

Norton™ Security

Product Manual



Norton™ Security Product Manual

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 22.7

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, LiveUpdate, Norton 360, and Norton are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Portions of this product Copyright 1996-2011 Glyph & Cog, LLC. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Chapter 1	Welcome to Norton	12
	About your Norton product	6
	System requirements for Norton Security	6
Chapter 2	Setting up your Norton account	12
	Creating a Norton account	9
	Signing in to your Norton account	10
	How to find your product key, PIN, or renewal code	10
Chapter 3	Downloading and installing Norton	12
	Downloading and installing Norton	12
	Installing Norton on additional devices	14
	Transferring your Norton license to a new device	16
	Activating your Norton product	16
	Troubleshooting with Norton Bootable Recovery Tool	17
Chapter 4	Understanding and responding to threats	21
	Resolving threats if your device is at risk	21
	Running LiveUpdate	22
	Responding to security risks	22
	Acting on quarantined risks or threats	24
	Types of risks	26
	Types of threats	26
	Types of viruses	27
Chapter 5	Managing your security	29
	Viewing details of your system activities	29
	Checking the trust level of a file	30
	Viewing the 30-Day Report	31
Chapter 6	Scanning your computer	32
	Running a Quick Scan	33
	Running a Full System Scan	33

	Scanning selected drives, folders, or files	33
	Running a custom scan	34
	Scheduling a scan	35
	Scanning your computer with Norton Power Eraser	37
	About Automatic Protection settings	37
	Turning off or turning on SONAR Protection	40
	Excluding security threats from scanning	40
	Adding items to the Signature Exclusions	41
	Clearing IDs of files that are excluded during scans	42
	Configuring boot time protection	42
	Turning on or turning off automatic tasks	43
	Running custom tasks	43
	Scheduling security and performance scans	44
Chapter 7	Keeping secure on the Internet	46
	Turning on or turning off Norton Firewall	47
	Customizing Program Rules	47
	Changing the order of firewall rules	48
	Turning off a Traffic rule temporarily	49
	Allowing a blocked program	49
	Turning off Firewall Block Notification	50
	Removing all devices from Intrusion Prevention exclusion list	50
	Turning off and turning on Browser Protection	51
	Turning off or turning on AutoBlock	52
	Unblocking AutoBlocked computers	53
	Adding a device to the Device Trust	53
	Turning off or turning on Download Intelligence	55
	Turning off or turning on spam filtering	55
	Defining the Internet usage of your Norton product	56
	Turning off or turning on Network Cost Awareness	57
Chapter 8	Securing your sensitive data	58
	Adding the Norton browser extensions	58
	Turning on or turn off Norton Safe Web	60
	Searching the web using Norton Safe Search	60
	Turning off or turning on Scam Insight	61
	Turning off or turning on Antiphishing	62
	Accessing Identity Safe	62
	Turning off or turning on Identity Safe	63
	Creating cloud vault	64
	Deleting your cloud vault	64
	Exporting your Identity Safe data	65

	Importing your Identity Safe data	66
	Disabling and enabling the Norton toolbar	67
Chapter 9	Keeping your PC tuned up	68
	Viewing the resource usage of running processes	68
	Optimizing your permanent disks manually	69
	Configuring performance alerts	69
	Running a scan to clean up disk clutter	71
	Running Diagnostic Report	71
	Managing startup items	71
	Optimizing your boot volume	72
Chapter 10	Protecting your media and data	74
	Backing up your files	74
	Restoring files	75
	Creating a new backup set	77
	Adding files and folders to a backup set	77
	Choosing a backup location	79
	Purchasing more online storage space	83
	Turning off or turning on backup	84
Chapter 11	Customizing settings	86
	Configuring Network Proxy Settings	86
	Customizing your Norton product settings	87
	Configuring Norton for best battery use	88
	Turning on or turning off Remote Management	89
	Securing your Norton product settings using a password	89
	Resetting your Norton product settings password	90
	Turning off or turning on Norton Product Tamper Protection	91
Chapter 12	Finding additional solutions	93
	Finding the version number of your product	93
	Checking for a new version of the product	93
	Solving problems with Norton Autofix	94
	Reasons for Fix Now failures	95
	Uninstalling your Norton product	97

Welcome to Norton

This chapter includes the following topics:

- [About your Norton product](#)
- [System requirements for Norton Security](#)

About your Norton product

Thank you for buying the latest Norton product!

Norton combines superior security and fast performance with an easy-to-use design to protect your devices from today's advanced threats. It safeguards your identity, protects your data, and keeps your computer running at peak performance.

Norton protects you whether you have a single computer or multiple devices to connect your family. Securing your data and information is our only concern. It's why Norton makes this bold promise: From the moment you subscribe, a Norton expert can help keep your devices virus-free or refund your money.

A single Norton subscription can protect all your computers, smartphones, or tablets across Windows, Mac, Android, and iOS operating systems. LiveUpdate automatically installs the latest virus definitions and product features on your devices to assure that you always have the best protection available.

If you have trouble configuring your Norton product, additional help is available. Your Norton product provides easy-to-use support options.

System requirements for Norton Security

To install Norton Security on your PCs, Macs®, smartphones, or tablets, make sure that they meet the minimum system requirements.

Norton Security Premium protects up to 10 devices and includes secure backup for PCs only. It does not include secure backup for Mac OS X.

Windows

◆ Operating systems

- Microsoft Windows® 10 and Windows® 10 Pro (32-bit and 64-bit)
- Microsoft Windows® 8.1 or later (32-bit and 64-bit)
- Microsoft Windows® 8 and Windows® 8 Pro (32-bit and 64-bit)
- Microsoft Windows® 7 (32-bit and 64-bit) Starter/Home Basic/Home Premium/Professional/Ultimate
- Microsoft Windows® Vista (32-bit and 64-bit) Starter/Home Basic/Home Premium/Business/Ultimate with Service Pack 1 or later
- Microsoft Windows® XP Home/Professional/Tablet PC/Media Center with Service Pack 3

Hardware

- 300 MHz for Microsoft Windows XP, 1 GHz for Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows 8/Windows 10
- 256 MB of RAM for Windows XP, 512 of RAM for Windows Vista, and 1GB of RAM (32-bit) or 2 GB RAM (64-bit) for Windows 10/8/7 (minimum of 512 MB RAM required for Recovery Tool)
- 300 MB of available hard disk space
- CD-ROM or DVD drive (if not installing by electronic download)

Browser support for Phishing Protection, Safe Search, and Password Management

The following browsers are supported for Phishing Protection, Safe Search, and Password Management.

- Microsoft Internet Explorer® 8.0 or higher (32-bit and 64-bit)^{1,2}
- Mozilla Firefox® (32-bit and 64-bit)^{2,3}
- Google Chrome™ (32-bit and 64-bit)²

Email clients

Norton Security supports email scanning on all POP3 compatible email clients.

Support for Antispam

The following email client is supported for Antispam:

- Microsoft Outlook 2002 and later

- ¹ Some protection features are not available in Microsoft Internet Explorer 10.0 or later.
- ² As made available by Symantec within your service period.
- ³ Norton extension is partially compatible with the latest and two previous versions of Mozilla Firefox.

Setting up your Norton account

This chapter includes the following topics:

- [Creating a Norton account](#)
- [Signing in to your Norton account](#)
- [How to find your product key, PIN, or renewal code](#)

Creating a Norton account

Your Norton account is where you monitor your connected devices and update your profile. You can also change your billing preferences or renew your product from your Norton account.

You created a Norton account if you made a purchase from the [Norton Online Store](#) or if you already downloaded and installed your product.

If you signed up for Norton Family, Norton Online Backup, or Norton Safe Web, you may also have a Norton account. Ensure that this account also has the Norton Security license associated with it.

To create a Norton account

- 1 Go to <https://manage.norton.com>
- 2 Click **Create account**.
- 3 Enter a valid email address and password for your account. You need to use these credentials to sign in to Norton in the future.
- 4 Choose your region.
- 5 Read the privacy policy and agree to it, and then click **Sign Up**.

Signing in to your Norton account

Sign in to your Norton account to monitor your devices, update your profile, or change your billing preferences.

To sign in to your Norton account

- 1 Go to <https://manage.norton.com>
- 2 Click **Sign in**.
- 3 Enter the email address and password that you used when you created your Norton account and click **Sign in**.
- 4 If you do not know your password, click **Forgot your password?**
Follow the instructions to receive an email with a new password link.

Note: If you have opted for the Two-Step Verification to access your Norton account, you have to use the verification code in addition to your password. For more information, see [Two-Step Verification for Norton account](#)

How to find your product key, PIN, or renewal code

This document helps you locate the product key, renewal code, or PIN that you need to activate or renew your Norton product:

- **Product key:** A 25-character alphanumeric string shown in five groups of five characters each, separated by hyphens, that you need to activate or renew your Norton subscription.
- **PIN:** A 13-character alphanumeric code provided by your service provider, which you need to activate your Norton product.
- **Renewal code:** A 19-character alphanumeric code that you need to extend your Norton subscription.

Finding your product key

- If you purchased your Norton product from the [Norton Online Store](#) or your product is already registered with your Norton account, you can [sign in](#) to Norton and get the product key. You can also find the product key in your order confirmation email.

Getting the product key from Norton

- 1 [Sign in](#) to your Norton account.
- 2 In the page that appears, click **Services**.
- 3 Click the Norton product for which you want to see the product key.
- 4 Write down or copy the product key.

Other ways to find the product key

- If you purchased your Norton product from a third-party website, look for the product key in the order confirmation email. If you do not find the email in your Inbox, check your spam or junk folder.
- If you purchased your Norton product as a boxed product, the product key is printed either on a sticker on the DVD or on a card kept inside the box.
- If the product came pre-installed on your device, your product key might be already stored in the product. All you need is to register your product with your Norton account. Once registered, you can get the product key by signing into your account. Some manufacturers may provide the product key on an activation card. If you have any problems, contact your device manufacturer.

Finding your PIN

- Your service provider may send the PIN to your registered email address. If you do not see the email, check your spam or junk folder. If you still cannot locate your PIN, contact your service provider.

Finding your renewal code

- If you purchased your renewal code from an online retailer, your renewal code can be found in your confirmation email. If you cannot find the confirmation email, check your spam or junk folder. These emails may be incorrectly marked as spam by some spam filters.
- If you purchased from the [Norton Online Store](#), your renewal code can also be found by signing into your Norton account.

Getting the renewal code from Norton

- 1 [Sign In](#) to Norton.
- 2 Locate your subscription renewal purchase, and click the order number.
- 3 Write down or copy the renewal code.

Downloading and installing Norton

This chapter includes the following topics:

- [Downloading and installing Norton](#)
- [Installing Norton on additional devices](#)
- [Transferring your Norton license to a new device](#)
- [Activating your Norton product](#)
- [Troubleshooting with Norton Bootable Recovery Tool](#)

Downloading and installing Norton

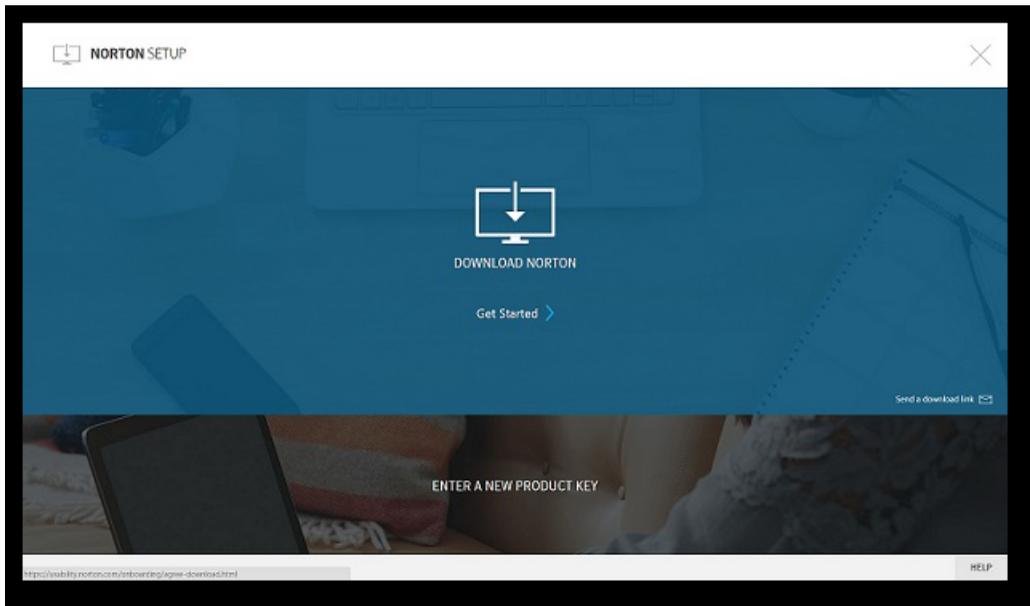
Protecting your devices and managing your Norton product is as easy as adding a new device to your Norton account.

To download and install Norton on your computer

- 1 Go to norton.com/setup.
- 2 If you are not signed in to your Norton account, enter your email address and Norton account password, and then click **Sign In**.

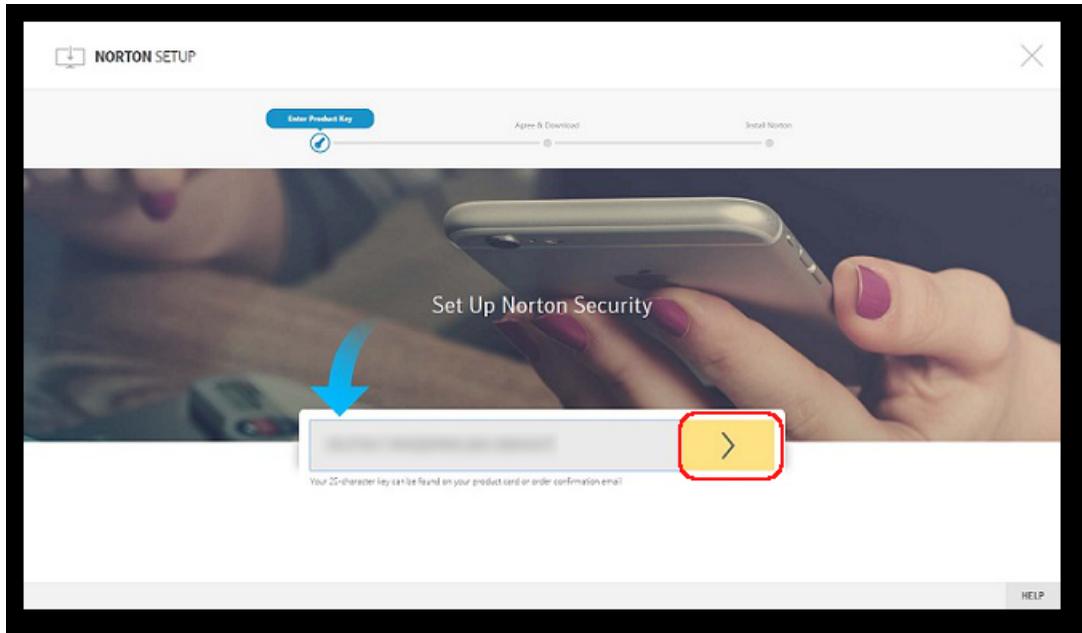
If you do not have an account, click **Create account**, and then complete the sign-up process.

