SecurityCoverage
Guaranteed Computer Protection

SecureIT Plus Service

Quick Start Guide

www.securitycoverage.com

Table of Contents

1. General Information

1.1. Who is SecurityCoverage?

SecurityCoverage is a managed security service provider based in Cedar Rapids, Iowa offering a centrally managed and fully automated security service to customers in the home, home office, and small business markets.

1.2. Why Are We Important?

By having the SecureIT Plus Service in place, you are going to:

- Experience minimal issues or downtime with virus and Internet related attacks
- Enjoy optimal computer performance and availability
- Lower the amount of time and money you spend on computer security
- Be able to rest assured that all of your computer security needs are addressed

---

2. What's Included?

2.1. Antivirus Software

Within the SecureIT Plus Service is a complete Antivirus client. We partnered with Symantec to provide you with the highly acclaimed Symantec Antivirus Corporate Edition client.

Symantec AntiVirus™ provides world class protection—automatically removing viruses, worms, and Trojan horses from your computer, delivering timely updates, and defending you against known and emerging threats. Symantec AntiVirus also detects certain non-virus threats, such as spyware, adware, and a variety of hacker devices.

Because Symantec is included as part of the SecureIT Plus Service, any anti-virus software that you currently have on your computer will need to be uninstalled before attempting to install this product. This also means that you will no longer need to worry about keeping your antivirus subscriptions up to date. Some examples of software that you may have are Norton Antivirus, Mcafee, AVG32, etc.

To uninstall this software, go into the Control Panel and click Add/Remove Programs. Find the software in the list, highlight it and click Add/Remove.

2.2. Spyware Detection Program

Provided within your SecureIT Plus Service is a built-in spyware removal program. This function utilizes the market leading product, Spybot Search & Destroy. If you already have a spyware prevention program on your computer, it can be uninstalled before installing this product. The most commonly used are Spybot, Ad-Aware, Pest Patrol, and SpyKiller to name a few.

To uninstall this software, go into the Control Panel and click Add/Remove Programs. Find the software in the list, highlight it and click Add/Remove.

2.3. Spyware Monitor

As part of your SecureIT Plus Service, you are also provided with an active Spyware Monitor. This program was specifically designed to run "real time" in the background on your computer. This feature will prevent malicious software from running and being installed on your computer. This would include spyware, adware, and even some Trojan horses and viruses as well. This is additional protection to ensure that your machine stays free from the Internet threats that are out there.

2.4. Pop-up Blocker Software

The SecureIT Plus Service also has a built in Pop-up Blocker designed to work exclusively with Internet Explorer to stop those annoying pop-ups received when "surfing" on the Internet. Any current pop-up blocking software can be uninstalled before installing this product. The most common pop-up blockers are the Google Bar, Stopzilla, Popup Stopper, Popup Eliminator, just to name a few.

To uninstall this software, go into the Control Panel and click Add/Remove Programs. Find the software in the list, highlight it and click Add/Remove.

2.5. Disk Maintenance Tool

Within the SecureIT Plus Service you also receive Executive Software's Diskeeper Professional client. The Diskeeper client is implemented to automatically reduce hard drive fragmentation and optimize the efficiency of your computer.

For a simple explanation of fragmentation, think about when you save a file to the hard drive. The file is split into "pieces" all over the hard drive. The more "pieces" a file is in, the harder time your computer has finding the file when you want to open it. Thus, when your fragmentation level gets too high on your hard drive, your computer will become much slower and opening files will take much longer. No matter how fast your hardware is, disk fragmentation can choke your machine's performance within a matter of days. The only way to ensure optimum speed and stability is with Diskeeper, the leader in automatic defragmentation for Windows.

The Diskeeper client is set to automatically run when it determines there are too many fragmented files on your computer. You should never again experience any performance issues due to fragmentation.

2.6. Automated Windows Updates

With the SecureIT Plus Service, you also receive automatic, behind the scenes updates of all Microsoft security and critical updates that are tested prior to deployment. If Microsoft releases a critical security patch for any reason, it will be tested and automatically applied to your computer once it is approved.

3. Installation

3.1. Remote Installation

Installation of our software is quick and easy. Simply put…we can do it for you!

When you put your CD in or run the secureit.exe from the online download, you will see a screen that looks like the following:

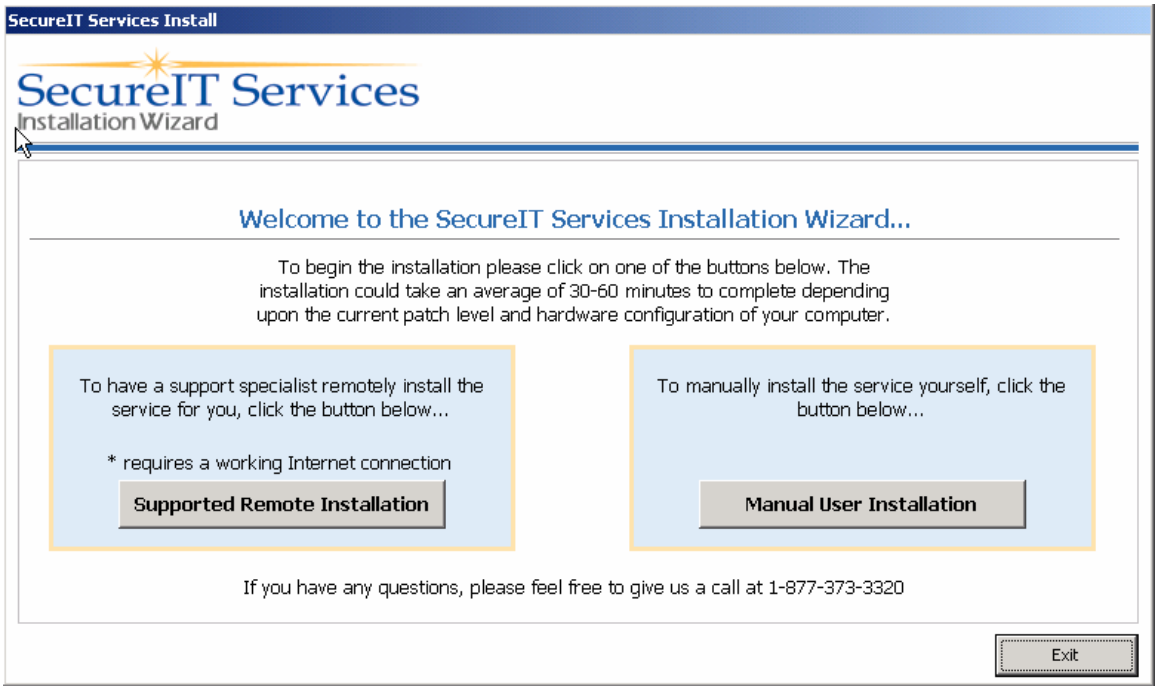


Figure 3-1

Ensure you are connected to the Internet and then click on **Supported Remote Installation** to see the following window:

