Welcome to System Shield™

- **How to purchase System Shield**
- **Upgrading from System Shield Personal Edition to Professional Edition**

- **General Help Topics**
  - License Agreement
  - Product overview: What is System Shield and what can it do for me?
  - How to upgrade your copy of System Shield
  - How to obtain product support

- **Using System Shield**
  - Getting started: Using System Shield for the first time
  - Configuring System Shield to work for you

License Agreement

Use of System Shield for any period of time binds you to this license agreement. Please read and understand it before using the software.

SYSTEM SHIELD LICENSE AGREEMENT

IOLO TECHNOLOGIES, LLC DISCLAIMS ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE OR DOCUMENTATION. SHOULD THE PROGRAM PROVE DEFECTIVE, THE PURCHASER ASSUMES THE RISK OF PAYING THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION AND ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES. IN NO EVENT WILL IOLO TECHNOLOGIES, LLC BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION TO DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND THE LIKE) ARISING OUT OF THE USE OR THE INABILITY TO USE THIS PRODUCT EVEN IF IOLO TECHNOLOGIES, LLC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, IOLO TECHNOLOGIES, LLC SHALL HAVE NO LIABILITY FOR ANY DATA STORED OR PROCESSED WITH THIS SOFTWARE, INCLUDING THE COSTS OF RECOVERING SUCH DATA. AS A RESULT, THIS SOFTWARE AND DOCUMENTATION ARE LICENSED "AS IS" AND YOU, THE LICENSEE, ARE ASSUMING THE ENTIRE RISK AS TO ITS QUALITY AND PERFORMANCE.

Information in this document is subject to change without notice and does not represent a commitment on the part of iolo technologies, LLC. The software described in this document is furnished under this license agreement. The software may be used or copied only under the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

USE OF THIS PRODUCT FOR ANY PERIOD OF TIME CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT AND SUBJECTS YOU TO ITS CONTENTS.

US GOVERNMENT RESTRICTED RIGHTS

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subdivision (b)(3)(ii) of the Rights in Technical Data and Computer Software clause at 25 2.227-7013. Contractor / manufacturer is:

IOLO TECHNOLOGIES, LLC

145 North Sierra Madre Blvd., Suite 1

Pasadena, CA 91107

Copyright and Trademark Acknowledgments

Return to System Shield Main Help Topics

How to purchase System Shield

We sincerely hope that System Shield proves itself a valuable addition to your set of system tools.

We've put together some information to make it easy for you to purchase a licensed copy of the software or upgrade your existing license in a fast and convenient manner.

What do I get if I purchase?

- Free unlimited access to telephone, internet, and fax based technical support privileges.
- Free upgrades to all minor updates (e.g. 3.0 to 3.1 to 3.2, etc.) and all service releases / fixes.
- Notification of and generous discounts on all new major version upgrades (e.g. version 3.0 to 4.0).
- Great software created by people dedicated to providing quality products to their customers!

How much does it cost?

- **Personal Edition**, Single Computer Installation: $39.95
- **Professional Edition**, Single Computer Installation: $129.95
- Click here for more information about the difference between System Shield Personal Edition and Professional Edition
- Click here for information on site licenses and multiple-computer discounts

How do I order?

Instant and secure web-based ordering using a credit card

Toll-free by telephone

1-877-239-4656 (7:00 AM until 5:00PM, Monday through Friday, Pacific Time)

Non-U.S. orders: 1-626-793-3993

By mail or fax

Click here to access a printable order form

You may fax or mail your order to us using the following information. Product is delivered when payment is received.

Fax to: **1-626-793-1554**

Mail to:

iolo technologies, LLC

145 North Sierra Madre Blvd.

Suite 1

Pasadena, CA 91107

I don't live in the Unites States. Do you have a reseller in my area?

We probably do. Please either contact us by email at sales@iolo.com, or visit our website at http://www.iolo.com/order for more information.

Can I use a purchase order?

Yes, we accept corporate purchase orders, however we may request credit references prior to final approval and delivery. Our terms are net payment within 30 days of delivery. Purchase orders are encouraged for larger quantity orders. If a purchase order is submitted for an amounts under $100.00 there will be an additional $20.00 processing and handling fee added to the total due. Please note that for amounts less than $100.00 credit card payments are preferred. For more information please contact iolo technologies sales department at **1-877-239-4656** or e-mail sales@iolo.com

How do I upgrade my copy of System Shield?

How do I license System Shield for more than one computer?

I'd like to resell this product

We are always looking for resellers interested in representing our products. If you are interested in reselling System Shield or any other iolo technologies product please contact us at 1-626-793-3993 or var@iolo.com.

Note: Prices and availability are subject to change without notice.

Return to System Shield Main Help Topics

System Shield Printable Order Form

You may use this order form for faxing or mailing orders for System Shield. To print this form, select File>Print Topic. Fax To: **1-626-793-1554** or call iolo toll-free at **1-877-239-4656** (US) or **1-626-793-3993** (non US).

ALL relevant information below is required to process your order.

Company Name (if applicable): _____

Your Name: _____

Phone Number: _____ FAX Number: _____

E-Mail Address (please verify!): _____

Street Address: _____

City: _____ State/County: _____ Zip/Postal: _____

Where did you obtain System Shield? _____

I would like to purchase:

[____] Copy(s) of **System Shield Personal Edition** at **$39.95** per copy or priced according to the multi-computer matrix if more than 4 copies.

[____] Copy(s) of **System Shield Professional Edition** at **$129.95** per copy or priced according to the multi-computer matrix if more than 4 copies.

