

## DSD-150 Interface

Username:  Password:

**D-Link** **securespot**

HOME MY ACCOUNT SUPPORT

### Thank You

Thank you for purchasing the securespot™ Internet Security Device.

View latest securespot™ enhancements! ([what's new](#))

If you would like to upgrade you firmware now, please [click here](#).

Continue here for [activation](#).

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

Username:  Password:

**D-Link** **securespot**

HOME MY ACCOUNT SUPPORT

## Congratulations on purchasing a D-Link securespot™ Complete Internet Security Solution!



with **McAfee**  
**VirusScan**

Virus and Spyware Protection

[Product Manual](#) [Data Sheet \(PDF\)](#)  
[Firmware](#)

[Already Activated?](#)

The securespot™ helps keep your network's PCs safe from hackers, viruses, spam, pop-ups and other undesired content.

This All-in-One Security Device includes a paid up annual subscription to the Bsecure™ security service for up to 4 users\*. To activate the service, you will need to activate the device in our secure entry form.

\*If you need more than 4 users, you will be prompted during your 5th registration to add more users.

Information submitted on this page is secure and strictly adheres to our Privacy Policy.



Username:  Password:



seurespot

[HOME](#)

[MY ACCOUNT](#)

[SUPPORT](#)

### D-LINK SERVICE AGREEMENT

Please read the service agreement below, check the box if you accept these terms and conditions and click the "Continue" button.

#### Terms and Conditions

**IMPORTANT:** Please review the following terms and conditions carefully. The Services, Software and Associated Materials described herein are being provided to you by D-Link Systems, Inc. ("D-Link") and Bsecure Technologies, Inc. ("Bsecure"), which are jointly referred to as "us" or "we" or words of similar effect. This Agreement is a legally binding contract between you and us pertaining to, among other things, the sale, licensing and use of all of the services ("Services"), devices ("Device") and/or software products ("Software") made available or provided by us to you, whether directly or indirectly through our authorized resellers or distributors and any and all associated media, manuals, printed materials and "online" or other electronic documentation ("Associated Materials"). By activating, installing, purchasing or using any of the Services, Devices, Software or Associated Materials, you hereby consent to be bound by the following terms and provisions of this Agreement.

To review this Agreement section by section, please click on the specific section of interest below.

I agree to these terms of the Service Agreement and wish to continue.

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

### WELCOME TO THE DEVICE ACTIVATION PAGE.

Information submitted on this page is secure and strictly adheres to our Privacy Policy.

#### Contact Information

Information is used only by the D-Link Support Team when needed. We respect your privacy.

First Name:  Last Name:

Address:

Line 2:

City / State:  Alabama

Zip / Postal Code:  Country: United States

Timezone: (IDLW) International Date Line West

Observe Daylight Savings

E-mail Address:

Password:  Confirm Password:

Phone:

#### Security Question & Answer

Forget your password? Retrieve it by being prompted by your security question.

Security Question:   
(Example: My dogs name?)

Security Answer:   
(Example: Lassie)

#### Survey

Please take a moment to fill out the following survey.

Where did you purchase your SecureSpot? Other

#### Promotion Code

Please provide any promotional codes you may have below.

Promotional Code:

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

Username:  Password:

**D-Link**

securespot

HOME

MY ACCOUNT

SUPPORT

## Activating securespot™

Thank you for activating your securespot™ Internet Security Device.  
Please click the link below to activate your advanced security services.

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

Username:  Password:

**D-Link**

securespot

HOME

MY ACCOUNT

SUPPORT

## Downloading securespot™

Thank you for activating your securespot™ Internet Security Device.  
Please follow the directions below to enable your advanced security services.



To use the online Wizard to configure your securespot™, [click here](#)

**1** Turn off all firewalls

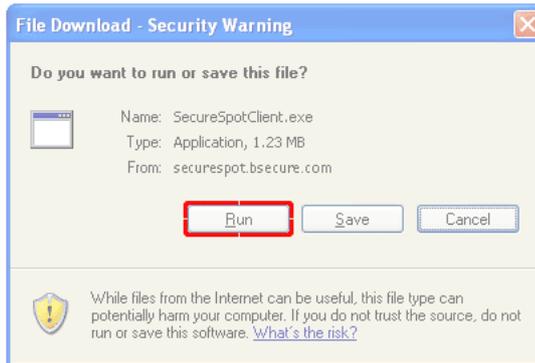
**2** Click the download button to begin installation

Select your Operating System

File name: SecureSpotClient.exe

### 3 Run the securespot setup file

A window will open asking what you want to do with a file called SecureSpotClient.exe. Click 'Run'.



You might see a confirmation message, asking if you're sure you want to run this software. Click 'Run' again.



### 4 Complete the installation.

You will be prompted to restart your computer after the installation has completed.



### 5 Launch securespot™

After the installation has finished, you can open securespot™ at any time by clicking the icon on your desktop or in your system tray.



securespot™ and the Thin Client will replace your existing PC security applications. Before you install the Thin Client, you will need to uninstall all security applications with Popup Blocker, AntiVirus Protection, Spam Blocker, and Spyware software; otherwise, it might conflict with your existing PC security applications.

I have already uninstalled the security applications

Download Thin Client

Cancel

**Program Setup** 

Thank you for installing D-Link SecureSpot Thin Client.

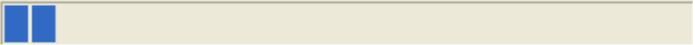
The installation has been completed successfully and your system is now protected.

If you wish to customize your settings now or in the future, please double click on the SecureSpot icon on your Windows desktop or on your system tray.



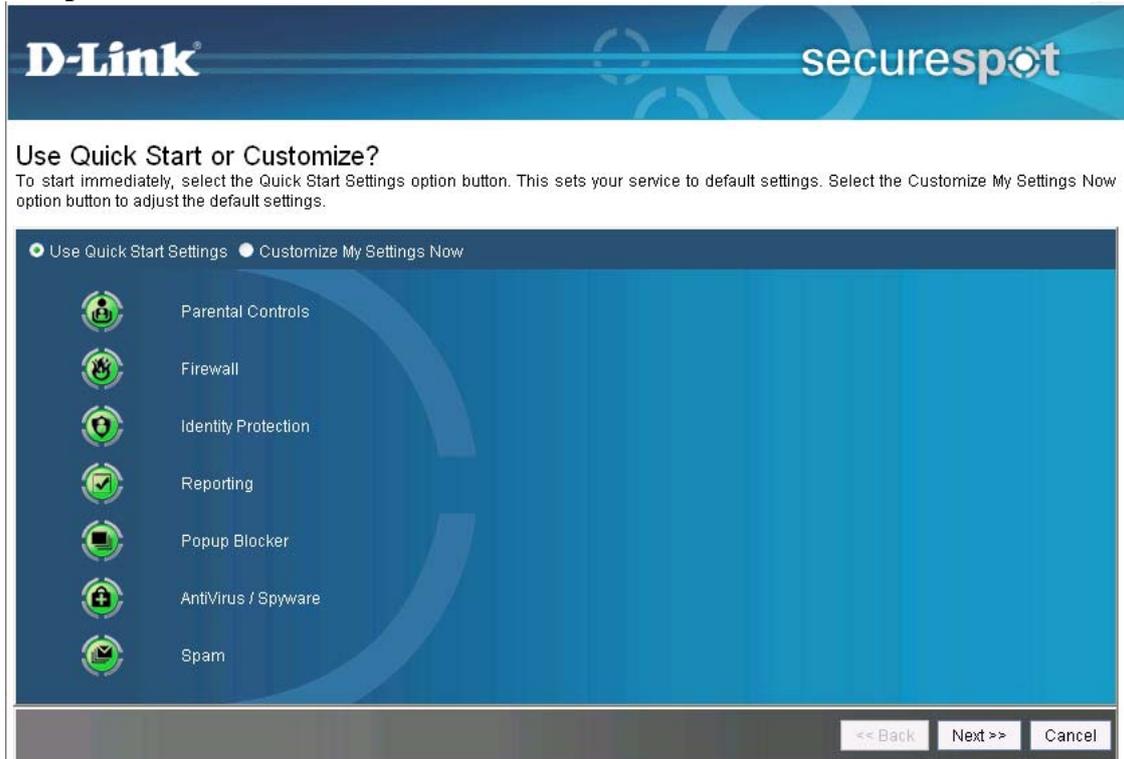
**D-Link SecureSpot Thin Client**

Please wait while downloading virus definitions...



To log into the unit to make changes, double click on the  icon in your task bar

## Setup Wizard



**D-Link** **securespot**

### Use Quick Start or Customize?

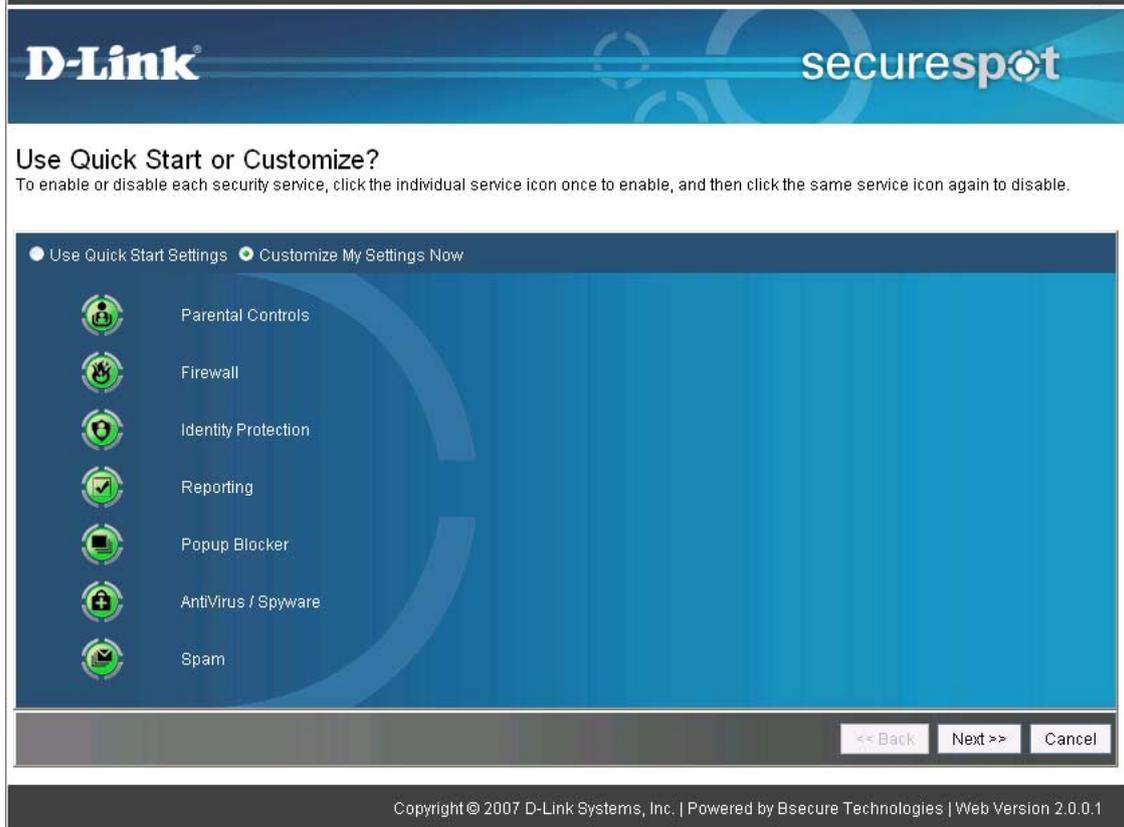
To start immediately, select the Quick Start Settings option button. This sets your service to default settings. Select the Customize My Settings Now option button to adjust the default settings.

