eSafe Desktop
Quick Start Guide

This quick start guide will help you to quickly setup eSafe Desktop. Please follow this entire manual to quickly learn how eSafe Desktop can solve common security issues and to ensure a trouble-free implementation.

If you wish to explore more advanced features of eSafe Desktop or require additional help, be sure to read the User's Manual.

Table of Contents

www.eAladdin.com

ALADDIN®

Securing the Global Village

Installation

Step 1. Insert the eSafe Desktop CD or locate the eSafe Desktop setup file that you downloaded from the Internet. Launch the eSafe Desktop setup program to start the installation.

Step 2. Select **Install eSafe Desktop** from the menu that appears.

Step 3. Select the language that you prefer for the eSafe Desktop interface. The default is English.

Step 4. This causes the **eSafe Desktop License Agreement** to appear.

Step 5. Read the conditions of the eSafe Desktop EULA and click **I accept** if you agree to these conditions.

Step 6. Follow the instructions that appear on screen.

Note: It is highly recommended that you click OK when the setup program offers to download the latest version from the Internet, including virus signature tables.

Upon completion, the setup program adds a program group to your **Start** menu. The group contains an icon to uninstall eSafe Desktop.

Uninstall

Step 1. Click the Windows **Start** button and select P**rograms | eSafe Desktop| Uninstall eSafe Desktop**.

Step 2. Follow the instructions that appear on screen.

Changing your protection level

The eSafe Watch screen contains a protection setting lever and buttons for accessing the configuration screens and the anti-virus module.

Protection setting lever

The protection setting lever lets you change your level of protection. It contains four settings: **Extreme**, **Normal**, **Low** and **Off**.

Extreme

eSafe Desktop exits Learn mode, thereby activating those sandboxes. The Sandbox, Personal Firewall and On-access scanner modules are all activated.

Normal

All modules are activated as configured.

Low

The Sandbox module is deactivated. On-access scanner and Personal Firewall modules are activated.

Off

All eSafe Desktop modules are deactivated.

Operation

Diagnostic Check

When you start Windows, eSafe Desktop loads and performs a diagnostic check of its component files.

Note: The diagnostic check does NOT scan your disk for viruses.

Warning Screens

eSafe Desktop intervenes whenever it detects a virus or a violation of its protective rules.

Don't Panic - your computer is safe

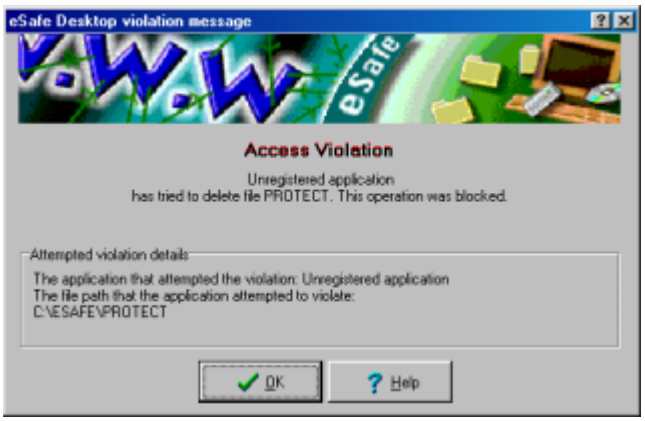
eSafe Desktop already intervened to prevent the potentially dangerous operation. Relax, take you time to read and understand the warning, nothing can happen - you are protected.

Read the warning

There are three types of warning screens, each of which contains different information and allows for different actions. These are:

- Access Violation
- eSafe Desktop Warning (virus/vandal found)
- eSafe Desktop Warning (Active Desktop)

Access Violation



This screen lets you know that a protective mechanism intervened to prevent a potentially dangerous action, usually from the Internet, from wreaking untold havoc on your computer. The following dialog box will appear when you click **OK**.

Note: It is important that you understand that active content has legitimate uses, and may be used by one of your legitimate programs. Take the time to make sure that the file that caused the violation is, in fact, part of a legitimate application that you want to use. The decision that you make can open a security hole, allowing this file to run in the future without your knowledge.

