

# Antivirus

## User Guide

# Copyright & License Information

---

Copyright © 2017 Antivirus, INC. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Antivirus, INC.

Marketing, distribution or use by anyone barring the people authorized by Antivirus, INC. is liable to legal prosecution.

## **Trademarks**

Antivirus is a registered trademark of Antivirus, INC. while Microsoft and Windows are registered trademarks of Microsoft Corporation.

## **License Terms**

Installation and usage of Antivirus is subject to user's unconditional acceptance of the Antivirus end-user license terms and conditions.

To read the license terms, visit [www.abc.com/eula](http://www.abc.com/eula) and check the End-User License Agreement for your product.

# Contents

---

<b>Getting Started .....</b>	<b>4</b>
Prerequisites.....	4
General guidelines .....	4
General requirements .....	4
Specific system requirements for various Microsoft Windows OS .....	4
Installing Antivirus .....	5
Registering Antivirus.....	6
<b>Antivirus Dashboard .....</b>	<b>7</b>
About Antivirus Dashboard.....	7
<b>Security Features .....</b>	<b>8</b>
Files & Folders .....	8
Scan Settings .....	8
Virus Protection.....	10
Advance DNAScan .....	12
How DNAScan is effective? .....	13
Block Suspicious Packed Files.....	14
Screen Locker Protection .....	14
Scan Schedule.....	15
Parental Control .....	16
Ensure the following requirements for effective control of Parental Control .....	17
Configuring Parental Control .....	17
<b>Index .....</b>	<b>24</b>

# Getting Started

---

You can install and use Antivirus on as many computing devices as your product key allows. This limit can be found in your product pack. You can install Antivirus on any combination of PC, laptop, or mobile with either Windows operating system (OS), Mac OS, or Android OS.

During installation, read each installation screen carefully and follow the instructions.

## Prerequisites

Following are the guidelines and system requirements.

### General guidelines

Remember the following guidelines before installing Antivirus on your system.

- Remove any other antivirus software program from your computer if you have any. Multiple antivirus software products installed on a single computer may result in system malfunction.
- Close all open applications, browsers, programs, and documents for uninterrupted installation.
- Ensure that you have administrative rights for installing Antivirus.

### General requirements

Ensure that your computer meets the following requirements.

- 1.4 GB free hard disk space on your computer
- Internet Explorer 6 or later
- Internet connection to receive updates

### Specific system requirements for various Microsoft Windows OS

Ensure that your computer meets the following system requirements for your operating system.

*Table 1: Operating systems*

Operating Systems (OS)	Minimum System Requirements
Windows 10	Processor: 1 gigahertz (GHz) or faster RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit
Windows 8.1 / Windows 8	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows 7	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows Vista	Processor: 1 GHz or faster RAM: 1 GB
Windows XP (32-bit) (Service Pack 3)	Processor: 300 Megahertz (MHz) Pentium or faster RAM: 512 MB

## Installing Antivirus

To install Antivirus, follow these steps:

1. Click the product installer.

The installation wizard performs a pre-install virus scan of the system. If a virus is found active in memory, then:

- The installer automatically sets the boot time scanner to scan and disinfect the system on the next boot.
- After disinfection of your computer, the computer restarts and you need to re-initiate the installation.

If no virus is found in the system memory, the installation proceeds.

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

2. At the end of the license agreement, there are two options **Submit suspicious files** and **Submit statistics** which are selected by default. If you do not want to submit the suspicious files or statistics or both, clear these options.
3. Select **I Agree** if you accept the terms and then click **Next**.

The Install Location screen appears. The default location where Antivirus is to be installed is displayed. The disk space required for the installation is also mentioned on the screen.

4. If the default location has insufficient space, or if you want to install Antivirus on another location, click **Browse** to change the location or click **Next** to continue.  
The installation is initiated. When installation is complete, a message appears.
5. Click **Register Now** to initiate the activation process or click **Register Later** to perform activation later.

# Registering Antivirus

You must register your product immediately after installing it. Unless you register the product, it will be considered as a trial version. A subscriber with registered license can use all the features without any interruptions, take the updates regularly, and get technical support whenever required. If your product is not regularly updated, it cannot protect your system against the latest threats.