Use Quick Start Settings  Customize My Settings Now

- Parental Controls
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam

<< Back Next >> Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1



**D-Link** **securespot**

### Use Quick Start or Customize?

To enable or disable each security service, click the individual service icon once to enable, and then click the same service icon again to disable.

Use Quick Start Settings  Customize My Settings Now

- Parental Controls
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam

<< Back Next >> Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

 **Parental Controls Setup Wizard**

Parental Controls feature protects your children from dangers of the Internet, giving you flexible control over Web sites and Internet applications.

Enabled  Disabled

**Category Template**

- Child – up to 8 years
- Youth – 9 to 12 years
- Adolescent – 13 to 17 years
- Adult – 18 years and older
- Enable Password Override

<< Back   Next >>   Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

 **Firewall Setup Wizard**

The Firewall features increases network security by blocking entry and exit points for hackers, Trojan programs, and other threats. *(You may customize the default blocked ports lists for the Low, Medium, and High Security levels.)*

Enabled  Disabled

**Security Level**

- User Defined  
*(This is the default setting.)*
- Enabled Low  
*(Firewall blocks a select group of known "problem" ports and applications.)*
- Enabled Medium  
*(Firewall blocks a large group of known "problem" ports and applications.)*
- Enabled High  
*(Firewall blocks the largest group of known "problem" ports and applications.)*
- Block Incoming Pings

<< Back   Next >>   Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

### Identity Protection Setup Wizard

The Identity Protection feature allows you to enter private information and prevent this information from being transmitted from your computer(s). All personal or private information is encrypted and contained within the device.

Enabled  Disabled

A large blue rectangular area with a subtle circular graphic on the left side, serving as the main content area for the Identity Protection Setup Wizard. At the bottom right of this area, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

### Reporting Setup Wizard

The Reporting feature creates a historical record of Web sites that can not be altered or erased. The Reporting area is where you configure and manage Internet activity reports.

Enabled  Disabled

A large blue rectangular area with a subtle circular graphic on the left side, serving as the main content area for the Reporting Setup Wizard. At the bottom right of this area, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

 **Popup Blocker Setup Wizard**

The Popup Blocker feature prevents unwanted and annoying popup windows from appearing while you surf the Internet.

Enabled  Disabled



<< Back   Next >>   Cancel

 **AntiVirus/Spyware Setup Wizard**

The AntiVirus/Spyware feature protects your network computers against viruses, trojans, worms, and spyware. This feature detects, blocks, and removes viruses and spyware that harm your computers and personal files, i.e., digital photos, financial spreadsheets, and music.

Enabled  Disabled



<< Back   Next >>   Cancel

### Spam Blocker Setup Wizard

The Spam Blocker feature allows you to define a personal "tag" for all your unwanted e-mails. This feature uses a series of techniques to "tag" unwanted e-mails with a user-defined prefix. Simply set up a rule in your Outlook, Outlook Express, or any other POP3 e-mail client to redirect this tagged e-mail to a spam folder.

Enabled  Disabled

**User-defined subject line tag**

Mark spam messages with  \*

\* Suspected junk e-mail will contain this prefix in the subject line of your incoming e-mail.

<< Back   Next >>   Cancel

Thank you! The securespot™ Setup Wizard is complete.

*At any time in the future, remember that you may change these and more settings through the "MY ACCOUNT" section of the securespot™ Web site.*

- Continue and make more changes in "My Account"
- Installation is complete!

<< Back   Finish   Cancel

### Welcome to the Secure "My Account" Web Control Center.

D-Link customers who've already registered their securespot™ use this page to change their settings, update contact info and administer their filtering and security services. (You may access this page and make changes from anywhere on the Internet.)



Email Address:

Password:  [Forget your password?](#)

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

**ACCOUNT SUMMARY**

The Account Summary option is used to view and edit contact information. This section is also the right place to download and install the latest version of the thin client security application to each computer on your network.

RICHARD ISAAC	IMPORTANT DATES
1 Giffnock avenue North Ryde, 2113 AU risaac@tpg.com.au	<b>Account Created:</b> 2/22/2007 <b>Next Billing Date:</b> 2/22/2008

**REGISTERED SYSTEMS**

The Registered Systems section is used to view and edit the list of active computers on your local network. You may also download and install the latest version of the thin client security application to each computer on your network.

**Note:** If you are re-installing the thin client, the program will first uninstall any existing programs, reboot, then install the new client.

**McAfee VirusScan** Windows

Virus and Spyware Protection

Computer Name	Description	MAC Address
TECH829-WS591XL		00:50:BA:09:65:10



<b>HOME</b>	<b>SUPPORT</b>
<ul style="list-style-type: none"> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Account Info</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Parental Control</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Firewall</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Identity Protection</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Reporting</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Popup Blocker</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> AntiVirus / Spyware</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Spam Blocker</li> </ul>	<div style="background-color: #333; color: white; padding: 5px; margin-bottom: 5px;"> <b>ACCOUNT INFO</b>                  The Account Info section is used to view and edit important contact, billing, active system and password information. The Account Summary option is the place to download thin client licenses to your computer.             </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 48%; border: 1px solid #333; padding: 5px; margin-bottom: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;"><b>ACCOUNT SUMMARY</b></div>                 The Account Summary option is used to view and edit contact information. This section is also the right place to download the thin client.             </div> <div style="width: 48%; border: 1px solid #333; padding: 5px; margin-bottom: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;"><b>BILLING INFORMATION</b></div>                 The Billing Information option is used to view and edit billing information.             </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 48%; border: 1px solid #333; padding: 5px; margin-bottom: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;"><b>CONTACT INFORMATION</b></div>                 The Contact Information section is used to view and edit important contact information.             </div> <div style="width: 48%; border: 1px solid #333; padding: 5px; margin-bottom: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;"><b>PASSWORD SECURITY</b></div>                 The Password Security section sets up security question information needed to retrieve a forgotten password.             </div> </div> <div style="border: 1px solid #333; padding: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px;"><b>CLIENT SECURITY</b></div>                 The Client Security section allows (or disallows) network computers to attach to the internet without needing the thin client software.             </div>

<b>HOME</b>	<b>SUPPORT</b>
<ul style="list-style-type: none"> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Account Info</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Parental Control</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Firewall</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Identity Protection</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Reporting</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Popup Blocker</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> AntiVirus / Spyware</li> <li style="border-bottom: 1px solid #333; padding: 2px 5px;"> Spam Blocker</li> </ul>	<div style="background-color: #333; color: white; padding: 5px; margin-bottom: 5px;"> <b>EDIT YOUR BILLING INFORMATION</b> </div> <div style="padding: 5px;"> <p><b>Credit Card Number:</b> <input type="text"/></p> <p><b>Expiration Date:</b> <input type="text" value="January"/> <input type="text" value="2007"/></p> <p><b>Credit Card Address:</b> <input type="text" value="1 Giffnock avenue"/></p> <p><b>Line 2:</b> <input type="text"/></p> <p><b>City / State / Zip:</b> <input type="text" value="North Ryde"/> <input type="text" value="2113"/></p> <p><b>Country:</b> <input type="text" value="Australia"/> <b>Currency:</b> <input type="text" value="Australian Dollar"/></p> </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**EDIT YOUR CONTACT INFORMATION**

<b>First Name:</b>	<input type="text" value="Richard"/>	<b>Last Name:</b>	<input type="text" value="Isaac"/>
<b>Address:</b>	<input type="text" value="1 Giffnock avenue"/>		
<b>Line 2:</b>	<input type="text"/>		
<b>City / State:</b>	<input type="text" value="North Ryde"/>		
<b>Zip / Postal Code:</b>	<input type="text" value="2113"/>	<b>Country:</b>	<input type="text" value="Australia"/>
<b>Timezone:</b>	<input type="text" value="(ACT) Australian Central Time"/>		
	<input checked="" type="checkbox"/> Observe Daylight Savings		
<b>E-mail Address:</b>	<input type="text" value="risaac@tpg.com.au"/>		
<b>Alt. E-mail Address:</b>	<input type="text"/>		
<b>Phone:</b>	<input type="text" value="61288991800"/>		

OK Apply Cancel

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**PASSWORD SECURITY**

The Password Security section sets up security question information needed to retrieve a forgotten password.

**Password Security**

Master Password

The Password Security section allows you to add or edit information needed to retrieve a forgotten administration password via email without having to contact Customer Support. If you forget your password and are unable to log in under My Account section, simply click on [Forgot Password?](#) link, provide the email address your account is registered under, provide the answer to your Security Question (below), and your password will be retrieved for you.

Please try to create a question and answer combination that children or other adults will not know the answer to.

<b>Security Question:</b> <small>(Example: My school mascot?)</small>	<input type="text" value="the best team in the world"/>
<b>Security Answer:</b> <small>(Example: Jaguars)</small>	<input type="text" value="manchester united"/>

OK Apply Cancel

HOME

SUPPORT

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**PASSWORD SECURITY**

The Password Security section sets up security question information needed to retrieve a forgotten password.

Password Security   
  **Master Password**

The Master Password is the password you created when registering your securespot™. This is the password that is used to login to My Account.

To better protect your account, make sure that your password is memorable for you but difficult for others to guess. Do not share your password with anyone, and never use the same password that you've used in the past.

**Current Password:**

**New Password:**

**Confirm Password:**

HOME

SUPPORT

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**CLIENT SECURITY**

The Client Settings section provides an option to allow (or disallow) network computers to attach to the internet without needing the thin client software. Example: If you want to prevent the attachment of new computers without AntiVirus and Spyware protection, choose Medium or High Security.