[____] Upgrade license(s) from System Shield **Personal Edition** to **Professional Edition** at **$100** per upgrade license or priced according to the multi-computer matrix if more than 4 licenses.

Delivery Method (check all the apply):

[__] E-Mailed Invoice with User ID and Serial number: FREE

[__] Postal delivery: $10.00 for US orders, $15.00 all others. Please allow up to 10 days for US and 20 days for all others.

I would like to pay using:

[__] MasterCard / Eurocard [__] Visa [__] American Express [__] Discover

Name on Card: _____

Credit Card Number: _____ Exp: _____

[__] I am enclosing a check or money order **paid in US Dollars, drawn on a US Bank, and payable to iolo technologies, LLC.**

Please FAX to (626) 793-1554, or mail to 145 N. Sierra Madre Blvd., Suite 1, Pasadena, CA 91107

There is a $20.00 processing fee for company purchase orders under $100.00 requesting net payment terms. Checks or money orders must be paid in US dollars and drawn on a US Bank. Orders are processed Monday through Friday, excluding US holidays. Please allow 24 hours for order processing. Prices and availability are subject to change without notice.

Licensing System Shield for more than one computer

System Shield is licensed on a "per-computer" basis. This means that you must purchase a license for each separate computer that it will be installed or used on, regardless of the number of people using the computers. Licenses are only sold in the blocks designated below. If you require a number of licenses that is not defined specifically in the blocks below, you should combine smaller blocks to arrive at an appropriate number of licenses (i.e. 200 licenses would require two 100-license blocks). Licenses for any less than five PC's are sold at single-user prices. If you require assistance before making a decision on a multi-computer license please do not hesitate to contact us toll-free at **1-877-239-4656** or sales@iolo.com.

Click here for more information about the difference between System Shield Personal Edition and Professional Edition

System Shield **Personal Edition**, single computer license: **$39.95**

System Shield **Personal Edition** Multi-Computer Pricing Matrix

Number of Computers	License Price
Up to 5	$149.95
Up to 10	$269.95
Up to 25	$599.95
Up to 50	$1039.95
Up to 100	$1499.95
Up to 250	$3295.95
Up to 500	$4499.95
Up to 1000	$6999.95
1001+	Contact iolo technologies

System Shield **Professional Edition**, single computer license: **$129.95**

System Shield **Professional Edition** Multi-Computer Pricing Matrix

Number of Computers	License Price
Up to 5	$449.95
Up to 10	$874.95
Up to 25	$1895.95
Up to 50	$3295.95
Up to 100	$4874.95
Up to 250	$9999.95
Up to 500	$14495.95
Up to 1000	$21995.95
1001+	Contact iolo technologies

Upgrade from **Personal Edition** to **Professional Edition**, single computer license: **$100**

Upgrade from **Personal Edition** to **Professional Edition**, Multi-Computer Pricing Matrix

Number of Computers	License Price
Up to 5	$350
Up to 10	$650
Up to 25	$1350
Up to 50	$2300
Up to 100	$3450
Up to 250	$6750
Up to 500	$10050
Up to 1000	$15050
1001+	Contact iolo technologies

Click here to purchase now using secure online ordering
Click here for other payment options
Note: Prices and availability are subject to change without notice.

Return to System Shield ordering information
Return to System Shield Main Help Topics

How to upgrade your copy of System Shield

Note: If you are looking for information on upgrading from System Shield Personal Edition to Professional Edition, click here.

One of the best ways to keep your software investment in top shape is to regularly check for and install available product updates. Software updates address incompatibility issues, add features, and expand existing functions and is an important responsibility of owning a computer. Unfortunately, the process of checking for and obtaining updates to your favorite software is often plagued with inconvenience and time-consuming searching, thus most people subscribe to an "if it isn't broken, don't fix it" mentality with regards to keeping their software up to date.

To combat the problems normally associated with keeping a software product up to date, iolo technologies has developed an extremely convenient and easy to use tool called **iolo WebUpdate™**. WebUpdate was created in order to provide owners of iolo products with an extremely easy to use and convenient solution when it comes to product updates. WebUpdate can automatically connect to an iolo update server using the Internet and check for the existence of available product updates based on the version of the product you are currently using. If updates are found, WebUpdate lists them with descriptions, and allows you to automatically download them to and install them on your computer, seamlessly and painlessly replacing your existing version with the very latest available. Additionally, WebUpdate always remembers how long it's been since it last checked for available updates and can be set to remind you when (and even automatically perform the update process) every specified amount of time. With iolo WebUpdate, the process of staying up-to-date becomes as simple as clicking a few buttons!

Using the WebUpdate tool

The WebUpdate tool is accessed by selecting the button labeled **Help**, and then selecting the option labeled **Check for product updates**, located on System Shield's main screen. Once the main WebUpdate screen appears, you must select the button labeled "Next" to connect to an iolo update server and check for any available updates. WebUpdate will then list any available updates and their description.

Note: If you have not registered System Shield with iolo technologies yet, you will be presented with a screen that prompts you to do so before connecting to an update server. Registration is highly recommended, but not necessary.

Configuring WebUpdate options

If you would like to modify the options related to the way WebUpdate operates, select the button labeled **Options** while within the WebUpdate wizard. This will display a dialog with WebUpdate's modifiable preferences. For more information on WebUpdate's options see WebUpdate: Options.

Downloading Updates

If updates are available, select the button labeled "Next" to begin downloading them. You will be presented with a status gauge as well as the estimated time it will take to complete the download process.

Installing Updates

Once all of the updates are downloaded, select the button labeled "Install Updates" to replace your existing version of System Shield with the newly downloaded update files.

