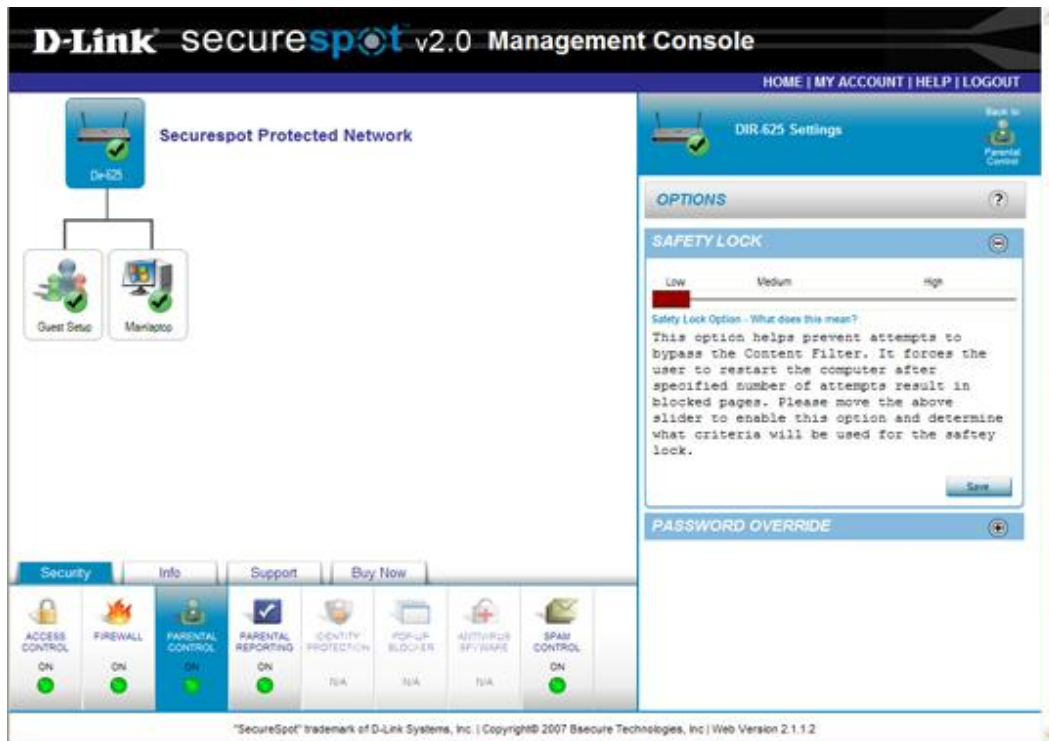


3. Click the  icon to hide/display descriptive Parental Control information.
4. Select the **ON** option button to enable the Parental Control service. (*The default is ON.*)
5. To customize the list of default blocked categories, click the **Categories** link on the Parental Controls Service panel. This feature facilitates more explicit content filtering through Web site category blocking and unblocking.



- In the Select Age Groups panel, select one of the age groups: **Custom**, **Child (0 – 8)**, **Adolescent (9 – 12)**, **Youth (13 – 17)**, or **Adult (18+)**.
- In the **Schedule** drop-down list box, select one of the schedule options: **Always**, **Never**, or a newly created schedule. (Select the **Scheduling** link under the Parental Control or Firewall Service panels to create a customized schedule.)
- Select the listed Web site categories check boxes that you want the filter to block. (**Note: If you clear the Child Porn category, a warning message appears on the screen.**) Clear any Web site categories that you do not want the filter to block.
- Click **Save** to save your settings. (Once your settings have been saved, the message “Parental Control Categories saved” appears on the Categories panel.)
- If you changed the settings, click **Apply Settings**.
- OR
- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Categories details, click the  icon.



6. To enable or disable the content filtering and password override, click the **Options** link on the Parental Controls Service panel. The **Safety Lock Option** is used to protect against users accessing multiple blocked sites. Additionally, **Status/Password Override** feature allows you to override the existing password with associated individual blocked sites with a new password.




To modify the Safety Lock option:

- Click and hold the slide control button, and then move the button to the desired safety lock setting. Release the slide control button, and then click it one more time. This will set the slide control button. *(The information beneath the slide control will change as you move the button to reveal the current setting.)*
- Click **Save** to save your settings. *(Once your settings have been saved, the message "Parental Control Options saved" appears on the Options Feature panel.)*
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Safety Lock details, click the  icon.



To modify the Status/Password Override option:

- Click the  icon to expand the **Password Override** panel.

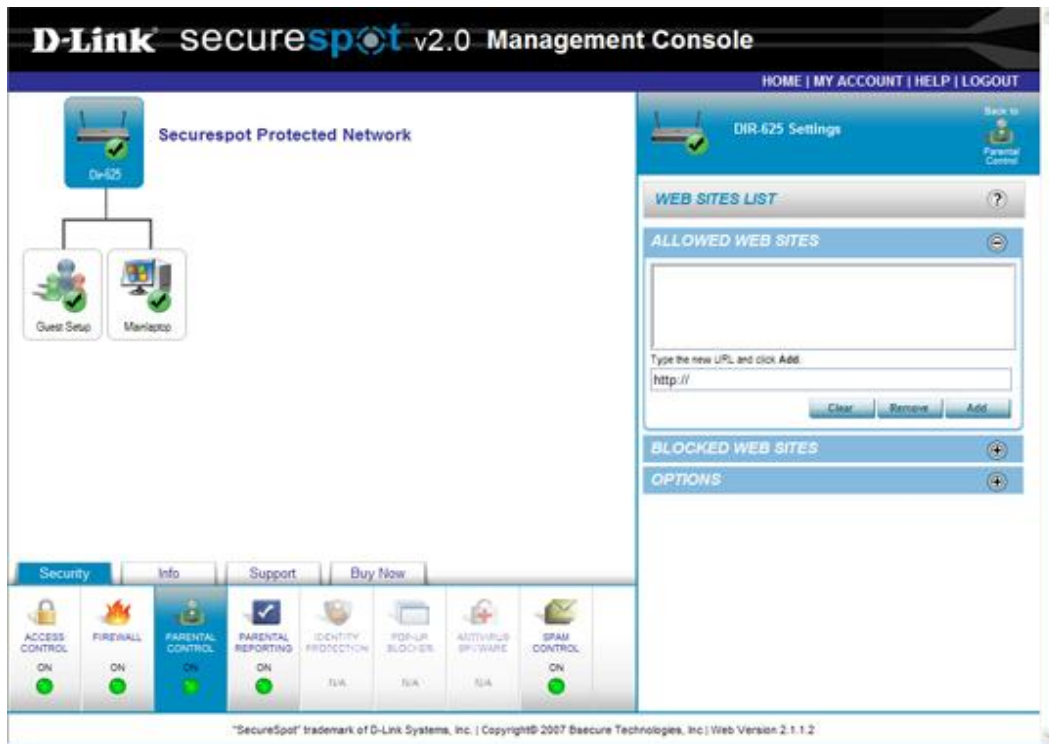


- To enable password override, select the **Enable Password Override** check box.
- Click **Save** to save your settings. (Once your settings have been saved, the message "Parental Control Options saved" appears on the Options Feature panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Password Override details, click the  icon.



7. To create customized lists of blocked/unblocked Web sites, click the **Site Lists** link on the Parental Controls Service panel. This feature enables you to block or allow specific Web sites by URL and create *white* lists if desired to control content filtering more specifically.



To create Allowed Web Sites List:


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

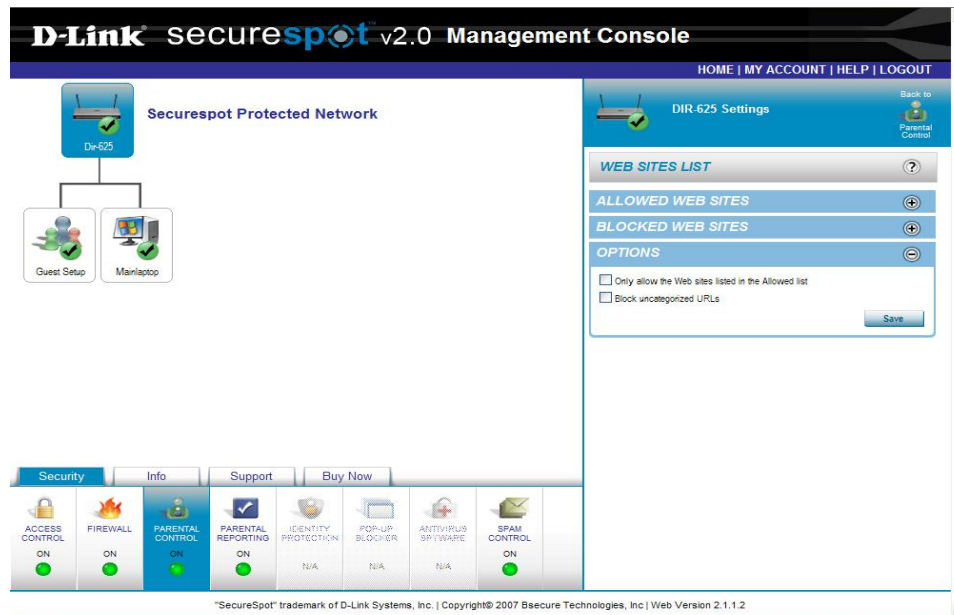
OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Allowed Web Sites details, click the  icon.

To create a White List:



- In the **Allowed Web Sites** List, type the URL of the Web site that you want to allow in the text box.
- Click **Add**. (*The Web site is added to the **Allowed Web Sites** List.*)
- Repeat the previous two steps to add additional Web sites to your **Allowed Web Sites** List.

- Click the  icon to expand the **Options** panel.




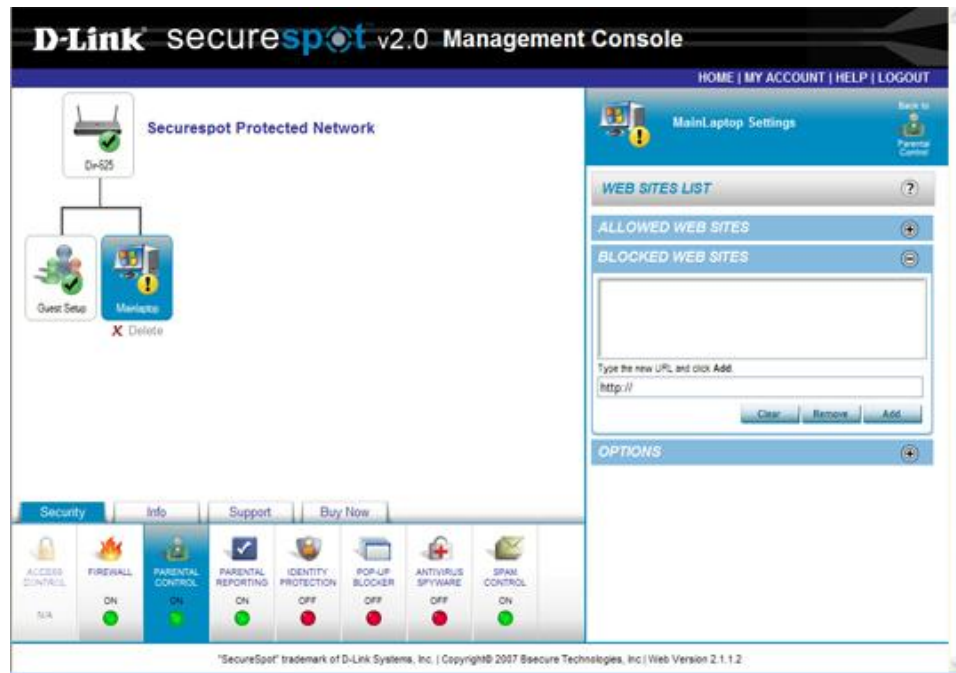
- Select the **Only Allow the Web sites listed in the Allowed list** check box. (*This will block access to all Web sites with the exception of those specified on the **Allowed Web Sites** list.*)
- Click **Save** to save your settings. (*Once your settings have been saved, the message "Parental Control Web Site Lists saved" appears on the Web Sites List panel.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Options details, click the  icon.



To create Blocked Web Sites List:

- Click the  icon to expand the Blocked Web Sites panel.
- In the provided text box, type the URL of a Web site that you want to block.
- Click **Add**. (*The Web site is added to the **Blocked Web Sites** List.*)




- Repeat the previous two steps to add additional Web sites to your **Blocked Web Sites** List. (Once your settings have been saved, the message "Parental Control Web Site Lists saved" appears on the Web Sites List panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Blocked Web Sites details, click the  icon.


To edit the Allowed and Blocked Web Site Lists:


- Click the  icon to expand the list that you want to edit: **Allowed Web sites** or **Blocked Web Sites**.
- To remove a single entry from a list, click (highlight) the Web site entry and click **Remove**. (The Web site is removed from the appropriate list.)