- Low Security** - Allow computers to attach to the network without requiring a thin client install for AV and Spyware. This works well in public areas and hotspots where many users come and go. If Parental Controls are enabled, it is possible to bypass protection by removing the securespot™ device or attaching to another network.
- Medium Security** - (default) Automatically requires all computers to have a thin client install for AV and Spyware, but does allow computers to roam outside the local network. If Parental Controls are enabled, it is possible to bypass protection by removing the securespot™ device or attaching to another network.
- High Security** - Automatically prompt new computers with a registration page that requires a thin client install for AntiVirus and Spyware protection. If Parental Controls are enabled, this ensures that children can NOT circumvent the filtering protection by removing the device from the network. If computers roam outside the network, they require the admin password to connect to the Internet.

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker



**PARENTAL CONTROLS**

The Parental Controls feature protects your home from dangers of the Internet, giving you flexible control over websites and internet applications.

Enable Parental Controls

**CATEGORIES**

The Categories section allows you to customize the list of default categories that are blocked.

**WEBSITE LISTS**

The Website Lists section allows you create custom lists of blocked / unblocked sites.

**OPTIONS**

The Options section allows you enable key filtering features of Password Override and Safety Lock.

**SCHEDULING**

The Scheduling section allows you to control Internet access by days and times of the day.

**PROFILES**

The Group Profiles section allows you to manage settings by global network, each computer and/or by person.

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**CATEGORIES**

THESE SETTINGS APPLY TO Local Network

The Categories section allows you to customize the list of categories blocked by default. Check (or uncheck) the types of sites you'd like to see blocked.

Age Group: Adult (18+)

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Alcohol                 | <input type="checkbox"/> Health/Medical            | <input checked="" type="checkbox"/> Pornography |
| <input type="checkbox"/> Art                     | <input type="checkbox"/> Holistic                  | <input type="checkbox"/> R Rated                |
| <input type="checkbox"/> Automobile              | <input type="checkbox"/> Humor                     | <input type="checkbox"/> Real Estate            |
| <input type="checkbox"/> Banner Ads              | <input type="checkbox"/> Information Technology    | <input type="checkbox"/> Recreational           |
| <input type="checkbox"/> Books and Literature    | <input type="checkbox"/> Instant Messaging         | <input type="checkbox"/> Reference              |
| <input type="checkbox"/> Chat                    | <input type="checkbox"/> Internet Radio            | <input type="checkbox"/> Religion               |
| <input checked="" type="checkbox"/> Child Porn   | <input type="checkbox"/> Internet Service Provider | <input type="checkbox"/> Religious Opinion      |
| <input type="checkbox"/> Comics                  | <input type="checkbox"/> Legal                     | <input type="checkbox"/> Search Engine          |
| <input type="checkbox"/> Community Organizations | <input type="checkbox"/> Lifestyle                 | <input type="checkbox"/> Self Defense           |

Default Settings

OK Save Cancel

HOME

SUPPORT

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**WEBSITE LISTS** THESE SETTINGS APPLY TO Local Network

The Website Lists section allows you create custom lists of blocked / unblocked sites. Choose either the Allowed and Blocked tab, then enter the web site URL to create your custom lists.

Allowed Websites	Blocked Websites	Website List Available Space 99.00 %

Enter new URL and press Add:  \* Allow only these sites

\*Please Note: If you check the "Allow only these sites" option, it will limit the user to your custom list only!

HOME

SUPPORT

-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker

**WEBSITE LISTS** THESE SETTINGS APPLY TO Local Network

The Website Lists section allows you create custom lists of blocked / unblocked sites. Choose either the Allowed and Blocked tab, then enter the web site URL to create your custom lists.

Allowed Websites	Blocked Websites	Website List Available Space 99.00 %

Enter new URL and press Add:  \* Block sites that are not categorized

\*Please Note: If you check the "Block sites that are not categorized" option, you will only be able to access sites with known categories.

**HOME** | **SUPPORT**

Account Info | Parental Control | Firewall | Identity Protection | Reporting | Popup Blocker | AntiVirus / Spyware | Spam Blocker

**PARENTAL CONTROLS OPTIONS** THESE SETTINGS APPLY TO **Local Network**

The Options section allows you enable key filtering features of Password Override and Safety Lock.

**STATUS / PASSWORD OVERRIDE**

This option will allow you to set up unique computer and user profiles instead of one global policy for all. Leaving this unchecked is simpler but less flexible.

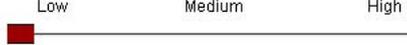
Enable Parental Controls (Per Profile)

This option will allow you to type in the administrator password to override the block page and access blocked web sites.

Enable Password Override for Blocked Sites

**SAFETY LOCK OPTION**

Low Medium High



Safety Lock Option - What does it mean?

This option helps prevent attempts to bypass the Content Filter. It forces the user to restart the computer after specified number of attempts result in blocked pages. Please move the above slider to enable this option and determine what criteria will be used for the safety lock.

Default Settings OK Save Cancel

**HOME** | **SUPPORT**

Account Info | Parental Control | Firewall | Identity Protection | Reporting | Popup Blocker | AntiVirus / Spyware | Spam Blocker

**SCHEDULING** THESE SETTINGS APPLY TO **Local Network**

The Scheduling section allows you to control Internet access by days and times of the day. Click on the black slider controls and move them to adjust times. You can drag one slider over another to set blocked times in the middle of the day. ■ Blocked ■ Unblocked

Day	6 AM	12 PM	6 PM	Status	Time Range
Sunday				Unblocked	12:00 AM to 12:00 AM
Monday				Unblocked	12:00 AM to 12:00 AM
Tuesday				Unblocked	12:00 AM to 12:00 AM
Wednesday				Unblocked	12:00 AM to 12:00 AM
Thursday				Unblocked	12:00 AM to 12:00 AM
Friday				Unblocked	12:00 AM to 12:00 AM
Saturday				Unblocked	12:00 AM to 12:00 AM

Reset OK Save Cancel

**Note:** You have the ability to create individual schedules by network, computer or user profile level by using the drop down list in the top right corner.

HOME
SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

### PROFILES

Control security policies for each computer or control them for each user.

Devices
Computers
Users

This window displays system information for your Securespot device. Click on the edit icon to the right to change the description.

Description	Signup Date	Last Modified
Local Network	2/22/2007 12:09:40 AM	2/22/2007 7:35:40 AM

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

HOME
SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

### PROFILES

Control security policies for each computer or control them for each user.

Devices
Computers
Users

This window displays all the registered computers on your Securespot network. Click on the edit icon to the right to add this computer to the group profile list.

MAC Address	Computer Name	Description
00:50:BA:09:65:10	TECH829-WS591XL	

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

<b>HOME</b>	<b>SUPPORT</b>
-------------	----------------

Account Info | Parental Control | Firewall | Identity Protection | Reporting | Popup Blocker | AntiVirus / Spyware | Spam Blocker

**PROFILES**  
 Control security policies for each computer or control them for each user.

Device Group	Computer Group	User Group

Devices | Computers | Users

This window lists all created user profiles. Click on the Add User Profile button on the far right to create a new user profile.

Click on the Associate Windows Profiles button to automatically link this profile to a Windows login. By doing this, the user will log in automatically to his/her personal settings when logging into Windows.

Profile  
richard

**Max Profiles: 4**
Associate Windows Profiles
Add User Profile

You must have at least one client (computer) installed in order to use profiles (users).

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

<b>HOME</b>	<b>SUPPORT</b>	<b>WIZARD</b>	<b>HELP</b>
-------------	----------------	---------------	-------------

Account Info | Parental Control | Firewall | Identity Protection | Reporting | Popup Blocker | AntiVirus / Spyware | Spam Blocker

**PERSONAL FIREWALL OPTIONS**  
 The Firewall increases network security by blocking entry and exit points for hackers, Trojan programs and other threats.  
 Enable Firewall

<b>SECURITY SETTINGS</b> Adjust default port lists commonly used by malicious code or create custom lists.	<b>SOFTWARE BLOCKING</b> Control the execution of unknown or undefined software.
<b>SOFTWARE SELECTIONS</b> Control usage of messaging, P2P and other popular programs known as security risks.	<b>DOWNLOAD BLOCKING OPTIONS</b> Control different file types entering your network with this advanced feature.
<b>INTRUSION DETECTION</b> View or modify the permissions for all Undefined Internet-based Applications.	

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

HOME
SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

SECURITY SETTINGS
THESE SETTINGS APPLY TO YOUR LOCAL NETWORK

**Security Level**

User Defined
  Low
  Medium
  High

The firewall has three levels of pre-set port lists. These settings block ports (or backdoors) commonly used by malicious code. In the Blocked Ports and Allowed Ports list below, advanced users may adjust port settings according to their custom needs.

Block incoming pings

Allowed Ports
Blocked Ports
Port Templates

INCOMING TCP PORTS

Port Number	Description

INCOMING UDP PORTS

Port Number	Description

Add New Allowed TCP Port Port Number:  Add Port(s)

To delete a port, click the trash bin icon next to the port number. To add a port, type the number in Add New Port and click the Block Port button, then Apply or OK to save and exit. OK Save Cancel

HOME
SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

SECURITY SETTINGS
THESE SETTINGS APPLY TO YOUR LOCAL NETWORK

**Security Level**

User Defined
  Low
  Medium
  High

The firewall has three levels of pre-set port lists. These settings block ports (or backdoors) commonly used by malicious code. In the Blocked Ports and Allowed Ports list below, advanced users may adjust port settings according to their custom needs.

Block incoming pings

Allowed Ports
Blocked Ports
Port Templates

OUTGOING TCP PORTS

Port Number	Description

OUTGOING UDP PORTS

Port Number	Description

Add New Allowed TCP Port Port Number:  Add Port(s)

To delete a port, click the trash bin icon next to the port number. To add a port, type the number in Add New Port and click the Block Port button, then Apply or OK to save and exit. OK Save Cancel

HOME

SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

SECURITY SETTINGS

THESE SETTINGS APPLY TO YOUR LOCAL NETWORK

Security Level

User Defined  Low  Medium  High

The firewall has three levels of pre-set port lists. These settings block ports (or backdoors) commonly used by malicious code. In the Blocked Ports and Allowed Ports list below, advanced users may adjust port settings according to their custom needs.

Block incoming pings

Allowed Ports    Blocked Ports    **Port Templates**

- Gaming
  - Games
    - Battlefield 2
    - Counter Strike
    - Everquest
    - Final Fantasy XI
    - World of Warcraft
  - Systems
    - PlayStation 2
    - Xbox 360 and Xbox Live
  - Skype
- TiVo Controls
  - TiVo
  - TiVoToGo
- VoIP Controls
  - Vonage

Add New    Allowed    TCP    Port    Port Number: 0    Add Port(s)

To delete a port, click the trash bin icon next to the port number. To add a port, type the number in Add New Port and click the Block Port button, then Apply or OK to save and exit.    OK    Save    Cancel

HOME

SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

SOFTWARE BLOCKING

THESE SETTINGS APPLY TO Local Network

The Software Blocking section allows you to control the execution of software that is not already defined in an approved list of known software.