If you want to perform the action that has been blocked, you must run the operation again after clicking Allow until next boot or Allow in future.

What happened?

The first part of the Access Violation screen describes the action.

The information appearing in the message provides you with the information that you need, to decide whether the action is a legitimate one that you want to allow.

In order to understand this information, you need to know that it contains two pieces of information. The first is the name of the program or application that attempts the action. The second is either the path to the threatened area of your hard disk or the rule being broken.

Offending application

If the action was performed by an application installed on your computer, the application name appears. If the action was performed by an application not installed on your computer, "Unregistered application" appears in place of the application name.

Threatened path or rule

If the second piece of information is a rule, you must decide whether this rule should apply to the application. If your application is expected to break this rule as part of normal operation, then the action is legitimate. If not, you can assume that the action is dangerous and should report it to your network administrator.

If the second piece of information is a file path, it indicates that the offending application attempted one of the following:

- Read a file containing sensitive information
- Make changes to the (existing) file
- Delete the file from your computer
- Move, copy or rename the file
- Create the file on your computer
- Execute the file

What should I do?

If you are familiar with the application, look to see if the threatened area contains files or data that this application is expected to use. If so, it is probably a legitimate operation, and as such should be allowed in the future. If you click **Allow in future**, eSafe Desktop changes the protective mechanism that intervened, to allow this in the future.

If the action is one that you do not recognize or do not want this application to perform, you should click **Do not allow**. This option lets eSafe Desktop know that it should warn you of such violations in the future.

If you are not familiar with the application or if you recognize it as an active content file, you should proceed with caution. Depending on the action that occurred, you should click either **Allow until next boot** or **Do not allow**.

Silent mode - don't ask me

At the bottom of the Access Violation screen there is check box. If you select it, eSafe Desktop stops sending you this screen when the same protective mechanism intervenes.

This will not prevent a similar Access Violation screen from appearing if a different protective mechanism intervenes.

Note: You cannot undo this because the same protective mechanism will not send you any more Access Violation screens.

---

eSafe Warning - virus/vandal found

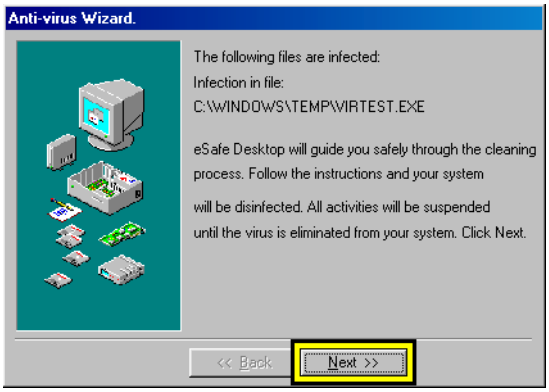
This warning occurs when a virus or vandal is encountered. It lists the path of the virus or vandal, and contains a button to run the Anti-virus Wizard. This wizard removes the virus found by the on-access scanner.

Note: If you do not want to run the wizard, click the x in the upper right corner to close the window.

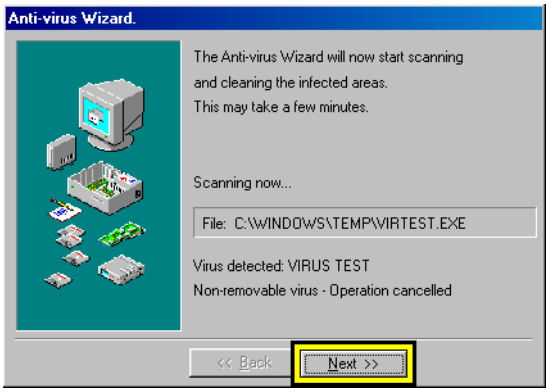
Running the Anti-virus Wizard

Step 1. Click **Run wizard** in the **eSafe Warning** screen.

Step 2. Click **Next**.

