Norton™ Security

Product Manual

Care for our Environment; 'It's the right thing to do.'
Symantec has removed the cover from this manual to reduce the Environmental Footprint of our products. This manual is made from recycled materials.

Norton™ Security Product Manual

Documentation version 22.0

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 Getting started 7
Activation protects you 7
About Norton Security main window 11
Sign In to your Norton account 19
About Norton Bootable Recovery Tool 20
Starting Norton Security from the command prompt 31
Responding to security status indicators 31
About Norton LiveUpdate 35
Configuring Network Proxy Settings 41

Chapter 2 Monitoring your system's performance 43
About System Insight 43
30-Day Report 70

Chapter 3 Protecting your files and data 73
About maintaining protection 73
About the Norton Security scans 74

Chapter 4 Responding to security issues 111
About keeping your computer secure 111
About solving connection problems 112
About responding to emergencies 113
What to do if a security risk is found 114

Chapter 5 Doing routine tasks 125
Turning on or turning off automatic tasks 125
Running custom tasks 126
Scheduling security and performance scans 127
Specifying Idle Time Out duration 128

Chapter 6 Protecting Internet activities 130
About the Smart Firewall 131
Turning off and turning on Browser Protection 160
Turning off or turning on Download Intelligence 161
Configuring the Download Insight Notifications option 162
Configuring the Show Report on Launch of Files option 163
Turning off or turning on Intrusion Prevention notifications 166
Excluding or including attack signatures in monitoring 167
Turning off or turning on AutoBlock 169
Unblocking AutoBlocked computers 170
Permanently blocking a computer that has been blocked by AutoBlock 170
About Intrusion Prevention exclusion list 171
Removing all devices from Intrusion Prevention exclusion list 172
Adding a device to the Device Trust 173
Changing the trust level of your network and devices 175
About the types of security risks 179
About Norton AntiSpam 180
Adding POP3 and SMTP ports to Protected Ports 192
Removing an email port from Protected Ports 193

Turning off or turning on Network Cost Awareness 194
Defining the Internet usage of Norton Security 195

Chapter 7 Securing your sensitive data 197
About Norton Safe Web 197
About Antiphishing 203
About Identity Safe 207
About Norton toolbar 247
Norton Identity Safe 251

Chapter 8 Keeping your computer tuned up 255
About disk and file fragmentation 255
Optimizing your permanent disks manually 256
About using optimization efficiently 257
About cleaning up disk clutter 258
Running a scan to clean up disk clutter 259
Running Diagnostic Report 259
Managing startup items 260
Disabling or enabling startup items 261

Chapter 9 Monitoring protection features 262
About Security History 262

Chapter 10 Customizing protection features 294
Feature summary 294
About turning off automatic features 298

Chapter 11 Customizing settings 303
Customizing Norton Security settings 303
Turning on or turning off Quick Controls services 305
About Automatic Protection settings 305
About Scans and Risks settings 312
About Antispyware and Updates settings 319

About the Intrusion and Browser Protection settings 322
Turning on or turning off Remote Management 323
Resetting your Norton product Settings password 324
Turning off the Norton product Settings password 325
Securing your Norton product Settings using a password 326
About Norton Product Tamper Protection 327

Chapter 12 Finding additional solutions 330
Finding the version number of your product 330
Finding the End-User License Agreement 331
About upgrading your product 331
Solving problems with Norton Autofix 334
Reasons for Fix Now failures 335
About Support 337
Uninstalling your Norton product 339

Index 344

Getting started

1

This chapter includes the following topics:

- Activation protects you
- About Norton Security main window
- Sign In to your Norton account
- About Norton Bootable Recovery Tool
- Starting Norton Security from the command prompt
- Responding to security status indicators
- About Norton LiveUpdate
- Configuring Network Proxy Settings

Activation protects you

Product activation verifies that you are authorized to use the software and initiates your subscription. It ensures that you have a genuine Norton product installed on your computer. Only genuine Norton products can receive updates from Symantec and in turn protect you from threats. Activation is a simple process that protects you from pirated or counterfeit software. Pirated software is something that is illegally copied or distributed, and not legitimately licensed. You put yourself under the risk of viruses, security breach,

system crashes, and much more if you use pirated software.

To activate the product, you need:

- a license or a product key
- a Norton account
- an Internet connection

When you activate Norton Security, you are prompted to sign in to Norton account. If you want to create an account or have problem accessing the account, See "Sign In to your Norton account" on page 19.

Norton account stores all your registered licenses that you can use with the Norton products. After signing in, you can do one of the following to activate the product:

- Enter a product key. For help on locating the product key, See "Where to find your product key or PIN?" on page 9.
- Use an existing license for this product. Your license is automatically registered with Norton account if you purchased the product from the Norton Store or you already activated your product.

  You can also transfer a license from one device to another at ease. If you transfer a license, the device from which the license is removed is no longer protected.

- Buy a new subscription.

You start to see activation alerts a few days before the product expiration date. If you do not activate the product within the time period that the alert specifies, the product stops working. However, you can activate it after the time period has elapsed, but you are not protected until you activate the product.

To activate Norton Security

1. In the Norton Security main window, click **Activate Now**.
   You can also click **Activate Now** from the activation alert.

2 If prompted, sign in to your Norton account with your Norton credentials.

3 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.

Where to find your product key or PIN?

There are different ways to locate your product key depending on how you acquired the product. The product key is a unique key that you need to activate the Norton product on your computer. The product key is a 25-character alphanumeric string that is shown in five groups of five characters each, separated by hyphens.

If you got the product from a service provider, you need an activation PIN. A PIN is a 13-character alphanumeric code provided by your service provider. To locate your PIN, See the section called “Finding your PIN” on page 10.

Finding your Norton Security product key

- If you purchased your Norton product from the Norton Store or your product is registered to your Norton account, you can log on to Norton and get the product key.
- If you purchased Norton Security from third-party websites or retail outlets, See the section called “Other ways to find the product key” on page 10.

Getting the product key from Norton

1 Sign in to Norton.

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 Norton Security from third-party websites, the product key is in the order confirmation email. If you do not find the email in your Inbox, check your spam folder.
- If you purchased Norton Security as a boxed product, the product key is printed either on a sticker on the back of the box or on a card kept inside the box.
- If the product came pre-installed on your device, you may find the product key in the text file at Program Files > Symantec. If you do not see the text file, you can contact your device manufacturer for the product key. Some manufacturers may provide the product key on an activation card.

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 folder. If you still cannot locate your PIN, contact your service provider.
- You can also find your PIN in the **Symantec** Folder under **My Documents**.

About problems during activation

If you cannot connect to the Symantec servers to activate your product, first check your Internet connection. You then need to see if you have parental control software, either installed or through your ISP, that might block the connection.

A connectivity problem can occur if you use parental control software. If you suspect that parental controls might block the connection, you can configure the parental controls so that they do not block the activation

procedure. You need to log in to your parental control software or to the Internet through your ISP as an administrator to change your configuration.

If you use a proxy server to connect to the Internet, you must configure the proxy settings. To configure the proxy settings, go to the Norton Security main window, and then click **Settings > Administrative Settings > Network Proxy Settings > Configure**.

About Norton Security main window

The Norton product main window acts as a security management interface. You can access the main features and monitor the performance of your computer from the main window.

As you use your computer, your Norton product monitors how well your computer and activities are protected from threats, risks, and damage. Your Norton product displays the protection status of your computer in the main window.

Depending on the security status of your computer, your Norton product shows your system status as **Secure**, **Attention**, or **At Risk**. If your system status is marked as **Attention** or **At Risk**, at the bottom of the main window, click **Fix Now** to resolve all the security threats on your computer.

The options that are available in the main window summarize the most essential security and the productivity issues that challenge users. They are:

Security	Includes all virus, spyware, and other security features.
Identity	Includes the protection against phishing and fraudulent websites.

Performance	Includes the performance tuning features, such as cleaning up unwanted files.

You can use the **30-Day Report** link at the top of the main window to view a summary of all the activities that your Norton product has performed to protect you in the last 30 days.

You can use the **Settings** link at the top of the main window to access the **Settings** window and configure the different features that your Norton product offers.

When you click the **Get Support** option in the **Help** drop-down menu, the Norton Autofix feature performs a scan and fixes problems automatically. If you need more information, click the **Open Support Web Site** link in the **Norton Autofix** window to access the Support website.

When your system status is **At Risk** or **Attention**, this section automatically provides you the **Fix Now** option to fix all the issues at once.

The options available when you double-click **More Norton** help you do the following:

Add Devices	Lets you install the latest version of the Norton product on other devices. This ensures that Norton protects your computer and other devices. You can use the **Open Norton** option to access your Norton account. You can use your Norton account credentials to sign in. After logging in, you can use the following options: ▪ **Download Norton**: You can download the Norton product to your current device or on another device. Access to Norton account may not be available in some versions of Norton Security.
Identity Safe	Lets you access the Norton Identity Safe website to download the Norton Identity Safe app for your Android and iOS devices. Norton Identity Safe may not be available in some versions of Norton Security.

Manage	Lets you access your Norton account. When you click the **Manage** icon, the Norton product main window displays a summary of features you can use to manage your Norton product. Click the **Manage My Protection** option to access your Norton account. You can use your Norton account credentials to sign in. Access to Norton account may not be available in some versions of Norton Security.

Family	Lets you monitor your child's activities on the Internet. Norton Family provides you advanced controls to monitor your child's online activities. Norton Family may not be available with some versions of Norton Security. In such case, you may not be able to access Norton Family options. When you click the **Family** icon, the Norton Security main window displays a summary of the features that you can use to keep your family safe online. Click the **Sign up now FREE** option to go to the Norton Family website. You can use your Norton account login credentials to sign in to Norton Family. If you register your product with your Norton account, your product directly logs you in to the Norton Family website.

Studio

Lets you access Norton Studio.

Norton Studio is a Windows 8 app that lets you manage your Norton products and Norton product keys from one location. You can view the security status of each of your devices and resolve the security issues by using the Norton Studio from any location around the world. You can go to Windows 8 App Store to download and install Norton Studio.

This option appears only in Windows 8. This option may not be available in some versions of Norton Security.

Backup	Lets you access the online storage and back up your data. Norton Online Backup may not be available in some versions of Norton Security. You can use the **Backup** icon to purchase online storage and back up your data to a secure online location. You need to accept the license agreement to use Norton Online Backup. Norton Online Backup provides a secure online backup solution that safeguards your important data against system crash, accidental deleting, virus infection, and other disasters. You can access or restore the backed up data from any computer that is connected to the Internet.

Your activation status or subscription status appears at the bottom of the main window. You can use the **Activate Now** option to activate or subscribe your Norton product.

Monitoring the protection status of a feature

The Norton Security main window acts as a security management interface. You can access the main features and monitor the performance of your computer from the main window.

At times, you may want to turn off any option for a particular purpose. But by doing so, the status of your

system changes to **Attention** or **At Risk**. In such cases, you can ignore the protection status of a particular feature to maintain a healthy overall system status. For example, you want to turn off **Browser Protection** for a limited period, and you still want the system status to be **Secure**. In this case, you can ignore the protection status of **Browser Protection** and then, turn off the option. When you ignore the protection status of a feature, it does not affect the overall **System Status**.

You can also monitor the protection status of the feature that has been ignored at any time.

You can ignore or monitor the protection status of only selected features that are available in the Advanced window.

The features are:

- Antivirus
- Antispyware
- SONAR Protection
- Smart Firewall
- Intrusion Prevention
- Email Protection
- Browser Protection
- Safe Surfing

To monitor the protection status of a feature

1. In the Norton Security main window, double-click **Security**, and then click **Advanced**.
2. In the window that appears, move your mouse pointer over the feature name.
3. In the pop-up that appears, do one of the following:
   - To ignore the protection status of the feature that affects your computer's overall health evaluation, click **Ignore**.
   - To monitor the protection status of the feature that has been ignored, click **Monitor**.

Sign In to your Norton account

A Norton account lets you access a variety of Norton offerings such as Norton Security, Norton Family, and so on. You need to sign in to your Norton account to do the following on your Norton product:

- Activate your product
- Renew your subscription
- Check your subscription status
- Access or create your cloud Vault

The Norton account offers you many benefits including:

- Simple management of all your Norton products at one place
- Convenient reinstall of your Norton products by using your product keys stored in your account

How do I sign in to Norton account?

To sign in, you need an email address and a password that you used while registering for Norton account. Type the email address and the password in the required fields and click **Sign In**.

If you stay signed in to your Norton account, you do not have to enter your Norton account credentials every time you want to access some of the features.

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.

I forgot my Norton account password

First, ensure that you are connected to the Internet. You must be connected to the Internet to sign in to your Norton account. Second, check the email address and password that you provided.

If you still cannot access your sign in, do the following:

1 Click **Forgot your password link?**

2 Type the email address that you used while registering for Norton account. Norton sends you an email that lets you reset the password.

3 Open the email and click the **Reset Password** link to create a new password.

I do not know if I have a Norton account

If you have installed or activated Norton Security, you most likely have a Norton account. Norton account is required to install or activate Norton Security.

If you have purchased Norton Security from Norton Store, a Norton account is automatically created for you.

If you have signed up for other Norton products, you may a Norton account. But, ensure that you are using the same account that has the Norton Security license associated with it.

I want to create a Norton account

If you are sure that you do not have a Norton account, you can create one at no cost. All you need is a valid email address. Symantec sends the product updates and other information related to your account to this email address.

To create a Norton account

1 Click **Sign up now!**

2 Enter a valid email address and password for your account. You need to use these credentials to log in to Norton account in future.

3 Choose your region.

4 Read the privacy policy and agree to it.

5 Click **Sign Up**.

About Norton Bootable Recovery Tool

Norton Bootable Recovery Tool scans and removes viruses, spyware, and other security risks from your

computer. Your computer might be infected with a virus if you experience any of the following symptoms:

- You cannot install Norton Security.
- You cannot start your computer.
- Your computer is extremely slow.

Norton Bootable Recovery Tool is integrated with Windows Preinstallation Environment (WinPE). Therefore, you can run Norton Bootable Recovery Tool only from a DVD or USB drive. You must use Norton Bootable Recovery Tool Wizard to create the Norton Bootable Recovery Tool DVD or USB drive.

You cannot run Norton Bootable Recovery Tool in WinPE for more than 72 hours. If you run Norton Bootable Recovery Tool for more than 72 hours, your computer restarts without any notification.

You can use the Norton Bootable Recovery Tool DVD or USB drive to recover a computer that is infected with viruses and other security threats. This security program is not a replacement for continuous, real-time protection from viruses and latest security risks. To protect your computer from future infections, be sure to install or continue using Norton Security that you already purchased.

Norton Bootable Recovery Tool detects and resolves the following security threats:

Viruses	Programs that infect another program, boot sector, partition sector, or document by inserting themselves or attaching themselves to that medium. Most viruses just replicate; many also do damage.

Trojan horses	Programs containing malicious codes that are disguised as or hiding in something benign, such as a game or utility.
Hacking tools	Tools that are used by a hacker to gain unauthorized access to your computer. One type of hacking tool, a keystroke logger, tracks and records your individual keystrokes and can send this information back to the hacker.
Spyware	Programs that can scan systems or monitor activity and relay the information to other computers or locations in cyberspace.
Adware	Programs that facilitate the delivery of advertising content through their own window, or by using another program's interface.

Trackware	Programs that track system activity, gather system information, or track user habits, and relay this information to third-party organizations. The information that is gathered by such programs is neither personally identifiable nor confidential. Trackware programs are installed with the user's consent, and may also be packaged as part of other software that is installed by the user.

Downloading the Norton Bootable Recovery Tool Wizard

If your attempt to install a Norton product fails, you can download the Norton Bootable Recovery Tool Wizard. This easy-to-use wizard helps you create Norton Bootable Recovery Tool on a DVD or USB drive. You can use Norton Bootable Recovery Tool to scan your computer and remove any security threats that prevent successful installation.

It is recommended that you download and install Norton Bootable Recovery Tool Wizard on a computer that does not have any security threats and create Norton Bootable Recovery Tool. If you create Norton Bootable Recovery Tool on an infected computer, there is a chance that the recovery DVD or USB drive might get infected.

You can download Norton Bootable Recovery Tool Wizard in one of the following ways:

- From the **Start** menu.
- From the Norton Support website.

To download the Norton Bootable Recovery Tool Wizard from the Start menu

1. Do one of the following:
   - In Windows XP, click **Start > Programs > Norton Security > Norton Recovery Tools**.
   - In Windows Vista or Windows 7, click **Start > All Programs > Norton Security > Norton Recovery Tools**.
   - In Windows 8, you can download Norton Bootable Recovery Tool Wizard from the Norton Support website.
2. Follow the on-screen instructions.

To download the Norton Bootable Recovery Tool Wizard from the Internet

1. Open your browser, and go to the following URL: http://www.norton.com/recoverytool
2. Follow the on-screen instructions.

Creating Norton Bootable Recovery Tool on a DVD

Norton Bootable Recovery Tool is integrated with Windows Preinstallation Environment (WinPE). Therefore, you can run Norton Bootable Recovery Tool only from a DVD or USB drive. To use it, you first need to burn it to a DVD.

If you choose to create Norton Bootable Recovery Tool on a re-writable DVD, all the data that are stored in the DVD are permanently deleted. Ensure that you back up all the data before creating Norton Bootable Recovery Tool on a re-writable DVD.

To create Norton Bootable Recovery Tool DVD

1. Open your DVD drive and insert an empty DVD.
2. In the **Norton Bootable Recovery Tool** main window, click **DVD**.

3 In the **Create on DVD media** window, do one of the following:
   - Select the DVD drive from the **Specify drive** drop-down list.
   - If you want to add drivers, click **Add** next to **Add drivers**.
   - If you want to change the default language, click **Change** next to **Specify language**. You can change the language in the **Select Language** window. By default, Norton Bootable Recovery Tool is created in English.
4 Click **Next**.
5 If you want to create Norton Bootable Recovery Tool on a re-writable DVD, click **Yes** to confirm.
6 Review the results and do one of the following:
   - Click **Done** to close Norton Bootable Recovery Tool.
   - Click **Back to Main** to create or update Norton Bootable Recovery Tool in another media.

Creating Norton Bootable Recovery Tool ISO file

You can create a Norton Bootable Recovery Tool ISO file on your computer. You can burn this ISO file to a DVD and use it as a recovery DVD on any computer. You can also use this ISO file to point to any virtual machine as a virtual DVD-ROM.

To create Norton Bootable Recovery Tool ISO file

1 In the **Norton Bootable Recovery Tool Wizard** main window, click **ISO file**.

2 In the **Create ISO file** window, do the following:
   - If you want to save the ISO file to a specific location, click **Change** next to **Select location**.

     You can browse and select the folder location.
   - If you want to add drivers, click **Add** next to **Add drivers**.
   - If you want to change the default language, click **Change** next to **Specify language**.

     You can change the language in the **Select Language** window. By default, Norton Bootable Recovery Tool is created in English.
3 Click **Next**.
4 Review the results and do one of the following:
   - Click **Done** to close Norton Bootable Recovery Tool.
   - Click **Back to Main** to create or update Norton Bootable Recovery Tool in another media.

Creating Norton Bootable Recovery Tool on a USB drive

You can create Norton Bootable Recovery Tool on a USB drive and use it to run Norton Bootable Recovery Tool on your computer.

When you create Norton Bootable Recovery Tool on a USB drive, all the data that are stored in this USB drive are permanently deleted, and the USB drive is formatted. Ensure that you back up all the data before creating Norton Bootable Recovery Tool on a USB drive.

To create Norton Bootable Recovery Tool on a USB drive

1 Insert the USB drive into the USB port of your computer.
2 In the **Norton Bootable Recovery Tool Wizard** main window, click **USB key**.

3 In the **Create on USB key** window, do the following:
   - Select the USB drive from the **Specify drive** drop-down list.
   - If you want to add drivers, click **Add** next to **Add drivers**.
   - If you want to change the default language, click **Change** next to **Specify language**.

     You can change the language in the **Select Language** window. By default, Norton Bootable Recovery Tool is created in English.
4 Click **Next**.
5 In the confirmation message, click **Yes** to let Norton Bootable Recovery Tool format your USB drive before creating Norton Bootable Recovery Tool.
6 Review the results and do one of the following:
   - Click **Done** to close Norton Bootable Recovery Tool.
   - Click **Back to Main** to create or update Norton Bootable Recovery Tool in another media.

Accessing Norton Bootable Recovery Tool Wizard

Norton Bootable Recovery Tool is integrated with Windows Preinstallation Environment (WinPE). Therefore, you can run Norton Bootable Recovery Tool only from a DVD or USB drive.

Norton Bootable Recovery Tool Wizard helps you create Norton Bootable Recovery Tool. You can create Norton Bootable Recovery Tool on a DVD or USB drive. You can use this media to run Norton Bootable Recovery Tool on your computer.

You can go to your Norton account and access the Norton Bootable Recovery Tool download link.

To access your Norton account, go to the following address:

https://account.norton.com

To access Norton Bootable Recovery Tool Wizard

1. Do one of the following:
   - Double-click the Norton Bootable Recovery Tool Wizard icon on your computer desktop.
   - In Windows XP, Windows Vista, and Windows 7, on the Windows taskbar, click **Start > All Programs > Norton Bootable Recovery Tool Wizard > Norton Bootable Recovery Tool Wizard**.
   - In Windows 8, you can access Norton Bootable Recovery Tool Wizard from the Norton Support website.
2. Follow the on-screen instructions to download Norton Bootable Recovery Tool Wizard.

Using the Norton Bootable Recovery Tool

If the installation of your Norton product fails, you can use the Norton Bootable Recovery Tool to scan and remove any security threats that prevent successful installation. If your computer is infected and you are not able to start your Windows operating system, you can use Norton Bootable Recovery Tool to remove threats and recover your computer.

Norton Bootable Recovery Tool is available on the product CD that you purchased. You can use the product CD as a recovery media.

If you have purchased this product as a download, go to the following URL to download the Norton Bootable Recovery Tool Wizard:

http://www.norton.com/recoverytool_n360

Norton Bootable Recovery Tool automatically downloads the latest virus definitions from Symantec servers and uses these virus definitions to secure your computer from all types of viruses and latest security threats. If Dynamic Host Configuration Protocol (DHCP) is enabled, virus definitions are automatically updated when your computer is connected to the Internet. Therefore, you

must use an Ethernet connection to update the virus definitions in Norton Bootable Recovery Tool. You cannot update the Norton Bootable Recovery Tool virus definitions by using a wireless network connection.

If the virus definitions are out of date, Norton Bootable Recovery Tool may not detect and remove all the latest security threats from your computer.

To use the Norton Bootable Recovery Tool

1. Insert the Norton Bootable Recovery Tool recovery media.
2. Turn on or restart your computer and enter to the BIOS mode.
   You can enter the BIOS mode by pressing the key that appears on the screen immediately after your computer restarts.
3. Select the recovery media on which you have created the 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 can be the Norton Bootable Recovery Tool DVD or USB drive.
4. Read the **Norton License Agreement**, and then click **I Agree**.
5. In the **Norton Bootable Recovery Tool** window, click **Norton Advanced Recovery Scan**.
6. In the **Scan** section, click **Start Scan**.
   When the scan is complete, the scan results window lists the following:
   - The total number of files scanned
   - The total number of threats detected
   - The total number of resolved threats
   - The total number of unresolved threats
   - The details of each detected threat

7 In the scan results window, do one of the following:
   - To fix all of the threats that are found on your computer, select **Set all action to Fix**.
   - To perform appropriate actions for each of the threats, select **Fix** or **Ignore**.
8 Click **Continue**.
9 If a confirmation dialog box appears, click **OK**.
10 In the **Scan Summary** window, review the scan summary and do one of the following:
   - Click **Done**.
   - To run another scan, click **Scan Again**.

Updating virus definitions on a USB drive

Symantec virus definitions are used in Norton Bootable Recovery Tool to scan your computer for the latest security risks. When you create Norton Bootable Recovery Tool on a USB drive, the latest virus definitions are automatically downloaded and included in the USB drive. You can update the virus definitions in Norton Bootable Recovery Tool on a USB drive that you created earlier.

To update Norton Bootable Recovery Tool virus definitions on a USB drive

1 Insert your Norton Bootable Recovery Tool USB drive into the USB port of your computer.
2 In the **Norton Bootable Recovery Tool Wizard** main window, click **Update USB key definitions**.
3 In the **Update USB key definitions** window, from the **Specify drive** drop-down list, select the **USB drive**.
4 Click **Next**.
5 Review the results and click **Done**.

Starting Norton Security from the command prompt

If you work from the command line (for example, writing a script or code), you can start Norton Security while you are still in DOS.

To start Norton Security from the command prompt

1 At the command-line prompt, type the directory where Norton Security is located, and the executable.

- In 32-bit version of Windows, Norton Security and the executable are located at the following path:

  \Program Files\Norton Security\Engine*version*\Uistub.exe

  Where *version* represents the version number of installed Norton Security.
- In 64-bit version of Windows, Norton Security and the executable are located at the following path:

  \Program Files (x86)\Norton Security\Engine64*version*\Uistub.exe

  Where *version* represents the version number of installed Norton Security.

2 Press **Enter**.

Responding to security status indicators

Your Norton product displays the security status of your computer under the **Security** section of the main window. Based on the security status of your computer, your Norton product shows your system status as **Protected**, **Attention**, or **At Risk**.

The system status indicator displays one of the following statuses:

Protected	Indicates that your computer is protected from threats, risks, and damages.

Attention	Indicates that your computer requires attention. At the bottom section of the Norton product main window, click **Fix Now** to resolve the security threats on your computer.
At Risk	Indicates that your computer is at risk. At the bottom section of the Norton product main window, click **Fix Now** to resolve the security threats on your computer.

Your Norton product displays individual security status for each protection category, such as Security, Identity, and Performance. Based on the security status of the different components of your computer, the status areas of the three protection categories are marked as **Protected**, **Attention**, or **At Risk**.

When your system status or protection categories statuses are marked as **At Risk** or **Attention**, at the bottom section of the Norton product main window, click **Fix Now** to resolve all the security threats on your computer.

When your system status or protection categories statuses are marked as **At Risk** or **Attention**, you can resolve the security issues directly from the main window.

To respond to security status indicators

1 In the Norton Security main window, click **Fix Now**.

2 Follow the on-screen instructions.

About the Norton product icon

When you install the Norton product, it places an icon in the notification area at the far right of the taskbar. This icon indicates the current security status of your computer. The Norton product displays an animated icon when it actively fixes any issues or wants to inform you about any warning or urgent issues.

You can see the following representations of the Norton product icon in the notification area:

Icon with a green check mark badge	Represents that your computer is fully protected.
Icon with an orange exclamation mark badge	Represents that there are some issues against your computer protection that require your attention.
Icon with a red cross mark badge	Represents that there are some urgent issues against your computer protection that require immediate resolution.
Icon with gray outer circle	Represents that the Silent Mode feature is turned on. This icon also displays the current protection status badge.

You can right-click the icon to see a shortcut menu for the Norton product. You can choose items on the shortcut menu to open the main window, to fix any issues that the Norton product detects, or to get additional help.

About the Norton product shortcut menu

The Norton product works in the background to keep your PC secure. The Norton product icon is available in

the notification area at the far right of the taskbar. The icon reassures you that your protection is up to date. It changes its color if any change in status occurs.

The messages that appear in the notification area may require a response from you, such as opening a window. More often, messages inform you about current activities, and they disappear after a few seconds.

You can right-click the **Norton Security** icon to access specific activities. Depending on the current activities, your options include the following:

Open Norton Security	Use this option to launch the Norton product main window to complete tasks, view current status, or access other features.
Run QuickScan	Use this option to run a Quick Scan to protect possible virus-infected areas of your computer.
Run LiveUpdate	Use this option to run LiveUpdate to check for definition updates and program updates.
View Recent History	Use this option to review the information about the security events for all of the categories.
Get Support	Use this option to resolve your problem easily using Norton Autofix.
Turn on/Turn off Silent Mode	Use this option to turn on or turn off Silent Mode.

Enable/Disable Smart Firewall	Use this option to turn on or turn off the firewall.
Enable/Disable Antivirus Auto-Protect	Use this option to turn on or turn off Antivirus Auto-Protect.

About Norton LiveUpdate

Symantec products download the latest protection updates regularly from Symantec servers. The protection updates safeguard your computer from the latest viruses and unknown security threats. Using the LiveUpdate technology, Symantec products help you to obtain and install these updates.

When LiveUpdate runs, it checks if your installed Norton product is up-to-date with the protection updates. If the product does not have the latest updates, LiveUpdate downloads the necessary protection updates for your device, processes the updates, and then deletes the older files and definitions from the temporary folder.

LiveUpdate takes little time to download and process the protection updates. However, you can cancel the LiveUpdate session at any time.

Your device should be connected to the Internet to obtain these updates. If your network uses proxy servers to connect to Internet, LiveUpdate uses the proxy settings in your product to download the latest updates. You can use the **Network Proxy Settings** option in the **Administrative Settings** window to configure the proxy settings of your network.

A connectivity problem can occur if you use parental control software. If you suspect that parental controls might block the connection, you can configure the parental controls so that they do not block the activation procedure. You need to log on to your parental control

software or to the Internet through your ISP as an administrator to change your configuration.

LiveUpdate cannot work if the **Network Cost Awareness** option in the **Firewall** window under **Settings** is set to **No Traffic** or **Economy**. Network Cost Awareness lets you define the amount of network bandwidth that Norton Security can use. Therefore, you must ensure that the **Network Cost Awareness** option is turned on and set to **No Limit** for LiveUpdate to run.

The **Network Cost Awareness** window appears when you run LiveUpdate and the policy is set to **No Traffic** or **Economy**. However, you can override the policy and complete the LiveUpdate task.

About protection updates

Protection updates are the files that keep your Norton product up-to-date with the latest antithreat technology. New viruses or threats can appear daily, so keeping the Norton product up-to-date helps defend latest threats against your device. Your Norton product uses LiveUpdate technology to obtain the protection updates for your device by contacting the Symantec server. LiveUpdate automates the process of downloading and installing the protection updates. For more information, See "About Norton LiveUpdate" on page 35.

To stay secure, Symantec recommends that you have the most recent version of your licensed Norton product and have the most up-to-date protection content. For more information, See "About upgrading your product" on page 331.

To obtain protection updates, your subscription to Norton Security should be active. If your subscription expires, your product cannot obtain any of the protection updates.

Protection updates include program and definition updates. Program updates are minor improvements to your installed Norton product. These differ from product upgrades, which are newer versions of the entire product. Program updates are usually created to extend

the operating system or hardware compatibility, adjust a performance issue, or fix program errors. Program updates are released on an as-needed basis.

Some protection updates may require that you restart your computer to complete the update process.

Definition updates are the files that keep you protected against viruses and emerging threats. The definition updates include the following:

- Virus definitions – Identifies the viruses that attack your device.
- Predefined firewall rules – Controls network traffic and network access for programs on your device.
- Intrusion prevention signatures – Identifies unauthorized access attempts to your device.
- Symantec spam definition files – Identifies the spam nature of emails that you receive.