Completing the Update

Once System Shield has been successfully updated, select the button labeled "Exit and Restart" to close down the currently running version of System Shield and restart with the newly updated version.

Note: This process may take up to a minute and your computer may appear to have stopped responding during this time. Please be patient and do not interrupt this process.

Return to System Shield Main Help Topics

How to obtain product support

If ever during the course of your use of this product you require assistance beyond this documentation, please do not hesitate to contact iolo technologies using the following information:

Web based support: http://www.iolo.com/support

Web based sales: http://www.iolo.com/order

Toll-Free Sales Phone: 877-239-4656

Customer Service Phone: 626-793-3993

Return to System Shield Main Help Topics

Getting started: Using System Shield for the first time

In simple terms, System Shield was designed to protect your system from unauthorized attempts at recovering data that was intended to remain private or confidential.

Most people believe that when a file is deleted, it is permanently and irrecoverably "gone". The error in this belief is that it relies on some basic assumptions that are very far from the truth.

Realistically, the following must be true in order for a file to be irrecoverably deleted:

1. The data within it must not exist anymore
2. Any evidence that the file itself ever existed must be erased

One may ask the question "Well, if I'm deleting a file, aren't these two requirements being met?" The answer is a very grave **no**.

As a matter of fact, the following is true of any file that has just been deleted:

1. The data within it still exists **in its entirety** on your drive.
2. All evidence that the file itself existed is still **very much intact**.
3. Using easily accessible software tools, the file can be **instantly undeleted and viewed** by anyone who has access to your computer.

Obviously, this poses a very significant security problem, and individual PC users who do not wish their data to be accessible after deletion are not the only ones that are subject to this predicament. Businesses, schools, government agencies, and military institutions that frequently deal with extremely sensitive, private, and confidential data are also left wide open and vulnerable to all attempts at breaching security and recovering proprietary information. This highly critical information usually represents dire consequences should it "accidentally" fall into the wrong hands.

- § System Shield is compatible with all Windows versions (95, 98, Me, 2000, XP, etc.) and all Windows file formats (FAT16, FAT32, NTFS)
- § System Shield uses methods approved by the US Department of Defense (DoD 5220.22) to ensure that **ALL** files that have been deleted are permanently disposed of, beyond all possible techniques of recovery.
- § It works by proactively finding files that have been deleted (which will still remain on your drive(s)) and eliminating the data that was once held within them, as well as permanently erasing all evidence that they ever existing on your system in the first place.
- § Its methods work as an after-the-fact defense mechanism, which means that it processes files that have already been deleted using the standard Windows deletion methods (i.e. send a file to the Recycle Bin and then empty it, etc.) One advantage of this approach is that you won't need to rely on a third party "secure" deletion tool to enforce security. Simply delete files as you always have, and then use System Shield to periodically clean up what is left. Another benefit of this technique stems from the fact that many applications delete files internally without giving you a chance to send them to an external secure deletion tool. For example, most word processing software store temporary copies of the documents you work on in order to provide "undo" functionality. When you save changes to your document, the word processor internally deletes these temporary copies (which in most cases hold your documents' data in its entirety). This means that, without your knowledge, there would be several copies of your document on your drive, existing as insecure deleted files. The benefit of System Shield is that **all** of these insecurely deleted files are processed, regardless of whether **you** deleted them or if they were internally created and deleted by another application.
- § It can be scheduled to run its cleaning operations on a regular unattended basis. Therefore, you never need to worry about remembering to clean up your system.
- § It is completely safe: No standard files are affected, and no harmful mechanisms are introduced to your system.

To get started, we recommend the following approach:

1. **Perform a security analysis on all of the drives on your system.**

   For more information see Performing a manual security analysis.
2. **Configure the way you would like to have System Shield deal with insecure data.**

   For more information see Configuring options.
3. **Perform a manual cleaning operation.**

For more information see Performing a cleaning operation.

4. **Set up a scheduled cleaning routine.**
   For more information see Scheduling unattended operations.
5. **Purchase System Shield if you have not already.**
   For more information see How to purchase System Shield.

Configuring System Shield to work for you
Return to System Shield Main Help Topics

Configuring System Shield to work for you

Return to System Shield Main Help Topics

Scheduling unattended operations

Return to Configuration Help Topics

Reading and interpreting information about the drives on your system

In System Shield's main screen, the tab labeled Drive(s) to Clean lists all available drives on your system. In addition to listing hard drives, it also presents helpful information about these devices in their corresponding columns, as described below.

Total space

The total space column displays the corresponding hard drive's maximum data capacity in gigabytes.

Free space

The free space column displays the amount of space in gigabytes left open for new data in the corresponding drive.

Last cleaned

The last cleaned column represents the last date that the corresponding hard drive was cleaned by System Shield.

Security Analysis

The security analysis column contains a tri-colored graph which allows you to determine the ratios between deleted file space, unused free space, and used file space on the corresponding drive.

For more information about how to perform a security analysis and what the various results indicate, see Performing a manual security analysis.

Return to Configuration Help Topics

Configuring options

Selecting drives to include in an operation

To choose which drives are included in the next operation, whether it be cleaning or analysis, make sure that the box that corresponds with the desired drive located in the tab labeled **Drive(s) to clean** is checked.