OR

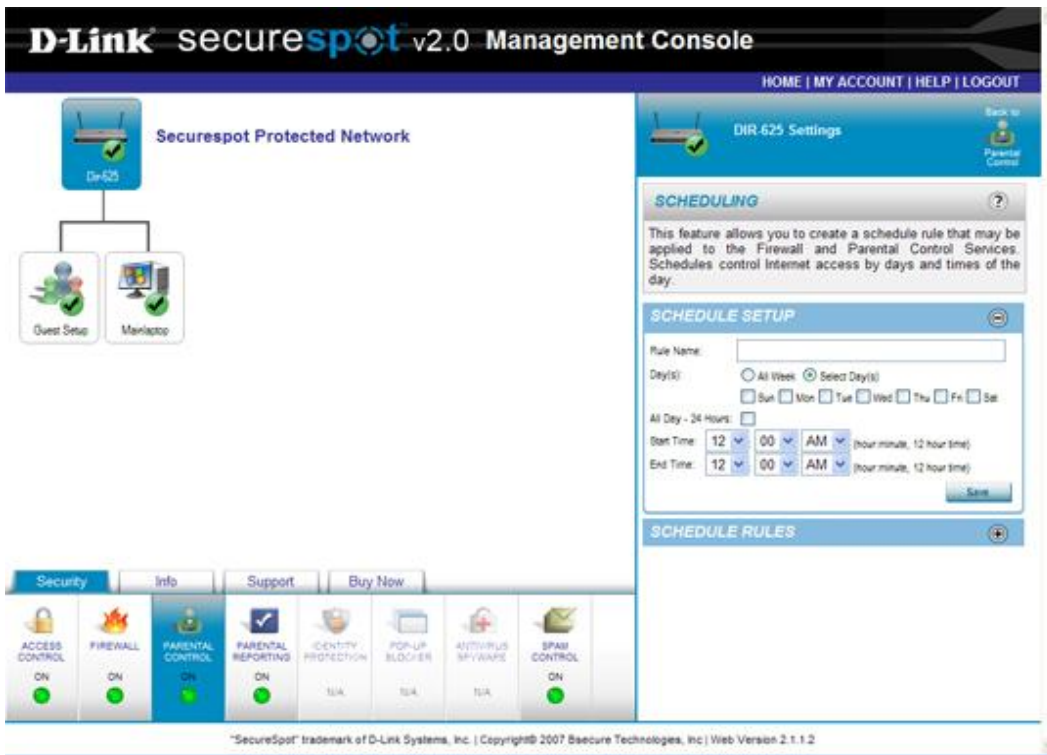
- To remove several entries from a list, click (highlight) the Web site entries and click **Clear**. (All entries are removed from the appropriate list.)

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.

- To hide Allowed and/or Blocked Web Sites details, click the  icon.

8. To control Internet access, click the Schedule Rules 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:

- In the **Rule Name** text box, type the name of the schedule that you want to create.
- Select the appropriate options for Days: **All Week** or **Select Day(s)**. *[If the **All Week** option button is selected, the individual day check boxes collapse (disappear).]*
- In the **Start** and **End Time** drop-down list boxes, select the appropriate time. *(Schedule times are hour and minute increments.)*

OR

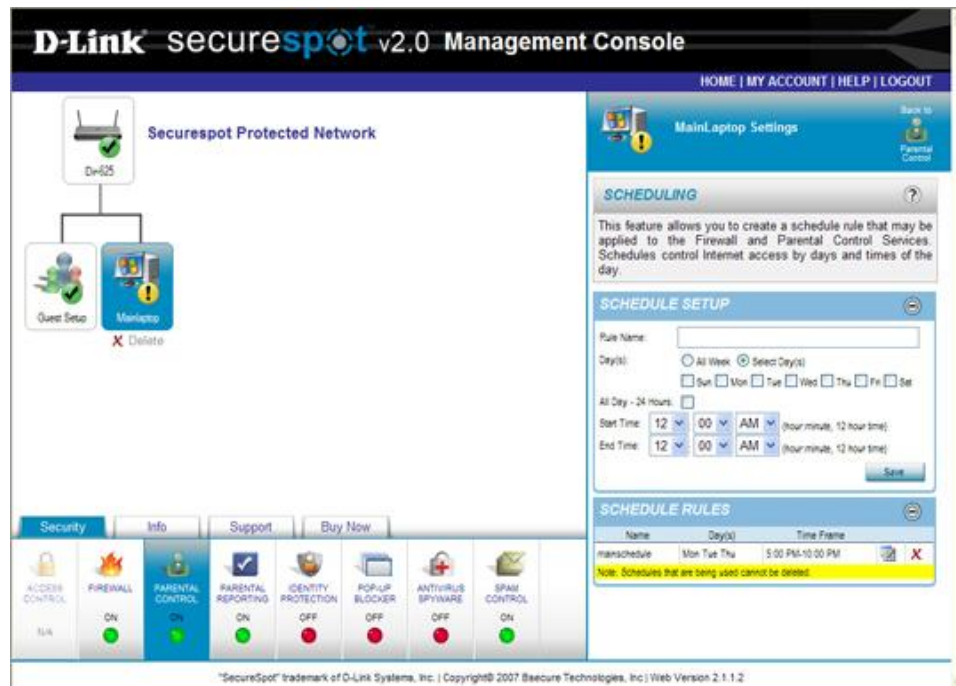
- Select the **All Day** check box if you want to block Internet Access for 24 hours. *[If the **All Day** check box is selected, the **Start** and **End Time** drop-down list boxes collapse (disappear).]*
- Click **Save** to save your settings. *(Once your settings have been saved, the message "Firewall Schedule Created" appears on the Scheduling panel, and the newly created schedule is added to the Schedules list.)*
- If you changed the settings, click **Apply Settings**.


OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Controls details, click the  icon.



To edit a Schedule:

- Click the  icon to expand the **Schedule** panel.




- Select the  icon to edit a schedule. (*The previously-saved schedule input appears in the Controls panel.*)
- After changes have been made to the schedule, click the **Update** button on the Controls panel. (*The updated schedule is added to the Schedules list.*)
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Schedules details, click the  icon.

To delete a Schedule:

- Click the  icon to expand the Schedule panel.

- Select the  icon beside the schedule that you want to delete. (*Note that Schedules that are being used can not be deleted.*)
- Once the schedule has been deleted, the message “Firewall Schedule removed” appears on the Scheduling panel.
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Parental Control Service panel without saving any changes.
- To hide Schedules details, click the  icon.

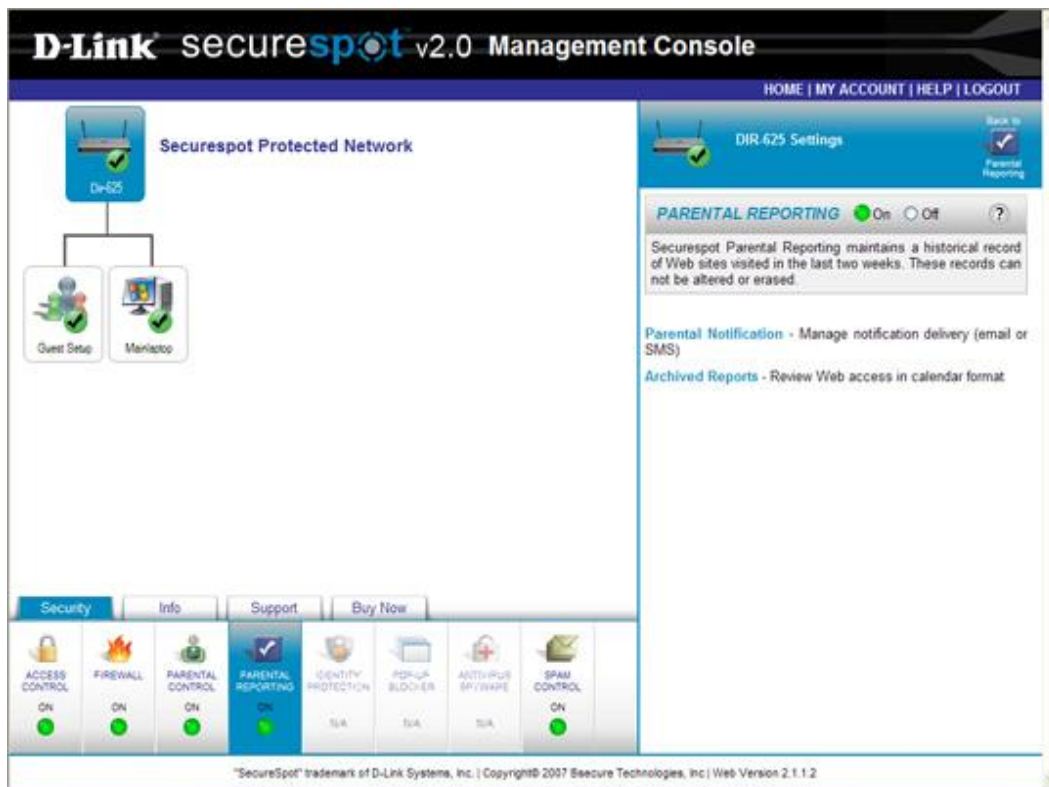
Parental Reporting Service


The Parental Reporting feature creates a historical record of the Web sites that can not 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. Currently, the Beta release is not able to send alerts for all categories. (*Note that it will only sends alerts when a user attempts to access a pornography or R-rated Web site.*)

To enable Reports:

1. Select a specific device on the network map.
2. Click the **Reporting** service under the **Security** tab.





3. Click the  icon to hide/display descriptive Reporting information.
4. Select the **ON** option button to enable the Reporting service. (*The default is ON.*)
5. To enable Parental Notification via e-mail and/or SMS notification alerts, click the **Parental Notification** link on the Parental Reporting Service panel.



To add Parental Notification via e-mail alerts:

- Select the On option button to enable the Parental Notification service.
- Enter an e-mail address in the text box and click Add. (Once your settings have been saved, the message "Parental Notification settings saved" appears on the Parental Notification Feature panel.)
- If you changed the settings, click **Apply Settings**.

OR


- Click the  icon to return to the Parental Reporting Service panel without saving any changes.
- To hide E-mail Addresses details, click the  icon.

To stop an E-mail Address from receiving alerts:

- Select the e-mail address in the list that you want to remove, and then click **Remove**. (Once your settings have been saved, the message "Parental Notification settings saved" appears on the Parental Notification Feature panel.)
- If you changed the settings, click **Apply Settings**.




OR

- Click the  icon to return to the Reporting Service panel without saving any changes.

- To hide E-mail Addresses details, click the  icon.





To add Parental Notification via SMS notification alerts:

- Select the **On** option button to enable the Parental Notification service.
- Click the  icon to expand the Mobile Devices panel.
- Enter a SMS number in the text box and click **Add**. (Once your settings have been saved, the message "Parental Notification settings saved" appears on the Parental Notification Feature panel.)
- If you changed the settings, click **Apply Settings**.
- Click the  icon to return to the Reporting Service panel without saving any changes.
- To hide Mobile Devices details, click the  icon.

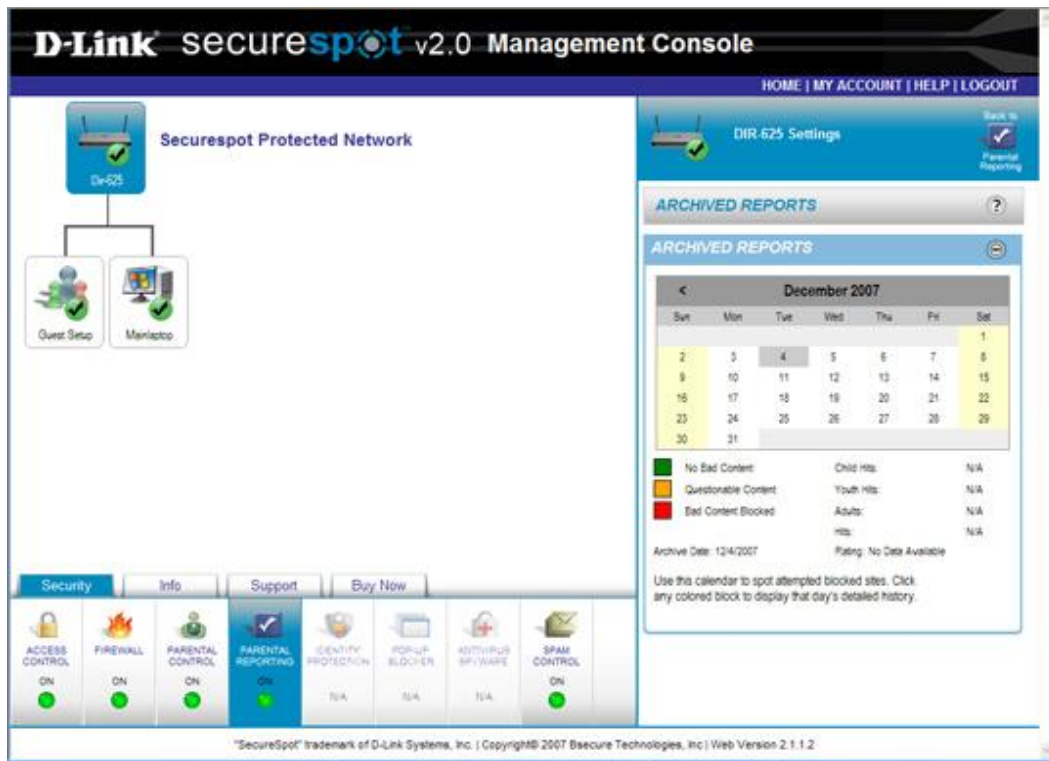
To stop a SMS number from receiving alerts:

- Select a SMS number in the list, and then click **Remove**. (Once your settings have been saved, the message "Parental Notification settings saved" appears on the Parental Notification Feature panel.)
- If you changed the settings, click **Apply Settings**.

OR



- Click the  icon to return to the Reporting Service panel without saving any changes.
- To hide Mobile Devices details, click the  icon.

6. To view a report, click the **Archived Reports** link on the Parental Reporting Service panel. This report includes the **Profile**, **Page**, **Category**, **Hits**, and **Age Group**.



- Click any colored block to view that day's detailed history.