3 In the **Norton Setup** window, click **Download Norton**.



To install a new product that is not yet registered to your Norton account, click **Enter a New Product Key**.

Enter your product key and click the next (>) icon.



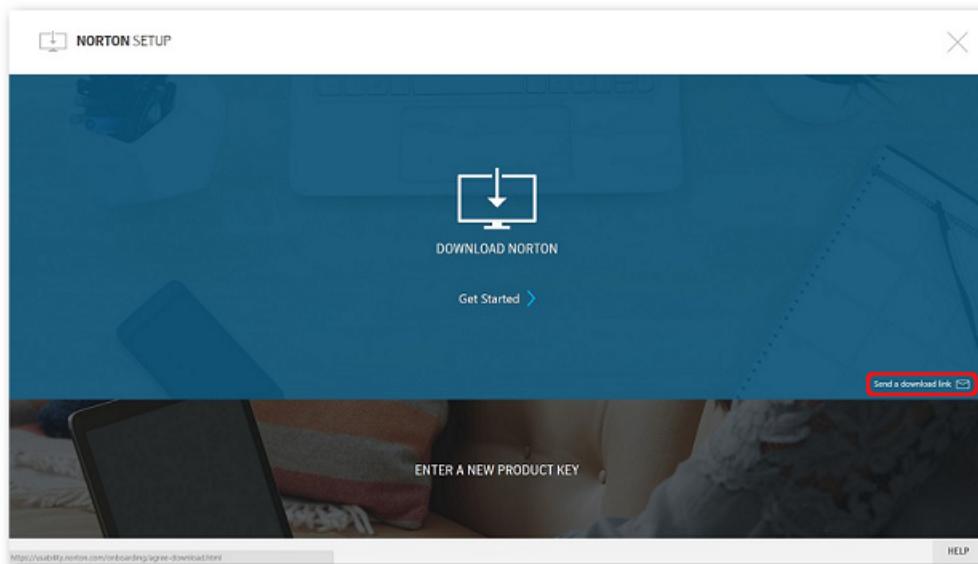
- 4 Click **Agree & Download**.
- 5 Click the area pointed by the on-screen blue arrow and follow the on-screen instructions.
 - For Internet Explorer or Microsoft Edge browser: Click **Run**.
 - For Firefox or Safari: On the top-right corner of the browser, click the **Download** option to view the downloaded files, and double-click the file that you downloaded.
 - For Chrome: On the bottom-left corner, double-click the file that you downloaded.
- 6 If the **User Account Control** window appears, click **Continue**.
- 7 Your Norton product gets downloaded, installed, and activated.

Installing Norton on additional devices

From your Norton account, you can send emails to additional devices and install Norton on the devices. The email contains the install link and instructions to install Norton.

To install Norton on a different device

- 1 [Sign in](#) to Norton.
- 2 If you are not signed in to your Norton account, enter your email address and Norton account password, and then click **Sign In**.
- 3 In the **Norton Setup** window, click **Send a download link**.



- 4 Enter an email address that you can access on your additional device and click the send button.
If you want to send multiple download links, click on **Click here**.
An email is sent to the email address with instructions to install the Norton product.
- 5 On the device where you want to download Norton, locate and open the email that you received from 'The Norton Team'.
- 6 Click **Install Now**.

- 7 Click **Agree & Download**.
- 8 Save the file on your computer and double-click the file to install Norton. By default, the file is saved in the Downloads folder on both Mac and Windows computers.

Follow the on-screen instructions.

Note: Norton AntiVirus for Mac cannot be managed through your Norton account.

Note: Norton Security Premium customers are redirected to the Norton Family page after clicking **Done**.

Transferring your Norton license to a new device

If your Norton product is installed on a device that you no longer use, you can transfer your Norton product from that device to another device using your Norton account.

To transfer your license to a new device

- 1 [Sign in](#) to Norton from your new device.
- 2 In the **Services** page, select your Norton product for which you want to transfer the license.
- 3 Under **Manage My Installs**, click the trash can icon under **Remove License** next to the device you no longer use.
- 4 Follow the install instructions to complete the installation. For install instructions, See [“Downloading and installing Norton”](#) on page 12.

Activating your Norton product

To use Norton’s security features, you must first activate your product. Product activation reduces software piracy and ensures that you have authentic Symantec software.

If you are connected to the Internet, product activation takes place automatically when you start the product for the first time after installation. If you did not activate your product during installation, Norton prompts for activation each time you start the product. Also, you receive an activation alert regularly until you activate the product.

To Activate your product

- 1 Start your Norton product.
- 2 In the main window of your Norton product, click **Renew** or **Activate Now**.
You can also click **Activate Now** from the activation alert.
- 3 If prompted, sign in to your Norton account with your Norton account credentials.
- 4 Do one of the following:
 - If you have product key, click **Enter a key**, type the product key, and follow the on-screen instructions.
 - If you have any licenses available, select the subscription and follow the on-screen instructions.
 - If you want to purchase a license, click **Buy a Subscription**. You are redirected to Norton Store website where you can complete your purchase.

Troubleshooting with Norton Bootable Recovery Tool

If you are unable to install Norton Security, open Norton Security, or you cannot start your computer, you can use Norton Bootable Recovery Tool to resolve the issue.

Norton Bootable Recovery Tool scans and removes viruses, spyware, and other security risks. You can run Norton Bootable Recovery Tool only from a DVD or a USB drive.

Note: Norton Bootable Recovery Tool is not a replacement for real-time protection from viruses and security risks.

Step 1: Download the Norton Bootable Recovery Tool ISO file on a computer that is not infected

To download the ISO file

- 1 Open the browser and go to the following URL:
<http://norton.com/nbrt>
- 2 Click **Download**.
- 3 Follow the on-screen instructions to download and save the Norton Bootable Recovery Tool ISO file.

Step 2: Create a Norton Bootable Recovery Tool bootable media

You can use any tool to burn the Norton Bootable Recovery Tool ISO file on a DVD or a USB drive as a bootable media. You can then run Norton Bootable Recovery Tool on any infected computer. You can also use this DVD as a recovery DVD on any computer.

Warning: If you create Norton Bootable Recovery Tool on a re-writable DVD or USB drive, all the files on DVD or USB drive are permanently deleted. Back up your data before you create Norton Bootable Recovery Tool on a re-writable DVD or USB drive.

Note: If you create Norton Bootable Recovery Tool on a USB drive, the USB drive should have a minimum space of 1 GB and should be formatted in FAT32 file system.

Step 3: Launch Norton Bootable Recovery Tool

After you create Norton Bootable Recovery Tool on a DVD or a USB drive, use the media to run Norton Bootable Recovery Tool.

To launch Norton Bootable Recovery Tool

- 1 Insert the Norton Bootable Recovery Tool DVD or USB drive that you created.
- 2 Turn on or restart the infected computer, then enter the BIOS mode by pressing the key that appears on the screen immediately after your computer restarts.
- 3 Select the DVD or the USB drive on which you created Norton Bootable Recovery Tool, and then press **Enter**. If you use a UEFI-enabled computer, select the recovery media under the **Legacy Boot** option instead of the **UEFI Boot** option. The recovery media is the Norton Bootable Recovery Tool DVD or USB drive.

- 4 In the **Welcome to NBRT** page, select the **Boot** option. If the booting fails, then select **Boot (Basic Video)** option.
- 5 In the **Select Language** drop-down list, select your preferred language, and then click **OK**.
- 6 Read the Norton license agreement and then click **Agree** to launch the tool.

Step 4: Scan and resolve threats

Norton Bootable Recovery Tool identifies and lists all the known security threats. You can choose what to do with the items that are identified as potential risks.

To scan and resolve threats

- 1 Read the Norton license agreement and then click **Agree** to launch the tool.
- 2 In the **Scan your computer** section, click **Start Scan**.

When the scan is complete, the **Scan Completed** window lists the following:

- The total number of files scanned
 - The total number of threats detected
- 3 In the **Scan Completed** window, review the scan results, and do one of the following:
 - To fix all of the threats that are found on your computer, select the **Action** column.
 - To perform appropriate actions for each of the threats, select the relevant threat that you want to resolve under the **Action** column.

Note: Review the scan results carefully before resolving the threats, since the files that are removed cannot be restored on your computer.

- 4 Click **Fix**.
- 5 In the confirmation dialog box, click **OK**.
- 6 The **Remediation window** displays the status of each threat under the **Action** column.
- 7 Click **Continue**.
- 8 In the **Reboot your computer** window, click **Reboot** to restart your computer.
 If you want to run the scan again, click **Scan Again**.

Norton Bootable Recovery Tool automatically downloads and updates the latest virus definitions from the Symantec servers when you initiate the scan and are

connected to the Internet. The latest virus definitions helps you secure your computer from the latest viruses and security threats.

Understanding and responding to threats

This chapter includes the following topics:

- [Resolving threats if your device is at risk](#)
- [Running LiveUpdate](#)
- [Responding to security risks](#)
- [Acting on quarantined risks or threats](#)
- [Types of risks](#)
- [Types of threats](#)
- [Types of viruses](#)

Resolving threats if your device is at risk

In the Norton main window, the color of Security, Identity, Backup, and Performance tiles indicates the status of each category as follows:

- **Green:** You are Protected.
- **Orange:** Your computer needs attention.
- **Red:** Your computer is at risk.

Note: The backup category is available only with Deluxe+ and Premium subscriptions.

Norton automatically fixes most issues that reduce your protection or system performance and displays the status as Protected in the main window. Norton displays issues that require your attention as **At Risk** or **Attention**.

To respond to Attention or At Risk status indicators

- 1 In the product main window, click the red or orange tile of the category that indicates **At Risk** or **Attention**.
- 2 Click **Fix Now** and follow the on-screen instructions.

Running LiveUpdate

Symantec recommends that you run LiveUpdate at regular intervals in the following cases:

- If you have turned off **Automatic LiveUpdate** option
- If your computer is not connected to the Internet for a long time

Note: To run LiveUpdate, you need a valid subscription and an Internet connection.

To run LiveUpdate manually

- 1 In the Norton product main window, double-click **Security**, and then click **LiveUpdate**.
- 2 In the **Norton LiveUpdate** window, when the LiveUpdate is completed successfully, click **OK**.

Responding to security risks

When a risk is detected, Norton removes the threat and quarantines it. You can view details about risks that were automatically resolved in the **Security History** window. In some cases, Norton requires your attention to manually resolve a detected security risk.

Viewing risks that were automatically resolved during a scan

To view risks automatically resolved during a scan

- 1 In the Norton product main window, double-click **Security**, and then click **History**.
- 2 In the **Security History** window, in the **Show** drop-down list, select **Resolved Security Risks**.
- 3 Select a risk in the list, then in the **Details** pane, view the action that was taken.

Fixing unresolved risks detected during a scan

In some cases, Norton does not automatically resolve a risk, but recommends an action for you to take before resolving the risk.

To fix unresolved risks detected during a scan

- 1 In the Norton product main window, double-click **Security**, and then click **History**.
- 2 In the **Security History** window, in the **Show** drop-down list, select **Unresolved Security Risks**.
- 3 Select a risk in the list if there are unresolved risks displayed.
- 4 Follow the Recommended Action in the **Details** pane.

Running Norton Power Eraser if you can't fix an unresolved risk

Run Norton Power Eraser if you think your system is infected. Norton Power Eraser is a powerful malware removal tool that eliminates security risks that are difficult to remove.

To run Norton Power Eraser

- 1 In the Norton product main window, click **Security**, and then click **Scans**.
- 2 In the **Scans** window, click **Norton Power Eraser**.
- 3 Click **Go**.

Note: Norton Power Eraser is an aggressive malware removal tool. Sometimes Norton Power Eraser may remove legitimate files along with malware, so you need to review the scan results thoroughly before you delete any file.

Restoring a file that was mistakenly identified as a security risk

By default, Norton removes security risks from your computer and quarantines them. If you think a file was mistakenly removed, you can restore the file from Quarantine to its original location and exclude it from future scans.

To restore a file from Quarantine

- 1 In the Norton product main window, click **Security**, and then click **History**.
- 2 In the **Security History** window, under **Show** drop-down menu, select **Quarantine**.
- 3 Select the file that you want to restore.
- 4 In the **Details** pane, click **Options**.
- 5 In the **Threat Detected** window, click **Restore & exclude this file**.
- 6 In the **Quarantine Restore** window, click **Yes**.
- 7 In the **Browse for Folder** dialog, select the folder or drive where you want to restore the file and then click **OK**.

Note: Exclude a program from the Norton product scans only if you are confident that the program is safe. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer.

Acting on quarantined risks or threats

Quarantined items are isolated from the rest of your computer so that they cannot spread or reinfect your computer. If you have an item that you think is infected, but is not identified as a risk by Norton, you can manually put the item in Quarantine.

You cannot open quarantined items accidentally and spread the virus, but you can evaluate the quarantined items for possible submission to Symantec.

Types of quarantined items:

Security risks

Items such as spyware and adware that are generally low risk and that another program requires to function properly.

You can restore these items if necessary.

Security threats

Viruses and other high-risk items.

To perform an action on a quarantined item

1 In the Norton product main window, double-click **Security**, and then click **History**.

2 In the **Details** pane, click **Options**.

You can use the **More Options** link to view more details about the item before you select an action for it. The link opens the **File Insight** window that contains more information about the risk.

3 In the **Threat Detected** window, select the action that you want to perform. Some of the options are:

Restore Returns the security risk that is quarantined to the original location on your computer.

This option is available only for manually quarantined items.

Restore & exclude this file Returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans

This option is available for the detected viral and non-viral threats.

Remove from history Removes the selected item from the Security History log

Submit to Symantec Sends the selected item to Symantec for evaluation of the security risk

In some cases, your Norton product might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can use this option to submit the item to Symantec for further analysis.