- Block unknown software
- Allow unknown software
- Prompt for action concerning unknown software

Default Settings

OK    Save    Cancel

**HOME** | **SUPPORT**

- Account Info
- Parental Control
- Firewall**
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

**SOFTWARE SELECTIONS** THESE SETTINGS APPLY TO Local Network

The Software Selections section allows you to control usage of several messaging, Peer to Peer (P2P) and other popular programs known as possible security and/or safety risks. Check the boxes of software you wish to block.

Application Name	Category
<input checked="" type="checkbox"/> Adium	Instant Messaging
<input checked="" type="checkbox"/> Adware/Spyware	Adware/Spyware
<input type="checkbox"/> AOL IM	Instant Messaging
<input checked="" type="checkbox"/> Ares	Peer-to-peer
<input checked="" type="checkbox"/> Bear Share	Peer-to-peer
<input checked="" type="checkbox"/> BitTorrent	Peer-to-peer
<input checked="" type="checkbox"/> Bopup Messenger	Instant Messaging

Default Settings OK Save Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

**HOME** | **SUPPORT**

- Account Info
- Parental Control
- Firewall**
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

**DOWNLOAD BLOCKING OPTIONS** THESE SETTINGS APPLY TO Local Network

Download Options section allows advanced control of which files are downloaded onto your systems. For example, you would like user "Juanita" to be prevented from downloading mp3 and mpeg file types.

Block all FTP downloads  
 Block all HTTP (web) based downloads

---

Choosing to block the following file types will prevent any download of all files of that type.

<input type="checkbox"/> au	<input type="checkbox"/> doc	<input type="checkbox"/> jpg	<input type="checkbox"/> ppt	<input type="checkbox"/> tiff
<input type="checkbox"/> avi	<input type="checkbox"/> exe	<input type="checkbox"/> js	<input type="checkbox"/> ra	<input type="checkbox"/> bt
<input type="checkbox"/> bmp	<input type="checkbox"/> gif	<input type="checkbox"/> movie	<input type="checkbox"/> ram	<input type="checkbox"/> wav
<input type="checkbox"/> cab	<input type="checkbox"/> gz	<input type="checkbox"/> mp3	<input type="checkbox"/> rm	<input type="checkbox"/> wmf
<input type="checkbox"/> class	<input type="checkbox"/> gzip	<input type="checkbox"/> mpeg	<input type="checkbox"/> swf	<input type="checkbox"/> xml
<input type="checkbox"/> css	<input type="checkbox"/> jar	<input type="checkbox"/> mpg	<input type="checkbox"/> tar	<input type="checkbox"/> xsl
<input type="checkbox"/> dat	<input type="checkbox"/> java	<input type="checkbox"/> pdf	<input type="checkbox"/> tgz	<input type="checkbox"/> zip
<input type="checkbox"/> dll	<input type="checkbox"/> jpeg	<input type="checkbox"/> png	<input type="checkbox"/> tif	

Default Settings OK Save Cancel

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

**D-Link SecureSpot Thin Client (Control Center)**

## Internet Application List

Highlight the file name and select the permission level by clicking on the options at lower right-hand corner.

Program	Product Name	Permission

**Permissions**

D-Link
securespot

HOME	SUPPORT	WIZARD	HELP		
<ul style="list-style-type: none"> <li> Account Info</li> <li> Parental Control</li> <li> Firewall</li> <li style="background-color: #0070C0; color: white;"> Identity Protection</li> <li> Reporting</li> <li> Popup Blocker</li> <li> AntiVirus / Spyware</li> <li> Spam Blocker</li> </ul>	<div style="background-color: #0070C0; color: white; padding: 5px; margin-bottom: 5px;"> <b>IDENTITY PROTECTION</b>            Help stop identity theft by preventing sensitive personal information from being sent to unauthorized destinations. (All information is encrypted and stored securely on the Securespot device.)  <input checked="" type="checkbox"/> Enable Identity Protection         </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> <div style="background-color: #0070C0; color: white; padding: 2px;"> <b>PROTECTED INFORMATION</b> </div>           Enter private information to be protected.         </td> <td style="width: 50%; padding: 5px;"> <div style="background-color: #0070C0; color: white; padding: 2px;"> <b>TRUSTED SITES</b> </div>           This is the list of sites that are allowed to access the Protected data on this computer.         </td> </tr> </table>			<div style="background-color: #0070C0; color: white; padding: 2px;"> <b>PROTECTED INFORMATION</b> </div> Enter private information to be protected.	<div style="background-color: #0070C0; color: white; padding: 2px;"> <b>TRUSTED SITES</b> </div> This is the list of sites that are allowed to access the Protected data on this computer.
<div style="background-color: #0070C0; color: white; padding: 2px;"> <b>PROTECTED INFORMATION</b> </div> Enter private information to be protected.	<div style="background-color: #0070C0; color: white; padding: 2px;"> <b>TRUSTED SITES</b> </div> This is the list of sites that are allowed to access the Protected data on this computer.				

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

D-Link SecureSpot Thin Client (Control Center)

### Identity Protection: Protected Information

This is the list of private data that are encrypted and stored on this computer. It could include credit card numbers, passwords, phone numbers etc. Please use the Add / Remove / RemoveAll button to edit the list.

Enter private data and click Add

Protected Information

D-Link SecureSpot Thin Client (Control Center)

### Identity Protection: Trusted Sites

The protected data stored on this computer can be sent to or accessed by the list of sites below. Please use the Add / Remove / RemoveAll button to modify the list.

Enter the address of a web site and click Add

Trusted Sites

<b>HOME</b>	<b>SUPPORT</b>	<b>WIZARD</b>	<b>HELP</b>
-------------	----------------	---------------	-------------

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

**TAMPER PROOF REPORTING OPTIONS**

The Reporting Option creates a historical record of web sites that can not be altered or erased. Use this area to enable and configure reporting.

Enable Network Reporting

**ARCHIVED REPORTS**

February 2007						
S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	1	2	3
4	5	6	7	8	9	10

■ No Bad Content
 ■ Questionable Content
 ■ Bad Content Blocked

**Archive Date:** 2/22/2007  
**Rating:** No Data Available

**Child Hits:** N/A  
**Youth Hits:** N/A  
**Adult Hits:** N/A  
**Hits:** N/A

Use this at-a-glance calendar to spot attempted blocked sites. Click on any colored block to display that day's detailed history.

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1

D-Link

securespot

<b>HOME</b>	<b>SUPPORT</b>	<b>WIZARD</b>	<b>HELP</b>
-------------	----------------	---------------	-------------

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

**POPUP BLOCKER OPTIONS**

The Popup Blocker prevents unwanted and annoying popup screens from appearing while you surf the Internet.

Enable Popup Blocker

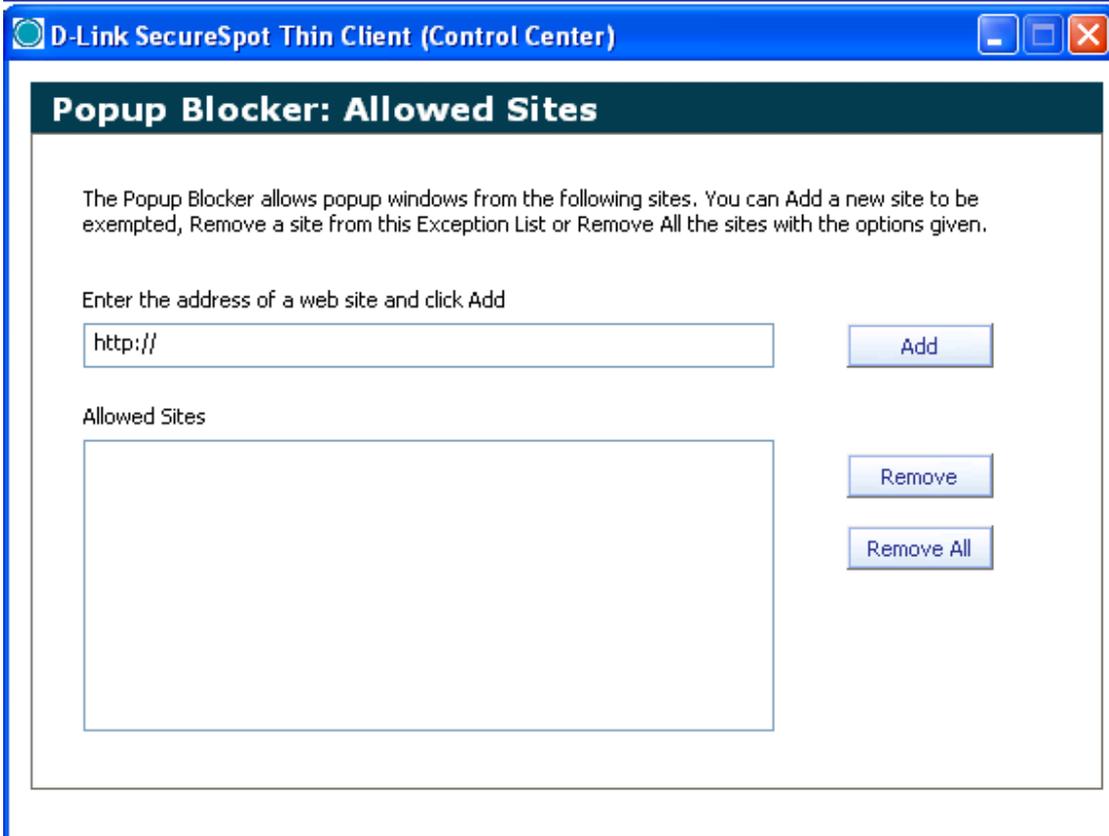
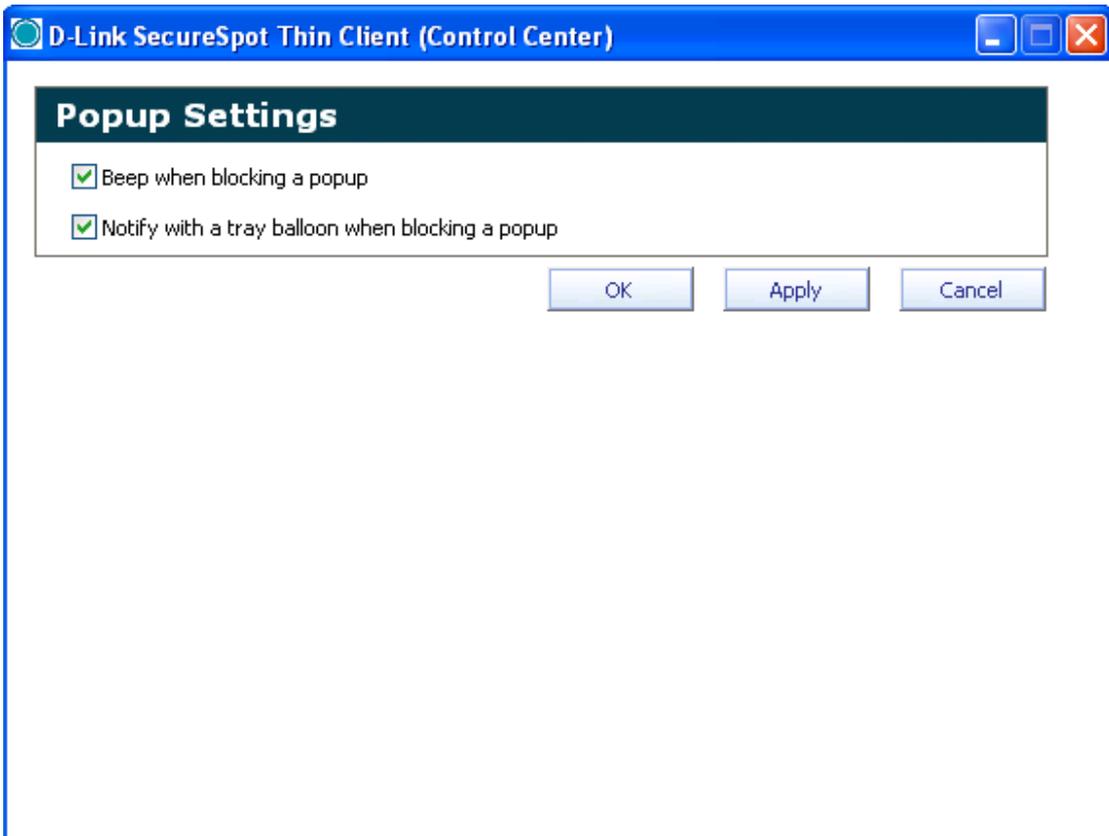
**SETTINGS**

