Robust Antivirus for Mac

User Guide

Robust Antivirus Technologies
www.abcexample.com

Copyright Information

Document Release History

Robust Antivirus for Mac was first published in 2000. The following table lists subsequent changes made to the software.

Date	Location	Description
MM-DD-YYYY	Chapter number and name, not page number	Added new section.
MM-DD-YYYY	Chapter number and name, not page number	Oldest entry is last
MM-DD-YYYY	Chapter number and name, not page number	Added new section.

Contents

1

Introduction

Robust Antivirus ensures maximum protection against any possible threats or malware that may infect your system when you browse online, work in network environment, and access emails. You can schedule scanning, set rules for Quarantine and Backup for files, set parental control, and block malicious emails and spams.

Mac Security Helps you customize the settings that concern the protection of files and folders in your system. You can set scanning preferences, apply rules for virus protection, schedule scanning, exclude files and folders from scanning, and set rules for quarantine and backup files.

Web Security Helps you set the protection rules to save your computer from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on.

Parental Control Parental Control in Web Security helps you monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

Email Security Helps you customize the protection rules for receiving emails from various sources. You can set rules for blocking emails which are suspicious of spam, or malware.

2

Using Robust Antivirus

To begin using Robust Antivirus, follow these steps:

Step 1: Get started	Step 2: Install Robust Antivirus	Step 3: Activate your license	Step 4: Run first scan

Step 1: Get started

Before you begin, ensure the following things:

Prerequisites

Remember the following guidelines before installing Robust Antivirus on your computer:

- Remove any other antivirus software, if you have it on your computer.
- Close all open programs before proceeding with installation.
- Keep a backup of your data in case your computer is infected with viruses.

System Requirements

To use Robust Antivirus, your system should meet the following minimum requirements:

- Mac OS X 10.6 or later
- Mac Computer with Intel Processor
- 512 MB of RAM
- 700 MB free hard disk space

Step 2: Install Robust Antivirus

To install Robust Antivirus on your computer, follow these steps:

1 Insert the installation CD/DVD into the drive.

A window with the installer and uninstaller packages appears.

In case, the installer does not appear, search for the disk image on your desktop and open it. Download or copy the installation file (Robust Antivirus.dmg) to your desktop, and then open it.

2 To launch the installer, click Robust Antivirus.pkg.

The user acceptance agreement screen appears.

3 Click Continue.

4 On the Welcome screen, click Continue.

The Read Me file appears. You are expected to read the Read Me file in its entirety.

5 Click Continue.

The End-User License Agreement screen appears. Read the agreement carefully.

6 Click Continue.

7 Click Agree to proceed with the installation.

8 To initiate the installation, click Install.

Robust Antivirus is set to be installed on your computer at the fixed location. Moreover, you cannot change the location while installing the software.

9 Provide your user credentials when prompted.

Robust Antivirus installation process starts.

10 To initiate the activation process, click Register Now.

11 Click Register Later or Continue to perform activation later.

12 On Summary page, click Close to close the installer window.

Step 3: Activate your license

Activate your license immediately after installation to receive security updates regularly against new threats and get technical support.

1 Go to Application > Robust Antivirus.

2 On the Robust Antivirus Dashboard, click Register Now. Alternatively, you can go to Menu > Help > Activation.

3 On the Registration Wizard, enter the 20-digit Product Key and click Continue.

The Registration Information appears.

4 Enter relevant information in the Purchased From and Register for text boxes and then click Continue.

5 Provide relevant information in the Name, Email Address, Contact Number text boxes. Select your choices in the Country, State and City lists.

In case your State/Province and City are not available in the list, you can type your locations in the respective boxes, and then click Continue.

A confirmation screen appears with the details entered in the preceding step. If any modifications are needed click Go Back to go to the previous screen and modify wherever required, and then click Continue.

Your product is activated successfully. The expiry date of your license is displayed.

6 To close the Registration Wizard, click Finish.

Step 4: Run first scan

On successful completion of installing Robust Antivirus, you must run a complete scan of your computer. The complete scan detects and cleans any possible virus and malware, removes all duplicate files, folders, images, and other junks, and optimizes scanning process in future. With Scan My Mac, you can scan the entire computer, files and folders including mapped network drives, folders, and files.