Turning off or turning on Automatic LiveUpdate

You can have LiveUpdate check for protection updates automatically by turning on the **Automatic LiveUpdate** option. So, your Norton product is up-to-date on its own. If you turn off this option, you must run LiveUpdate manually at regular intervals to obtain the protection updates.

You can:

- Configure Automatic LiveUpdate from Quick Controls
- Configure Automatic LiveUpdate from Settings

If you are connected to the Internet, Automatic LiveUpdate downloads product updates and definition updates every hour. If you have an Integrated Services Digital Network (ISDN) router that is set to automatically connect to your Internet service provider (ISP), it may incur charges each time. If you do not want this setup, you can turn off the automatic connection on your ISDN router, or turn off the **Automatic LiveUpdate** option. You can also define the amount of bandwidth that Norton Security can use by using the **Network Cost Awareness** option.

Configure Automatic LiveUpdate from Quick Controls

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, do one of the following:
   - To turn off Automatic LiveUpdate, uncheck **Automatic LiveUpdate**, in the **Select the duration** drop-down list, select how long you want to turn off Automatic LiveUpdate, and then click **OK**.
   - To turn on Automatic LiveUpdate, check **Automatic LiveUpdate**.

Configure Automatic LiveUpdate from Settings

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. On the **Antispyware and Updates** tab, under **Updates**, in the **Automatic LiveUpdate** row, do one of the following:
   - To turn off Automatic LiveUpdate, move the **On/Off** switch to the right to the Off position.

     In the **Select the duration** drop-down list, select how long you want to turn off Automatic LiveUpdate, and then click **OK**.
   - To turn on Automatic LiveUpdate, move the **On/Off** switch to the left to the On position.

How to run Norton LiveUpdate manually

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

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

To run LiveUpdate manually

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

Checking for the latest protection updates date

Protection updates contain the information that allows your Norton product to recognize and alert you to the presence of a specific virus or security threat. It also can upgrade your product to include a new feature and can improve your product's performance. Norton Security shows the date on which you last updated the protection updates.

To check for the latest protection update date

1. In the Norton Security main window, click **Security**.
2. Under the security status indicator, check the date next to **Protection Updates**.
3. If the date is older than a day or two, run LiveUpdate immediately.

Turning on or turning off Apply updates only on reboot

Certain of the protection updates that are downloaded during a LiveUpdate session require system restart for the updates to work. On Windows 7 or later, all the downloaded updates can be applied instantly without a system restart. However, the **Apply updates only on**

reboot option lets you choose how these updates need to be applied.

This option is available only on Windows 7 or later.

If you turn off this option, the downloaded updates can be applied instantly without a system restart. By default, this option is turned off. You see the following options on the **Norton LiveUpdate** window:

- **Apply Now**

  If you choose this option, the downloaded updates are applied instantly without a system restart.
- **Apply Later**

  If you choose this option, the downloaded updates are applied the next time you restart your computer.

If this option is turned on, the downloaded updates are applied only after a system restart. You see the following options on the **Norton LiveUpdate** window:

- **Restart Now**

  If you choose this option, your computer restarts after the updates are applied.
- **Restart Later**

  If you choose this option, the downloaded updates are applied the next time you restart your computer.

To turn on or turn off Apply updates only on reboot

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click the **Antispyware and Updates** tab.
4. In the **Apply updates only on reboot** row, do one of the following:
   - To turn off **Apply updates only on reboot**, move the **On/Off** switch to the right to the **Off** position.
   - To turn on **Apply updates only on reboot**, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.

6 Click **Close**.

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 Security 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**.

Monitoring your system's performance

2

This chapter includes the following topics:

- About System Insight
- 30-Day Report

About System Insight

Your Norton product continuously monitors your computer to keep it free of any problems and run at peak efficiency. The Norton product constantly scans the vital areas of your computer including memory, registry keys, and running processes. It monitors the important activities such as general file operation, network traffic, and Internet browsing. In addition, your Norton product ensures that the activities that it performs on your computer do not degrade the overall performance of your computer.

System Insight provides you a centralized location where you can view and monitor the activities that you perform on your system. System Insight displays such information in the **Graphs** window.

You can use the **Graphs** window for the following:

- To view monthly history of the important system activities that you performed or that occurred over a period of the last three months.

  The Events graph that appears at the top of the window provides a pictorial representation of important system activities. The activities include

application installations, application downloads, disk optimizations, threat detections, performance alerts, and Quick Scans.

The graph displays the activities as icon or stripe, and the description for each icon or stripe is provided 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 **View Details** link in the pop-up lets you view additional details about the activity in the **Security History** window. You can use the tabs at the top of the graph to obtain details for the current month and details for the last two months.

- To rearrange the organization of files on your computer.

  Optimizing your system helps you maximize the usable free space on a disk by grouping files based on how they are accessed. The **Optimize** option at the top of the Events graph lets you defragment your system.

- To view and analyze the effect of the Norton product on the performance of your computer.

  The CPU usage chart that appears at the left of the window provides a graphical representation of your CPU usage. The graph displays the percentage of the overall system CPU usage and Norton-specific CPU usage.

You can use the **Performance Monitoring** option to monitor the performance of your computer. To access the **Performance Monitoring** option, go to the Norton product main window, click **Settings > Administrative Settings > Performance Monitoring**.

Accessing the Graphs window

System Insight provides you a centralized location where you can view and monitor your system activities. System Insight displays such information in the **Graphs** window. You can access the **Graphs** window to view details

about the important system activities and CPU usage. You can also defragment your boot volume.

To access the Graphs window

- In the Norton Security main window, double-click **Performance**, and then click **Graphs**.

About monitoring system activities

System Insight provides information about the important system activities that you performed or that occurred over a period of the last three months. You can use the tabs at the top of the graph to obtain details for the current month and for the last two months. System Insight displays the information in the **Graphs** window. The **Graphs** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. You can use the tabs at the top of the graph to obtain details for the current month and for the last two months. The activities include:

Installs	Provides the details about the installation activities that you performed on your system over a period of the last three months. The details include the application that you installed, the date on which you installed the application, and the total number of installations on that date.

Downloads	Provides the details about the application-download activities that you performed on your system over a period of the last three months. The details include the date on which you downloaded a file and the total number of downloads on that date. You can click the file name link to view additional details about the downloaded file such as the Download Insight report, file name, reputation level, and recommended action.
Optimized	Indicates the optimization activities that you performed on your system over a period of the last three months.
Detections	Provides the details about the threat detection activities that the Norton product performed on your system over a period of the last three months. The details include the date on which your Norton product detected a threat and the total number of threats that your Norton product detected on that date. The **View Details** link provides additional details about the risk such as the risk impact and the origin of the risk. The details also include the action that a threat has performed on your system and the action that Symantec recommends you to resolve the threat.

Alerts	Provides the details about the performance alerts that your Norton product displayed over a period of the last three months. The details include the monitored date and the number of performance alerts generated. The **View Details** link provides additional details about performance-related activities, program name, program location, and system resources utilization.
Quick Scans	Provides the details about Quick Scans that your Norton product performed on your system over a period of the last three months. The details include the date on which a Quick Scan was performed and the number of Quick Scans that were performed on that date. The **View Details** link provides additional details such as the scan time, total items scanned, total risks detected, total risks resolved, and recommended action.

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 Security 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.

About performance alerting

Your Norton product monitors your system performance. If it detects an increased usage of system resources by any program or process, it notifies you with performance alerts. Performance alerting works only when the **Performance Monitoring** option and **Performance Alerting** option are turned on.

Performance alerting notifies you with information about the program name and resources that the program uses excessively. The **Details & Settings** link in the performance notification alert lets you view additional details about the resource consumption by the program. The **File Insight** window opens and displays the reputation details of the file, the origin of the file, the

process ID, and the complete resource usage list of the program. From the **File Insight** window, you can choose to exclude the program from being monitored. You can use the **Settings** option in the **File Insight** window to turn off the **Performance Alerting** option.

Performance alerts are not displayed when your computer is idle or in Silent Mode.

For each system resource, such as CPU, memory, and hard disk, there is a resource consumption threshold defined. When the resource consumption of a program exceeds the defined threshold limit, your Norton product alerts you with a performance alert.

You can use the **Resource Threshold Profile for Alerting** option to configure the threshold limit. To access the **Resource Threshold Profile for Alerting** option, go to the Norton product main window, and then click **Settings > Administrative Settings > Performance Monitoring > Resource Threshold Profile for Alerting**.

You can use the **Use Low Resource Profile On Battery Power** option to let your Norton product automatically change the resource threshold profile to low when your computer runs on battery power.

You can use **High-Usage Alert for** option to configure your Norton product to alert for high usage of CPU, memory, disk, and handles.

In addition, you can add programs to the **Program Exclusions** list using the **Program Exclusions** option. When you add a program to the **Program Exclusions** list, your Norton product does not alert you when the program exceeds the defined resource consumption threshold limit.

You can view all the performance-related logs under the **Performance Alert** category in the **Security History** window.

Configuring performance alerts

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

You can use the following options to configure performance alerts:

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.

To configure performance alerts

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Performance Alerting** row, do one of the following:
   - To turn off performance alerts, move the **Performance Alerting** switch to the **Off** position.
   - To turn on performance alerts, move the **Performance Alerting** switch to the **On** position.
   - To suppress the performance alerts, move the **Performance Alerting** switch to the **Log Only** position.

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 the left to the **On** position.
- If you want your Norton product to monitor the memory usage, move the **Memory** switch to the left to the **On** position.
- If you want your Norton product to monitor the disk usage, move the **Disk** switch to the left to the **On** position.
- If you want your Norton product to monitor the handle count, move the **Handles** switch to the left to the **On** position. By default, this option is turned off.

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

Configuring the resource threshold profile

The threshold limit for the system resources determines at which point your Norton product should notify you with performance alerts. When a specific program exceeds the threshold limit of using your system resources, your Norton product notifies you with a performance alert.

To configure the resource threshold profile

1 In the Norton Security main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.

3 Under **Performance Monitoring**, in the **Resource Threshold Profile for Alerting** row, select one of the following options:

Low	Configures a low threshold limit for alerting. Symantec recommends you to select this option when your computer runs on battery power.
Medium	Configures a medium threshold limit for alerting. By default, the threshold limit is set to medium.
High	Configures a high threshold limit for alerting. Symantec recommends you to select this option when your computer runs tasks that require high resource.

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

Turning off or turning on the Use Low Resource Profile On Battery Power option

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 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.

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

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

1. In the Norton Security 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 the right to the **Off** position.
4. Click **Apply**, and then click **Close**.

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

1. In the Norton Security 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 the left to the **On** position.
4. Click **Apply**, and then click **Close**.

Excluding programs from performance alerts

Your Norton product lets you exclude programs from performance alerts. You can add the programs that consume high CPU, memory, or disk usage to the **Program Exclusions** list. When you add a program to the **Program Exclusions** list, your Norton product does not alert you when the program exceeds the resource consumption threshold limit.

To exclude a program from performance alerts

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
4. In the **Program Exclusions** window, click **Add**.
5. In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
6. Click **Open**.
7. In the **Program Exclusions** window, click **Apply**.
8. Click **OK**.
9. In the **Settings** window, click **Close**.

Removing programs from Program Exclusions

The **Program Exclusions** window lists all the programs that are excluded from performance alerts. If you want, you can remove any of the programs that you already added to the **Program Exclusions** window. When you remove a program, the program appears in the performance alert the next time it crosses the defined threshold limit for resource consumption.

To remove a program from Program Exclusions

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
4. In the **Program Exclusions** window, select the program that you want to delete, and then click **Remove**.
   To remove all the programs available in the **Program Exclusions** window, click **Remove All**.
5. In the **Program Exclusions** window, click **Apply**.
6. Click **OK**.
7. In the **Settings** window, click **Close**.

About the CPU usage meter

Your Norton product monitors the overall system CPU usage and the Norton-specific CPU usage. Your Norton product displays the CPU usage meter in the **Graphs** window. The CPU usage meter is a real-time graph of CPU utilization.

The graph displays a performance time for the last 90 minutes or for the duration since you started your computer. The blue pattern in the graph depicts the overall system usage, and the yellow pattern depicts the Norton-specific usage. The gray blocks that are labeled as **Idle** indicate the idle period of your computer. The gray blocks include the period when your computer is in shutdown, sleep, or log out state.

Viewing the CPU graph and memory graph

Your Norton product monitors the overall system CPU usage and memory usage and the Norton-specific CPU usage and memory usage. The graph on the left of the **Graphs** window displays the CPU usage meter.

To view the CPU graph and memory graph

1. In the Norton Security main window, double-click **Performance**, and then click **Graphs**.
2. In the **Graphs** window, on the left pane, click **Usage**.
3. Do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
   - To magnify or shrink the graph, click **10m**, **30m**, **1D**, **1W**, or **1M** next to the **Zoom** option.

Obtaining historical data of your CPU and memory usage

The **Zoom** options also provide you the historical data of the CPU graph and memory graph. For example, if you select the **1D** option, Norton Security displays the data of CPU graph or memory graph for the last one day.

To view historical data of your CPU or memory usage

1. In the Norton Security main window, double-click **Performance**, and then click **Graphs**.
2. In the **Graphs** window, on the left pane, click **Usage**.
3. Do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
4. Do one of the following:
   - To obtain historical data for the last one day, click **1D**.
   - To obtain historical data for the last one week, click **1W**.
   - To obtain historical data for the last one month, click **1M**.

Identifying resource-consuming processes

You can click at any point on the CPU graph or memory graph to obtain a list of top three processes that consume maximum resources of your computer at that point. You can click a process that is available in the list to get more information about the process in the **File Insight** window.

To identify resource-consuming processes

1. In the Norton Security main window, double-click **Performance**, and then click **Graphs**.
2. In the **Graphs** window, on the left pane, click **Usage**.
3. Do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
4. Click at any point on the graph to obtain a list of resource-consuming processes.
5. Click the name of a process to obtain additional information about the process in the **File Insight** window.

About optimization

The data storage space on a disk is divided into discrete units. These units are called clusters. When files are written to the disk, they are broken up into cluster-sized pieces. When all of the file pieces are located in adjacent or contiguous clusters, the file can be accessed quickly.

Your computer's hard disk stores all of your files, applications, and the Windows operating system. The bits of information that make up your files gradually spread over the disk. This process is known as fragmentation. The more that you use your computer, the more fragmented the hard disk gets.

When a fragmented file is accessed, the disk performance is slower. The performance is slower because the drive head locates, loads, saves, and keeps track of all of the fragments of the file. If free space is also fragmented, the drive head might have to track adequate free space to store temporary files or newly added files.

Optimization rearranges file fragments into adjacent or contiguous clusters. When the drive head accesses all of the file data in one location, the file is read into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. Optimization consolidates free space to avoid fragmenting newly added files. It adds extra space after major data structures so that they can grow without immediately becoming fragmented again.

You can optimize your boot volume manually by using the **Optimize** option in the **Graphs** window.

You can also configure your Norton product to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Your Norton product automatically schedules the optimization when it detects the installation of an application on your computer. The optimization process starts next time when your computer is idle.

You can use the **Idle Time Optimizer** option in the **Administrative Settings** window to optimize the boot volume during idle time.

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 Security 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 Security 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**.

About the Idle Time Optimizer

Idle Time Optimizer lets you configure your Norton product to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Your Norton product automatically schedules the optimization when it detects the installation of an application on your computer and your computer is idle. If you start using your computer again, your Norton product stops the optimization task, and starts optimizing the next time that your computer is idle. This way, the background job of optimization does not affect the performance of your computer.

Optimization rearranges file fragments into adjacent or contiguous clusters in the hard disk. It improves the computer performance by reading the files into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. In addition, it consolidates free space to avoid fragmenting newly added files.

You must turn on the **Idle Time Optimizer** option under **Administrative Settings** in the **Settings** window to optimize the boot volume during idle time. By default, this option is turned on.

Turning off or turning on Idle Time Optimizer

Your Norton product automatically schedules the optimization when it detects the installation of a new application on your computer. Your Norton product runs this optimization only when your computer is idle.

You can use the **Idle Time Optimizer** option to optimize the boot volume during idle time. By default, this option is turned on.

To turn off Idle Time Optimizer

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Optimizer** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**, and then click **Close**.

To turn on Idle Time Optimizer

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Optimizer** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

Monitoring background jobs of your Norton product

The **Background Tasks** window provides the details of the background tasks that your Norton product performs and lets you view and monitor the background tasks. Your Norton product runs most of the background tasks when your computer is idle. Performing all background tasks when your computer is idle helps your computer to run at peak efficiency when you use your computer. However, you can manually start or stop a task at any time. You can also specify the **Idle Time Out** duration. After the **Idle Time Out** duration is reached, your Norton product identifies the computer as idle and runs the background tasks.

To monitor background jobs

1. In the Norton Security 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, view the details of background jobs.

5 Do one of the following:
- To run a background job, click the play icon that appears before the name of the background job.
- To stop a running background job, click the stop icon that appears before the name of the background job.

6 Click **Close**.

Configuring the power source

You can choose the power source for your Norton product to perform the background tasks. Background tasks are Norton-specific tasks that your Norton product performs when your computer is idle.

Background tasks include Quick Scan, Automatic LiveUpdate, Norton Community Watch, Norton Insight, Full System Scan, and Insight Optimizer. Your Norton product consumes more power when it runs the background tasks. By default, your Norton product performs these tasks only when your computer is connected to external power. If your computer is running on battery power, your Norton product does not perform the background tasks. It helps extend the battery power of your computer.

However, you can choose the power source to perform the background tasks. You can configure the power source for each of the background tasks.

To configure the power source

1 In the Norton Security 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 **Power Source** column, click the **Configure** link for the background task that you want to configure the power source.

5 In the **Power Source** window, select one of the following:

- **External**

  Allows the background task to run only when your computer uses external power.

- **External and Battery**

  Allows the background task to run when the computer uses either external power or battery power.

  If you choose this option, Norton Security performs the background task when the computer is idle. It does not consider the type of power source the computer uses.

6 Click **OK**.

7 In the **Background Tasks** window, click **Close**.

About Norton Insight

Norton Insight allows the smart scanning of files on your computer. It improves the performance of your Norton product scans by letting you scan fewer files without compromising the security of your computer.

A Norton scan can identify threats on your computer in the following ways:

The Blacklist technique	At regular intervals, your Norton product obtains definition updates from Symantec. These updates contain signatures of known threats. Each time when the Norton product obtains the definition updates, it performs a scan of all of the files that are available on your computer. It compares the signature of the files against the known threat signatures to identify threats on your computer.

The Whitelist technique	The Norton product obtains specific information about the Files of Interest and submits the information to Symantec during idle time. The information includes things such as file name, file size, and hash key. Symantec analyzes the information of each File of Interest and its unique hash value and provides a confidence level to the file. The Symantec server stores the hash value and confidence level details of the Files of Interest. The server provides the details immediately after you open the **Norton Insight** window. Even the slightest modification of the file causes a change in the hash value and the confidence level of the file. Typically, most Files of Interest belong to the operating system or known applications, and they never change. These files do not require repeated scanning or monitoring. For example, Excel.exe is a file that never changes but you always scan it during a normal security scan.

Symantec assigns the following confidence levels to Files of Interest:

Trusted	Symantec analyzes the file as trusted based on the statistical evaluation that is done on the files that are available within the Norton Community. If the file has three green bars, Symantec rates the file as **Norton Trusted**. The files that have three green bars display a Norton Trusted pop-up text when you move the mouse pointer over the green bars.
Good	Symantec analyzes the file as good based on the statistical evaluation that is done on the files that are available within the Norton Community. Symantec rates the trusted files as follows: ■ If the file has two green bars, Symantec rates the file as **Good**. ■ If the file has one green bar, Symantec rates the file as **Favorable**.
Unproven	Symantec does not have enough information about the file to assign a trust level to the file.
Poor	Symantec has only a few indications that the file is not trusted.

The Whitelist technique that Norton Insight uses also helps in heuristic detection of suspicious applications. Normally, the execution behavior of well-known applications appears identical to the execution behavior of unknown applications. Such behavior results in false identification of good applications as suspicious, and therefore, necessitates security applications to maintain a low heuristic detection threshold. However, keeping a low detection threshold does not provide a complete heuristic protection against malicious applications. The Norton product uses the Whitelist technique that helps maintain a high heuristic detection threshold. It excludes well-known applications from heuristic detection to prevent false detection of well-known applications and to ensure a high detection rate of malicious applications.

Viewing the files using Norton Insight

Norton Insight provides reputation information about the Files of Interest that are available on your computer. Your Norton product lets you view specific categories of files based on the option that you select in the **Norton Insight** window.

The drop-down list that is available in the **Norton Insight** window provides you the following options:

All Running Processes	Lists the processes that run on your computer.
All Files	Lists the Files of Interest.
Startup Items	Lists the programs that run when you start your computer.
All Loaded Modules	Lists all the files and programs that are currently loaded on to the program memory space.

Highest Performance Impact	Lists the programs that consume maximum resources of your computer. Your Norton product displays a list of top 10 resources that highly affect the performance of your computer.
Highest Community Usage	Lists the files that have the maximum community usage.
User Trusted Files	Lists the Files of Interest that you manually trusted in the **File Insight** window. This category does not list the files that do not belong to the File of Interest even if you manually trust the files. You can also remove the user trust from all of the Files of Interest that you manually trusted. You can use the **Clear All User Trust** option next to the drop-down list to remove the user trust.
Untrusted Files	Lists the files that are not Norton Trusted. You can manually trust all the files that are not trusted by clicking the **Trust All Files** option next to the drop-down list.

You can view file details such as file name, trust level, community usage, and resource usage. There may be instances when the trust level of a file has changed or a process running might have stopped running. You can refresh the **Norton Insight** window to update the file list

and file details. The coverage meter provides a graphical representation of the percentage of the Norton Trusted Files and the total Files of Interest. The higher the percentage, the lesser time the scan takes.

To view the files using Norton Insight

1. In the Norton Security main window, double-click **Security**, and then click **Run Scans**.
2. In the **Scans** window, select **Norton Insight**, and then click **Go**.
3. In the **Norton Insight** window, select an option from the **Show** drop-down list to view a category of files. You may need to scroll down to view all the files that are listed in the details area.
4. Click **Close**.

To refresh the list of files

- In the **Norton Insight** window, at the top of the file icon, click the refresh icon.

Checking the trust level of a file

Norton Insight lets you check the reputation details of the Files of Interest that are available on your computer. You can view details such as signature of the file and the date on which the file was installed. You can also view details such as the trust level, community usage, resource usage, and the source of the file. You can use the **Locate** option to find the location of the file on your computer. When you right-click a file that is available on your computer, the shortcut menu displays **Norton Security** option and then **Norton File Insight** option. You can use the options to check the details of a File of Interest.

Your Norton product displays the **Norton 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.

The Symantec server stores the hash value and trust level details of the File of Interest. The server provides the file details immediately after you open the **Norton Insight** window. However, you can use the **Check Trust Now** option in the **File Insight** window to update the trust value of a file. You can also manually trust any well-known files. You can change the trust level of any file to **User Trusted** other than the files that are Norton Trusted.

You can determine the resource usage of a file that is available on your computer. The **File Insight** window displays the CPU graph and the system resource usage details for the running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage by the process.

To check the trust level of a file

1. In the Norton Security main window, double-click **Security**, and then click **Run Scans**.
2. In the **Scans** window, select **Norton Insight**, and then click **Go**.
3. In the **Norton Insight** window, click a file for which you want to check the details.
4. In the **File Insight** window, view the details of the file.
5. Click **Close**.

To check the trust level of a specific file

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

To find the location of the file

❖ In the **File Insight** window, click **Locate**.

To refresh the trust level of the file

❖ In the **File Insight** window, in the **Details** tab, click **Check Trust Now**.

To manually trust the file

❖ In the **File Insight** window, in the **Details** tab, click **Trust Now**.
You can manually trust the files that are poor, unproven, or not Norton trusted.

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.
- Select **Run Key change** to include registry changes.

30-Day Report

The **30-Day Report** is a summary of all the activities that your Norton product has performed to protect you in the last 30 days. The **30-Day Report** is automatically displayed every 30 days after you install your Norton product.

The Norton product performs various activities to protect you from viruses, infected downloads, identity theft, and other online threats. The Norton product also runs

various background tasks to clear unwanted files and tune up your computer.

Some of the activities that the Norton product performs are:

- Scanning your files
- Running an Automatic LiveUpdate
- Analyzing your downloads
- Blocking intrusions
- Securing your network
- Fixing infected files
- Saving your logins to different websites using the Identity Safe feature
- Maintaining the trust level of files in your computer
- Clearing up the unnecessary files and tuning up your computer

The **30-Day Report** window displays the following:

- Top four activities that your Norton product has done for you in the last 30 days
- LiveUpdate status

The **Details** option in the **30-Day Report** window lets you view the complete list of activities that your Norton product has performed.

Can I stop the Norton product from displaying the 30-Day Report?

Yes, if you do not want your Norton product to automatically display the **30-Day Report** every 30 days, you can turn off the **30-Day Report** option in the **Administrative Settings** window.

To turn off the 30-Day Report

1. In the Norton Security 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 the right to the **Off** position.

How do I manually view the 30-Day Report?

The **30-Day Report** is automatically displayed every 30 days after you install your Norton product. However, you can also manually view the report using the **30-Day Report** option in the Norton Security main window. The **30-Day Report** option is available only when the Norton product has performed any activity on your computer.

Protecting your files and data

3

This chapter includes the following topics:

- About maintaining protection
- About the Norton Security scans

About maintaining protection

After you have installed your Norton product and run LiveUpdate, you have complete protection from viruses and other security risks. However, new security risks are a constant threat. Security risks can spread when you start your computer from an infected disk or when you run an infected program. You can do several things to avoid security risks.

Practicing regular file maintenance and keeping your security protection up to date helps in protecting your computer.

To avoid security risks:

- Stay informed about the latest viruses and other security risks by logging in to the Symantec Security Response website at the following URL:

  http://securityresponse.symantec.com

  The website includes extensive, frequently updated information on viruses and automatic virus protection.
- Keep **Automatic LiveUpdate** turned on at all times to continually receive definition updates.

- Run LiveUpdate regularly to receive new program updates.
- Keep **Auto-Protect** turned on at all times to prevent viruses from infecting your computer.
- Watch for email messages from unknown senders. Do not open attachments from these senders.
- Keep **Email Protection** turned on to avoid sending or receiving infected email attachments.
- Keep all recommended maximum protection settings turned on.
- Keep the default options turned on at all times.

You should be always prepared in case a virus infects your computer.

About the Norton Security scans

Your Norton product scans secure your computer from all types of viruses and unknown threats using the latest virus definitions. It also scans all the Internet activities that are performed on your computer to protect your computer from the Internet-based threats that exploit software vulnerabilities.

Your Norton product automatically performs different types of scans to secure your computer from latest threats. It also lets you run different types of scans manually to secure your computer.

By using the Norton product, you can run the following types of scans:

Scans and Tasks	The Norton product scan uses the latest virus definitions that are available locally in the computer. If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer. The three types of scans that are available under **Scans and Tasks** are **Quick Scan**, **Full System Scan**, and **Custom Scan**. You can also improve your computer's performance by running **Custom Tasks**.
Norton Power Eraser	Norton Power Eraser is a powerful malware removal tool that can help you clean up the security risks that are difficult to remove. Norton Power Eraser uses aggressive techniques than normal scan process; sometimes there is a risk that Norton Power Eraser flags a legitimate program for removal. Review scan results carefully before removing any files using Norton Power Eraser.

Scan Facebook Wall	**Scan Facebook Wall** lets you scan the links and URLs that are available on your Facebook profile. When you run the **Scan Facebook Wall** option, the Norton product takes you to the Facebook login webpage. After you log in to your Facebook profile, Norton Safe Web prompts for your permission to access your Facebook profile information. After you have allowed Norton Safe Web to access your Facebook profile information, Norton Safe Web scans your Facebook newsfeed.
Norton Insight	**Norton Insight** allows the smart scanning of files on your computer. It improves the performance of your Norton product by letting you scan fewer files without compromising on the security of your computer. When you run **Norton Insight**, your Norton product takes you to the Norton Insight window where you can view the trust level of all running processes, files, and startup items.

Diagnostic Report	**Diagnostic Report** gathers information about your computer including the operating system, installed programs, and hardware. If you think that your computer has any software- or hardware-related problems, you can use this report to troubleshoot them.

Your Norton product keeps your computer secure from latest threats by automatically running Full System Scan when your computer is in the idle state.

Accessing Norton Security scans

You can use Norton Security scans to secure your computer from all types of viruses and unknown threats.

You can access Quick Scan from the Norton product icon on the taskbar.

You can also scan any particular folder using the On-Demand Scan feature. The On-Demand Scan is available when you right-click the file or folder that you want to scan.

To access the scan from the Norton product main window

1. In the Norton Security main window, double-click **Security**, and then click **Run Scans**.
2. In the window that appears, do one of the following:
   - In the **Scans and Tasks** pane, select the scan that you want to run.
   - Run **Norton Power Eraser** to scan your computer using Norton Power Eraser.
   - Run **Scan Facebook Wall** to scan the links that are available on your Facebook wall.

To access the scan from the notification area

- In the notification area on the taskbar, right-click the **Norton Security** icon, and then click **Run Quick Scan**.

To scan a particular file or folder

- Right-click the file or folder, select **Norton Security**, and then click **Scan Now**.

About Computer Scan

Your Norton product automatically downloads latest virus definition regularly and secures your computer from all types of viruses and unknown threats. When the Norton product performs a Computer Scan, it uses the latest virus definitions that Symantec provides.

The threat detections that are based on the local definition are specified with a specific name. For example, if a Trojan horse is detected, the scan results of the Computer Scan displays the threat as Trojan.Foo. You can click the **Run Scans** option available in the **Security** tab to access the different types of computer scans.

If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer.

You can run the following types of computer scans:

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. **Quick Scan** takes less time to scan than a Full System Scan because this scan does not scan your entire computer.

Full System Scan	Scans your computer for all types of viruses and security threats. **Full System Scan** performs a deep scan of your computer to remove viruses and other security threats. It checks all boot records, files, and running processes to which the user has access. Consequently, when you run a Full System Scan with administrator privileges, it scans more files than when you run it without administrator privileges.
Custom Scan	Scans a specific file, folder, drive, or removable drive that you choose.
Custom Task	Runs LiveUpdate, frees disk space, and optimizes your disk volume.

Computer Scan provides details about the scanned items. You can view the details such as total number of files scanned, security risks detected, security risks resolved, and the total items that require attention. It also provides you the different ways to resolve any items that were not automatically resolved during the scan. You can also view the severity of the risk, the name of the risk, and the status of the risk about the resolved items.

Running a Full System Scan

Full System Scan performs a deep scan of the system to remove viruses and other security threats. It checks all boot records, files, and running processes to which the user has access. Consequently, when you run a **Full System Scan** with administrator privileges, it scans

more files than when you run it without administrator privileges.

To run a Full System Scan

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

Running a Quick Scan

Quick Scan is a fast scan of the areas of your computer that the viruses and other security risks often target. Because this scan does not scan your entire computer, it takes less time to run than a **Full System Scan**.