OR

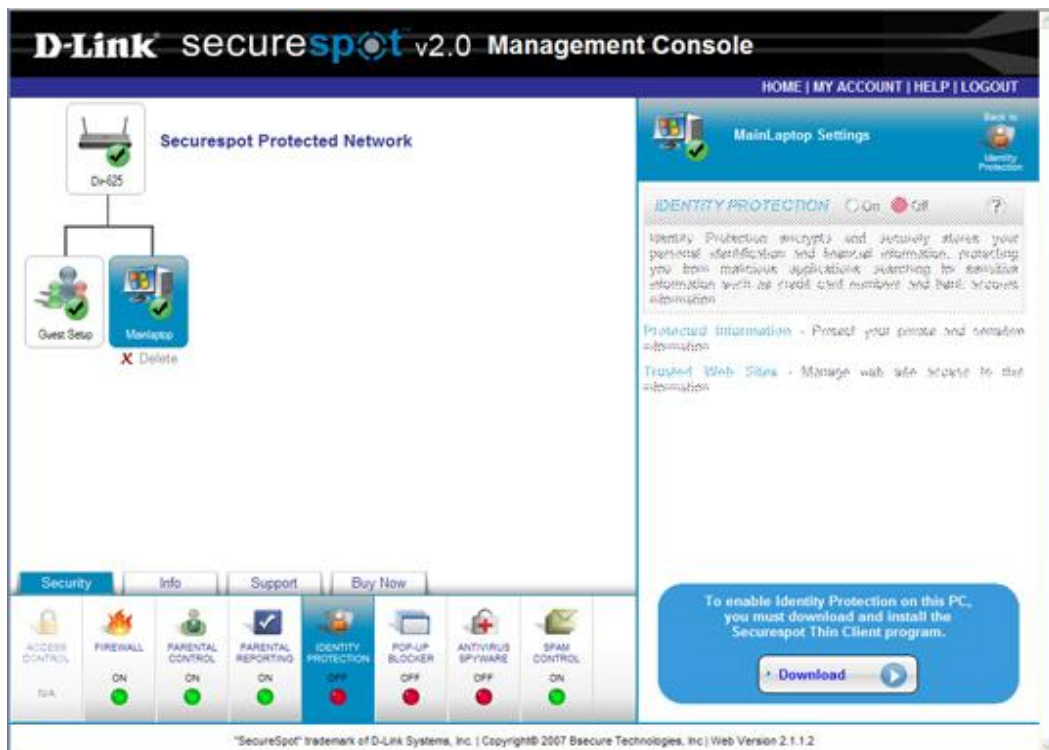
- Click the  icon to return to the Parental Reporting Service panel without saving changes.
- To hide Archived Reports details, click the  icon.

Identity Protection Page

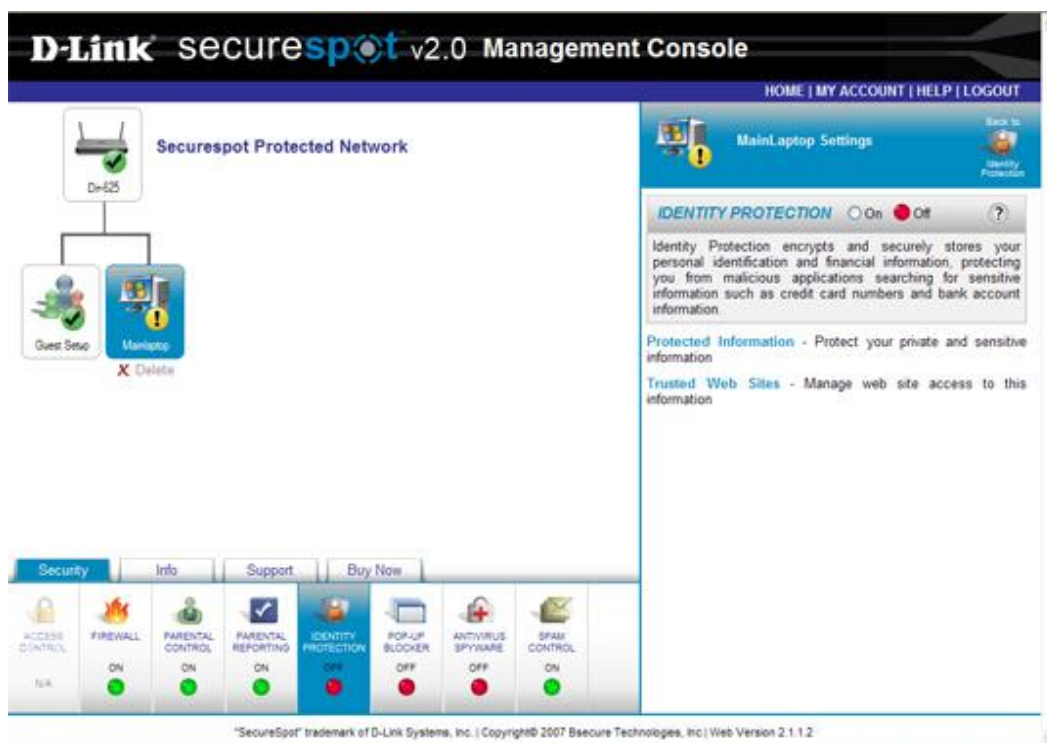
The Identity Protection Page allows you to enter private information [e.g., Social Security Number (SSN), credit card numbers, bank account numbers, etc.] and prevent this information from being transmitted from your computer(s). For example, if a user attempts to send an online form containing their SSN, they will receive a prompt notifying them of the fact that their correspondence contains private information and ask them to verify that they want to send this information.


To activate Identity Protection:

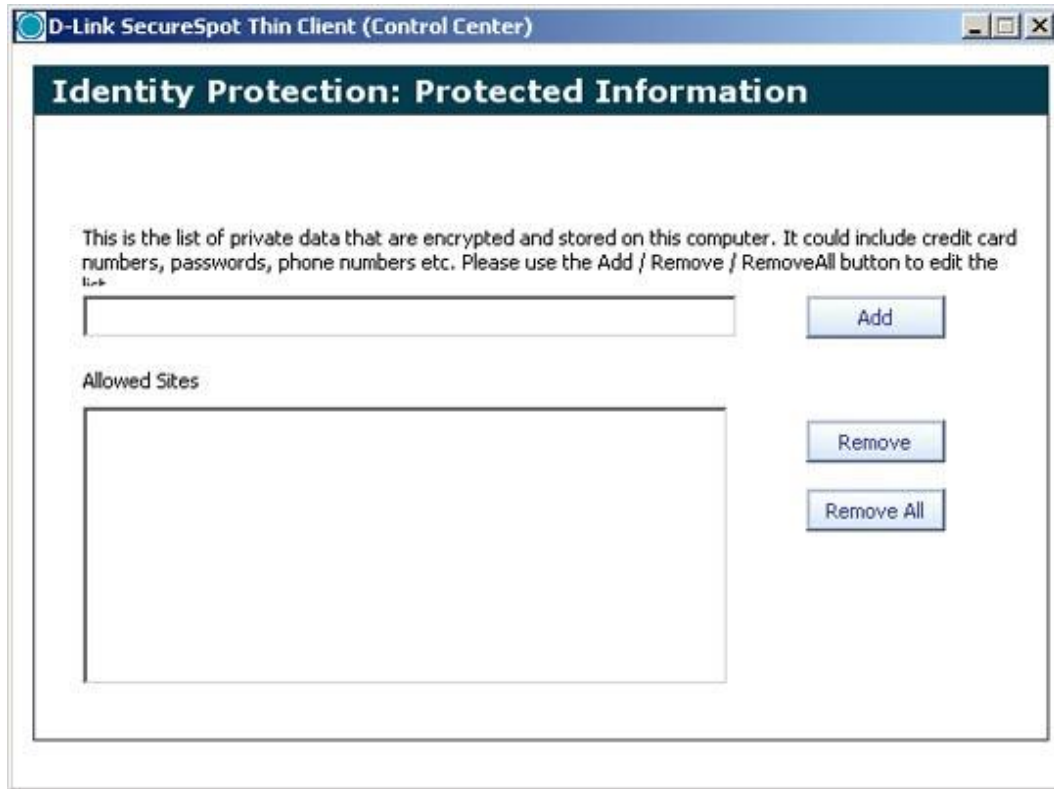
1. Select a PC on the network map.
2. Click the **Identity Protection** service under the **Security** tab.



3. To enable the Identity Protection service on the selected PC, click **Download** at the bottom of the Identity Protection Service panel to download the Thin-Client application.
4. A **File Download** pop-up window will appear on your screen prompting you to Run or Save the *SecurespotClient.exe* file. Click **Run**.
5. After *SecurespotClient.exe* has been successfully downloaded, you will be prompted to automatically RESTART your computer.
6. After you have downloaded the Thin-Client program and restarted your computer, a **Securespot Program Setup** pop-up window will appear on your screen. The Securespot Thin-Client program will now download the latest virus definition files to your PC.
7. Launch Securespot Security Services and select a PC on the network map.
8. Click the Identity Protection service under the **Security** tab.



9. Click the  icon to hide/display descriptive Identity Protection information.
10. Select the **ON** option button to enable the Identity Protection service. (*The default is OFF.*)
11. To protect your private information, click the Protected Information link on the Identity Protection home page.

**To add private information to the protect list:**

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

To delete private information from the protect list:

- In the list of protect information, select the data that you want removed from the list.
- Click **Remove**. (*The information is removed from the protect list.*)

OR

- Click **Remove All** to delete ALL private information from the protect list.

12. 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 home page.

**To add a Web site to the protection list:**

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

To delete a Web site from the protection allow list:

- In the allow list, select the address that you want removed from the list.
- Click **Remove**. (*The information is removed from the allow list.*)

OR

- Click **Remove All** to delete ALL Web sites from the protection allow list.

Pop-up Blocker Service

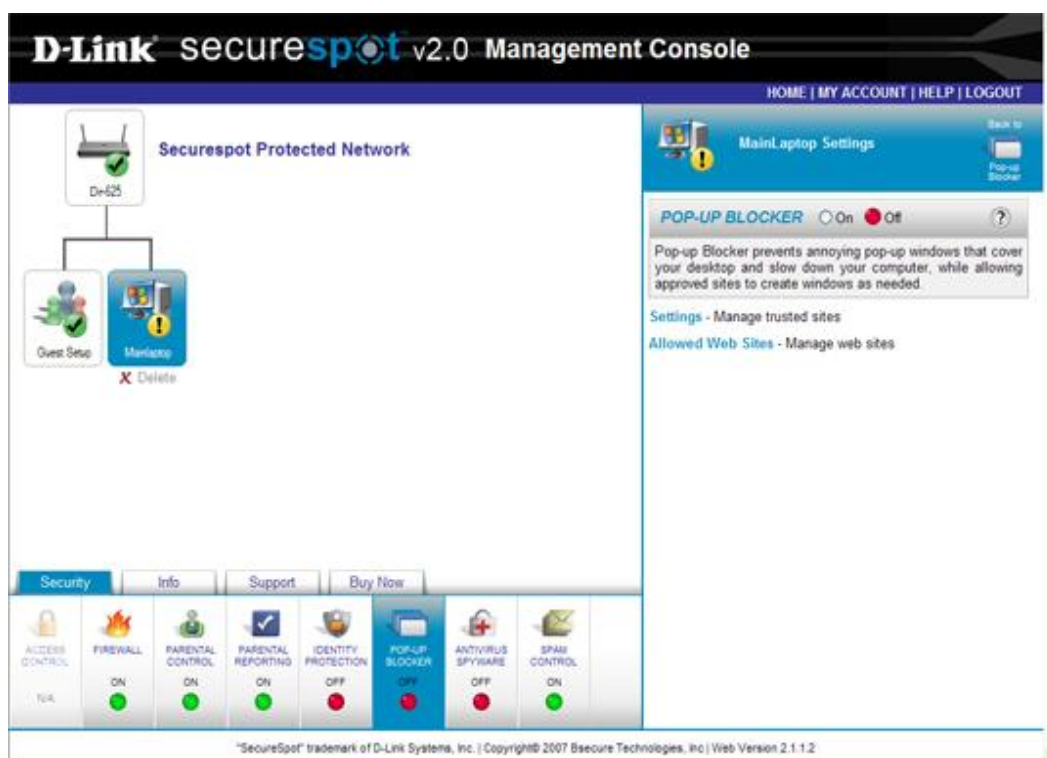
This feature blocks annoying pop-up windows that slow down your computer and cover up your desktop, while allowing approved sites to create pop-up windows as needed.


To enable the Pop-up Blocker:

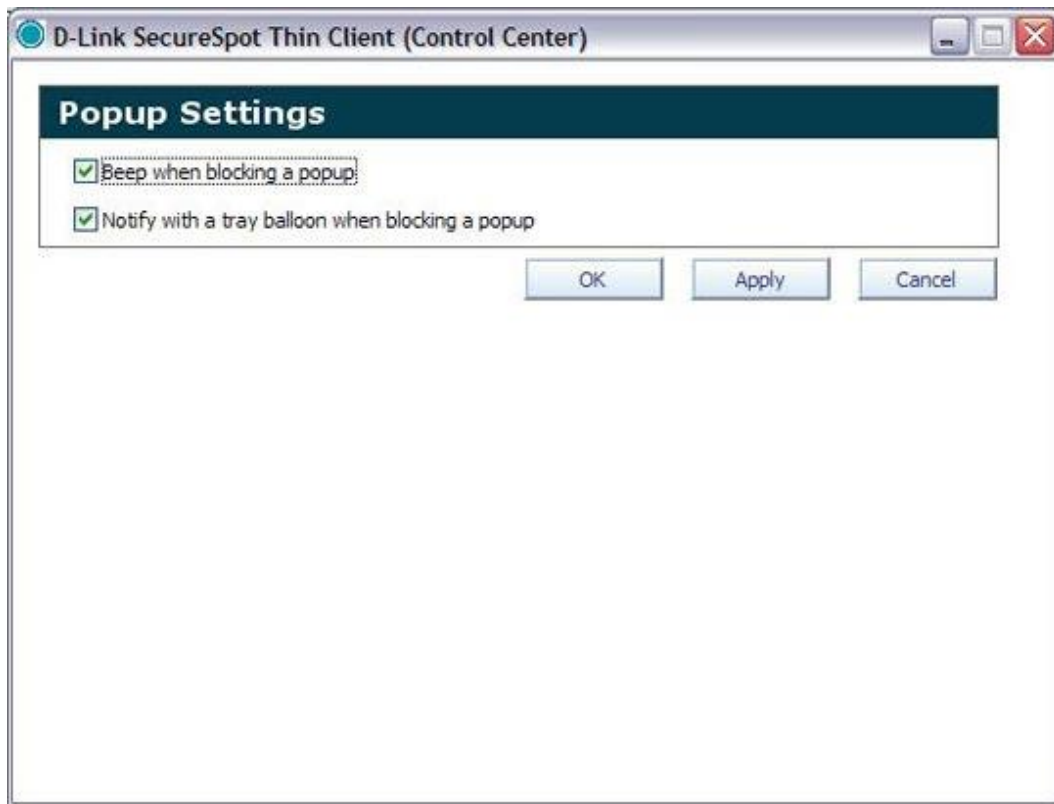
1. Select a PC on the network map.
2. Click the **Pop-up Blocker** service under the **Security** tab.