You can also navigate to this window by using the **Options** link in the **File Insight** window for some risks.

4 Follow the on-screen instructions.

Types of risks

A risk is anything that can be exploited to harm your PC and its data, or that can be used to steal your data. Your Norton product protects your system from a variety of risks.

Risks fall into several categories:

Malicious software

These programs are deliberately designed to cause damage to your PC. They include threats such as viruses, worms, and Trojan horses. Malicious software is sometimes called malware.

Spyware

These programs conceal themselves on your PC. They monitor what you do, or look through the information that is stored on your PC, and send the information back to their creators.

Vulnerabilities

These risks consist of flaws in legitimate software that can be exploited, either to cause damage, block data, or steal information. Vulnerabilities are usually exploited through network connections.

Types of threats

Threats consist of the software that has been deliberately designed to destroy, modify, disclose, or block your data.

Threats fall into the following categories:

Viruses

Viruses are the small programs that attach themselves to other programs and replicate themselves.

Worms

Worms are like viruses in that they copy themselves from PC to PC, but they do not attach themselves to other programs.

Trojan horses

These destructive programs claim to be some other type of program, but they cause damage when they run.

Your Norton product scans your PC for viruses, worms, Trojan horses, and other software that is intentionally destructive. It also monitors your Internet connection to protect you from the Internet-based threats that exploit software vulnerabilities.

Types of viruses

A virus is a small program that is designed to alter the way your PC operates, without your knowledge or permission.

To be a virus, a program must do the following:

- Run on its own, without you having to take any action
- Make copies of itself so that it can spread to other PCs

Although not all viruses are intended to cause damage, even harmless viruses can affect the performance and stability of your PC. Your Norton product attempts to remove all viruses from your PC.

Viruses fall into the following recognized categories:

File infectors	These viruses infect program files. When infected files run, they can attach the viruses that they carry to other program files. Your Norton product scans all program files on your PC to find and eliminate file infectors.
Boot viruses	These viruses attach themselves to the system areas of your PC and become active as soon as your PC starts. They can attach themselves to disks or other storage devices that is connected to your PC. Your Norton product scans the system areas of your PC to find and remove boot viruses.
Multipartite viruses	These viruses use the techniques of both boot and file infector viruses. Your Norton product scans for such viruses and eliminates them.
Macro viruses	These viruses attach themselves to the data files that contain executable components, such as some spreadsheet, presentation, and word-processing files. These viruses that are spread when a program runs the executable portion of a data file. Your Norton product scans data files for macro viruses and removes them.

Your Norton product scans your PC for both known viruses and unknown viruses.

Known viruses are automatically detected and repaired. Unknown viruses are detected by analyzing each executable file for various characteristics common to viruses. In addition, your Norton product automatically updates itself over the Internet to expand and refine its list of known viruses.

Managing your security

This chapter includes the following topics:

- [Viewing details of your system activities](#)
- [Checking the trust level of a file](#)
- [Viewing the 30-Day Report](#)

Viewing details of your system activities

System Insight lets you view details of the system activities that you performed or that occurred over the last three months in the **Graphs** window. The activities include application installations, application downloads, disk optimizations, threat detections, performance alerts, or Quick Scans.

You can use the tabs at the top of the Events graph to obtain details for the current month and for the last two months. The **Graphs** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. The pop-up that appears when you move the mouse pointer over an icon provides you the details about the activity. The details include the date on which an activity was performed and the number of such activities that you performed on that date. The **View Details** link provides additional details of the activity in the **Security History** window.

To view details of your system activities

- 1 In the Norton product main window, double-click **Performance**, and then click **Graphs**.
- 2 In the **Graphs** window, click the tab for a month to view the details.
- 3 In the Events graph, move the mouse pointer over the icon or the stripe for an activity.

- 4 In the pop-up that appears, view the details of the activity.
- 5 If the **View Details** option appears in the pop-up, click **View Details** to view additional details in the **Security History** window.

Checking the trust level of a file

Norton Insight shows the reputation of **Files of Interest** on your computer. You can view a file's signature and the date when the file was installed. You can also view the trust level, community usage, resource usage, and the source of the file.

Note: Your Norton product displays the **File Insight** option only when you right-click a File of Interest. In Windows Safe mode, you cannot access this option for any file. Your Norton product also categorizes any file for which you open the **File Insight** window to view details as a File of Interest.

From the File Insight window, you can update the trust value of a file or manually trust any file.

To check the trust level or location of a file

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, select **Norton Insight**, and then click **Go**.
- 3 In the **Norton Insight** window, view the file's details or perform the following actions:
 - To find the location of the file, click **Locate**.
 - In the **Details** tab, click **Trust Now** to manually trust the file.
You can manually trust files that are poor, unproven, or not Norton trusted
- 4 Click **Close**.

To check the trust level of a specific file

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, select **Norton Insight**, and then click **Go**.
- 3 In the **Norton Insight** window, click **Check a Specific File**.
- 4 Browse to the location of the file for which you want to check the details.
- 5 Select the file, and then click **Open**.

- 6 In the **File Insight** window, view the details of the file.
- 7 Click **Close**.

Viewing the 30-Day Report

The **30-Day Report** automatically displays all the activities that Norton performs each month. In the Norton product main window, you can also click the 30-Day Report option to manually open the report.

Every time Norton scans your files, runs LiveUpdate, analyzes your downloads, blocks intrusions, or fixes infected files, information about the activity is logged in the 30-Day Report. The Details option in the 30-Day Report window shows the complete list of activities that Norton performed.

If you do not want the 30-Day Report to automatically display each month, you can turn off the option. You can still manually open the report.

To turn off the 30-Day Report

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
- 3 In the **30-Day Report** row, move the **On/Off** switch to **Off**.

How do I manually view the 30-Day Report?

You can also manually view the report using the **30-Day Report** option in the Norton product main window. The **30-Day Report** option is available only when the Norton product has performed any activity on your computer.

Scanning your computer

This chapter includes the following topics:

- [Running a Quick Scan](#)
- [Running a Full System Scan](#)
- [Scanning selected drives, folders, or files](#)
- [Running a custom scan](#)
- [Scheduling a scan](#)
- [Scanning your computer with Norton Power Eraser](#)
- [About Automatic Protection settings](#)
- [Turning off or turning on SONAR Protection](#)
- [Excluding security threats from scanning](#)
- [Adding items to the Signature Exclusions](#)
- [Clearing IDs of files that are excluded during scans](#)
- [Configuring boot time protection](#)
- [Turning on or turning off automatic tasks](#)
- [Running custom tasks](#)
- [Scheduling security and performance scans](#)

Running a Quick Scan

A Quick Scan helps you to scan the possible virus-infected areas of a computer that the viruses and other security risks often targets. Because this scan does not scan your entire computer, it takes less time to run than a Full System Scan.

During idle time, your Norton product runs a Quick Scan when there is a definition update.

To run a Quick Scan

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Quick Scan**.
- 3 Click **Go**.
- 4 On the **Results Summary** window, do one of the following:
 - If no items require attention, click **Finish**.
 - If there are items require attention, review the risks in the **Threats Detected** window.

Running a Full System Scan

Full System Scan checks all boot records, files, and running processes to which the user has access. This scans your computer thoroughly and takes longer time.

To run a Full System Scan

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Full System Scan**.
- 3 Click **Go**.

Scanning selected drives, folders, or files

Occasionally, you might want to scan a particular file, removable drives, any of your computer's drives, or any folders or files on your computer. For example, when you work with removable media and suspect a virus, you can scan that particular disk. Also, if you have received a compressed file in an email message and you suspect a virus, you can scan that individual element.

To scan individual elements

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
- 3 Click **Go**.
- 4 In the **Scans** window, do one of the following:
 - To scan specific drives, click **Run** next to **Drive Scan**, select the drives that you want to scan, and then click **Scan**.
 - To scan specific folders, click **Run** next to **Folder Scan**, select the folders that you want to scan, and then click **Scan**.
 - To scan specific files, click **Run** next to **File Scan**, select the files that you want to scan, and then click **Add**.
You can also press **Ctrl**, and select multiple files to scan.
You can use the following options to suspend a scan:

Pause	Suspends a custom scan temporarily. Click Resume to continue the scan.
Stop	Terminates the scan.
- 5 In the **Results Summary** window, do one of the following:
 - If no items require attention, click **Finish**.
 - If any items require attention, review them on the **Threats Detected** window.

Running a custom scan

When you run a custom scan, you do not have to redefine what you want to scan. You can run a custom scan from the **Scans** window.

To run a custom scan

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
- 3 Click **Go**.

- 4 In the **Scans** window, click **Run** next to the custom scan that you want to run.

You can use the following options to suspend a custom scan:

Pause	Suspends a custom scan temporarily. Click Resume to continue the scan.
Stop	Terminates a custom scan. Click Yes to confirm.

- 5 In the **Results Summary** window, do one of the following:
 - If no items require attention, click **Finish**.
 - If any items require attention, review the risks on the **Threats Detected** window.

Scheduling a scan

Your Norton product automatically detects the idle state of your computer and runs Quick Scans. However, you can schedule a Full System Scan according to your preferences. You can also set up a schedule for a Quick Scan and for the custom scans that you create.

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (daily, weekly, or monthly), you are presented with additional options. For example, you can request a monthly scan, and then schedule it to occur on multiple days instead.

In addition to the custom scans that you create, your Norton product lets you schedule the Full System Scan and Quick Scan.

You can also schedule the scan to run in specific time intervals (hours or days).

Note: Your Norton product lets you select multiple dates if you schedule a monthly scan.

To schedule a custom scan

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
- 3 Click **Go**.

- 4 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the custom scan that you want to schedule.
- 5 In the **Edit Scan** window, on the **Scan Schedule** tab, do one of the following:
 - If you do not want to run the scan at any particular time, but want to keep the scan options and scan items saved, select **Do not schedule this scan**.
 - To run the scan at specific time intervals, select **Run at a specific time interval**.
 - To run the scan at specific time every day, select **Daily**.
 - To run the scan on a specific day on a week, select **Weekly**.
 - To run the scan on a specific day on a month, select **Monthly**.

These frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
- 6 Under **Run the scan**, do the following:
 - To run the scan only at idle time, check **Only at idle time**.
 - To run the scan only when your computer is connected with external power source, check **Only on AC power**.
 - To prevent your computer from going to a Sleep or Standby mode, check **Prevent standby**.
- 7 Under **After scan completion**, select the state at which your computer should be after the scan is complete. Your options are:
 - **Stay On**
 - **Turn Off**
 - **Sleep**

This option works only if you have configured the power options in your computer using the Windows Control Panel.
 - **Hibernate**

This option works only if you have configured the power options in your computer using the Windows Control Panel.
- 8 Click **Next**.
- 9 In the **Scan Options** tab, click **Save**.

Scanning your computer with Norton Power Eraser

Norton Power Eraser is a powerful malware removal tool that can help you eradicate the security risks that are difficult to remove. If a program hijacked your computer and you have difficulty detecting or removing it, Norton Power Eraser may remove that security risk from your computer. It takes on difficult to detect crimeware known as scareware or rogware that cybercriminals use to trick you into unknowingly download threats onto your computer.

Norton Power Eraser includes detection and removal capabilities for the security risks that impersonate legitimate applications (fake antivirus software), often known as scareware, rogware, or scamware. The tool uses more aggressive techniques than your Norton product; hence there is a risk that it flags legitimate programs for removal. You should carefully review the scan results before removing any files.

When you scan and fix threats, Norton Power Eraser creates a system restore point. If you removed any essential files, Norton Power Eraser lets you restore the files using the **Undo Previous Fix** option. Norton Power Eraser lists the recent repair sessions where you can view and restore the essential files.

To scan using Norton Power Eraser

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Norton Power Eraser**, click **Norton Power Eraser**.
- 3 Click **Go**.
- 4 In the **Norton Power Eraser** window, click **OK**.
- 5 In the **Norton Power Eraser** main window, click **Advanced Options**.
- 6 Under **System Scan**, click **Scan Now**.
- 7 Review the scan results and follow the on-screen instructions to fix the security risks detected.

About Automatic Protection settings

Automatic Protection settings help you configure Boot Time Protection and Real Time Protection features of your Norton product. You can configure these settings to change the way your Norton product detects and removes threats. Removable Media Scan checks for viruses when you insert any removable media.

Boot Time Protection increases security when you start your computer. Boot Time Protection ensures that Auto-Protect runs during boot time. This allows your Norton product to scan files before they are used by another program or the operating system.

You can use the Real Time Protection options to determine what gets scanned. It also actively detects unknown security risks on your computer. You can determine what happens when a security risk or risk-like activity is encountered. Auto-Protect is a very important component of Real Time Protection, so always keep Auto-Protect on.

How do I customize Automatic Protection settings?

Auto-Protect loads into memory and provides constant protection while you work. It checks for viruses and other security risks every time that you run programs on your computer.

Auto-Protect checks for viruses when you insert any removable media, access the Internet, or use the document files that you receive or create.

To customize Automatic Protection settings

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 In the window that appears, set the option to your preferred settings.
- 4 Click **Apply**.

Note: Default settings are recommended for normal users. If you want to turn off a feature temporarily, turn it on as soon as possible. If you want low-risk items removed automatically, configure SONAR Advanced mode.

How do I customize SONAR Advanced mode?

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. You can configure how SONAR removes a threat using SONAR Advanced Mode settings.

To set SONAR to remove threats automatically

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, click **Antivirus**.
- 3 Under **Remove Risks Automatically**, set the slider to **Always**.
- 4 Under **Remove Risks if I Am Away**, set the slider to **Always**.
- 5 Click **Apply**.

How do I exclude a file from Auto-Protect and scans?

If you think your Norton product identifies a valid application as a security risk, you can exclude the file from Norton scans.

To exclude file from Norton scans

- 1 In the Norton product main window, double-click **Security**, and then click **History**.
- 2 In the **Security History** window, in the **Quarantine** view, select the item that you want to restore.
- 3 In the **Details** pane, click **Options**.
- 4 In the **Threat Detected** window, click **Restore**.
- 5 Click **Yes**.

How do I add my POP3 and SMTP email programs to Protected Ports?

Your Norton product protects the email accounts that use non-SSL POP3 and SMTP ports. To ensure email protection, Symantec recommends that you check the POP3 and SMTP port numbers for your email program. If your email program does not use the default port numbers, you must manually add the port numbers to the Protected Ports window. Protected Ports feature helps protect your email program from viruses and other security threats.

Your Internet service provider (ISP) provides you the port numbers for your email program.