To initiate Scan My Mac, follow these steps:

1. On the Robust Antivirus Dashboard, click the Scan My Mac list showing at the bottom right.
2. On the scan option, click Scan My Mac to initiate complete scanning of your computer.

Upon completion of the scan, you can view the scan report under Reports > Scanner Reports.

3

Robust Antivirus Features

The Robust Antivirus features include the most important features that help you set the scanning preference, protection rules for your computer, scanning schedule, set rules for Quarantine and Backup for files, apply protections for online browsing, set parental control, and block malicious emails and spams.

These features provide optimum protection to your system. Moreover, these features must be kept enabled all the time. If you disable these features, for any reasons, then the corresponding icons for them will turn red.

Mac Security

The Mac Security option on Dashboard helps you customize the settings that concern the protection of files and folders in your system. With Mac Security, you can set scanning preferences, apply rules for virus protection, schedule scanning, exclude files and folders from being scanned, and set rules for quarantine and backup files.

Mac Security includes the following:

Scan Settings

With Scan Settings, you can customize the way a scan is to be performed and the action that needs to be taken when a virus is detected. However, the default settings are optimal and can provide the required protection for your computer.

To configure Scan Settings, follow these steps:

1. On the Robust Antivirus Dashboard, click Mac Security.

   The Mac Security setting details screen appears.

2. Click Scan Settings.
3. Set the appropriate option for scan type, action to be taken if virus is found in the files, and whether you want to take the backup of the previous setting.
4. Click Save to save your settings.

Select scan type

- *Automatic (Recommended)*: Automatic scanning type is the default scanning mode, which is recommended as it ensures optimal protection that your computer requires. This setting is an ideal option for novice users as well.

- *Advanced*: Select Advanced mode if you want to customize the scanning behavior. This is ideal for experienced users only. When you select the Advanced option, the Configure button is enabled and you can configure the Advanced setting for scanning.

Action to be taken when virus is found

The action that you select here will be taken automatically if the virus is found, so select an action carefully. The actions and their descriptions are as follows:

Actions	Description
Repair	Repairs the infected system. While scanning, if a virus is found it repairs the file or automatically quarantines it, if it cannot be repaired. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware, then Robust Antivirus automatically deletes the file.
Delete	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. Once the files are deleted, they cannot be recovered.
Skip	Takes no action. If this option is selected the files are scanned but no action is taken on the infected files, and they are skipped. Select this option if you want to take no action even if a virus is found. When the scan is over a summary report appears providing all the scan details.
Backup before taking action	Takes a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from the Quarantine menu.

Configuring Advanced Scan Type

To configure Advanced Scan type, follow these steps:

1 On the Robust Antivirus Dashboard, click Mac Security.

The Mac Security setting details screen appears.

2 Click Scan Settings.

3 In Scan type, select Advanced.

The Configure button is enabled.

4 Click Configure.

The Advanced Scan setting details screen appears.

5 Check *Items to be scanned* for Windows-based malwares.

By default this option is selected.

6 Select one of the following items for scanning:

- *Scan executable files*: Select this option if you want to scan only the executable files.

- *Scan all files*: Select this option if you want to scan all types of files. However, it takes time to execute this option, and the scanning process slows down considerably.

7 Turn *Scan archived files* ON, and then configure the scanning preference for the archive files such as zip files and so on.

8 To close the Archive Files screen, click OK. To close the Advanced Scan setting, click OK and then click Save to save your settings.

Scan archive files

If you select *Scan archive files*, then the scanner will also scan archive files such zip files, archive files, and so on. If you select *Scan archive files*, the Configure button is enabled and helps you configure the way scanner should treat malicious archive files. You can scan files of various archive file types till five levels down so to ensure no files are left from being scanned.

The following are the actions that you can select to be taken when a virus is found in any of the archive files:

Actions	Description
Quarantine	Select this option if you want to quarantine an archive file that contains a virus.
Delete	Select this option if you want to delete an archive file that contains virus-infected files. However, you are not notified if a file is deleted, though its report is generated as you may see in the Reports list.
Skip	Select this option if you want to take no action even if a virus is found in any of the archive files. However, this option is selected by default.

Archive Scan level

Set the scan level till which you want to scan the archive files. You can set till five levels down inside the archive files. By default, the scanning is set to level 2. However you can increase the archive scan level which may though affect the scanning speed.