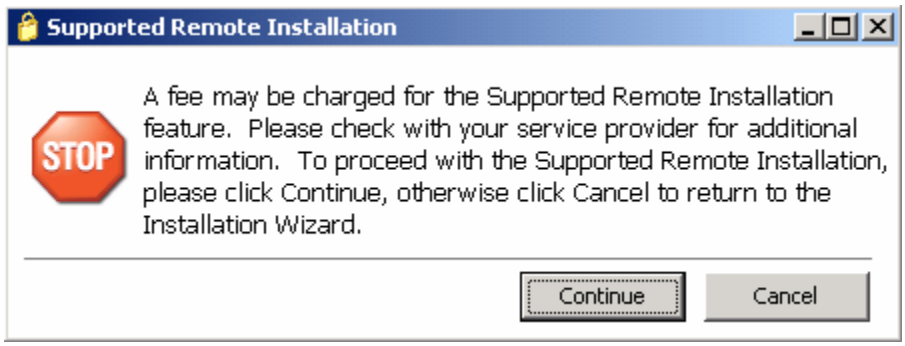


Figure 3-2

If you are unaware of any fee that may be charged for taking advantage of the Remote Support Installation feature and having a technical specialist assist you with the installation of the service, please contact your service provider. If you are OK being charged this fee, click "Continue" to proceed. If you would rather do the installation yourself, click on "Cancel" and you will be taken back the main installation screen (see figure 3-1).

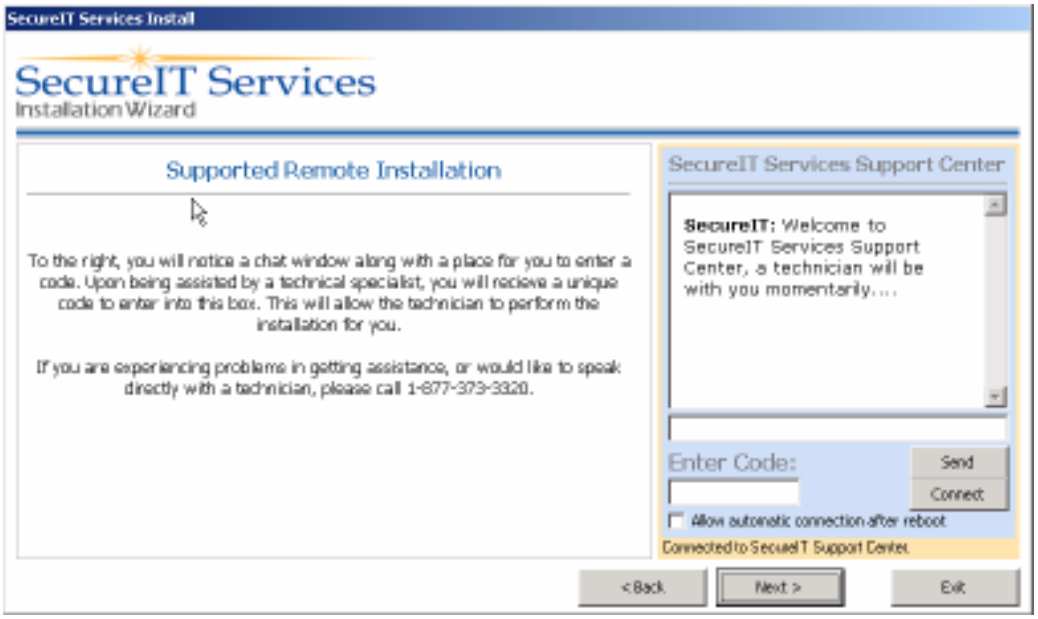


Figure 3-3

At this point, a technician will have already been notified that you are awaiting assistance. Within a matter of moments, you will receive a response back from a technical specialist asking how they can be of assistance.

Here you can chat back and forth with a technical specialist to assist you in installing the service or to actually have the technician perform the installation for you. If you are experiencing problems in getting assistance, please give us a call at 1-877-373-3320.

3.2. Do It Yourself

If you prefer to do it yourself, below are step-by-step instructions, including screenshots. When you put your CD in or run the secureit.exe from the online download, you will see a screen that looks like the following:

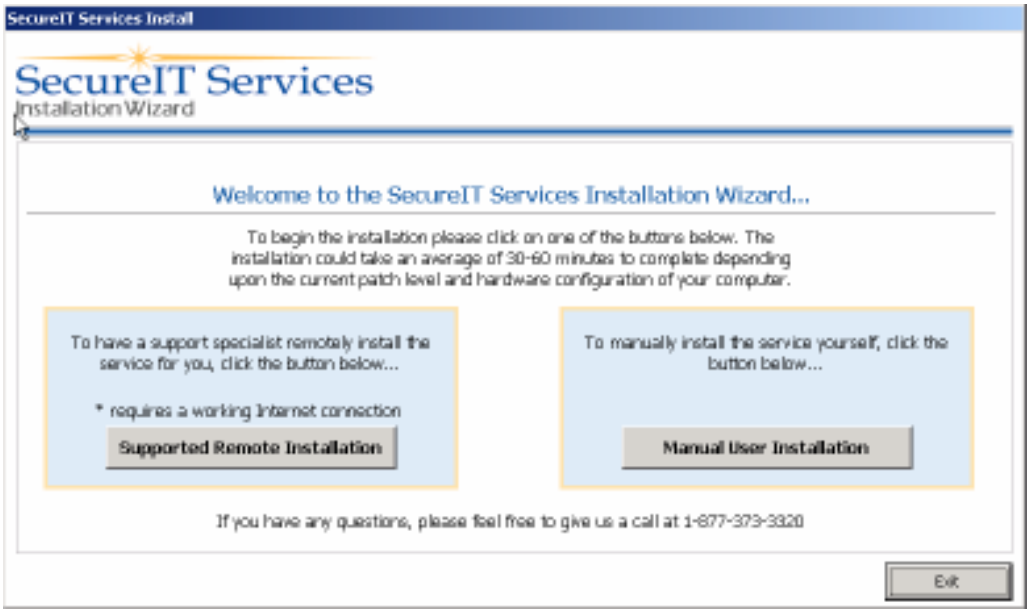


Figure 3-4

Click **Manual User Installation** and you will see a screen that looks like the following:

Figure 3-5

Here a check will be made to ensure that your system meets the minimum system requirements needed to run the service properly. They are as follows:

- System Memory (98 MB for Windows 98/ME & 128 MB for Windows 2000/XP)
- Administrative Rights (Only applies to Windows 2000 and XP. User has to have administrative rights to install the service)
- Windows Version (Windows 98 SE, ME, 2000 or XP are the supported operating systems)
- Available Hard Disk Space (200 MB of free space required to install the service)
- Previously Installed Antivirus Software (Will check for a multitude of anti-virus software and will bring up a window telling you to uninstall before proceeding, if found.)

If your system does not meet the minimum requirements needed to install the service, it will dispay a box telling you the necessary action that will need to be taken before the service can be installed.

NOTE: If you have other Virus Scanning Software already installed on your Computer you will be given a message that you need to uninstall it before continuing the Installation of SecureIT Plus Services. (See figure 3-6).