To run a Quick Scan

1. In the Norton Security main window, double-click **Security** and then click **Run 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 any items require attention, review the risks on the **Threats Detected** window.

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 Security main window, double-click **Security**, and then click **Run 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.

About the Results Summary window

Your Norton product displays the **Result Summary** window when you run a manual scan. At the end of a scan, the **Results Summary** window provides the summary of the scan results.

If your most recent scan was a Quick Scan, this window shows the results of a fast scan of the areas of your computer. Viruses, spyware, and other risks often target these areas.

If your most recent scan was a Full System Scan, this window shows the results of a comprehensive scan of your entire computer.

The **Result Summary** window displays the following information:

- Total items scanned
- Total security risks detected
- Total security risks resolved
- Total items that require your attention

Configuring the scan options

Your Norton product lets you configure scan options for each scan that you customize. By default, the scan options reflect the current **Computer Scans** settings in the **Settings** window. The changes that you make are applicable to the current scan only.

In addition to the custom scans that you create, you can configure the scan options for the default scans. You can configure scan options for Full System Scan, Quick Scan, Drive Scan, Folder Scan, and File Scan.

To configure the scan options

1. In the Norton Security main window, double-click **Security**, and then click **Run 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 scan that you want to schedule.
5. In the **Edit Scan** window, on the **Scan Options** tab, configure the scan options as required.
6. Click **Save**.

About the Threats Detected window

Your Norton product displays the **Threats Detected** window when it detects threats. At the end of a scan, the **Threats Detected** window provides you different ways to resolve any items that were not automatically resolved during the scan.

The **Threats Detected** window provides the information such as the severity of the risk, the name of the risk, and the status of the risk. It also provides the action that you can take to resolve the item. The **Threats Detected** window provides you the different options such as **Fix**, **Manual Fix**, **Exclude**, **Get Help**, and **Rescan** to resolve the item.

It also provides the **Ignore** option only once during the first-time detection of low-risk items.

Ignore option is available until you do not change the default settings for the **Low Risks** option. To access the **Low Risks** option, go the Norton product main window, and then click **Settings > Antivirus > Scans and Risks > Exclusions / Low Risks**.

The options in the **Threats Detected** window vary based on the types of files that the Norton product identified as infected during the scan.

Selecting the scan items

When you configure a custom scan, you must select the items that you want to include in the scan. You can include individual files, folders, or drives. You can include multiple drives, folders, and files to add to the scan. You can also exclude items from the scan.

When you select a drive, all the items in the drive including the files and folders are automatically added to the scan. When you select a folder, all of the files in folder are added to the scan.

To select the scan items

1. In the Norton Security main window, double-click **Security**, and then click **Run 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 add items for a new scan, click **Create Scan**.
     You must provide a name for the scan in the **Scan Name** box.
   - To add items for an existing scan, in the **Edit Scan** column, click the edit icon for the scan that you want to modify.
5. In the window that appears, on the **Scan Items** tab, do the following:
   - To add drives, click **Add Drives**, in the **Scan Drives** dialog box, select the drives to be scanned, and click **Add**.
   - To add folders, click **Add Folders**, in the **Scan Folders** dialog box, select the folders to be scanned, and click **Add**.
   - To add files, click **Add Files**, in the **Files to Scan** dialog box, select the files to be scanned, and then click **Add**.

   If you need to remove an item from the list, select the item, and then click **Remove**.

6 Click **Next**.
7 In the **Scan Schedule** tab, select the scan schedule as required, and then click **Next**.
8 In the **Scan Options** tab, click **Save**.

Creating a custom scan

You can create a custom scan if you regularly scan a particular segment of your computer. This custom scan lets you scan the segment frequently without having to specify it every time. You can also schedule the custom scan to run automatically on specific dates and times or at periodic intervals. You can schedule a scan according to your preferences. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work.

You can delete the scan when it is no longer necessary. For example, if you work on a project for which you need to swap files frequently with others. In this case, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

1 In the Norton Security main window, double-click **Security**, and then click **Run Scans**.
2 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
3 Click **Go**.
4 In the **Scans** window, click **Create Scan**.
5 In the **New Scan** window, in the **Scan Name** box, type a name for the scan.
You cannot specify a scan name that is already in use.
6 On the **Scan Items** tab, add the items that you want to scan. See "Selecting the scan items" on page 84.
7 On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 88.

8 On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 82.

9 Click **Save**.

Editing a custom scan

You can edit a custom scan that you created. You can include additional files or folders to the scan or remove the files and folders that you do not want to scan. You can also change the name of the scan.

You can edit a custom scan in the **Scans** window.

To edit a custom scan

1 In the Norton Security main window, double-click **Security**, and then click **Run 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 modify.

5 In the **Edit Scan** window, on the **Scan Items** tab, select the items that you want to scan. See "Selecting the scan items" on page 84.

6 On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 88.

7 On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 82.

8 Click **Save**.

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 Security main window, double-click **Security**, and then click **Run 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.

Deleting a custom scan

You can delete custom scans that you created if they are no longer needed.

To delete a custom scan

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

4 In the **Scans** window, in the **Delete** column, click the delete icon next to the custom scan that you want to delete.
5 Click **Yes** to confirm that you want to delete the scan.

Scheduling a scan

Your Norton product automatically detects the idle state of your computer and runs a Full System Scan. 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).

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

To schedule a custom scan

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

Scheduling a Full System Scan

Your Norton product automatically detects the idle state of your computer and runs a Full System Scan. Full System Scan protects your computer against infection without compromising the performance of your computer. You can schedule a Full System Scan on specific dates and times or at periodic intervals.

You can schedule a Full System Scan in the **Scans** window.

To schedule a Full System Scan

1 In the Norton Security main window, double-click **Security**, and then click **Run 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 **Full System Scan**.

5 In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.

6 Click **Next**.

7 In the **Scan Options** tab, click **Save**.

Scheduling a Quick Scan

Quick Scan scans the important locations of your computer that the viruses and other security threats often target. When you perform a Quick Scan, your Norton product scans only the running processes and the loaded programs. Quick Scan takes less time to scan than a Full System Scan because this scan does not scan your entire computer.

Your Norton product lets you schedule a Quick Scan. You can schedule a Quick Scan in the **Scans** window.

To schedule a Quick Scan

1. In the Norton Security main window, double-click **Security**, and then click **Run 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 **Quick Scan**.
5. In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
6. Click **Next**.
7. In the **Scan Options** tab, click **Save**.

Editing a scheduled scan

You can change the schedule of any scheduled custom scan, **Quick Scan**, or **Full System Scan** from the **Scans** window.

To edit a scheduled scan

1. In the Norton Security main window, double-click **Security**, and then click **Run 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 scan that you want to edit.
5. In the **Edit Scan** window, on the **Scan Schedule** tab, change the schedule as required.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.

6 Click **Next**.

7 In the **Scan Options** tab, click **Save**.

Running a scan at the command prompt

You can scan with your Norton product from the command prompt without opening the Norton product main window. You type the path and name of the file that you want to scan or customize the scan by adding a specific command. The following are some frequently used commands:

/?	NAVW32 launches help and terminates.
/A	Scans all drives
/L	Scans the local drives
/S[+|-]	Enables (+) or disables (-) subfolders scanning
/B[+|-]	Enables (+) or disables (-) boot record scanning and master boot record scanning (for example, NAVW32 C: /B+ or NAVW32 C: /B-)
/BOOT	Scans only the boot records
/QUICK	Runs a Quick Scan
/SE[+|-]	Enables (+) or disables (-) a Quick Scan

/ST[+|-]	Enables (+) or disables (-) scanning of stealth items
[folder_path]*[?]	Scans the files that matches specified wild card
[drive|folder|file]	Scans the specified drive, folder, or file
/SESCAN	Performs Quick Scan in the background. Your Norton product displays the **scans** window only when a threat is detected.

To run a scan from the command prompt

1 At the command prompt, type the path in which Norton Security is located and the executable's file name.
The following examples show the syntax of a scan command:

- **`"\Program Files\Norton Security\Engine\version\NAVW32" /command_name`**
  Where *version* represents the version number of Norton Security and *command_name* represents the command.
- **`"\Program Files\Norton Security\Engine\version\NAVW32" [path]file_name`**
  Where *version* represents the version number of Norton Security and *[path] file_name* represents the location, name, and extension of the file.

2 Press **Enter**.

Scanning your computer with Norton Power Eraser

Norton Power Eraser is a powerful malware removal tool that can help you clean up 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 rogueware 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, rogueware, or scamware. The tool uses more aggressive techniques than Norton Security; 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.

For more information about Norton Power Eraser, see Norton Power Eraser Tutorials.

To scan using Norton Power Eraser

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

Scanning your Facebook wall

Norton Safe Web protects your computer from malicious URLs when you use Facebook. It scans each URL that is available on your Facebook wall and displays the Norton rating icons for the scanned URLs.

You can also check if a URL is safe or unsafe. Norton Safe Web scans your Facebook News feed and provides you the safety status for each of the URL. This way, you are not only protected from unsafe sites but you can also let other Facebook users know the security status of any website.

However, Norton Safe Web requires your permission to scan the URLs that are available on your Facebook wall. When you install the Norton Safe Web Facebook app, the app asks for your permission to access your Facebook wall. You can choose to allow or deny permission to let Norton Safe Web access your Facebook wall.

The auto-scan feature in Norton Safe Web application page helps you protect your Facebook wall offline. Norton Safe Web scans the News Feed on your Facebook wall every day and protects you from malicious links. When Norton Safe Web detects a malicious link, it notifies you with a post on your Facebook wall. To activate **Norton Auto-Scan**, move the **Auto-Scan On/Auto-Scan Off** slider to the left to the **Auto-Scan On** position. The app asks for additional permission to automatically post in your wall when malicious links are identified.

To remove the malicious link from your Facebook wall, go to your Facebook wall and remove the malicious link. You can also click **See Norton Safe Web Report** to view Norton ratings and other details about this malicious link. When no malicious activity is detected on your

Facebook wall, Norton Safe Web posts a message notifying that your Facebook wall is safe. Norton Safe Web posts this message on your Facebook wall once in every 30 days.

If you later decide to remove Norton Safe Web from your Facebook profile, you can use the **Account Settings** option of Facebook.

The following are the safety states that Norton Safe Web provides after it scans the links on your Facebook wall:

Norton Secured	Indicates that the site has best security practices. The sites with this rating do not harm your computer and you can visit these sites with confidence.
Safe	Indicates that the site is safe to visit and Norton Trusted. The sites with this rating do not harm your computer and so you can visit this site.
Caution	Indicates that the site may have security threats. Symantec recommends you to be cautious while you visit such websites.
Warning	Indicates that the site has security risks. The sites with this rating may install malicious software on your computer. Symantec recommends that you do not visit this site.

Untested	Indicates that Norton Safe Web has not yet tested this site and it does not have sufficient information about this site.

Enabling your Facebook Wall Scan

The Norton Safe Web feature scans your Facebook wall and analyzes the security levels of links that are posted in the last 24 hours. It then displays the security status of the scanned URLs. However, Norton Safe Web requires your permission to scan your Facebook wall.

To enable your Facebook Wall

1. In the Norton Security main window, double-click **Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Scan Facebook Wall**, click **Scan Facebook Wall**.
3. Click **Go**.
4. In the Facebook login webpage, log in to your Facebook profile.
5. Give your permission for the app to access your public profile, friend list, and news feed.
6. Click **Auto-Scan On** to let Norton Auto-Scan protect your Facebook account.
7. Give your permission for the app to post publicly on your behalf.

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.

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 Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. On the **Automatic Protection** tab, under **Real Time Protection**, in the **SONAR Protection** row, do one of the following:
   - To turn off SONAR Protection, move the **On/Off** switch to the right to the Off position.
   - To turn on SONAR Protection, move the **On/Off** switch to the left to the On position.
4. In the **Settings** window, click **Apply**.

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 Security 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.

When you exclude a known security risk from Norton Security 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 Security 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.

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 Security 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**.

About the Silent Mode that you turn on manually

Your Norton product lets you manually turn on Silent Mode for a specified duration. When Silent Mode is turned on, your Norton product suppresses alerts and suspends background activities for the duration that you specify. You can verify the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. The Norton Security icon in the notification area changes from yellow outer circle to gray to display the turn-on status of Silent Mode. Turning on Silent Mode manually before you perform your tasks helps you prevent alerts, notifications, or background activities interrupting you for the specified duration.

You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. After the

specified duration, your Norton product turns off Silent Mode. You can also manually turn off Silent Mode at any time. Your Norton product notifies you after Silent Mode is turned off. The activities that are suspended when Silent Mode is turned on run after Silent Mode is turned off.

Turning on or turning off Silent Mode manually

You can manually turn on Silent Mode for a specified duration before you perform any important task on your computer. You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. The Norton Security icon displays the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. Your Norton product notifies you after Silent Mode is turned off. After Silent Mode is turned off, your Norton product also displays alerts if it detected any security activities that occurred during the Silent Mode session.

You can turn on or turn off Silent Mode from the **Silent Mode Settings** section of the **Settings** window. You can also turn on or turn off Silent Mode by using the Norton Security icon in the notification area.

To turn on Silent Mode from the Administrative Settings window

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **Silent Mode** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.
6. In the **Settings** window, click **Close**.

To turn off Silent Mode from the Administrative Settings window

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **Silent Mode** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**, and then click **Close**.

To turn on Silent Mode from the notification area

1. In the notification area on the Windows taskbar, right-click the Norton Security icon, and then click **Turn on Silent Mode**.
2. In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.

To turn off Silent Mode from the notification area

- In the notification area on the Windows taskbar, right-click the Norton Security icon, and then click **Turn off Silent Mode**.

To turn off or turn on Silent Mode from Quick Controls

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, do one of the following:
   - To turn off Silent Mode, uncheck **Silent Mode**.
   - To turn on Silent Mode, check **Silent Mode**, and select the duration for which you want Silent Mode to be turned on from the Turn on Silent Mode dialog box, and click **OK**.

About the Silent Mode that turns on automatically

When you watch a movie, play games, or make a presentation, you run the application in the full-screen mode. Your Norton product detects the application that you run in the full-screen mode and automatically

enables Silent Mode. When Silent Mode is enabled, your Norton product suppresses most of the alerts and suspends background activities. Only those activities run that are involved in protecting your computer from viruses and other security threats. Minimum background activities also ensure high performance of your computer. The activities that are suspended run after you finish using the application in the full-screen mode.

Silent Mode also helps you maintain an uninterrupted Media Center Extender session. A Media Center Extender session is an extended session of Media Center to an entertainment device, such as a television. The alerts and notifications that appear during a Media Center Extender session disconnect the session between the host computer and the entertainment device. Your Norton product identifies a Media Center Extender session as an active full-screen application and turns on Silent Mode. When Silent Mode is enabled, your Norton product suppresses alerts and notifications and suspends background activities to provide uninterrupted sessions for Silent Mode options such as Full Screen Detection or Media Center applications.

Turning off or turning on Full Screen Detection

You can use the **Full Screen Detection** option in the **Settings** window to turn on or turn off Silent Mode automatically when your Norton product detects a full-screen application. By default, the **Full Screen Detection** option remains turned on after you install Norton Security.

To turn off Full Screen Detection

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **Full Screen Detection** row, move the **On/Off** switch to the right to the **Off** position.

4 In the **Settings** window, click **Apply**, and then click **Close**.

To turn on Full Screen Detection

1 In the Norton Security main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3 Under **Silent Mode Settings**, in the **Full Screen Detection** row, move the **On/Off** switch to the left to the **On** position.
4 In the **Settings** window, click **Apply**, and then click **Close**.

About Quiet Mode

Your Norton product automatically enables Quiet Mode when you perform tasks that require higher utilization of your system resources. When Quiet Mode is turned on, your Norton product suspends the background activities and lets the task use the maximum resources for better performance.

You can choose to set your Norton product to automatically enable Quiet Mode when you do the following tasks:

- IMAPI 2.0 Disk Burn
- User-Specified Programs

The following table explains about the various options:

IMAPI 2.0 Disk Burn	When you use a Media Center application to burn a CD or a DVD, your Norton product automatically enables Quiet Mode, if the **IMAPI 2.0 Disk Burn** option is turned on. By default, the **IMAPI 2.0 Disk Burn** option is turned on. When Quiet Mode is enabled, your Norton product suspends background activities to improve the performance of your disk-burning session. However, your Norton product continues to display alerts and notifications during the session. Your Norton product supports the following Media Center disk-burner applications to turn on Quiet Mode: ▪ IMAPI 2.0 ▪ J. River MEDIA CENTER (version 13.0.125 and later) Your Norton product turns on Quiet Mode as soon as you start burning a CD or a DVD using a Media Center application. Your Norton product turns off Quiet Mode after the disk-burning session is complete. You cannot turn off Quiet Mode during the disk-burning session by turning off the **IMAPI 2.0 Disk Burn** option in the **Settings** window.

User-Specified Programs	Your Norton product automatically turns on Quiet Mode when it detects or a disk-burning session. In addition, you can manually add the programs for which you want your Norton product to turn on Quiet Mode to the **Quiet Mode Programs** list. When your Norton product detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, your Norton product suspends the background activities but does not suppress alerts and notifications. You can also add or remove a running program to the **Quiet Mode Programs** list.

Turning off or turning on the Quiet Mode options

You can turn off or turn on the Quiet Mode options, such as **IMAPI 2.0 Disk Burn** and **User-Specified Programs** in the **Settings** window. By default, the IMAPI 2.0 Disk Burn option is turned on. If you perform a task for IMAPI 2.0 Disk Burn option that you turned on, your Norton product detects the task and automatically turns on Silent Mode. For example, you turn on the **IMAPI 2.0 Disk Burn** option and start burning a disk using a Media Center application. In this case, your Norton product detects the disk-burning session and turns on Quiet Mode.

Your Norton product turns on Quiet Mode as soon as you start burning a CD or a DVD. Once Quiet Mode is turned on, it turns off only after the TV program recording session or disk-burning session is complete. You cannot

turn off Quiet Mode during the sessions by using the options in the **Settings** window.

To turn off or turn on IMAPI 2.0 Disk Burn

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **IMAPI 2.0 Disk Burn row**, do one of the following:
   - To turn off detection of a disk burning session, move the **On/Off** switch to the right to the **Off** position.
   - To turn on detection of a disk burning session, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

About User-Specified Programs

Your Norton product automatically turns on Quiet Mode when it detects a disk-burning session. In addition, you can manually add the programs for which you want your Norton product to turn on Quiet Mode to the Quiet Mode Programs list. When your Norton product detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, your Norton product suspends the background activities but does not suppress alerts and notifications.

You can also add a running program to the Quiet Mode Programs list. However, when you add a running program, your Norton product does not detect the current running instance of the program to turn on Quiet Mode. Your Norton product turns on Quiet Mode the next time when you execute the program.

You can also remove a running program from the Quiet Mode Programs list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the

programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

You can view the details of the programs that you add to the Quiet Mode Programs list or remove from the list in the **Security History** window.

Adding programs to User-Specified Programs

You can manually add the programs for which you want your Norton product to turn on Quiet Mode to the Quiet Mode Programs list. When you execute the program that you added to the list, your Norton product detects the program and turns on Quiet Mode.

You can also add a running program to the **Quiet Mode Programs** list. However, when you add a running program, your Norton product does not detect the current running instance of the program to turn on Quiet Mode. Your Norton product turns on Quiet Mode the next time when you execute the program.

You can only add the programs that have .exe file extension to the **Quiet Mode Programs** list.

To add a program

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings,** in the **User-Specified Programs** row, click **Configure**.
4. In the **Quiet Mode Programs** window, click **Add**.
5. In the **Add Program** dialog box, navigate to the location of the file that you want to add to the Quiet Mode Programs list.
6. Select the file, and then click **Open**.
7. In the **Quiet Mode Programs** window, click **OK**.

Removing programs from User-Specified Programs

You can remove a program from the **Quiet Mode Programs** list. After you remove a program, your Norton product does not turn on Quiet Mode the next time when it detects a running instance of the program.

You can also remove a running program from the **Quiet Mode Programs** list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

To remove a program

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **User-Specified Programs** row, click **Configure**.
4. In the **Quiet Mode Programs** window, select the program that you want to delete, and then click **Remove**.
5. In the confirmation dialog box, click **Yes**.
6. In the **Quiet Mode Programs** window, click **Apply** and then click **OK**.

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 Security 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 Early Launch Anti-Malware Protection

The **Early Launch Anti-Malware Protection** feature provides enhanced security level during the boot time when you start your computer. It ensures better protection by running all the necessary components of the Norton product that are required to block any malware from functioning when you start your computer.

This option is available only on Windows 8 or later.

To turn on or turn off early launch anti-malware protection

1 In the Norton Security main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3 In the **Antivirus** settings window, click the **Automatic Protection** tab.
4 In the **Early Launch Anti-Malware Protection** row, do one of the following:
   - To turn on **Early Launch Anti-Malware Protection**, move the **On/Off** switch to the left to the **On** position.
   - To turn off **Early Launch Anti-Malware Protection**, move the **On/Off** switch to the right to the **Off** position.
5 In the **Settings** window, click **Apply**, and then click **Close**.

Responding to security issues

4

This chapter includes the following topics:

- About keeping your computer secure
- About solving connection problems
- About responding to emergencies
- What to do if a security risk is found

About keeping your computer secure

Installing the latest version of Norton product is the best way to keep your PC protected against malicious threats and viruses. It is recommended that you maintain the latest virus definitions. If you have an active Internet connection, the definitions are updated automatically.

In addition, there are several security best practices you should follow to avoid threats and protect your PC and data from malicious viruses:

To avoid email threats, do the following:

- Open only those email attachments that come from a trusted source and that you expect to receive.
- Delete all unwanted messages without opening them.
- Do not respond to email that you suspect is spam. Delete it.
- Be wary of any email that requests confidential information, and confirm the authenticity of the request before you reply.

To protect yourself from phishing attempts, do the following:

- When you visit a website, type the address directly into your browser rather than clicking a link.
- Provide personal information only on trusted sites. Examples include the sites that have "https" in the web address or that have a lock icon at the bottom of the browser window.
- Do not provide personal information to any unsolicited requests for information.

To avoid viruses, worms, and Trojan horses, do the following:

- Transfer files to your PC only from a well-known source or a trusted source.
- Do not send or receive files over instant messaging connections.
- Terminate an instant messaging connection if a person on your buddy list sends strange messages, files, or web links.

To avoid spyware, do the following:

- Do not approve suspicious error messages from within your browser.
- Be suspicious of "free deal" offers because spyware may come as part of such a deal.
- Carefully read the End User License Agreement for the programs that you install. Also, do not install a program if other programs are installed as part of the required program.

About solving connection problems

Your Norton product uses an Internet connection to support several of its protection features. If you use a proxy server to connect to the Internet, you must configure the proxy settings of the Norton product. You can configure Network Proxy Settings in the **Administrative Settings** window.

If you cannot connect to the Internet after you install the Norton product, you can use the Support features to help you troubleshoot your connection problem.

About responding to emergencies

Your Norton product automatically downloads definition updates regularly and secures your computer from latest viruses and unknown threats. In addition, the Norton product monitors your Internet activities to protect your computer from the Internet-based threats that exploit software vulnerabilities.

However, security issues can arise, and you need to decide which action to take.

If you think that your computer is infected with a virus or with destructive software, you can take the following actions:

Quick Scan	Helps you to scan the possible virus-infected areas of a computer that the viruses and other security risks often target Because this scan does not scan your entire computer, it takes lesser time to run than a Full System Scan.
Full System Scan	Checks all boot records, files, and running programs to protect your computer from viruses and spyware When you run a Full System Scan with administrator privileges, it scans more files than when you run it without administrator privileges. This scan might take more time than the other scans.

Custom Scan	Scans a specific file, folder, drive, or removable drive that you choose. You can also create your own scan and schedule it to run at a specific time.
Custom Task	Checks for vulnerabilities and risks, and protects your computer by running the following checks: **LiveUpdate** **Internet Explorer Temporary Files** **Windows Temporary Files** **Internet Explorer History** **Disk Optimization**

When you right-click a folder, the shortcut menu displays Norton Security and then **Scan Now** option. You can use this option to scan any particular file or folder. Norton Insight scan is simultaneously run along with this scan. Thus this option scans a file using both local definitions and definitions that are hosted in the cloud.

What to do if a security risk is found

Your product provides many solutions and features for handling viruses and other security threats that it detects.

When your Norton product detects a security risk on your computer, you must take appropriate action on the risk. Your Norton product notifies you when it detects a security risk. You can view details about the risk in the window that appears and select an action that you want the Norton product to perform on the risk.

By default, the Norton product removes the security risk from your computer and quarantines it. However, you

can restore the file from the Quarantine to its original location and exclude it from future scans.

Exclude a program from Norton Security 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.

In some cases, the Norton product requires your attention to manually resolve the detected security risk. You can access the Symantec Security Response website and refer the manual removal instructions.

In some cases, the 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 submit the item to Symantec for further analysis.

In addition, your product provides solutions for security risks, such as spyware and adware.

About detecting viruses, spyware, and other risks

Viruses and other security threats can be detected during a manual or customized scan. Auto-Protect detects these threats when you perform an action with an infected file. Threats can also appear when you send an email message, or during a manual or customized scan.

Security risks, such as spyware and adware, can also be detected when these activities are performed.

The files that can potentially infect your system when your computer first starts up are scanned first.

These files include the following:

- Files that are associated with the processes that are currently running in memory
- Files with startup folder entries
- Files with system start INI file entries
- Files with system start batch file entries
- Files that the system start registry keys refers

If an infected file is detected during this portion of the manual scan, it is repaired or removed. Any unnecessary references are also removed from your computer. Before attempting to repair, quarantine, or delete any infected file that has a process running in memory, your product attempts to terminate the process. You are alerted and prompted to close all unnecessary programs before the process is terminated.

You can view information about detected viruses and other security threats in Security History.

Reviewing Auto-Protect notifications

Auto-Protect scans files for viruses, worms, and Trojan horses when you perform an action with them, such as moving them, copying them, or opening them. It also scans for spyware, adware, and other security risks.

If Auto-Protect detects suspicious activity, it logs a notification in Security History that tells you that a risk was found and resolved.

If Auto-Protect detect one or more viruses it either repairs or deletes the viruses and notifies you. The notification provides information on which file was repaired or deleted and which virus, Trojan horse, or worm infected the file. No further action is necessary.

To review Auto-Protect notifications

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

2 In the **Security History** window, in the **Show** drop-down list, select the category for which you want to review Auto-Protect alerts.
Auto-Protect options are:

Recent History	Review Auto-Protect notifications that you received in the last seven days.
Full History	Review all of the Auto-Protect notifications that you have received.
Resolved Security Risks	Review all of the resolved security threats. The **Resolved Security Risks** category includes the infected files that the Norton product repairs, removes, or quarantines.
Unresolved Security Risks	Review the list of unresolved security risks. The **Unresolved Security Risks** category includes the infected files for which the Norton product was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action.

3 In the right pane, under **Recommended Action** click the **Options** link.
The option name appears as **Restore & Options** for few items.
If one or more security risks such as spyware are found, you can take action on these items, if required.

4 In the **Threat Detected** window, select the appropriate action on the risk.
The following are some of the options that are available in the **Threat Detected** window:

Restore & Exclude this file	Returns the selected Quarantine item to its original location and excludes the item from being detected in the future scans. This option is available for the detected viral and non-viral threats.
Exclude this program	Excludes the security risk from future scan. Your Norton product adds the security risk to the appropriate exclusions list.
Manual Fix (recommended)	Lets you resolve the risk using a manual fix tool. If you resolve a threat manually, you must remove the threat information from the **Security History** window.
Remove this file (may cause browser to close) (recommended)	Removes the security risk from your computer and quarantines it. This option is available for the security risks that require your attention.

Remove this file (may cause browser to close)	Removes the selected security risk from the computer and quarantines it. This option is available for the security risks that require your attention for manual removal. This option is also available for the security risks that are manually quarantined.
Remove from history	Removes the selected security risk item from the Security History log.
Get help (recommended)	Takes you to the Symantec Security Response website. This option is available for the security risks that require your attention for manual removal. You can refer the Symantec Security Response website for manual removal instructions or other information about the risk.

Submit to Symantec	Sends the security risk to Symantec. In some cases, the 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.

Responding to Worm Blocking alerts

If a program tries to email itself or a copy of itself, it could be a worm trying to spread through email. A worm can send itself or send a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for worms. If it detects a worm, you receive an alert notifying you that a malicious worm was found.

Worm Blocking alert appears only when you enable the **Ask me what to do** option under **How to increase protection** in the **Email Antivirus Scan** window. If the **Ask me what to do** option is disabled, the Norton product automatically quarantines the detected worm and notifies you.

The alert presents you with options and asks you what to do. If you do not send an email message at that time, then it is probably a worm and you should quarantine the file.

To respond to Worm Blocking alerts

❖ In the alert window, select the action that you want to take. Your options are:

Quarantine	Permanently stops the worm by putting it in Security History. While in Security History, the worm is unable to spread. This Quarantine is the safest action.
Allow	Sends the email message for which you have received the worm blocking alert. If you allow the email message, it could infect the recipient's computer. Select this option if you are sure that the email is not infected with a worm.
Ignore	Ignores this risk.

If a malicious worm is found, it should be quarantined.

To quarantine a worm-infected file

1 In the alert, in the drop-down list, click **Quarantine**.

2 After the worm has been quarantined, perform the following tasks:

- Run LiveUpdate to ensure that you have the latest definition updates.

  See "About protection updates" on page 36.
- Scan your computer.

  See "Running a Full System Scan" on page 79.

If nothing is detected, submit the infected file to Symantec Security Response. Also, indicate that the file was detected and that you have scanned it with the latest definition updates. Symantec Security Response replies to you within 48 hours.

About responding to risks detected during a scan

At the end of a scan, the **Results Summary** window provides the summary of the scan results. You can use the **Threats Detected** window to resolve any items that were not automatically resolved during the scan.

You can use the **Show** drop-down list that is available in the **Security History** window to resolve any items that were not automatically resolved during the scan. The **Recommended Action** section in the **Security History** window displays the action that you should take to resolve the security threat.

About actions when your Norton product cannot repair a file

One of the common reasons that your Norton product cannot automatically repair or delete an infected file is that you do not have the current definition updates. Run LiveUpdate, and then scan again.

If that does not work, read the information on the **Security History - Advanced Details** window to identify

the types of files that cannot be repaired. You can take one of the following actions, depending on the file type:

Infected files	You can view the file type of the detected risk. This information helps you to decide the action that can be taken depending on the file type. For example, you can view the infected files with the following file name extensions (any file can be infected): ■ .exe ■ .doc ■ .dot ■ .xls Use the **Threats Detected** window to solve the problem.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using your operating system disks.

Doing routine tasks

5

This chapter includes the following topics:

- Turning on or turning off automatic tasks
- Running custom tasks
- Scheduling security and performance scans
- Specifying Idle Time Out duration

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, and downloading protection updates. 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 Security 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 Security main window, double-click **Security**, and then click **Run 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 Security 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**.

Specifying Idle Time Out duration

You can set the duration after which your Norton product should identify your computer as idle. You can select a value (in minutes) between 1 minute and 30 minutes. When you do not use your computer for the specified duration, your Norton product identifies your computer as idle. The Norton product then runs the activities that are scheduled to run at idle time.