3. To enable the Pop-up Blocker service on the selected PC, click **Download** at the bottom of the Pop-up Blocker Service panel to download the Thin-Client application.
4. A **File Download** pop-up window will appear on your screen prompting you to Run or Save the *SecurespotClient.exe* file. Click **Run**.
5. After *SecurespotClient.exe* has been successfully downloaded, you will be prompted to automatically RESTART your computer.
6. After you have downloaded the Thin-Client program and restarted your computer, a **Securespot Program Setup** pop-up window will appear on your screen. The Securespot Thin-Client program will now download the latest virus definition files to your PC.
7. Launch Securespot Security Services and select a PC on the network map.
8. Click the Pop-up Blocker service under the **Security** tab.



9. Click the  icon to hide/display descriptive Pop-up Blocker information.
10. Select the **ON** option button to enable the Pop-up Blocker service. (*The default is OFF.*)
11. To control pop-up settings, click the **Settings** link on the Pop-up Blocker Service panel.



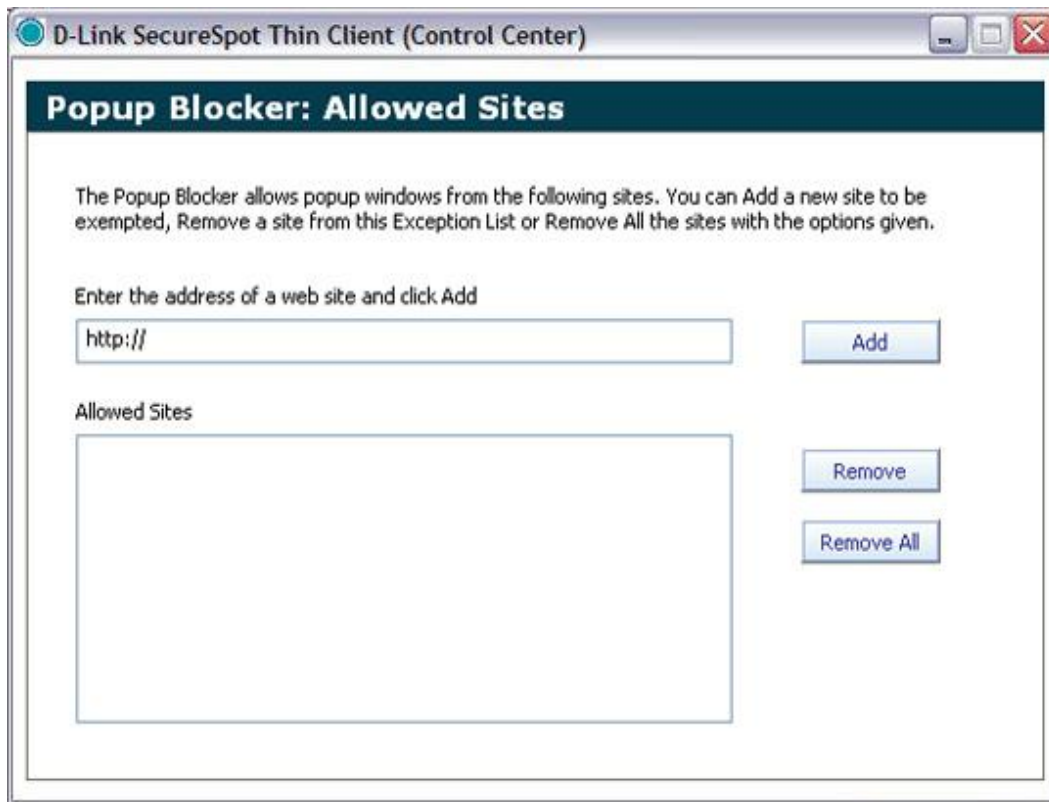
To adjust pop-up notification settings:

- Check the box next to the notification features you want to activate.
- Click **Apply**, and then **OK** to save your settings. This will return you to the Popup Blocker Options home page.

OR

- Click **Cancel** to return to the Popup Blocker Options home page without saving changes.

12. To create a list of Web sites from which you want to allow pop-up windows, click the **Allowed Web Sites** link on the Popup Block Service 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., your Internet banking Web site, mortgage company Web site, 401 Benefits, etc.)*



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

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

- From the Allowed Sites list, select the Web site address that you want to remove from the Allowed List.
- Click **Remove**.

OR

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

AntiVirus/Spyware Service

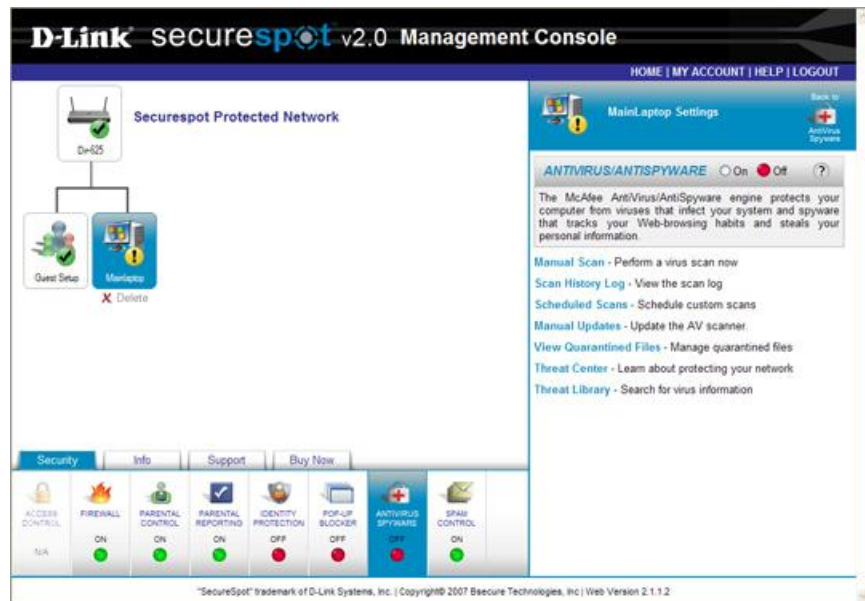
This feature protects your computer from viruses that infect your system and spyware that steals your personal information and tracks your Web-browsing habits and steals your personal information.


To enable AntiVirus/Spyware:

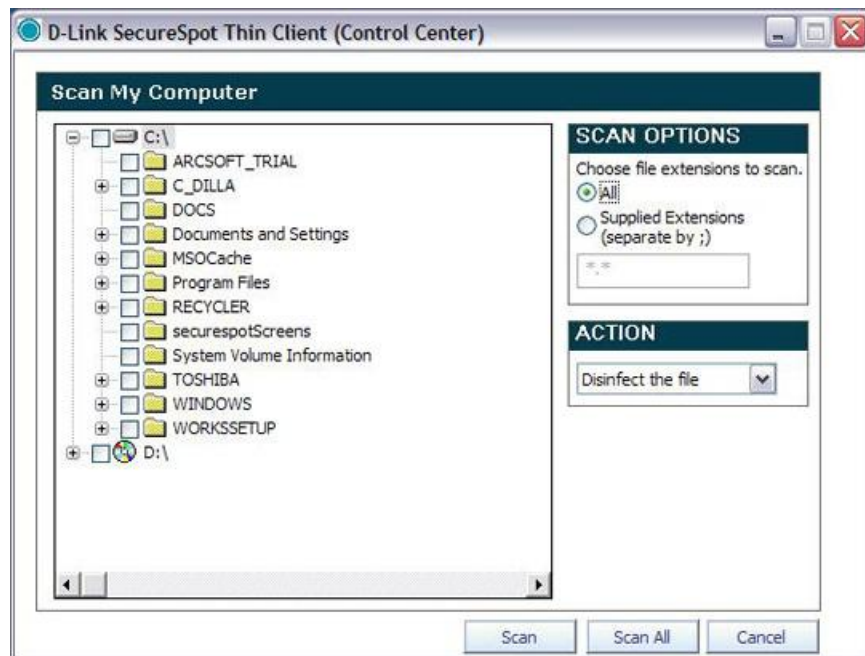
1. Select a PC on the network map.
2. Click the **AntiVirus/Spyware** service under the **Security** tab.



3. To enable the AntiVirus/Spyware service on the selected PC, click **Download** at the bottom of the AntiVirus/Spyware Service panel to download the Thin-Client application.
4. A **File Download** pop-up window will appear on your screen prompting you to Run or Save the *SecurespotClient.exe* file. Click **Run**.
5. After *SecurespotClient.exe* has been successfully downloaded, you will be prompted to automatically RESTART your computer.
6. After you have downloaded the Thin-Client program and restarted your computer, a **Securespot Program Setup** pop-up window will appear on your screen. The Securespot Thin-Client program will now download the latest virus definition files to your PC.
7. Launch Securespot Security Services and select a PC on the network map.
8. Click the AntiVirus/Spyware service under the **Security** tab.



9. Click the  icon to hide/display descriptive AntiVirus/Spyware information.
10. Select the **ON** option button to enable the Virus/Spyware Protection service. (*The default is OFF.*)
11. To perform a manual virus scan on your computer for viruses and spyware, click the **Manual Scan** link on the AntiVirus/Spyware home page. (*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.*)



To perform a manual virus scan:

- To choose a specific folder to scan, select the check box next to the folder that you wish to scan. Additionally, you can view deeper subfolders by clicking the plus signs (expand icons) to the left of the check boxes. Click the minus sinus (collapse icons) to close the folder again.
- To select CERTAIN types of scanned files, select the **Supplied Extensions** option button in the **Scan Options** dialog box.

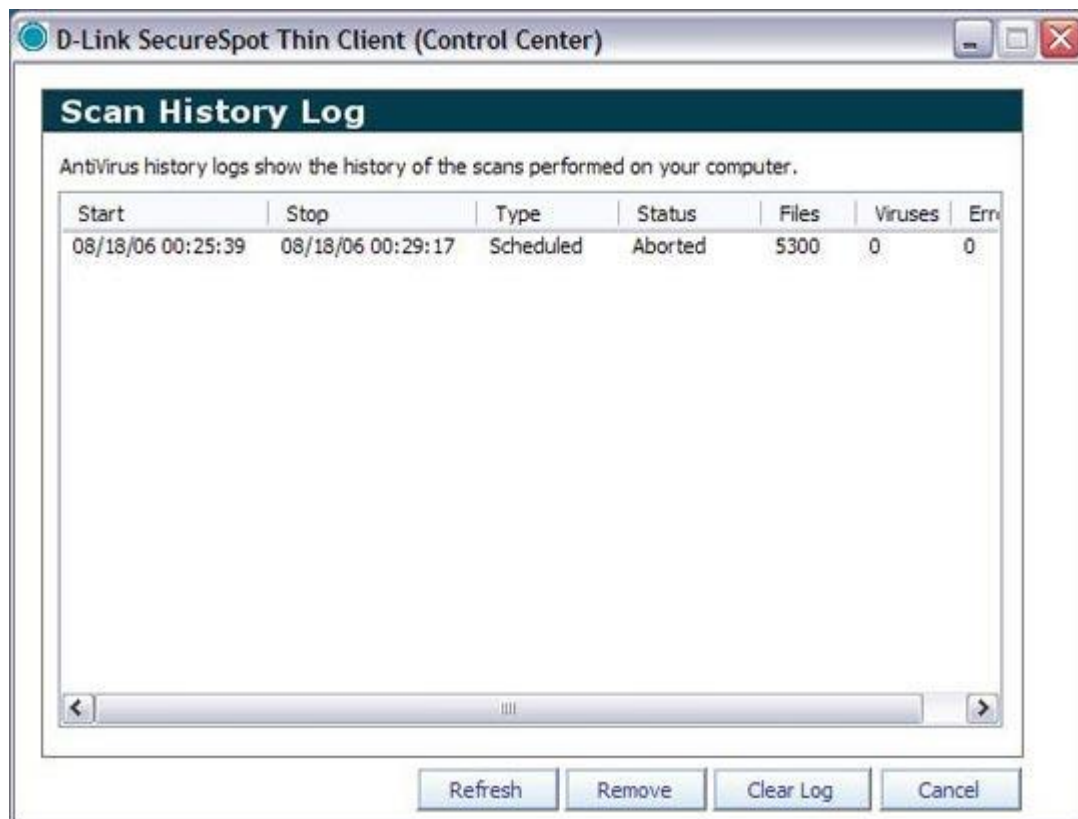
OR

- Select the **All** option button in the **Scan Options** dialog box to scan ALL files.
- To scan the selected file types in ALL system folders and drives, click **Scan All**.