To register Antivirus online, follow these steps:

1. Select **Start > Programs > Antivirus > Activate Antivirus**.
2. On the Registration Wizard, enter the 20-digit Product Key and click **Next**.  
The Registration Information appears.
3. Enter relevant information in the **Purchased From** and **Register for** text boxes, and then click **Next**.
4. Provide your **Name**, **Email Address**, and **Contact Number**. Select your **Country**, **State**, and **City**.  
If your State/Province and City are not available in the list, you can type your locations in the respective boxes.
5. Click **Next** to continue.  
A confirmation screen appears with the details you entered.  
If any modifications are needed, click **Back** to go to the previous screen and make the required changes.
6. Click **Next** to continue.  
Your product is activated successfully. The expiry date of your license and the count of the registered devices are displayed.
7. Click **Finish** to close the Registration Wizard.

## Note

---

After you register Antivirus, you are prompted to create an account with Antivirus RDM, which allows you to manage your device remotely.

# Antivirus Dashboard

---

The Antivirus Dashboard serves as the main interface to all the features of Antivirus. Antivirus protects your system even with the default settings. You can open Antivirus to check the status of protection, to manually scan the system, view reports, and update the product.

You can manually start Antivirus in any one of the following ways:




- Select **Start > Programs > Antivirus > Antivirus**.
- On the taskbar, double-click the **Antivirus** icon or right-click the **Antivirus** icon and select **Open Antivirus**.
- Select **Start > Run**, type Scanner and press the **Enter** key.

## About Antivirus Dashboard

While working with computer system, you are connected to the Internet, external drives, and send and receive email communications. This makes your system exposed to viruses that try to infiltrate into your system.

### Tips

If the antivirus detects any threat in your system, it is indicated through color coded icons. You must pay attention to the detected threats.

Color	Icons	Description
Green		Indicates that Antivirus is configured with optimal settings and your system is protected.
Orange		Indicates that a feature of Antivirus needs your attention at your earliest convenience, but not immediately.
Red		Indicates that Antivirus is not configured with optimal settings and your immediate attention is needed. The action corresponding to the message needs to be carried out immediately to keep your system protected.

*Table 2: Status icons*

# Security Features

---

Antivirus Protection Center includes the following features.

Features	Description
Files & Folders	Includes Scan Settings, Virus Protection, Advance DNAScan, Block Suspicious Packed Files, Automatic Rogueware Scan, Anti-Keylogger, Screen Locker Protection, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Includes Email Protection, Trusted Email Clients Protection, and Spam Protection.
Internet & Network	Includes Firewall Protection, Browsing Protection, Malware Protection, Phishing Protection, Browser Sandbox, Safe Banking, News Alert, and IDS/IPS.
Parental Control	Allows parents to control the Internet access, application access, and computer access for the children and other users.
External Drives & Devices	Includes Autorun Protection, Scan External Drives, Data Theft Protection, and Scan Windows Mobile.

*Table 3: Security features*

## Files & Folders

With this feature, you can configure the protection settings for files and folders in your system.

Files & Folders includes the following protection settings.

## Scan Settings

This feature helps you initiate the scanning of your system and select an action to be taken when a virus is detected. However, the default settings are optimal that ensures the required protection to your system.

To configure Scan Settings, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Settings**.
4. Under [Select scan mode](#), select **Automatic (Recommended)** to initiate the scan automatically, or select **Advanced** for [advanced level scanning](#).



5. Under [Select action to be performed when virus is found](#), select an appropriate action.
6. If you want to take a backup of the files before taking an action on them, select **Backup before taking action**.
7. To save your settings, click **Save Changes**.

### Select scan mode

You can select one of the following scan modes:

- **Automatic (Recommended):** It is the default scan type and is recommended as it ensures the optimal protection to your system. This setting is an ideal option for novice users.
- **Advanced:** This option helps you customize the scan method. This is ideal for experienced users. When you select the Advanced option, the Configure button is activated and you can configure the Advanced settings for scanning.