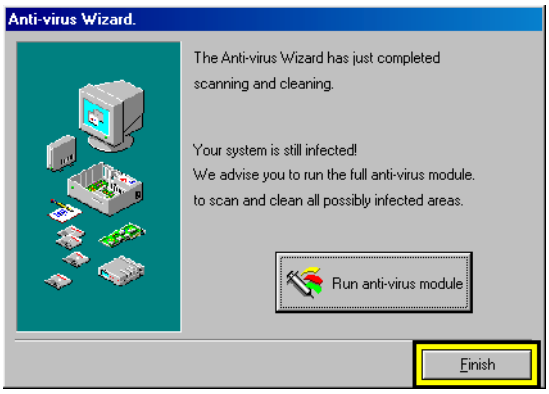


Step 3. Click **Next** again.



Step 4. Click **Scan Now**.

Step 5. Click **Finish**.



Note: If you want to perform an on-demand virus check of other files, click Run anti-virus module instead of Finish.

eSafe Warning - Active Desktop

The Active Desktop allows you to place Internet sites directly on your Windows Active Desktop. As a result, the eSafe Desktop warns you of when you attempt to place a sites on the Active Desktop containing potentially dangerous ActiveX, Java or active scripts.

The warning screen allows you to place the item on a list of trusted items, remove it from the Active Desktop, or edit the list of trusted and untrusted sites. eSafe Desktop allows you to access all pages of the sites listed as trusted, and prevents you from accessing any page in sites listed as untrusted.

Allowing placement of active content on the Active Desktop

Click **Allow always** in the **eSafe DesktopWarning** dialog box.

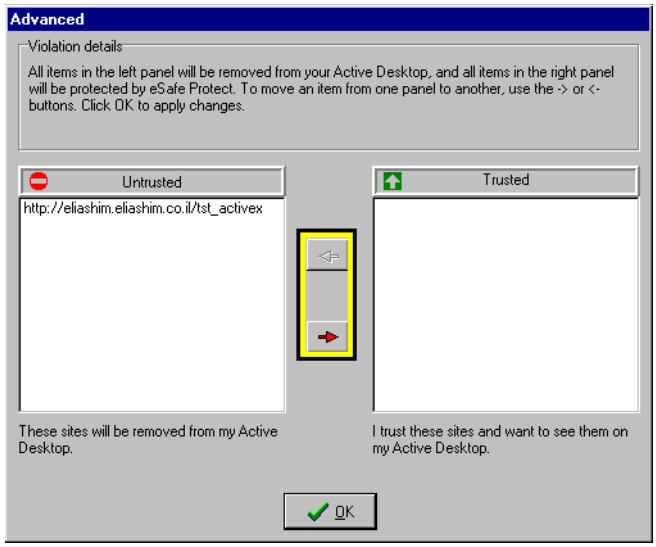
Preventing placement of active content on the Active Desktop

Click **Don't allow** in the **eSafe Desktop Warning** dialog box.

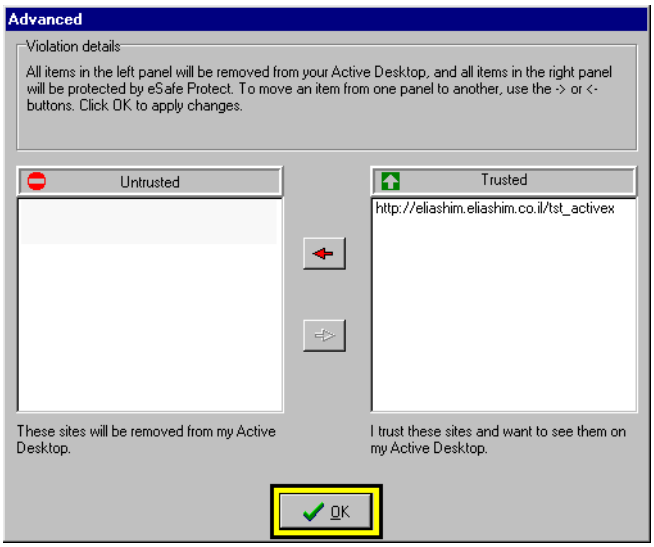
Making changes to the lists of trusted and untrusted sites

Step 1. Click **Advanced** in the **eSafe DesktopWarning** dialog box.