To specify Idle Time Out duration

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Out** row, in the drop-down list, select the duration that you want to specify.
   You might need to scroll the window to view the option.
4. In the **Settings** window, click **Apply**.

Protecting Internet activities

6

This chapter includes the following topics:

- About the Smart Firewall
- Turning off and turning on Browser Protection
- Turning off or turning on Download Intelligence
- Configuring the Download Insight Notifications option
- Configuring the Show Report on Launch of Files option
- Turning off or turning on Intrusion Prevention notifications
- Excluding or including attack signatures in monitoring
- Turning off or turning on AutoBlock
- Unblocking AutoBlocked computers
- Permanently blocking a computer that has been blocked by AutoBlock
- About Intrusion Prevention exclusion list
- Removing all devices from Intrusion Prevention exclusion list
- Adding a device to the Device Trust
- Changing the trust level of your network and devices

- About the types of security risks
- About Norton AntiSpam
- Adding POP3 and SMTP ports to Protected Ports
- Removing an email port from Protected Ports
- Turning off or turning on Network Cost Awareness
- Defining the Internet usage of Norton Security

About the Smart Firewall

The Smart Firewall monitors the communications between your computer and other computers on the Internet. It also protects your computer from such common security problems as the following:

Improper connection attempts	Warns you of connection attempts from other computers and of attempts by programs on your computer to connect to other computers
Port scans	Cloaks the inactive ports on your computer thereby providing protection against attacks through hacking techniques such as port scanning
Intrusions	Monitors the network traffic to or from your computer for suspicious behavior and stops any attack before they threaten your system

A firewall blocks hackers and other unauthorized traffic, while it allows authorized traffic to pass. The Windows Firewall feature monitors all inbound communications to your computer. However, Windows Firewall does not monitor the outbound communications from your computer to the Internet.

Symantec recommends that you keep the **Smart Firewall** option turned on to let your Norton product

monitor all inbound and all outbound communications of your computer. The Smart Firewall feature automatically creates program rules for each program that you run. When the **Smart Firewall** option is turned on, the Norton product retains the **Automatic Program Control** settings for all programs.

Turning off Smart Firewall reduces your system protection. Always ensure that the Smart Firewall is turned on.

Turning off or turning on Smart Firewall

Smart Firewall monitors communications between your computer and the other computers on the Internet. It also protects your computer from common security problems.

If you must turn off the Smart Firewall, you should turn it off temporarily to ensure that it is turned on again automatically. To ensure that your computer remains protected, you can turn on the Smart Firewall manually before the time that you specify concludes.

When the Smart Firewall is turned off, your computer is not protected from Internet threats and security risks.

To turn off Smart Firewall

1. In the Norton Security 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 the right to the **Off** position.
4. Click **Apply**.
5. In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off Smart Firewall.
6. Click **OK**.
7. Click **Close**.

To turn on Smart Firewall

1. In the Norton Security 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 the left to the **On** position.
4. Click **Apply**.
5. Click **Close**.

To turn off Smart Firewall from Quick Controls

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, uncheck **Smart Firewall**.

To turn on Smart Firewall from Quick Controls

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, check **Smart Firewall**.

To turn off Smart Firewall from the notification area

1. In the notification area on the taskbar, right-click the Norton Security icon, and then click **Disable Smart Firewall**.
2. In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off Smart Firewall.
3. Click **OK**.

To turn on Smart Firewall from the notification area

- In the notification area on the taskbar, right-click the Norton Security icon, and then click **Enable Smart Firewall**.

About firewall rules

A firewall is a security system that uses rules to block or allow connections and data transmission between your computer and the Internet. Firewall rules control how the Smart Firewall protects your computer from

malicious programs and unauthorized access. The firewall automatically checks all traffic that comes in and out of your computer against these rules.

The Smart Firewall uses two kinds of firewall rules:

Program rules	Control network access for programs on your computer.
Traffic rules	Control all the incoming and the outgoing network traffic.

Program Rules

On the **Program Control** tab, you can do the following:

- Rename the program description.
- Modify the rules for a program.
- Add a rule for a program.
- Modify the access settings of a program rule.
- Modify the priority of rules for a program by changing the sequence of rules in the list.
- Remove a program rule.
- View the trust level of a program.

You can create Program rules in the following ways:

Automatically customize Internet access settings	Lets the firewall automatically configure access for programs the first time that users run them. This method is the easiest way to create firewall rules.
Use Firewall settings	Manages the list of programs that can access the Internet.

Respond to alerts	Lets the firewall notify you when a program attempts to access the Internet. You can then allow or block Internet access for the program. In some instances, such as when you watch a movie, you might prefer not to be alerted with any messages. In such cases, you can turn on Automatic Program Control. Your Norton product does not prompt you with any firewall alerts in this state. The firewall notifies you only if you have changed the General Settings options of Smart Firewall from their default, recommended settings.

Traffic Rules

The **Traffic Rules** tab displays a list of predefined traffic rules. Some of the default Traffic rules are read-only and are locked. You cannot modify these rules.

The rules appear in the order of their priority levels. Rules that appear higher in the list override the rules that appear lower in the list.

You can add a new Traffic rule on this tab. You can also do the following activities:

Modify a Traffic rule	You can change the settings of a Traffic rule that does not function the way you want. However, you cannot modify some of the default rules that are read-only.

Turn off a Traffic rule	You can disable a Traffic rule. However, you cannot turn off some of the default rules that are read-only.
Change the priority of a Traffic rule	You can change the priority of a Traffic rule by changing the order in which it appears in the list. Only advanced users or users at the direction of technical support, should perform this action.

About the order in which firewall rules are processed

The Smart Firewall processes Traffic rules before it processes Program rules. For example, when there is a Program rule that allows Internet Explorer to access Internet using port 80 with TCP protocol and a Traffic rule that blocks TCP communication through port 80 for all applications. The Internet Explorer application cannot access the Internet as the Norton product gives precedence to Traffic rules over the Program rules.

Within the list of Traffic rules, rules are processed in order of appearance, from top to bottom. **Program Rules** entries are not processed in order. The rules within each **Program Rules** entry, however, are processed in order of appearance, from top to bottom.

For example, you have a Program rule for the Symantec pcAnywhere application that blocks the use of the application with any other computer. You add another rule for the same application that allows its use with a specific computer. You then move the new rule before the original rule in the program rule list. Your Norton product processes the new rule first and lets you use Symantec pcAnywhere with that specific computer. It

then processes the original rule and prevents its use with any other computer.

Turning off Automatic Program Control

Automatic Program Control automatically configures Internet access settings for Web-enabled programs the first time that they run. When a program tries to access the Internet for the first time, Automatic Program Control creates rules for it.

Automatic Program Control configures Internet access only for the versions of programs that Symantec recognizes as safe. An alert occurs when an infected program tries to access your computer.

If you want to determine the Internet access settings for your programs, you can turn off Automatic Program Control. When a program tries to access the Internet for the first time, an alert prompts you to configure access settings.

Symantec recommends that Automatic Program Control remain set to **On**. By turning it off, you might make the incorrect decisions that can allow malicious programs to run or block critical Internet programs and functions.

To turn off Automatic Program Control

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. In the **Firewall** settings window, click **Advanced Program Control**.
4. In the **Automatic Program Control** row, move the **On/Off** switch to the right to the **Off** position.
5. Click **Apply**.

Adding a program to Program Control

You can add a program to Program Control to control their ability to access the Internet. When you add the program, you can configure its access settings in Program Rules. You can allow, block, or create the

custom rules that are specific to the program that you add.

Manually configured Firewall settings for programs override any settings that Automatic Program Control makes. However, Symantec recommends you to retain the settings that Automatic Program Control makes as and when you run your programs.

To add a program to Program Control

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Program Control** tab, click **Add**.
4. In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
5. Click **Open**.
6. In the **Security Alert** window, analyze the reputation information of the program.
   Your Norton product fetches and displays the reputation information and the recommended access setting.

7 In the **Options** drop-down list, select the access level that you want this program to have.
Your options are:

Allow Always	Allow all access attempts by this program.
Block Always	Deny all access attempts by this program.
Manual configure	Create the rules that control how this program accesses the Internet. You can set the following criteria for a rule: **Action** **Connections** **Computers** **Communications** **Advanced** **Description** If you select this option, you must follow the instructions in the wizard that appears and configure the rule.

8 Click **OK**.

Removing a program from Program Control

You can remove programs from Program Control if necessary. In this case, your Norton product removes all the rules that are associated with the application that you remove.

To remove a program from Program Control

1 In the Norton Security 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 remove.
4 Click **Remove**.
5 In the **Confirmation** dialog box, click **Yes**.
The confirmation dialog box appears only when the **Automatic Program Control** option is turned off.
6 Click **Apply**.

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 Security 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**.

Adding Traffic rules and Program rules

Program Control automatically creates most of the firewall rules that you need. You can add custom rules if necessary.

Only experienced users should create their own firewall rules.

You can add the following types of firewall rules:

- Traffic rules
- Program rules

To add a Traffic rule

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Traffic Rules** tab, click **Add**.
4. Follow the instructions in the **Add Rule** wizard.
5. In the **Traffic Rules** window, click **OK**.

To add a Program rule

1. In the Norton Security 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 to which you want to add a rule.
4. Click **Modify**.
   You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
5. In the **Rules** window, click **Add**.
6. Follow the instructions in the **Add Rule** wizard.
7. In the **Rules** window, click **OK**.

Using the Add Rule Wizard

The **Add Rule** Wizard leads you through the steps that are necessary to create firewall rules.

To use the Add Rule Wizard

1 Open the **Add Rule Wizard** by creating a Traffic rule or a Program rule.

2 In the first panel of the **Add Rule Wizard**, select the action that you want for this rule. Your options are:

Allow	Allow communication of this type. For example, consider a Traffic rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Allow**, Smart Firewall allows all connections that satisfy the criteria of this Traffic rule.
Block	Prevent communication of this type. For example, consider a Traffic rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Block**, Smart Firewall blocks all connections that satisfy the criteria of this Traffic rule.

Monitor	

	Update the **Firewall – Activities** category in the event log each time that communication of this type takes place. This option lets you monitor how often this firewall rule is used. Your Norton product notifies you every time that the traffic matching the monitor rule criteria passes through your computer. You can use the links in these notifications to view the logs. You can view the event log under **Firewall – Activities** category in the **Security History** window. Your Norton product creates separate action rules to allow or block the programs that have only a **Monitor** rule associated with them. The **Monitor** rule must be of higher order than the action rule for successful log entry of the network event that is related to the program. The monitor rule only logs the traffic events in the **Security History** window. You need to create another Allow or Block rule to handle the network traffic. You can monitor and allow or block the traffic

	by enabling the **Create a Security History log entry** option in the **Add Rule Wizard** or the **Modify Rule Wizard**.

3 Click **Next**.

4 Select the type of connection for the rule. Your options are:

Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to inbound and to outbound connections.

5 Click **Next**, and then select the computers that apply to the rule. Your options are:

Any computer	The rule applies to all computers.
Any computer in the local subnet	This rule applies only to computers in the local subnet. An organization's network is divided into subnets to facilitate efficient Internet communications. A subnet represents all of the computers in the same LAN.

Only the computers and sites listed below	The rule applies only to the computers, sites, or domains that you specify. You can specify the names and addresses of computers that apply to the rule. The details of the specified computers appear in the list. You can also remove computers from the list. When you select this option, the **Add** option becomes available. When you click **Add**, your Norton product displays the **Networking** dialog box in which you can specify individual computers, a range of computers, or specify all computers on a subnet or network. You can use the **Add** option or the **Remove** option to add or remove a computer.

6 Click **Next**, and then select the protocols for the rule. Your options are:

TCP	The rule applies to TCP (Transmission Control Protocol) communications.
UDP	The rule applies to UDP (User Datagram Protocol) communications.
TCP and UDP	The rule applies to TCP and to UDP communications.
ICMP	The rule applies to ICMP (Internet Control Message Protocol) communications. This option is available only when you add or modify a Traffic rule.
ICMPv6	The rule applies to ICMPv6 (Internet Control Message Protocol for Internet Protocol version 6) communications. This option is available only when you add or modify a Traffic rule.

All	The rule applies to all supported protocols. When you select this option, you cannot specify the types of communications or ports that apply to the rule.

7 Select the ports for the rule. Your options are:

All types of communication (all ports, local and remote)	The rule applies to communications that use any port.
This rule will apply only if it matches all of the ports listed below	The rule applies to the ports that you specify. You can specify the ports by selecting from the listed ports or by adding specific ports or port ranges. If you select ICMP or ICMPv6 protocol, you can specify the commands. To do so, select a command from the list of known commands or add specific commands or command ranges. When you select this option, the **Add** option becomes available. You can use the **Add** option or the **Remove** option to specify or remove a port or a command.

8 Click **Next**.

9 Check **Create a Security History log entry** if you want the Norton product to create an entry in the firewall event log.
Your Norton product creates an entry when a network communication event matches this rule. You can view the event log in the **Security History** window under **Firewall – Activities**. If you selected the **Monitor** option in the **Action** window, then the **Create a Security History log entry** option is automatically checked. You cannot uncheck the box to turn off this option as it is the default setting.

10 Under **Apply rule for NAT IPv6 traversal traffic**, select an option. Your options are:

- **On**
- **If Explicity requested**
- **Off**

11 Click **Next**, and then, in the text box, type a name for this rule.

12 Click **Next**, and then review the new rule settings.

13 Click **Finish**.

14 When you have finished adding rules, click **Close**.

Modifying Traffic rules and Program rules

You can change an existing firewall rule if it does not function the way that you want. You can use the **Modify** option to change the settings of an existing firewall rule. When you change a rule, the firewall uses the new criteria of the modified rule to control network traffic.

You cannot modify some of the default rules that are read-only. However, you can view the settings of these rules by using the **View** option.

To modify a Traffic rule

1 In the Norton Security 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 change.
4 Click **Modify**.
5 In the **Modify Rule** window, make the necessary changes to modify any aspect of the rule.
6 When you have finished changing the rule, click **OK**.

To modify a Program rule

1 In the Norton Security 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 change.
4 Click **Modify**.
You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
5 In the **Rules** window, select the rule that you want to change.
6 Click **Modify**.
7 In the **Modify Rule** window, make the necessary changes to modify to change any aspect of the rule.
8 When you have finished changing the rule, click **OK**.

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.

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 Security 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 Security 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.

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 Security 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**.

Removing a firewall rule

You can remove some of the firewall rules if necessary. However, you cannot modify some of the default Traffic rules that appear in the list. You can view the settings of these rules by using the **View** option.

Do not remove a firewall rule unless you are an advanced user. Removing a firewall rule can affect firewall functionality and reduce the security of your computer.

To remove a Traffic rule

1. In the Norton Security 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 remove.
4. Click **Remove**.
5. In the **Confirmation** dialog box, click **Yes**.

To remove a Program rule

1. In the Norton Security 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 contains the rule that you want to remove.
4. Click **Modify**.
   To remove all the program rules that are associated with the program, click **Remove**.

5 In the **Rules** window, select the rule that you want to remove.
6 Click **Remove**.
7 In the **Confirmation** dialog box, click **Yes**.
8 Click **OK**.

Turning off and turning on 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 Security main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Advanced Program Control** tab, move the slider next to **Show Firewall Block Notification** to the **Off** position.

About Norton Firewall Diagnosis

There may be times when firewall may block the network traffic that you want to allow based on its configuration settings. In such cases, you may have issues in accessing the Internet, the Network, or another computer to perform tasks such as sharing resources.

When you experience network connection problems, Norton Firewall acts quickly in identifying the cause of failure and provides its diagnosis. Your Norton product displays the **Firewall Diagnostics Wizard** when you encounter network connection problems.

Norton Firewall Diagnosis is available only in Windows 7 or later.

The Wizard contains the problem diagnosis report that is unique for different cases of network blocks. For instance, a network block can occur in any of the following cases:

- The uncommon protocol that is handling the traffic is blocked
- The currently active firewall rule is conditioned to block the traffic that you want to allow
- The traffic has violated the process policy of the firewall
- The traffic has violated the traffic policy of the firewall
- The traffic comes from the restricted zone of networks or computers
- The traffic matches an Intrusion Prevention attack signature

You can use the **Firewall Diagnostics Wizard** as a guide to troubleshoot the network connection problem by yourself.

For each case of network block, the Wizard contains the firewall's analysis of the cause and the possible solutions to fix the block.

Your Norton product recommends that you use the **Firewall Diagnostics Wizard** to remove any type of block. The solutions in the Wizard let you analyze the issue and take a suitable action to resolve the problem.

Using the Wizard to troubleshoot the problem has the following advantages:

- It automatically tries to fix the problem by itself
- It lets you modify the settings that are related to the block
- It lets you view the log details related to the network block event
- It provides you the option to turn off firewall as the last means to resolve the issue

About the reputation information in firewall alerts

Firewall alerts notify you of connection attempts from other computers and of attempts by programs on your computer to connect to other computers. The reputation details in the firewall alerts help you make more definite decisions on whether to allow or block communication attempts of networking applications.

You can use the reputation details to determine the trustworthiness of programs and running processes on your computer that access the network. The reputation-based security technology provides reputation ratings for files on the Internet based on the information that is collected from Norton customers.

Your Norton product obtains specific information such as file name and hash key about the file and sends this information to the Symantec server. The Symantec servers analyze the file information and provide a trust level for the file. This reputation information is sent back to your computer. Based on the reputation information of the program, you can allow or block the inbound traffic or outbound traffic. If any of the file is suspicious or vulnerable, your Norton product assigns **Poor** or **Bad** trust level.

Your computer must be connected to the Internet to access the latest reputation information that Symantec collects. If your computer is not connected to the Internet, your Norton product uses the reputation information that is available locally.

In the left pane of the firewall alerts, you can find the following reputation information:

Prevalence	Shows the user prevalence of the file. This data is based on the information that millions of Norton Community Watch customers shared and Symantec's research analysis. The different categories are: ▪ **Very Few Users** Indicates that the file has very low user prevalence. ▪ **Few Users** Indicates that the file has average user prevalence. ▪ **Many Users** Indicates that the file has high user prevalence.
Age	Indicates the age of the file based on the data that millions of Norton Community Watch customers shared and Symantec's research analysis.

Trust Level

Shows the trust level of the file.

Symantec assigns the following trust levels:

- **Trusted** - Indicates the file that is Norton Trusted.
- **Good** - Symantec has high indications that the file is trusted.
- **Unproven** - Symantec does not have enough information about the file to assign a trust level to the file.

  The file is neither safe nor unsafe.
- **Poor** - Symantec has only a few indications that the file is not trusted.
- **Bad** - Symantec has very high indications that the file is not trusted.

  This file is suspicious and can harm your computer.

If the **Firewall Alert** window displays **Poor** or **Bad** reputation, Symantec recommends that you select the **Terminate** or **Block Always** option from the **Options** drop-down list. This action terminates or blocks all access attempts by the program or process. This program or process is suspicious and can harm your computer.

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, Chrome 17.0 or later, or Firefox 10.0 or later browsers.

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 Security 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, do one of the following:
   - To turn off Browser Protection, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Browser Protection, move the **On/Off** switch to the left to the **On** position.
5. Click **Apply**.
6. If you turned off Browser Protection, in the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Browser Protection.
7. In the Security Request window, click **OK**.
8. In the **Settings** window, click **Close**.

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 Download Intelligence

1. In the Norton Security 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 the right to the **Off** position.
5. In the **Settings** window, click **Apply**.
6. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Download Insight, and then click **OK**.
7. In the **Settings** window, click **Close**.

To turn on Download Intelligence

1. In the Norton Security 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 the left to the **On** position.

5 In the **Settings** window, click **Apply**, and then click **Close**.

Configuring the Download Insight Notifications option

You can use the **Download Insight Notifications** option to choose when you want Download Insight to display notifications.

By default, the **Download Insight Notifications** option is set to **On**. Based on the type of application you use to download your file, your Norton product does one of the following:

- Notifies you each time when you download an executable file.
- Notifies you only when you download a file that is infected with a local virus identification. If the file that you download is infected with a cloud virus identification, your Norton product removes the file from your computer and notifies you with the threat details.

When the **Download Insight Notifications** option is set to **Risks Only**, Download Insight notifies only when you download an infected or a suspicious executable file.

Setting the **Download Insight Notifications** to **Risks Only** does not turn off analysis of all the other executable files that you download. Whether or not you receive notifications of all files, Security History keeps a record of all the Download Insight activities. You can review the summary of the Download Insight alerts and notifications in Security History.

To configure the Download Insight Notifications option

1 In the Norton Security main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 Click the **Intrusion and Browser Protection** tab.

4 Under **Download Intelligence**, in the **Download Insight Notifications** row, do one of the following:

- To receive Download Insight notifications only for the infected or the suspicious executable files that you download, move the **Download Insight Notifications** switch to the right to the **Risks Only** position.
- To receive Download Insight notifications for all files that you download, move the **Download Insight Notifications** switch to the left to the **On** position.

5 In the **Settings** window, click **Apply**, and then click **Close**.

Configuring the Show Report on Launch of Files option

The **Show Report on Launch of Files** option lets you specify when and for what type of file you want to be prompted to select a suitable action. For example, you can specify the type of downloaded files for which Download Insight asks you to decide what to do with the file and how frequently these prompts for a suitable action must appear.

You can use the following options to configure **Show Report on Launch of Files**:

Always	When you set the **Show Report on Launch of Files** option to **Always**, Download Insight prompts you for a suitable action in case of safe and unknown files. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has a safe or an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. In the case of unsafe files, your Norton product identifies them as threats and removes them.

Unproven Only	When you set the **Show Report on Launch of Files** option to **Unproven Only**, Download Insight prompts you to select a suitable action for unknown files only. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. By default, the **Show Report on Launch of Files** option is set to **Unproven Only**. In this case, your Norton product allows the execution of the safe files without prompting you for a suitable action. In the case of unsafe files, your Norton product identifies them as threat and removes them.
Never	When you set the **Show Report on Launch of Files** option to **Never**, Download Insight does not prompt you to select a suitable action for any type of file that you download. In this case, the **Download Insight** window does not appear whenever you try to launch any downloaded file. The alert messages that you suppress and the activity details can be reviewed at any time in Security History.

To configure the Show Report on Launch of Files option

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. Click the **Intrusion and Browser Protection** tab.
4. Under **Download Intelligence**, in the **Show Report on Launch of Files** row, do one of the following:
   - If you want Download Insight to prompt you for a suitable action in case of safe and unknown files, move the **Show Report on Launch of Files** switch to the **Always** position.
   - If you want Download Insight to prompts you to select a suitable action for unknown files only, move the **Show Report on Launch of Files** switch to the **Unproven Only** position.
   - If you do not want Download Insight to prompt you to select a suitable action for any type of file, move the **Show Report on Launch of Files** switch to the **Never** position.
5. In the **Settings** window, click **Apply**, and then click **Close**.

Turning off or turning on Intrusion Prevention notifications

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks. Whether or not you receive notifications, Intrusion Prevention activities are recorded in Security History. The Security History entries include information about the attacking computer and information about the attack.

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks based on a particular signature.

To turn off or turn on Intrusion Prevention notifications

1. In the Norton Security 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 **Notifications** row, do one of the following:
   - Move the **On/Off** switch to the right to the **Off** position.
   - Move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**, and then click **Close**.

To turn off or turn on an individual Intrusion Prevention notification

1. In the Norton Security 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 Signatures** row, click **Configure**.
5. In the **Intrusion Signatures** window, click an attack signature, and then click **Properties**.
6. In the **Signature Properties** window, uncheck or check **Notify me when this signature is detected**.
7. Click **OK**.
8. In the **Intrusion Signatures** window, click **OK**.
9. In the **Settings** window, click **Apply**, and then click **Close**.

Excluding or including attack signatures in monitoring

In some cases, benign network activity may appear similar to an attack signature. You may receive repeated

notifications about possible attacks. If you know that the attacks that trigger these notifications are safe, you can create exclusion for the attack signature that matches the benign activity.

Each exclusion that you create leaves your computer vulnerable to attacks.

If you have excluded the attack signatures that you want to monitor again, you can include them in the list of active signatures.

To exclude attack signatures from being monitored

1. In the Norton Security 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 Signatures** row, click **Configure**.
5. In the **Intrusion Signatures** window, uncheck the attack signatures that you want to exclude, and then click **OK**.
6. In the **Settings** window, click **Close**.

To include the attack signatures that were previously excluded

1. In the Norton Security 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 Signatures** row, click **Configure**.
5. In the **Intrusion Signatures** window, check the attack signatures that you want to include, and then click **OK**.
6. 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.

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 you want to stop all traffic to and from your computer, you can use the **Block All Network Traffic** option.

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 Security 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 Security 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**.

Permanently blocking a computer that has been blocked by AutoBlock

You can permanently block a computer that has been blocked by AutoBlock. The permanently blocked computer is removed from the AutoBlock list and added as a Restricted computer in the Device Trust.

To permanently block a computer that has been blocked by AutoBlock

1. In the Norton Security 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**, click the computer that you want to block permanently.
6. Under the **Action** column, select **Restrict** from the drop-down list.
7. In the Intrusion AutoBlock window, click **OK**.
8. In the **Settings** window, click **Close**.

About Intrusion Prevention exclusion list

The Intrusion Prevention System in your Norton product scans all the network traffic that enters and exits your computer. When a device on your network requests access to your computer, Intrusion Prevention scans this request to ensure that it is not a virus attack. If the information matches an attack signature, Intrusion Prevention blocks the traffic from the suspicious device and protects your computer. Scanning every request from all the devices that access your computer increases the scan time which slows down the network speed of your computer.

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 configure the trust level of a device using the Device Trust under Network Settings. You can exclude these trusted devices from Intrusion Prevention scan. Excluding Full Trust devices from the Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a device that is set to Full Trust, 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.

When a device on your network attempts to infect your computer, AutoBlock stops all access requests from this device. If you add this device to the Intrusion Prevention exclusion list, your Norton product removes the device from the exclusion list.

Ensure that the IP address of the devices that are added to Intrusion Prevention exclusion list never changes.

If you find that any of the devices that you excluded from the Intrusion Prevention scan is infected, you can purge the saved exclusion list. When you purge the exclusion list, your Norton product removes all the IPS excluded devices from the exclusion list.

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. If you add this device to the Intrusion Prevention exclusion list, your Norton product removes the device from the exclusion list.

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 Security 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**

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

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 Security 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**.

Changing the trust level of your network and devices

The trust level determines the default level of access that devices on your network have to your computer. Any device on your network that is not explicitly Trusted or Restricted uses the trust level of your network. The initial network trust level is set based on the configuration of your computer.

Ensure that you change the trust level of a device to Full Trust, if it is a known device, and is connected to your network.

The following conditions are necessary for the trust level of a device to be Private:

- The computer should not have a public IP address.

  Your computer does not have a public IP address if it is not directly connected to the Internet.
- The computer should be connected to a LAN through a secure connection.
- The network category should be private in Windows Vista.

If you use a wireless network that is not secure, the default trust level of all the devices that are on the network is **Public**.

The trust level of a device also depends on the trust level of its network. When you change the trust level of a network, your Norton product assigns the same trust level to all the devices that are connected to that network. However, your Norton product does not change the trust level of the devices that you individually trust or restrict.

You can modify these settings if you want to change the trust level for the following:

- Your network
- Devices that are connected to your network

To change the trust level of your network

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **General Settings** tab, in the **Network Trust** row, click **Configure**.

4 In the **Network Trust** window, under **Trust Level**, choose one of the following:

Full Trust	Adds the network to the Full Trust list. All the network traffic that your computer receives from a Trusted network is filtered and allowed through firewall. However, known attacks and infections are still monitored. You should select this setting only when you are sure that the network is completely safe.
Private	Adds the network to the Private list. This setting lets you share files, folders, media, and printers on your computer with other devices on your network. You can set up remote desktop connections with other devices on your network. Your computer is protected from known attacks and all unexpected traffic.

Public	Adds the network to the Public list. Your Norton product blocks files, folders, media, and printer sharing, and remote desktop connections with other devices over the network by default. To share files, folders, media, and printers and set up remote desktop connection with devices over the network you can configure the **Traffic Blocking Exceptions** setting. You are protected from known attacks and all unexpected traffic.
Restricted	Adds the network to the Restricted list. The devices that are on Restricted network cannot communicate with your computer. However, you can still use the network to browse websites, send email messages, or transmit other communications.

5 Click **Apply**, and then click **OK**.

To change the trust level of a device

1 In the Norton Security 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, under **Trust Level**, choose one of the following for the device you want to configure:

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.

5 Click **Apply** and then click **OK**.
Your Norton product displays the trust level status of each restricted device on the icon of the device.

About the types of security risks

Security risks, such as spyware and adware, can compromise your personal information and privacy. Spyware and adware programs are closely related. In some cases, their functionalities might overlap; but while they both collect information about you, the types of information that they collect can differ.

Spyware programs might put you at risk for identity theft or fraud. These programs might log your keystrokes, capture your email and instant messaging traffic. These programs also steal sensitive personal information such as passwords, login IDs, or credit card numbers. These

programs can then send your compromised data to other people.

Adware displays advertisements on your computer and collects information about your web browsing habits. It then gives this data to companies that can send you advertisements based on these preferences.

Tracking cookies are the small files that programs can place on your computer to track your computing activities. Tracking cookies can then report that information back to a third party.

Some programs rely on other programs that are classified as security risks to function. For example, a shareware or freeware program that you download might use adware to keep its price low. In this case, you might want to allow the security risk program to remain on your computer. Also, you might need to restore the security risk program if Spyware Protection has removed it.

Norton Security allows joke programs and other low-risk items to be installed on your computer by default. You can change your settings in the **Settings** window so that Norton Security detects these security risks.

About Norton AntiSpam

Norton AntiSpam lets you categorize the email messages that you receive in your email programs into spam email and legitimate email. It filters legitimate email into the Inbox folder and spam email into the Junk folder or the Norton AntiSpam folder.

Norton AntiSpam uses Symantec enterprise-class, spam-filtering technology to classify the spam email messages from legitimate email messages. Norton AntiSpam uses a real-time filter delivery mechanism and filters email messages using various local filters at different levels. The local filters classify the email messages as spam or legitimate. If the local filters classify the email message as legitimate, Norton

AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Symantec web server for additional analysis.

When the email message is classified as spam, Norton AntiSpam changes the subject of the email message and sends it to your email client. The email client identifies the change in the subject of the email message and moves it to the Junk folder or the Norton AntiSpam folder.

The Norton AntiSpam local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as spam or legitimate. For these filters to work efficiently, Norton AntiSpam requires antispam definition updates at regular intervals through LiveUpdate. These updates contain signature information of spam and legitimate email messages. The updates also contain any new rule that Symantec creates to filter spam email messages.

Norton AntiSpam uses predefined email rules and the user-defined Allowed List and Blocked List, to expedite the scanning of email. It accepts email messages from the list of allowed email senders and blocks email messages from the list of blocked email senders.