This step is VERY IMPORTANT. If you do not do this, your SecureIT Plus Service may not run correctly. You can do this by clicking "Continue" which will take you to Add/Remove Programs. Then find your currently installed software in the list (Norton Antivirus, Trend Micro, AVG, McAfee, etc.) and click Remove to uninstall it.

Figure 3-5

Once your system has met all of the minimum system requirements, click "Next" to proceed.

Option 1: At this point, if the setup detects that any Windows Updates need to be installed, you will see a screen that looks similar to the following: (This information box will vary depending upon what operating system the service is installed on.)

Figure 3-6

Be advised that this is not a required step; however, it's recommended that dial-up users install the updates due to the amount of time it would take them if they wanted to manually install updates from the Windows Updates site. Some of these updates may require the computer to be restarted to complete installation successfully.

NOTE: This feature is not available for users who acquire the service via online download.

Option 2: If the setup does not detect that any Windows Updates need to be installed, you will automatically get taken to the User License Agreements (see below).

Figure 3-7

Upon reading the Service Agreement and agreeing to the terms, click **I Accept the agreement** and click **Next**. You will then see a screen that looks like the following:

Figure 3-8

Upon reading the Third Party Agreement and agreeing to the terms, click **I Accept the agreement** and click **Next**. This will bring you to a screen that looks like the following:

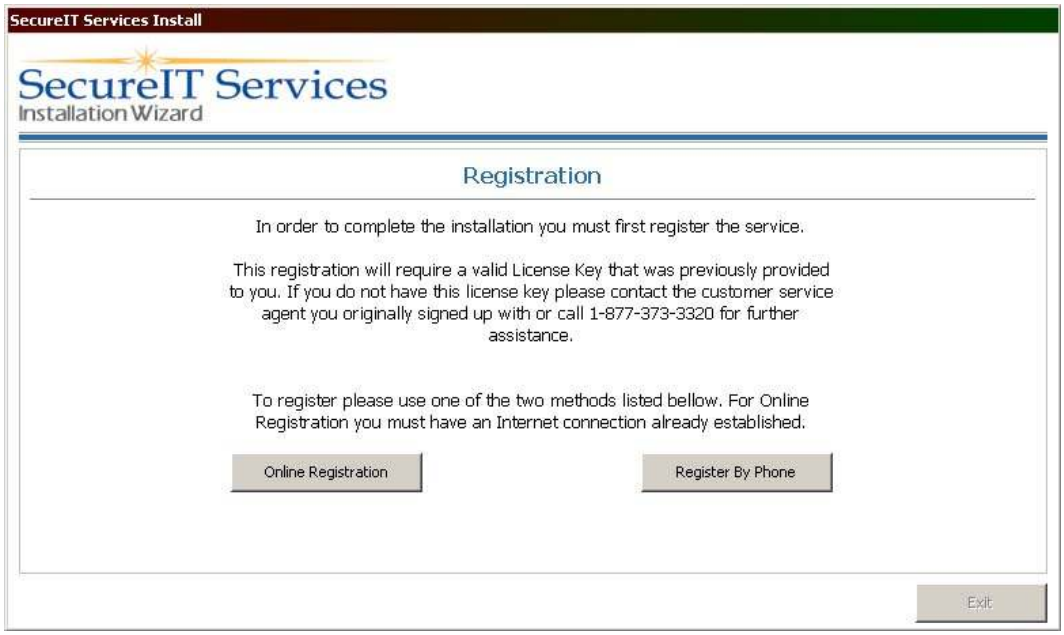


Figure 3-9

Here you can register the service via **Online Registration** (requires an Internet connection) or you can **Register By Phone.** (See appropriate section below.)

Online Registration:

By clicking **Online Registration**, you will see a screen that looks like the following:

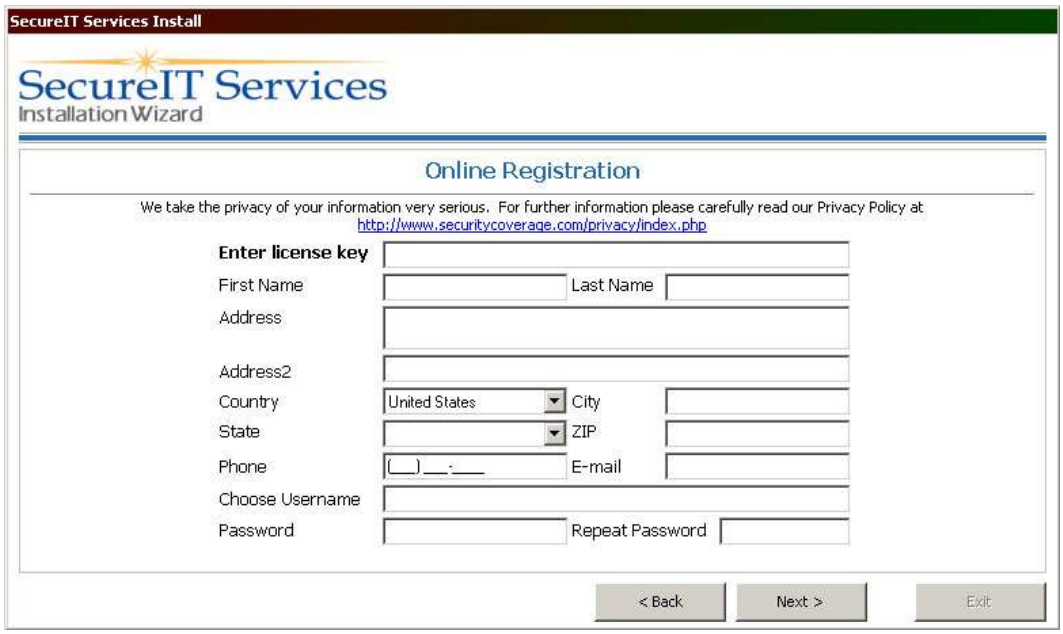


Figure 3-10

Type in your license key (which you would have received from your provider) here, and once input correctly, that box will turn green. Once you see this happen, make sure to fill in all of the other fields and take note of your username and password as you will use this

information to obtain rollup statistics from our reporting system which we will detail later on. Once you are sure you have typed all the other information in correctly, click **Next** to proceed and you will see a screen that looks like the following (go to figure 3-12).