OR

- To scan the selected file types in CERTAIN folders and drives, click **Scan**.
- A Scan Progress pop-up window opens, and the scanning process begins. When the scan is finished, *Scan complete* is displayed at the top of the pop-up window. Any infected files are displayed on the pop-up window.
- Click **Cancel** to return to the AntiVirus/Spyware home page without saving changes.

12. To view the scan log, click the **Scan History Log** link on the AntiVirus/Spyware home page.



To view virus scan history:

- 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**. (*You will receive a verification prompt; click **Yes**.*)
- Click **Cancel** to return to the AntiVirus/Spyware home page without saving changes.

13. To set up a scheduled automated scan, click the **Scheduled Scans** link on the AntiVirus/Spyware home page.

To view quarantined potentially unwanted program (PUP) files that were found during a manual or automated scan:

- Start a scan.
- A **Bsecure AntiVirus Services pop-up window** appears on the screen and displays the PUP file and Program Name.



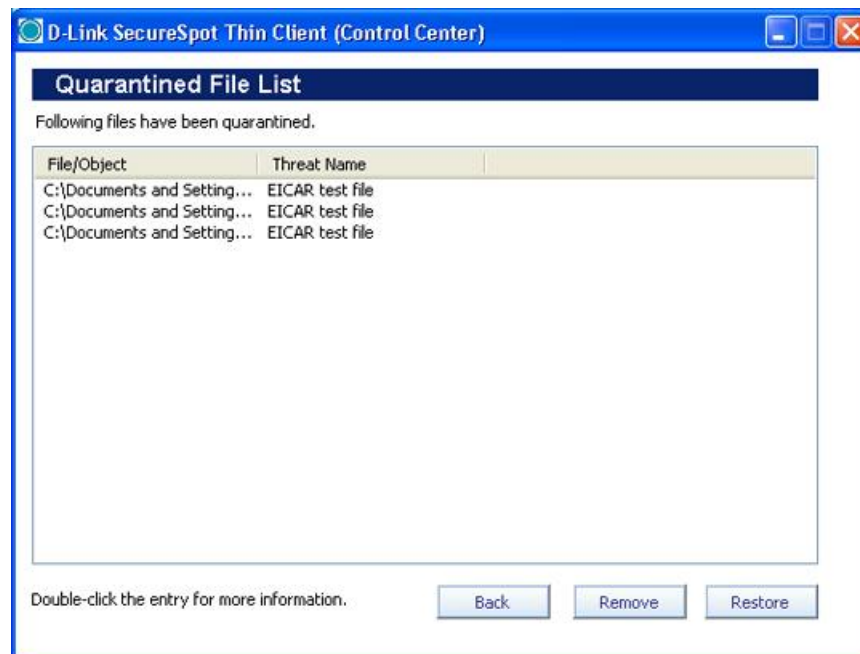
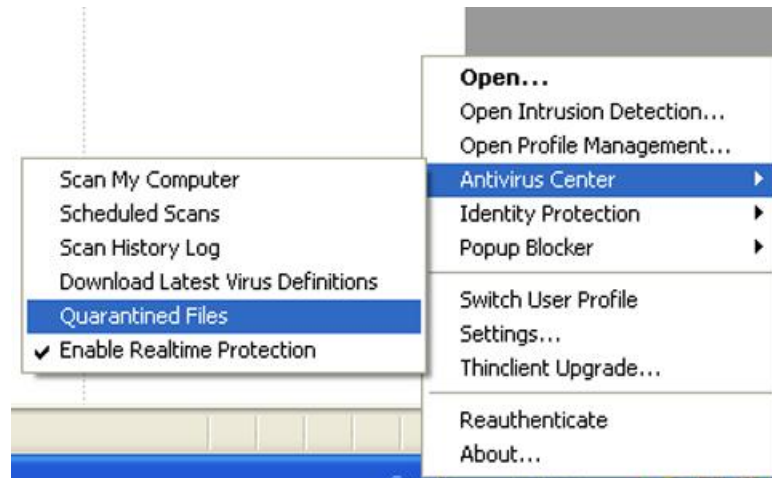
- Click the McAfee link at the bottom of the pop-up window for detailed threat information.
- Click **Allow** to permit system access to the file. (*If the same PUP file is detected again, it will be silently allowed.*)
- Click **Quarantine** to repair the buffer/object/file. (*If repair fails, then the filename is added to a quarantined list and file access is denied.*)
- Double-click the object/file to launch the McAfee Web site.
- Click **Restore** to repair and release the file/object from the quarantined list.
- Click **Remove** to delete the file/object permanently.
- Click **Back** to return to the AntiVirus Center home page without saving changes.

To view quarantined PUP files that were found during a real-time scan:

- Download a file/program from the Internet.
- A **Bsecure AntiVirus Services** pop-up window appears on the screen and displays the PUP file and Program Name.



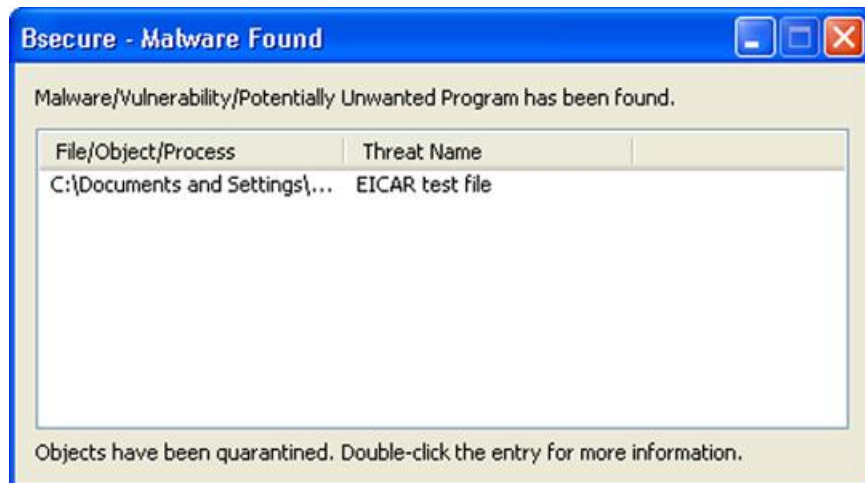
- Click the McAfee link at the bottom of the pop-up window for detailed threat information.
- Click **Allow** to permit system access to the file. *(If the same PUP file is detected again, it will be silently allowed.)*
- Click **Quarantine** to repair the buffer/object/file. *(If repair fails, then the filename is added to a quarantined list and file access is denied.)*
- Close the pop-up window.
- From the securespot tray icon, click the **Quarantined Files** submenu under AntiVirus Center. A **Quarantined File List** dialog box will appear on the screen with a list of quarantined files. *(If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file.)*



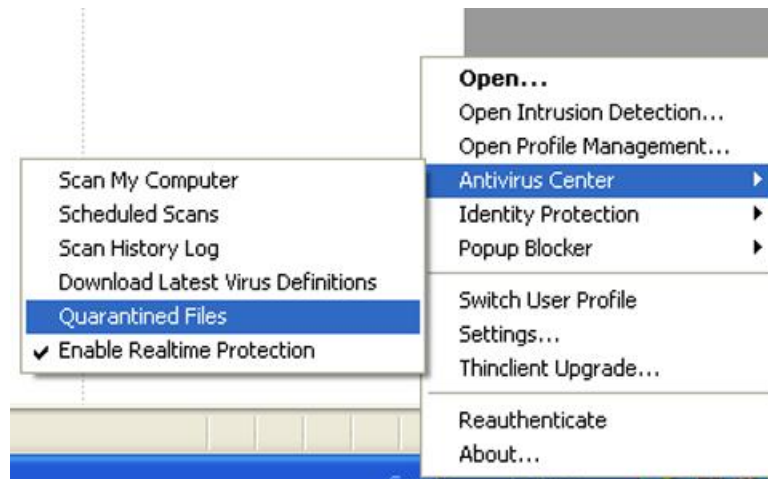
- Double-click the object/file to launch the McAfee Web site.
- Click **Restore** to repair and release the file/object from the quarantined list.
- Click **Remove** to delete the file/object permanently.
- Click **Back** to return to the AntiVirus Center home page without saving changes.

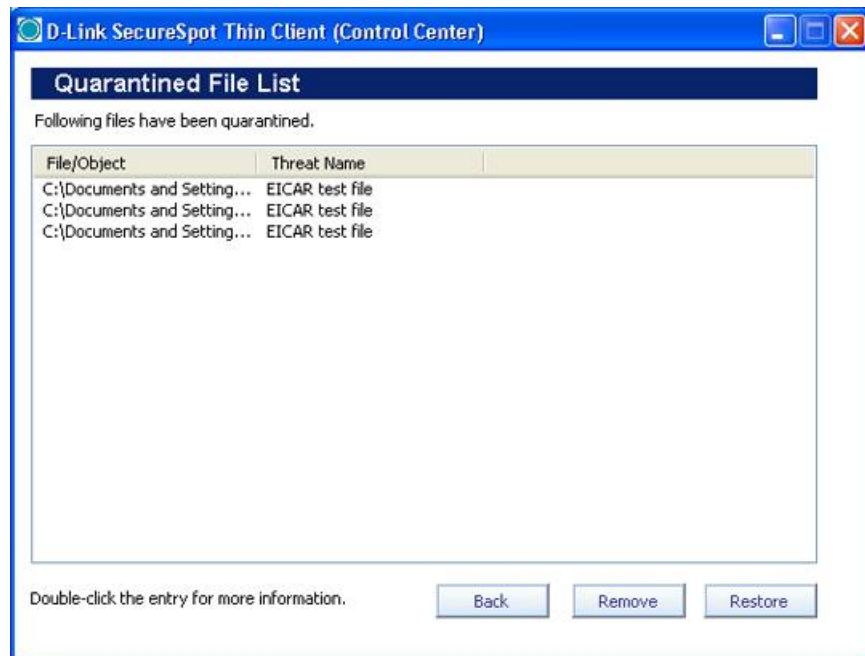
To view viruses that were found during a manual or automated scan:

- Start a scan.
- A **Bsecure pop-up window** appears on the screen and displays the Virus file and Threat Name.



- For more threat information, double-click the file/object to launch the McAfee Web site.
- Close the pop-up window.
- From the securespot tray icon, click the **Quarantined Files** submenu under AntiVirus Center. A **Quarantined File List** dialog box will appear on the screen with a list of quarantined files. *(If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file.)*

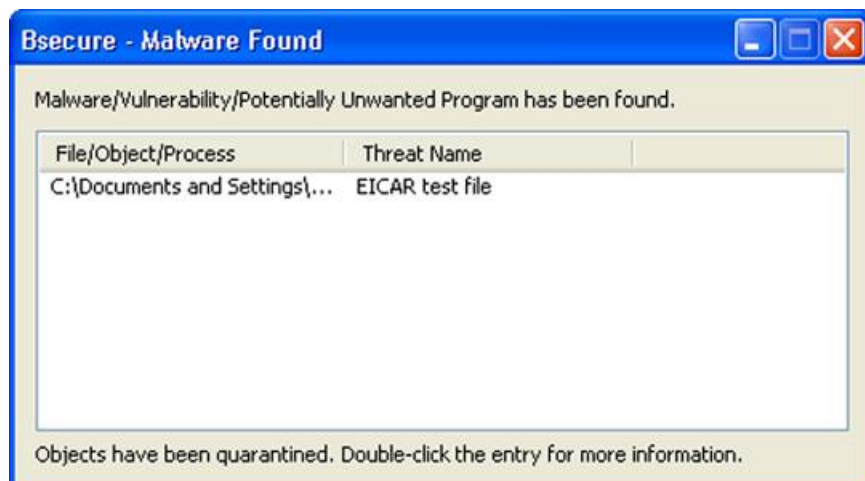




- Double-click the object/file to launch the McAfee Web site.
- Click **Restore** to repair and release the file/object from the quarantined list.
- Click **Remove** to delete the file/object permanently.
- Click **Back** to return to the AntiVirus Center home page without saving changes.

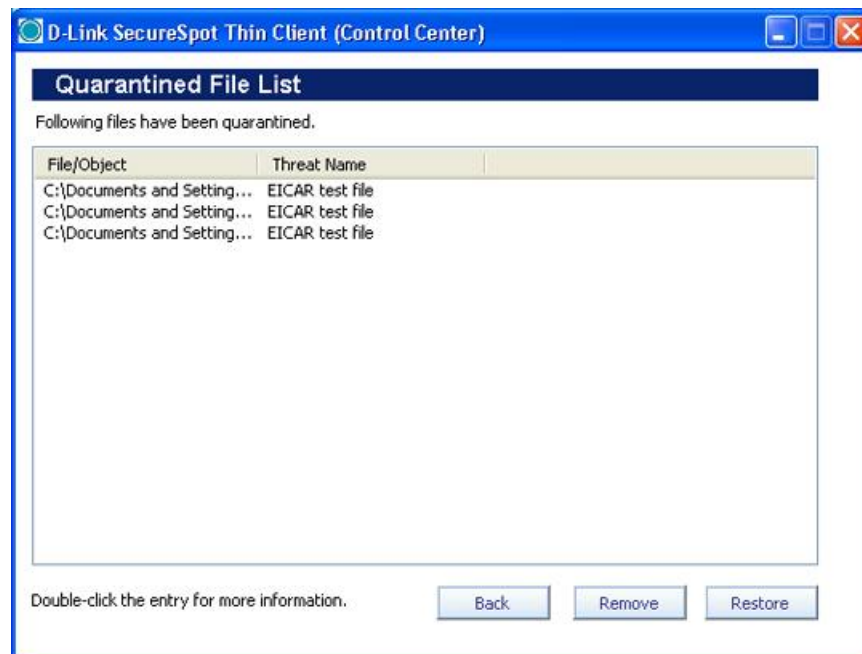
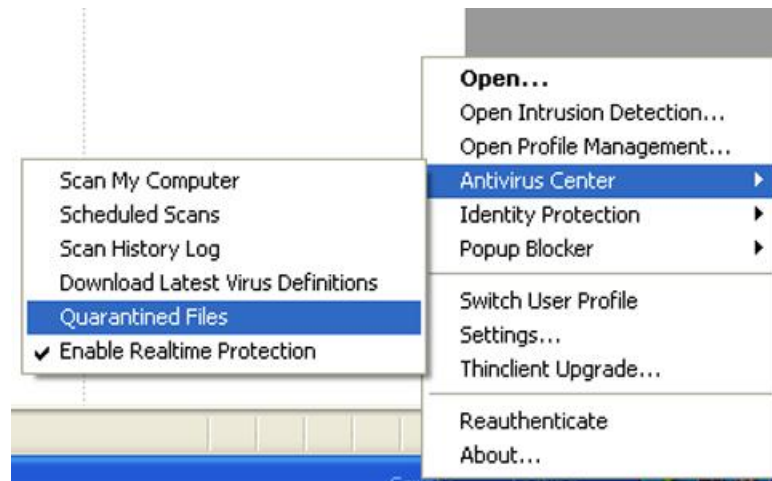
To view viruses that were found during a real-time scan:

- Download a file/program from the Internet.
- A **Bsecure pop-up window** appears on the screen and displays the Virus file and Threat Name.