To add POP3 and SMTP ports to Protected Ports

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 In the **Antivirus** settings window, click **Scans and Risks** tab.
- 4 Under **Protected Ports**, click **Configure**.
- 5 In the **Protected Ports** window, click **Add**.
- 6 In the **Add Port to protect** window, in the **Port Type** drop-down list, do one of the following:
 - To add the incoming email port, click **POP3**.
 - To add the outgoing email port, click **SMTP**.
- 7 In the **Port** box, type the port number.

The port number must be between 1 and 65535.

- 8 Click **OK**.
- 9 In the **Protected Ports** window, click **Apply**, and then click **OK**.
- 10 In the **Settings** window, click **Close**.

Turning off or turning on SONAR Protection

SONAR protects you against malicious code even before virus definitions are available through LiveUpdate. By default, SONAR Protection is turned on to proactively detect unknown security risks on your computer.

When you turn off SONAR Protection, you are prompted with a protection alert. This protection alert lets you specify the amount of time for which you want SONAR Protection to be turned off.

Note: When Auto-Protect is turned off, SONAR Protection is also disabled. In this case, your computer is not protected against emerging threats.

To turn off or turn on SONAR Protection

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 On the **Automatic Protection** tab, under **Real Time Protection**, move the **SONAR Protection** switch to **Off** or **On**.
- 4 Click **Apply**.
- 5 If prompted, select the duration until when you want the SONAR feature to be turned off, and click **OK**.
- 6 In the **Settings** window, click **Close**.

Excluding security threats from scanning

You can use **Scan Exclusions** window and **Real Time Exclusions** window to exclude viruses and other high-risk security threats from scanning.

To exclude high-risk security threats from scanning

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 In the **Antivirus** settings window, click the **Scans and Risks** tab.
- 4 Under **Exclusions / Low Risks**, do one of the following:

- In the **Items to Exclude from Scans** row, click **Configure**.
 - In the **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection** row, click **Configure**.
- 5 In the window that appears, click **Add Folders** or **Add Files**.
 - 6 In the **Add Item** dialog box, click the browse icon.
 - 7 In the dialog box that appears, select the item that you want to exclude from the scan.
 - 8 Click **OK**.
 - 9 In the **Add Item** dialog box, click **OK**.
 - 10 In the window that appears, click **Apply**, and then click **OK**.

Adding items to the Signature Exclusions

To exclude a security risk from scans, you must add the specific security risk to the **Signature Exclusions** window. You can select a known risk by name and add it to the list.

Note: When you exclude a known security risk from your Norton product scans, the protection level of your computer reduces. You should exclude items only if you are confident that they are not infected.

To add a signature to the Signature Exclusions

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 In the **Antivirus** settings window, click the **Scans and Risks** tab.
- 4 Under **Exclusions / Low Risks**, in the **Signatures to Exclude from All Detections** row, click **Configure**.
- 5 In the **Signature Exclusions** window, click **Add**.
- 6 In the **Security Risks** window, click on a security risk that you want to exclude and then click **Add**.
- 7 In the **Signature Exclusions** window, click **Apply**, and then click **OK**.

Clearing IDs of files that are excluded during scans

Your Norton product tags all trusted and favorable files with **Trusted** and **Good** trust levels. When a file is tagged as **Trusted** or **Good**, the Norton product does not scan this file again. This can improve the scan performance of the Norton product on your computer.

However, if you want the Norton product to scan all the files in your computer, you must clear the reputation information of the excluded files.

Note: When you clear IDs of files that are excluded during scans, it might take a longer time to complete scan.

Your Norton product excludes the **Trusted** and **Good** files from being scanned. However, if you want the Norton product to scan all the files in your computer, you must clear the reputation information of the excluded files.

To clear IDs of files that are excluded during scans

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 In the **Antivirus settings** window, click the **Scans and Risks** tab.
- 4 Under **Exclusions / Low Risks**, in the **Clear file IDs excluded during scans** row, click **Clear All**.
- 5 In the **Warning** window, click **Yes**.

Configuring boot time protection

The boot time protection feature provides enhanced security level from the time you start your computer. As soon as you start your computer, your Norton product starts Auto-Protect and all required drivers and plug-ins start functioning. This feature ensures higher level of security from the moment you turn on your computer.

To configure boot time protection

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
- 3 On the **Automatic Protection** tab, in the **Boot Time Protection** row, click on one of the settings. Your options are:
 - **Aggressive**
 - **Normal**

- **Off**
- 4 Click **Apply**, and then click **Close**.

Turning on or turning off automatic tasks

Your Norton product runs automatic tasks as it quietly works to protect your computer. These automatic tasks include scanning for viruses, monitoring your Internet connection, downloading protection updates, and other important tasks. These activities run in the background when your computer is turned on.

If any item needs your attention, your Norton product displays a message with the information on the current status or prompts you to do something. If you do not see any messages, then your computer is protected.

You can open your Norton product at any time to see the status of your computer at a glance or to view protection details.

When a background activity is in progress, your Norton product notifies you with a message in the notification area that is located at the far-right of the task bar. You can see the results of the latest activities the next time you open the Norton product main window.

To turn on or turn off automatic tasks

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Tasks Scheduling**.
- 3 In the **Task Scheduling** window, on the **Automatic Tasks** tab, do the following:
 - Check the feature that you want to run automatically.
Check the **Tasks** check box to check all the features at once.
 - Uncheck the feature that you do not want to run automatically.
Uncheck the **Tasks** check box to uncheck all the features at once.
- 4 Click **Apply**, and then click **Close**.

Running custom tasks

Your Norton product automatically checks your system and chooses the best settings to keep your system secure. However, you can run some specific tasks. You can choose the specific tasks that you want to run by using the options available in the **Custom Tasks** window.

Your Norton product lets you choose your own combination of tasks for a one-time scan. You can run LiveUpdate, back up your data, clear browsing history, free disk space by cleaning up disk clutter, and optimize your disks.

To run custom tasks

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, under **Scans and Tasks**, click **Custom Task**, and then click **Go**.
- 3 In the **Custom Tasks** window, check the tasks that you want to run.
To select all the tasks, check **Tasks**.
- 4 Click **Go**.

Scheduling security and performance scans

Use the Task Scheduling settings to have your Norton product examine your system automatically for security and performance issues. You can specify when and how often your Norton product performs those examinations.

You have the following options for scheduling security and performance scans:

Automatic (Recommended)	Examine your PC for security and performance issues whenever your PC is idle. This setting provides the maximum protection.
Weekly	Examine your PC one or more times each week for security and performance issues. You can pick the days of the week and the time of day on which the scan performs.
Monthly	Examine your PC once each month for security and performance issues. You can pick the day of the month and the time of day on which the scan performs.
Manual Schedule	Do not perform a scheduled security or performance scan of your PC. If you choose this option, you should perform manual security and performance scans of your PC periodically to maintain protection.

Your computer's performance is maximized if you schedule your critical operations to occur when your computer is idle. When you schedule your scans weekly or monthly and check the **Run only at idle time** option, your Norton product scans your computer when it is idle. Symantec recommends that you check **Run only at idle time** to experience better performance of your computer.

To schedule security and performance scans

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Tasks Scheduling**.
- 3 On the **Scheduling** tab, under **Schedule**, select an option.

When you click **Weekly** or **Monthly**, you must select the time and day to run the automatic tasks. You also have the option of specifying that the automatic tasks must run only when the PC is idle.

- 4 Click **Apply**, and then click **Close**.

Keeping secure on the Internet

This chapter includes the following topics:

- [Turning on or turning off Norton Firewall](#)
- [Customizing Program Rules](#)
- [Changing the order of firewall rules](#)
- [Turning off a Traffic rule temporarily](#)
- [Allowing a blocked program](#)
- [Turning off Firewall Block Notification](#)
- [Removing all devices from Intrusion Prevention exclusion list](#)
- [Turning off and turning on Browser Protection](#)
- [Turning off or turning on AutoBlock](#)
- [Unblocking AutoBlocked computers](#)
- [Adding a device to the Device Trust](#)
- [Turning off or turning on Download Intelligence](#)
- [Turning off or turning on spam filtering](#)
- [Defining the Internet usage of your Norton product](#)
- [Turning off or turning on Network Cost Awareness](#)

Turning on or turning off Norton Firewall

Smart Firewall monitors communications between your computer and the other computers on the Internet. It also protects your computer from common security problems. When the Smart Firewall is turned off, your computer is not protected from Internet threats and security risks.

If you need to turn Smart Firewall off, you should only turn it off for a specified duration, after which it is turned on again automatically.

To turn or turn off Norton Firewall

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **General Settings** tab, in the **Smart Firewall** row, move the **On/Off** switch to **Off** or **On**.
- 4 Click **Apply**.
- 5 If prompted, select the duration until when you want the Firewall feature to be turned off, and click **OK**.

To disable or enable Norton Firewall from the Windows notification area

- 1 In the notification area on the taskbar, right-click the Norton product icon, and then click **Disable Smart Firewall** or **Enable Smart Firewall**.
- 2 If prompted, select the duration until when you want the Firewall feature to be turned off, and click **OK**.

Customizing Program Rules

After you use your Norton product for a while, you might need to change the access settings for certain programs.

To customize Program Rules

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Program Control** tab, in the **Program** column, select the program that you want to change.

- 4 In the drop-down list next to the program that you want to change, select the access level that you want this program to have. Your options are:

Allow	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Custom	Create the rules that control how this program accesses the Internet.

- 5 Click **Apply**.

Changing the order of firewall rules

Each list of firewall rules is processed from the top down. You can adjust how the firewall rules are processed by changing their order.

Note: Do not change the order of the default Traffic rules unless you are an advanced user. Changing the order of default Traffic rules can affect firewall functionality and reduce the security of your computer.

To change the order of Traffic rules

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Traffic Rules** tab, select the rule that you want to move.
- 4 Do one of the following:
 - To move this rule before the rule above it, click **Move Up**.
 - To move this rule after the rule below it, click **Move Down**.
- 5 When you are done moving the rules, click **Apply**.

To change the order of Program rules

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Program Control** tab, select the program that contains the rule that you want to move.
- 4 Click **Modify**.
- 5 In the **Rules** window, select the rule that you want to move.

- 6 Do one of the following:
 - To move this rule before the rule above it, click **Move Up**.
 - To move this rule after the rule below it, click **Move Down**.
- 7 When you are done moving the rules, click **OK**.
- 8 In the **Firewall** settings window, click **Apply**.

Turning off a Traffic rule temporarily

You can temporarily turn off a Traffic rule if you want to allow specific access to a computer or a program. You must remember to turn on the rule again when you are done working with the program or computer that required the change.

Note: You cannot turn off some of the default firewall rules that appear in the list. You can only view the settings of these rules by using the **View** option.

To turn off a Traffic rule temporarily

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Traffic Rules** tab, uncheck the box next to the rule that you want to turn off.
- 4 Click **Apply**.

Allowing a blocked program

Sometimes the Smart Firewall blocks certain programs from accessing the Internet. Such programs might include certain streaming-media programs, network games, or custom business applications that are provided by your employer. If you know that the program's Internet activity is not a threat to your security, you can unblock the program's Internet access.

To allow a blocked program

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Program Control** tab, select the program that you want to allow access to the Internet.

- 4 In the **Access** drop-down list for the program entry, click **Allow**.
- 5 Click **Apply**.

To allow a blocked program from the Security History window

- 1 In the Norton product main window, double-click **Security**.
- 2 Click **History**.
- 3 In the **Security History** window, in the **Show** drop-down list, select **Firewall - Activities**.
- 4 Select the firewall activity that is associated with the blocked program.
- 5 Click **More Options**.
- 6 In the **Security History - Advanced Details** window, under **Actions**, click **Allow**.

Turning off Firewall Block Notification

When Automatic Program Control is turned on, Smart Firewall automatically blocks malicious applications and applications with low reputation from connecting to the Internet or communicating with other machines on your network.

Your Norton product notifies you when Smart Firewall blocks an application from connecting to the network. If you do not want to see the notification, you can turn this off by using **Advanced Program Control**.

To turn off Firewall Block Notification

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **Advanced Program Control** tab, move the **Show Firewall Block Notification** switch to **Off**.

Removing all devices from Intrusion Prevention exclusion list

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. You can then select the **Exclude from IPS scanning** option to exclude these trusted devices from Intrusion Prevention scan. Excluding Full Trust devices from Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a Full Trust device from Intrusion Prevention scan, your Norton product does not scan any information that

is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

If you find that any of the devices that you excluded from Intrusion Prevention scan is infected, you can purge the saved exclusion list and remove all the devices.

You can purge the saved exclusion list under the following circumstances:

- Any of the devices that you excluded from Intrusion Prevention scan is infected.
- Any of the devices that you excluded from Intrusion Prevention scan attempts to infect your computer.
- Your home network is infected.

When a device on your network attempts to infect your computer, AutoBlock stops all the access requests from this device.

When you remove all the devices from the saved exclusion list, Intrusion Prevention scans every request from all the devices that access your computer.

To remove all the devices from the Intrusion Prevention exclusion list

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 Click the **Intrusion and Browser Protection** tab.
- 4 Under **Intrusion Prevention**, in the **Exclusion List** row, click **Purge**.
- 5 In the confirmation dialog box, click **Yes**.
- 6 In the **Settings** window, click **Close**

Turning off and turning on Browser Protection

You can choose whether you want to protect your browser by allowing your Norton product to block unknown programs from accessing your computer.

By default, the **Browser Protection** option is turned on. In this case, your Norton product proactively blocks new or unknown malware programs before they attack your computer. By protecting your browser, your Norton product secures your sensitive information and prevents the attackers from controlling your system remotely. This feature checks for browser vulnerabilities in Internet Explorer 7.0 or later or Firefox 10.0 or later browsers.

Note: Always keep the Browser Protection setting turned on to protect your browser against attacks by malicious websites.

To turn off or turn on Browser Protection

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 Click the **Intrusion and Browser Protection** tab.
- 4 In the **Browser Protection** row, move the **On/Off** switch to **Off** or **On**.
- 5 Click **Apply**.
- 6 If prompted, select the duration until when you want the Browser Protection feature to be turned off, and click **OK**.
- 7 In the **Settings** window, click **Close**.

Turning off or turning on AutoBlock

When an attack is detected from a computer, the attack is automatically blocked to ensure that your computer is safe. If a different *attack signature* is detected from the same computer, your Norton product activates AutoBlock. The AutoBlock feature blocks all traffic between your computer and the attacking computer for a specific time period. During this period, AutoBlock also blocks the traffic that does not match an attack signature.