Advanced options for popup control.

**ALLOW LIST**

View and edit the list of allowed sites to allow popups.

Copyright © 2007 D-Link Systems, Inc. | Powered by Bsecure Technologies | Web Version 2.0.0.1



-  Account Info
-  Parental Control
-  Firewall
-  Identity Protection
-  Reporting
-  Popup Blocker
-  AntiVirus / Spyware
-  Spam Blocker



**ANTIVIRUS / SPYWARE**

Advanced security that protects your network computers against viruses, trojans, worms and spyware.  
 Enable AntiVirus / Spyware

**SCAN MY COMPUTER**

Perform a virus scan on the programs and files on your computer.

**SCHEDULED SCANS**

Create scheduled scans that can be performed automatically.

**SCAN HISTORY LOG**

View the history log of the scans performed on this computer.

**UPDATES**

Manually update your virus definition files if necessary.

**THREAT CENTER**

Learn everything you need to know about protecting your environment.

**THREAT LIBRARY**

Search for information on viruses.

Note: If you currently have an AntiVirus product installed, (including McAfee®), we strongly recommend that you first uninstall the AntiVirus and also any AntiSpyware software before installing the securespot™ software.



Virus and Spyware Protection

**D-Link SecureSpot Thin Client (Control Center)** \_ □ ×

**Scan My Computer**

- ⊕ A:\
- ⊕ C:\
  - Documents and Settings
  - MSOCache
  - Program Files
  - RECYCLER
  - System Volume Information
  - WINDOWS
- D:\
- E:\

**SCAN OPTIONS**

Choose file extensions to scan.

All

Supplied Extensions (separate by ;)

\* \*

---

**ACTION**

Disinfect the file ▾

---

**LAST SCAN**

Not Available

Scan Scan All Cancel

**D-Link SecureSpot Thin Client (Control Center)**

### Scheduled Scans

Last Scan: Not Available  
Specify the times you want to run the automated scans on your computer.

Name	Time	Description
Default daily scan.	Daily	Default daily scan.

**D-Link SecureSpot Thin Client (Control Center)**

### Scan History Log

AntiVirus logs show the history of the scans performed on your computer.

Start	Stop	Type	Status	Files	Viruses	Err
-------	------	------	--------	-------	---------	-----



## AntiVirus Updates

Welcome to your AntiVirus Update System.

	Last Update:	02/21/2007
	Last Scan:	Not Available
	# of Detectable Viruses:	15276
	Virus Engine Version:	5294
	Virus Definition Date:	02/21/2007

When your Internet Protection Service reauthenticates, it checks and updates the AntiVirus Definition files if necessary.

- Do not check for updates during authentication.
- Do not ask when there are updates (automatically download and install)

Click Next to check for updates (Please note that the Control Center will be closed during this operation).

Next

Close

# The Secure Spot will redirect you to a McAfee website when clicking on THREAT CENTRE & THREAT LIBRARY TABS.

Address [http://www.mcafee.com/us/threat\\_center/default.asp](http://www.mcafee.com/us/threat_center/default.asp) Go

**McAfee** Global Sites \ About McAfee \ Threat Center \ Contact Us \ Search this

[Home & Home Office](#) \ [Small & Medium Business](#) \ [Enterprise](#) \ [Partners](#)

---

## McAfee Threat Center

Arm yourself with up-to-the-minute knowledge about **threats** and **vulnerabilities** from McAfee Avert® Labs.

**BREAKING ADVISORY**

February 14, 2007. McAfee Avert Labs has identified an unpatched vulnerability in Microsoft Word upon review of a user-submitted sample. This vulnerability comes on top of recently patched vulnerabilities in PowerPoint, Excel and Word. Office users should exercise great care opening Office documents from unknown sources or that arrive unexpectedly.

[Learn More](#)

February 13, 2007. Microsoft has released twelve Security Bulletins for February. The affected components include Microsoft Windows, Microsoft Office, Microsoft Visual Studio, Microsoft Step-by-Step Interactive Training, Microsoft Antivirus, and Microsoft Data Access Components. Some of the flaws addressed were previously public. These include Microsoft Data Access Components (CVE-2006-5559), Microsoft Word (CVE-2006-5994, CVE-2006-6456, CVE-2007-6561, CVE-2007-0515), and Microsoft Excel (CVE-2007-0671).

[Learn More](#)

Current Malware		Current Vulnerabilities	
	Date Published		Date Public
Backdoor-DKT	02 Feb 2007	MS07-010 MS AV Vuln	13 Feb 2007
Downloader-BAIM711	19 Jan 2007	MS Word RCE	08 Feb 2007
W32/Stration.gen.ldr	07 Nov 2006	MS07-015 MS Excel RCE	01 Feb 2007
JS/Downloader-AUD	15 Jun 2006	MS07-014 Word Mail F..	25 Jan 2007
W32/Mytob.gen@MM	02 Mar 2005	MS07-014 Word Count ..	12 Dec 2006
<a href="#">See Recent Malware</a>		MS07-014 MS Mail Dat..	09 Dec 2006

**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 user systems.

**McAfee Avert Labs Sage Report**



**Paying a Price for the Open Source Advantage**

McAfee Avert Labs debuts new security journal. The premier issue examines the role of open source in malware development.

[Download Sage](#)

**McAfee Avert Labs Blog**

Read about security research as it happens

**McAfee Security Updates**

Am I up to date? Read about McAfee Product Content releases.

**Threat Center Resources**

- Get Foundstone free tools
- Tools and utilities
- Whitepapers
- Security advisories

Address <http://vil.nai.com/vil/default.aspx> Go

**McAfee** Global Sites \ Threat Center \ About McAfee \ Cont

[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	15 Jan 2007	Downloader-BAIM711	21 Jan 2007
Downloader-BAIM711	21 Jan 2007	JS/Downloader-AUD	06 Oct 2006
Generic Malware.alzip	01 Jun 2005	JS/Exploit-BO.gen	01 Oct 2006
W32/Bagle.gen!Salty	28 Feb 2006	JS/Wonka	09 Oct 2006
W32/Mytob.gen@MM	18 May 2005	Puper	29 Sep 2005
W32/Stration.gen.ldr	24 Dec 2006	VBS/Psyme	08 Oct 2006
<a href="#">View Threat Key</a>		W32/Mytob.gen@MM	18 May 2005
		<a href="#">View Threat Key</a>	

**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

**Resources**

- Anti-Spyware Coalition
- AV-Comparatives
- ICSA Labs
- Stay Safe Online
- Virus Bulletin

HOME

SUPPORT

WIZARD

HELP

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker



SPAM

LAUNCH WIZARD

The Spam feature saves time and protects your computers by helping redirect junk, phishing and pharming emails to spam folders.

Enable the Spam Blocker

SPAM TAG



Use this area to define a personal "tag" for unwanted emails. This feature uses a series of techniques to "tag" unwanted emails with a user defined prefix. Suspected junk email will contain this prefix in the subject line of your incoming mail. Simply set up a rule in your Outlook, Outlook Express or any other POP3 email client to redirect this tagged email to a spam folder.

HOME

SUPPORT

- Account Info
- Parental Control
- Firewall
- Identity Protection
- Reporting
- Popup Blocker
- AntiVirus / Spyware
- Spam Blocker

SPAM TAG

THESE SETTINGS APPLY TO YOUR LOCAL NETWORK

Spam Subject Tag:

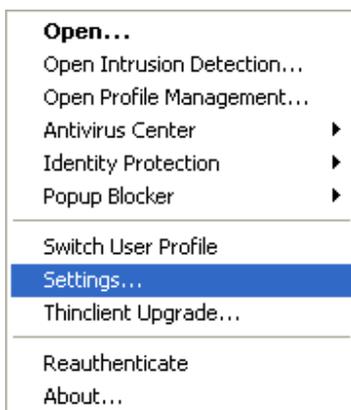
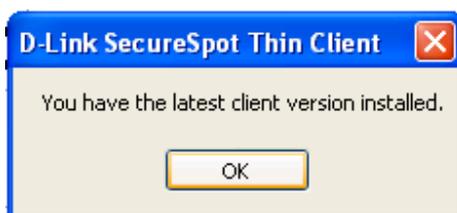
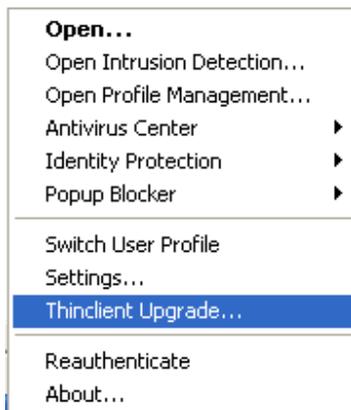
Use this area to define a personal "tag" for unwanted emails. The default is "SPAM".