Cleaning options

Remove deleted file names from your system

The names of the files on your system are kept in a central database located in their corresponding drive. When you delete a file, its name in this database is marked for future reference as a deleted file. This tells the operating system not to display it when listing the contents of the directory it is contained within. There are two main security risks involved herein:

1. Undelete utilities can use these "marked" filenames to obtain information about how to trawl your drive looking for the original file's data which can be pieced back together and lead to a successful undeletion.
2. Even if an undelete tool cannot successfully piece the original file's data back together using the marked filename, it has inherently breached the security of your data simply by knowing that a file used to exist with a specific name. Imagine if you had removed a file named "secret plans.doc". If your system is left uncleaned, an undelete tool will at best be able to fully recover this file, and at worst be able to report back to the investigator that the file "secret plans.doc" did indeed exist on your system. The bottom line is that filenames themselves pose a significant security risk and should be eliminated to ensure protection of data confidentiality.

When this option is enabled, System Shield will remove all references to deleted files from the databases kept on the selected drives. This procedure alone is an excellent method of security enforcement which does not take long to complete and will prevent any software-based undeletion tool from reading in a list of deleted files and attempting to recover them using standard methods.

Remove deleted file information from your system

When you delete a file, Windows does not erase the data that is contained within the file and stored on the drive – it merely marks the file as "available space", which tells the operating system that the space which is occupied by this file may be overwritten if necessary. Data from deleted files usually remains on the drive for months and years before the operating system specifically decides that it needs to overwrite the area of the drive that used to be occupied by a specific file, and hence we encounter a scenario where data from an unlimited number of previously deleted files is vulnerably sitting around in various locations at any given time. This data can be easily brought back using a basic undeletion tool if the deleted filename still exists (see above), or may be equally as easily recovered using a standard drive sector/hex editor.

When this option is enabled, all of the space on your drive that used to be occupied by files (which are now deleted) will be thoroughly purged and cleaned so as to prevent any tools from extracting data from a file that was intended to be removed.

Cleaning techniques

The following options exist with relation to the removal of deleted file information, and may be accessed by selecting the button labeled **Cleaning Techniques** located in System Shield's **Cleaning Options** tab.

Note: These options are only available with the Professional Edition of System Shield.

General Options

Write Signature

When System Shield overwrites the space on your drives that are occupied by deleted files, it uses a special pattern of characters to do so. These characters can range from meaningless zeros and ones, to a special phrase or message that you intend anyone who may be attempting to extract data from your drive to see.

To change the string of characters that used to overwrite deleted file space, you may either select a preset pattern from the drop-down box labeled **Signature to write**, or manually type a pattern or message directly into this box.

Write Method

System Shield provides two ways in which signature data can be written to the drive:

US Department of Defense (DOD 5220.22-M) alternating cycle

You can choose to utilize the write method required by the US Department of Defense, which specifies that

"**hard disk media is sanitized by overwriting with a character, then the character's complement, and then a random character.**" Note that this technique requires at least three overwrite passes to conclude a full cycle.

Use literal (non-cyclical) characters

You can choose to have SystemShield repeatedly overwrite data using the specified signature characters only. Specifically, instead of cycling through each character in the signature and then the character's complement and then a random character, System shield would simply write the same character in the signature for each overwrite pass. The method is useful for those who wish to send a legible message to anyone who dares attempt to inappropriately view the data on their hard drive(s).

Number of Passes

The number of passes option is used to specify the amount of times System Shield will write over the data that is currently occupied by deleted files on your hard drive(s). The advantage to writing over this space at an increasing level is that the more overwrites which are performed, the more difficult it becomes to recover the data that previously resided on the drive. The disadvantage to increasing the number of overwrites is that each additional pass requires an equivalent amount of time to complete, so if a single-pass takes 5 minutes to finish, a seven-pass session will require 35 minutes.

Some basic guidelines to follow when selecting the number of passes to use:

- One pass will stop all software-based data recovery methods such as undeletion utilities, hex, drive, and sector editors, or anything else that purely uses software in order to find and extract data that was once on your system.
- Seven passes will stop all hardware-based recovery methods. This is the technique required by the US Deparment of Defense (DoD 5220.22) as well as many other government agencies. Hardware-based methods are used by professional data-extraction facilities such as forensic science agencies and data recovery companies. Such methods can find data on your drive even after it has been overwritten up to six times. This is due to a "diminishing layers" effect that occurs on all magnetic-based media (hard/floppy/zip drives, etc). This layering phenomenon can be described as follows: As information is overwritten on magnetic media, each overwrite causes the data that previously occupied a specific location to simply become less "bright" than the new data that now rests on top of it. Software that reads the magnetic media is instructed to only recognize the brightest layer. However, using hardware extraction methods such as an electron microscope, these layers can be traced and read up to seven levels down by simply ignoring the brighter layers of data that rest on top of the dimmer, older layers.

Advanced Options

NTFS write buffer size

Under NTFS formatted drives, System Shield is able to use a very efficient writing method that makes use of the advanced features available in this file system. One of these techniques involves the use of variable-size data buffers. When writing to a drive, a data buffer is the chunk of information (in this case comprised of your signature bytes) that is written to the drive at one time. The size of this buffer can range from very small (only a few kilobytes) to very large (several thousand kilobytes), and can make drastic differences in the speed of the operation. As a general rule, slower and older drives work most efficiently with a smaller buffer size (between 100 and 1000), and newer/faster drives have the capacity to better handle large buffer sizes (between 1000 and 20000), translating into quicker writing speeds. The ability to alter the NTFS buffer size is made available because of the very significant differences in speed that can be obtained through adjustment. There is no automatic way of determining your drives' most efficient setting, so some experimentation is in order if your goal is to reach the fastest potential writing speed. If you are unsure about this setting, it is recommended to leave it at its default value of 1000, although no harm will result from experimentation with other values.

Note: This value **only** affects NTFS-based operations.