Norton AntiSpam also automatically imports the lists of addresses from supported email programs during the initial integration. It helps you keep your list of allowed and blocked email senders in sync with your current address books. When Norton AntiSpam imports the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Turning off Norton AntiSpam increases your exposure to receive unsolicited email messages. Always ensure that Norton AntiSpam is turned on. It secures your email client from unwanted online content.

You can review all the antispam statistics under the **AntiSpam** category in the **Security History** window.

Configuring Client Integration

The **Client Integration** tab lists the supported email programs, or clients, that are installed on your computer and their associated address books. When you select an email program, your Norton product adds a **Norton AntiSpam** drop-down list or a few options to the toolbar of the supported email program. You can use the **Norton AntiSpam** drop-down list or the options to classify the email messages as spam or legitimate. You can also use these options to empty the spam folder and to open the **Settings** window to configure the Norton AntiSpam settings. If your email program does not have a Junk folder, it also adds a Norton AntiSpam folder in the folders area. You can use the Norton AntiSpam folder to sort and store spam messages. However, if your email client has a Norton AntiSpam folder from the previous version of your Norton product, Norton AntiSpam uses the Norton AntiSpam folder and not the Junk folder.

The following email clients do not support client integration:

- Thunderbird
- Windows Mail/Windows Live Mail
- Outlook Express

When you classify an email message as spam or legitimate, Norton AntiSpam lets you send the misclassified email message as feedback to Symantec. You can use the **Feedback** option to send the misclassified email message to Symantec for analysis.

You can also import the list of addresses that are present in the supported email program into the Norton AntiSpam Allowed List and Blocked List. Norton AntiSpam automatically adds the new email addresses from the address book of your supported email program once in a day when your computer is idle. However, if you want to manually import addresses, use the **Import** option in the **Allowed List** window.

When you open your email client, the welcome screen appears. If you do not want the welcome screen to

appear in the future, check the **Don't show this again** option before you click **Close**. Your Norton product notifies the successful integration of Norton AntiSpam with your email client.

Norton AntiSpam also automatically imports the lists of addresses from the supported email programs during the initial client integration. It helps you keep your list of allowed and blocked email senders in sync with your current address books. When Norton AntiSpam imports the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Your Norton product supports Norton AntiSpam integration with Microsoft Outlook 2002/2003/2007/2010/2013.

To configure Client Integration

1. In the Norton product main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Client Integration** tab, turn on or turn off the programs with which you want Norton AntiSpam to integrate.
4. Select one or more address books to be imported automatically into your Allowed List.
5. Click **Apply**, and then click **Close**.

Setting Address Book Exclusions

When you add an email address to the Address Book Exclusions list, Norton AntiSpam does not import the address into the Allowed List and Blocked List. If you delete an email address from the Allowed List or Blocked List, Norton AntiSpam automatically adds the address to the Address Book Exclusions list. However, when you delete an email address that you manually added to the Allowed List or Blocked List, Norton AntiSpam does not add the address to the Address Book Exclusions list.

You cannot add a domain name to the Address Book Exclusions list. When you delete a domain name from the Allowed List or Blocked List, Norton AntiSpam does not add the domain name to the Address Book Exclusions list.

You can specify Address Book Exclusions before you import the address book. Add all email addresses to the Address Book Exclusions list that you do not want to import from the address book of your email program.

To add entries to the Address Book Exclusions list

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 **Address Book Exclusions** row, click **Configure**.
4. In the **Address Book Exclusions** window, click **Add**.
5. In the **Add Email Address** dialog box, type the email address.
   Optionally, type the name that corresponds to the email address for easy identification.
6. Click **OK** to close the **Add Email Address** dialog box.
7. Click **OK** to save and close the **Address Book Exclusions** window.

To edit or delete entries in the Address Book Exclusions list

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 **Address Book Exclusions** row, click **Configure**.
4. In the **Address Book Exclusions** window, select the item with which you want to work.

5 Do one of the following:
- To edit an entry, click **Edit** to open the **Edit Email Address** window, edit the details, and then click **OK**.
- To delete an entry, click **Remove**.

6 Click **OK** to save and close the **Address Book Exclusions** window.

Identifying authorized senders

If you are sure that an email address or domain is safe and do not want Norton AntiSpam to block them, you can add them to the **Allowed List**

When your computer is idle, Norton AntiSpam automatically imports the address book entries and Safe Sender List entries once in a day.

If you have added a new supported email program, you can import its address book manually to your **Allowed List** immediately or at any time. You can also add names and domains to the **Allowed List** individually.

Before you import the address book, you can specify your Address Book Exclusions. Norton AntiSpam does not import the email addresses that you add to the **Address Book Exclusions** list.

To import an address book

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 **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, click **Import**.
5 In the **Allowed List** window, click **Apply**.
6 Click **OK**.

To add entries to your Allowed List

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 **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, click **Add**.
5 In the **Add Email Address** dialog box, in the **Address Type** drop-down list, select the address type.
You can select one the following options.
   - **Email**
   - **Domain**
6 Do one of the following:
   - To add an email address, type the email address that you want to allow, and optionally, the name of the sender.
   - To add a domain name, type the address of the domain (for example, symantec.com), and optionally, the name of the domain.
7 Click **OK**.
8 In the **Allowed List** window, click **Apply**.
9 Click **OK**

To edit or delete entries in the Allowed List

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 **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, select the item that you want to edit or delete.

5 Do one of the following:
- To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and click **OK**.
- To delete an entry, click **Remove**.

  When you delete an entry that was imported, Norton AntiSpam automatically adds it to the Address Book Exclusions list.

6 In the **Allowed List** window, click **Apply**.

7 Click **OK**.

Identifying senders of spam

If you do not want to receive any email messages from a specific address or domain, you can add it to the Blocked List. Norton AntiSpam marks all email messages from this address or domain as spam.

Norton AntiSpam also automatically imports the lists of addresses that are available in the Blocked Sender lists of your email program into the Blocked List during the initial client integration or address book import.

Norton AntiSpam lets you type invalid email addresses to the Blocked List.

Always add suspicious email addresses and domains to the Blocked List, so that you do not receive unsolicited email messages from such addresses or domains.

To add entries to the Blocked List

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 **Blocked List** row, click **Configure**.

4 In the **Blocked List** window, click **Add**.

5 In the **Add Email Address** dialog box, in the **Address Type** drop-down list, select the address type.
You can select one of the following:
- **Email**
- **Domain**

6 Do one of the following:
- To add an email address, type the email address that you want to block, and the name of the sender.
- To add a domain, enter the address of the domain (for example, symantec.com), and the name of the domain.

7 Click **OK**.

8 In the **Blocked List** window, click **Apply**.

9 Click **OK**.

To edit or delete entries in the Blocked List

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 **Blocked List** row, click **Configure**.

4 In the **Blocked List** window, select the item with which you want to work.

5 Do one of the following:
- To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and then click **OK**.
- To delete an entry, click **Remove**.
  When you delete an entry that was imported, Norton AntiSpam automatically adds it to the **Address Book Exclusions** list.

6 In the **Blocked List** window, click **Apply**.

7 Click **OK**.

Setting the Feedback option

Email messages in the email client might sometimes get wrongly classified as spam or legitimate. The **Feedback** option lets you send the misclassified email message as feedback to Symantec for analysis.

The **Feedback** option is available only when Microsoft Outlook is installed on your computer.

To set the Feedback option

1. In the Norton product main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Client Integration** tab, in the **Feedback** row, select any one from the following three options:

On	Automatically sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Ask Me	Prompts you before Norton AntiSpam sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Off	Does not send the misclassified email message to Symantec

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

About Web Query

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam

make it difficult to identify valid email messages, but some spam contains offensive messages and images. The Web Query is a feature of Norton AntiSpam that your Norton product uses to classify the email messages more effectively.

An effective spam filtration is possible when each email message that you receive is scanned through different filters. With only one or two levels of email filters, a high percentage of legitimate emails are misclassified as spam or spam is misclassified as legitimate. To avoid such misclassification, Norton AntiSpam employs different filters. Each email filter uses a unique approach to filter spam email messages from legitimate email messages.

The email messages that you receive in your email program undergo scanning through different local filters of Norton AntiSpam. The local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as legitimate or spam. If the local filters classify an email message as spam, Norton AntiSpam changes the subject of the email message. Norton AntiSpam then sends the email message to your email client. If the local filters fail to classify the email message as spam, Norton AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Web Query filter for additional analysis.

The Web Query filter analyzes the signature and URL hashes of the email message and then sends the analysis report to Norton AntiSpam. If the email message is identified as spam, Norton AntiSpam alters the subject of the email message and sends it to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends that you keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

Turning off or turning on Web Query

Norton AntiSpam uses local filters to identify spam email messages. The email messages that the local filters do not identify as spam are then scanned additionally through the Web Query filter. Web Query filter analyzes the signature and URL hashes of the email messages to classify them as legitimate email or spam email.

If the email message is identified as spam, then Norton AntiSpam alters the subject of the email message. Norton AntiSpam then sends the email message to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends you to keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

To turn off the Web Query filter

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 **Web Query** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**, and then click **Close**.

To turn on the Web Query filter

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 **Web Query** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

Adding POP3 and SMTP ports to Protected Ports

The Norton product automatically protects the default POP3 and SMTP ports to protect your email program from viruses and other security threats.

The Norton product supports all email accounts that use non-SSL POP3 and SMTP communication protocols and does not support SSL-encrypted email ports. The Norton product also scans all incoming and all outgoing email messages.

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. This helps protect your email program from viruses and other security threats.

If the port numbers of your email program are not added to the **Protected Ports** window, your email program is not protected. Your Internet service provider (ISP) provides you the port numbers for your email program.

You can add only the port numbers that are not assigned to any other protocols by Internet Assigned Numbers Authority (IANA). The standard ports that are assigned to other protocols by IANA are blocked. For more information, see IANA website.

To add POP3 and SMTP ports to Protected Ports

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Filter** tab, in the **Protected Ports** row, click **Configure**.
4. In the **Protected Ports** window, click **Add**.

5 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**.
6 In the **Port** box, type the port number.
   The port number must be between 1 and 65535.
7 Click **OK**.
8 In the **Protected Ports** window, click **Apply**, and then click **OK**.
9 In the **Settings** window, click **Close**.

Removing an email port from Protected Ports

If you do not want your Norton product to protect a port, you can remove the port from the **Protected Ports** window.

The Norton product automatically protects the default SMTP port 25 and the default POP3 port 110. You cannot remove the default ports.

To remove an email port from Protected Ports

1 In the Norton Security main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Protected Ports** row, click **Configure**.
4 In the **Protected Ports** window, click the port that you want to remove, and then click **Remove**.
5 Click **Apply** and then click **OK**.
6 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 Norton Security. If you do not want to restrict the Internet usage of Norton Security, you can turn off **Network Cost Awareness**.

If you feel that Norton Security uses too much network bandwidth, you can turn on **Network Cost Awareness**. Then, you can set up policies to restrict the Internet usage of Norton Security. 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 Network Cost Awareness

1. In the Norton Security 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 the right to the **Off** position.
4. In the **Settings** window, click **Apply**, and then click **Close**.

To turn on Network Cost Awareness

1. In the Norton Security 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 the left to the **On** position.
4. In the **Settings** window, click **Apply**, and then click **Close**.

Defining the Internet usage of Norton Security

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

To define the Internet usage of Norton Security

1. In the Norton Security 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 the left to the **On** position.
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 Security to receive all product and virus definition updates based on the Windows 8 cost awareness policy. By default, the **Auto** policy has unlimited Internet connection on LAN and Wi-Fi.

  The **Auto** option is available only in Windows 8.

- **No Limit**

  Allows Norton Security use the network bandwidth that is required to receive all product and virus definition updates. If you do not use Windows 8, the default policy is set to **No Limit**.

- **Economy**

  Allows Norton Security access the Internet only to receive critical product updates and virus definitions.

  If you have a limited Internet connection, you can select the **Economy** option to ensure protection from critical security threats.

- **No Traffic**

  Blocks Norton Security from connecting to the Internet. If you choose this policy, Norton Security 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**.

Securing your sensitive data

7

This chapter includes the following topics:

- About Norton Safe Web
- About Antiphishing
- About Identity Safe
- About Norton toolbar
- Norton Identity Safe

About Norton Safe Web

Norton Safe Web helps you surf, search, and shop more safely on the Internet. By using Norton Safe Web, you can check if a website is malicious or not even before you visit it. Norton Safe Web analyzes the websites you visit and detects if there are any viruses, spyware, malware, or other security threats that exist on the websites. Based on the analysis, Norton Safe Web provides safety ratings for all the websites.

In addition, Norton Safe Web lets you view the community rating and user reviews of the websites you visit.

Norton Safe Web supports Internet Explorer, Firefox, or Chrome browsers.

You can view the site safety status of any website using the **Full Safe Web Report** option on the **Norton Safe Web** pop-up window.

For each website that you want to know the site safety status, Norton Safe Web lets you do the following:

- View the Norton rating.
- View the community rating.
- Add your reviews.
- View the user reviews.
- View a list of keywords that are tagged to the website.
- View the threat information and the general information about the website.

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

When you search the Internet using Google, Yahoo, or Bing search engines, Norton Safe Web displays the site rating icons next to the search results. As you move the mouse pointer over the Norton icon, a pop-up appears with site safety and shopping safety information. The pop-up displays brief information about the safety of the site. Norton Safe Web also provides a detailed report about the safety of the websites you visit.

You can click the icon next to the search results or the **Full Safe Web Report** option in the **Norton Safe Web** pop-up window to view the detailed report. The report is displayed on the Norton Safe website.

Norton Safe Web provides the following website safety states when you browse through the Internet:

SECURE	You can see Norton Secured icon next to the search results. Symantec has analyzed this page and determined that the website is VeriSign trusted and is safe to visit.

SAFE	You can see a green OK icon next to the search results. When you visit a website with this status, you can see a similar status icon on the **Norton toolbar**. Norton Safe Web has analyzed this website and determined that it is safe to visit.
UNTESTED	You can see a gray question mark icon next to the search results. When you visit this website, the **Norton toolbar** shows a green OK icon. Norton Safe Web has not analyzed this website and it does not have sufficient information about this website. As Symantec has not tested the website, it is recommended that you do not visit this website.
UNSAFE	You can see a red cross (x) icon next to the search results. When you visit a website with this status, you can see a similar status icon on the **Norton toolbar**. Norton Safe Web has analyzed this website and determined that the website is unsafe to visit. This website may attempt to install malicious software on your computer.

CAUTION	You can see an orange exclamation mark icon next to the search results. When you visit a website with this status, you can see a similar status icon on the **Norton toolbar**. Norton Safe Web has analyzed this website and determined that this website has some threats that are classified as **Annoyance Factors**. These annoyance factors are not dangerous, but it can install unwanted applications on your computer without your permission.

In addition to the site safety information, Norton Safe Web provides the online shopping safety information in the **Ecommerce Safety Information** session.

When you visit any website that has an unsafe status, Norton Safe Web blocks that webpage. If you still want to view the website, use the **Continue to site anyway** option that appears on the blocked page.

You can block malicious pages using the **Block Malicious Pages** option under the **Safe Surfing** section of the **Identity Protection Settings** window.

If you turn off this option, Norton Safe Web does not block the unsafe websites. However, **Norton toolbar** displays the status of these sites as unsafe even when the option is turned off.

In addition, Norton Safe Web protects your computer while you use Facebook. It scans each URL that is available on your Facebook wall and displays the Norton rating icons for the scanned URLs. You can also let other Facebook users know about the security status of any website.

To scan your Facebook wall using Norton Safe Web, use the **Scan Facebook Wall** option in the **Scans** window. The option appears when you click the **Run Scans** option in the **Tasks Scans** window.

Turning off or turning on Norton Safe Web

Norton Safe Web protects your computer while you browse the Internet using Internet Explorer, Firefox, or Chrome browsers. It analyzes the security levels of the websites that you visit and indicates if the websites are free from threats. It provides you a safe environment on the web by displaying the site rating icons next to each search result. The site rating icons lets you know if a website is malicious or not even before you visit it.

You can turn off or turn on Norton Safe Web in the **Safe Surfing** section under **Identity Protection** settings window.

To turn off or turn on Norton Safe Web

1. In the Norton Security main window, double-click **Identity**, and then click **ID Settings**.
2. Under **Safe Surfing**, in the **Norton Safe Web** row, do one of the following:
   - To turn off Norton Safe Web, move the **On**/**Off** switch to the right to the **Off** position.
   - To turn on Norton Safe Web, move the **On**/**Off** switch to the left to the **On** position.
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.

When you install Norton Security, it adds the **Norton Safe Search** box to the browsers. The supported browsers are Internet Explorer, Firefox, and Chrome.

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.

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.

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.

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 Security main window, double-click **Identity**, and then click **ID Settings**.
2. Under **Safe Surfing**, in the **Scam Insight** row, do one of the following:
   - To turn off Scam Insight, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Scam Insight, move the **On/Off** switch to the left to the **On** position.
3. Click **Apply**, and then click **Close**.

About Antiphishing

Antiphishing protects you from visiting unsafe websites. When Antiphishing is turned on, the Antiphishing component analyzes the security level of the websites that you visit. It then displays the results in the **Norton Safe Web** pop-up window. Antiphishing also blocks navigation to the websites that are confirmed to be fraudulent or suspicious.

Antiphishing provides you the following information about the websites you visit:

- If the website is safe to enter confidential information
- If the website is fraudulent
- If the website is suspicious
- If the website is known to give annoying results

The **Norton Safe Web** pop-up window in Internet Explorer, Firefox, or Chrome browsers lets you view more details about the safety status of the websites you visit.

In addition, the **Norton Safe Web** pop-up window includes information about Norton Secured websites. Website hackers often mimic company websites to create fraudulent websites. Antiphishing identifies the fraudulent websites.

Symantec analyzes the pages of these sites and verifies if they belong to the company that it represents. You can be confident that the information that you provide goes to the company with which you want to do business.

Even when you turn off the **Antiphishing** option, your computer is protected from Internet threats using the Norton Safe Web feature. However, you cannot use the **Report this site** option to submit the evaluation of the website to Symantec.

The **Norton Safe Web** pop-up window displays the following messages:

Icon	Message
SECURE	You can see Norton Secured icon next to the search results. Symantec has analyzed this page and determined that the website is VeriSign trusted and is safe to visit.
SAFE	You can see a green OK icon next to the search results. When you visit a website with this status, you can see a similar status icon on the Norton toolbar. Norton Safe Web has analyzed this site and determined that it is safe to visit.

Icon	Message
UNTESTED	You can see a gray question mark icon next to the search results. When you visit this website, the Norton toolbar shows a green OK icon. Norton Safe Web has not analyzed this site and it does not have sufficient information about this site. As Symantec has not tested the site, it is recommended that you do not visit this site.
UNSAFE	You can see a red cross (x) icon next to the search results. When you visit a website with this status, you can see a similar status icon on the Norton toolbar. Norton Safe Web has analyzed this page and determined that the site is unsafe to visit. This website may attempt to install malicious software on your computer.

Icon	Message
CAUTION	You can see an orange exclamation mark icon next to the search results. When you visit a website with this status, you can see a similar status icon on the Norton toolbar. Norton Safe Web has analyzed this site and determined that this site has some threats that are classified as Annoyance Factors. These annoyance factors are not dangerous, but it can install unwanted applications on your computer without your permission.

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 Security main window, double-click **Identity**, and then click **ID Settings**.

2 Under **Safe Surfing**, in the **Antiphishing** row, do one of the following:
   - To turn off Antiphishing, move the **On**/**Off** switch to the right to the **Off** position.
   - To turn on Antiphishing, move the **On**/**Off** switch to the left to the **On** position.
3 Click **Apply**.
4 If prompted, select the duration until when you want the Antiphishing feature to be turned off, and click **OK**.

Reporting an incorrect evaluation of a website

On rare occasions, Antiphishing may report incorrect evaluation of a website. For example, you might visit a site that you shop with regularly and Antiphishing reports that the site is fraudulent. On the contrary, you might visit a website that you suspect is a phishing site, but Antiphishing reports that no fraud was detected. In either case, you can report the website to Symantec for further evaluation.

To report an incorrect evaluation of a website

1 Open your browser and go to the website that you think is evaluated incorrectly.
2 On the Norton toolbar, click **Norton Safe Web Indicator**.
3 In the pop-up that appears, click **Report this site**.
4 In the confirmation dialog box, click **Submit**.

About Identity Safe

Identity Safe helps you manage your identities and provide additional security while you perform online transactions.

The following features in Identity Safe provide secure storage of your sensitive information:

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

In addition to being a depository of sensitive information, Identity Safe provides the following features:

- Protects you from identity theft when you perform online transactions.
- Lets you easily manage multiple credit card information.
- Provides you the ease of carrying and using your Identity Safe data when you are on the move.

  By saving your data using a cloud vault, you can access your sensitive Identity Safe data from any computer that has Norton Security installed or through the Identity Safe website.

Norton Security adds the **Norton toolbar** to the Internet Explorer, Firefox, and Chrome browsers. The **Norton toolbar** has the following components:

- **Norton Safe Search**

- **Safe Web** indicator
- **VAULT IS OPEN/VAULT CLOSED** menu
- **SHARE VIA**
- Norton Toolbar settings

When you have logins in Identity Safe, the **VAULT IS OPEN** menu displays the entire list of logins stored in the Identity Safe. Instead of you have to access a website and to enter the login information, you can directly click a login from the stored list to access the website.

If you turn off Identity Safe, you cannot access your logins and Identity Safe features from the Norton toolbar.

You can access Identity Safe even after the product expires. However, the product might not detect the latest attacks, as the virus definition is not updated after the product expires. Hence, it is not safe to browse the Internet after Norton Security expires as you are vulnerable to online thefts and phishing attacks.

About setting up Norton Identity Safe account

Identity Safe helps you manage your sensitive information and provide additional security while you perform online transactions. Identity Safe provides a secure storage for your personal information such as your address, login information, passwords, and credit card details.

Identity Safe lets you store the following:

- Login information such as user IDs and passwords of your email accounts
- Personal information such as your address, date of birth, passport number, and social security number.
- Credit card details including card number and card expiry date.

You can store your sensitive information only after you set up Identity Safe and create your 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 Norton Security. When you move your Identity Safe data from local vault to cloud vault, the data in your local vault is permanently removed.

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

The Identity Safe data is stored online using your Norton account. You can create only one cloud vault for a Norton account.

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**.

After you turn on Identity Safe, you must log in to Identity Safe to access the various features.

To turn off or turn on Identity Safe from Quick Controls

1. In the Norton Security 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 Security main window, double-click **Identity**, and then click **ID Settings**.

2 In the **Identity Protection** settings window, in the **Identity Safe** row, do one of the following:
   - To turn off Identity Safe, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Identity Safe, move the **On/Off** switch to the left to the **On** position.

3 Click **Apply**, and then click **Close**.

About Identity Safe vaults

Identity Safe lets you create a cloud vault and save all your sensitive 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 Norton Security. 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.

When you access Identity Safe for the first time, you must sign in to Identity Safe using your Norton account credentials. If you do not have a Norton account, you can click **Sign in** to create a Norton account.

After you sign in to Norton account, you must create your Identity Safe cloud vault. You must provide a password to create your cloud vault. We recommend you to set a strong password for your cloud vault, as it is a depository of all your sensitive information. To access your vault, you need to enter your Norton account credentials and the vault password.

When you set up a cloud vault, Identity Safe automatically imports the logins that you have saved in Internet Explorer. The imported logins appear in the **VAULT IS OPEN** menu on the Norton toolbar and in the **Logins** window.

Internet Explorer version 10 does not allow Identity Safe to import the login details.

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

In addition to the features such as saving logins, cards, and notes, you can do the following using your Identity Safe vault:

- Import your Identity Safe data from the file you already backed up. You can also import the data that you stored in portable profile from an older version of the product to the current version.
- Export your Identity Safe data to .DAT file.
- Reset your Identity Safe.

  Symantec does not store your Vault password. As only you know the vault password, no one including Symantec can see your Vault data. In case you forget your Vault password, Symantec cannot retrieve it for you. You only need to reset your vault by deleting your existing Vault and creating a new one. In such cases, we use your Norton account password to validate your request to delete your Vault.

See "Signing in to cloud vault" on page 213.
See "Resetting Identity Safe" on page 216.

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 Norton Security. 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 Security 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**.

Signing in to cloud vault

Identity Safe lets you create a cloud vault to save your Identity Safe data. You must log in to your Norton account to create a cloud vault. The Identity Safe data is stored online using your Norton account.

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

You can create only one cloud vault per Norton account. If you already have a Norton account, you can log in with your credentials or create a new account.

Using your Norton product, you can access vaults created using multiple Norton account. You can use **Account Menu** available at the bottom of the **Norton Identity Safe** window to access vaults associated to multiple Norton accounts.

If you forget your cloud vault password, you can use the **Show password hint** link to get the password hint. If you still cannot recollect your password, for security

reasons Norton forces you to delete the existing vault and create a new vault.

When you type the wrong password for three times, the **Need to delete your Vault? click here** link is displayed. You can use the link to delete the vault. To delete your vault you need to provide your Norton account credentials.

To sign in to cloud vault from the Settings window

1. In the Norton Security main window, double-click **Identity**, and then click **ID Settings**.
2. In the **Identity Safe** row, click **Configure**.
3. In the **Get started** window, click **Sign in**.
4. Enter your Norton account credentials and click **Sign In**.
5. In the **Vault Closed** window, type your cloud vault password.
6. Click **Open**.

To sign in to cloud vault from Norton toolbar

1. Open your browser.
2. On the Norton toolbar, click **VAULT IS CLOSED**.
3. In the **Get started** window, click **Sign In**.
4. Enter your Norton account credentials and click **Sign In**.
5. In the **Vault Closed** window, type your cloud vault password.
6. Click **Open**.

To sign in with a different Norton account

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the **Vault Closed** window, click **Account Menu** available at the bottom of the window.
3. Select **Sign in as a different user**.
4. In the **Get started** window, click **Sign in**.
5. Enter a different Norton account credential and click **Sign In**.

6 In the **Vault Closed** window, type your cloud vault password.

7 Click **Open**.

Syncing local vault to cloud vault

You can sync the Identity Safe data from your local vault to the cloud vault. When you move the data from your local vault to cloud vault, all the data in your local vault is removed permanently.

The latest versions of Norton Security support only the cloud vault feature. If you have local vault created using the earlier versions, you need to move your local vault to cloud. You can no longer continue to use local vault. You can use the **Merge** option in the **Go Cloud?** window to move your local vault to cloud.

The **Go Cloud?** window is enabled only when you have created a local vault.

The following are the benefits of moving your Identity Safe data online:

- Lets you access your Identity Safe data from any computer.

  Your computer must have the Norton Security installed and must be connected to the Internet.

- Lets you access your Identity Safe data on any device through the Norton Identity Safe website.
- Provides a convenient means to automatically synchronize Identity Safe data across different computers using your Norton account.

You must log in to your Norton account to move the Identity Safe data from your local vault to cloud vault.

To sync local vault to cloud vault

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 In the **Norton Identity Safe** window, under **Sign In or create account** type your Norton account email address, and click **Next**.

3 In the **Go Cloud?** dialog box, click **Yes, Convert**, to set up your cloud vault.
You can also click **No, Stay local** for now and use the **Convert to Cloud Vault** option available in the **General** tab of Identity Safe Settings window to move your local vault to cloud vault.

4 In the **Cloud Vault: Norton account** window, enter your details and click **Agree & sign Up**.

5 Once you receive the setup complete message, click **Finish**.

6 In the **Cloud vault setup complete** dialog box, do one of the following:
- Click **Merge** to delete your local vault, and sync your local vault with the cloud vault.
- Click **Keep Both** to retain your local vault along with your cloud vault.

7 In case if you have different passwords for the local vault and cloud vault, Norton Security displays a confirmation message. Select one of the following:
- Click **Keep Existing Password** to retain the password stored in the cloud vault.
- Click **Keep Imported Password** to overwrite the password stored in the cloud vault with the password stored in the local vault.

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

Resetting Identity Safe

You may need to reset your Identity Safe in the following occasions:

- You experience a computer failure.
- You forget your Identity Safe password.

If you forget your Identity Safe password, you cannot recover it. You can only reset your Identity Safe by deleting your Identity Safe vault and store all your data again.

If you enter an incorrect password for three times, Identity Safe provides you an option to delete your vault.

If you delete the vault, you lose all the Identity Safe data that you stored, such as your login information, address, cards, and notes.

To delete your vault and reset your Identity Safe

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the **Vault Closed** dialog box, type your Identity Safe password.
   If you enter an incorrect password for three times, the **Need to delete your Vault? click here** option appears.
3. Click **click here** available next to the **Need to delete your vault?** option.
4. In the **Delete Vault** window, click **Yes, Delete My Vault**.
5. In the waning dialog box, click **Yes**.
6. Type your Norton account password and click **Sign In**.
7. In the confirmation dialog box, click **OK**.
8. In the **New Vault creation: Vault password** window, in the **Vault Password** box, type your password, and then click **Next**.
9. In the **New Vault creation: confirm password** window, type the password again to confirm and then click **Next**.
10. In the **New Vault creation: password Hint** box, type a hint for the password and then click **Next**.
11. Click **Finish**.

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.

You must be logged 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.

Logging in and logging out of Identity Safe

You can log in to or log out of Identity Safe from the following areas:

- The **Identity** section in the Norton Security main window
- The **Identity Safe** section in the Identity Protection **Settings** window
- The **Account Menu** option at the bottom of the **Norton Identity Safe** window

- The Norton toolbar

To secure your Identity Safe data from others, log out of Identity Safe whenever you are away from your computer.

To view or edit your confidential data, you must be logged in to Identity Safe.

To log in to Identity Safe

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe.**
2. In the **Vault Closed** window, in the **Enter Vault Password to Open** box, type the vault password.
3. Click **Open**.

To log out of Identity Safe

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the **Norton Identity Safe** window, click on the slider switch available at the bottom of the window to the left.

To log in to Identity Safe from the Norton toolbar

1. Open your browser.
2. On the **Norton toolbar**, click **VAULT IS CLOSED**.
3. In the **Vault Closed** window, type your vault password.
4. Click **Open**.

To log out of Identity Safe from the Norton toolbar

1. Open your browser.
2. On the Norton toolbar, click the **VAULT IS OPEN** menu available at the bottom, and then click **Close Vault**.

Configuring Identity Safe settings

You can use the various features in Identity Safe to manage your personal sensitive information. You can configure Identity Safe in such a way to access it from

various devices and make it work more effective and smart.

To configure Identity Safe settings

1 In the Norton Security 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. Your options are:

General	Lets you configure the Norton toolbar settings. **Toolbar Options**: You can enable or disable the Norton Safe Web feature. By default, the option is turned on. **Browser Extensions**: You can view the status of the Norton toolbar that is installed in the following browsers: ▪ Internet Explorer ▪ Google Chrome ▪ Mozilla Firefox Status indicates if the Norton toolbar is successfully enabled on the browser or you need to manually enable it. You can use the open browser settings link to enable the toolbar. You can configure the **General** settings even without logging in to vault.