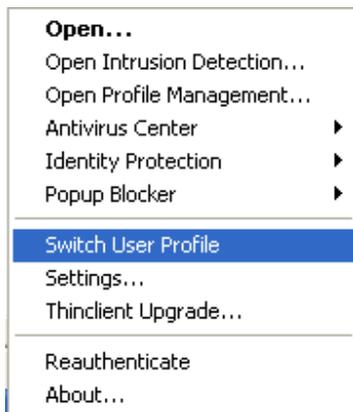
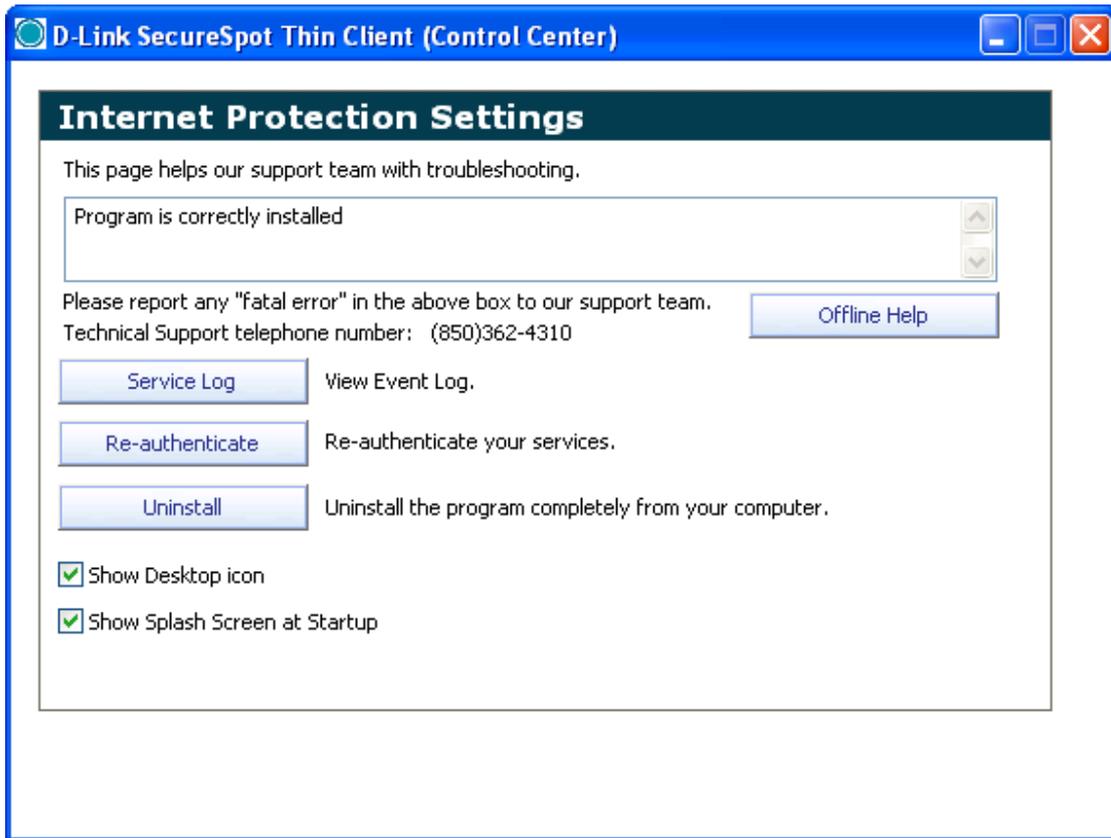
OK

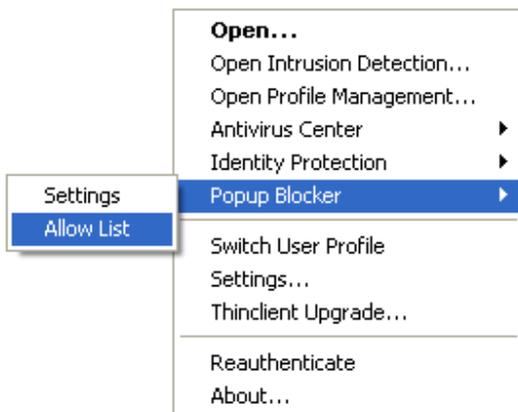
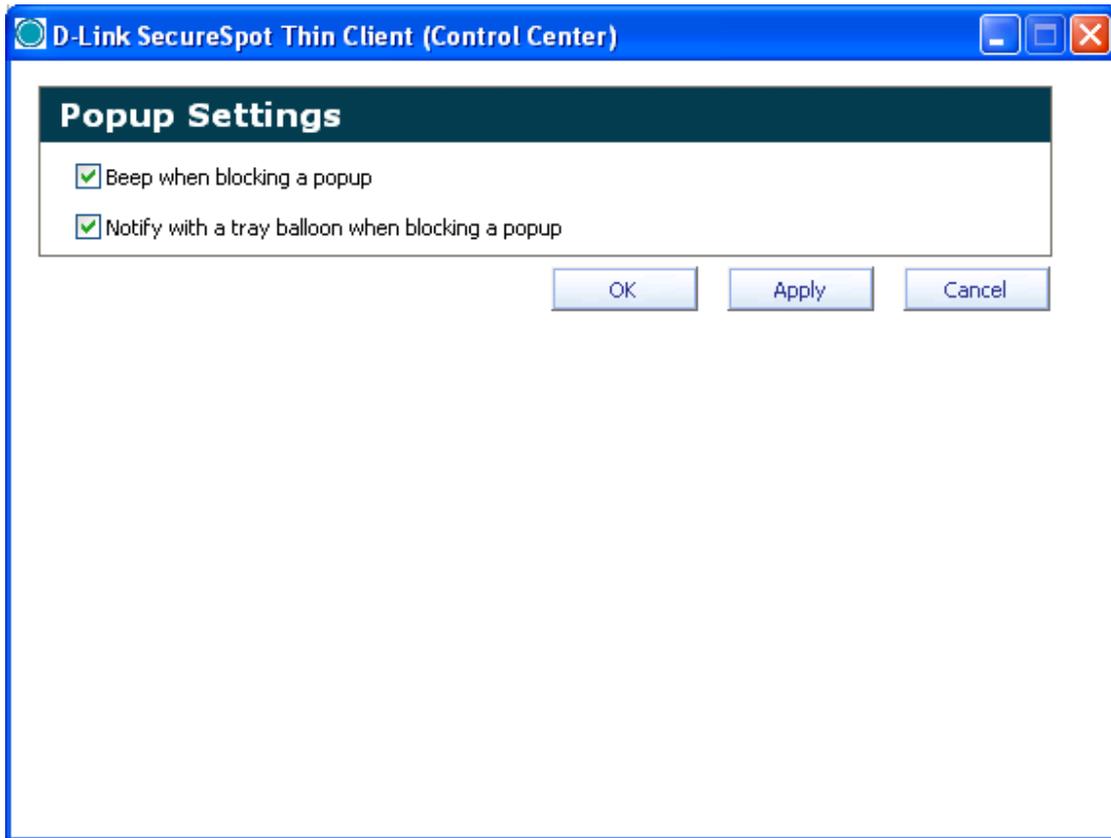
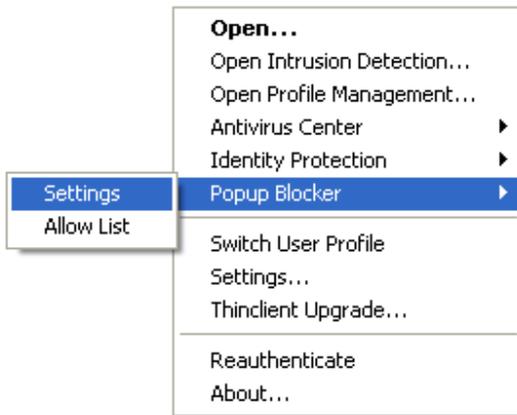
Save

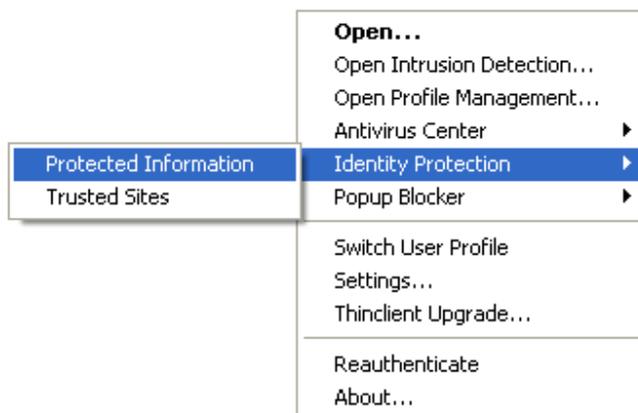
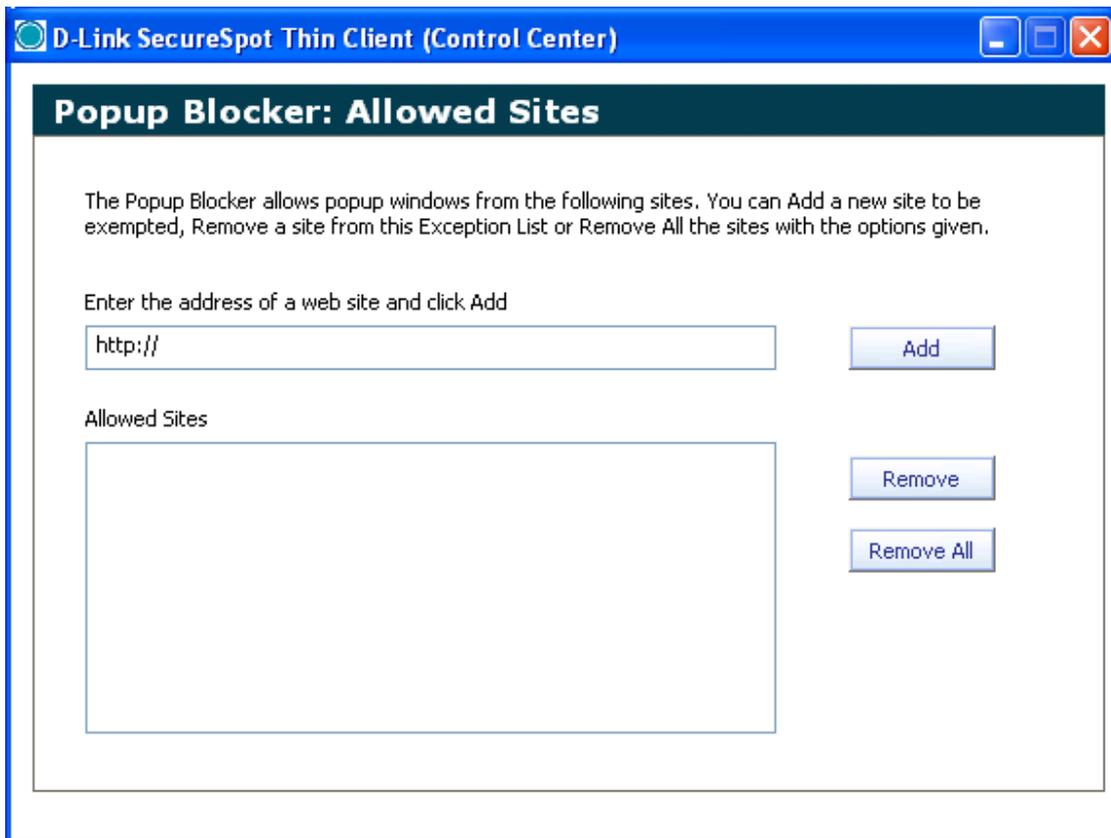
Cancel