Note: You can specify the period for which you want your Norton product to block the connections from attacking computers. By default, your Norton product blocks all traffic between your computer and the attacking computer for a period of 30 minutes.

AutoBlock stops traffic between your computer and a specific computer.

If AutoBlock blocks a computer or computers that you need to access, you can turn off AutoBlock.

To turn off or turn on AutoBlock

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 Click the **Intrusion and Browser Protection** tab.
- 4 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
- 5 In the **Intrusion AutoBlock** window, under **AutoBlock**, do one of the following:
 - To turn off Intrusion AutoBlock, click **Off**.

- To turn on Intrusion AutoBlock, click **On (Recommended)**, and then in the **AutoBlock attacking computers for** drop-down list, select how long you want to turn on AutoBlock.
- 6 In the **Intrusion AutoBlock** window, click **OK**.
 - 7 In the **Settings** window, click **Close**.

Unblocking AutoBlocked computers

In some cases, benign network activity can appear to be similar to an attack and AutoBlock blocks the network activity automatically to ensure that your computer is safe. The list of computers that AutoBlock has currently blocked may include the computer that you should be able to communicate with.

If a computer that you need to access appears on the list of blocked computers, you can unblock it. You may want to reset your AutoBlock list if you have changed your protection settings. To reset the AutoBlock list, you can unblock all of the computers that are on the list at one time.

To unblock an AutoBlocked computer

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 Click the **Intrusion and Browser Protection** tab.
- 4 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
- 5 In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, select the IP address of the computer.
- 6 Under the **Action** column, select **Unblock** from the drop-down list.
- 7 In the Intrusion AutoBlock window, click **OK**.
- 8 In the **Settings** window, click **Close**.

Adding a device to the Device Trust

You can manually add a device to the Device Trust. You can add a device by specifying the following:

- The name or description of the device
- The IP address or physical address of the device

Note: If you trust a device that is not on your network, you can expose your computer to potential security risks.

To add a device to the Device Trust

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **General Settings** tab, in the **Device Trust** row, click **Configure**.
- 4 In the **Device Trust** window, click **Add**.
- 5 In the **Add Device** window, in the **Name** box, type the name of the device that you want to add to your network.

The maximum character length of the device name should not exceed 15 characters.

- 6 In the **IP or Physical Address** box, type the IP address or physical address of the device that you want to add to the Device Trust.

You can use the following formats in the **IP or Physical Address** box:

IPv4 address	172.16.0.0
IPv6 address	fe80::12ac:fe44:192a:14cc
Physical address	11-22-c3-5a-fe-a4
Resolvable host	ftp.myfiles.com

The address that you provide is not verified until the device is physically found on the network.

- 7 Select an option from the **Trust Level** drop-down menu. Your options are:

Full Trust Adds a device to the Full Trust list.
 Full Trust devices are monitored only for known attacks and infections. You should select this setting only when you are sure that the device is completely safe.

Restricted Adds a device to the Restricted list.
 Restricted devices do not have access to your computer.

- 8 If you want the device to be excluded from Intrusion Prevention scans, check **Exclude from IPS Scanning**.
- 9 Click **Add Device**.

Turning off or turning on Download Intelligence

Download Insight protects your computer against any unsafe file that you may run or execute after you download it using a supported browser. By default, the **Download Intelligence** option is turned on. In this case, Download Insight notifies you about the reputation levels of any executable file that you download. The reputation details that Download Insight provides indicate whether the downloaded file is safe to install.

There may be times when you want to turn off Download Insight. For example, if you want to download an unsafe file. In this case, you must turn off Download Insight so that your Norton product lets you download the file and does not remove it from your computer.

You can use the **Download Intelligence** option to turn off or turn on Download Insight.

To turn off or turn on Download Intelligence

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 Click the **Intrusion and Browser Protection** tab.
- 4 In the **Download Intelligence** row, move the **On/Off** switch to **Off** or **On**.
- 5 Click **Apply**.
- 6 If prompted, select the duration until when you want the Download Intelligence feature to be turned off, and click **OK**.
- 7 In the **Settings** window, click **Close**.

Turning off or turning on spam filtering

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

To control these spam mails you can use the spam filtering. By default, spam protection remains active. If for any reason you want to disable it, you can turn it off from within the program itself.

Note: Turning off Norton AntiSpam increases your exposure to receive unsolicited email messages.

To turn off or turn on spam filtering

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
- 3 On the **Filter** tab, in the **AntiSpam** row, move the **On/Off** switch to **Off** or **On**.
- 4 Click **Apply**.
- 5 If prompted, select the duration until when you want the Norton AntiSpam feature to be turned off, and click **OK**.
- 6 In the **Settings** window, click **Close**.

Defining the Internet usage of your Norton product

If you think that your Norton product uses too much of your network bandwidth, you can restrict the Internet usage of your Norton product. You can set up policy for each network connection that your Norton product uses to connect to the Internet.

The **Network Cost Awareness** settings window lists all the network connections that your computer uses to connect to the Internet. You can view the status of the network connections that are currently in use. The network policy that you set up defines the amount of network bandwidth that your Norton product can use.

To define the Internet usage of your Norton product

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **General Settings** tab, in the **Network Cost Awareness** row, click **Configure**. If the **Configure** option is disabled, move the **On/Off** switch to **On**.
- 4 In the **Network Cost Awareness** settings window, under the **Policy** column, click the drop-down list next to the network connection for which you want to set up a policy.
- 5 Select one of the following:
 - **Auto** Allows Norton to receive all product and virus definition updates based on the Windows cost awareness policy.

Note: The Auto option is available only in Windows 8 or later.

- **No Limit** Allows Norton to use the required network bandwidth to receive all product and virus definition updates. If you use Windows 7 or earlier, the default policy is **No Limit**.
 - **Economy** Allows Norton to access the Internet only to receive critical product updates and virus definitions. If you have a limited Internet connection, **Economy** ensures you are protected from critical security threats.
 - **No Traffic** Blocks your Norton product from connecting to the Internet. If you choose this policy, Norton cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.
- 6 Click **Apply**, and then click **OK**.
 - 7 In the **Settings** window, click **Close**.

Turning off or turning on Network Cost Awareness

You can set up policies to restrict the Internet usage of your Norton product. If you do not want to restrict the Internet usage of your Norton product, you can turn off **Network Cost Awareness**.

If you feel that your Norton product uses too much network bandwidth, you can turn on **Network Cost Awareness**. Then, you can set up policies to restrict the Internet usage of your Norton product. Your Norton product connects to the Internet based on the policy that you set up in the **Network Cost Awareness** settings window. By default, **Network Cost Awareness** is turned on.

To turn off or turn on Network Cost Awareness

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
- 3 On the **General Settings** tab, in the **Network Cost Awareness** row, move the **On/Off** switch to **Off** or **On**.
- 4 In the **Settings** window, click **Apply**, and then click **Close**.

Securing your sensitive data

This chapter includes the following topics:

- [Adding the Norton browser extensions](#)
- [Turning on or turn off Norton Safe Web](#)
- [Searching the web using Norton Safe Search](#)
- [Turning off or turning on Scam Insight](#)
- [Turning off or turning on Antiphishing](#)
- [Accessing Identity Safe](#)
- [Turning off or turning on Identity Safe](#)
- [Creating cloud vault](#)
- [Deleting your cloud vault](#)
- [Exporting your Identity Safe data](#)
- [Importing your Identity Safe data](#)
- [Disabling and enabling the Norton toolbar](#)

Adding the Norton browser extensions

After you install your Norton product, you are prompted to add the Norton browser extensions to your web browsers. Norton adds the extensions to Internet Explorer, Firefox, and Chrome browsers.

You must enable the Norton browser extensions to easily access all the browser-specific features of Norton Security. The Norton browser extensions include:

Norton toolbar	A toolbar that warns you of dangerous sites when you browse online, helping to protect you from identity theft and online scams.
Norton Safe Search	A secured search engine that uses Ask.com to generate the search results. Norton Safe Search ranks the search results based upon the site safety status and Norton rating.
Norton Home Page	A web page that uses the Norton Safe Search feature to enhance your web search experience. It provides the site safety status and Norton rating for each of the search result generated.
Norton Identity Safe	A secure location where you can store all of your sensitive information such as logins, personal information, and financial information. You can use this information to log in to websites, automatically fill online forms, and online payments.

To add the Norton browser extensions

- 1 In the notification alert that appears at the bottom-right corner, click **Enable Now/Install Now**.

Note: The notification alert automatically disappears after five minutes of inactivity. If you want to enable the Norton extension at a later time, click **Remind Me Later**.

- 2 In the **Enable Norton Security Add-On** pop-up, follow the on-screen instructions to enable the extension.
- 3 Click **OK**.
 A new browser window opens with the Norton toolbar enabled.
- 4 After you have enabled Norton toolbar, you can enable Norton Home Page and Norton Safe Search extensions for your browser. You can use the **Click To Enable** option and follow the on-screen instructions to enable these features.

Turning on or turn off Norton Safe Web

Norton Safe Web protects you when you surf, search, or shop online using Internet Explorer, Firefox, or Chrome. It analyzes the security level of websites that you visit and shows if the websites are free from threats. It provides site rating icons next to search results so that you know if a website is malicious or not before you visit it.

By default, Norton Safe Web is turned on and all Safe Web options are turned on. This is the recommended setting.

To turn on or turn off Norton Safe Web

- 1 In the Norton product main window, double-click **Identity**, and then click **ID Settings**.
- 2 Under **Safe Surfing**, in the **Norton Safe Web** row, move the **On/Off** switch to **On** or **Off**.
- 3 Click **Apply**, and then click **Close**.

Searching the web using Norton Safe Search

Norton Safe Search enhances your web search experience. When you search the Internet using Norton Safe Search, it uses Ask.com to generate the search results. Norton Safe Search provides the site safety status and Norton rating for each of the search results generated.

Norton Safe Search provides you the intelligent search-as-you-type feature that displays search suggestions when you type a few letters of the search phrase.

Note: Norton Safe Search feature is available only for some regions including Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Italy, Japan, Netherlands, Norway, Spain, Sweden, Switzerland, the United States, and the United Kingdom. The Privacy Safeguard feature is available only for the United States, the United Kingdom, and Canada.

You can use Norton Safe Search even when you turn off the Identity Safe features.

Note: Norton Safe Search is supported only in the Internet Explorer, Firefox, or Chrome browsers.

To search the web using Norton Safe Search

- 1 Open your browser.
- 2 On the **Norton toolbar**, in the **Norton Safe Search** box, type the search string that you want to search.
- 3 Do one of the following:
 - Click **Safe Search**.
 - In the pop-up window that appears, select a search suggestion that matches your search string.

Enabling Norton Safe Search

When you install your Norton product, it adds the Norton toolbar to the supported browsers. When you open your browser, you are prompted to enable the **Norton Safe Search** box on your toolbar. To enable Norton Safe Search, click **Enable Now** in the pop-up window. If you do not want Norton Safe Search to be your default search provider, click **No Thanks**.

If you have manually disabled Norton Safe Search box and want to enable it again, do the following:

- 1 Open your browser.
- 2 On the Norton toolbar, click the settings (...) icon.
- 3 In the menu that appears, move the switch next to **Norton Safe Search** to **On**.

Turning off or turning on Scam Insight

Scam Insight prevents you from divulging your sensitive information such as Social Security Numbers or credit card information, to fraudulent websites. It helps you detect the websites that are suspicious or vulnerable using reputation-based threat detection. It mainly focuses the websites that require you to enter your personal information.

You can use the **Scam Insight** option in the **Identity Protection settings** window to turn on or off the Scam Insight feature.

The **Norton Safe Web** pop-up window helps you understand if the website that you visit is safe or unsafe.

To turn off or turn on Scam Insight

- 1 In the Norton product main window, double-click **Identity**, and then click **ID Settings**.
- 2 Under **Safe Surfing**, in the **Scam Insight** row, move the **On/Off** switch to **Off** or **On**.
- 3 Click **Apply**, and then click **Close**.

Turning off or turning on Antiphishing

Antiphishing protects you from visiting unsafe websites. The Antiphishing feature analyzes the security level of all the websites that you visit and displays the results in the **Norton Safe Web** pop-up window. Antiphishing also blocks the websites that are confirmed to be fraudulent.

The **Norton Safe Web** pop-up window helps you understand if the website that you visit is safe or unsafe.

You can turn off or turn on Antiphishing in the **Safe Surfing** section of the **Identity Protection** settings window.

To turn off or turn on Antiphishing

- 1 In the Norton product main window, double-click **Identity**, and then click **ID Settings**.
- 2 Under **Safe Surfing**, in the **Antiphishing** row, move the **On/Off** switch to **Off** or **On**.
- 3 Click **Apply**.
- 4 If prompted, select the duration until when you want the Antiphishing feature to be turned off, and click **OK**.
- 5 Click **Close**.

Accessing Identity Safe

You can access the Identity Safe settings from the following areas:

- From the **Identity** section in the product main window
- From the Norton toolbar

You can access all the Identity Safe data even after the product expires. The following are the features that you can view or access after the product expires:

Logins	You can view the stored login information, such as your login credentials for your online bank account, email user ID, and password.
Addresses	You can view your stored personal information, such as name, date of birth, postal address, email address, and phone numbers.
Wallet	You can view your stored financial information, such as credit card information, bank account information, and credit payment details.
Notes	You can view the text that you entered for future reference.

Note: You must be signed in to Identity Safe to access the Identity Safe features. The Identity Safe features are supported only in the Internet Explorer, Firefox, and Chrome browsers.

Turning off or turning on Identity Safe

Identity Safe helps you manage your identity and provide additional security while you perform online transactions. You can use the various features in Identity Safe to manage your personal data such as addresses, date of birth and credit card information.

You can turn off or turn on the Identity Safe from the **Quick Controls** in the **Settings** window or from the **Settings** window for **Identity Protection**.

Note: After you turn on Identity Safe, you must sign in to Identity Safe to access the various features.

To turn off or turn on Identity Safe from Quick Controls

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Quick Controls**, do one of the following:
 - To turn off Identity Safe, uncheck **Identity Safe**.
 - To turn on Identity Safe, check **Identity Safe**.

To turn off or turn on Identity Safe from the Settings window

- 1 In the Norton product main window, double-click **Identity**, and then click **ID Settings**.
- 2 In the **Identity Protection** settings window, in the **Identity Safe** row, move the **On/Off** switch to **Off** or **On**.
- 3 Click **Apply**, and then click **Close**.