- For more threat information, double-click the file/object to launch the McAfee Web site.
- Close the pop-up window.

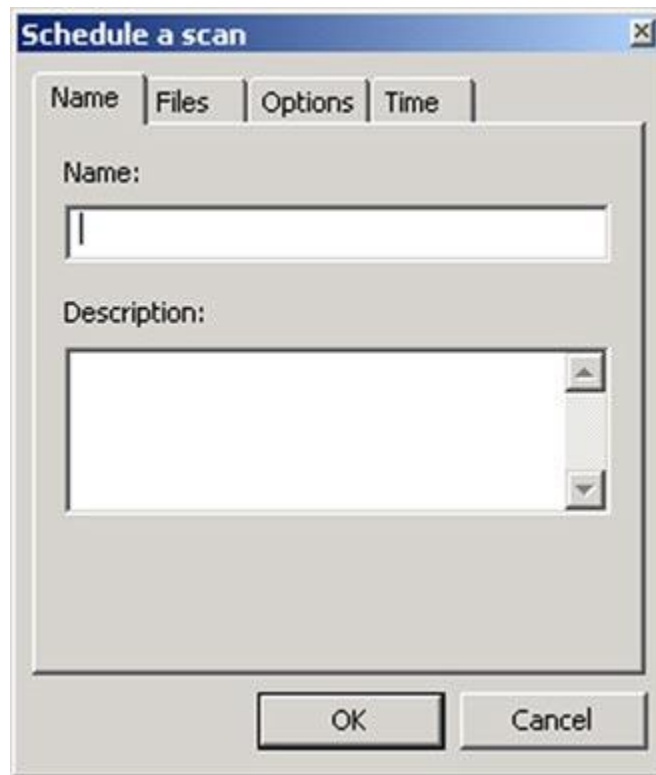
- From the securespot tray icon, click the **Quarantined Files** submenu under AntiVirus Center. A **Quarantined File List** dialog box will appear on the screen with a list of quarantined files. *(If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file.)*



- Double-click the object/file to launch the McAfee Web site.
- Click **Restore** to repair and release the file/object from the quarantined list.
- Click **Remove** to delete the file/object permanently.
- Click **Back** to return to the AntiVirus Center home page without saving changes.

To schedule an automatic scan:

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



- Type a name and description for the scheduled scan, and then click **OK**.
- Click the **Files** tab. Check the boxes next to the folders or drives you want scanned, and then click **OK**.
- 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 list box, select what action you want performed when detection of an infected file has occurred:
 - a. **Disinfect the file** – Cleans infected files automatically when they are found.
 - b. **Warn me before taking action** – Let's you choose what to do with each infected file when it is found.
 - c. **Delete infected file** – Deletes infected files automatically when there are found.
- Click **OK**.
- Click the **Time** tab. Select the option button for the desired automatic scan frequency: **Daily**, **Weekly**, or **Monthly**. (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.)
- Click **OK**.
- Click **Scan now** to start a scheduled scan.
- Click **Cancel** to return to the AntiVirus/Spyware home page without saving changes

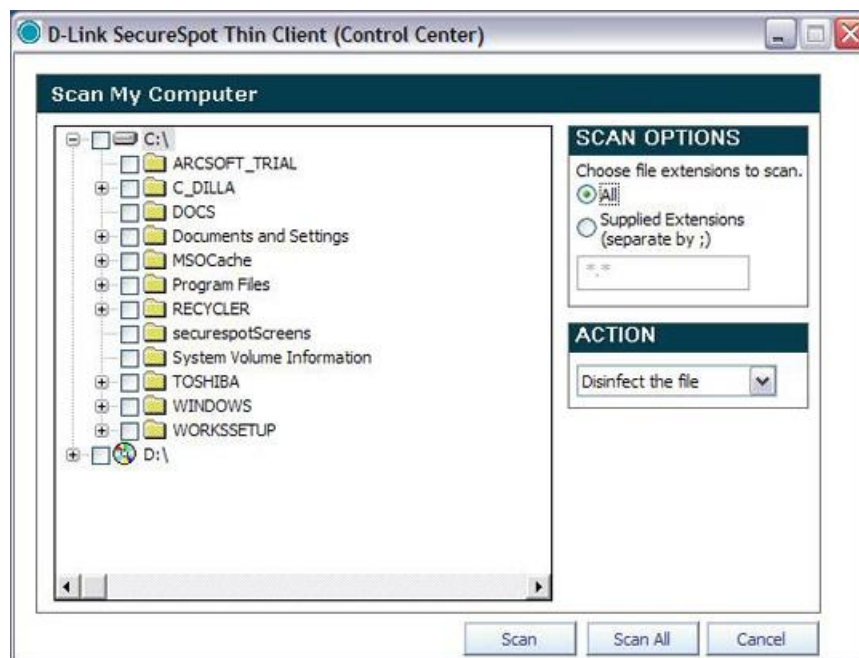
To delete a scheduled scan:

- Select the scan that you want to cancel.
- Click **Remove**. (*The scan is permanently removed from the schedule.*)

To edit a scheduled scan:

- Select the scan that you want to edit.
- Follow the steps under Scheduling an Automatic Scan to edit the details of your scheduled scan.

14. To update your virus definition file updates, click the **Manual Updates** link on the AntiVirus/Spyware home page. You can manually check for updates at any time. Make sure you have not missed an update, or catch up if you cancelled the last update notification.



To update your virus definition file updates:

- Click **Next** to check for updates. (*The Securespot Client Control Center will be closed during this operation.*)



- An update pop-up window will appear when the virus definition files have been updated. Click **Close**.
- Click **Back** to return to the AntiVirus/Spyware home page without saving changes.

15. To view quarantined files, click the View Quarantined Files link on the AntiVirus/Spyware home page.

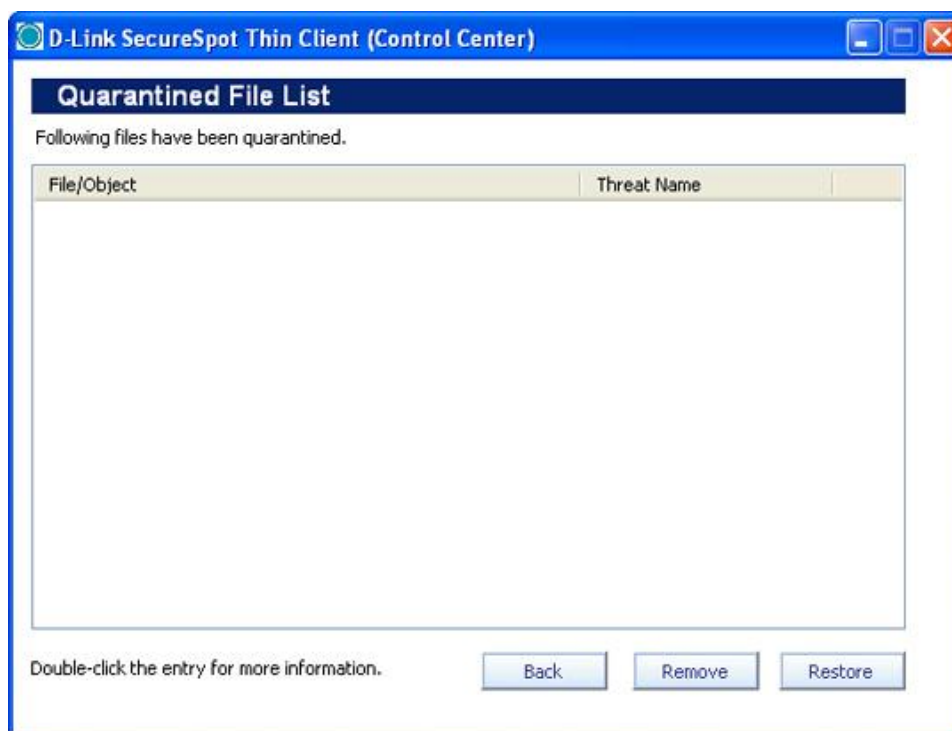
To view quarantined potentially unwanted program (PUP) files that were found during a manual or automated scan:

1. Start a scan.
2. A **Bsecure AntiVirus Services** pop-up window appears on the screen and displays the PUP file and Program Name.
3. Click the McAfee link at the bottom of the pop-up window for detailed threat information.
4. Click **Allow** to permit system access to the file. *(If the same PUP file is detected again, it will be silently allowed.)*
5. Click **Quarantine** to repair the buffer/object/file. *(If repair fails, then the filename is added to a quarantined list and file access is denied.)*
6. Close the scan.

7. Click the **Quarantined Files** link on the AntiVirus Center home page. *(If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file.)*
8. Double-click the object/file to launch the McAfee Web site.
9. Click **Restore** to repair and release the file/object from the quarantined list.
10. Click **Remove** to delete the file/object permanently.
11. Click **Back** to return to the AntiVirus Center home page without saving changes.

To view quarantined PUP files that were found during a real-time scan:

12. Download a file/program from the Internet.
13. A **Bsecure AntiVirus Services** pop-up window appears on the screen and displays the PUP file and Program Name.
14. Click the McAfee link at the bottom of the pop-up window for detailed threat information.
15. Click **Allow** to permit system access to the file. *(If the same PUP file is detected again, it will be silently allowed.)*
16. Click **Quarantine** to repair the buffer/object/file. *(If repair fails, then the filename is added to a quarantined list and file access is denied.)*
17. Close the pop-up window.
18. Click the **Quarantined Files** link on the AntiVirus Center home page. *(If the potential threat has been quarantined and is not listed, then AntiVirus Services have successfully repaired the file.)*



19. Double-click the object/file to launch the McAfee Web site.
20. Click **Restore** to repair and release the file/object from the quarantined list.
21. Click **Remove** to delete the file/object permanently.
22. Click **Back** to return to the AntiVirus Center home page without saving changes.

16. To launch the McAfee® Threat Center, click the Threat Center link on the AntiVirus/Spyware Service panel.

The screenshot shows the McAfee Threat Center interface. At the top, there's a navigation bar with links for Home & Home Office, Small & Medium Business, Enterprise, and Partners. Below this, the main header features the McAfee logo and a search bar. The central content area is divided into several sections: a 'Threat Center' banner with the text 'Up-to-the-minute knowledge about threats and vulnerabilities from top-ranked McAfee Avert® Labs.'; a 'BREAKING ADVISORY' section dated August 14, 2007, regarding Microsoft Security Bulletins; a 'Current Malware' table listing threats like GPCoder.h and W32/Zhelatin.gen!ml; and a 'Current Vulnerabilities' table listing items like MS07-048 Vista Headl... and MS07-046 MS GDI. On the right side, there's a 'Global Threat Condition' section showing an 'Elevated' status, a 'McAfee AudioParasitics' podcast advertisement, and a 'McAfee Avert Labs Sage Report' section.

McAfee® Threat Center | Need Help? | Global Sites | Keyword Search

Home & Home Office | Small & Medium Business | Enterprise | Partners

Threat Center

Up-to-the-minute knowledge about threats and vulnerabilities from top-ranked McAfee Avert® Labs.

Protect what you value.

BREAKING ADVISORY

August 14, 2007. Nine Security Bulletins have been released by Microsoft to address 14 CVE identified vulnerabilities. The affected products include Microsoft Windows, Office, Virtual PC, and Virtual Server. Six of the bulletins have been rated by the vendor as critical with the three remaining being rated important.

Learn More

July 31, 2007. Apple today released Security Update 2007-007 and two other updates to patch vulnerabilities in iPhone, Safari, and Mac OS X. The worst of the patched flaws would allow for remote code execution without user interaction.

Learn More

Current Malware		Current Vulnerabilities	
	Date Published		Date Public
GPCoder.h	16 Jul 2007	MS07-048 Vista Headl...	14 Aug 2007
W32/Zhelatin.gen!ml	04 Jul 2007	MS07-046 MS GDI	14 Aug 2007
Phish-BuyPhony	01 Jul 2007	MS07-042 XML Core	14 Aug 2007
W32/Stration.gen.dll	07 Nov 2006	MS07-039 Active Dir ..	10 Jul 2007
PWS-Banker.gen.ac	17 May 2006	MS07-038 MS Vista FW	10 Jul 2007
		MS07-031 MS SChannel	12 Jun 2007

See Recent Malware | View Malware Threat Key

Global Threat Condition

Elevated

Learn More

McAfee Avert Labs has developed a general ranking system that indicates the severity of known global threats and how they impact the Internet, business operations, and home users' systems.