Select archive type to scan

You can select the archive file types that you want to scan from the archive files list. Some of the common archive file types are selected by default. However, you can change your setting as you prefer.

Types	Description
Select All	Select this option to select all the archive file types available in the list.
Deselect All	Select this option to clear all the archive types available in the list.

When the scan is complete, a summary report appears providing details about all the actions taken and other scan details, irrespective of the option that you had configured.

Virus Protection

With Virus Protection, you can continuously monitor your computer from viruses, malware, and other malicious threats. These threats try to sneak into your computer from various sources such as email attachments, Internet downloads, file transfer, file execution and so on.

It is recommended that you always keep Virus Protection enabled to keep your computer clean and protected from any potential threats. However, Virus Protection is enabled by default that you can disable if required.

To configure Virus Protection, follow these steps:

1. On the Robust Antivirus Dashboard, click Mac Security.

   The Mac Security setting details screen appears.

2. To protect your computer from malicious threats, turn Virus Protection ON.
3. To configure Virus Protection further, click Virus Protection.
4. On the Virus Protection screen, do the following:
   - *Items to scan* – Select this checkbox if you want to scan Windows-based malwares. However, this checkbox is selected by default.
   - *Scan network volume* – Select this option if you want to scan network volumes that are mounted on your computer. However, this option is turned on by default.
   - *Display notifications* – Select YES if Display notifications is selected, it displays an alert message whenever a malware is detected. This feature is selected by default.
   - If virus found – Select an action to be taken when virus is found in a file such as Repair, Delete, and Deny Access.
   - Backup before taking action – Select this option if you want to take a backup of a file before taking an action on a file. Files that are stored in backup can be restored from the Quarantine menu.
5. To save your setting, click Save.

Action to be taken when virus is detected

Actions	Description
Repair	While scanning, if a virus is found it repairs the file or automatically quarantines it, if it cannot be repaired.
Delete	Deletes a virus-infected file without notifying you.
Deny Access	Restricts access to a virus infected file from use.

Turning Off Virus Protection

Turn Virus Protection OFF. However when you try to turn off Virus Protection, an alert message is displayed. Turning Virus Protection OFF is suggested only when you really require this. Moreover, you can set it off for a certain period of time so that it turns ON automatically thereafter.

The following are the options for turning Virus Protection OFF for a certain period:

- Turn on after 15 minutes
- Turn on after 30 minutes
- Turn on after 1 hour
- Turn on after next reboot
- Permanently disable

Select an option and click OK.

Once you turn off Virus Protection, its icon color changes from green to red in Menu Bar Tray, which means that Virus Protection has been disabled temporarily or permanently based on your selection. If you have selected any of the options for turning off temporarily or after next boot then the icon color changes back from red to green after the certain time passes or at the next boot. If you have selected to disable permanently, then the icon color remains red until you enable Virus Protection manually.

Schedule Scans

With Schedule Scans, you can define time when to begin scanning of your computer automatically. You can schedule multiple number of scan schedules so that you can initiate scanning of your computer at your convenient time. Frequency can be set for daily and weekly scans, that can additionally refine your request to schedule it to occur at fixed boot at fixed time.

Configure Schedule Scans

To configure Schedule Scans, follow these steps:

1. On the Robust Antivirus Dashboard, click Mac Security.
2. On the Mac Security setting screen, click Schedule Scans.

   The Scheduled Scans details screen appears. Here you see a list of all schedules for scanning, if you had defined any before.
3. To create a new schedule for scanning, click Add.

   The Add Scheduled Scan screen appears where you can create a new scan schedule name, its frequency, and other details.
4. In the Scan name text box, type a scan schedule name.
5. Set Scan Frequency:
   - *Daily*: Select the Daily option if you want to initiate scanning of your computer daily. However this option is selected by default.
   - *Weekly*: Select the Weekly option if you want to initiate scanning of your computer on a certain day of the week. When you select the Weekly option, the Weekly list is enabled where you can select a day of the week.
6. Set Scan Time:

- *Start scan at first boot*: Select the *Start scan at First Boot* option to schedule the scanner to scan at first boot of the day. When you select Start at first boot, you do not have to specify the time of the day to start the scan. Scanning takes place only during the first boot irrespective at what time you start the system.
- *Start scan at Fixed Time*: Select the *Start scan at fixed time* option if you want to initiate the scanning of your computer at a certain time. When you select Fixed Time, the Start Time list is enabled where you can fix the time for scanning. However this option is selected by default.