Import/Export	Lets you import and export the Identity Safe data that is stored in the vault. **Import Vault**: You can import data from the backed up or exported file. When you import the Identity Safe data you have the following options: ▪ **Merge the imported data with existing data** ▪ **Replace existing data with imported data** **Export Vault**: You can back up the Identity Safe data in .DAT or .CSV file formats. You can select one of the following: ▪ **Identity Safe Backup Format – DAT File** ▪ **Plain text – CSV file (Logins & Notes only)** Symantec recommends that you back up all of your Identity Safe data periodically. When you export your data, provide password to keep your Identity Safe data from being misused. **Automatic Backup**: Your vault is backed up automatically and stored locally in your device. To disable automatic backup, uncheck **Enable automatic backups**. By default, this option is enabled. The backed-up vault files are stored in the following system location: **Users\<User Name>\My Documents\Norton Identity Safe Backups\<Norton account name>**. To access the backed-up vault files, click the **here** link.

Security	Lets you change your Identity Safe password and configure the security levels for your password. Your options are: **Vault Access**: You can configure the following security settings to open and close your vault. Your options are: ▪ **Ask for my password at the beginning of each Login session**: Prompts you to enter your vault password each time you access Identity Safe. Symantec recommends that you use this option to make your login credentials more secure. ▪ **Ask for my password before filling a login or form**: Prompts for your Identity Safe password with every online form before it autofills any login. You can specify that individual logins require the entry of your Identity Safe password before autofill. ▪ **Close vault after *minutes* minutes of inactivity**: Automatically logs you out of Identity Safe when do not use your Identity Safe for a specified time period. You can set the idle timeout period as 15, 30, or 45 minutes. This option is useful if you are frequently in an area where other people have access to your computer. ▪ **Close Vault upon sleep**: Automatically logs you out of Identity Safe when your system is in suspended state. **Vault Password**: Lets you change the vault password. Using the **Change Vault Password** option, you can change your Identity Safe vault password and set a new password hint.

Browsing	**Login Saving**: Lets you configure Norton Identity Safe to save and fill your login credentials. Your options are: ▪ **Save my credentials when I log in to a website**: Lets you save the login credentials for the websites that you visit. Your options are: Always, No, or Ask. ▪ **Turn off the browser's password manager**: Lets you specify how you want the browser's password manager to work. Your options are: **Yes**, **No**, or **Ask**. **Infobar**: Lets you configure Norton Identity Safe to display the list of identities in the infobar. Your options are: ▪ **Display my Logins when I have multiple Logins for one site**: Displays your logins each time you visit a website that has multiple logins. ▪ **Display my fill options each time I visit a page with a form**: Displays the Addresses each time you visit a webpage with forms to fill your personal details. ▪ **Prompt me to open my Vault**: Prompts you to open your vault each time you visit a website with fields to fill in. **Filling**: Lets you configure Norton Identity Safe to fill your identities automatically when you visit a website. Your options are: ▪ **Auto-fill my Logins when I visit websites**: You can enable the option to automatically fill your login details when you visit a website. ▪ **Auto-fill on sites containing security threats**: Lets you specify how you want Identity Safe to respond to the websites that have security threats. Your options are: **Yes**, **No**, or **Ask**.

About Logins

The **Logins** feature in Identity Safe lets you view all the logins that you have stored in Identity Safe. Login

information includes login credentials of your emails, Internet banking, social networking, and online shopping.

Identity Safe provides you the option to save your logins when you enter your login information in a website's login page. You can instantly save your login information in Identity Safe.

To manage your logins, you must be logged in to Identity Safe.

Identity Safe offers the following features:

- Safely stores website login information
- Lets you save multiple IDs or accounts and passwords for a website
- Intelligently searches for a specific login
- Lets you save the website name with a name other than the default name
- Displays the login ID and lets you show or hide the password
- Displays the strength of the password for your login
- Lets you quickly launch the website login page
- Fills in your login automatically when you revisit websites
- Lets you manually add logins
- Lets you change the URL of your saved logins
- Lets you access the login features that you saved for a website even after Norton Security expires.

The Identity Safe features are supported in the Internet Explorer, Firefox, and Chrome browsers.

If your vault is closed when you access a website that requires your login details, Norton Identity Safe automatically opens the Infobar. In the Infobar, you can enter your vault password and then choose the login to use on the website.

The Infobar is shown only if you click on a field in a website that requires your login details.

You can use the **VAULT IS OPEN** menu that is available on the **Norton toolbar** to view and autofill the details of

the saved logins. If you have saved multiple logins for a same website, you can also choose a login from the drop-down list.

You need to validate your vault password for managing the login credentials, if you have selected **Require Vault password** option in the **Logins** window.

Saving Logins

Norton Identity Safe automatically saves your login details when you enter them for the first time. After Identity Safe saves a login, it automatically fills the login details next time you visit the website.

You must be logged in to Identity Safe to save and autofill passwords. If the password or user name field is blank, Identity Safe does not prompt you to save the login.

If you do not want your logins to be saved automatically, you can configure the **Save my credentials when I log in to Websites** option in the browsing window. You can set **Always**, **No**, or **Ask**. By default, this option is set to **Always**.

After Identity Safe saves a login, it automatically fills the login details next time you visit the website.

To save additional logins for a website

1. Go to the webpage for which you want to save another login.
   Your login credentials automatically appear on the webpage.
2. Clear the login credentials that appear on the webpage.
3. Type the new login, and then click the option or link that logs you in.
4. In the prompt **Do you want to replace your saved Login for this site?**, click **Save New**.

You can see this prompt only for the first additional login that you save for the same website.

5 On the infobar, in the **Do you want to replace your saved Login for this site?** confirmation message that appears, click **Save** to add the newly entered login details.

6 Enter a reference name for the new login in the **Save as** text box, and click **Save**.

Managing Logins

Identity Safe lets you add a new login or change the title, URL, user name, and password for the logins that you have saved in the **Logins** window. The updated information is automatically filled the next time you visit that webpage.

You can use the arrow available next to the URL to quickly launch a login webpage.

To add a login manually

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 Click the drop-down menu at the top of the window and choose **New Login**.

3 In the **CREATE LOGIN** window, in the **Title** box, type a name for the login.

4 In the **Tags** box, type the category of the login.

5 In the **Login URL** box, type the URL of the website. Ensure that you prefix the URL with HTTP or HTTPS.

6 In the **Username** dialog box, type the user name of the login.

7 In the **Password** box, type the password of your login.

8 Use the following options to configure the login security:

Require Vault password	Prompts for your Identity Safe password before it autofills any login. You should select this option to make your login credentials more secure. For example, you can use this option for your online banking website.
Auto-fill	Automatically fills your login for the website when you visit. Symantec recommends that you select this option to fill the login information for the webpage.
Auto-submit	Automatically logs you in to the website.

9 Click **Save**.

To edit a login

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2 In the left pane, click **Logins**.
3 Click the login that you want to edit.
You can use **Sort by** option available at the top of the **Logins** pane to locate a login faster. You can also directly search for a login in the **Search your Vault box**.
4 In the window that appears, click **Edit** and do the required changes.
5 Click **Save**.

To delete a login

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the left pane, click **Logins**.
3. Click the login that you want to delete.
   You can use **Sort by** option available at the top of the **Logins** pane to locate a login faster. You can also directly search for a login in the **Search your Vault box**.
4. In the window that appears, click **Delete**.
5. In the warning dialog box, click **Yes**.

About Addresses

The Addresses feature lets you view all the personal information that you want Identity Safe to manage. Personal information includes information such as name, date of birth, postal address, email address, and phone numbers.

Identity Safe provides you the option to save your identities when you fill your personal information in a website form.

To manage your addresses, you must be logged in to Identity Safe.

You can use the information that you store in the addresses to do the following:

- Automatically fill forms
- Provide sensitive information without having to type it while you are online

In this way, Identity Safe protects your Identity Safe data from being stolen or misused.

When you click on a field in an online form, Norton Identity Safe opens Infobar that seeks your permission to automatically fill the form. On the Infobar, you can choose the address that you want to use and then click **Fill**. If you do not want to see the Infobar again on the online form, click **Don't Ask**. You can open the Infobar

anytime using the option **VAULT IS OPEN** > **OPTIONS** > **Show Infobar for this site**.

Managing Addresses

Identity Safe lets you add a new address detail or change the saved details.

All the addresses you have saved are listed in the **Addresses** window. You can edit the details of any address that you have saved. You can also delete an address if it is no longer needed.

To add an address

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. Click the drop-down menu at the top of the window and choose **New Address**.
3. In the **CREATE ADDRESS** window, select the region and enter your personal information such as, name, sex, date of birth, address, and contact information.
4. Select **Require Vault Password** to prompt for your Identity Safe password before it autofills your address in the website.
5. Click **Save**.

To edit an address

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the left pane, click **Addresses**.
3. In the **Addresses** window, click the address that you want to edit.
   You can use **Sort by** option available at the top of the **Addresses** pane to locate an address faster. You can also directly search for an address in the **Search your vault**.
4. If you are prompted to provide a password, type your vault password, and then click **OK**.
5. Click **Edit** and modify the required details.
6. Click **Save**.

To delete an address

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. In the left pane, click **Addresses**.
3. In the **Addresses** window, click the address that you want to delete.
   You can use **Sort by** option available at the top of the **Addresses** pane to locate an address faster. You can also directly search for an address in the **Search your vault**.
4. If you are prompted to provide a password, type your vault password, and then click **OK**.
5. Click **Delete**.
6. In the **Warning** dialog box, click **Yes**.
   You need to validate your vault password for deleting the address, if you have selected **Require Vault password** option when you created the address.

About Wallet

The **wallet** option in Identity Safe lets you manage your financial information, such as card information, bank account information, and credit payment details.

You can use the wallet to do the following:

- Automatically fill credit card or bank details whenever you do online transactions.
- Choose any card details for use with websites.
- Secure your financial information while you are online.

In this way, Identity Safe protects you from keyloggers that steal and misuse your identity. Banking and other e-commerce websites have forms with fields for credit cards or other financial information. When you click on a field in such websites, Norton Identity Safe opens Infobar that seeks your permission to automatically fill the form. On the Infobar, you can choose the payment that you want to use and then click **Fill**.

You can also use the Open Fill Assistant icon in the **VAULT IS OPEN** menu to list the payments that you saved. You can then select a payment, and drag and drop the details on to the form.

You can use the sort option to arrange the payments based on the name, modified date, and used date. You can also search for payments saved in your vault.

In addition, wallet provides you the following features:

- Lets you protect the financial information by adding one more level of security.
- Recognizes the webpages that have forms and immediately displays a pop-up window with the list of cards.
- Provides you a quick view of any of your cards and bank accounts that is not password-protected. Identity Safe provides additional security for your password-protected wallet by not displaying the summary of the wallet.

Adding Wallet

You can create a wallet to add details of a card, bank account, or payment. As the wallet comprises of all the sensitive financial information it is always safe to keep it password-protected. During online payment transactions, based on the payment mode you select such as, credit card or Internet banking, Identity Safe automatically fills the details in the respective fields.

If you have more than one credit card, you can create multiple wallets with different sets of information. When you visit a transactional website, you can provide the credit card details that are present in any of the wallet that you created.

You can also create anonymous cards for use on unfamiliar websites where you may be uncomfortable providing your personal information. You can automatically fill online forms when you visit a website.

To add a card payment detail

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. Click the drop-down menu at the top of the window and choose **New Payment**.
3. In the **CREATE PAYMENT** window, in the **Title** box, type a name for the payment.
4. In the **Tags** box, type the category of the payment, such us Home, and Personal.
5. Select **Credit Card** from the **Type** drop-down box.
6. In the **Card** drop-down box, select the type of the card such as Visa, and Master.
7. In the **Number** box, type the card number.
8. In the **Expiration Date** box, select the date till which the card is valid.
9. In the **Card Holder's Name** box, type the name of the card holder as printed on the card.
10. In the **Billing Address** drop-down box, select the address that you have stored in the **Addresses** tab to map with the payment.
11. In the **Card Note** box, type the information that you want to remember about the card.
12. Select **Require vault Password** to prompt for your Identity Safe password before it autofills your wallet information in the website.
13. Click **Save**.

To add a bank account payment detail

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. Click the drop-down menu at the top of the window and choose **New Payment**.
3. In the **CREATE PAYMENT** window, in the Title box, type a name for the payment.
4. In the **Tags** box, type the category of the payment, such us Home, and Personal.
5. Select **Bank account** from the **Type** drop-down box.

6 In the **Bank** box, type the name of the bank.
7 In the **Account Owner** box, type the name of the bank account holder.
8 In the **Routing Number** box, type the routing number.
9 In the **Account Number** box, type the bank account number.
10 Select **Require vault password** to prompt for your Identity Safe password before it autofills your wallet information in the website.
11 Click **Save**.

Managing Wallet

All wallets that you have saved are listed in the **Wallet** window. You can view and edit the summary of a wallet that you created. You can also delete a wallet if it is no longer needed.

When you lock your wallet with a password, Identity Safe provides additional security to your wallet. You cannot view the summary of the locked wallet. You cannot edit, or delete a wallet unless you provide the password.

If you have multiple cards, use the scroll arrows to browse the list.

To edit a payment detail in Wallet

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2 Click the **Wallet** tab.
3 In the **Wallet** window, click the payment that you want to edit.
You can use **Sort By** option available at the top of the **Wallet** pane to locate a wallet faster. You can also directly search for a wallet in the **Search your vault**.
4 If you are prompted to provide a password, type your vault password, and then click **OK**.
5 Click **Edit**.

6 Modify the required details that you want to change.

7 Click **Save**.

To delete a payment detail in Wallet

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 Click the **Wallet** tab.

3 In the **Wallet** window, click the payment that you want to delete.
You can use **Sort By** option available at the top of the **Wallet** pane to locate a wallet faster. You can also directly search for a wallet in the **Search your vault**.

4 If you are prompted to provide a password, type your vault password, and then click **OK**.

5 Click **Delete**.

6 In the **Warning** dialog box, click **Yes**.
You need to validate your vault password for deleting the wallet, if you have selected **Require Vault password** option when you created the wallet.

Managing Notes

Identity Safe stores and manages your sensitive information. The Notes option in Identity Safe stores the information points or hints that you want to refer later. You can use Notes to save information such as meeting points, day to day work, and even the quotes that you like the most.

You can also view, edit, and delete the notes that you have saved.

To create a note

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 Click the drop-down menu at the top of the window and choose **New Notes**.

3 In the **NEW NOTE** window, in the **Title** box, type a name for the note.

4 In the **Tags** box, type the category of the note, such as Home, Personal, and Official.

5 In the **Text** box, type the data of your reference.

6 Select **Require Vault password** to prompt for your vault password before editing the note.

7 Click **Save**.

To edit a note

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 In the left pane, click **Notes**.

3 In the **Notes** window, click the note that you want to edit.
You can use **Sort by** option available at the top of the **Notes** pane to locate a note faster. You can also directly search for a note in the **Search your vault**.
You need to validate your vault password for editing the note, if you have selected **Require Vault password** option when you created the note.

4 Click **Edit**.

5 Modify the required details that you want to change.

6 Click **Save**.

To delete a note

1 In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.

2 In the left pane, click **Notes**.

3 In the **Notes** window, click the note that you want to delete.
You can use **Sort by** option available at the top of the **Notes** pane to locate a note faster. You can also directly search for a note in the **Search your vault box**.
You need to validate your vault password for deleting the note, if you have selected **Require Vault password** option when you created the note.

4 Click **Delete**.

5 In the warning dialog box, click **Yes**.

About Fill Assistant

The Fill Assistant feature helps you fill online forms if Identity Safe skips to fill in some fields in the forms. The Identity Safe uses the addresses and the wallets that you saved to automatically fill forms and bank details on websites. This way, you do not need to fill the lengthy forms that ask for your personal information such as name, date of birth, and phone number. You also need not type your bank details or credit details every time you shop online. If the fields in an online form are not filled, Identity Safe displays the **Open Fill Assistant** Infobar. You can click on the **Open Fill Assistant** option to open the **Fill Assistant** pane. You can use Fill Assistant to fill in such fields. All you need is to choose an address or a wallet from the Fill Assistant and then drag and drop the required information to the webpages.

Identity Safe may not or incorrectly fill in a field in an online form if:

- The field names in the online form do not match the ones that are stored in your Addresses or Wallet. For example, the country or region field can be named differently that Identity Safe cannot recognize.
- The field does not have a name associated to it.
- The data that a field accepts is different from what is stored in your addresses or wallet. For example, the date of birth is stored as number in addresses but the online form accepts only words.

Some websites may require some of your personal information such as your email or phone number. In those websites, you can use Fill assistant to quickly enter the required details. You just need to drag and drop the information in your addresses or wallet to the text field in the online form. For example, if you want to fill the phone number in an online form, drag and drop the phone number details from the Addresses to the text box in the online form. This way, Fill Assistant not only saves you from incorrectly filling the fields but also prevents hackers and keyloggers from accessing your personal information. You need to have Norton toolbar

enabled on your browsers to use Fill Assistant. To open Fill Assistant, on the Norton toolbar, click **VAULT IS OPEN**, and then click the **Open Fill Assistant** icon at the bottom of the pop-up.

The Fill Assistant feature has the following options:

Addresses	Lets you view and choose all the addresses that you have saved in your vault.
Wallet	Lets you view and choose all the wallets that you have saved in your vault.

You can use the **Move to other Side** icon to shift Fill Assistant window from right to left and vice versa

Adding Tags

The Tags feature lets you add tags to **Logins**, **Addresses**, **Wallet**, and **Notes**. When you add tags, the information in your vault is categorized and grouped to let you easily identify and access them.

For example, if you add the tag Social to all the social networking logins in your vault. You can use the Social tag in the **Tags** pane to easily view and access all of your social networking websites.

To add a tag to your existing Identity Safe data

1. In the Norton Security main window, double-click **Identity**, and then click **Identity Safe**.
2. Choose the data to which you want to add a tag. For example, if you want to add a tag to a login, click **Logins** and then click the login from the list.
3. In the window that appears, click **Edit**.
4. In the **Tags** field, type the category of the data.

If you want to add more than one tag to your data, separate each tag with a comma.

Permanently 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 Norton Security from your device, you can still continue to use your vault from other devices. If you think that you may use your vault data at a later time, do not delete your vault.

When you delete a vault, all of the Identify Safe data that are stored in the vault is permanently removed.

To delete your cloud vault

1. In the Norton Security 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 waning dialog box, click **Yes**.
6. Type your Norton account password to validate and click **Sign In**.
7. In the confirmation window, click **OK**.

About Norton Identity Safe General settings

When you install Norton Security on your system, it automatically adds Norton toolbar to your browsers. Some browsers, seek for your permission to add the toolbar, it is always safe to grant access to add the Norton toolbar. Using Norton toolbar you can know the security level of the websites you visit. You can save your identities and credentials from being stolen by knowing the fraudulent website even before you enter it.

The **General** settings window lets you configure the features of Norton toolbar. You can enable or disable

the Norton Safe Web feature. By default, the feature is turned on.

You can view the status of the Norton toolbar for the following browsers:

- **Internet Explorer**
- **Google Chrome**
- **Mozilla Firefox**

About Norton Identity Safe Import/Export settings

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer. The backup files are saved as .DAT files.

You can protect the files that you backed up with a password. Symantec recommends that you use a password to keep your Identity Safe data more secure. The backup password does not need to be the same as your Identity Safe password. You must provide the password when you restore the Identity Safe data that you backed up.

You can import your Identity Safe data from the file that you previously backed up. 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>**.

When you import the Identity Safe data you can do the following:

- Merge the imported data in to the vault that you are currently logged in.
- Replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

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 Security 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 logged in or replace the existing Identity Safe data that you stored in your vault

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 Security 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 Security display 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**.

About Norton Identity Safe Browsing settings

The **Browsing** tab in the **Settings** window lets you configure the way you want Identity Safe to collect, store, and display the login information for the webpages you visit. You can configure Identity Safe to display your cards that you created for the websites that have forms. You can also configure the autofill settings for the websites that contain security threats.

Symantec recommends you to keep the default settings for logins.

You can configure the following options in the **Browsing** window:

Login Saving	Lets you configure Norton Identity Safe to save and fill your login credentials. Your options are: **Save my credentials when I log in to a website**: Lets you save the login credentials for the websites that you visit. Your options are: **Always**, **No**, or **Ask**. **Turn off the browser's password manager**: Lets you specify how you want the browser's password manager to work. Your options are: **Yes**, **No**, or **Ask**.

Infobar

Lets you configure Norton Identity Safe to display the list of identities in the infobar. Your options are:

- **Display my Logins when I have multiple Logins for one site**: Displays your logins each time you visit a website that has multiple logins.
- **Display my fill options each time I visit a page with a form**: Displays the Addresses each time you visit a webpage with forms to fill your personal details.
- **Prompt me to open my Vault:** Prompts you to open your vault each time you visit a website with fields to fill in.

Filling

Lets you configure Norton Identity Safe to fill your identities automatically when you visit a website. Your options are:

Auto-fill my Logins when I visit websites: You can enable the option to automatically fill your login details when you visit a website.

Auto-fill on sites containing security threats: Lets you specify how you want Identity Safe to respond to the websites that have security threats. Your options are: **Yes**, **No**, or **Ask**.

About Norton Identity Safe Security settings

You can change your Identity Safe password in the **Security** tab of the **Settings** window. You can also use this option to set the level of security that you want for Identity Safe password usage.

The following sections let you change the Identity Safe password and set security levels for your password:

Vault Access

You can configure the following security settings to open and close your vault.

Your options are:

- **Ask for my password at the beginning of each login session:**

  Prompts you to enter your vault password each time you access Identity Safe.
- **Ask for my password before filling a login or form:**

  Prompts for your Identity Safe password with every online form before it autofills any login. You can specify that individual logins require the entry of your Identity Safe password before autofill.
- **Close Vault after <minutes> minutes of inactivity:**

  Automatically logs you out of Identity Safe when do not use your Identity Safe for a specified time period. You can set the idle timeout period as 15, 30, or 45 minutes. This option is useful if you are frequently in an area where other people have access to your computer.
- **Close Vault upon sleep:**

  Automatically logs you out of Identity Safe when your system is in suspended state.

Vault Password

Lets you change the vault password.

You can use the **Change Vault Password** to change your vault password and set a new password hint.

Changing the Identity Safe password

You should change your Identity Safe password regularly to prevent unauthorized access to your personal information stored in Identity Safe. You can change the password from the Security tab in the Norton Identity Safe **Settings** window.

If you want to change the Identity Safe password of your cloud vault, the password you provide must have the following characteristics:

- At least eight characters
- At least one capital letter
- At least one numeral (0 through 9)
- At least one symbol (for example, * > & $ %)
- The password must not match with your Norton account user name.

You can set your password hint here if you did not provide it when you configured Identity Safe.

To change the Identity Safe vault password

1. In the Norton Security 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 **Security** tab.
4. In the **Vault Password** row, click **Change Vault Password**.
5. In the **Change Vault Password** window, type the current password and the new password, and confirm the new password.
6. Click **OK**.
7. In the confirmation dialog box, click **OK**.

About Norton toolbar

When you install Norton Security, it adds the Norton toolbar to Internet Explorer (Toolbar), Firefox (Extensions), and Chrome browsers (Extensions).

You have the following options in the Norton toolbar:

Norton Safe Search	You can use the Norton Safe Search option to enhance your web search experience. The Norton Safe Search uses Ask.com to generate the search results. Norton Safe Search generates the search results based upon the site safety status and Norton rating for each of the search results.
Safe Web indicator	Lets you know if the website you visit is safe or unsafe. The Antiphishing and Norton Safe Web features, analyze the security level of the websites you visit. It then displays the results in the **Norton Safe Web** pop-up window. You can click on the Safe Web indicator to view the threats detail in the **Norton Safe Web** pop-up window. If you suspect that the result is wrong, you can use the **Report this site** option to notify Symantec for further evaluation.

VAULT IS OPEN/VAULT IS CLOSED menu	Lets you view the logins that you have saved in Identity Safe. Some websites require login information. You can use the **VAULT IS OPEN** menu to fill the details in those websites. The **VAULT IS OPEN** menu displays the list of logins that you saved. You can select a login from the list and a use it to log in to the website. You can use the following icons available at the bottom of the **VAULT IS OPEN** menu: ▪ Open Fill Assistant: Lets you view the Fill Assistant pane that appears on the right side of your browser. You can drag and drop the identities from the Fill Assistant pane to fill in the fields in the website. ▪ Open Norton Identity Safe: Lets you access the Norton Identity Safe main window. ▪ Close Vault: Lets you view the open or close status of the vault. You can click on the option to close the vault. You have to close the **Norton Identity Safe** main window before you close the vault using the toolbar. You should be logged in to any of the Identity Safe vault to access the **VAULT IS OPEN** menu.

SHARE VIA	Lets you share the website with your friends through the popular networking sites such as Facebook, Twitter, LinkedIn, Yahoo Mail, Hot Mail, or Google Mail. Websites with security threats are not allowed to share.
Settings icon (•••)	Lets you configure the Norton toolbar and Norton Identity Safe settings. Your options are: ▪ **Toolbar Options**: Lets you enable or disable the Norton Safe Search and Norton Safe Share features available in the toolbar. ▪ **Open Identity Safe Settings**: Lets you configure Identity Safe in such a way to access it from various devices and make it work more effective and smart.

In Google Chrome browser, the **Norton toolbar** can be accessed as a Chrome Extension. In the Extensions page of the Chrome browser, you can enable or disable the **Norton toolbar**, and uninstall the **Norton toolbar** from your Chrome browser.

If the **Norton toolbar** is enabled, you can access the following options:

Allow in incognito	Lets you browse the Internet in stealth mode without storing data of your browsing session in browsing or download histories.

Allow access to file URLs	Lets you view the URL location of the downloaded file.

If you have uninstalled the **Norton toolbar** from your Chrome browser, you must reinstall Norton Security to access the **Norton toolbar** on your Chrome browser again.

When you uninstall Norton Security, you can continue to use the Norton toolbar for free.

Your computer must be connected to the Internet to avail this option. Norton Security does not offer to leave the **Norton toolbar** if you upgrade your product to the latest version or choose to reinstall another Norton product.

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 in Internet Explorer, Mozilla Firefox, and Google Chrome browsers

- 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 Identity Protection**, uncheck **Enabled**.

To enable the Norton toolbar in Internet Explorer, Mozilla Firefox, and Google Chrome browsers

❖ 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 Identity Protection**, check **Enabled**.

Norton Identity Safe

Norton Identity Safe helps you store and manage your sensitive information such as your logins, personal information, and financial information. Identity Safe encrypts and stores all your sensitive information to a cloud-based vault. You can access the cloud vault using a password from a PC, laptop, tablets, smartphones, and the Norton Identity Safe website.

In addition to being a depository of your sensitive information, Identity Safe does the following:

- Protects you from identity theft and fraudulent or suspicious websites when you perform online transactions.
- Lets you easily manage and automatically fill multiple credit card information.
- Provides you the ease of securely carrying and using your sensitive information when you are on the move. By saving your data to a cloud vault, you can access your sensitive data from any computer that has Norton Security or through the Norton Identity Safe website.

Frequently asked questions

- How do I get started with Identity Safe?
- What type of information I can store in a vault?
- Why do I need to enable the Norton toolbar?
- Do I need to back up my Identity Safe data?

How do I get started with Identity Safe?

When you access Identity Safe for the first time, you must sign in to Identity Safe using your Norton account credentials. If you do not have a Norton account, you can click **Sign in** to create a Norton account

After you sign in to Norton account, you must create your Identity Safe cloud vault. You must provide a password to create your cloud vault. We recommend you to set a strong password for your cloud vault as it is a depository of all your sensitive information. See "Creating cloud vault" on page 212.

You can use the **Password Generator** feature to create unique and a strong password for your vault.

You can create only one cloud vault for a Norton account.

What type of information I can store in a vault?

Following are the categories and the type of information that you can store in your Identity Safe vault:

- **Logins** - Your user ID and passwords for the websites you visit, such as online bank account, email, and shopping websites. See "Managing Logins" on page 227.
- **Addresses** - Your personal information, such as name, date of birth, postal address, email address, and phone numbers. See "Managing Addresses" on page 230.

- **Wallet** - Your financial information, such as credit card details and bank account details. See "Managing Wallet" on page 234.
- **Notes** - Any text that you enter for future reference. See "Managing Notes" on page 235.

Why do I need to enable the Norton toolbar?

You must enable the Norton toolbar to easily access all the features of Identity Safe from your Internet browser. Norton Toolbar includes the following features:

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. For more information on how to use the Norton Safe Search feature, See "Searching the web using Norton Safe Search" on page 201.
Norton Safe Web	A site safety indicator for the websites that you visit. It analyzes the security level of the websites you visit and displays if the website you visit is safe.
Identity Safe vault	A secure online 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.

Norton Safe Share	A safe way to share the websites you visit, with your friends. You can share using social networking websites such as Facebook, Twitter, LinkedIn, Yahoo Mail, Outlook, and Gmail.
Fill Assistant	A feature that lets you easily fill the lengthy online web forms that ask for your personal, and financial information. You can drag and drop an address or a wallet from the **Fill Assistant** pane to automatically fill in the online web forms. For more information on the autofill feature, See "About Fill Assistant" on page 237.

Norton Security adds the Norton toolbar to Internet Explorer, Firefox, and Chrome browsers that are installed on your computer. If the Norton toolbar is not automatically enabled, you can manually enable it. For information on enabling the Norton toolbar in your browser, See "Disabling and enabling the Norton toolbar" on page 250.

Do I need to back up my Identity Safe data?

Norton Identity Safe automatically backs up your Identity Safe data to your computer in to a DAT file. However, you can also manually back up your Identity Safe data to your computer or any portable storage device. You can then import the data that you backed up in to your Identity Safe vault. For information on exporting or backing up your Identity Safe data, See "Exporting your Identity Safe data" on page 241.

Keeping your computer tuned up

8

This chapter includes the following topics:

- About disk and file fragmentation
- Optimizing your permanent disks manually
- About using optimization efficiently
- About cleaning up disk clutter
- Running a scan to clean up disk clutter
- Running Diagnostic Report
- Managing startup items
- Disabling or enabling startup items

About disk and file fragmentation

Your computer's hard disk stores all of your files, applications, and the Windows operating system. Over time, the bits of information that make up your files gradually spread over the disk. This process is known as fragmentation. The more you use your computer, the more fragmented your disks become.

When a fragmented file is accessed, the disk performance is slower. The performance is slower because the drive head locates, loads, saves, and keeps track of all of the fragments of the file. If free space is also fragmented, the drive head might have to track

adequate free space to store temporary files or newly added files.

Norton Security optimizes your permanent disks to improve your computer's efficiency and speed. The optimization process rearranges the scattered file fragments into adjacent or contiguous clusters. When the drive head accesses all of the file data in one location, the file is read into the memory faster. Optimization also consolidates free space to avoid fragmenting newly added files. It adds extra space after major data structures so that they can grow without immediately becoming fragmented again.

Optimizing your permanent disks manually

Optimizing your computer's permanent disks can improve performance and reliability. Norton Security 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.

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 Norton Security performs automatic optimization, you can optimize your disks manually.