Creating cloud vault

Identity Safe lets you create a cloud vault and save your Identity Safe data. You can create one cloud vault for each Norton account. You cannot create a new local vault. However, you can move your existing local vault data to cloud vault when you upgrade to the Norton product. When you move your Identity Safe data from local vault to cloud vault, the data in your local vault cannot be accessed. cloud vault provides you the ease of using your Identity Safe data when you are on the move.

You can access the Identity Safe cloud vault from any computer that is connected to the Internet.

To create cloud vault

- 1 In the Norton product main window, double-click **Identity**, and then click **Identity Safe**.
- 2 In the **Get started** window, click **Sign In**.
If you do not have a Norton account, use the **Sign up now!** link to create a new Norton account.
- 3 In the **New Vault creation: Vault password** window, in the **Vault Password** box, type your password, and then click **Next**.
- 4 In the **New Vault creation: confirm password** window, type the password again to confirm, and then click **Next**.
- 5 In the **New Vault creation: password hint** box, type a hint for the password, and click **Next**.
If you already have a backup of your Identity Safe data, click **Import** and select the backed-up file to merge to the new account.
- 6 Click **Finish**.

Deleting your cloud vault

Your cloud vault is encrypted and can be accessed only by using your Norton account and vault passwords. To delete your cloud vault, you have to do it manually. Even if you uninstall the Norton product from your device, you can still continue to use your vault from other devices.

Warning: When you delete a vault, all of the Identify Safe data that are stored in the vault is permanently removed. If you think that you may use your vault data at a later time, do not delete your vault.

To delete your cloud vault

- 1 In the Norton product main window, double-click **Identity**, and then click **Identity Safe**.
- 2 In the **Vault Closed** window, type your password incorrectly for three times.
- 3 Click the **Click here** link next to the **Need to delete your Vault?** option.
- 4 In the **Delete Vault** window, click **Yes, Delete My Vault**.
- 5 In the warning dialog box, click **Yes**.
- 6 Type your Norton account password to validate and click **Sign In**.
- 7 In the confirmation window, click **OK**.

How do I access my cloud vault account after I uninstall my Norton product?

- 1 [Sign in](#) to the Norton Identity Safe website with your Norton account credentials.
- 2 In the **Open your vault** window, type your vault password and click **Open Vault**.

Exporting your Identity Safe data

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer. Your vault password cannot be reset. So, Symantec recommends that you back up your vault data periodically. When you enable automatic backup feature, backups of your vault are automatically created and stored locally on your device. You can access your vault backups at **Users\<User Name>\My Documents\Norton Identity Safe Backups\<Norton account name>**.

You can retrieve Identity Safe data when your product expires.

To export your Identity Safe data

- 1 In the Norton product main window, double-click **Identity**, and then click **Identity Safe**.
- 2 In the **Norton Identity Safe** window, click the **Settings** icon available at the bottom of the window.
- 3 Click the **Import/Export** tab.
- 4 In the **Export** pane, select the file format.

You can select one of the following:

- **Identity Safe Backup Format – DAT File**

If you want to back up your data with a password for more security, type and confirm the password.

- **Plain Text – CSV file (Logins & Notes only)**
- 5 Click **Export**.
 - 6 In the **Validate Password for Identity Safe** window, type your vault password to export your Identity Safe data.
 - 7 In the confirmation dialog box, click **OK**.

Importing your Identity Safe data

You can import your Identity Safe data from the file that you previously backed up. You can also import the Identity Safe data from the portable profile that you saved in the older version of your Norton product.

The Merge imported data with existing data and Replace existing data with imported data options appear when you import Identity Safe data from a backup file. You can merge the imported data in to the vault that you are currently signed in or replace the existing Identity Safe data that you stored in your vault

Note: When you import, the file size must not be more than 15 MB for .CSV files and 35 MB for .NPM files.

To import your data

- 1 In the Norton product main window, double-click **Identity**, and then click **Identity Safe**.
- 2 In the **Norton Identity Safe** window, click the **Settings** icon available at the bottom of the window.
- 3 Click the **Import/Export** tab.
- 4 In the **Import** row, click **Import**.
- 5 In the **Vault Import** window, select one of the following options:
 - **Merge imported data with existing data**
 - **Replace existing data with imported data**
- 6 Click **Import**.
- 7 Browse to the location of the file that you want to import.
- 8 Select the file, and then click **Open**.
- 9 If you have different passwords for the logins that you stored in the currently using vault and the importing vault, Norton displays a confirmation message. Select one of the following:

- Click **Keep Existing Password** to retain the password that is stored in the cloud vault.
- Click **Keep Imported Password** to overwrite the password that is stored in the cloud vault with the password stored in the importing vault.

10 In the confirmation dialog box, click **OK**.

Disabling and enabling the Norton toolbar

You can hide the **Norton toolbar** if you do not want to see the evaluation of every website that you visit. When you hide the toolbar, Norton Identity Safe does not display the **Norton Safe Web** pop-up window. However, Identity Safe notifies you about suspicious and fraudulent websites or if an error needs your attention.

To disable the Norton toolbar

- ◆ Launch your Internet browser and do one of the following:
 - On Internet Explorer, right-click on the menu bar, uncheck **Norton Toolbar**, and then click **Disable** in the **Disable add-on** dialog box.
 - On Mozilla Firefox, click **Tools > Add-ons > Extensions**. In the **Extensions** page, under **Norton Identity Safe Toolbar**, click **Disable**.
 - On Google Chrome, go to the following URL: `chrome://extensions`. In the **Extensions** page, under **Norton Security Toolbar** and **Norton Identity Protection**, uncheck **Enabled**.

To enable the Norton toolbar

- ◆ Launch your Internet browser and do one of the following:
 - On Internet Explorer, right-click on the menu bar, check **Norton Toolbar**, and then click **Enable** in the **Enable add-on** dialog box.
 - On Mozilla Firefox, click **Tools > Add-ons > Extensions**. In the **Extensions** page, under **Norton Identity Safe Toolbar**, click **Enable**.
 - On Google Chrome, go to the following URL: `chrome://extensions`. In the **Extensions** page, under **Norton Security Toolbar** and **Norton Identity Protection**, check **Enabled**.

Keeping your PC tuned up

This chapter includes the following topics:

- [Viewing the resource usage of running processes](#)
- [Optimizing your permanent disks manually](#)
- [Configuring performance alerts](#)
- [Running a scan to clean up disk clutter](#)
- [Running Diagnostic Report](#)
- [Managing startup items](#)
- [Optimizing your boot volume](#)

Viewing the resource usage of running processes

File Insight shows the CPU graph and the system resource usage for running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage by the process.

To determine the resource usage of a running process

- 1 In the **File Insight** window, in the left pane, click **Activity**.
- 2 In the **Show** drop-down list, do one of the following:
 - Select **Performance** to view the performance graph of the process.
 - Select **Performance Alert** to view the performance alert-related details of the process.
 - Select **Network** to view the network activities of the process.
- 3 Click **Close**.

Optimizing your permanent disks manually

Optimizing your computer's permanent disks can improve performance and reliability. Your Norton product automatically checks your permanent disks for fragmentation and optimizes them if they are more than 10 percent fragmented. You can always check the latest reports to see if optimization is necessary.

Note: You can run Disk optimization only when disk has more than 15 percent of free space.

Some programs, such as movie-editing programs or programs that require large amounts of disk space, can work more efficiently if your disks are optimized. If you prefer not to wait until the product performs the automatic optimization, you can optimize your disks manually.

Note: During the disk optimization process, solid-state drives (SSD) are defragmented only in Windows 8 or later.

To optimize your permanent disks manually

- 1 In the Norton product main window, double-click **Performance**, and then click **Optimize Disk**.
- 2 When the activity is complete, click **Close**.

Configuring performance alerts

You can use the **Performance Alerting** option in your Norton product to receive *performance alerts* when there is an increased usage of system resources by any program or process.

To configure performance alerts

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.

3 Under **Performance Monitoring**, in the **Performance Alerting** row, move the switch to:

Off

Turns off performance alerts.

Select this option if you do not want your Norton product to notify you with performance alerts.

On

Turns on performance alerts.

Select this option if you want your Norton product to notify you with performance alerts when a program or process exceeds the threshold limit of the system resource usage.

Log Only

Monitors and records the system resource usage.

Select this option if you want your Norton product to only monitor the system resource usage of every program or process running on your computer.

By default, the **Performance Alerting** option is set to **Log Only**.

When a program or process exceeds the threshold limit of the system resource usage, your Norton product records these details in the **Security History** window. You can view the details that are related to performance alerts under **Performance Alert** category in the **Security History** window.

4 Under **High-Usage Alert for**, do one of the following:

- If you want your Norton product to monitor the CPU usage, move the **CPU** switch to **On**.
- If you want your Norton product to monitor the memory usage, move the **Memory** switch to **On**.
- If you want your Norton product to monitor the disk usage, move the **Disk** switch to **On**.
- If you want your Norton product to monitor the handle count, move the **Handles** switch to **On**.

By default, this option is turned off.

- 5 Click **Apply**, and then click **Close**.

Running a scan to clean up disk clutter

Various activities, such as extensive web browsing or a series of software installations produce temporary files. You can run a manual cleanup scan to remove the temporary files immediately.

To clean up your disk clutter

- 1 In the Norton product main window, double-click **Performance**, and then click **File Cleanup**.
- 2 When the activity is complete, click **Close**.

Running Diagnostic Report

Diagnostic Report gathers information about your computer, which includes the operating system, programs, and hardware. You can use this report to find and fix the issues.

The Diagnostic Report is a real-time report with a timestamp. The product does not generate this report automatically. You need to use the **Diagnostic Report** option in the **Scans** window and manually generate the report.

If your Norton product finds any issues on your computer, you can use the **Fix Now** option to resolve the issues.

You can save, email, or print the report when needed for review.

To run Diagnostic Report

- 1 In the Norton product main window, double-click **Security**, and then click **Scans**.
- 2 In the **Scans** window, select **Diagnostic Report**, and then click **Go**.

Managing startup items

Startup Manager monitors and lists the programs that automatically start when you turn on your computer. To reduce the start time of your computer and improve the performance, you can delay the start of some of the programs when you turn on your computer.

Your Norton product delays the start of the delayed programs by five minutes. The first delayed program in the **Startup Manager** window starts five minutes after you

start your computer. Every subsequent delayed program starts with a further delay of ten seconds.

To delay startup items

- 1 In the Norton product main window, double-click **Performance**, and then click **Startup Manager**.
- 2 In the **Startup Manager** window, in the **Delay Start** column, select the program that you want to delay.
- 3 Click **Apply**.
- 4 Click **Close**.

To run delayed startup items manually

- 1 In the product main window, double-click **Performance**, and then click **Startup Manager**.
- 2 In the **Startup Manager** window, click **Run Delayed Items Now**.
- 3 Wait for the program to start, and then in the **Startup Manager** window, click **Close**.

Optimizing your boot volume

The **Optimize** option lets you optimize your boot volume to improve the boot time of your computer. Optimization of your boot volume maximizes the usable free space by rearranging file fragments into adjacent and contiguous clusters. When the drive head of your hard disk accesses all of the file data in one location, the file is read into the memory faster.

When you use the **Optimize** option, your Norton product optimizes the drive that contains the boot volume. Therefore, it requires more time to complete optimization.

You can access the **Optimize** option at the top of the security status graph in the **Graphs** window. You can also optimize your boot volume using the **Insight Optimizer** option in the **Background Tasks** window. The **Insight Optimizer** row in the background jobs list that is available in the **Background Tasks** window displays the details of the boot volume optimization process. You can view details such as timestamp, duration, and status of the background job.

To optimize your boot volume from the Graphs window

- 1 In the Norton product main window, double-click **Performance**, and then click **Graphs**.
- 2 In the **Graphs** window, at the top of the security status graph, click **Optimize**.

To optimize your boot volume from the Background Tasks window

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
- 3 In the **Background Tasks** row, click **Configure**.
- 4 In the **Background Tasks** window, under the **Norton Tasks** column, click the play icon that appears before **Insight Optimizer**.

Protecting your media and data

This chapter includes the following topics:

- [Backing up your files](#)
- [Restoring files](#)
- [Creating a new backup set](#)
- [Adding files and folders to a backup set](#)
- [Choosing a backup location](#)
- [Purchasing more online storage space](#)
- [Turning off or turning on backup](#)

Backing up your files

After you provide your Norton product with your preferred backup settings, running a backup is very easy. In fact, if you scheduled all backup sets to run backups automatically, you do not need to do anything at all. Your Norton product performs automatic backups for all backup sets when your PC is turned on but not engaged in performing any other tasks. However, your Norton product does not back up your files automatically if the backup destination is a CD, DVD, or Blu-ray disc. Backing up to these destinations needs your intervention.

Whether you have set your Norton product to back up your PC automatically or not, you can always run a backup. For example, you have added or modified important files and you want to be sure they are safe. In this case, you can run a backup manually. You can also run a backup at the end of the day if you do not want to wait for an automatic backup to occur.

You can view the details of your backup activity under the backup category in the **Security History** window.

To back up your files

- 1 In the Norton product main window, double-click **Backup**, and then click **Run Backup**.
- 2 Follow any instructions for performing the backup that your Norton product provides.

For example, if you choose to back up your files to CDs, then your Norton product asks you to insert a recordable CD.

- 3 In the **Backup** window, click **Close**.

Restoring files

The reason to have a good backup is to restore your files from the backup if the need arises. Your Norton product provides an easy method to restore your backed-up files.

By default, your Norton product displays the backup location of the most recent backup set you ran and the original locations of the files.

Note: To restore files from online backup, you must set the **Network Cost Awareness** option in the **Firewall Settings** window to **No Limit**.

When you restore files, you can change any of the following settings:

Restore From

You can choose any of the backup sets to restore the files.

If you backed up your data in an external media, you must connect it to your computer to restore those files. Your Norton product lists all the backup sets that you ran backup for and that your PC can currently detect.

Files

You can restore the backed up files in a backup set that you selected. You can use the **Search** option to search for files by name and add the selected file to restore. You can also check the **Restore All Files and Categories** option next to the **Files** heading to select all file categories. In addition, you can browse for backed up files based on file categories and folders by using the **Browse for Files and Folders** option.

You can filter the backed up files in a backup set by the backup file categories.

Restore To

You can restore to the original locations of the files, or navigate to a new location where you can restore your files. Your Norton product displays the total number of files and the total size of the files that you have selected for restoration.

If files with the same name are present at the original location, the files that you restore replace those files.

Warning: If you backed up files to CDs or DVDs, do not restore files by copying them directly to your PC from the backup disks. When your Norton product backs files up to CDs or DVDs, it sometimes has to split files between two discs. Directly copying a file back from a disc, therefore, may only copy part of the file. Such a file appears to be damaged when you try to use it. Instead, let your Norton product restore your files for you.