7 Set Scan priority.

- *High*: Select the High option if you want to have the scanning priority at high.
- *Low*: Select the Low option if you want to have the scanning priority at low. However this option is selected by default.

8 Scan location:

- Click Configure to open the Scan location screen, where you can select files and folders for scanning. You can set multiple locations. Select the Drives, folder or multiple folders to be scanned and press OK. You can configure Exclude Subfolder while scanning specific folder. This will ignore scanning inside the subfolders while scanning.

9 Scan settings:

- Click Configure to open the Scan Settings screen. Under Scan Settings, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advance options while scanning. By default setting is set for adequate options for scanning.
- ▪ In Scan type, select one of the options from Automatic and Advanced.
  To know about how to configure scan setting, see Scan Settings, p-10.
- ▪ Select YES if you want to have a backup of files before taking any action on them, otherwise select NO if you want no backup of files. This option is selected by default.

10 To save your settings, click Save.

Edit Schedule Scan

You can modify any of the scheduled scans whenever required. To edit a scheduled scan, follow the steps:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Schedule Scans.

A list of all scan schedules appears.

3 Select a scan schedule and then click Edit.

4 In the Add Schedule Scan screen, change the scan schedule as required.

5 To save your settings click Save and then click Close.

Remove Schedule Scan

If you do not require a scan schedule, you can remove it whenever you require. To remove a scan schedule, follow these steps:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Schedule Scans.

A list of all scan schedules appears.

3 Select a scan schedule, and then click Remove.

4 Click YES to confirm if you are sure to remove the scan schedule, and then click Close.

Exclude Files & Folders

With Exclude Files & Folders, you can decide which files and folders should not be included during scanning for known viruses or issues. This helps you avoid unnecessary repetition of the scanning of the files which have already been scanned or you are sure should not be scanned. You can exclude files from scanning from both of the scanning modules Mac Security Scanner and Virus Protection.

! Total Security Scanner scans files and folders when you scan manually while Virus Protection scans each file and folder when accessed automatically.

Configure Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Exclude Files & Folders.

The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning, if you have added any.

3 Click Add.

4 On the New Exclude Item screen, click the File button or Folder button to add relevant files or folder to the list.

When you add a folder you can check Exclude Subfolders so that the subfolders are also excluded from scanning.

5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.

6 To close the Exclude Files and Folders screen, click Close.

Edit Exclude Files & Folders

You can change your setting for Exclude Files & Folders if you require so in the following way:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Exclude Files & Folders.

The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning that you have added.

3 Under Location, select a file or folder, and then click Edit.

4 On the New Exclude Item screen, click the File button or Folder button to add another file or folder to the list.

When you add a folder you can check Exclude Subfolders so that the subfolders are also excluded from scanning.

5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.

6 To close the Exclude Files and Folders screen, click Close.

Remove Exclude Files & Folders

You can remove any files or folders that you included in the Exclude Files & Folders list if you require in the following way:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Exclude Files & Folders.

The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning that you have added.

3 Under Location, select a file or folder, and then click Remove. You can remove all files and folders from the list by clicking Remove All.

The selected files or folders are removed from the exclusion list.

4 To close the Exclude Files and Folders screen, click Close.

Quarantine & Backup

Quarantine & Backup helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Robust Antivirus encrypts the file and keeps it inside the Quarantine folder. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of infected file before repairing if the Backup before repairing option is selected in the Scanner Settings.

With Quarantine & Backup, you can also set a rule for removing the files after a certain period and having a backup of the files.

Configure Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1 On the Robust Antivirus Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Quarantine & Backup.

3 In Delete files automatically after, drag the slider to select days after which the files should be removed from the Quarantine folder automatically.

! Setting this feature helps in removing the quarantine/backup files after the configured period. The removal of files is set to 30 days by default.

4 Click View Files to see the quarantined files. You can take any of the following actions on the quarantined files:

- *Add File*: You can add files from folders and drives to be quarantined manually.
- *Restore Selected*: You can restore the selected files manually if required so.
- *Submit Selected*: You can submit the suspicious files to Robust Antivirus research lab for further analysis from the Quarantine list. Select the file which you want to submit and then click Submit.
- *Delete Selected*: You can delete the selected files from the quarantine list.
- *Remove All*: You can remove all the Quarantine files from the Quarantine list.
- Submit Quarantine file functionality.