Automatically removing files in your Recycle Bin

It's easy to forget that when you delete something in Windows, it isn't really deleted, but is rather moved into a temporary storage area called the Recycle Bin. This is extremely helpful in that it allows you to easily change your mind about whether or not to remove these files, however it can be a significant security risk if you forget about something sensitive and leave it vulnerably sitting in your Recycle Bin, ready for anyone to quickly and simply recover and view. System Shield includes an option which allows you to empty your Recycle Bin automatically before performing a system cleaning operation so that any files that reside in the Recycle Bin beforehand will be permanently and securely removed.

To have System Shield empty the Recycle Bin when performing a cleaning operation, select the box labeled **Automatically empty Recycle Bin** located within the Cleaning Options tab.

Note: This option is available under Windows 95 **only** if it has been updated with all pertinent service releases and update packs. Versions of Windows later than Windows 95 will work without these essential updates.

Return to Configuration Help Topics

Specifying preferences

Drive security analysis options

The drive security analysis options correspond to the way System Shield handles the automatic and manual implementation of its security analysis functions. For more information on performing a security analysis, or interpreting the results thereof, see Performing a manual security analysis.

The following options are available:

Analyze drive(s) on startup

If you would like System Shield to automatically perform ad security analysis of your drive(s) whenever it is started, ensure that the box labeled **Analyze drive(s) on startup** is checked. If this option is enabled, the following preferences are available:

- **Automatically scan selected drives on startup**

  If this option is selected, System Shield will scan every drive that is displayed in the list located under the tab labeled **Drive(s) to clean**, whenever it starts.

- **Automatically scan all drives on startup**

  If this option is selected, System Shield will scan only those drives that were chosen for inclusion at the time that the application was last closed.

Analyze drive(s) after cleaning

Many people find that it is helpful to have a visual indication of the results obtained from a cleaning operation. If you would like System Shield to automatically scan each drive that was cleaned after the process has completed, ensure that the box labeled **Analyze drive(s) after cleaning** is checked. If this option is enabled, the following preferences are available:

- **Automatically update analysis after all drives have been cleaned**

  If this option is selected, System Shield will update the security analyses that correspond with the drives that were included in a cleaning operation, after the operations for **all** drives have been completed.

- **Automatically update analysis after each drive has been cleaned**

  If this option is selected, System Shield will update the security analyses that correspond with the drives that were included in a cleaning operation, after the cleaning operations have been completed for **each** drive.

Return to Configuration Help Topics

Performing a manual security analysis

Introduction

System Shield includes a unique function called **Drive Security Analysis**, which can easily be used to provide you with a quick and clear snapshot of the security state of one or more drives on your system. Using the results delivered by the Security Analysis, you can ascertain the current level of risk and vulnerability that your data is exposed to, and take the appropriate actions if any.

The analysis results are presented under the column labeled **Security Analysis** within the **Drive(s) to Clean** tab of System Shield.

Performing a Drive Security Analysis

To perform a security analysis on a group of selected drives, following these steps:

1. Open System Shield and switch to the tab labeled **Drive(s) to Clean**
2. Select the drives you wish to scan by checking their corresponding boxes
3. Select the button labeled **Analyze Drive(s)**
4. Choose the option from the drop down menu labeled **Selected Drives**

To perform a security analysis on all available drives, following these steps:

1. Open System Shield and switch to the tab labeled **Drive(s) to Clean**
2. Select the button labeled **Analyze Drive(s)**
3. Choose the option from the drop down menu labeled **All Drives**

Reading the results of a security analysis

After a drive analysis has been completed, the results will be displayed as colors that represent the percentage ratios between deleted files, unused free (clean) space, and occupied file space. The colored parts of this display are described as follows:

Red (Unsafe deleted files)

Red represents the percentage of space on your drive that is occupied by data that can easily be recovered using simple undelete applications or hex editors. This type of space poses the absolute highest security risk and should be immediately eliminated (see performing a cleaning operation).

Yellow (Unused free space)

Yellow represents the percentage of space on your drive that is occupied by space that is not officially allocated as having been occupied by a deleted file or an existing file. However, this in no way means that the space represented by this color is free of private or confidential past information. If you have used your computer for any length of time without cleaning deleted file information using System Shield (see performing a cleaning operation), it is almost a certainty that space marked as unused will indeed house at least some data that was purportedly removed in the past.

Green (Used file space)

Green represents the amount of space on the corresponding drive that is comprised of files that are visible and useable by the operating system. System Shield does not deal with data that have not been deleted; so ensuring proper security for these this type of data is the responsibility of the PC user.

Return to Configuration Help Topics

Performing a cleaning operation

A cleaning operation takes place when System Shield performs a configured procedure on one or more drives that are installed on your PC. Operations can take place either automatically or manually.

For more information on configuring System Shield's cleaning options, see Configuring options.

For more information on setting up an unattended cleaning schedule, see Scheduling unattended operations.

Starting a manual cleaning operation

To perform a cleaning process manually, follow these steps:

1. Select the drive(s) that you would like to clean by checking their corresponding box under the tab labeled **Drives to Clean**.
2. Review and configure the options that affect how the selected drive(s) will be cleaned. For more information see Configuring options.
3. Switch to the labeled **Drives to Clean** so that you can monitor the cleaning process as it takes place.
4. Select the button labeled **Clean Drive(s)**.