Register By Phone:

If you do not or cannot have connection to the Internet at the time of the installation, you can click on **Register By Phone**. This would bring up the following screen:

Figure 3-11

Enter your License Key you received when you signed up for the service, verify that the box turns green after inputting the key, and then call the toll free number listed to complete your registration by phone. The support person who answers will ask you for some information to create an online reporting account with us, and then will ask you to read them your license key and your registration code. Once you read these two items to the support person, they will give you a **Unique ID Code** based on the information you gave them. Once you input this code in the appropriate box, it will also turn green and then you will see that **NEXT** button will no longer be grayed out and you will be able to click it. Click **Next** to proceed; and continue the installation process. You will then see a screen that looks like the following:

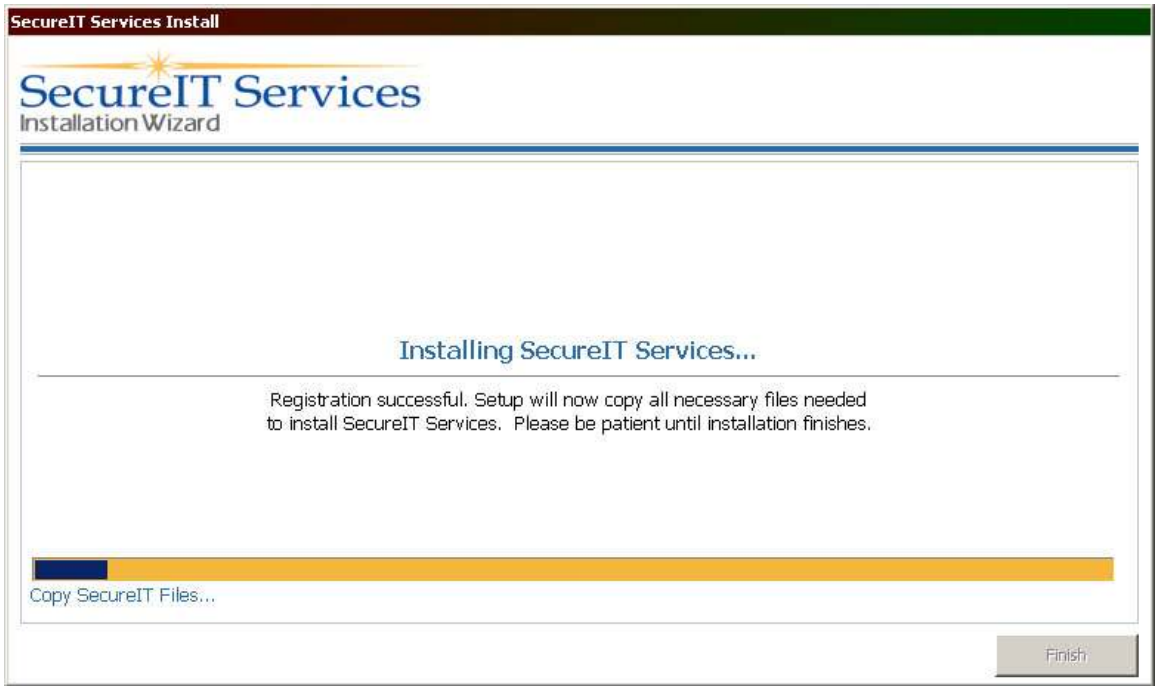


Figure 3-12

Here you will see that the setup will start to prepare the system for installation of the SecureIT Services. The installation process may take several minutes, but once complete you will see a screen that looks like the following:

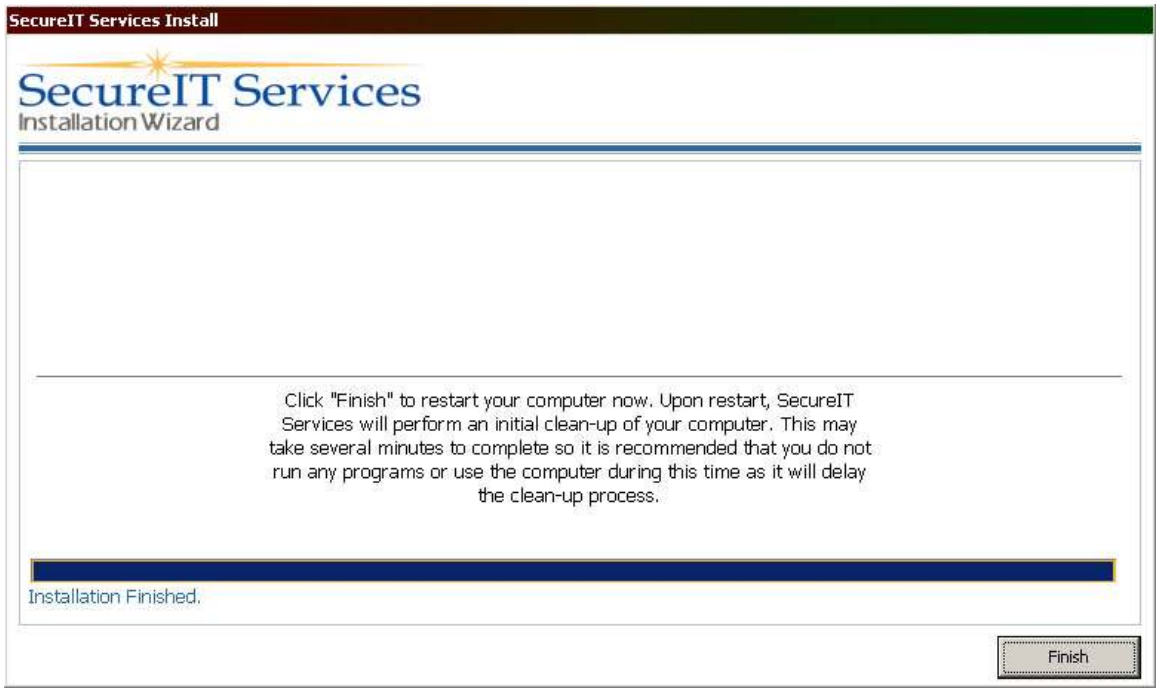


Figure 3-13

Upon clicking "Finish", your machine will automatically reboot itself and when it comes back up, the initial cleanup of the computer will begin.

3.3. Initial Clean-Up

NOTE: It is **VERY IMPORTANT** to allow your computer to finish this process! This process can take quite a long time depending upon your Internet connection and the hardware configuration of your computer. Please be patient during this process.

Figure 3-14

During the initial cleanup, the first thing that you will see is that the service will prepare the system for cleanup. Once this is done, it will go through a series of steps as part of the update and cleanup process that will update and protect your SecureIT/3rd party components. Once this has been done, the last thing that happens is the spyware scan will run a scan of your computer for spyware and fix any issues that it finds. While this is running, there will be an icon in the lower right hand corner in your system tray that will flash back and forth between a padlock and a magnifying glass (see page 12). This process will vary depending on the hardware configuration of your computer and the speed of your Internet connection as well. Once the scan is complete, the flashing will stop and your icon will resume being a "padlock" again.

> **NOTE for Windows 98 and Windows ME:** While the spyware scan is running, you will notice a "Spybot Search & Destroy" program running down on your toolbar. You will not be able to maximize or close this window, which helps prevent possible performance issues with some of the older machine configurations. Once the scan finishes this program will fix the problems it finds and then close itself. You will see this program run in the toolbar each time a scheduled spyware scan happens, but it should not cause any issues or problems for you or your computer.