  In Quarantine, when you select a file and click the Submit button , a prompt appears requesting permission to provide your email address. You also need to provide a reason for submitting the files. Select one of the following reasons:

- *Suspicious File* – Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
- *File is un-repairable* – Select this reason if Robust Antivirus has been able to detect the malicious file on your system during its scans, but has not been able to repair the infection of the file.
- *False positive* – Select this reason if a non-malicious data file that you have been using and are aware of its function, has been detected by Robust Antivirus as a malicious file.

Web Security

With Web Security, you can set the protection rules to save your computer from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on. You can also set parental control to monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

Web Security includes the following:

Browsing Protection

With Browsing Protection, you can block malicious websites while browsing so that you do not come in contact with malicious websites and you are secure. However, Browsing Protection is enabled by default.

Configure Browsing Protection

To configure Browsing Protection, follow these steps:

1 On the Robust Antivirus Dashboard, click Web Security.

2 Enable Browsing Protection.

You can disable Browsing Protection whenever you prefer.

Phishing Protection

With Phishing Protection, you can prevent access to phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. It usually appears to have come from well-known organizations and sites such as banks, companies and services with which you do not even have an account and, ask you to visit their sites telling you to provide your personal information such as credit card number, social security number, account number or password.

Phishing Protection automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the Internet. It also prevents identity theft by blocking phishing websites, so you can do online shopping, banking and website surfing safely.

Configure Phishing Protection

To configure Phishing Protection, follow these steps:

1. On the Robust Antivirus Dashboard, click Web Security.
2. Enable Phishing Protection.

You can disable Phishing Protection whenever you prefer. However, you are advised always to keep Phishing Protection enabled.

Parental Control

With Parental Control, the parents can have full control over the Internet activity of their children or other users. Parents can decide which websites their children should visit and which they should not. Using the Parental Control feature, the parents can restrict categories of websites or block specific websites. The parents can also schedule Internet accessibility for their children.

Parental Control is smart enough to categorize all the sites accessed. It has a list of categories of sites that you can allow or deny based on your requirement. This is perfect for parents, who want to ensure that their kids visit the right kind of websites and are not exposed to materials unsuitable for kids.

Important things to do before configuring parental control!

To get utmost benefits from the parental control feature, we recommend you follow a few steps:

Configure Parental Control

To configure Parental Control, follow these steps:

1. On the Robust Antivirus Dashboard, click Web Security.
2. On the Web Security setting screen, click Parental Control.
3. Configure the following options based on your requirement:

- *Restrict access to websites based on the category*: When you select this option, you restrict access to all websites under a similar category.
- *Restrict access to websites as specified by user*: When you select this option, you restrict access to specific websites only.
- *Schedule Internet access*: This option helps you schedule Internet accessibility for your children or other users.

4 To save your settings, click Save.

Restrict access to websites based on category

The Restrict access to websites based on the category feature in Parental Control has a vast range of website categories to allow or deny access to them based on the requirements. Once you restrict or allow a website category, all the websites falling under a category are blocked or allowed. This is helpful if you are sure to restrict or allow all the websites under a category. Moreover, if you want to restrict most of the websites in a category but allow certain websites of that category, which is either required or you rely on, you can do so by excluding such websites in the Exclude list.

To configure access restriction for website categories, follow these steps:

1 On the Robust Antivirus Dashboard, click Web Security.

2 On the Web Security setting screen, click Parental Control.

3 Under Restrict access to websites, switch *Based on the category* to YES to restrict website categories.

The Configure button is enabled.

4 Click Configure.

- A list of website categories whose access can be allowed or denied appears. Click the Allow or Deny button available next to each category that you want to allow or restrict as required. Moreover, the default settings are perfect for novice users and they can retain the default settings for their children.
- You can also exclude a website from being blocked, despite it being in the blocked category, by adding it to the Exclude list. For example, if you have blocked the Social Networking and Chat category, but you still want to provide access to Facebook, you can do so by enlisting the website in the Exclude list.

  i. On the Web Category list, click Exclude for excluding the websites.

  ii. Enter the URL of the website in the list that you want to allow users to access and then click Add.