Monitoring the progress of a cleaning operation

During a cleaning operation, various visual cues will appear and be updated which allow you to supervise the procedure as it takes place. These items are described as follows:

- **Active cleaning icon**

  A small animated icon appears near the listed drive that is currently being cleaned.
- **Italicized text**

  The label of the drive that is currently being cleaned is displayed in italicized text.
- **Security Analysis column text**

  The text within the column labeled security analysis is updated with the current status of the corresponding drive.
- **Current drive progress**

  The progress bar labeled **Progress for current drive** indicates the percentage of completion for the currently selected drive.
- **Total drive progress**

  The progress bar labeled **Total progress** indicates the combined percentage of completion for all currently selected drive(s). When this progress bar is 100% full, the cleaning procedure will have finished.
- **Completion time indicator**

  Located in the status bar of System Shield's main window, a label indicating the estimated time required to complete the cleaning operation will be displayed in the format **HOURS:MINUTES:SECONDS**.

Canceling a cleaning operation

If you would like to cancel a currently running cleaning operation, select the button labeled **Interrupt Cleaning** from System Shield's main window, and then select the option labeled **Cancel cleaning**. Alternatively, if the System Shield window is in the foreground, you may press the Esc key on your keyboard to immediately cancel a cleaning operation.

Pausing a cleaning operation

If you would like to temporarily pause a currently running cleaning operation, select the button labeled **Interrupt Cleaning** from System Shield's main window, and then select the option labeled **Pause cleaning**.

Resuming a paused cleaning operation

To resume a paused cleaning operation, select the button labeled **Resume Cleaning** from System Shield's main window.

Canceling a paused cleaning operation

To cancel a paused cleaning operation, ensure that the System Shield window is in the foreground and then press the Esc key on your keyboard.

Return to Configuration Help Topics

Scheduling unattended operations: Introduction

One of the most useful tools contained in System Shield is the ability to schedule cleaning actions to take place automatically at specified intervals. Using the unattended scheduling functions you can set up system cleaning operations to take place automatically, thus ensuring the greatest level of security and protection for your PC – without you having to remember to perform the operations yourself.

Unattended scheduling in System Shield essentially works like so:

1) You configure the options and preferences to be considered when performing a clean
2) You enable unattended scheduling and specify a schedule interval
3) Cleaning actions take place automatically at this interval using iolo technologies' Task Agent application which is included with System Shield, as well as most other iolo products.

Return to Scheduling Help Topics
Return to Configuration Help Topics

Scheduling unattended operations: Enabling automatic cleaning

To enable unattended scheduling, first select the tab labeled **Scheduling**, and then ensure that the box labeled **Enable Automatic Cleaning** is checked. When a scheduling is enabled, the corresponding options become active and available. When scheduling is disabled these options become unavailable and inactive.

For more information about configuring the scheduling options, see Scheduling unattended operations: Configuring the cleaning action

The Task Agent "tray icon"

When unattended scheduling is activated, a small red wrench icon will appear next to your system clock (usually at the lower right side of your screen). This tiny program is the "engine" behind the scheduling mechanism. It keeps track of when items are due to be run and launches them accordingly. It also provides you with a way to quickly access scheduling properties or the main System Shield application if necessary. The actual Task Agent program itself is very small (only 41k) in order to conserve system resources by not requiring the main System Shield application to be loaded at all times.

The properties for the Task Agent tray icon can be accessed by clicking on the icon with your right mouse button.

Return to Scheduling Help Topics
Return to Configuration Help Topics

Scheduling unattended operations: Configuring the cleaning action

When System Shield performs an unattended cleaning operation, it uses the last set of configuration options that were specified in System Shield. For more information see Configuring options.

Return to Scheduling Help Topics
Return to Configuration Help Topics

Utilizing action logs

Return to Configuration Help Topics

Utilizing action logs: Introduction

All of the cleaning actions that are performed by System Shield's tools, whether automatic or manual, are stored in log files by default. These logs track such things as the drives being worked with, the cleaning options and techniques specified, the times and dates these operations are performed, and so on. They are your way of historically monitoring what takes place in the program.

Return to Utilizing action logs Help Topics

Return to Configuration Help Topics

Utilizing action logs: Reading the logs

Operation start and close

The log information that is displayed is organized into chronological sections from top to bottom that each begin with something similar to the following:

```
========================================
OPERATION START: 5/18/2002 11:05:56 AM
========================================
```

…and end with something similar to the following:

```
========================================
OPERATION COMPLETE: 5/18/2002 11:06:00 AM
========================================
```

The information that is contained within these two markers corresponds to the actions that took place while the tool was being used (either manually, or automatically).

Options specified

After the indicated start of the operation, the log file will report the states of the various options specified for that particular instance. For example:

```
Preparing to clean drive: E
Purge deleted file names:   Yes
Eliminate deleted file data:   No
Empty Recycle Bin before cleaning:   No
This is a manual operation
```

Action progress

The actual cleaning process is denoted by the text marker "Start Cleaning…" All logged actions after this marker are representative of the events that took place during the cleaning action. For example:

```
Start Cleaning...
  Drive E:  Removing deleted filename entries
  Drive E:  521 total filename entries processed.
  Drive E:  Cleaning complete
```

Return to Utilizing action logs Help Topics

Return to Configuration Help Topics

Utilizing action logs: Working with log data

Clearing (resetting) the log file information

Over time, the information in your log files will begin to age and lose its current relevance. At this point, you may decide to reset the information contained therein. You may do this in the following manner:

1) From the tab labeled **Logs**, select the button labeled "**Clear Logfile**".
2) Confirm your decision to permanently erase the information in the log by selecting "**Yes**" when the confirmation prompt appears. If you would like to cancel the removal process select "**No**".