Once all the updates and scans are complete, you will see the following screen:

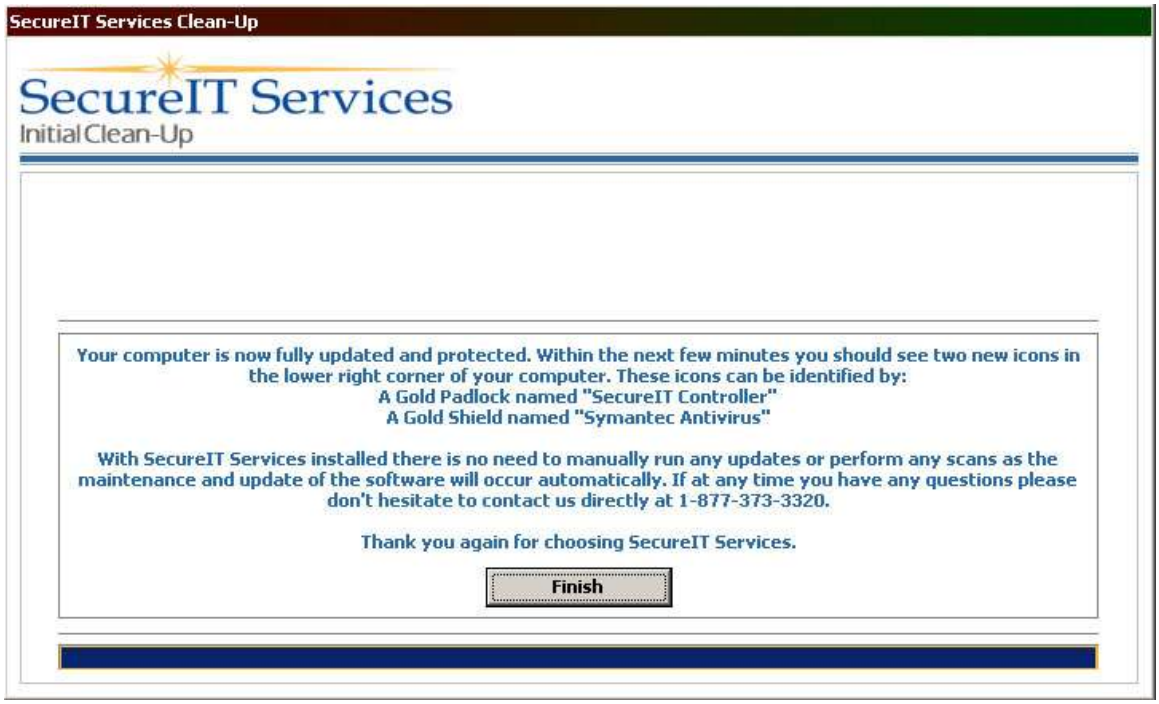


Figure 3-15

Once you have fully read the above dialog box and written down our toll free customer service number, click "Finish". If you experience any problems with your SecureIT Services or have any questions regarding the service, please call this toll free number and our technical support group will promptly assist you.

4. Modules

4.1. Management Console

Once you have successfully installed your SecureIT Plus Service, there are many things that can be configured to suit your needs. These are done in the Management Console (see below). To get to the Management Console you can right click on the "padlock" in your system tray or simply double click on the icon on your desktop.

Figure 4-1

4.1.1 Status & Update

In this section you can **View SecureIT Status** or **Update All Components**. Let's go through a brief description of each item:

View SecureIT Status

By clicking this link, a check will be made to ensure that your SecureIT Services are working properly and are completely up to date by comparing the versions on our servers with the versions listed on your machine. In order for this process to happen correctly, you MUST be connected to the Internet.

If an Internet connection is not detected and you use dial-up, we will try and automatically dial your default connection. If we still can not get connected to the Internet, you will see an error in the management console that looks like the following:

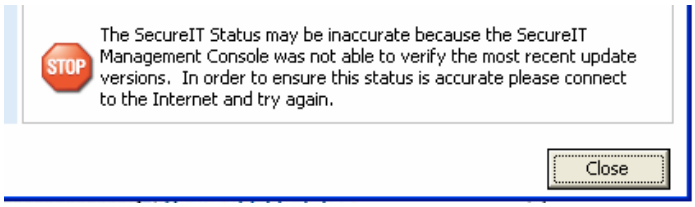


Figure 4-2

If the machine is connected to the Internet when you click "View SecureIT Status" and everything is working and updated properly, you should see a screen like the one below:

Figure 4-3

If there is a problem with one of the components not running correctly or if one of the components is not completely up to date, you will see a screen that looks like the following:

Figure 4-4

For example, here you will see that the SecureIT Components are not fully running, that the anti-virus software is out of date, and the pop-up blocker is not running. By clicking on each link, you would see similar windows like the following:

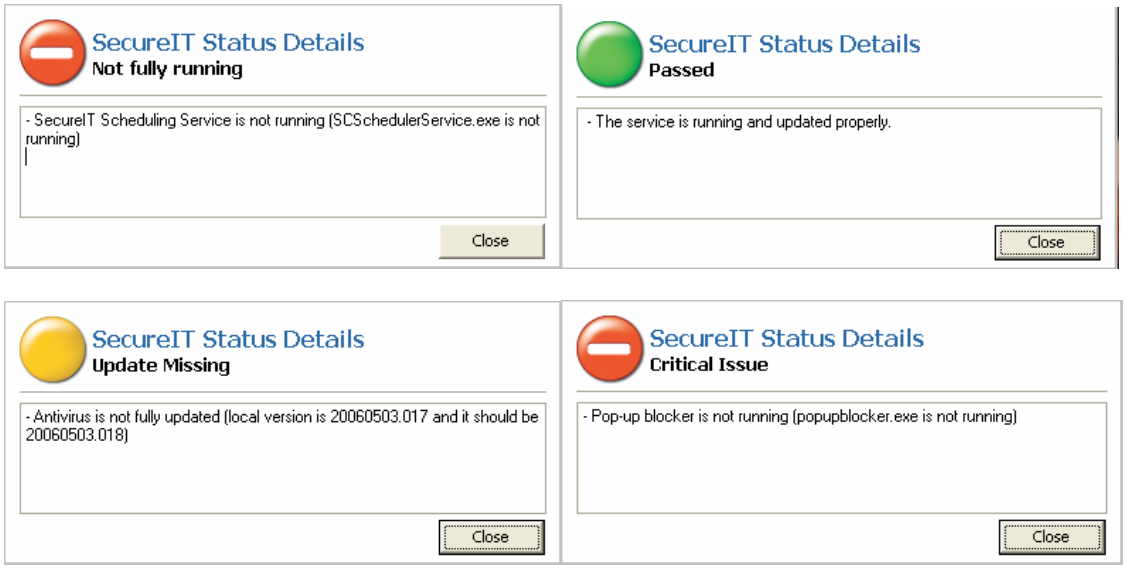


Figure 4-5

As you can see here, not only will it give you details that the service is not fully running, passed, has an update missing, or has a critical issue, but it will also give you exact details on what services/programs are not running and what the versions you should have to be fully up to date.

Update All Components

By clicking this, SecureIT Services will update all of your SecureIT components and all third party components including anti-virus and spyware protection as well. Upon clicking **Update All Components**, you will see a screen that looks like the following:

Figure 4-6

SecureIT Services will update your spyware definition files first, then it will update your virus definition files and then if there are any SecureIT updates, it will take care of installing them as well.