  Similarly, if you want to remove a website from the exclusion list, select the URL that you want to remove and click Remove. Click Remove All to delete all the URLs from the exclusion list.

  iii. To save the changes, click OK.

5 Click OK and then click Save to save your settings,.

Restrict access to websites as specified

The Restrict access to websites as specified by user feature in Parental Control helps you block specific websites. This is helpful when you are sure to restrict certain websites and when your list is shorter than it can be in a website category. This is also helpful when a website does not fall into a correct category, or you have restricted a website category, yet a certain website is accessible that you want to block.

To configure access restrictions for specific websites, follow these steps:

1. On the Robust Antivirus Dashboard, click Web Security.
2. On the Web Security setting screen, click Parental Control.
3. Under Restrict access to websites, switch *As specified by user* to YES to restrict specific websites.

   The Configure button is enabled.
4. Click Configure.

   A list for adding websites appears.
5. Enter the URL of the website to be blocked and then click Add.

   You can add as many websites as you require. Moreover, you can remove any website whenever you require so. Select the websites that you want to remove and click Remove. You can also remove all the websites in the list by clicking Remove All.
6. Click OK.
7. To save your settings, click Save.

Schedule Internet access

The Schedule Internet access feature in Parental Control helps you schedule Internet accessibility for your children so as you have full control over their browsing time. You can allow your children access the Internet without any restriction or can schedule Internet accessibility. You can schedule days and times when your children should access the Internet.

To configure Schedule Internet access, follow these steps:

1. On the Robust Antivirus Dashboard, click Web Security.
2. On the Web Security setting screen, click Parental Control.
3. Switch *Schedule Internet access* to YES to configure Internet accessibility to your children.

   The Configure button is enabled.
4. Click Configure.

   The Schedule Internet Access setting details screen appears.
5. Select one of the following:

   - *Always allow access to the Internet*: Select this option if you want to allow access without any restriction to your children.

- *Allow access to the Internet as per the schedule*: Select this option if you want to schedule Internet accessibility for your children. When you select this option, the routine chart for the days of the week is enabled.
  - Click a cell in the routine chart for a time period of a day. You can select any time period of any day based on your requirement.
  - If you want to schedule a regular period of time for the entire week (like 8:00 AM to 10:00 AM for all days in a week), hover over the time period, or if you want to restrict access to Internet for an entire day (like Sunday) hover over the day, an arrow appears. Click the time period or the day, your restriction applies accordingly. Your children can access the Internet only during the allowed schedule.

6 To save your setting, click OK.

Time Specification	Description
Allowed Time	All the cells appearing in green indicate allowed time frequency for accessing the Internet.
Blocked Time	All the cells that are not appearing green indicate blocked time frequency for accessing the Internet.

Email Security

With Email Security, you can customize the protection rules for receiving emails from various sources. You can set rules for blocking emails which are suspicious of spam, or malware.

Email Security includes the following.

Email Protection

With Email Protection, you can enable protection rules for all incoming emails. You can block the infected attachment in the emails that may be suspicious of malware, spam, and viruses. You can also customize the action that needs to be taken when a malware is detected in the emails.

However, Email Protection is enabled by default and the default settings provide the required protection to the mailbox from malicious emails. We recommend that you always keep Email Protection enabled to ensure email protection.

Configure Email Protection

To configure Email Protection, follow these steps:

1 On the Robust Antivirus Dashboard, click Email Security.

2 On the Email Security setting screen, enable Email Protection.

Protection against malwares coming through emails is enabled.

3 To configure further, protection rules for emails, click Email Protection.

4 Turn *Notify on email* ON if you want an alert message when a virus is detected in an email or attachment.

! The alert message on virus includes the following information: Virus Name, Sender Email Address, Email Subject, Attachment Name, and Action Taken.

5 Select one of the following actions to be taken if virus is found.

- *Repair*: Select Repair to get your emails or attachment repaired when a virus is found
- *Delete*: Select Delete to delete the infected emails and attachments.

! If the attachment cannot be repaired then it is deleted.

6 Switch *Backup before taking action* to YES if you want to have a backup of the emails before taking an action on them.

You can revert to default settings anytime you require so by clicking Set Defaults.