## Thin Client screenshots









D-Link SecureSpot Thin Client (Control Center)



### IDENTITY PROTECTION: PROTECTED INFORMATION

Prevent unwanted disclosure of your private and personal information. All personal or private information is encrypted and contained within the device.

Administrative Password:

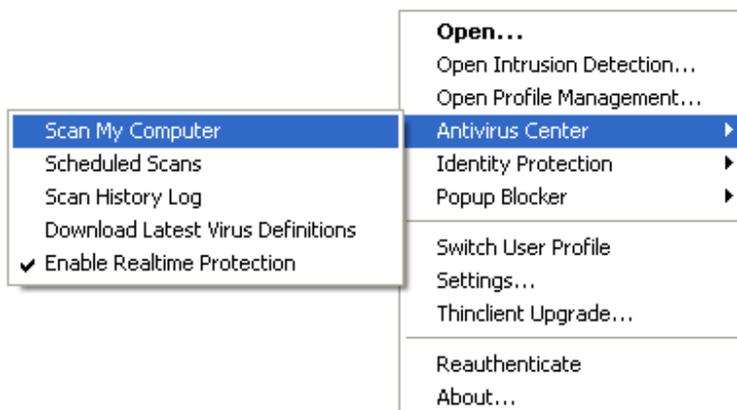
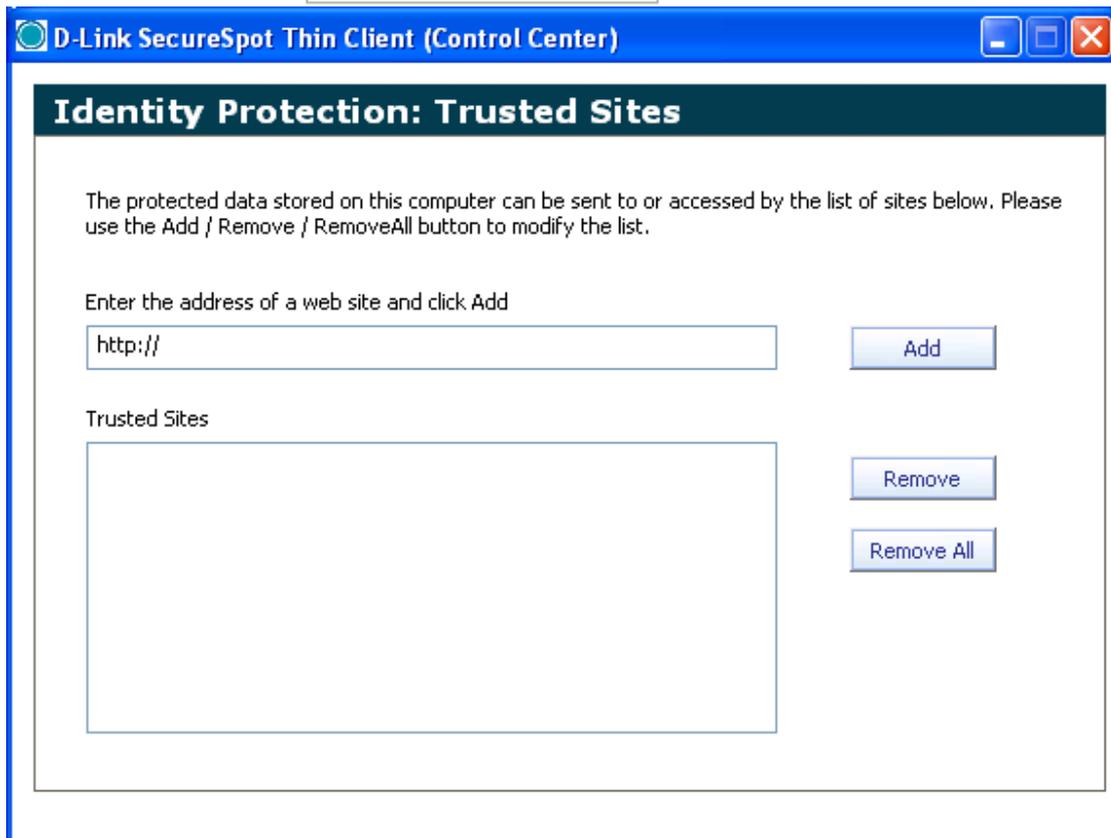
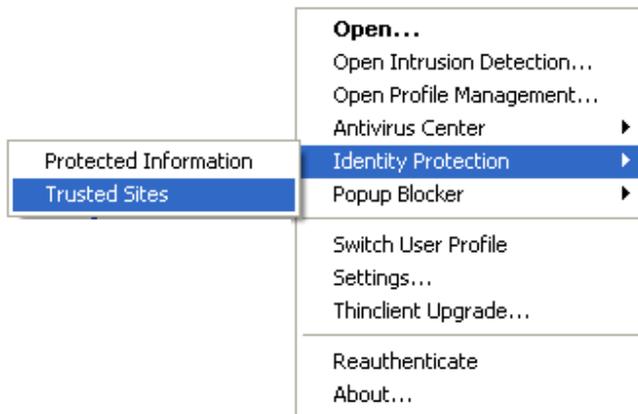
D-Link SecureSpot Thin Client (Control Center)

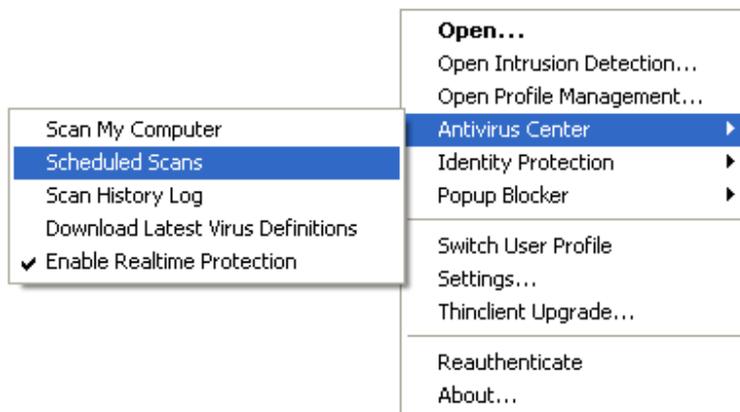
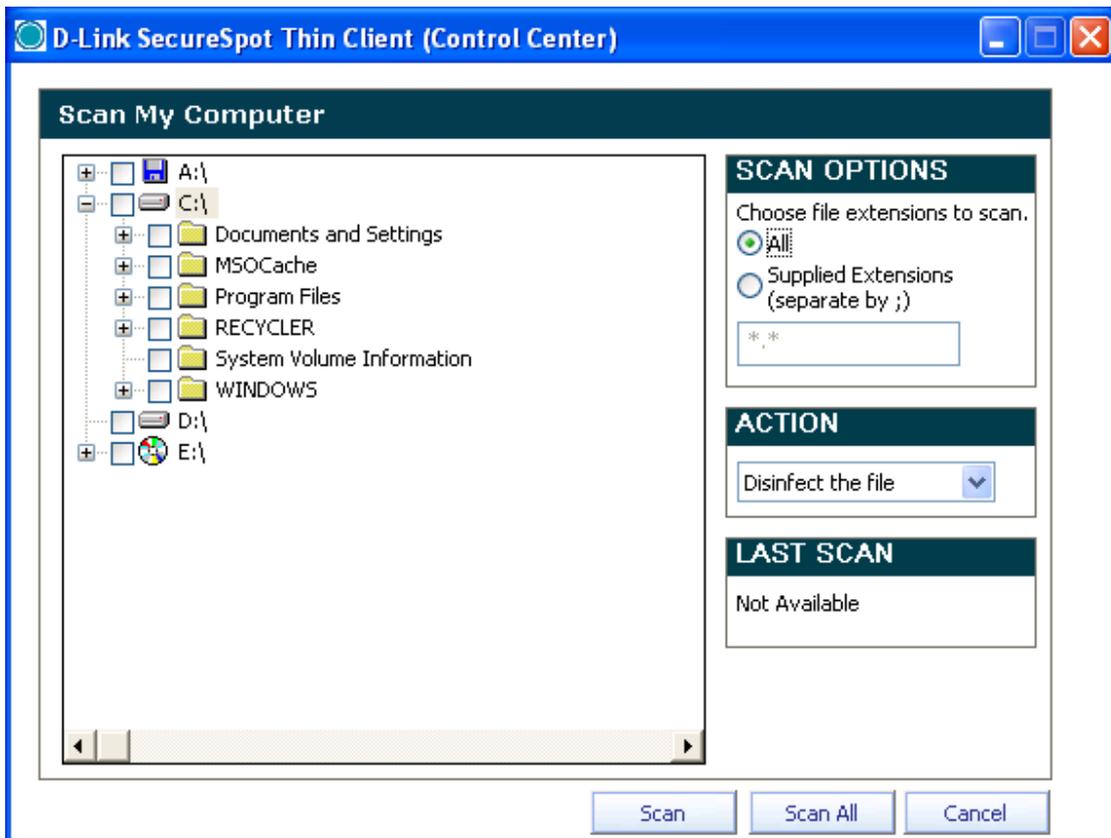
### Identity Protection: Protected Information