McAfee® AudioParasitics

Podcasts from McAfee Avert® Labs

Computer security's Red Pill

McAfee Avert Labs Sage Report

Sage

The Future of Security

The second issue of McAfee Avert Labs security journal gazes into the crystal ball to divine what threats and defenses will attract your attention during the next five

17. To launch the McAfee® Threat Library, click the Threat Library link on the AntiVirus/Spyware Service panel.

The screenshot shows the McAfee Threat Library interface. It features a search bar at the top with the text 'Search McAfee Avert® Labs Threat Library'. Below this, there's a 'Threat Information Library Search' section with a search box and a 'Search' button. The main content area is divided into two columns: 'Top Corporate User Malware' and 'Top Home User Malware', each listing threats like Downloader-AAP and JS/Downloader-AUD. On the right side, there's a 'Threat Resources' section with links to Anti-Malware Tips, Hoaxes, Malware Alerts, and a 'DAT Information' section with links to DAT Readme, DAT Downloads, and Sign up for Avert DAT Notification Service.

McAfee® Threat Center | Need Help? | Global Sites | Keyword Search

Home & Home Office | Small & Medium Business | Enterprise | Partners

Search McAfee Avert® Labs Threat Library

More than 180,000 threats exist today. The McAfee Avert Labs Threat Library has detailed information on viruses, Trojans, hoaxes, vulnerabilities and Potentially Unwanted Programs, where they come from, how they infect your system, and how to mitigate or remediate them.

Threat Information Library Search

Search for Threats: Search

Search in Category: All Threats Display: 10

Top Corporate User Malware		Top Home User Malware	
Listed Alphabetically		Listed Alphabetically	
Downloader-AAP	22 Feb 2007	JS/Downloader-AUD	19 Jun 2007
Generic Malware.a.zip	01 Jun 2005	JS/Exploit-BO.gen	26 Apr 2007
W32/Mytob.gen@MM	18 May 2005	JS/Wonka	09 Oct 2006
W32/Stration.gen.dll	24 Dec 2006	Puper	29 Sep 2005
W32/Zhelatin.gen!ml	11 Jul 2007	VBS/Pyryme	08 Oct 2006

View Threat Key

Threat Resources

- Anti-Malware Tips
- Hoaxes
- Malware Alerts
- Malware Check and Removal Tool "Stinger"
- McAfee Avert Labs Threat News
- Newly Discovered Malware
- Newly Discovered PUPs
- Recent Vulnerabilities
- Recently Updated Malware
- Recently Updated PUPs
- Search Threat Library
- Submit a Virus Sample
- Tools and Utilities
- Virus Calendar

DAT Information

- DAT Readme
- DAT Downloads
- Sign up for Avert DAT Notification Service

McAfee Avert Labs Blog

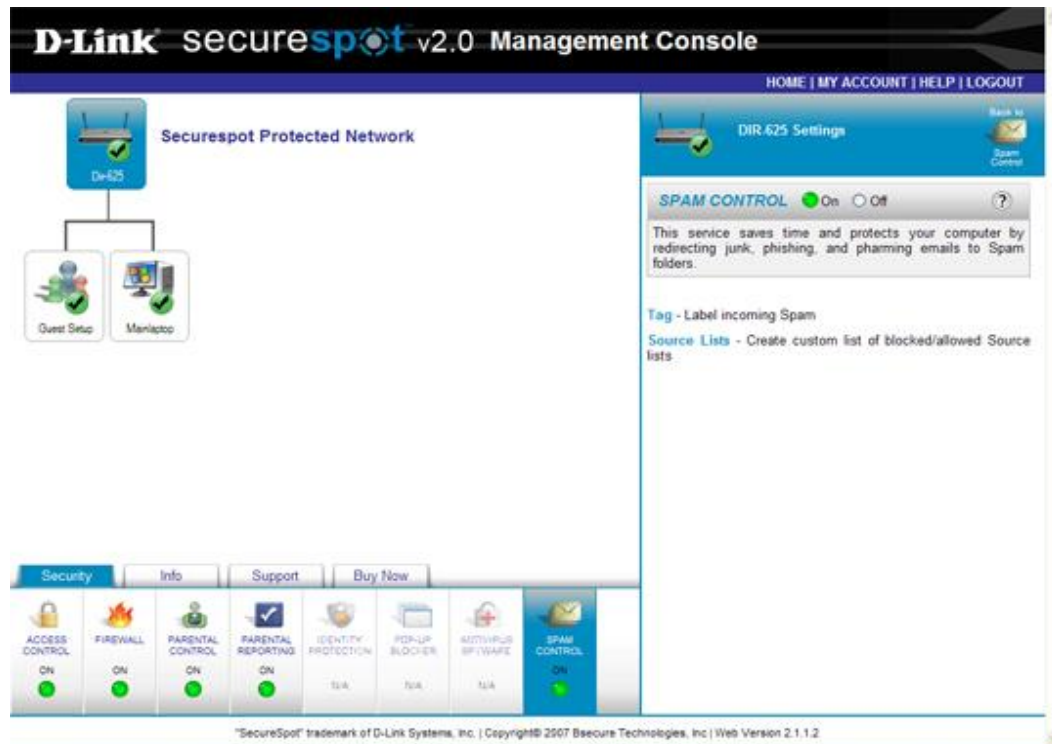
- Read about security research as it happens


Spam Control Service

This feature stops unwanted e-mail from filling up your inbox and it provides Antiphishing protection at the same time. You may add this protection directly into Microsoft Outlook or other e-mail accounts without changing addresses, forwarding e-mail, giving out passwords.

To enable Spam Control:

1. Select a specific device on the network map.
2. Click the **Spam Control** service under the **Security** tab.





3. Click the  icon to hide/display descriptive Spam information.
4. Select the **ON** option button to enable the Spam Control service. (*The default is ON.*)
5. If you want to define a personal tag to an unwanted e-mail, click the **Tag** link on the Spam Control Service panel.

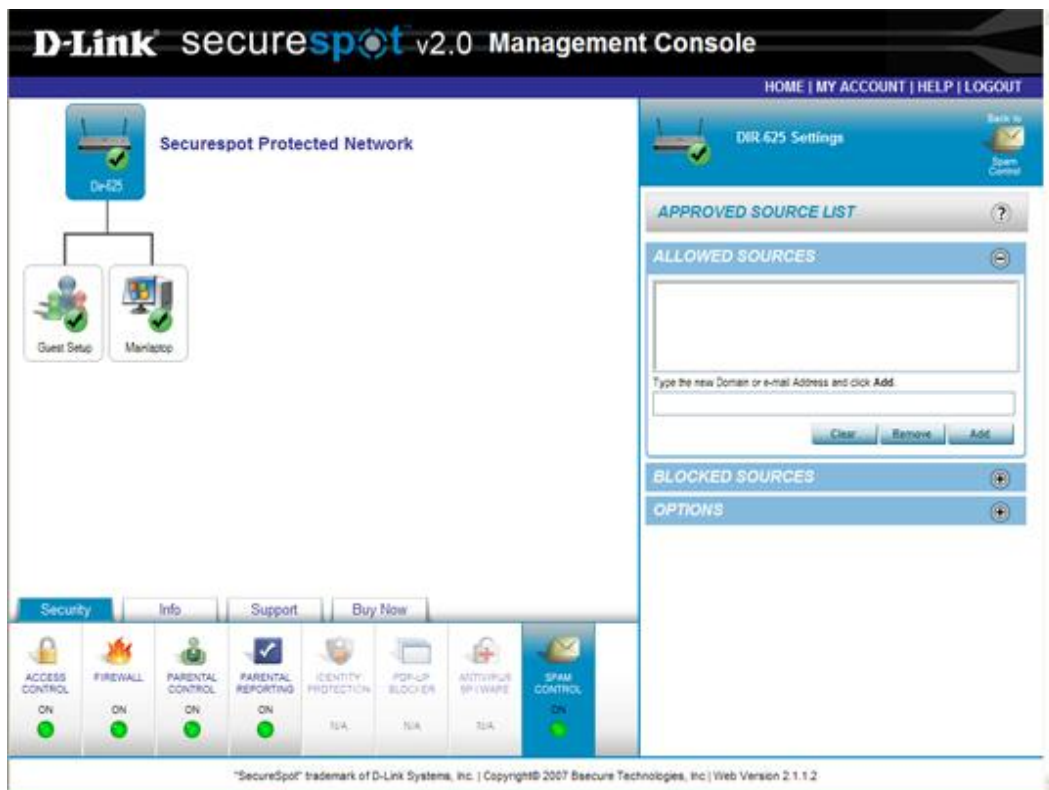


- Type the prefix in the **Spam Subject Tag** text box. (*The default is Spam.*)
- Click **Save** to save your settings. (Once your settings have been saved, the message “Spam settings updated” appears on the Spam Control service panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Spam Control Service panel without saving any changes.
- To hide Spam Tag details, click the  icon.



6. If you want to create an approved domain list, click the Source Lists link on the Spam Control




To create an Allowed Source List:

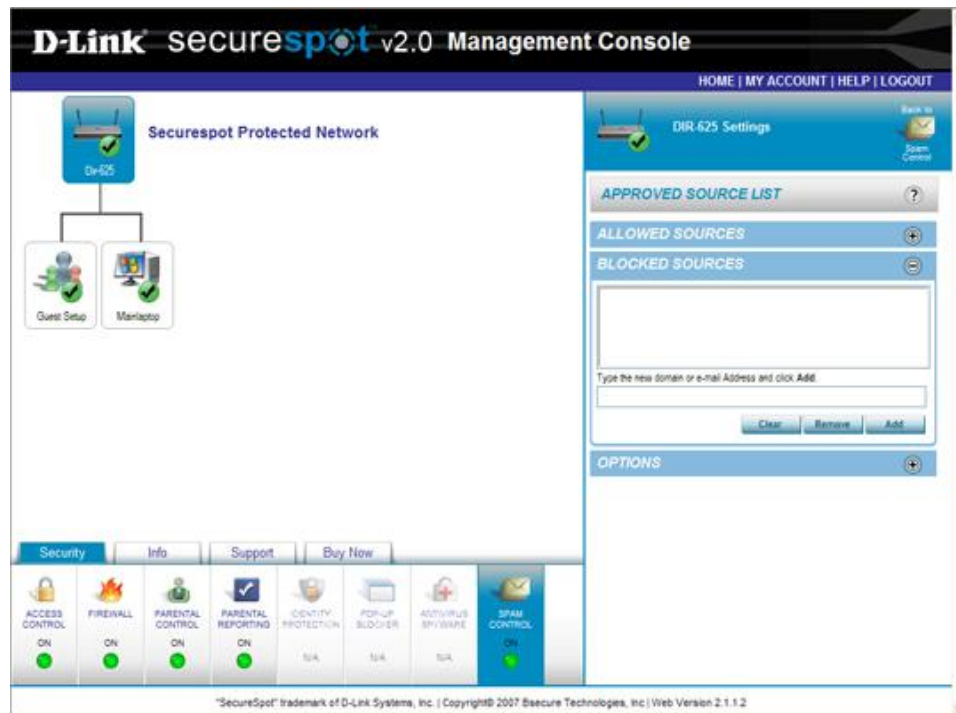
- In the provided text box, type the Domain and/or e-mail address that you want to allow.
- Click **Add**. (*The Domain and/or e-mail address is added to the **Allowed Source List**.*)
- Repeat the previous two steps if you want to add additional Domain and/or e-mail addresses to your **Allowed Source List**. (*Once your settings have been saved, the message "Spam Lists saved" appears on the Approved Source List panel.*)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Spam Control Service panel without saving any changes.
- To hide Allowed Source List details, click the  icon.



To create a Blocked Source List:

- Click the  icon to expand the Blocked Source List panel.
- In the provided text box, type the Domain and/or e-mail address that you want to block.
- Click **Add**. (*The Domain and/or e-mail address is added to the **Blocked Source List**.*)




- Repeat the previous two steps to add additional Domain and/or e-mail addresses to your **Blocked Source** List. (Once your settings have been saved, the message "Spam Lists saved" appears on the Blocked Source List panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Spam Control Service panel without saving any changes.
- To hide Blocked Source List details, click the  icon.



To edit the Allowed and Blocked Source Lists:

- Click the  icon to expand the list that you want to edit: **Allowed Domain List** or **Blocked Domain List**.
- To remove a single entry from a list, click (highlight) the Domain and/or e-mail address entry and click **Remove**. (The Domain and/or e-mail address is removed from the appropriate list.)


OR

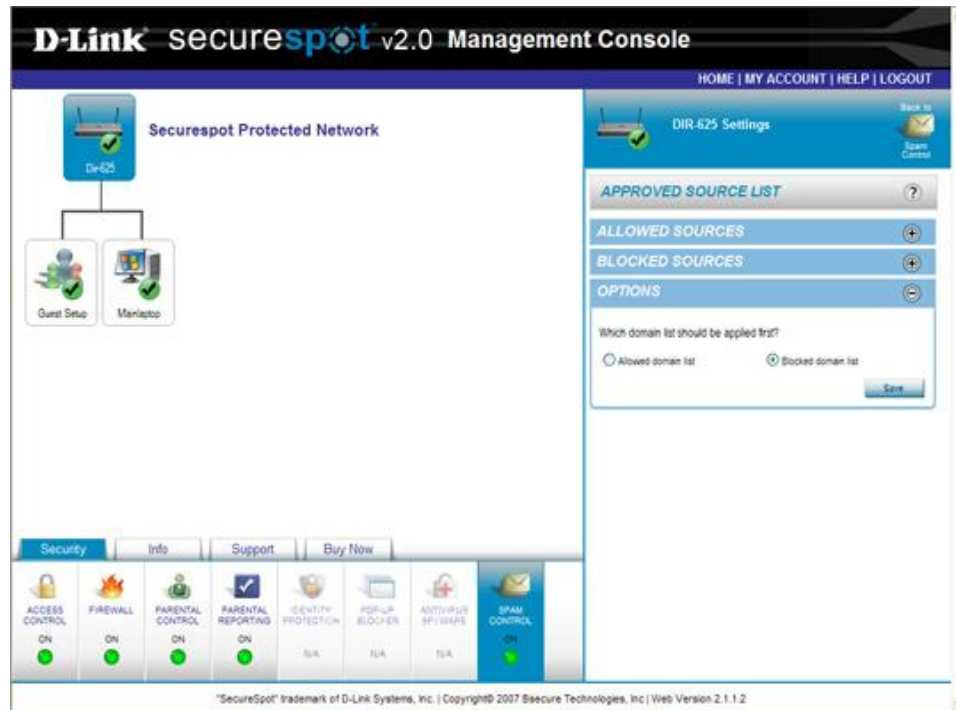
- To remove several entries from a list, click (highlight) the Web site entries and click **Clear**. (All entries are removed from the appropriate list.)