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

To optimize your permanent disks manually

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

About using optimization efficiently

Norton Security automatically optimizes the permanent disk in your computer as necessary and does not require you to take any action to accomplish that task. You can, however, adopt some practices that help Norton Security perform automatic optimization more efficiently.

The following practices can help make automatic optimization more efficient:

Occasionally leave your computer turned on when you do not use the computer	Norton Security performs disk optimization when your computer is idle. If you turn off your computer whenever you finish your work, Norton Security cannot perform automatic optimization. If you turn off your computer during optimization, Norton Security restarts the optimization process when you turn on your computer again.
Set a schedule for optimization	Norton Security automatically optimizes the hard disk as needed. You can also set a schedule for optimization.
Remove the large files that you no longer need	Large files are often more fragmented than the smaller files. These fragmented files affect the performance of your computer.

About cleaning up disk clutter

Over time, the permanent disk in your computer can accumulate many temporary and unneeded files. Eventually, these files can significantly reduce the available disk storage space and affect the performance of your computer. Norton Security automatically cleans up accumulated disk clutter.

The temporary files that clutter your computer can come from the following sources:

Software installations	When you install software on your computer, the installation process creates temporary files as part of the installation process. In some cases, the installer might not clean up these temporary files when the installation finishes.
Web browsing	When you browse a webpage, your browser downloads the text and graphics that comprise the contents of the page. When you finish viewing the page, the browser can leave the downloaded contents on your computer. The downloaded contents help to display the webpage more quickly if you view the page again. These browser files accumulate over time.

Program errors	During normal operation, some programs create temporary files to improve efficiency while you work. If a program ends unexpectedly because of a software error, those temporary files can be left behind.

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

Running Diagnostic Report

Norton Security 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. Norton Security does not generate this report automatically. You need to use the **Diagnostic Report** option in the **Scans** window and manually generate the report.

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

Managing startup items

Norton Security 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.

Norton Security 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 Security 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 Norton Security 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**.

Disabling or enabling startup items

Whenever you start your computer, there are some programs that automatically start and run in parallel. These programs are called startup items. The startup items increase the start time of your computer.

Startup Manager helps you manage the startup items of your computer efficiently. If you do not want a program to automatically start when you turn on your computer, you can disable the program using Startup Manager. You can also delay a startup item that you want to start at a later time.

To disable startup items

1. In the Norton Security main window, double-click **Performance**, and then click **Startup Manager**.
2. In the **On/Off** column, uncheck a program that you do not want to automatically start when you turn on your computer.
3. Click **Apply** to save the changes.
4. Click **Close**.

To enable startup items

1. In the Norton Security main window, double-click **Performance**, and then click **Startup Manager**.
2. In the **On/Off** column, check a program that you want to automatically start when you turn on your computer.
3. Click **Apply** to save the changes.
4. Click **Close**.

Monitoring protection features

9

This chapter includes the following topics:

- About Security History

About Security History

Security History window lets you do the following:

- View the summary of alerts and event messages.
- View the results of scans that are run on your computer.
- View the items that you submitted to Symantec Security Response website.
- Manage Quarantine items.
- Monitor the security tasks that your products perform in the background.

Security History lets you monitor the security tasks that your product performs in the background. In addition, the alerts that you receive can be reviewed at any time in Security History. If you cannot review an alert when you receive it, you can review it later in Security History.

The alerts, scan results, and other security items that are related to various product features appear under their respective categories in the **Security History** window. For example, the security items that are related to the Quarantine feature appear under the **Quarantine** category. In addition, the **Security History** window displays details of each item in the **Details** pane.

Based on their functionalities, Security History broadly organizes all categories into the following groups:

- **All Activity**
- **Protection and Performance**
- **Submissions and Errors**
- **Performance**
- **Informational**

By default, the following information categories are available in the **Security History** window:

- **Recent History**
- **Full History**
- **Scan Results**
- **Resolved Security Risks**
- **Unresolved Security Risks**
- **Quarantine**
- **SONAR Activity**
- **Firewall – Network and Connections**
- **Firewall – Activities**
- **Intrusion Prevention**
- **Social Protection**
- **Download Insight**
- **AntiSpam**
- **Identity**
- **Norton Product Tamper Protection**
- **Performance Alert**
- **Network Cost Awareness**
- **Sites reported to Symantec**
- **Norton Error Reporting**
- **Email Errors**
- **Norton Community Watch**
- **File Cleanup**
- **Disk Optimization**
- **Silent Mode**

- **LiveUpdate**

You can view the security items based on the category of events that you select and the search string that you provide. Norton product restricts the number of search results that appear on each page in the **Security History** window. Therefore, Security History divides the items that are returned for any search criteria and displays them on separate pages. You can use the pagination scroll at the bottom of the window to navigate to different pages sequentially. In case you want to view a specific page, you can use the **Go to page** option to open the page. The maximum number of items that appear per page is 100.

Based on the security status of an item in an information category, you can take an appropriate action to resolve a risk or a threat. The actions that you can perform include the following:

- Restore and exclude a quarantined item.
- Remove an item from Security History.
- Submit an item to Symantec for further analysis.
- Trust or restrict devices on a selected network.
- Remove the trusted or restricted status of devices on the selected network.
- Allow a selected program to access the Internet.
- Configure your Norton product to notify you when it blocks a selected attack signature.

Your Norton product also lets you save the security events history. You can view the security event information whenever you want. If you want to analyze the security events for a particular day, you can save the Security History logs for that day. You can later import the file into Security History and analyze the data.

Opening Security History

Security History provides a record of all the activities that Norton Security performed on your computer.

You can access Security History from the following areas:

- **Security** tab of the product main window
- Various alert windows and notifications
- Notification area of the Windows taskbar
- **Threats Detected** section in different **Scan** windows

Viewing items in Security History

Security History provides a record of all the activities that your Norton product performed on your computer.

You can view details about all the activities including:

- Security History alerts and event messages
- Results of different scans
- Information that you submitted to Symantec Security Response website
- Quarantined items
- Norton Firewall activities
- File Cleanup activities
- Security tasks that your Norton product performed in the background

Based on their functionalities, all Security History categories appear under the following groups in the **Show** drop-down list:

- **All Activity**
- **Protection and Performance**
- **Submissions and Errors**
- **Performance**
- **Informational**

The items that are related to the various product features appear under their respective categories in the **Security History** window. For example, the security items that are related to the Quarantine feature appear under **Quarantine** category in the **Security History** window. In addition, the **Security History** window displays details of each item in the **Details** pane.

To view items in Security History

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

2 In **Security History** window, in the **Show** drop-down list, select the category of items that you want to view. Your options are:

Recent History	The **Recent History** view in the **Security History** window displays the alerts that you received during the last 7 days. It lists the history of certain recent security events.
Full History	The **Full History** view in the **Security History** window displays the complete Security History.
Scan Results	You can scan your computer to check if any virus, spyware, malware, or security risk has infected your computer. The **Scan Results** view in the **Security History** window displays the details about the scans that are run on your computer.

Resolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Resolved Security Risks** view in the **Security History** window displays a list of security risks that your Norton product has detected and then repaired, quarantined, or removed. The quarantined items are listed in the **Quarantine** view. You can also view the quarantined items in the **Quarantine** view.
Unresolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Unresolved Security Risks** view in the **Security History** window displays a list of security risks that your Norton product was not able to repair, remove, or quarantine. Certain threats require system restart. Logs for such threats can be cleared only after you restart your system.

Quarantine	The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide an action to take on them. The **Quarantine** view in the **Security History** window displays all of the security risks that are isolated in the Security History Quarantine.
SONAR Activity	Symantec Online Network for Advanced Response (SONAR) identifies new threats based on the suspicious behavior of applications. SONAR detects and protects your computer against malicious code even before virus definitions are available through LiveUpdate. The **SONAR Activity** view in the **Security History** window displays details about the security risks that SONAR detects. This category also lists any activity that modifies the configuration or the settings of your computer. The **More Details** option for this category provides details about the resources that this activity affects.

Firewall - Network and Connections	The firewall monitors the communications between your computer and other computers on the Internet. The **Firewall - Network and Connections** category in the **Security History** window displays information about the networks that your computer connects to. It also displays the actions that you have taken to trust or to restrict networks and computers. This category also displays a history of all of the TCP/IP network connections that were made with your computer. Network connections are logged when the connection is closed. The **Security History - Advanced Details** window for this category lets you modify trust or restrict settings for computers and networks.

Firewall - Activities	The firewall monitors the communications between your computer and other computers on the Internet. The firewall maintains rules to control Internet access to and from your computer. The **Firewall - Activities** view in the **Security History** window displays the rules that firewall creates. The rules that you create also appear in this view. The **Security History - Advanced Details** window for this category shows the created Program rules. It also lets you allow a blocked program rule.
Intrusion Prevention	Intrusion Prevention scans all the network traffic that enters and exits your computer for known threats. The **Intrusion Prevention** view in the **Security History** window displays details about recent Intrusion Prevention activities. The **Security History - Advanced Details** window for this category lets you control whether or not to be notified when Intrusion Prevention detects an **Intrusion Prevention** signature.

Social Protection	Social Protection lists the threats that your Norton product detected when you performed your social networking activities. These threats are usually tricks that online scammers use to take advantage of the various sharing features in social networking websites. Your Norton product provides an overview and analysis of each social threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape. You can select a specific threat and click the **Learn More** option to learn on how to stay protected from the particular social threat.

Download Insight	Download Insight processes any executable file that you download for analysis of its reputation level. It then informs you about the processing results based on the Download Insight settings. The **Download Insight** view in the **Security History** window displays details of all events that Download Insight processes and notifies. This view also contains information about the actions that you take based on the reputation data of the events.
AntiSpam	Norton AntiSpam protects your computer from exposure to unsolicited email. The **AntiSpam** view in the **Security History** window displays details about the email messages that AntiSpam has processed.

Identity	The various features of Identity Safe help you manage your identities and provide additional security while you perform online transactions. The **Identity** view in the **Security History** window displays the Antiphishing definitions that your Norton product downloads when you run LiveUpdate to obtain the latest virus definitions.
Norton Product Tamper Protection	Norton Product Tamper Protection lets you protect your Norton product from any attack or modification by unknown, suspicious, or malicious applications. The **Norton Product Tamper Protection** view in the **Security History** window displays details about unauthorized attempts to modify Symantec processes. The tasks that your Symantec product blocks also appear in the list.

Performance Alert	The performance alert feature lets you view, monitor, and analyze the impact of the system activities on your computer. The **Performance Alert** view in the **Security History** window provides details about the impact of the processes that run on your computer. The details include the process name, the resources used, the extent of resource utilization, and the overall impact of the process on your computer. In addition, logs related to performance alerts and the programs that you have excluded from performance alerts also appear in the list.
Network Cost Awareness	Network Cost Awareness lets you set up policies and restrict the Internet usage of your Norton product. You can define the amount of network bandwidth that your Norton product can use. The Network Cost Awareness view in the Security History window provides details about the actions that you performed to restrict the Internet usage of your Norton product.

Sites reported to Symantec	In some cases, you might have submitted evaluation of certain webpages to Symantec. The **Sites Reported to Symantec** view in the **Security History** window displays all the websites that you reported to Symantec to verify authenticity.
Norton Error Reporting	Your Norton product may generate errors in some cases. For example, an error can occur when you run LiveUpdate or scan a folder. Engine errors, timeout errors, and program errors are some of the types of errors. The **Norton Error Reporting** view in the **Security History** window displays any error that your Norton product has generated.

Email Errors	Email errors include any failure that occurs when your Norton product tries to send, download, or scan an email message that you send or receive. The **Email Errors** view in the Security History displays details about any Email Error alerts that you receive when an Email error occurs. Details include the **Error ID** and the **Error message**. This view also displays information about subject, sender address, and the recipient address that are related to the email message in the alert.
Norton Community Watch	The Norton Community Watch feature lets you submit any suspicious security or suspicious application data to Symantec for analysis. Symantec assesses the data to determine the new threats. The **Norton Community Watch** view in the **Security History** window displays a list of files that you have submitted to Symantec for analysis. Files, at various stages of submission, also appear in the list.

File Cleanup	The File Cleanup feature removes unwanted temporary files including leftover Internet browser files, Internet search words, and other temporary files. The **File Cleanup** view in the **Security History** window shows the list of the File Cleanup activities that were performed on your computer.
Disk Optimization	Disk optimization is a process in which the physical locations of files are streamlined. Files and metadata are re-arranged to improve data access time. The disk optimization view in the **Security History** window shows the list of the disk optimization activities that were performed on your computer.

Silent Mode	Silent Mode suppresses alerts and notifications and temporarily suspends most of the background activities. The **Silent Mode** view in the **Security History** window displays the summary of the Silent Mode sessions. The summary includes the following information: ▪ The type of Silent Mode such as Silent Mode or Quiet Mode. ▪ The type of program that turns on Silent Mode such as disk burning or running a program in full screen mode. ▪ The name of User-Specified program that turns on Silent Mode. ▪ Whether Silent Mode is turned on or turned off.

LiveUpdate	LiveUpdate obtains the latest virus definition updates and the program updates to all the Symantec products that you installed on your computer. These updates protect your computer from newly discovered threats. The **LiveUpdate** view in the **Security History** window shows the details of the LiveUpdate activities on your computer. The details include the severity, the status, and the duration of the LiveUpdate sessions on your computer.

3 Click a row to view details for that item.
If you want to view additional information about an item, click the **More Options** option in the **Details** pane or double-click the particular row. You can view the advanced details about the item in the **Security History-Advanced Details** window and take actions as needed. For some categories, the **More Options** option opens the **File Insight** window that displays the details about the selected Security History event. You must use the **Options** link in the **Security History** window to select an action that your Norton product must perform on any item in these categories. The **Options** link is also available in the **File Insight** window for certain items. You must use the **Restore** link in the **Security History** window to restore a selected quarantine item to its original location. The **Restore** link is also available in the **File Insight** window for certain items.

About the File Insight window

The **File Insight** window provides details about any File of Interest that is available on your computer. This option of file analysis is available for the files that you download, scan, or use to perform an activity.

You can access the **File Insight** window in different ways. For example, you can use the various notifications, alerts, scan and performance-related windows, and the shortcut menu of the various files that are present on your computer to open the window. Security History provides a centralized location where you can access the **File Insight** windows of the various events that are related to Security Risks, Download Insight, and Performance.

The File Insight window lets you view more details of events that belong to some of the following categories in the **Security History** window:

Resolved Security Risks	Lets you view the detailed information about the resolved security risks in an organized way. The **Resolved Security Risks** category includes the infected files that Norton Security repairs, removes, or quarantines. This category mostly includes the medium-level or the high-level risks that are either quarantined or blocked. The **File Insight** window provides details about the risk level, the origin, and the activity report of the resolved security risks on your system.

Unresolved Security Risks	Lets you view the detailed information about the unresolved security risks in an organized way. The **Unresolved Security Risks** category includes the infected files for which Norton Security was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of the unresolved security risks on your system.
Quarantine	Lets you view the detailed information about quarantined security risks in an organized way. The **Quarantine** category includes the infected files that are isolated from the rest of your computer while they await your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of quarantined security risks on your system.

Download Insight	Lets you view the reputation details of a file that you download. You can use these details to determine the safety level of the file and then decide the action that you want to perform.
Performance Alert	Lets you view the performance details of any File of Interest that is available on your computer. The information includes the general details, the origin and lineage information, the resource usage, and the actions that the file has performed on your system.

The **File Insight** window provides various details about the **Security History** item. These details are classified in different tabs in the **File Insight** window.

About the Threat Detected window

The **Threat Detected** window appears whenever your Norton product detects a security risk on your computer. You can use this window to view details about the risk and select an action for the risk. Sometimes, you may want to access the **Threat Detected** window for the same risk again. In that case, the window can be opened at any time from Security History. Security History is the centralized location where you can access the **Threat**

Detected windows of risks that belong to some of the following categories:

Resolved Security Risks	This category includes the security risks or the infected files that your Norton product has detected and then repaired, quarantined, or removed.
Unresolved Security Risks	This category includes the security risks or the infected files that your Norton product was not able to repair, remove, or quarantine.
Quarantine	This category includes the security risk items that are isolated from the rest of your computer while they await your attention for a suitable action.

The action options in the **Threat Detected** window for a risk vary depending on the risk type and its severity level. The following are some of the options that are available in this window:

Restore	Returns the security risk that is quarantined to the original location on your computer
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
Remove this file	Removes the security risk from your computer and quarantines it

Exclude this program	Excludes the security risk from future scan
Remove from history	Removes the selected security risk item from the Security History log
Get help	Takes you to the Symantec Security Response website
Submit to Symantec	Sends the security risk to Symantec

Searching in Security History

You can search the items that are listed in Security History. You can use the **Quick Search** option to find items using a keyword or the name of a security risk. If you want to view all of the Security History items that pertain to a particular security risk, you can filter the items using **Quick Search**. For example, if you want to view all of the alerts that Auto-Protect has generated, you can type Auto-Protect and filter the list.

You can clear the search results and return to the current Security History list by clicking the black cross (x) icon in the **Quick Search** box.

The **Quick Search** option works on the current view only. If you want your search to include all of the items in Security History, you must select the **Full History** view.

To search in Security History

1. In the **Security History** window, in the **Quick Search** text box, type the name of the item that you want to search.
2. Click **Go**.

Exporting or Importing Security History information

Your Norton product lets you export the Security History events to a file. You can export and save the Security History events and view them at your leisure.

For example, you can analyze the security events on a particular day. You can use the **Quick Search** option to obtain a list of all of the items that are related to a particular security risk. You can then use the **Export** option to save the list in the Security History log. You can later import the log file and analyze the data.

Security History stores the information in a separate file. When the file size reaches its maximum size limit, information that is related to new events overwrites the information that is related to older events. You can export the log periodically, if you want to keep the entire Security History information.

You can save your log file in one of the following file formats:

- Security History Log Files (.mcf)

  The .mcf file format is the Security History Log Files format and is proprietary to Symantec.

  When you use this file type option, you can view the file only in the **Security History** window.
- Text Files (.txt)

  The data is saved in a comma-separated text format.

  When you use this file type option, you can open and view the file externally without using Security History.

You can import only the log files that have .mcf file extension. When you import a log file, the exported list of Security History information in the log file appears. This list replaces the current security events list. You can select an option in the **Show** drop-down list to view the option-specific details that are saved in the log file. To revert to the current Security History list you must click the **Close file: *file_name*.mcf** link.

To export Security History information

1. In the Norton Security main window, double-click **Security**, and then click **History**.
2. In the **Security History** window, in the **Show** drop-down list, select an option.
3. Click **Export**.
4. In the **Save As** dialog box that appears, navigate to a location and specify the name for the file.
   The category name in the **Show** drop-down list appears as the default file name. You can provide a file name of your choice.
5. In the **Save as type** box, select the format in which you want to save your log file.
6. Click **Save**.

To import Security History information

1. In the Norton Security main window, double-click **Security**, and then click **History**.
2. In the **Security History** window, click **Import**.
3. In the **Open** dialog box that appears, browse to the folder that has the file you want to import.
4. Select the .mcf file and click **Open**.
   You can only open log files of .mcf format in the **Security History** window. You can open and view log files of .txt file externally without using Security History.
   In the import mode, you cannot make modifications to the information. For example, you cannot clear the logs. You can revert to the current Security History list by closing the file.

Managing items in the Quarantine

The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide on an action to take on them. Quarantined items are isolated from the rest of your computer so that they cannot spread or reinfect your computer. In some cases, you may have an item that you think is infected, but is

not identified as a risk by the Norton product scans. You can manually place such items in the Quarantine.

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

The Security History Quarantine includes the following groups of items:

Security risks	Includes the 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	Includes viruses and other high-risk items.

Once an item has been quarantined, you have several options. All of the actions that you take on quarantined items must be performed in the Security History Quarantine.

To perform an action on a quarantined item

1. In the Norton Security 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.

Adding an item to the Quarantine

Security History Quarantine provides a safe location on your computer in which you can isolate items while you decide on an action to take on each item.

The **Quarantine** view in the **Security History** window displays a list of quarantined items. You can view the name and the risk status of each quarantined item.

You can manually add an item to the Security History Quarantine. You can use the **Add to Quarantine** option in the **Quarantine** view in the **Security History** window to quarantine the items that you suspect are infected. This action has no effect on the items that are already quarantined.

You cannot add a known Good File or a Windows application to Quarantine.

To add an item to the Quarantine

1 In the Norton Security main window, double-click **Security**, and then click **History**.
2 In the **Security History** window, in the **Quarantine** view, click **Add to Quarantine**.
3 In the **Manual Quarantine** dialog box, in the **Description** text box, type a short name for the item that you want to add.
This text appears in the Quarantine, so you should use a recognizable description.
4 Click **Browse**.
5 In the **Select File to Quarantine** dialog box, browse to the item that you want to add, select it, and then click **Open**.
6 Click **Add**.
7 In the **Security History** window, click **Close**.

Restoring an item from the Quarantine

Some programs rely on other programs that are classified as security risks to function. The program may not function if a particular security file is removed. All of the removed security risks are automatically backed up in the Security History Quarantine. This way, your Norton product lets you restore any risk to regain the functionality of a program that requires the risk program to run.

For example, a shareware or freeware program that you download may use adware to keep its price low. In this case, you can allow the security risk program to remain on your computer or restore it if Spyware Protection has removed it.

Some quarantined items are successfully disinfected after your Norton product rescans them. You can also restore such items.

If you restore an item to a directory other than its original location, it may not function properly. Therefore, it is recommended that you reinstall the program.

To restore an item from the Quarantine

1. In the Norton Security 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, do one of the following:

- Click **Restore & exclude this file**.

  This option returns the selected quarantine item to its original location without repairing it and excludes the item from being detected in the future scans.

- Click **Restore**.

  This option returns the selected quarantine item to its original location without repairing it. This option is available only for manually quarantined items

5 In the **Quarantine Restore** window, click **Yes**.
In case of non-viral threats, you can use the option that is available in this window to exclude the security risk. Your Norton product does not detect the security risks that you exclude in the future scans.

6 In the **Browse for Folder** dialog, select the folder or drive where you want to restore the file and then click **OK**.

7 Click **Close**.

Manually submitting an item to Symantec

When a virus or other risk is detected, it is automatically submitted to Symantec Security Response website for analysis. If you have turned off the option to submit risks automatically, you can manually submit them from the Security History Quarantine. You must have an Internet connection to submit an item.

When you submit files to Symantec automatically or manually, you contribute to the effectiveness of your Symantec product. For example, you can submit an item that has not been detected during scanning that you believe may be a security risk. Symantec Security Response analyzes the file. If it is identified as a security risk, it is added to a future definition update.

Personally identifiable information is never included in submissions.

In some cases it is necessary for Symantec Security Response to block submissions of a particular type or volume. These items appear as **Not Submitted** in Security History.

To manually submit an item to Symantec

1. In the Norton Security 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 submit to Symantec.
3. In the **Details** pane, click **Options**.
4. In the **Threat Detected** window, click **Submit to Symantec**.
5. In the dialog box that appears, click **OK**.

Customizing protection features

10

This chapter includes the following topics:

- Feature summary
- About turning off automatic features

Feature summary

Use the information in this section to familiarize yourself with the product.

This section includes the following information:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

For more information, select one of the sub-entries for this Help topic.

About virus and security risk protection features

Virus and security risk protection features provide comprehensive virus prevention and security risk detection for your computer. Known viruses are automatically detected and repaired. Instant messenger attachments, email message attachments, Internet downloads, and other files are scanned for viruses and other potential risks. In addition, the definition updates

that Automatic LiveUpdate downloads when your computer is connected to the Internet keeps you prepared for the latest security risks.

Your computer is continually monitored and protected from known and unknown threats by the following features:

Auto-Protect	Checks for viruses and other security risks every time that you run programs on your computer. Auto-Protect options let you customize the protection of your computer. Auto-Protect options are: ▪ Loads into memory when Windows starts, providing constant protection while you work. ▪ Checks for viruses and security risks every time that you use software programs on your computer. It also checks every time when you insert removable media, access the Internet, or use document files. ▪ Monitors your computer for any unusual symptoms that may indicate an active threat.
Automatic LiveUpdate	Notifies you of program updates and downloads definition updates automatically. See "About Norton LiveUpdate" on page 35.

Compressed File Scan	Detects viruses, spyware, and other security risks in compressed files during manual scans. See "What to do if a security risk is found" on page 114.
Email Protection	Protects your computer against the threats that you may receive through email attachments. You can use the **Email Antivirus Scan** option and the **AntiSpam** option to configure your email program for protection against viruses and other security threats.
Heuristic Protection	Detects the new and the unknown viruses by analyzing an executable file's structure, and behavior. Also, by analyzing other attributes such as programming the logic, computer instructions, and any data that is contained in the file.
Quick Scan	Checks for the infections that have processes running in memory and the infections that the startup folders and files refer. See "Running a Quick Scan" on page 80.

About Norton Family

The **Norton Family** option lets you create your Norton Family account. Norton Family is a parental control application that provides a smart way to keep your

children safe when they are online. Norton Family helps parents to get a better understanding of what children do online, so that they can better protect and guide them.

You can use the **Family** icon in the **More Norton** section on the main window to create your Norton Family account. The icon may not be available with some versions of Norton Security. In such case, you may not be able to access Norton Family options. You need to install the Norton Family client on each computer that your children use. If your children use the same computer, you need to create user accounts for each child and install the Norton Family client on the computer.

You can also use the **Norton Family** link in the **Web Protection** pane in the Norton Security advanced window to create your Norton Family account. Symantec recommends that you use your Norton account credentials to register with Norton Family.

After you set up your account, you can configure your settings in Norton Family website to monitor your children's Internet activities. You can sign in to your Norton Family account at any time to view their online activities. You can also use the **Family** icon on the main window to sign in to your account and view your child's Internet activities.

The following Norton Family features help you manage the Internet activities of your child:

- Android device monitoring
- Web monitoring and blocking
- Time limits
- Social network monitoring
- Search monitoring
- House rules

Norton Family may not be available with some versions of Norton Security. In such case, you may not be able to access the Norton Family options.

About turning off automatic features

Your Symantec product is set by default to provide complete protection for your computer. Many of these settings include the automatic features that provide continuous protection. Under certain circumstances, you might need to turn off an automatic feature to complete a task.

When you have completed the task for which you turned off the automatic feature, make sure that you turn the feature on again.

See "Turning off Auto-Protect temporarily and turning it on again" on page 298.
See "Turning off or turning on spam filtering" on page 299.

Turning off Auto-Protect temporarily and turning it on again

If you have not changed the default option settings, Auto-Protect loads when you start your computer. Auto-Protect also guards against viruses, Trojan horses, worms, and other malicious threats. It checks programs for viruses when programs run and monitors your computer. It also checks the removable media for any activity that might indicate the presence of a virus. When Auto-Protect detects a virus or virus-like activity, it alerts you.

In some cases, Auto-Protect might warn you about a virus-like activity that you know are not the work of a virus. If you perform such an activity and want to avoid the warning, you can turn off Auto-Protect.

If you have set a password for settings, Norton Security asks you for the password before you can view or change the settings.

When you turn off **Auto-Protect**, **SONAR Protection** and **Download Intelligence** are also turned off.

To turn off Auto-Protect temporarily

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Auto-Protect** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.
5. In the dialog box that appears, in the **Select the duration** drop-down list, select how long you want to turn off Auto-Protect, and then click **OK**.

To turn on Auto-Protect

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Auto-Protect** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.

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.

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

To turn off 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 the right to the **Off** position.

4 Click **Apply**.
5 In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off spam filtering.
6 Click **OK**.
7 In the **Settings** window, click **Close**.

To 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 the right to the **Off** position.
4 Click **Apply**, and then click **Close**.

Turning off or turning on Norton Community Watch

Norton Community Watch helps in identifying new security risks by submitting selected security and application data to Symantec for analysis. This analysis helps Symantec to provide the solutions that identify the new threats and risks more efficiently. Symantec assesses the data to determine the new threats and their sources. The collective efforts from Norton security product users help in quick identification of solutions for these threats and risks.

You can use the **Norton Community Watch** option to send information about a suspicious file to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. The Norton Insight feature uses the Symantec-assessed information to detect the security threats.

Norton Community Watch collects and submits detailed data about the Norton-specific errors and components only. It does not collect or store any personal information of any user.

You can use the **Security History** window to review the information that has been sent to Symantec.

To turn off or turn on Norton Community Watch

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Administrative Settings** window, in the **Norton Community Watch** row, do one of the following:
   - To turn off Norton Community Watch, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Norton Community Watch, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

Turning off or turning on security protection features

There may be times when you want to turn off a security protection feature. For example, you might want to see if the Smart Firewall prevents a webpage from appearing as expected.

Turning off security protection features reduces your computer's security. When you turn off a feature, you can specify the amount of time it should remain off. After that time limit, the feature turns on automatically.

To ensure that your computer remains protected, you can turn on security protection features manually before the specified time frame concludes.

To turn off a security protection feature

1. In the Norton Security 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 the right to the **Off** position.
4. Click the **Intrusion and Browser Protection** tab.
5. In the **Intrusion Prevention** row, move the **On/Off** switch to the right to the **Off** position.
6. In the **Settings** window, click **Apply**.

7 In the **Select the duration** drop-down list, select the amount of time that the security protection feature should be turned off, and then click **OK**.

To ensure that your computer remains protected, you can turn on security protection features manually before the specified time frame concludes.

To turn on a security protection feature

1 In the Norton Security 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 the left to the **On** position.
4 Click the **Intrusion and Browser Protection** tab.
5 In the **Intrusion Prevention** row, move the **On/Off** switch to the left to the **On** position.
6 In the **Settings** window, click **Apply**.

Customizing settings

11

This chapter includes the following topics:

- Customizing Norton Security settings
- Turning on or turning off Quick Controls services
- About Automatic Protection settings
- About Scans and Risks settings
- About Antispyware and Updates settings
- About the Intrusion and Browser Protection settings
- Turning on or turning off Remote Management
- Resetting your Norton product Settings password
- Turning off the Norton product Settings password
- Securing your Norton product Settings using a password
- About Norton Product Tamper Protection

Customizing Norton Security 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, Norton Security 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 **Default All** 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 Security 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**.

Turning on or turning off Quick Controls services

In the **Settings** window, you can turn on or turn off the following **Quick Controls** services:
- **Silent Mode**
- **Safe Surfing**
- **Identity Safe**
- **Automatic LiveUpdate**
- **Smart Firewall**
- **Norton Tamper Protection**

You should leave all of the services turned on except Silent Mode.

To turn on or turn off Quick Controls services

1 In the Norton Security main window, click **Settings**.
2 In the **Settings** window, under **Quick Controls**, do one of the following:
- To turn on a service, check its check box.
- To turn off a service, uncheck its check box.

  If an alert or a message appears, select the duration from the drop-down menu, and then click **OK**.

About Automatic Protection settings

The **Boot Time Protection** option on the **Automatic Protection** tab provides an enhanced security level from the time you start your computer. This option ensures better security by running all the necessary components

that are required for computer protection as soon as you start your computer.

The **Real Time Protection** settings on the **Automatic Protection** tab let you control the scanning and monitoring of your computer. It protects your computer by continuously checking for viruses and other security risks.