### Action to be performed when a virus is found

Configure one of the following actions that must be taken when a virus is detected:

Action	Description
<b>Repair</b>	Select this option if you want to repair an infected file. If a virus is found during a scan in a file, it repairs the file. If the file cannot be repaired, it is quarantined automatically. If the infectious file has a Backdoor, Worm, Trojan, or Malware, Quick Heal Total Security automatically deletes the file.
<b>Delete</b>	Select this option if you want to delete an infected file. The infected file is deleted without notifying you. Once the files are deleted, they cannot be recovered.
<b>Skip</b>	Select this option if you want to take no action on an infected file.
<b>Backup before taking action</b>	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from Quarantine.

Table 4: Actions for infections

### Configuring Advanced Scan Mode

To configure Advanced Scan mode, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Settings**.
4. Under [Select scan mode](#), select **Advanced**.

The Configure button is activated.

5. Click **Configure**.

The advanced scan setting details screen appears.

6. Under **Select item to scan**, select **Scan executable files** if you want to scan only the executable files or select **Scan all files** if you want to scan all files.

However, the Scan executable files option is selected by default.

It takes time to carry out **Scan all files** and the process may slow down your system.

7. Select one of the following items for scanning:

- **Scan archive files**: Select this option if you want to scan the archive files such as zip files and RAR files.
- **Scan packed files**: Select this option if you want to scan packed files.
- **Scan mailboxes**: Select **Quick scan of mailboxes** for a brief scan or else select **Through scan of mailboxes** to scan thoroughly.

8. Click **OK**.

9. Click **Save Changes** to save your settings.

## *Scan archive files*

This feature helps you further set the scan rules for archive files such as ZIP files, RAR files, and CHM files.

To configure the Scan archive files feature, follow these steps:

1. On the [advanced scan setting](#) screen, select **Scan archive files**.

The Configure button is activated.

2. Click the **Configure** button.

The Scan archive files details screen appears.

3. Under **Select action to be performed when virus is found**, select one of the following options: Delete, Quarantine, and Skip.

4. In **Archive Scan Level**, select the level till you want to scan the files and folders.

The default scan level is set to level 2. However, increasing the default scan level may affect the scan speed.

5. Under **Select the type of archive that should be scanned**, select the archive files types.

6. Click **OK** to save your settings.

## Virus Protection

Viruses from various sources such as email attachments, Internet downloads, file transfer, and file execution try to infiltrate your system. This feature helps you to

continuously keep monitoring for viruses. Importantly, this feature does not re-scan the files that have not changed since the previous scan. This helps in maintaining lower resource usage.

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. However, Virus Protection is turned on by default.

To configure Virus Protection, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Virus Protection** on.
4. Click **Virus Protection**.

The Virus Protection details screen appears.

5. Set the following options as per requirement:
  - **Display alert message** – Select this option if you want to get the alerts on various events such as when malware is detected. However, this option is selected by default.
  - **Select action to be performed when virus is detected** – Select an appropriate action when a virus is detected during the scan.
  - **Backup before taking action** – Select this option if you want to take a backup of a file before taking an action. Files that are stored in the backup can be restored from Quarantine.
  - **Enable sound when threat is detected** – Select this option if you want to be alerted with sound whenever a virus is detected.
6. Click **Save Changes** to save your setting.

### *Turning off Virus Protection*

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. However, you can turn Virus Protection off when it is absolutely necessary. While you turn Virus Protection off, you have a number of options to turn the feature only temporarily, so that it turns on automatically after the select time interval passes.

To turn off Virus Protection, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Virus Protection** off.
4. Select one of the following options:
  - Turn on after 15 minutes

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

5. Click **OK** to save your settings.

After you turn Virus Protection off, the icon color of the Files & Folders option on Dashboard changes from green to red and a message “System is not secure” is displayed.

## Advance DNAScan

DNAScan is an indigenous technology of Antivirus to detect and eliminate new and unknown malicious threats in your system. Advance DNAScan technology successfully traps suspected files with very less false alarms. Additionally, it quarantines the suspected file so that malware does not harm your system.

The quarantined suspicious files can be submitted to the Antivirus research labs for further analysis that helps in tracking new threats and curb them on time. After the analysis, the threat is added in the known threat signature database and the solution is provided in the next updates to the users.

To configure Advance DNAScan, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Advance DNAScan**.