You may notice the "padlock" icon down in the lower right hand corner flashing between different icons during the update process (see page 21). Once the update procedure is finished, this screen will tell you that all updates finished successfully.

4.1.2 Actions

In this section you can **Run Security Scans** or **Run Disk Maintenance**. Let's go through a brief description of each item:

Run Security Scans

This is where the scanning and maintenance activities take place. Here your computer can be scanned for viruses and spyware and your hard drive defragmenter as well. By clicking on **Run Security Scans**, you will see a window like the following:

Figure 4-7

Here a full spyware scan of your computer will be completed and any problems that are found or threats that are detected will automatically be removed/fixed. Depending on what operating system you are using, you will actually see a window come up on the screen and perform the scan or else everything will be minimized at the bottom of the screen. Once the spyware scan has completed, your computer's hard drive will be fully scanned for viruses. However, the scan DOES automatically run at 5 AM every Sunday morning. If your computer is turned off during that time it will run at next startup. When the machine runs a virus scan, you will see a window that looks like the following:

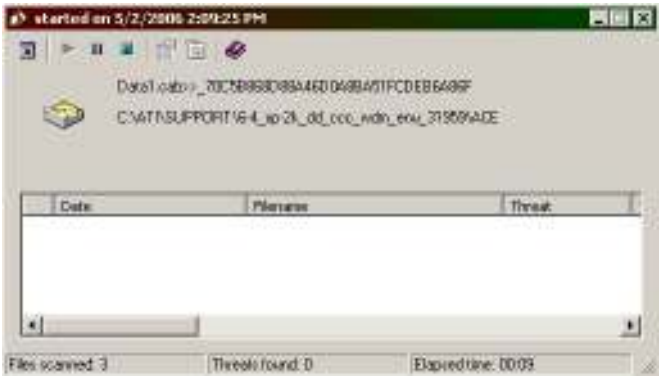


Figure 4-8

You may notice the "padlock" icon down in the lower right hand corner flashing between different icons during the scanning process (see page 21). Once both of these scans have completed, your screen will tell you that all scans have completed successfully.

Run Disk Maintenance

Clicking on this button will run the Diskeeper software. You will notice a little icon in your system tray (lower right hand corner of the screen.) that looks like a hand holding a disc. You will also see a screen that looks like the following:

Figure 4-9

Some Windows users may find that when starting the Disk Maintenance tool, a "Windows Security Alert" dialog box will appear. Be sure to click the button "Unblock" listed at the base of the dialog box (highlighted with a red box below). This alert was generated due to windows not yet recognizing the reporting systems within the SecureIT Plus Service. Once unblocked, this alert shouldn't appear again.

Figure 4-10

Once you start the Disk Maintenance program, you CANNOT stop it. It will run until it has finished defragmenting your drive to its satisfaction. In addition, the Diskeeper program is set on a "smart" schedule where it will automatically check to see if the machine needs to be defragmented on a daily basis.

If the machine does need to be defragmented, the program is smart enough to know it should only defragment the machine when it is not in heavy use. This will ensure that you do not experience performance issues in using the machine while the program performs its maintenance. Once the operation is complete, your screen will tell you that the disk maintenance has completed successfully.

4.1.3 Settings

In this section you will be able to modify **Pop-up Blocker Settings** and **Set** your **Component Schedule** as well. Let's go through a brief description of each item:

Pop-up Blocker Settings

Here you will be able to modify your pop-up blocker settings. Once you click on **Pop-up Blocker Settings**, you will see a screen that looks like the following:

Figure 4-11

On the **General** tab there are several customizable options. Let's take a look at the **Functional Features** and what they mean:

- **Enable Pop-up Blocker:** This option should stay enabled at all times but allows the integrated pop-up blocker to be disabled by removing the check.

- **Allow CTRL to bypass the pop-up checking:** If you find a link on a web page in which you want the pop-up window to come up, you can "bypass" the pop-up blocker by holding the CTRL key down on your keyboard and clicking on the link. This will allow the pop-up generated to appear.

- **Suppress pop-ups generated when loading HTML pages:** Many times a web page will load additional web pages when loading. By checking this box these additional pages will be blocked.

- **Allow pop-ups generated by JavaScript:** Another method used by web pages to display pop-ups is by JavaScript. Checking this setting stops these types of pop-ups from occurring.

- **Enable Sound:** When a pop-up is blocked, as a default your computer will make a sound (if you have a soundcard and internal/external speakers are present). You can choose the sound it makes by clicking on **Change** and browsing to the location of the sound that you would like to use or if you want to hear NO sounds, uncheck this box.

Now click on the **White List** tab. This is where you would enter specific sites that you do not want the pop-up blocker to block (see figure 4-11).

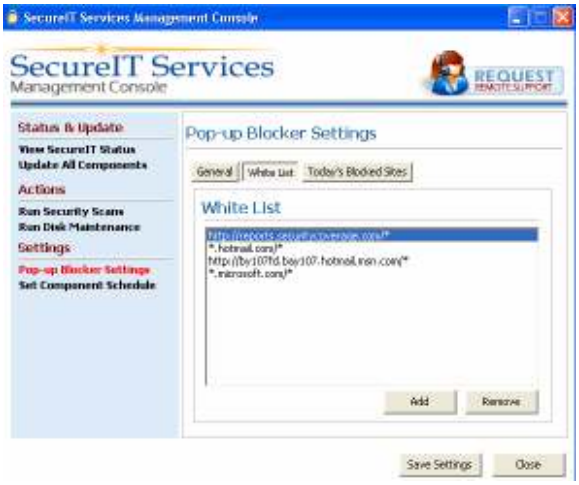


Figure 4-12

Figure 4-13

For example, say that you went to www.securitycoverage.com and the pop-ups that were normally visible when you entered the site are now gone. What you would do is go into your **Pop-up Blocker Settings** and click on **Today's Blocked Sites** (see figure 4-12). Here you will see that the site www.securitycoverage.com is in the list. At this point just highlight the entry that you want added and click the **Add To White Lis**t button. Click **Save Settings** and **Close**, that is all there is to it. In some cases for the changes to take effect, you may have to close out of your browser and launch it again. Now the next time you visit www.securitycoverage.com, you would see your pop-ups again.

In cases where you would like to make sure that no pop-ups appear within the web pages of sites you are looking at, you can use wildcards in your entry.

For example, if you do not want any pop-ups to show up on any sites that end in securitycoverage.com, you would put the wildcard in from of the entry and type http://*.securitycoverage.com and then click **Add To White List**.

In cases where you would like to make sure that no pop-ups show up on any of the pages that you are browsing the website www.securitycoverage.com , then you would add the wildcard in the back of the entry and type http://www.securitycoverage.com/* and click **Add To White List.**

Set Component Schedule

When you click on **Set Component Schedule**, you will see a window that looks like the following:

Figure 4-13

Here you can set the times and days of the week that you want the program to scan for updates. It is best to set the schedule for a time when you are away from the computer (i.e. early morning). If you are not sure, these fields can be left on the default settings.