Step 2. Select the item to be moved and click the arrow pointing to the target list.



Step 3. Click **OK**.



Scanning for Viruses

The on-demand scanner scans and cleans all files susceptible to viruses on the disks and directories that you select.

When should I scan for viruses?

Although eSafe Desktop contains an on-access scanner that checks files as you access them, it is a good idea to initiate a scan of all floppy diskettes and CDs the first time you enter them into your computer.

You should scan archive files that you copy from the network or other source. The on-access scanner only inflates and scans archives downloaded from the Internet.

If a virus is discovered in an archive file, you should inflate the archive and scan all files individually. Due to the nature of scanning archive files, if an infected file contains more than one virus, it is possible that not all viruses are reported. Furthermore, it is always best to scan the files whenever you extract them from an archive file.

You should scan you hard disk(s) on a regular basis. We recommend scanning your disks at least once a week. If you leave your computer on during lunch breaks or overnight, you can schedule the anti-virus scanner to automatically scan your hard disk during off hours. For more information, contact your network administrator.

Why bother?

There are a number of ways in which a virus can enter your computer without being scanned by the on-access scanner. For example, files located on your computer prior to installation of eSafe Desktop may never have been scanned.

The on-access scanner is designed to scan for viruses without interfering with normal operation. This requires it to make certain assumptions that the on-demand scanner does not, such as ignoring files copied from one directory to another on the same hard disk.

Finally, as new viruses are discovered, eSafe creates updates that your network administrator automatically distributes to you over the network. A new virus can theoretically slip through by being scanned by the on-access scanner before the virus becomes known and the scanner updated. By initiating a scan, you check all files using the latest version of eSafe Desktop.

How do I scan for viruses?

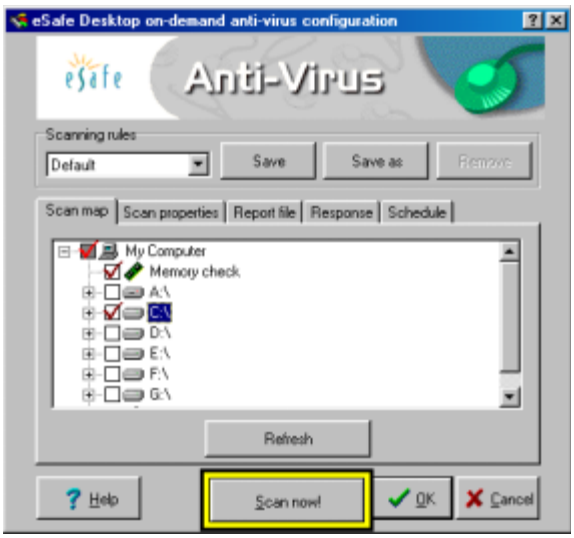
Scanning for viruses

Step 1. Select **Start|Programs|eSafe|Run eSafe Anti-virus**.

Note: An alternate method is to double click the eSafe icon in at the far right of Windows Taskbar, then click the ANTI-VIRUS button on the eSafe Watch screen that appears.

Step 2. Select the drives to scan. You can open the tree to be more specific and select specific directories or files.

Step 3. Click **Scan Now**.



Scanning for viruses from Windows Explorer

Step 1. Right-click the file, folder, or drive.

Step 2. Select **Scan for viruses** if available. If not, open the **Select to** option and select **Scan for virus**.

Rescue Diskette

What is it?

An eSafe Desktop rescue diskette is a clean, locked diskette. It contains: its own boot files, an image of the hard disk boot sectors, the partition table, the configuration stored in CMOS RAM, and the files necessary to successfully remove viruses from an infected hard disk.

Who needs it?

Anyone with a computer, who does not want to lose data if a virus destroys the boot sectors, partition table, or configuration stored in CMOS RAM. Each rescue diskette is for a specific computer only, and you cannot use the rescue diskette of another computer.