The Advance DNAScan details screen appears.

4. Select either of the following options as per requirement:
  - **Enable DNAScan:** Select this option to enable DNAScan.
  - **Enable Behavior detection system:** Select this option if you want to enable Behavior detection system. The running applications will be monitored for their behavior. You can also set a security alert level from the **Select Behavior detection level** list either as **High**, **Moderate**, or **Low**.
    - **High:** If you select this security level, Antivirus will closely monitor the behavior of a running application and will alert you if any unusual application behavior is noticed. You may receive more alerts and sometimes even for genuine files.
    - **Moderate:** If you select this security level, Antivirus will send alert if any suspicious activity of a running application is noticed.
    - **Low:** If you select this security level, Antivirus will send alert only if any malicious activity of a running application is noticed.

Note: If you have selected Moderate or Low security level, **Behavior detection system** will also block many unknown threats in the background without prompting you for any action if it finds the application behavior suspected.

- **Do not submit files:** Select this option if you do not want to submit suspicious files to the Antivirus research labs.
- **Submit files:** Select this option if you want to submit the suspicious files to the Antivirus Research labs for further analysis. You can also select **Show notification while submitting files** to get prompts for permission before submitting the files.

### Caution

---

If the option **Show notification while submitting files** is not selected, Antivirus will submit the suspicious files without notifying you.

## How DNAScan is effective?

Advance DNAScan detects files by studying their characteristics and behavior.

### *Detection by Characteristics*

Thousands of new and polymorphic threats, which change their code/file information, are born daily. Detecting them by their signature requires time. Our Advance DNAScan technology detects such threats in real time, with zero-time lapses.

Whenever DNAScan detects a new malicious threat in your system, it quarantines the suspicious file and displays a message along with the file name. However, if you find that the file is genuine, you can also restore that file from quarantine by using the option provided in the message box.

### *Detection by Behavior*

If the option **Behavior detection system** is enabled, DNAScan continuously monitors the activities performed by an application in your system. If the application deviates from its normal behavior or carries out any suspicious activity, **Behavior detection system** suspends that application from executing further activities that may cause potential damage to the system.

Upon detecting such an application, it prompts you to take an appropriate action from the following options:

- **Allow:** Take this action if you want to allow the application to run. Select this action if you are sure the applications are genuine.
- **Block:** Take this action if you want to block the application from running.

## *Submitting suspected files to us*

You can submit the suspicious files either automatically or manually. The submission takes place automatically whenever Antivirus updates itself and finds new quarantined DNAScan-suspected files. This file is sent in an encrypted file format to the Antivirus research labs.

You can also submit the quarantined files manually if you think they should be submitted immediately. You can submit the files in the following way:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Tools**.
3. Under Cleaning & Restore Tools, click **View Quarantine Files**.

The Quarantine dialogue appears.

A list of the files that have been quarantined is displayed.

4. Select the files that you want to submit to the Antivirus labs and then click **Send**.
5. Click **Close** to close the Quarantine dialogue.

## Block Suspicious Packed Files

Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the computer systems. This feature helps you identify and block such suspicious packed files.

It is recommended that you always keep this option enabled to ensure that the suspicious files are not accessed and thus prevent infection.

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Block Suspicious Packed Files** on.

However, Block Suspicious Packed Files is turned on by default.

## Screen Locker Protection

Malicious programs that lock the screen preventing access to your computer are known as screen lockers. With Screen Locker Protection, you can create a short-cut key combination to initiate a clean-up of your computer and remove such malicious programs. By pressing the short-cut key, you can initiate cleaning up of your computer and remove the malicious program.

## *Configuring Screen Locker Protection*

1. Open **Antivirus**.

2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Screen Locker Protection**.
4. To enable Screen Locker Protection, select **Protect from screen lockers**. However, this option is selected by default.
5. Select an alphabet from the drop-down list to create a short-cut combination with **Ctrl+Alt+Shift**. Here **A** is selected by default.
6. Click **Save Changes**.

### Note

---

You have to restart your computer at least once after you install the product to activate this feature.