4.1.4 Request Remote Support

If you have an issue that you cannot figure out, or a question that you cannot find the answer for, then you can click in the right hand corner of the Management Console where there is a picture of a girl with a headset where it states **Request Remote Support** (see figure 4-13). You will see a window that looks like the following:

Figure 4-14

Here you can get assistance in one of two ways:

Request Assistance

By clicking on **Request Assistance** you will send a message to our tech support team via chat that you are waiting to be helped. This operation requires you to be connected to the Internet, so if you are not connected we will automatically try and connect you. If you are connected to the Internet and click **Request Assistance**, you will see a window that looks like the following:

Figure 4-15

Here you will be able to chat with an online support technician about your issue. If need be a technician can also give you a code to allow remote assistance to your machine to diagnose and fix the problem for you. For dial-up users that have one phone line and do not have a cell phone or users who prefer not to cover verbal instructions over the phone, this is a perfect alternative.

Remote Support

If it is determined that it is going to require some investigation work on our end to resolve your issue, a support technician can remotely connect to your machine. This happens by the technician giving you a one time code that you would input in the box marked **Enter Code**. The technician would then enter the same code on their side, and this would complete the remote connection. While a technician is remotely connected to your machine, they have complete control over your mouse and keyboard. We encourage you to watch us while we are remotely connected to make sure you are completely comfortable while we are accessing your computer. Once the technician is done diagnosing and fixing your issue, we will disconnect the remote session and cannot get reconnected without you entering in another unique code. This way you can be assured that we cannot access your computer and information unless you request us to. You can also call our toll free support number listed to take advantage of the above options as well.

4.2. SecureIT Controller

This module is located in the lower right hand corner in your system tray and looks like a padlock. This is the place where you would be notified of any activity that is going on with the software. The following notifications will be made when their performed action takes place:

Running a spyware scan - The SecureIT Controller icon will flash between a "padlock" and a "magnifying glass" to signify a spyware scan is being run.

Blocking a pop-up - The SecureIT Controller would flash between a "padlock" and a "stop sign" to signify a pop-up is being blocked.

Running a virus scan - The SecureIT Controller would flash between a "padlock" and a "shield" to signify a virus scan is being run.

Updating virus definition files - The SecureIT Controller would flash between a "padlock" and a "shield" to signify that your virus definition files are currently being updated.

Updating SecureIT Components - The SecureIT controller would flash between a "padlock" and a "globe" to signify that your SecureIT Components are being updated.

If you would double click on the SecureIT Controller while the above actions were taking place, you would see one the following windows to also give you details on what the service is doing.

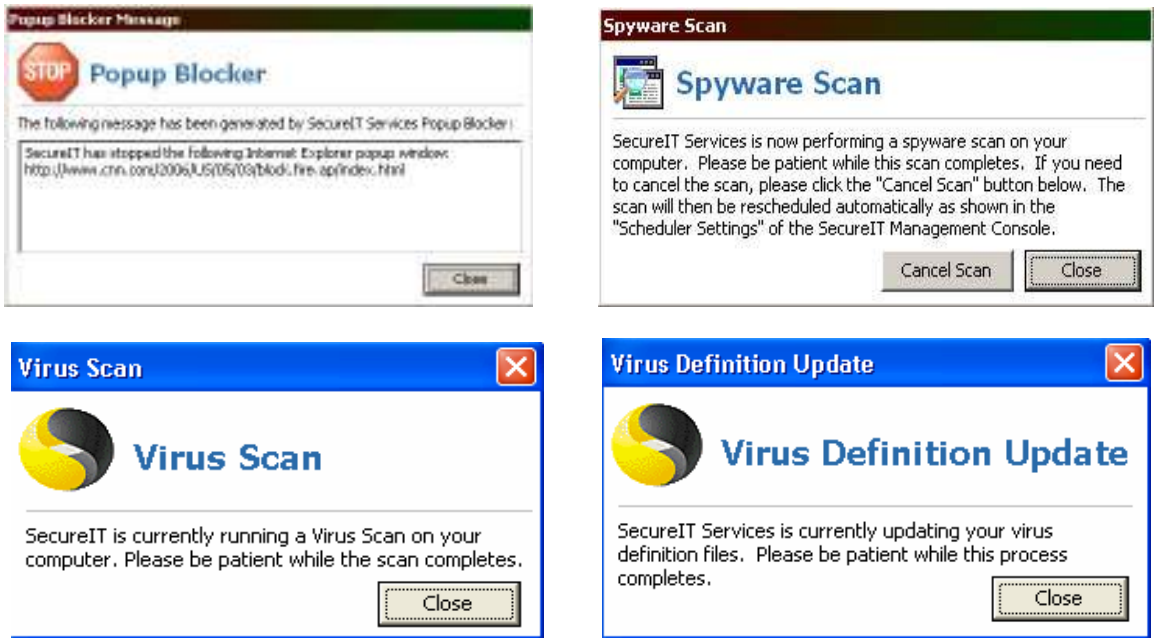


Figure 4-16

Open SecureIT Management Console: Will open the module shown on page 13.

Open SecureIT Online Reports: We will cover this in more detail in the next section.

Balloon Notices: If you don't like the balloon notices that come up when your SecureIT Plus Service detects something, you can click on this to disable those notices. Balloon notices are not available in Windows 98 and Windows ME.

Pop-up Blocker Settings: This is another way to access and modify your pop-up blocker settings (see page 18 for further details).

4.3. SecureIT Online Reports

One of the additional features that make the SecureIT Plus Service unique is the online reports. These reports are updated every 24 hours and reassure you that your machine is being well protected and that scans and updates are being applied regularly and successfully. To find out more, right click the lock in your system tray and click **Open SecureIT Online Reports**.

You will see a web page that looks like the following. Enter your **Username** and **Password** that you created when you registered your service on page 6 / 7 and click **LOGIN**.

Once logged on, you will see the **Summary Report**. It will show, as a default, last month's report. However, you can click on the dropdown box and choose another timeframe. Your choices are **Last Week**, **Last Month**, **Last 3 Months**, **Last 6 Months** or **Last Year**. Click the period you would like to report on and hit the **Filter** button. This will update the report information accordingly. This report will give you such information as:

- **Virus information:** Shows how many viruses have been eradicated from your computer and how many virus updates have been applied.
- **Spyware:** Shows how many spyware threats have been detected and removed.
- **Pop-up blocker:** Shows the number of pop-ups that have been blocked.
- **Critical patch status:** Shows what tested Microsoft Critical and Security updates have been applied to your computer and which ones are still missing.

- **Disk volume:** Shows the amount of used hard drive space vs. the amount of free space that you have left.

Let's review some of the other reports which are found on the left hand side, as you can see above.

Viruses caught: This is a detailed report of the total amount of viruses eradicated from your computer, the dates they were found, and the names of the viruses.

Virus definitions applied: This is a detailed report that shows the total number of virus definition files applied, the dates on which they were updated and the version that they were updated to.