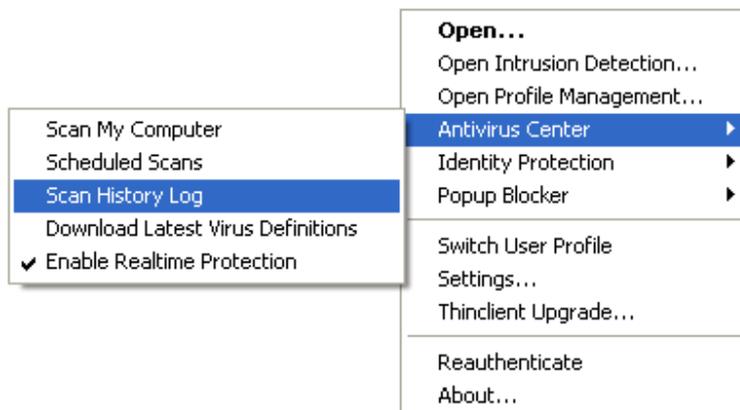
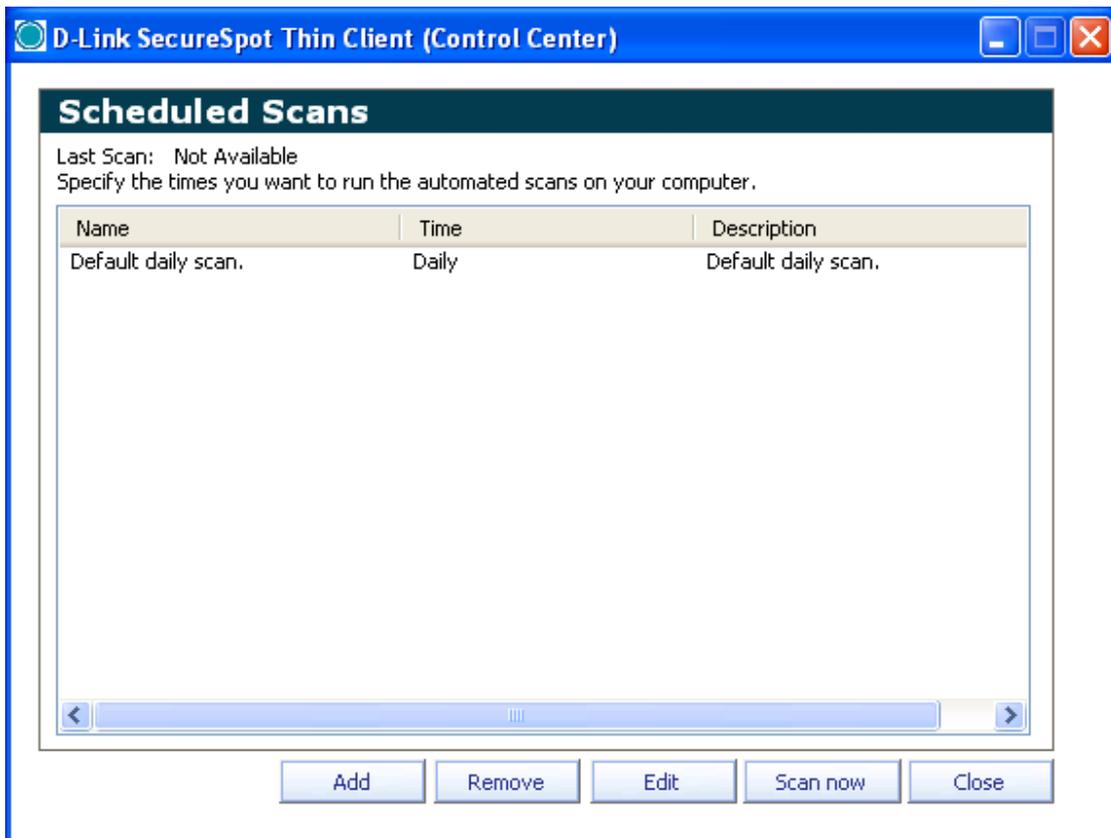
This is the list of private data that are encrypted and stored on this computer. It could include credit card numbers, passwords, phone numbers etc. Please use the Add / Remove / RemoveAll button to edit the list.

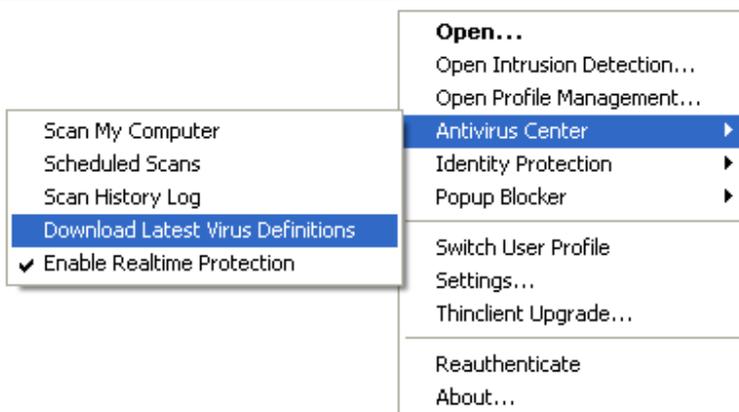
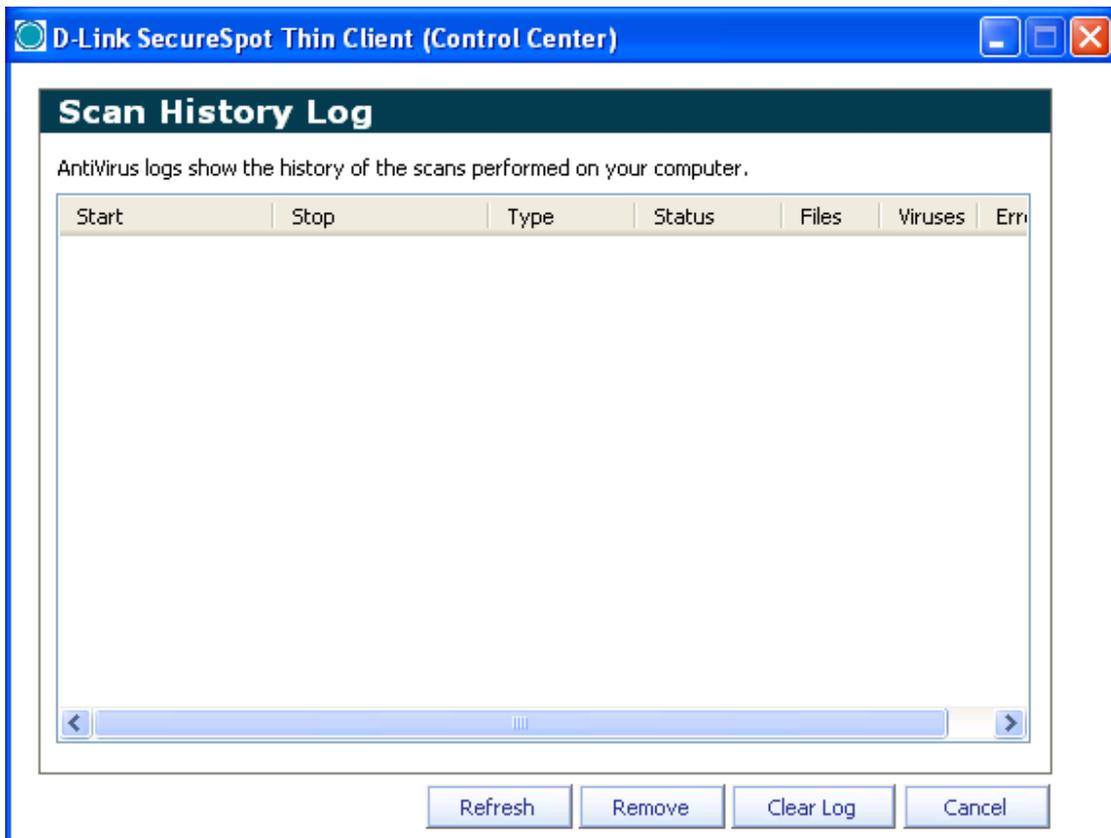
Enter private data and click Add

Protected Information









**D-Link SecureSpot Thin Client (Control Center)**

## AntiVirus Updates

Welcome to your AntiVirus Update System.

Last Update:	02/21/2007
Last Scan:	Not Available
# of Detectable Viruses:	15276
Virus Engine Version:	5294
Virus Definition Date:	02/21/2007

When your Internet Protection Service reauthenticates, it checks and updates the AntiVirus Definition files if necessary.

Do not check for updates during authentication.

Do not ask when there are updates (automatically download and install)

Click Next to check for updates (Please note that the Control Center will be closed during this operation).

[Next](#) [Close](#)

- Open...**
- Open Intrusion Detection...
- Open Profile Management...**
- Antivirus Center ▶
- Identity Protection ▶
- Popup Blocker ▶

---

- Switch User Profile
- Settings...
- Thinclient Upgrade...

---

- Reauthenticate
- About...

D-Link SecureSpot Thin Client (Control Center)

## PROFILES

Securespot security policies can be used to control your entire network's security from the device, control security policies for each computer or control them for each user.

Administrative Password:

D-Link SecureSpot Thin Client (Control Center)

## Profile Management

You can create a profile for each family member and configure it. First item in the list is the primary profile for the account. You can add/remove/edit filter profiles. If your OS supports multiple Windows logins, you can associate a filter profile with one or more Windows logins.

Profile	Windows Login(s)
richard	tech829

**Active User Profile: richard**

NOTE: Changes to the active secondary profile will not take effect until you close the Control Center.

- Open...**
- Open Intrusion Detection...
  - Open Profile Management...
  - Antivirus Center ▶
  - Identity Protection ▶
  - Popup Blocker ▶
- 
- Switch User Profile
  - Settings...
  - Thinclient Upgrade...
- 
- Reauthenticate
  - About...

**D-Link SecureSpot Thin Client (Control Center)**

### Internet Application List

Highlight the file name and select the permission level by clicking on the options at lower right-hand corner.

Program	Product Name	Permission
---------	--------------	------------

Permissions

Add Remove Refresh Apply

- Open...
- Open Intrusion Detection...
- Open Profile Management...
- Antivirus Center ▶
- Identity Protection ▶
- Popup Blocker ▶

---

- Switch User Profile
- Settings...
- Thinclient Upgrade...

---

- Reauthenticate
- About...

**D-Link** seurespot

HOME   MY ACCOUNT   SUPPORT

### Welcome to the Secure "My Account" Web Control Center.

D-Link customers who've already registered their seurespot™ use this page to change their settings, update contact info and administer their filtering and security services. (You may access this page and make changes from anywhere on the Internet.)



Email Address:

Password:  [Forget your password?](#)