You can use the **Real Time Protection** options to determine what gets scanned and what the scan looks for. It also provides you with advanced protection by proactively detecting unknown security risks on your computer. You can determine what happens when a security risk or risk-like activity is encountered.

You can use the following **Real Time Protection** options:

Auto-Protect	

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. It also monitors your computer for any unusual symptoms that might indicate an active threat.

You can stay protected by using the following option:

- **Removable Media Scan**

  Checks for boot viruses when you access removable media

  After the removable media has been scanned for boot viruses, it is not scanned again until it is reinserted or formatted. If you still suspect that a boot virus infects your removable media, ensure that Auto-Protect is turned on to rescan the removable media. You then insert the removable media and open it from My Computer for Auto-Protect to rescan it. You can also scan it manually to verify that it is not infected.

SONAR Protection	

	Symantec Online Network for Advanced Response (SONAR) provides the real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies the emerging threats that are based on the behavior of applications. SONAR is quicker than the traditional signature-based threat detection techniques. It also detects and protects your computer against malicious code even before virus definitions are available through LiveUpdate. **SONAR Protection** includes the following options: ▪ **Network Drive Protection** This option protects all the network drives that are connected to your computer. You can enable or disable protection of your network drives. As network drives are prone to infection, Symantec recommends you to keep this option turned on for better protection. ▪ **SONAR Advanced Mode** The Norton product provides you the greatest control over low-certainty threats only if this option is turned on. **Remove Risks**

	▪ **Automatically** This option lets the low-certainty threats behave as high-certainty threats when **SONAR Advanced Mode** option is enabled. In this case, the Norton product automatically removes the threats and notifies you. ▪ **Remove Risks if I Am Away** This option lets the Norton product to automatically remove low-certainty threats if it does not get any response from you when **SONAR Advanced Mode** option is enabled. ▪ **Show SONAR Block Notifications** This option lets you enable or disable SONAR Block notifications. The Norton product suppresses the SONAR Block notifications when you set the **Show SONAR Block Notifications** option to **Log Only**.

Early Launch Anti-Malware Protection	This feature provides better protection by running all the necessary components of the Norton product that block malware intrusion when you start your computer. This feature is available only in Windows 8.

About Scans and Risks settings

Scans and Risks settings let you customize the scans that the Norton product performs on your computer. You can configure a scan based on the digital signature and trust level of the files on your computer. You can define how the Norton product should behave when it scans email messages.

You can use the following **Scans and Risks** settings:

Computer Scans	

The Norton product lets you run different types of scans to detect and prevent any virus infection on your computer. The scans are Quick Scan, Full System Scan, and customized scans. You can use the various Computer Scans options to customize the scans that the Norton product performs on your computer. You can also specify scanning of compressed files.

The Computer Scans options also let you specify scans to detect rootkits, other stealth items, tracking cookies, and unknown security threats. Your options are:

- **Compressed File Scan**

  Scans and repairs the files inside compressed files.

  When you turn on this feature, your Norton product scans and detects viruses and other security risks in the files within compressed files and removes the compressed files.
- **Rootkits and Stealth Items Scan**

  Scans for rootkits and other security risks that might be hidden on your computer.
- **Network Drives Scan**

  Scans the network drives that are connected to your computer.

  Your Norton product performs a **Network Drives**

	Scan during **Full System Scan** and **Custom Scan**. By default, the **Network Drives Scan** option is turned on. If you turn off this option, your Norton product does not scan network drives. ▪ **Heuristic Protection** Scans your computer to protect against unknown security threats. Your Norton product uses heuristic technology to check suspicious characteristics of a file to categorize it as infected. It compares the characteristics of a file to a known infected file. If the file has sufficient suspicious characteristics, then your Norton product identifies the file as infected with a threat. ▪ **Tracking Cookies Scan** Scans for the small files that programs might place on your computer to track your computing activities. ▪ **Full System Scan** A Full System Scan thoroughly examines your entire computer for viruses, spyware, and different security vulnerabilities. You can use the **Configure** option to schedule the Full System Scan.

Protected Ports	Protected Ports settings protect the POP3 and SMTP ports of your email program. You can use this option to manually configure your POP3 and SMTP email ports for email protection. If the SMTP and POP3 port numbers that your Internet service provider (ISP) has provided for your email program is different from the default SMTP and POP3 port numbers, you must configure your Norton product to protect the ports.
Email Antivirus Scan	Email Antivirus Scan protects you from the threats that are sent or received in email attachments. You can use the Email Antivirus Scan options to define how the Norton product should behave when it scans email messages. Based on the options you choose, your Norton product automatically scans the email messages that you send or receive.

Exclusions / Low Risks	

Exclusions options specify the items such as folders, files, and drives that you exclude from Norton product scans. Scans, signatures, and low-risk items are some items that you can exclude from scanning.

Exclusions options also let you choose which categories of risks you want your Norton product to detect. Your options are:

- **Low Risks**

  Lets you manage the low-risk items that are found in your computer.

  You can specify how you want your Norton product to respond to low-risk items.
- **Items to Exclude from Scans**

  Lets you determine which disks, folders, or files you want to exclude from risk scanning.

  You can add new exclusion items or edit the added items in the excluded-items list. You can also remove items from the excluded-items list.
- **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection**

  Lets you determine which disks, folders, or files you want to exclude from Auto-Protect scans and SONAR scans.

  You can add the new items

	that need to be excluded or modify the items that you already excluded. You can also remove items from the excluded-items list. ■ **Signatures to Exclude from All Detections** Lets you select known risks by name and remove a risk name from the excluded-items list You can also view the risk impact that is based on the performance, privacy, removal, and stealth impact. ■ **Clear file IDs excluded during scans** Lets you remove the reputation information of the files that are excluded from scanning. You can use the **Clear All** option to clear the reputation information of the files that are excluded from scanning. Exclusions reduce your level of protection and should be used only if you have a specific need.

About Antispyware and Updates settings

Antispyware protects your computer against the security risks that can compromise your personal information and privacy.

Your Norton product protects your computer from vulnerabilities through the latest program updates and definition updates. Automatic LiveUpdate obtains the latest virus definitions through definition updates and

keeps your computer secure from the latest security threats.

You can use the following Antispyware and Updates settings:

Antispyware	Antispyware options let you choose which categories of risk you want Norton Security to detect for Auto-Protect, manual, and email scans.

Updates	Definition updates contain the information that lets your Norton product recognize and alert you to the presence of a specific virus or security threat. You can use the options under **Updates** to obtain the latest virus definitions through definition updates and keep your computer secure from the latest security threats. Your options are: ▪ **Automatic LiveUpdate** Automatic LiveUpdate automatically checks for definition and program updates when you are connected to the Internet. ▪ **Apply updates only on reboot** Lets you choose how the program updates obtained by Automatic LiveUpdate need to be applied to your computer. Certain program updates may require you to restart your computer for the updates to complete. When you turn on this option, program updates that require system restart are automatically applied the next time you restart your system. However, program updates that do not require system restart are applied instantly. By default, this option is turned off. This option is available only in Windows 7 or later.

About the Intrusion and Browser Protection settings

Intrusion Prevention scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects your computer against most common Internet attacks.

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. The Norton product runs LiveUpdate automatically to keep your list of attack signatures up to date. If you do not use Automatic LiveUpdate, you should run LiveUpdate once a week.

The Norton product also provides the Browser Protection feature to protect your browser from malicious programs.

The Browser Protection feature is available for Internet Explorer 7.0 or later, Chrome 17.0 or later, and Firefox 10.0 or later.

With increasing Internet use, your browser is prone to attack by malicious websites. These websites detect and exploit the vulnerability of your browser to download malware programs to your system without your consent or knowledge. These malware programs are also called drive-by downloads. The Norton product protects your browser against drive-by downloads from malicious websites.

The **Intrusion and Browser Protection** settings also include the **Download Intelligence** option to protect your computer against any unsafe file that you download. Download Intelligence provides information about the

reputation level of any executable file that you download using the browser. Download Intelligence supports only downloads using the HTTP protocol, Internet Explorer 6.0 browser or later, Chrome 10.0 browser or later, and Firefox 3.6 browser or later. The reputation details that Download Intelligence provides indicate whether the downloaded file is safe to install. You can use these details to decide whether you want to install the executable file.

Turning on or turning off Remote Management

Remote Management lets you remotely manage your Norton product using your Norton account and Norton Studio app. Norton Studio is a Windows 8 Store application and works only on Windows 8. 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 and Norton Studio app. 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 Remote Management

1. In the Norton Security 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 the left to the **On** position.
4. Click **Apply**, and then click **Close**.

To turn off Remote Management

1. In the Norton Security 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 the right to the **Off** position.
4. Click **Apply**, and then 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.

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**.

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.
3 In the list of currently installed programs, do one of the following:
   - In Windows XP, click **Norton Security**, and then click **Change/Remove**.
   - In Windows Vista, Windows 7, or Windows 8, click **Norton Security**, 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 the Norton product Settings password

You can protect your Norton product Settings with a password using the **Settings Password Protection** option. If the **Settings Password Protection** option is turned on, you need to enter the Settings password each time to view or configure your Norton product settings. You cannot access the product settings without providing your Settings password.

In case you forget your Settings password, you can reset it using the **reset settings password** option in the **Select Your Uninstall Preference** window.

You can turn off the **Settings Password Protection** option if you do not require password protection for the Norton product settings.

To turn off the Norton product Settings password

1. In the Norton Security main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the dialog box that appears, in the **Password** box, type your Settings password, and then click **OK**.
4. Under **Product Security**, in the **Settings Password Protection** row, move the **On/Off** switch to the right to the **Off** position.
5. 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.

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

To secure your Norton product Settings using a password

1. In the Norton Security 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 the left to the **On** position.
4. Do one of the following:
   - In the **Settings Password Protection** row, click **Configure**.
   - In the **Settings** window, 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**.

About Norton Product Tamper Protection

Norton Product Tamper Protection prevents outside programs from making changes to the Norton product. This security feature also prevents Windows System Restore from changing Norton files, which results in the **Restoration Incomplete** message.

Norton Product Tamper Protection protects Norton Security 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.

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.

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.

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 Norton Product Tamper Protection

1. In the Norton Security main window, click **Settings**.
2. Under **Product Security**, in the **Norton Product Tamper Protection** row, move the **On/Off** switch to the right to the **Off** position.
3. Click **Apply**.
4. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Norton Product Tamper Protection.
5. Click **OK**.
6. In the **Settings** window, click **Close**.

To turn on Norton Product Tamper Protection

1. In the Norton Security 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 the left to the **On** position.

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

Finding additional solutions

12

This chapter includes the following topics:

- Finding the version number of your product
- Finding the End-User License Agreement
- About upgrading your product
- Solving problems with Norton Autofix
- Reasons for Fix Now failures
- About Support
- 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 Security main window, click **Help**.
2. In the **Help** drop-down menu, click **About**.
   You can note the version number of your product in the window that appears.

Finding the End-User License Agreement

End-User License Agreement (EULA) is a legal document that you agree to while installing the product. EULA contains information such as the restriction on sharing or usage of the software, the user rights on the software, and other terms and conditions.

To know more about product license agreements and third-party notices, visit the EULA page.

To find the End-User License Agreement

1. In the Norton Security main window, click **Help**.
2. In the **Help** drop-down menu, click **About**, and then click **User License Agreement**.
3. Read the Norton License Agreement and click **Close**.

About upgrading your product

Norton Security helps you upgrade your product if you have an active subscription. You can upgrade your current product to the latest version without any cost as long as you have an active subscription with the current product. If a new version of your product is available, Norton Security lets you download the new version.

The **Automatic Download of New Version** option automatically downloads the latest available version of Norton Security and prompts you for free installation. To get the latest version of Norton Security as made available by Symantec, you need to turn on the **Automatic Download of New Version** option. To turn on the **Automatic Download of New Version** option, go to the Norton Security main window and then click **Settings > Administrative Settings > Automatic Download of New Version > On**.

If you choose to install the latest version of the product, Norton Security downloads and seamlessly installs the latest version. Ensure that you have saved all your important data such as pictures and financial records before you install the new version of the product.

If you download and install the latest version of your product, your subscription status remains the same as your previous version of product. For example, you have 200 days of subscription left with your current version of product and you upgrade your product to the latest version. In this case, the subscription status of your upgraded product remains 200 days only.

If a new version is not available, the webpage informs you that no new version is available and your product is up to date. Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats.

Product upgrade is different from the protection updates that are processed by LiveUpdate. The main differences are as follows:

- Product upgrade lets you download and install a new version of the entire product.
- Protection updates are the files that keep Norton Security up to date with the latest antithreat technology.

If a new version of the product is not available, ensure that you have all the latest protection updates. LiveUpdate automates the process of obtaining and installing protection updates. You can run LiveUpdate or turn on Automatic LiveUpdate to obtain the latest updates.

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.

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

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 Norton Security 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.

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 Security main window, click **Help**.
2. In the **Help** drop-down menu, click **New Version Check**.
   The website displays whether a new version is available or not.

   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

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 the Norton Security 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.

Support offerings can vary based on the language or product.

When you click the **Get Support** option in the **Help** drop-down menu, Norton Security 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 Norton Security. For more information, See "Configuring Network Proxy Settings" on page 41.

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 Security main window, click **Help**.
2. In the Help drop-down menu, click **Get Support**.

3 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 Symantec 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 94.

- **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. For instructions, See "How to run Norton LiveUpdate manually" on page 39.

- **LiveUpdate failure**

  If **LiveUpdate** fails, **Fix Now** also fails. To solve common issues with **LiveUpdate**,

- **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 Norton Security" on page 195.

- **Firewall does not allow the traffic**

  Make sure your product's Firewall settings are enabled to allow traffic. For more information, See "Turning off or turning on Smart Firewall" on page 132.

- **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**. For more information, See "How to run Norton LiveUpdate manually" on page 39.

About Support

If you have purchased Norton Security, you can access Support from the product.

Support offerings may vary based on the language or product.

About Norton Support

The Norton Support website provides a full range of self-help options. You can access Norton Support from the product.

By using Norton Support website, you can do the following:

- Find help with your product download, product subscription, product activation, product installation, and other issues.
- Download older product manuals.
- Manage your products and services using Norton account.
- Search Norton Forum to get more help about installing, configuring, and troubleshooting your Norton product. You can post your questions in the forum and get answers from other users and experts. You may find the forum a place where you can share tips, ideas, and suggestions about the Norton product. You need to first register for Norton Forum to start posting your questions.
- Find information about the latest viruses and risks, and find tips that help you stay protected.

- Access Norton Online Store and Norton product download page.

Support offerings may vary based on the region, language, or product.

To know more about the Support offerings, see the Support Policy page.

In addition to the self-help options, you can use the **Contact Us** option at the top of the webpage to contact the technical support team in the following ways:

Live Chat	Chat in real time with a support representative. For more complex technical issues, chat offers the option to allow a support representative to connect remotely to your computer and resolve your problem.
Phone	Speak to a support representative in real time.
Norton Forums	Search for additional product help about installing, configuring, and troubleshooting errors.

About keeping your subscription current

Subscription period lengths vary for each Norton product. To maintain uninterrupted protection, you must keep your subscription active. If your subscription expires, you cannot obtain updates of any kind and the product no longer functions.

You can use Norton Automatic Renewal service to get uninterrupted protection by automatically renewing your subscription at the regular subscription price. For more

information on this service, go to the Norton Automatic Renewal service FAQ page.

When you renew your subscription, the protection updates and new product features are available throughout the subscription period. Please note that features may be added, modified, or removed during this period.

You can know more about your subscription from the Norton account website. To access your Norton account, from the Norton Security main window, click **Help** > **Account**.

To know the various offerings from Norton, visit http://us.norton.com/comparison/promo.

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 8 **Start** screen.

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 How to download and install my Norton product on my device.

During uninstallation, your Norton product offers to leave the Norton Identity Safe for free to search and browse safely over the Internet even after the product is uninstalled. You can choose to keep the Norton Identity Safe that comprises Norton Safe Search and Norton Safe Web features without any cost. Norton Safe Search provides site safety status and Norton rating for each

of the search results generated. Norton Safe Web analyses the security levels of the websites you visit and indicates if the websites are free from threats.

Your computer must be connected to the Internet to avail this option. Norton Security does not offer to leave the Norton toolbar if you upgrade your product to the latest version or choose to reinstall another Norton product.

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**.
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 later, click **Programs > Programs and Features**.

     The **Programs** option in Windows 7 or later is available when you select the **Category** option in the **View by** drop-down list.
3. In the list of currently installed programs, do one of the following:
   - In Windows XP, click **Norton Security**, and then click **Change/Remove**.
   - In Windows Vista, Windows 7, or Windows 8, click **Norton Security**, and then click **Uninstall/Change**.

4 In the page that appears, 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 toolbar after uninstall, click **Keep & Continue**.
- To uninstall your Norton product without keeping the Norton toolbar, click **No, Thanks**.

6 To uninstall your Norton product, click **Next**.

7 Do one of the following:

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

Norton Security 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 > Norton Security > Uninstall Norton Security**.

2 In the page that appears, 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.

3 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**.

4 To uninstall your Norton product, click **Next**.

5 Do one of the following:

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

Norton Security is not fully uninstalled until you restart your computer.

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

1 On the **Start** screen, right-click **Norton Security**, and then click **Uninstall**.

2 In the list of currently installed programs, click **Norton Security**, and then click **Uninstall/Change**.

3 In the page that appears, 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 Identity Safe after uninstall, click **Keep & Continue**.
- To uninstall your Norton product without keeping the Norton Identity Safe, click **No, Thanks**.

5 To uninstall your Norton product, 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.

Index

A

accessing Norton Security scans
  Computer Scan 77
  Facebook Scan 77
  Reputation Scan 77
Activation
  using license or key 7
activation
  problems 10
  troubleshooting 10
Add Rule Wizard
  opening 141
  using 141
Address Book Exclusions
  setting 183
addresses
  adding allowed 185
  adding blocked 187
  importing allowed 185
adware
  about 179
  found by Auto-Protect 116
  in freeware programs 179
Alerts
  performance 48
  search 285
  security history 262
  Worm Blocking 121
Allowed List 185
Antiphishing
  about 203
  hiding the toolbar 250
  showing the toolbar 250
  turning off 206
  turning on 206
AntiSpam
  about 180
  Address Book Exclusions 183
  Allowed List 185
  Blocked List 187
  Client Integration 182
  Feedback 189
  Web Query 189
Antispyware
  about 319
Apply updates only on reboot
  turning off or turning on 39
attacks
  network 131
Auto-Protect
  functions 294
  notifications 116
  turn off or turn on 298
AutoBlock
  a device 170
Automatic LiveUpdate
  turning off or turning on 37
Automatic Program Control
  turning on and off 137

Automatic protection
about 305
automatic tasks
turn off or turn on 125

B

background jobs
monitoring 61
backup
Identity Safe data 240
Backup and Restore
about 240
Bandwidth
defining usage 195
Blocked List 187
blocking
spam 180
Boot Time Protection
configure 109
Browser Protection
about 322
turn off or turn on 160
Browsing
options 243
Browsing Options
about 243

C

Cards
about 231
adding 232
deleting 234
duplicating 234
update image 232
updating 234
Cleanup
browser cache files 258
cache files 258
how to 259
Internet temporary files 258
Cleanup *(continued)*
websites cache files 258
Computer
protecting 113
computer
blocking with AutoBlock 169
protection status 17
Configure
30-Day Report 70
automatic tasks 125
background jobs 61
Blocked list 187
boot time protection 109
client integration 182
download insight notifications 162
early launch anti-malware protection 110
Identity Safe 219
idle time out 128
performance alerts 50
power source 62
quiet mode 106
resources threshold 52
settings password 326
silent mode 103
Configuring
Automatic LiveUpdate 37
connections 112
CPU graph
obtaining historical data 56
resource-consuming processes 57
CPU usage
about 56
viewing 56
custom scans
adding files 85
adding folders 85
configure scan options 82
creating 85

custom scans *(continued)*
deleting a scan 87
editing 86
running a custom scan 86
scheduling 88
select items 84
Custom task
backup 126
disk optimization 126
file cleanup 126
LiveUpdate 126
customer support
about 337
customizing
Allowed List 185

D

device
changing trust level 175
purging from exclusion list 172
Device trust
add a device 173
Diagnostic Report
running 259
disk fragmentation
about 255
disk optimization
how to 256
disks
cleaning up 258
domains
adding allowed 185
adding blocked 187
Download Insight
configuring alerts 163
Download Insight notifications
turn off or turn on 162
Download Intelligence
turn off or turn on 161

E

Early launch anti-malware protection
turn off or turn on 110
email
spam 180
Email port
remove from protected ports 193
emergency
preparations 73
EULA
of Norton Security 331
Events graph
accessing 44
CPU usage meter 56
monitoring activities 45
exclusion list
remove a program 55

F

Feedback
Norton AntiSpam 189
file extensions
of infected files 123
File IDs
clearing 99
File Insight
about 281
filter
importing allowed 185
Web Query 189
filtering
identifying email senders 185, 187
SSL 180
Firewall 131
firewall rules
about 133
adding 141
changing the order of 152
creating 141

firewall rules *(continued)*
modifying 151
processing order 136, 152
removing 154
turning on and off 153
Full System Scan
run a scan 79
scheduling 90

H

high-risk security threats
excluding from scanning 98

I

Identity Safe
about 207
accessing 217
backing up 241
changing password 246
configuring 219
logging in and out 218
logins 224
Norton toolbar 218
restoring data 241
turning off 210
Identity Safe profiles
about 211
Identity Safe settings
scam insight 202
Idle Time Optimizer
about 60
turn off or turn on 60
Idle Time Out
setting durartion 128
integration with email clients 182
Internet
connection problems 112
Intrusion AutoBlock
blocking computers permanently 170
Intrusion AutoBlock *(continued)*
turn off or turn on 169
unblocking computers 170
Intrusion Prevention
about 322
exclusion list 171
turn off or turn on 301
turning individual notifications on and off 166
Intrusion Prevention notifications
turn off or turn on 166
Intrusion Prevention scan
exclusion list 171
purging devices 172
remove devices 172

K

keystroke logging 179

L

LiveUpdate
about 35
Login
adding manually 227
configuring 219
creating new folder 227
deleting 227
editing 227
managing 227
saving 226
low resource profile on battery
turn off or turn on 53

M

main window
messages 111
maintaining protection
about 73
avoiding security risks 73

Manage
startup items 260
Manage Logins
about 224
Manual Repair window
reviewing remaining risks in 80, 123
Media Center Extender
Silent Mode 102
Memory graph
about 56
obtaining historical data 56
messages 111

N

Network
changing trust level 175
Network Cost Awareness
defining bandwidth 195
turn off or turn on 194
Network Proxy Settings
configuring 41
new version
check 332
upgrade 331
Norton account
create 19
reset password 19
Sign In 19
Norton AntiSpam 180
about 180
Address Book Exclusions 183
Feedback 189
SSL 180
Web Query 189
Norton Autofix
solve problems 334
Norton Bootable Recovery Tool
about 20
accessing 27
creating ISO file 25
Norton Bootable Recovery Tool *(continued)*
creating on DVD 24
creating on USB 26
updating definitions 30
using 28
Norton Bootable Recovery Tool Wizard
downloading 23
Norton Community Watch
turn off or turn on 300
Norton Family
about 296
settings 296
Norton Firewall Diagnosis
about 155
Norton Insight
about 63
check trust level 68
Files of Interest 66
refreshing trust level 66
trusted files 63
viewing processes 66
Norton LiveUpdate
about 35
how to run 39
Norton Power Eraser
scan 94
Norton Product Tamper Protection
about 327
turn off or turn on 328
Norton Safe Search
searching Web 201
Norton Safe Web
about 197
enabling 97
Scan Facebook Wall 95
turning off 201
turning on 201
Norton Security
activation 7

Norton Security *(continued)*
boot time protection 109
custom tasks 126
EULA 331
icons 33
idle time out 128
main window 11
maintaining your subscription 338
new version 332
Norton Autofix 334
optimization 255
password 326
quiet mode 104
remote management 323
security history 262
security status 31
settings 303
settings password 325
shortcut menu 33
silent mode 100–102
starting from the command prompt 31
system status 11
uninstalling 339
upgrade 331
version number 330
Norton Security Scan
file insight 281
Norton Security scan
about 74
accessing Norton Security scans 77
command line scanning 92
Computer Scan 74
Facebook scan 74
Full System Scan 79
Idle Time Scan 74
Insight Network scan 74
Quick Scan 80
Reputation Scan 74
Norton Security settings
resetting password 324
Norton Support
website 337
Norton toolbar
about 247
settings 217
Notes
deleting 235
saving 235
updating 235
notification area icon 111
notifications
Intrusion Prevention 166

O

Online transactions
identity theft 207
Optimization
about 58
best practice 257
boot volume 59
defragment boot volume 60
run manually 256
Options
Client Integration 182

P

password
changing 246
editing 227
saving 226
strong 251
Performance
about alerts 48
disk cleanup 258
disk fragmentation 255
disk optimization 256
file fragmentation 255
monitoring 56

Performance *(continued)*
optimize boot volume 59
run disk cleanup 259
performance alerts
configure low resource profile 53
configure threshold 52
excluding programs 54
removing programs from exclusion list 55
turning off or turn on 50
Performance scans
scheduling 127
Personal data
backing up 241
Personal Firewall
turn off or turn on 301
PIN
locate 9
See also product key
POP3 port 192
port scans 131
Power source
configure 62
preparing for emergencies
maintaining protection 73
Product Key
locate 9
See also PIN
Program Control
turning on and off 137
Program Rules
adding programs 137
customizing 140
removing programs 139
Program rules
adding 141
changing 151
removing 154
programs
adding to Program Rules 137
configuring Internet access 141
programs *(continued)*
creating firewall rules 141
removing from Program Rules 139
Protected ports
adding POP3 and SMTP 192
email port removal 193
Protection
settings 305
protection
maintaining 111
preparing for emergencies 73
system scans 79
Protection features
Auto-Protect 294, 298
Automatic LiveUpdate 294
disable 298
Email protection 294
Heuristic protection 294
Norton Community Watch 300
smart firewall 301
spam filter 299
Protection updates
about 319
definition updates 36
get manually 39
last updated date 39
program updates 36
proxy server
configuring 41

Q

Quarantine
add an item 290
adding items 265
managing items 287
restore items 291
security history 262
submit for analysis 292
worm-infected file 121

Quick Controls
turn off or turn on 305
Quick Scan
run a Insight Network Quick Scan 80
run a scan 80
scheduling 90
Quiet Mode
about 104
disk burning 104
options 106
turn off or turn on 106
TV recording 104
User-Specified Programs 107

R

Remote management
turn off or turn on 323
repair
actions 123
infected files 123
removable media 123
system files 123
report
turn off or turn on 70
Responding
about 113
responding to emergencies 113
restore
Identity Safe data 240
restoring items
Quarantine 291
Results Summary
about 82
resolved risks 82
total items scanned 82
Risks
add to Quarantine 290
detection of 115
responding to 123
restore from Quarantine 291
Risks *(continued)*
submit from Quarantine 292
risks
intrusions 131
port scans 131
rules
changing 141, 151
creating 141

S

Safe Web
turning off 201
turning on 201
Scam Insight
turn off or turn on 202
scan at the command prompt
command line scanning 92
Scan Complete
appearing after a scan 123
Scan Complete window
appearing after a scan 79–80
Scan Facebook Wall
about 95
enabling 97
scanned
total items scanned 82
scanning
entire computer 79
individual elements 80
Scans
clearing file IDs 99
command line 92
Computer Scan 78
Custom Scan 78
custom scan 82, 126
deleting custom scans 87
editing a scheduled scan 91
editing custom scan 86
excluding threats 98
Facebook scan 95, 97
file 80

Scans *(continued)*
floppy disk 80
folder 80
Full System Scan 78
hard drive 80
problems found during 123
protection features 294
Quick Scan 78
removable drive 80
running custom scans 86
scheduling a quick scan 90
scheduling custom scans 88
scheduling full system scan 90
security and performance scans 127
security history 262
security risk found 114
using Norton Bootable Recovery Tool 28
using Norton Power Eraser 94
worm alerts 121
scheduled scan
editing 91
Security History
about 262
adding items to the Quarantine 265
firewall alerts 265
full alert history 265
import or export 286
manual scan results 265
network alerts 265
opening 264
Quarantine 287
Quick Search 285
recent alert history 265
resolve risks 123
searching 285
security risks 265
submission, items to Symantec 265
Security History *(continued)*
suspicious email 265
traffic alerts 265
viewing items 265
viewing quarantined items 265
security risks
about 179
attacks 131
found by Auto-Protect 114, 116
managing protection using the main window 179
other programs 179
port scans 131
Security scans
scheduling 127
Security Status
responding to 31
security status indicator
viewing 17
Settings
browser protection 160, 322
customizing 303
download intelligence 161
intrusion protection 322
network cost awareness 195
Norton Product Tamper Protection 328
Quick Controls 305
remote management 323
scans and risks 312
web query 191
settings password
resetting 324
turn off 325
Settings Password Protection
configuring 326
resetting 324
turn off 325
Signature Ezclusions
excluding items 99

signatures
including and excluding 167
Silent Mode
Full Screen Detection 102
turn off or turn on 101, 103
turn on automatically 102
turn on manually 100
Smart Firewall
about 131
customizing 133
turn off or turn on 132
SMTP port 192
SONAR Protection
turn off or turn on 97
Spam filter
turn off or turn on 299
spyware
about 179
detection of 115
found by Auto-Protect 116
managing protection using the main window 179
settings 305
SSL (Secure Sockets Layer)
Norton AntiSpam 180
startup items
delay and run 260
disable or enable 261
Startup Manager
delay and run delayed items 260
disable or enable startup items 261
subscription
maintaining 338
Support
chat, phone, forum 337
Self Help 337
Symantec Security Response
item submission 292
viewing submitted files 265
system activities
viewing the details 47
System Insight
about 43
Events graph 43
monitoring activities 45
Performance graph 43
system status graph
activity details 47

T

Taskbar icons
about 33
technical support
about 337
Threats
avoiding 73
infected items 83
protection from 131
resolve any items 83
submit from Quarantine 292
threat detected window 283
Threats Detected
about 83
resolving the risk 83
Traffic Rules
adding 141
changing 151
removing 154
trust level
changing 175
device 175
network 175

U

User-Specified Programs
about 107
adding programs 108
Quiet Mode 107
removing programs 109

V

version number
checking 330
virus and spyware
settings 305
virus protection
about 294
instant messenger 294
system scans 79
updates 294
Viruses
automatic protection 294
descriptions 294
detection of 115
submit from Quarantine 292
unknown threats 294

W

Web Query
about 189
turn off or turn on 191
webpages
protection 203
reporting 207
Worm alerts
responding to 121
worms
found by Worm Blocking 121
in email messages 121

Norton from Symantec products protect consumers from traditional threats with antivirus, antispam, and Spyware Protection. They also protect against bots, drive-by downloads, and identity theft, and are light on system resources. In addition, Symantec provides services such as online backup and PC Tuneup, and is a trusted source for family online safety. For more information, please click one of the following links:

Antivirus | Antispam | Spyware Protection | Online Backup