Spyware issues fixed: This is a detailed report that shows the total number of spyware related issues fixed. It includes details such as names, descriptions, number found, and the dates on which the spyware was removed.

Pop-ups blocked: This is a detailed report of the total number of pop-ups blocked, the date and time in which they were blocked, and the website location that was blocked.

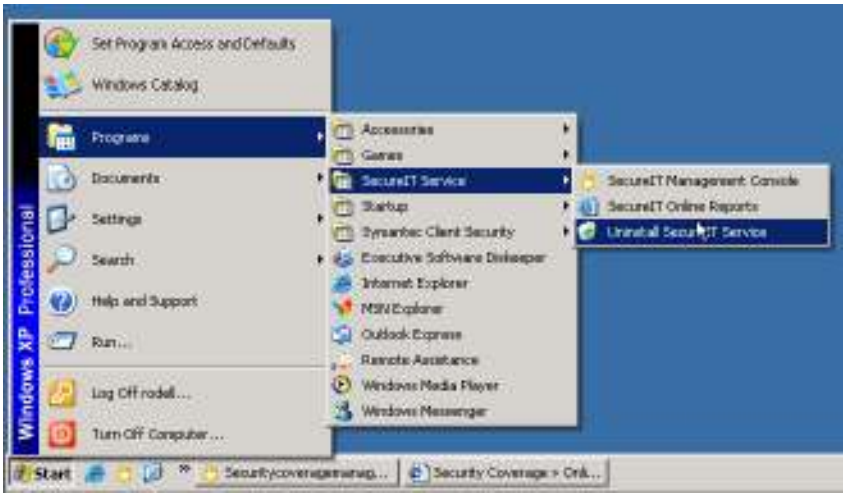
Microsoft patches applied: This is a detailed report of the Microsoft critical and security update patches that you have applied and the patches that still need to be applied, the patch number and the Microsoft bulletin in which additional information can be found.

Hard drive statistics: This is a detailed report of the amount of hard drive space that you have used on your computer vs. the amount that you have left. It includes details such as total number of files, total number of fragmented files, excess fragments, average fragments file and average file size.

5. Uninstall Methods

5.1. Using Program Uninstaller

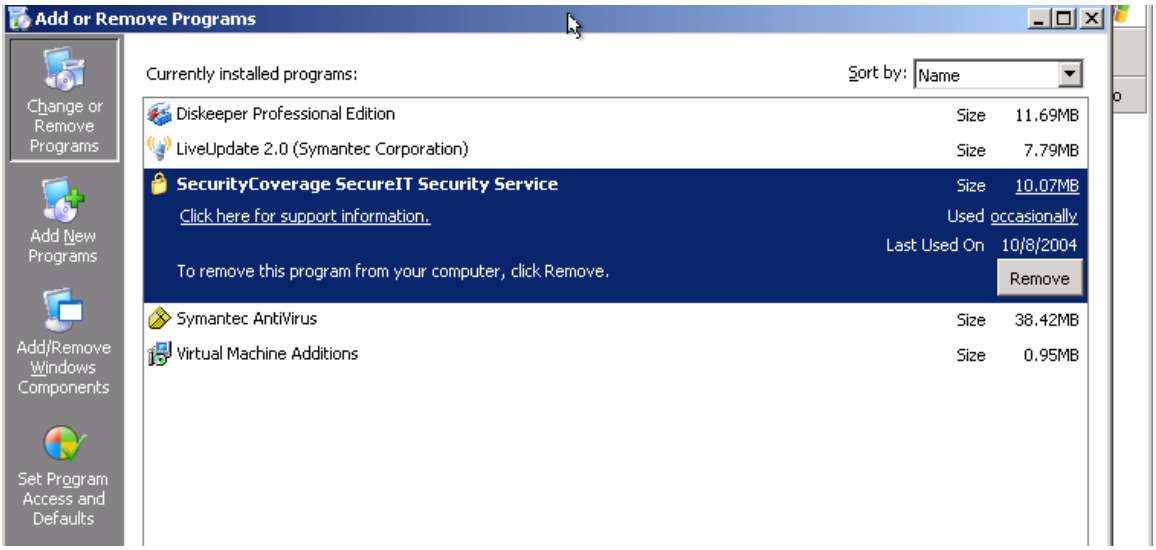
Before uninstalling, make sure that you close down and save everything that you are working on. Then click **Start** - **Programs** - **SecureIT Services – Uninstall SecureIT Service** (see below).



A window will open and ask you "Are you sure you want to completely remove SecureIT Services?" Click **Yes**. This will start the uninstall script and your software will be completely removed including all 3rd party software components. This process could take several minutes, but once the process is done, a window will open telling you to restart your computer. Once you do so, the uninstall process will be complete.

5.2. Using Windows Uninstaller

You can also uninstall the software using the Windows uninstaller. Make sure that you close all running applications before attempting to uninstall the software. Once this is done, click **Start** - **Settings** - **Control Panel**. The click **Add/Remove Programs** and find **SecurityCoverage SecureIT Security Service** in the list and click **Remove** (see next page for graphic).



This will fully remove all SecureIT software and also any other related 3rd Party software (Symantec Antivirus, Spybot Search & Destroy, and Executive Software Diskeeper.) Once again, you will need to reboot the machine for the uninstall process to be complete.

---

6. Service & Support

6.1. FAQ/How to Section

Q: Do I still have to have a separate anti-virus program?
A: No, the SecureIT Plus Service will provide you with everything you need to safely navigate the Internet and effectively and efficiently use your computer.

Q: Is there anything that I need to do to keep things updated?
A: No, this service applies all updates and runs all of its various scans behind the scenes without you having to worry.

Q: Do I have to leave my computer on all of the time?
A: No, if you happen to have your computer off at the time the program runs its various scanning processes and updates, they will automatically run the next time that you turn your computer on. The one advantage of leaving the PC running on the days when the software is scheduled to run updates is this will assure the updates don't interrupt you or take performance away from the PC when you are using it.

Q: How do I know that I am being protected?
A: You will receive a monthly e-mail detailing the activities that have been executed by your SecureIT Plus software. In addition you can check the Online Reports anytime, which are updated every 24 hours.

Q: What if I have/use a firewall?
A: Since our service never contacts your computer, and the vast majority of firewalls are designed to block INCOMING traffic, this software is compatible with 99+% of all firewalls

Q: What happens if I get a virus or some type of spyware on my computer?
A: In the very unlikely case that you do get a virus or spyware threat on your computer that materially affects its performance or damages it in some way, we will remove the problem at no cost AND give you a free month of service as well.

6.2. Tech Support Info

If you need to contact us at any time for support purposes, we may be reached at the following numbers and locations:

- Remote Installation Chat Feature (found within the Management Console)
- Toll free at 1-877-373-3320
- E-mail at support@securitycoverage.com

If you would like to meet with us or contact us, our contact information is:

SecurityCoverage, Inc.
230 2nd St SE, Suite 212
Cedar Rapids, IA 52401
319-298-4700
info@securitycoverage.com

Thank you for choosing the SecureIT Plus Service, the industry's only guaranteed computer protection service.

Your SecurityCoverage Team