7 To save your settings, click Save.

Spam Protection

With Spam Protection, you can block all unwanted emails such as spam, phishing and porn emails, from reaching into your mailbox. Spam Protection is enabled by default, and we recommend you always keep the feature enabled.

Configure Spam Protection

To configure Spam Protection, follow these steps:

1 On the Robust Antivirus Dashboard, click Email Security.

2 On the Email Security setting screen, turn Spam Protection ON.

3 To configure further protection rules for spam, click Spam Protection.

4 Turn *Tag subject with text* ON to include the tag “spam” to the suspicious emails.

5 Select one of the following:

- Turn White List ON if you want to allow emails from the email addresses enlisted in the whitelist to skip from spam protection filter, and then click Configure to enter the email addresses.
- Turn Black List ON if you want to filter out emails from the email addresses enlisted in the blacklist and then click Configure to enter the email addresses.

6 Click OK.

7 To save your settings, click Save.

Setting spam protection rule for White List

White List is the list of email addresses from which all emails are allowed to skip from spam protection filter irrespective of their content. No emails from the addresses listed here are passed through the SPAM filter. It is suggested that you configure only such email addresses which you rely on fully.

To add email addresses to the White List, follow these steps:

1 Turn White List ON.

The Configure button is enabled.

2 Click Configure.

3 Enter the email addresses in the list and click Add.

Edit or Remove Email: To edit an email address, select the email address in the list and click Edit. To remove an email address, select an email address and click Remove.

Import White List: You can import the White List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

Export White List: You can export the White List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.

4 To save your settings, click OK.

Setting spam protection rule for Black List

Black List is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -". This feature should be specifically evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.

To add email addresses to the Black List, follow these steps:

1 Turn Black List ON.

The Configure button is enabled.

2 Click Configure.

3 Enter the email addresses in the list and click Add.

Important: While entering an email address, be careful that you do not enter the same email address in the blacklist that you entered in the whitelist, else a message appears.

Edit or Remove Email: To edit an email address, select the email address in the list and click Edit. To remove an email address, select an email address and click Remove.

Import Black List: You can import the Black List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

Export Black List: You can export the Black List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.

4 To save your settings, click OK.

Adding Domains to White List or Black List

To add specific domain in the White List or Black List, follow these steps:

1 Turn White List or Black List On and click Customize.

2 Type the domain and click Add. For editing an existing entry, click Edit.

Note: The domain should be in the format: *@mytest.com.

3 To save the changes, click OK.

4

Technical Support

Our support system includes the following.

Web Support

With Web Support, you can submit your queries and see FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions. Moreover, it is advisable that you check with your queries in FAQ at least once before you make use of other support systems as you may get an answer to your question in FAQ itself.

To use Web Support, follow these steps:

1. On the Robust Antivirus menu bar, go to Help > Support.
2. On the Support screen, click Visit FAQ under Web Support to view FAQ or submit your queries.

Check the answer to your queries in FAQ. If you do not find an appropriate answer, then submit your queries to us.

Email Support

With Email Support, you can send us an email about your queries so that experts at Robust Antivirus can reply to you with an appropriate answer.

To use Email Support, follow these steps:

1. On the Robust Antivirus menu bar, go to Help > Support.
2. On the Support screen, click Submit under Email Support to submit your queries.

Clicking on the Submit button redirects you to our Support webpage where you can submit your queries online.

Phone Support

With Phone Support, you can call us for instant support from our Robust Antivirus technical experts.

The following is the contact number for phone support: 1800 2000 5000.

Remote Support

With Remote Support, you can get us connected to your system remotely. Remote Support is useful when you need solutions carried by our experts. However, it is advised that you make use of this support when you are connected over telephone.

To use Remote Support, follow these steps:

1. On the Robust Antivirus menu bar, go to Help > Support.
2. Click Remote Support.

   The Remote Support terms agreements screen appears.
3. Click I Agree.

   The details for remote access such as IP address and remote access ID are displayed. Provide these details to the remote support engineers who will connect to your system. Robust Antivirus Support executive will remotely access your system to fix the issue.

Live Chat Support

With Live Chat Support, you can log on to the chat room of Robust Antivirus and ask about your issues that you may be facing. You can get technical support directly from with Robust Antivirus technical executives.

Head Office

Robust Antivirus Technologies

Pune 411005, India

Email: support@robustantivirus.com.

Website: www.abcexample.com