## Scan Schedule

Scanning regularly helps you keep your system free from virus and other types of infections. This feature allows you to define a schedule when to begin scanning of your system automatically. You can define multiple numbers of scan schedules to initiate scan at your convenience.

### *Configuring Scan Schedule*

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Scan Schedule**.  
The Scan Schedule details screen appears.
4. To define a new scan schedule, click **New**.
5. In **Scan Name**, type a scan name.
6. Under Scan Frequency, select the following options based on your preferences:
  - Scan Frequency:
    - Daily: Select this option if you want to initiate scanning of your system daily. This option is selected by default.
    - Weekly: Select this option if you want to initiate scanning of your system on a certain day of the week. When you select the Weekly option, the Weekdays drop-down list is activated so you can select a day of the week.
  - Scan time:
    - Start at first boot: This helps you schedule the scanner to begin at the first boot of the day. If you select this option, you do not need to specify the time of the day to start the scan. Scanning takes place only during the first boot regardless what time you start your system.

- **Start at:** Select this option to initiate the scanning of your system at a certain time. If you select this option, the time drop-down list is activated where you can set the time for scanning. However, this option is selected by default.

You can further define how often the scan should begin in the **Everyday** and **Repeat scan after every** options.

- **Scan priority.**
  - **High:** Helps you set high scan priority.
  - **Low:** Helps you set low scan priority . However, this option is selected by default.
- 7. Under **Scan Settings**, you can specify scan mode, define the advanced options for scanning, action to be performed when virus is found and whether you want a backup of the files before taking any action on them. However, the default setting is adequate for scanning to keep your system clean.
- 8. In the **Username** text box, enter your username and your password in the **Password** text box.
- 9. **Run task as soon as possible if missed:** Select this option if you want to initiate scanning when the scheduled scan is missed. This is helpful in case your system was switched off and the scan schedule passed, later when you switch on your system, the scan schedule will automatically start as soon as possible.

This option is available only on Microsoft Windows Vista and later operating systems.

10. Click **Next**.

The Configure Scan Schedule screen for adding folders to be scanned appears.

11. Click **Add Folders**.

12. In the Browse for Folder Window, select the drives and folders to be scanned. You can add multiple numbers of drives and folders as per your requirement.

If you want to exclude subfolders from being scanned, you can also select **Exclude Subfolder**. Click **OK**.

13. On the Configure Scan Schedule screen, click **Next**.

14. A summary of your scan schedule appears. Verify and click **Finish** to save and close the Scan Schedule dialogue.

15. Click **Close** to close the Scan Schedule screen.

## Parental Control

Parental Control is a very effective method to control the Internet access, application access, and computer access by the children and other users. This feature ensures that the children and other users do not visit inappropriate types of Web sites, and can only



access the allowed applications so that they are safe from any virus threats. Parents can also limit access to the computer and Internet on a day and time basis.

## Ensure the following requirements for effective control of Parental Control

To get the maximum benefits from the Parental Control feature, we recommend that you configure the following options:

### First step

Check if you are logged in as an Administrative user to the computer on which you have installed Antivirus. In case you are not an administrative user, we recommend that you [create an Administrator account](#) and configure it. Do not share the administrative credentials with the users for whom you are creating restricted accounts.

### Second step

Create separate [Standard accounts](#) (Restricted user) for your children or other users. This way, they will have only limited access to the computer. This also helps you apply different protection policies to different users. The protection policies could include website preferences for each restricted user and a schedule for Internet access.

### Third step

Set a password to restrict unauthorized users from modifying the settings or removing Antivirus from the computer. To see how to set password to Antivirus, see [Antivirus Password Protection](#).

## Configuring Parental Control

To configure Parental Control, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Parental Control**.  
The Parental Control setting details screen appears.
3. Select **Display alert message**, if you want to receive alert message when the users visit a blocked website.
4. Under **Select whom to apply the settings**, select one of the following options:
  - **Apply to all users**: Select this option if you want to apply the same setting to all users. If you select this option, the **All Users** option is displayed below.
  - **Apply to specific users**: Select this option if you want to apply different settings to different users. If you select the **Apply to specific users** option, a list of all users is displayed below.

5. To configure further settings, click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.

The protection rules screen appears. You can configure any or all of the following options based on your requirement.