To restore files

- 1 In the Norton product main window, double-click **Backup**, and then click **Restore Files**.
- 2 In the **Restore Files** window, do one or more of the following:
 - Under **Restore From**, change where to restore from.
 - Under **Files**, specify what to restore.
 - Under **Restore To**, change where to restore the files to.
- 3 Click **Restore Files**.
- 4 Follow the on-screen instructions to finish restoring your files.

Creating a new backup set

You can create multiple backup sets with different configurations. For example, you can create a backup set to back up your pictures to your local fixed disk. You can create another backup set to back up your videos to a CD. You can also configure different schedules for each backup set.

When you create a new backup set, your Norton product applies the default configuration for the backup set. You can change the configuration if the default configuration does not meet your needs.

You can identify each backup set with a backup set name. The default name of a backup set is **DefaultSet**. You can save a backup set with the default name as well. But, whenever you create a new backup set, you must provide a name for the backup set. The maximum character length of a backup set name is 32 characters. You cannot create more than 10 backup sets.

To create a new backup set

- 1 In the Norton product main window, double-click **Backup**, and then click **Backup Sets**.
- 2 On the **Summary** tab, under **Things You Can Do**, click **Create new backup set**.
- 3 In the window that appears, type a name for your backup set, and then click **OK**.
- 4 On the **What** tab, under **File Types**, select a file category.
- 5 In the **Manage Backup Sets** window, click **Save Settings**.

Adding files and folders to a backup set

You are not limited to backing up the files that your Norton product automatically detects and places into its file categories. You can add files to the set of files to be backed up, and you can exclude files from being backed up as well.

Your Norton product lets you select a file or folder from your computer that you want to include in your backup. The **Add or exclude files and folders** option on the **What** tab in the **Manage Backup Sets** window provides you the options to add files and folders to a backup set.

You can also right-click a file or a folder and add it to a backup set using the Norton Security option on the shortcut menu. The shortcut menu is available after you configure your backup and when the **Manage Backup Sets** window and the **Restore Files** window are closed. When you add a file to the backup set, your Norton product lists the information in the window that appears when you click **Add or exclude**

files and folders option. You can view all the files and folders that you added to the backup.

You can also remove an addition from the list of items that is included or excluded from backup by using the **Remove from list** option. This option is available in the window that appears when you click **Add or exclude files and folders**.

To add a file to a backup set

- 1 In the Norton product main window, double-click **Backup**, and then click **Backup Sets**.
- 2 On the **What** tab, click **Add or exclude files and folders**.
- 3 In the window that appears, click **Include File**.
- 4 In the file selection window that appears, navigate to file that you want to add, click to select it, and then click **Open**.
- 5 Click **OK**.
- 6 In the **Manage Backup Sets** window, click **Save Settings**.

To add a folder to a backup set

- 1 In the Norton product main window, double-click **Backup**, and then click **Backup Sets**.
- 2 On the **What** tab, click **Add or exclude files and folders**.
- 3 In the window that appears, click **Include Folder**.
- 4 In the folder selection window that appears, navigate to the folder that you want to add, and then click **OK**.
- 5 Click **OK**.
- 6 In the **Manage Backup Sets** window, click **Save Settings**.

To add a file or folder to a backup set in Windows Explorer

- 1 In Windows Explorer, right-click the file or folder, select **Norton Security > Add to Backup**.

The **Add to Backup** option in the shortcut menu is enabled only after you configure your backup and when the **Manage Backup Sets** window and **Restore Files** window are closed.

- 2 Click the backup set to which you want to add the file or the folder.

Choosing a backup location

Your Norton product can back up your files to several kinds of storage locations. The speed, safety, and quantity of your backup depend on the choice of your location. No one backup location is the best in all situations and for all users.

You can choose any storage location that your Norton product offers for your backup location, depending on your PC and the connected devices. Use the information in the following table to choose a location that best meets your needs for safety, speed, and storage capacity:

Secure Online Storage

Your subscription to your Norton product comes with an allocation of storage space on a secure server that is located on the Internet. This location is the safest, most secure backup choice available because it stores your information in a remote location. As a consequence, even the disasters that might damage or destroy your PC cannot affect your backups. Online backups can take place automatically, as long as your PC has an active Internet connection. However, you require a reasonably fast Internet connection.

You can configure the Internet bandwidth that backup uses to back up your files using **Bandwidth Throttle** on the **Where** tab of the **Manage Backup Sets** window.

You can alter the following bandwidth throttle states:

- **Fastest (recommended)**
- **High usage**
- **Moderate usage**
- **Low usage**

You can buy more online storage space whenever you want.

Note: To use the **Secure Online Storage** option, you must set the Network Cost Awareness option in the Firewall settings window to **No Limit**.

C: (Local Fixed Disk)

This choice backs your files up to a special folder on drive C of your PC. Backing up to drive C is very quick and convenient, and is only limited to the amount of free space available on your drive. You can run automatic backups with this choice. Backing up to drive C is a convenient but an unsafe backup method. Any mechanical problem that the drive might experience can damage both your original files and your backups. If you use drive C for quick and automatic backups, you must back up your files occasionally to a different drive or another location.

Other internal or external drive

This choice provides for fast, convenient backups. You can run automatic backups and always have access to your backed up files as long as the drive is connected to your PC.

Although using another drive is safer than using drive C, doing so still leaves your data at risk from any PC hardware malfunctions.

If you choose to back up to another drive, you should also back up your files occasionally to some other location.

CD, DVD, or Blu-ray discs

This choice requires that you have recordable CDs, DVDs, or Blu-ray discs and an optical drive in your PC to record on those discs. You must be present to insert and remove discs when requested. Therefore, you cannot select automatic scheduling of backups when you back up to CDs, DVDs, or Blu-ray discs.

Backing up to CDs, DVDs, or Blu-ray discs is slower than backing up to other media. Backing up to CDs, DVDs, or Blu-ray discs is also less convenient because you must be present during the backup.

By using your Norton product, you can back up your data to any of the following optical media types if your optical drive supports them:

- CD-R
- CD-RW
- DVD+R
- DVD-R
- DVD+R DL
- DVD-R DL
- DVD+RW
- DVD-RW
- DVD RAM
- BD-R
- BD-RE

You should store your backup discs in a safe place elsewhere to provide protection against a disaster that occurs at your computer's location.

Note: When you select the CD or the DVD Drive as the backup location for the first time, your Norton product prompts you to configure the optical backup drive on your computer. Your Norton product lets you install the optical driver.

Network drive

You can use this choice if your PC is connected to a local network that offers a storage location to which you have access. Depending on the speed of your network, this choice can be almost as fast as backing up to an internal drive or external drive.

This choice does not appear if your PC is not connected to a network that offers a storage device to which you have access.

To back up your data to an external network drive, you must map the external network drive to your computer. When you map a drive, you must also specify a drive letter for the connection.

Flash drive and removable storage devices, including iPod

Flash drives and the other data storage devices that are attached to your PC can also serve as backup locations.

Your Norton product displays such devices as external disk drives. If such a device is always attached to your PC, you can use it for automatic backups.

The amount of storage space that is available on these devices can be less than on hard disks. If you use a flash drive for backups, you should also back up your files occasionally to another storage location.

When you select Secure Online Storage as the backup location, your Norton product prompts you to register to your Norton account. You must be connected to the Internet to register to your Norton account.

To use Secure Online Storage as a backup location, you must set the **Network Cost Awareness** option in the Firewall settings window to **No Limit**.

Note: You must activate your Norton product with a valid license key to use the online storage space.

To choose a backup location

- 1 Make sure that the device to which you want to back up your data is connected to your PC and turned on.
- 2 In the Norton product main window, double-click **Backup**, and then click **Backup Sets**.

- 3 On the **Where** tab, select the location and device where you want your backups to be stored.

If the device or location does not appear on the list, click **Refresh List**.

- 4 Click **Save Settings**.

Purchasing more online storage space

Your Norton product subscription comes with an allotment of secure online storage space. When your Norton product performs an online backup, it calculates the amount of space that it needs for the backup. If your online storage does not contain sufficient space for the backup, your Norton product notifies you and provides you an option to buy more space.

You do not have to wait until your Norton product tells you that you need more online storage space. You can purchase additional space at any time.

You must be connected to the Internet to purchase more online storage space.

Symantec provides 25 GB of online storage for each Norton product key. You can share the online storage space that is allocated to you using your Norton account among your computers. For example, you have two computers having Norton product installed on them and registered with the same Norton account. You can share the storage space among your two computers. You use 10 GB of online storage space for your first computer. When you activate the online storage for your second computer using the same Norton account, that computer can use the remaining 15 GB of space.

Note: The online storage space differs based on the product that you use.

To purchase additional online storage space when backing up

- 1 When your Norton product notifies you that it needs more online storage space, click **Buy More Storage**.

Your browser opens to a secure page, on which you can purchase additional online storage space.

- 2 Follow the instructions on the secure webpage to purchase additional online storage space.

To purchase additional online storage space at other times

- 1 In the Norton product main window, double-click **Backup**, and then click **More Storage**.

Your browser opens to a secure page, on which you can purchase additional online storage space.

- 2 Follow the instructions on the webpage to purchase additional online storage space.

Turning off or turning on backup

When the **Backup** option is turned on, your Norton product automatically backs up your files when your computer is idle. However, if you want to temporarily disable backup, you can turn it off from within the program.

When you turn off backup, the backup status in the Norton product main window changes from **Protected** to **Disabled**. In the Disabled state, your Norton product disables all automatic backup of files. You can use the **Run Backup** option in the main window if you want to back up your files from all the backup sets.

You can turn off or turn on backup from the **Settings** window, **Backup Settings** window, or from the **Backup Details** window.

To turn backup off or turn on backup from the Settings window

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Quick Controls**, do one of the following:
 - To turn off backup, uncheck **Backup**.
 - To turn on backup, check **Backup**.

To turn off or turn on backup from the Backup Settings window

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Backup Settings**.
- 3 In the **Backup Settings** window, do one of the following:
 - To turn off backup, move the **On/Off** switch to **Off**.
 - To turn on backup, move the **On/Off** switch to **On**.
- 4 In the **Settings** window, click **Apply**.

To turn off or turn on backup from the Backup Details window

- 1** In the Norton product main window, click **Backup**, and then click **View Details**.
- 2** In the **Backup Details** window, under **Things You Can Do**, do one of the following:
 - To turn off backup, click **Turn Off Backup**.
 - To turn on backup, click **Turn On Backup**.

Customizing settings

This chapter includes the following topics:

- [Configuring Network Proxy Settings](#)
- [Customizing your Norton product settings](#)
- [Configuring Norton for best battery use](#)
- [Turning on or turning off Remote Management](#)
- [Securing your Norton product settings using a password](#)
- [Resetting your Norton product settings password](#)
- [Turning off or turning on Norton Product Tamper Protection](#)

Configuring Network Proxy Settings

When you use a proxy server to connect to the Internet, you must specify the proxy server details. The **Network Proxy Settings** window lets you enter automatic configuration settings, proxy settings, and proxy server authentication settings. The Network Proxy settings let you connect to the Internet while you perform tasks such as activating the product or accessing the support options.

To configure Network Proxy Settings

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
- 3 In the **Network Proxy Settings** row, click **Configure**.
- 4 In the **Network Proxy Settings** window, do the following:

- If you want your browser to automatically detect network connection settings, under **Automatic Configuration**, check **Automatically detect settings**.
 - If the proxy server requires an automatic configuration URL, under **Automatic Configuration**, check **Use automatic configuration script**. Type the URL of the PAC file in the **URL** box.
 - If your network uses a proxy server, under **Proxy Settings**, check **Use a proxy server for your HTTP connections**. In the **Address** box, type the URL or IP address of your proxy server, and in the **Port** box, type the port number of your proxy server. You can specify a value from 1 to 65535.
 - If your proxy server requires a user name and password, under **Authentication**, check **I need authentication to connect through my firewall or proxy server**. Type the user name in the **Username** box and password in the **Password** box.
- 5 In the **Network Proxy Settings** window, click **Apply**.

Customizing your Norton product settings

The default Norton product settings provide a safe, automatic, and efficient way to protect your computer. However, if you want to change or customize your protection settings, you can access most features from the **Settings** window.

You can configure the Norton product settings in the following ways:

- You can use the **On/Off** switch to turn on or turn off a feature. When you turn off a feature, the color of the **On/Off** switch turns red, which indicates that your computer is vulnerable to security threats. When you turn on a feature, the color of the **On/Off** switch turns green, which indicates that your computer is protected against security threats.
- You can drag the slider of a protection feature to your preferred setting. Most often, your Norton product provides the slider setting for you to decide whether to resolve security threats automatically or ask you before it takes an action.
- You can configure a protection feature by either selecting the options that are provided for the configuration or by providing the required information. Most of these options are available as check boxes for you to check or uncheck. You can also use the **Use Defaults** option to reset the configuration to the default level.
- You can select a preferred option from the drop-down list.
- You can check or uncheck the **Quick Controls** options to turn on or turn off a feature.

The Norton product also provides the **Use Defaults** option in most of the **Settings** window. You can use this option to reset the configuration to the default level.

To customize the Norton product settings

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, click the protection feature that you want to customize.
- 3 In the window that appears, set the option to your preferred settings.
You may need to click a tab to access the settings that are listed under that tab.
- 4 In the **Settings** window, do one of the following:
 - To save the changes, click **Apply**.
 - To close the window without saving the changes, click **Close**.

Configuring Norton for best battery use

When your computer runs on battery power, it is important that all active software programs consume minimum resource usage. By reducing resource usage, your computer gains longer battery life and becomes more energy efficient.

You can configure a low threshold profile and ensure that all programs consume minimum resource usage. When the resource usage of a program or a process exceeds the low threshold limit, your Norton product notifies you with a *performance alert*. You can choose to close the program or the process manually and free the resource.

If the **Use Low Resource Profile On Battery Power** option in the **Administrative Settings** window is turned on, your Norton product automatically changes the threshold profile to low when your computer runs on battery power. By default, this option is turned on.

Note: Symantec recommends that you keep the **Use Low Resource Profile On Battery Power** option turned on.

To turn off or turn on the Use Low Resource Profile On Battery Power option

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.

- 3 Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to **Off** or **On**.
- 4 Click **Apply**, and then click **Close**.

Turning on or turning off Remote Management

Remote Management lets you remotely manage your Norton product using your Norton account. When you turn on the **Remote Management** option, you can view your Norton product details and fix some security issues of your device.