OR

- Click the  icon to return to the Spam Control Service panel without saving any changes.
- To hide Allowed and/or Blocked Domain List details, click the  icon.



To create a Source List Rule:

- Once you have created Allowed and/or Blocked Source Lists, you may create a Source List rule.
- Click the  icon to expand the **Options** panel.



- Select the Source list that you want applied first(**Allow** or **Blocked**).
- Click **Save** to save your settings. (Once your settings have been saved, the message "Spam Lists saved" appears on the Approved Source List panel.)
- If you changed the settings, click **Apply Settings**.

OR

- Click the  icon to return to the Spam Control Service panel without saving any changes.
- To hide Options details, click the  icon.

Appendix – Backup and Firmware Upgrade

To download the Securespot v2.1.2 Security Services to your D-Link router, you must upgrade the router firmware to v3.0. Use the following procedure to upgrade your firmware:

1. Open any Web browser and login to the D-Link Router Product Page.
2. Select the **Tools** menu.

The screenshot shows the D-Link DIR-625 router web interface. The top navigation bar includes the D-Link logo and a menu with the following items: DIR-625, SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a list of links: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled "ADMINISTRATOR SETTINGS" and contains the following sections:

- ADMINISTRATOR SETTINGS**: A text box explaining that the 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. It also states that by default there is no password configured and it is highly recommended to create a password to keep the router secure. Below this text are two buttons: "Save Settings" and "Don't Save Settings".
- ADMIN PASSWORD**: A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password :" and "Verify Password :".
- USER PASSWORD**: A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password :" and "Verify Password :".
- SYSTEM NAME**: A section with the label "Gateway Name :" followed by an input field.
- ADMINISTRATION**: A section containing the following options:
 - Enable Remote Management : ☐
 - Remote Admin Port : 8080
 - Remote Admin [Inbound Filter](#) :
 - Details :

On the right side of the interface, there is a "Helpful Hints..." section with the following text:

For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new and passwords to avoid having to reset the router in case they are forgotten.

Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.

Choose a port to open for remote management.

Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the [Advanced -- Inbound Filter](#) screen and create a new filter.

More...

At the bottom of the interface, there is a "WIRELESS" section.

3. Select the **System** link on the **Tools** menu.

D-Link

DIR-625

SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SYSTEM SETTINGS

Save To Local Hard Drive:

Load From Local Hard Drive:

Restore To Factory Default:

Restore all settings to the factory defaults.

Reboot The Device:

Helpful Hints...

Once your router is configured the way you want it, you can save the configuration settings to a configuration file.

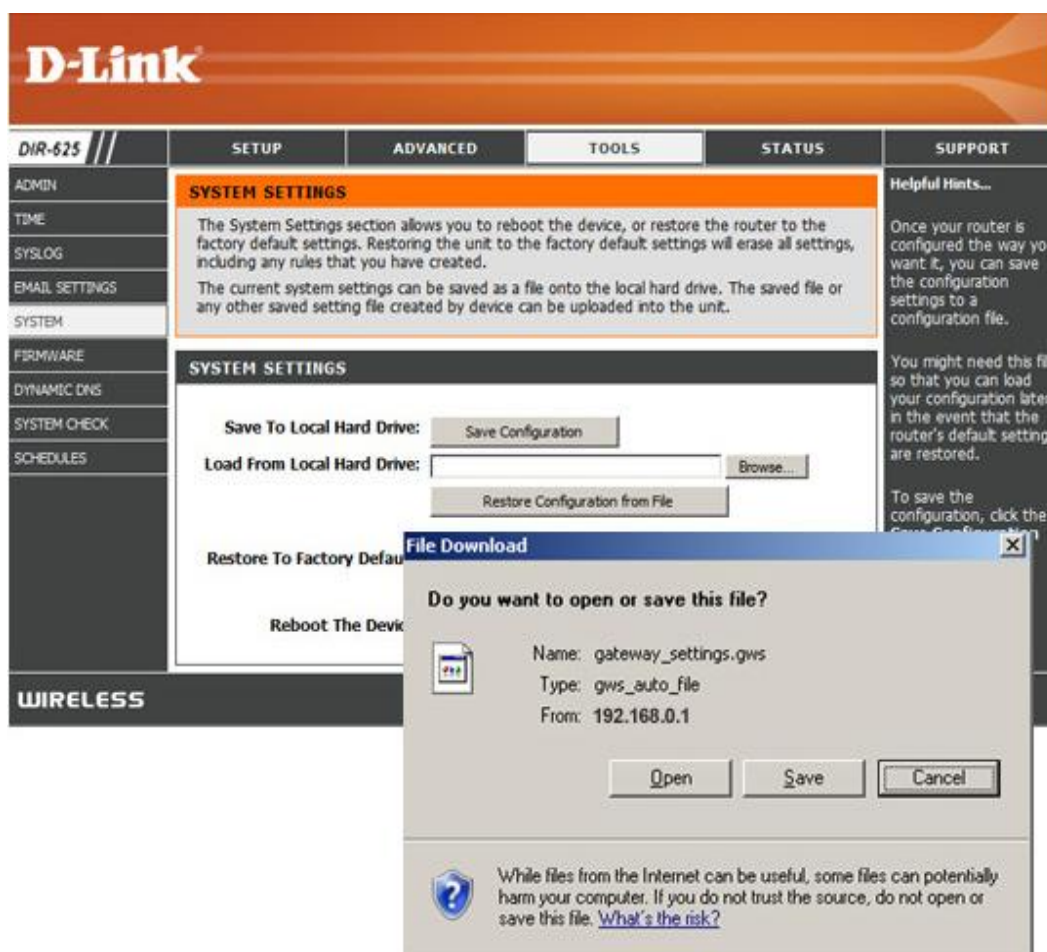
You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

To save the configuration, click the **Save Configuration** button.

[More...](#)

WIRELESS

4. Click the **Save Configuration** button. (To retain your existing router configuration settings, you must manually save these settings before you upgrade the router firmware.)
5. A **File Download** pop-up window appears on your screen. Click the **Save** button.



- Type admin in the **User name** text box.
- Leave the **Password** text box blank.
- Click **OK**.

6. Select the **Firmware** link on the **Tools** menu. Verify the version in the Firmware Information section.

D-Link

DIR-625 //

ADMIN	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
ADMIN	FIRMWARE There may be new firmware for your DIR-625 to improve functionality and performance. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button below to start the firmware upgrade. <div> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </div>				Helpful Hints... Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router. More...
TIME	FIRMWARE INFORMATION Current Firmware Version : 3.00 Current Firmware Date : 2007/02/27 Latest Firmware Version : 3.00 Click here to access firmware online.				
SYSLOG	FIRMWARE UPGRADE Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> System screen. To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button. <div> Upload : <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/> </div>				
EMAIL SETTINGS	FIRMWARE UPGRADE NOTIFICATION OPTIONS Automatically Check Online for Latest Firmware Version : <input checked="" type="checkbox"/> Email Notification of Newer Firmware Version : <input type="checkbox"/>				
SYSTEM					
FIRMWARE					
DYNAMIC DNS					
SYSTEM CHECK					
SCHEDULES					

WIRELESS

7. Click the **Browse** button in the Firmware Upgrade section.
8. Select the appropriate firmware file (*.bin), and then click the **Open** button.
9. Click the **Upload** button.
10. Click the **OK** button. When firmware upgrade is done, an **Upload Succeeded** pop-up window appears on your screen.

D-Link

UPLOAD SUCCEEDED

The router will now be reprogrammed using the uploaded firmware file. Please wait 41 seconds for this process to complete, after which you may access these web pages again. Pressing reload or back on your browser may cause this operation to fail.

WIRELESS

Restore Configuration Settings

This option restores all configuration settings back to the settings that were in effect for your previous version of firmware. Use the following procedure to restore your previous configuration settings:

1. Click the **Tools** menu.

The screenshot shows the D-Link DIR-625 web interface. The top navigation bar includes the D-Link logo and a menu with the following items: DIR-625, SETUP, ADVANCED, **TOOLS** (highlighted), STATUS, and SUPPORT. On the left side, there is a vertical menu with the following items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled "ADMINISTRATOR SETTINGS" and contains the following sections:

- ADMINISTRATOR SETTINGS**: A text box explaining that the 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. By default, there is no password configured. It is highly recommended that you create a password to keep your router secure. Below this text are two buttons: "Save Settings" and "Don't Save Settings".
- ADMIN PASSWORD**: A section with the instruction "Please enter the same password into both boxes, for confirmation." Below this are two input fields: "Password :" and "Verify Password :".
- USER PASSWORD**: A section with the instruction "Please enter the same password into both boxes, for confirmation." Below this are two input fields: "Password :" and "Verify Password :".
- SYSTEM NAME**: A section with the label "Gateway Name :" followed by an input field.
- ADMINISTRATION**: A section with the following options:
 - Enable Remote Management : ☐
 - Remote Admin Port : 8080
 - Remote Admin [Inbound Filter](#) :
 - Details :

On the right side of the interface, there is a "Helpful Hints..." section with the following text:

For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new and passwords to avoid having to reset the router in case they are forgotten.

Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.

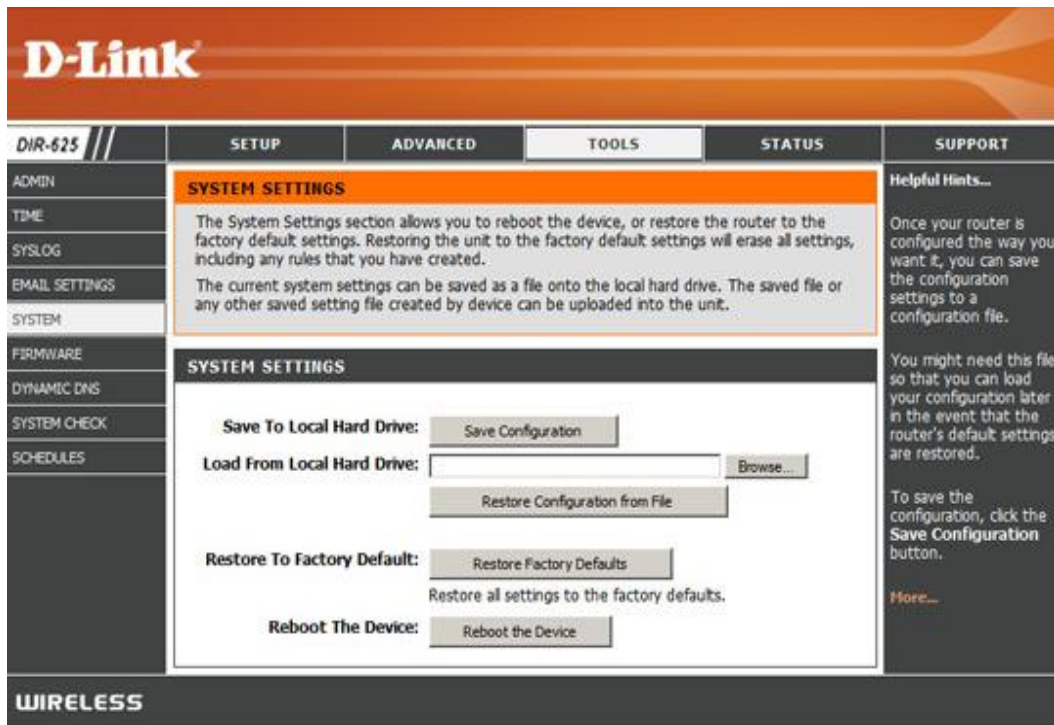
Choose a port to open for remote management.

Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the [Advanced -- Inbound Filter](#) screen and create a new filter.

[More...](#)

At the bottom of the interface, there is a "WIRELESS" section.

2. Select the **System** link on the **Tools** menu.



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 then click the **Open** button.
6. Click the **Restore Configuration from File** button in the System Settings page. (Please wait while the configuration is being restored.)

D-Link

DIR-625 //

SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SYSTEM SETTINGS

Save To Local Hard Drive:

Load From Local Hard Drive:

Restore To Factory Default:

Restore all settings to the factory defaults.

Reboot The Device:

WIRELESS

Helpful Hints...

Once your router is configured the way you want it, you can save the configuration settings to a configuration file.

You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

To save the configuration, click the **Save Configuration** button.

[More...](#)

7. When Restore Configuration is done, a **Restore Succeeded** pop-window appears on your screen.

D-Link

RESTORE SUCCEEDED

The restored configuration file has been uploaded successfully.

Press the button below to continue configuring the router if the previous page doesn't restore in 5 seconds.

WIRELESS

8. Click **Continue** if the System Settings page does not reappear on your screen within 5 seconds.