- [Internet Browsing Control](#)
- [Application Control](#)
- [PC Access Control](#)

6. After configuration, click **Save Changes** to save your settings.

## *Internet Browsing Control*

Internet Browsing Control includes the following options.

### Setting Restrict access to particular categories of website

With this feature, you can restrict access to the websites by categories. If you restrict a website category, all the websites under that category will be blocked.

If you want to restrict most of the websites in a category but allow certain websites in that category, you can do so by restricting that category and enlisting such websites in the exclusion list.

To restrict access to the website categories, follow these steps:

1. Open **Antivirus**.
  1. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
  2. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
  3. On the protection rules screen, select **Internet Browsing Control**.
  4. Select **Restrict access to particular categories of website**. A list of website categories appears.
  5. On the Web Category screen, select an age group under **Block the website categories based on age group** for restricting access to certain types of websites for your children or other users. If you can select a certain age group, optimum settings will be applied. You may customize the predefined settings for an age group if required. To reset the customized settings of an age group, refresh the same age group. You may revert to the default settings anytime by selecting the Default option.
  6. Under **Select access rights for below categories of website**, turn on a website category to allow access to the websites or turn off to deny access. Moreover, the default settings are optimal and ideal for novice users.

If you want to exclude a certain website from the blocked category, enlist such a website in the exclusion list. For example, if you have blocked the **Streaming Media and Downloads** category, but you still want to allow access to **YouTube**, you can do so by enlisting YouTube in the exclusion list.

- On the Web Category dialogue, click the **Exclude** button.
- In the **Enter URL** text box, enter the URL of the website that you want to allow users to access and then click the **Add** button. Click **OK**.

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

7. Click **OK** and then confirm your preference. Click **OK**.
8. To save your settings, click **Save Changes**.

### Setting Restrict access to particular website

With this feature, you can block access to specific websites. This is helpful when you want to restrict access to certain websites or if you have a shorter list of websites to restrict.

This option is also helpful when a websites does not fall in a selected category or you have restricted a websites category yet a certain website is still accessible.

To restrict access to a particular website, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
4. On the protection rules screen, select **Internet Browsing Control**.
5. Select **Restrict access to particular website** and then click the **Block List** button.
6. Click the **Add** button.
7. In the **Enter website** text box, enter the URL of a website and then click **OK**. If you want to block all subdomains of the website, select **Also block subdomains**.

For example, if you block **www.abc.com** and its subdomains, the subdomains such as **mail.abc.com** and **news.abc.com** will also be blocked.

8. Click **OK** and then click **OK**.
9. To save your settings, click **Save Changes**.

## Setting Schedule Internet access

With this feature, you can restrict your children to access Internet as per the configured time slot only. As soon as the configured time slot is over, access to the Internet is blocked.

To set Schedule Internet access, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
4. On the protection rules screen, select **Internet Browsing Control**.
5. Select **Schedule Internet access** and then click the **Configure** button.

The Schedule internet access chart appears.

6. Under **Specify when the user can access the Internet**, select any of the following options:

- **Always allow access to the Internet:** Select this option if you want to allow other users the Internet access without any restriction.
- **Allow access to the Internet as per the schedule:** Select this option if you want to set restriction for accessing the Internet.

The day and time schedule chart is activated.

- Select the cells for the days and times during which you want to allow access to the Internet.

The selected cells are highlighted which indicates the allowed schedule.

7. Click **OK** and then click **OK**.
8. To save your settings, click **Save Changes**.

## *Application Control*

Application Control includes the following options.

### Setting Restrict access to particular categories of applications

With this feature, you can restrict access to the applications by categories. If you restrict an application category, all the applications under that category will be blocked.

If you want to restrict most of the applications in a category but allow certain applications in that category, you can do so by restricting that category and enlisting such applications in the exclusion list.

To restrict access to the categories of applications, follow these steps:

1. Open **Antivirus**.

2. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
4. On the protection rules screen, select **Application Control**.
5. Select **Restrict access to particular categories of application** and then click the **Categories** button. A list of application categories appears.
6. Turn on an application category to allow access to the applications in that category or turn off to deny access.

If you want to exclude certain applications from the blocked category, enlist such an application in the exclusion list.