When the **Remote Management** option is turned on, your Norton product sends details related to your Norton product to your Norton account. When this option is turned off, your Norton product does not publish any of its details.

By default, the **Remote Management** option is turned off.

In some cases, you are prompted to enter your Norton account password when turning on **Remote Management** option.

To turn on or turn off Remote Management

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
- 3 In the **Remote Management** row, move the **On/Off** switch to **On** or **Off**.
- 4 Click **Apply**, and then click **Close**.

Securing your Norton product settings using a password

You can secure your Norton product settings from unauthorized access by setting up a password for your product settings. The **Settings Password Protection** option in the **Administrative Settings** window lets you secure your Norton product settings using a password.

After you set up a password for the Norton product settings you must enter the password each time to view or configure your product settings.

By default, the **Settings Password Protection** option is turned off. You must turn on the **Settings Password Protection** option to set up a password for your product settings.

Note: The password must be between 8 and 256 characters in length.

To secure your Norton product settings using a password

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
- 3 Under **Product Security**, in the **Settings Password Protection** row, move the **On/Off** switch to **On**.
- 4 Click **Apply**.
- 5 In the dialog box that appears, in the **Password** box, type a password.
- 6 In the **Confirm Password** box, type the password again.
- 7 Click **OK**.
- 8 In the **Settings** window, click **Close**.

Resetting your Norton product settings password

If you forget your Norton product settings password, you can reset the password. You can reset your Norton product settings password using the **Reset settings password** option in the **Select Your Uninstall Preference** window.

To access the **Select Your Uninstall Preference** window, you must choose to uninstall your Norton product. However, you need not uninstall the product to reset your settings password.

Note: The **reset settings password** option appears in the **Select Your Uninstall Preference** window only if the **Settings Password Protection** option is turned on. To use the **Settings Password Protection** option, go to the Norton product main window, and then click **Settings > Administrative Settings > Product Security**.

To reset your Norton product Settings password

- 1 On the Windows taskbar, do one of the following:
 - In Windows XP, Windows Vista, or Windows 7, click **Start > Control Panel**.
 - In Windows 8, on the **Apps** screen, under **Windows System**, click **Control Panel**.
 - In Windows 10, click **Start > All apps**, under **Windows System**, click **Control Panel**.
- 2 In **Windows Control Panel**, do one of the following:
 - In Windows XP, double-click **Add or Remove Programs**.

- In Windows Vista, double-click **Programs and Features**.
 - In Windows 7 or Windows 8, click **Programs > Programs and Features**. The **Programs** option in Windows 7 or Windows 8 is available when you select the **Category** option in the **View by** drop-down list.
 - In Windows 10, click **Uninstall a program**.
- 3 In the list of currently installed programs, do one of the following:
 - In Windows XP, click your Norton product, and then click **Change/Remove**.
 - In Windows Vista, Windows 7, Windows 8, or Windows 10, click your Norton product, and then click **Uninstall/Change**.
 - 4 At the bottom of the **Select Your Uninstall Preference** window, click **Reset settings password**.
 - 5 In the dialog box that appears, in the **Reset Password Key** box, type the randomly generated key that is displayed against **Reset Password Key**.
 - 6 In the **New Password** box, type the new password.
 - 7 In the **Confirm New Password** box, type the new password again.
 - 8 Click **OK**.

Turning off or turning on Norton Product Tamper Protection

Norton Product Tamper Protection protects the Norton product files from an attack or modification by any virus or other unknown threat. You can protect your product from accidental modification or deletion by keeping the **Norton Product Tamper Protection** option turned on.

If you want to temporarily turn off **Norton Product Tamper Protection**, you can turn it off for a specified duration.

Note: You cannot run System Restore on your computer when **Norton Product Tamper Protection** is turned on. You must temporarily turn off **Norton Product Tamper Protection** to run a successful System Restore.

To turn off or turn on Norton Product Tamper Protection

- 1 In the Norton product main window, click **Settings**.
- 2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.

- 3 Under **Product Security**, in the **Norton Product Tamper Protection** row, move the **On/Off** switch to **Off** or **On**.
- 4 Click **Apply**.
- 5 If prompted, select the duration until when you want the feature to be turned off, and click **OK**.
- 6 In the **Settings** window, click **Close**.

Finding additional solutions

This chapter includes the following topics:

- [Finding the version number of your product](#)
- [Checking for a new version of the product](#)
- [Solving problems with Norton Autofix](#)
- [Reasons for Fix Now failures](#)
- [Uninstalling your Norton product](#)

Finding the version number of your product

If you want to upgrade your Norton product or want to reach the customer support for assistance, you must know the full version number of the Norton product installed on your computer. This helps you get exact solution for your problems.

To find the version number of your product

- 1 In the Norton product main window, click **Help**.
- 2 In the **Help Center** window, under **General Information**, click **About**.

Checking for a new version of the product

You can upgrade your product to the latest version if you have an active subscription. If a new version is made available by Symantec, you can download and install the new version of your product. You can also let your Norton product notify you when a new version of your product is available. You can do so by turning on the **Automatic Download of New Version** option in the **Administrative Settings** window. The latest version of your product may contain new and enhanced features for better protection against security threats.

When you check for a new version, details about your product such as product name and version are sent to Symantec servers. The servers then check whether a new version of the specified product is available or not.

If a new version is available, you can download and install it from the webpage. If a new version is not available, the webpage informs you about it. In such case, you can run LiveUpdate to obtain latest program and definition updates and keep the existing version of your product up to date.

The upgrade process might not work if your browser is incompatible to communicate with the Symantec servers. The supported browsers are Internet Explorer 6.0 or later, Chrome 10.0 or later, and Firefox 3.6 or later.

Note: Your product must be activated, and you need the Internet to check and install new version of the product.

To check for a new version of the product

- 1 In the Norton product main window, click **Help**.
- 2 In the **Help Center** window, click **New Version Check**.

The website displays whether a new version is available or not.

Note: This option is available only if you have an active subscription or service.

- 3 If a new version is available, follow the on-screen instructions to download the new product.

Solving problems with Norton Autofix

Note: Your device must be connected to the Internet to resolve issues using Norton Autofix.

Norton Autofix provides additional product support with one-click access from your Norton product main window. It performs a Quick Scan of your computer and repairs problems without your intervention. If the problem persists, you can use the **Open Support Web Site** option to go to the Norton Support website for help using our online forum, chat, email, or telephone.

In addition, the Norton Support website provides access to the knowledge base articles. These articles can help you resolve your technical problems.

The support technicians can help you solve more complex problems by using remote-assistance technology. The remote-assistance technology allows Symantec support technicians to access your computer as remote users so that they can perform maintenance or service.

Note: Support offerings can vary based on the language or product.

When you click the **Get Support** option in the **Help Center** window, your Norton product checks your Internet connection. To access Norton Autofix, ensure that your computer is connected to the Internet.

If you use a proxy server to connect to the Internet, you must configure the proxy settings of your Norton product.

If you do not know your proxy settings, contact your Internet service provider or network administrator for assistance.

To solve a problem using Norton Autofix

- 1 In the Norton product main window, click **Help**, and then click **Get Support**.
- 2 In the Norton Autofix window, do one of the following:
 - If there is a problem connecting to the Internet, ensure that your device is connected and then click **Retry** to complete the Autofix process.
 - If you still have problem with the Internet connection, click **Skip** to continue with other Norton Autofix processes.
 - If the problem is not fixed automatically, click **Open Support Web Site** for further assistance.
 - If you cannot connect to the Support website, use the **click here** link to get the support contact numbers.
 - If the problem is fixed, click **Close**.

Reasons for Fix Now failures

Your Norton product works silently in the background to protect you from all types of security threats. If Norton detects any significant issues that may block your protection or reduce your system performance, it performs a fix now task.

In some circumstances, the fix now task fails.

The reasons for Fix Now failures and how to resolve them:

- **Subscription expiration**

Ensure that your subscription is active. To check your subscription, on the main window, click **Help** and then click **Subscription Status**.

- **Slow Internet connection**
 Your product obtains the updates from the Norton servers. If your Internet connectivity is slow, the updates that are required to fix issues in your product cannot be downloaded. Ensure that your connection has better speed to download all virus definitions.
- **Computer is completely infected**
 If your computer is severely infected and the product does not have enough updates to clean the viruses, **Fix Now** may fail. Run **Norton Power Eraser** to clean up your computer. For instructions, See [“Scanning your computer with Norton Power Eraser”](#) on page 37.
- **Threats not completely removed**
 When the threats are removed, the Norton product prompts you to restart your computer. If you skip to restart, the **Fix Now** may fail at a later stage when you run it.
- **Protection updates are outdated**
 In some cases, you may not have the latest protection updates if you have upgraded to the latest version of the product. Run **LiveUpdate** several times to get the latest protection updates.
- **LiveUpdate failure**
 If **LiveUpdate** fails, **Fix Now** also fails.
- **No Internet connection**
 Ensure that your device is connected to the Internet. Check that the parental control settings and proxy settings do not block your connection.
- **Network Cost Awareness is set to Economy or no Traffic**
 If the Network Cost Awareness option is set to **Economy** or **No Traffic** mode, your computer cannot get the latest updates. To change this setting, See [“Defining the Internet usage of your Norton product”](#) on page 56.
- **Firewall does not allow the traffic**
 Make sure your product’s Firewall settings are enabled to allow traffic. For more information, See [“Turning on or turning off Norton Firewall”](#) on page 47.
- **Date and time is not correct**
 If your computer date and time was changed manually or incorrect, **Fix Now** may fail. Ensure that you have set the date and time correct.
- **Not enough space on your computer**
 If there is not enough space on the disk to install the updates, **Fix Now** may fail. Free some space on the disk and run **LiveUpdate**.

Uninstalling your Norton product

You can remove your Norton product from your computer in the following ways:

- From Windows **Control Panel**.
- From the **Start** menu.
- From Windows **Start** screen (Windows 8/8.1).

Note: You should print out the Uninstalling your Norton product Help topic before continuing with the uninstallation. You cannot access online Help during uninstallation.

If you want to reinstall your Norton product on your computer, you must uninstall your Norton product from your computer. You can reinstall the product using the installation file that you downloaded from Norton. To reinstall your Norton product, See [“Downloading and installing Norton”](#) on page 12.

To uninstall your Norton product from Windows Control Panel

- 1 Do one of the following:
 - On the Windows Taskbar, click **Start > Control Panel**.
 - In Windows 8, go to **Apps**, and under **Windows System**, click **Control Panel**.
 - In Windows 10, click **Start > All apps**, and under **Windows System**, click **Control Panel**.
- 2 In Windows **Control Panel**, do one of the following:
 - In Windows XP, double-click **Add or Remove Programs**.
 - In Windows Vista, double-click **Programs and Features**.
 - In Windows 7 and Windows 8, click **Programs > Programs and Features**. The **Programs** option is available when you select the **Category** option in the **View by** drop-down list.
 - In Windows 10, click **Uninstall a program**.
- 3 In the list of currently installed programs, do one of the following:
 - In Windows XP, click your Norton product, and then click **Change/Remove**.
 - In Windows Vista, Windows 7, Windows 8, or Windows 10, click your Norton product, and then click **Uninstall/Change**.

- 4 If you do not want to keep Norton Home Page as your default home page and Norton Safe Search as your default search provider, select the check box that appears at the bottom.
- 5 Under **Select Your Uninstall Preference**, click one of the following:
 - **I plan to reinstall a Norton product. Please leave my settings behind.**
 Lets you retain your settings, passwords, and preferences for Norton features before you uninstall your Norton product.
 Select this option if you want to reinstall your Norton product or another Norton product.
 - **Please remove all user data.**
 Lets you completely remove your Norton product without saving your settings, passwords, and preferences.
- 6 If your Norton product offers to install the Norton toolbar after uninstall, do one of the following:
 - To keep the Norton toolbar after uninstall, click **Keep & Continue**.
 - To uninstall your Norton product without keeping the Norton toolbar, click **No, Thanks**.
- 7 Click **Next**.
- 8 Do one of the following:
 - Click **Restart Now** (recommended) to restart your computer.
 - Click **Restart Later** to restart your computer later.

Your Norton product is not fully uninstalled until you restart your computer.

To uninstall your Norton product from the Start menu

- 1 On the Windows taskbar, click **Start > All Programs/All apps > Norton Security > Uninstall Norton Security**.
- 2 If you do not want to keep Norton Home Page as your default home page and Norton Safe Search as your default search provider, select the check box that appears at the bottom.
- 3 Under **Select Your Uninstall Preference**, click one of the following:
 - **I plan to reinstall a Norton product. Please leave my settings behind.**
 Lets you retain your settings, passwords, and preferences for Norton features before you uninstall your Norton product.
 Select this option if you want to reinstall your Norton product or another Norton product.
 - **Please remove all user data.**

Lets you completely remove your Norton product without saving your settings, passwords, and preferences.

- 4 If your Norton product offers to install the Norton toolbar after uninstall, do one of the following:
 - To keep the Norton toolbar after uninstall, click **Keep & Continue**.
 - To uninstall your Norton product without keeping the Norton toolbar, click **No, Thanks**.
- 5 Click **Next**.
- 6 Do one of the following:
 - Click **Restart Now** (recommended) to restart your computer.
 - Click **Restart Later** to restart your computer later.

Your Norton product is not fully uninstalled until you restart your computer.

To uninstall your Norton product from the Start screen in Windows 8/8.1

- 1 On the **Start** screen, right-click your Norton product, and then click **Uninstall**.
- 2 In the list of currently installed programs, click your Norton product, and then click **Uninstall/Change**.
- 3 If you do not want to keep Norton Home Page as your default home page and Norton Safe Search as your default search provider, select the check box that appears at the bottom.
- 4 Under **Select Your Uninstall Preference**, click one of the following:
 - **I plan to reinstall a Norton product. Please leave my settings behind.**
 Lets you retain your settings, passwords, and preferences for Norton features before you uninstall your Norton product.
 Select this option if you want to reinstall your Norton product or another Norton product.
 - **Please remove all user data.**
 Lets you completely remove your Norton product without saving your settings, passwords, and preferences.
- 5 If your Norton product offers to install the Norton toolbar after uninstall, do one of the following:
 - To keep the Norton Identity Safe after uninstall, click **Keep & Continue**.
 - To uninstall your Norton product without keeping the Norton Identity Safe, click **No, Thanks**.

6 Click **Next**.

7 Do one of the following:

- Click **Restart Now** (recommended) to restart your computer.
- Click **Restart Later** to restart your computer later.

Your Norton product is not fully uninstalled until you restart your computer.