Viewing, printing, or modifying the log files

In order to make it easy to view, modify, and print log information System Shield provides you with the ability to view log information in your default text editor (usually Windows Notepad application). Using your text editor you can view the contents of the file at a larger scale, print it, or edit the contents of the file and resave it. To open the log file in your text editor use the following steps:

1) From the tab labeled **Logs**, select the button labeled "**View logfile in Text Editor**".
2) Your default text editor will open with the corresponding log information loaded. Once the information is displayed in your text editor you may print it or modify and resave it. If you modify the information in a log, you will need to "refresh" System Shield's logfile display in order to view the changes. You can do this by either switching to another tab and then back to the tab labeled **Logs**, or by restarting the application.

Return to Utilizing action logs Help Topics
Return to Configuration Help Topics

Utilizing action logs: Enabling and disabling logging

To toggle the setting which tells System Shield whether or not to save cleaning action events to a log you may use the following steps.

To enable logging:

From the tab labeled **Logs**, ensure that the box labeled **Save cleaning operation details to logfile** is checked.

To disable logging:

From the tab labeled **Logs**, ensure that the box labeled **Save cleaning operation details to logfile** is unchecked.

Return to Utilizing action logs Help Topics
Return to Configuration Help Topics

Scheduling unattended operations: Specifying a schedule

To modify the schedule that is adhered to when automatic cleaning actions are initiated, select the button labeled **Change Schedule** from the tab labeled **Scheduling**. This will bring up the Scheduled Items Properties dialog. This window contains all of the available scheduling options for a given tool. The scheduling options are broken down into three sections:

Timed Intervals

Every XX Minutes

This option will trigger at the next run date and time, then wait for the specified number of minutes, and then run again, etc. For example, if you specify "every 30 minutes" and the action initially started at 1:00, the next run time would be 1:30, then at 2:00, and so on.

Every XX Hours at XX minutes after the hour

This option will trigger at the next run date and time, wait for the specified number of hours, then wait until the specified minutes are matched on the clock, and then run again, etc. For example, if you specify "every 5 hours at 30 minutes after the hour" and the action initially started at 1:00, the next run time would be 6:30, then at 11:30, and so on.

Every XX Days at the following time: XX

This option will trigger at the next run date and time, wait for the specified number of days, then wait until the specified time is matched on the clock, and then run again, etc. For example, if you specify "every 5 days at 1:00" and the action initially started on Sunday at 2:00, the next run time would be on the following Saturday at 1:00 (Friday at 1:00 would not have been a total of 5 days yet), then on the next Thursday at 1:00 (exactly 5 days from then), and so on.

Every XX Weeks starting on XX

This option will trigger at the next run date and time, wait for the specified number of weeks, then wait until the specified day, and then run again, etc. For example, if you specify "every 1 week starting on Sunday" and the action initially started on Monday, the next run time would be 13 days from then (the first Sunday would not have yet been a week), on a Sunday, and then exactly 7 days later on the next Sunday, and so on.

Every XX Months starting on day XX of the month

This option will trigger at the next run date and time, wait for the specified number of months, then wait until the specified day of the month, and then run again, etc. For example, if you specify "every 1 month starting on day 1 of the month" and the action initially started January 2, the next run time would be March 1 (February 1 would not have been a month yet and February 2 does not match the specified "day 1"), the next run time would be April 1, and then May 1, and so on.

Externally Triggered Intervals

Externally triggered intervals are intervals that are triggered by something that you manually perform such as turning the computer on, etc. The following external triggers are available:

Each time Windows starts

This option will run the action at the start of each Windows session.

Next Run Date and Time

The next run date and time options provide a manual way to override when the action will next run. Remember, the timed interval options base their schedules on when the last time and date maintenance for a specific tool was run.

Return to Scheduling Help Topics
Configuring System Shield to work for you

Scheduling unattended operations: What happens if one or more actions are not performed on time?

If any of your regularly scheduled items are not run at their designated time, they are automatically run the next time the Task Agent application is loaded. Their schedules are set to reflect a last run date and time of that at which they were successfully executed, and schedules are adjusted accordingly.

Return to Scheduling Help Topics

Configuring System Shield to work for you

Scheduling unattended operations: How often should I run the automatic cleaning action?

Although there are no real disadvantages to automatically running a clean operation more often than needed, here is what we have found to be the most appropriate intervals:

Personal, low-risk based security

If you do not frequently keep highly-secure or extremely confidential information on your computer, or are merely concerned about securing private information that carries no materially tragic consequences should it fall into the wrong hands, we recommend a conservative approach to cleaning as follows:

- Remove deleted filenames: Every 3-5 days
- Remove files in Recycle Bin: Every 3-5 days
- Remove deleted file information: Every 7 to 14 days
- Number of recommended overwrite passes: 1

Medium level security

If you occasionally keep highly sensitive information on your PC such as passwords, credit card numbers, personal letters, private pictures, etc., or if potentially dire consequences may arise should any of the information kept on your system fall into the wrong hands, we recommend the following approach to cleaning:

- Remove deleted filenames: Every 1-2 days
- Remove files in Recycle Bin: Every day
- Remove deleted file information: Every 3 to 5 days
- Number of recommended overwrite passes: 1

High level security

If you frequently deal with very sensitive or confidential information, or tend to keep information on your computer that would be highly dangerous if it fell into the wrong hands, we recommend the following approach to cleaning:

- Remove deleted filenames: Every day
- Remove files in Recycle Bin: Every day
- Remove deleted file information: Every 1 to 3 days
- Number of recommended overwrite passes: 7

Absolute mission-critical security

If the information on your PC absolutely must remain private at all costs, we recommend the following approach to cleaning:

- Remove deleted filenames: Every day
- Remove files in Recycle Bin: Every day
- Remove deleted file information: Every day
- Number of recommended overwrite passes: 10

Return to Scheduling Help Topics
Configuring System Shield to work for you

WebUpdate: Options

Automatically Check for Updates Every X Days

Using this option you can modify two elements of the WebUpdate tool:

1) To toggle WebUpdate's automatic checking and reminder system, uncheck the box labeled **Automatically check for updates every...**. If this box is unchecked, WebUpdate will no longer remind you when it has been a certain amount of time since you have last checked for product updates.
2) To adjust the amount of days WebUpdate waits before checking for new updates, enter a new value in the box labeled **Automatically check for updates every...**. The minimum amount of days WebUpdate will wait is one day, and the maximum it will is 360 days.