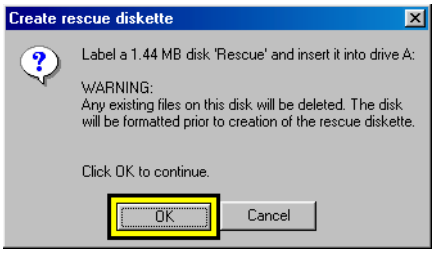
This diskette is necessary to clean and restore the hard disk if your computer does become infected with a virus that affects the boot sectors, partition table, or configuration stored in CMOS RAM. Without it, you may need to reformat the entire disk.

How do I create a rescue diskette?

Creating a rescue diskette

Step 1. Click Windows **Start** button and select **Programs | eSafe Desktop | Make Rescue Diskette**. This causes the following window to appear.

Step 2. Click **Yes**. This causes the following window to appear.



Step 3. Label a 1.44 Mb floppy disk as your eSafe rescue diskette, place it in your floppy drive and click **OK**.

Step 4. Click **Finish**, then remove and lock the diskette.

Advanced configuration

You should begin by making changes that you want to apply to **all** users.

Step 1. Click **Advanced configuration**. This opens the **Advanced configuration** , which is divided into the following four modules:

a. Sandbox for protection from hostile Java, ActiveX, and other malicious mobile code.

b. Personal Firewall for port control and Internet content filtering.

c. Administrator for applying user protection settings and desktop lockdown.

d. Anti-virus for customizing virus scan operation.

Step 2. Select the module to edit by clicking its button on the left.

Step 3. Edit the configuration.

Step 4. Click **Exit**.

Sandbox – anti-vandal protection

The Sandbox limits Internet applications to a **confined** area that prevents hackers from using your Internet applications to access areas of the drives containing vital information. Sandbox configuration is organized into four tabs.

- **Sandbox boundaries**
  Displays and defines the areas of the hard drive and privilege settings that the protected applications are allowed to access.
- **Operation mode**
  Defines whether the Sandbox is **enabled**, in **Learn mode** or **disabled**.
- **Enforcement**
  Defines how the Sandbox reacts when a violation occurs.
- **Media to monitor**
  Defines which drives are monitored for violations.

Note: The default configuration is designed to require minimal changes.

Placing the Sandbox in Silent mode

Silent mode prevents users from receiving warning messages. All events are still logged for use by the report generator. By default, only the **Freeze Desktop** Sandbox is in Silent mode.

Step 1. Select the Sandbox to place in **Silent mode** from the drop down menu.

Step 2. Select the **Enforcement** tab.

Step 3. Select an **Illegal activity**.

Step 4. Select the **Silent mode** check box.

Step 5. Repeat steps 3 and 4 for each of the other illegal activities.

Step 6. Click **Save**.

Blocking access to certain files – advanced users only

You may want to create a general purpose Sandbox to serve as an access control mechanism that is active continuously. A general purpose Sandbox restricts access to selected directories. You can also restrict certain directories to **Read-only** to prevent users from modifying the files contained inside.

Step 1. Select the **Blank** Sandbox from the drop down menu.

Step 2. Click **Save as**.

Step 3. Name the new Sandbox and click **OK**.

Step 4. Edit the access rights based on paths.

Step 5. Select the **Enforcement** tab and place each illegal activity in Silent mode.

Step 6. Enter the **Privileges** tab of the **Administrator** module and assign the new Sandbox to the user.

eSafe Desktop comes with the following two **General purpose** sandboxes defined.

Blank

This Sandbox restricts access to the C:\ESAFE\PROTECT\DATA directory to prevent users from deleting eSafe Desktop. It is enabled by default.

Freeze Desktop

This Sandbox allows only read and execute privileges on the **Windows Desktop** and **Start** menu. This prevents users from modifying, deleting or adding new icons to the **Windows Desktop** or **Start** menu. The **Freeze Desktop** Sandbox is **not** enabled by default. To **enable** this Sandbox, you must go to the **Privileges** tab of the **Administrator** module and assign it to the user.

Note: You can use the Save as option to create additional Sandboxes based on existing ones, but they will not become active unless you assign them in Administrator|Privileges.

Personal Firewall – port control and content filter

The Personal Firewall blocks ports used by Trojan horses and other vandals, and filters out inappropriate content. This submodule is organized into five tabs.