- On the Application Category dialog, click the **Exclude** button.
- Click the **Add** button and browse an application to add to the exclusion list. Click **OK**.

Similarly, if you want to remove an application from the exclusion list, select the application and click **Remove**. Click **Remove All** to delete all the applications from the exclusion list.

7. Click **OK** and then click **OK**.
8. To save your settings, click **Save Changes**.

## Restrict access to particular application

With this feature, you can block user access to specific applications. This is helpful when you want to restrict user access to certain applications or if you have a shorter list of applications to restrict.

This option is also helpful when an application does not fall in a selected category or you have restricted an application category yet a certain application is still accessible.

To restrict access to a particular application, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
4. On the protection rules screen, select **Application Control**.
5. Select **Restrict access to particular application** and then click the **Block List** button.
6. Click the **Add** button and browse an application to block it.

Similarly, if you want to remove an application from the blocked list, select the application and click **Remove**. Click **Remove All** to delete all the applications from the blocked list.

7. Click **OK** and then click **OK**.
8. To save your settings, click **Save Changes**.

Note: Application Control will function only if Virus Protection is enabled.

## *PC Access Control*

With this feature, you can restrict your children to access your computer or laptop as per the configured time slot only. As soon as the configured time slot is over, the computer will be locked. However, they can log on with their credentials after the allotted time is over but for forty-five seconds only. They can log in as many times as they prefer, however the computer will be locked every forty-five seconds.

To configure PC Access Control, follow these steps:

1. Open **Antivirus**.
2. On the Antivirus Dashboard, click **Parental Control**. The Parental Control setting details screen appears.
3. Click a user available under **Select whom to apply the settings**. Users are displayed based on the options whether you have selected **Apply to all users** or **Apply to specific users**.
4. On the protection rules screen, select **PC Access Control** and then click the **Configure** button. The Schedule PC access chart appears.
5. Under **Specify when the user can access the PC**, select any of the following options:
  - **Always allow access to the PC:** Select this option if you want to allow users to access your computer without any restriction.
  - **Allow access to PC as per the schedule:** Select this option if you want to set a time-slot for accessing the computer.
    - Daily access time limit: Lets you allot time on hourly basis. Users can access the computer for the allowed time duration at any point of time during a day.
    - Daily access time-slots (clock time): Select the cells for the days and times during which you want to allow access to the computer. Users can access the computer only during the allowed time window.

The selected cells are highlighted which indicates the allowed schedule.
6. Click **OK** and then click **OK**.
7. To save your settings, click **Save Changes**.

## Creating an Administrator account

This feature allows you to install and remove an application on your system or change any settings, including Parental Control. This ensures that only you as a parent have full control on your system.

To create an Administrators account, follow these steps:

1. Click **Start > Control Panel**.
2. Click **User Accounts**.
3. Your account type is displayed below your user name. Check if your account type is Administrator. If your account type is not Administrator, you need to change it to Administrator Account.

## Antivirus Password Protection

You can protect the settings of Antivirus by turning Password Protection on. Password Protection ensures that your settings are protected from modification by any unauthorized users.

## Creating restricted user accounts

The restricted user accounts limit the users only to their account and prevent them from taking full control of the computer. This helps protect your computer by preventing a user from making changes that may affect security privileges.

To create restricted user accounts, follow these steps:

For Microsoft Windows XP operating system:

1. Click **Start > Control Panel > User Accounts**.
2. Under **User Accounts**, click **Create a New User Account**.
3. Fill in **Account Name** and click **Next**.
4. Select **Limited**.
5. Click **Create Account**.

For Microsoft Windows Vista/Windows 7 operating system:

1. Click **Start > Control Panel > User Accounts**.
2. Under **User Accounts**, click **Manage Other Account**.
3. Click **Create a New User Account**.
4. Fill in **Account Name** and select **Standard user**.
5. Click **Create Account**.

# Index

---

	<b>D</b>	online, 7	
DNA Scan, 13			<b>S</b>
	<b>P</b>	Scan Schedule, 16	
Parental Control, 17		Scan Settings, 9	
	<b>R</b>		<b>V</b>
Registration		Virus Protection, 11	