Connect using a Proxy Server

If you or your company uses a proxy server to access the internet you will need to specify this before using WebUpdate. Use the following steps to set up WebUpdate for use via a proxy server:

1) Select the button labeled **Options** from the main WebUpdate wizard
2) Check the box labeled **Connect using a Proxy Server**.
3) In the box labeled **Proxy Server**, specify the server name or address
4) In the box labeled **Proxy username**, specify your username for use with the proxy server
5) In the box labeled **Password**, specify your password for the proxy server
6) Select the button labeled **OK**.

Return to How to upgrade your copy of System Shield
Return to System Shield Main Help Topics

Licensing System Shield

Tips for successfully entering your licensing information

Below are some common mistakes that are made while attempting to license System Shield:

1) Spaces **anywhere** in the User ID or Serial Number will result in an error.

Correct Example:
12345-SP123-1234567890

Incorrect Example:
12 345 – sh 123 – 123456 7890

2) The User ID may include a "-" and a number at the end. This information is necessary.

Correct Example:
johndoe@domain.com-3

Incorrect Examples:

- johndoe
- John Doe - 3
- johndoe@domain.com
- johndoe@domain.com - 3

Note: If you purchased System Shield from a reseller, this User ID will not appear as an email address.

3) The **only** letters in the serial number are **SP** or **SR**. Every other character is a number. The User ID is not case sensitive.

4) If your User ID appears as an email address, it **must** be the e-mail address **shown in your invoice** usually followed by a hyphen (dash) and a number. You may **not** substitute your current e-mail address for the address shown in the original invoice unless you have issued an updated User ID and corresponding serial number.

5) If after following these steps you receive an message relating to incorrect or invalid licensing information, please re-check the above steps once again and ensure that you are following them carefully. Please also verify that you are typing the information in **exactly** as it is shown on your invoice.

Note: Your licensing information is unique to your purchase of this product. Please keep this information private and safe.

Return to System Shield Main Help Topics

Upgrading from System Shield Personal Edition to Professional Edition

System Shield is offered in two different versions, tailored to your security requirements:

System Shield Personal Edition $39.95 (click here for multi-computer pricing)

- Protection from all **software-based** data recovery tools such as file-undelete products, hex/disk editors, etc.
- Ability to schedule unattended data clean-up operations automatically
- Compatible with all Windows versions (95, 98, Me, 2000, XP) and all Windows file formats (FAT16, FAT32, NTFS)
- Comprehensive drive security analysis which provides a graphical representation of current risk level

System Shield Professional Edition $129.95 (click here for multi-computer pricing)

All features and functions contained in Personal Edition, plus:

- Protection from all forms of **advanced hardware-based** recovery mechanisms such as specialized forensic techniques and electron microscopes
- Full compliance with US (DoD 5220.22), German, and all other known published government-level data disposal security requirements
- Ability to customize data wiping security signature

Upgrade from System Shield Personal to System Shield Professional Edition $100

How to Upgrade

If you are currently licensed as a System Shield Personal Edition user and would like to upgrade to the Professional Edition, you may do so using the following steps:

1. Purchase an upgrade license. Click here to order securely online, or here to see additional ordering options.
2. Enter your new licensing information. To do this, follow these steps:
    a. Select the button labeled **Help** from the main System Shield screen.
    b. Select the option labeled **Upgrade to Professional Edition**, and then **Enter upgrade licensing information**
    c. You will be presented with the System Shield licensing screen. Enter your new licensing information here, and finally select the button labeled **OK** to complete the upgrade process. If you have questions about entering your licensing information, click here.

Note: Prices and availability are subject to change without notice.

Return to System Shield ordering information
Return to System Shield Main Help Topics

What is the difference between System Shield Personal Edition and Professional Edition

System Shield is offered in two different versions, tailored to your security requirements:

System Shield Personal Edition $39.95 (click here for multi-computer pricing)

- Protection from all **software-based** data recovery tools such as file-undelete products, hex/disk editors, etc.
- Ability to schedule unattended data clean-up operations automatically
- Compatible with all Windows versions (95, 98, Me, 2000, XP) and all file formats (FAT16, FAT32, NTFS)
- Comprehensive drive security analysis which provides a graphical representation of current risk level

System Shield Professional Edition $129.95 (click here for multi-computer pricing)

All features and functions contained in Personal Edition, plus:

- Protection from all forms of **advanced hardware-based** recovery mechanisms such as specialized forensic techniques and electron microscopes
- Full compliance with US (DoD 5220.22), German, and all other known published government-level data disposal security requirements

Ability to customize data wiping security signature

Upgrade from System Shield Personal to System Shield Professional Edition $100

Click here for information on how to upgrade from System Shield Personal Edition to Professional Edition

Note: Prices and availability are subject to change without notice.

Return to System Shield ordering information
Return to System Shield Main Help Topics