- **Firewall map**
  Controls access to specific Ports and IP addresses.
- **Content Filter**
  Allows you to block content based on specific forbidden words.
- **Privacy**
  Prevents sensitive information, such as personal details and credit card numbers, from being submitted to sites that are not secure.
- **Operation times**
  Specifies the time of day when the Personal Firewall is active.
- **Enforcement**
  Defines how the Personal Firewall reacts when a violation occurs.

Configuring the Content Filter

Step 1. Select one of the existing Personal Firewalls from the drop down menu.

Step 2. Select the **Content Filter** tab and review the content.

Step 3. Add or remove any words that you feel necessary. Defaults are usually sufficient.

Note: You also need to assign the Personal Firewall(s) in Administrator|Privileges.

Administrator – assignment of protective functions

The **Administrator** module allows you to grant and restrict system privileges, and assign specific eSafe Desktop functions to users. It contains the following elements:

- **Reports**
  Defines the information to be logged for reports.
- **Privileges**
  Assigns Privileges, Sandboxes, and Personal Firewalls.
- **Password**
  Prevents unauthorized modification to eSafe Desktop configuration.
- **Boot operations**
  Assigns operations to be performed when the PC boots-up.
- **Active modules**
  Enables activation/deactivation of **Sandbox**, **Personal Firewall** and **Anti-virus** modules.

Note: You can use Administrator|Active Modules to isolate problems when

trouble-shooting by enabling and disabling specific Sandboxes and Personal Firewalls.

Activating and editing desktop lockdown

Step 1. Click the **Privileges** tab.

Step 2. Open the **Privileges** tree in the left pane and double-click **Enforce User Privileges**. This activates system policy protection.

Step 3. Open the user branch and the subsequent **Privileges**.

Step 4. Open each group of privileges that you want to edit. The green check mark enables the function, while the red X disables that function.

Step 5. Double-click each privilege that you want to change from enable to disable or vice-versa.

Step 6. Click **Apply**.

Note: Other security programs and products, such as the Windows Policy Editor, Fortress, and Foolproof, duplicate many of the desktop lockdown features of eSafe. If you are using any other security products, DO NOT enable the desktop lockdown feature of eSafe Desktop because doing so may cause conflicts.

Enabling Sandboxes and Personal Firewalls

Step 1. Click the **Privileges** tab.

Step 2. Open the user branch in the left pane.

Step 3. Open **Sandboxes** or **Personal Firewalls** in the right pane.

Step 4. Select the Sandbox or Personal Firewall that you want to apply and click the red arrow above to move it to the user in the left pane.

Step 5. Repeat for each Sandbox and Personal Firewall you want to enable.

Step 6. Click **Apply**.

Disabling/enabling eSafe Desktop modules

If you are using other anti-virus or content filtering products, you may want to disable certain eSafe Desktop modules that could conflict with your existing software.

Step 1. Click the **Modules** tab.

Step 2. Disable any modules you do **not** want to use.

Auto-updating of anti-virus signature tables

When you initially installed eSafe Desktop, an auto-update utility was installed on the PC. This checks the eSafe FTP site every 7 days (default). If there is a new virus signature table, it downloads it and installs the update to the ESPLAN directory on the server. When users log on, it pushes the update to the PCs to protect them from the latest virus and vandal threats.

The auto-update utility allows you to change the frequency that it checks the FTP site for new signature tables.

Regular vs. hot update

Regular updates consist of virus signature tables that have been tested and approved by QA. These updates are considered 100% reliable. However, the test process cannot always keep up with the latest breaking viruses. The auto-update utility does not download **hot updates**.

Whenever a new virus is discovered, a hot update is prepared to detect and possibly remove the virus. This update is considered very reliable, but never the less, has not been tested as thoroughly as the regular update. In some cases the hot update may only detect a virus, but not be able to remove it without damaging or deleting the infected file.

Step 1. Open your browser and go to http://www.esafe.com/udate.html .

Step 2. At the eSafe update site, select **Updates| Hot update**.

Step 3. Execute the downloaded file at the server that will deploy it.