

# 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

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

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Norton, and LiveUpdate, are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Macintosh, Mac, Mac OS, the Mac logo, Safari, Tiger, Snow Leopard and Lion are trademarks of Apple Computer, Inc. Firefox is a registered trademark of Mozilla Corporation. Other names may be trademarks of their respective owners.

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

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

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

Symantec Corporation  
350 Ellis Street,  
Mountain View, CA 94043  
<http://www.symantec.com>

# Contents

Chapter 1	Getting started .....	8
	About Norton Security .....	8
	About the Norton product main window .....	14
	Opening and closing Norton Security on Mac .....	18
	About the Norton Security menu .....	19
	About the Norton Security shortcut menu .....	20
	How to check your Mac user account type .....	21
	Viewing recent activities .....	21
	Viewing network activities .....	23
Chapter 2	Activating your product .....	25
	Activation protects you .....	25
	Activating your Norton product on Mac .....	26
	Where to find your product key .....	27
Chapter 3	Managing Norton products .....	30
	Creating a Norton account .....	30
	Accessing your Norton account .....	31
Chapter 4	Identifying fraudulent websites .....	32
	About Safe Web .....	32
	Disabling or enabling Safe Web .....	34
	About Norton Safe Web .....	34
	About Norton Phishing Protection .....	36

	Disabling or enabling Norton Phishing Protection .....	37
	About Norton toolbar .....	38
Chapter 5	Guarding files .....	42
	About File Guard .....	42
	Disabling or enabling File Guard .....	43
	Adding files to File Guard .....	43
	Removing files from File Guard .....	44
	Granting access to guarded files for Mac OS X applications .....	45
	Turn on or turn off guarded file access notification .....	46
Chapter 6	Scanning your Mac manually .....	47
	About Norton Security scans .....	47
	Running a Quick Scan .....	48
	Running a full system scan .....	49
	Scanning a specific file or folder .....	50
	About Scan Facebook Wall .....	50
	Scanning your Facebook wall .....	52
	Running scans from the command line .....	53
Chapter 7	Keeping secure on the Internet .....	54
	About Vulnerability Protection .....	54
	Turning off or turning on Vulnerability Protection .....	55
	Excluding or including attack signatures .....	55
	Getting information about attack signatures .....	57
	Enabling or disabling notifications for blocked attack signatures .....	57
	Configuring the port scan sensitivity .....	59

Chapter 8	Customizing settings .....	61
	About Automatic Scans settings .....	63
	Turning off or turning on Automatic Scans .....	64
	Including files for Automatic Scans .....	65
	Excluding files from Automatic Scans .....	66
	Removing files from the Automatic Scans exclusion list .....	66
	Removing files from Automatic Scans list .....	67
	About Scheduled Scans .....	67
	Turning on or turning off Scheduled Scans .....	68
	Customizing Scheduled Scans settings .....	68
	About Idle Scans .....	71
	Turning off or turning on Idle Scans .....	72
	Customizing Idle Scans settings .....	73
	About Firewall settings .....	75
	About Connection Blocking settings .....	80
	Configuring Connection Blocking settings .....	81
	About access settings for an application .....	84
	Configuring the access settings for an application .....	85
	Customizing the specific access settings for an application .....	87
	Editing the access settings of an application .....	89
	Removing access settings for an application .....	94
	About access settings for a service .....	95
	Configuring the access settings for services .....	96
	Customizing the specific access settings for a service .....	99
	Editing the access settings for a service .....	101

Removing the access settings for a service .....	103
About firewall rule for IP addresses .....	105
Configuring firewall rules for an IP address .....	106
Modifying firewall rules for an IP address .....	107
Removing firewall rule for an IP address .....	108
About configuring firewall for an application .....	109
Setting up firewall rules for an application .....	110
Customizing the firewall rule for an application .....	111
Removing the firewall rule for an application .....	112
About Location Awareness settings .....	112
Disabling or enabling Location Awareness .....	113
Viewing Location Awareness settings .....	113
Exporting the connection blocking settings for a network location .....	114
About advanced protection .....	115
Disabling or enabling advanced protection features .....	117
Configuring Norton DeepSight Community Download .....	118
Configuring Norton DeepSight Community Submission .....	119
Configuring AutoBlock settings .....	120
Managing Excluded IP addresses .....	121
Configuring Signatures settings .....	123
Chapter 9	
Managing items in Quarantine .....	125
About Norton Security Quarantine .....	125
Repairing an item in the Quarantine .....	125
Restoring an item from the Quarantine .....	126

	Deleting an item from the Quarantine .....	127
Chapter 10	Protecting against new threats .....	128
	About LiveUpdate .....	128
	About program updates and definition updates .....	128
	Checking for updates manually .....	129
Chapter 11	Finding additional solutions .....	131
	Checking for virus names and definitions .....	131
	Uninstalling Norton Security on Mac .....	132
Chapter 12	Service and support solutions .....	133
	About support .....	133
	About Self Help .....	135
	Contact Support .....	135
	Support Policy .....	136
	Keeping your subscription current .....	136

# Getting started

# 1

This chapter includes the following topics:

- [About Norton Security](#)
- [About the Norton product main window](#)
- [Opening and closing Norton Security on Mac](#)
- [About the Norton Security menu](#)
- [About the Norton Security shortcut menu](#)
- [How to check your Mac user account type](#)
- [Viewing recent activities](#)
- [Viewing network activities](#)

## About Norton Security

Norton Security delivers today's fast and light all-in-one solution to protect your Mac and all your online activities.

Norton Security delivers continuous and up-to-date protection from different types of security threats. Norton Security protects you from identity theft attempts, phishing attempts, and other network attacks. It analyzes the security levels of the websites you visit and indicates whether the website is secure. In addition, it protects your sensitive data including your credit card and online banking details from the malicious programs.



Norton Security monitors the network activity of your Mac and manages the incoming and the outgoing access attempts. The Firewall settings contain the rules that specify the access settings for the applications, services, and ports in your Mac. It also contains access settings for the IP addresses in the network to which your Mac is currently connected. Based on the firewall rules, Norton Security allows or blocks the incoming or the outgoing connections that use a particular application, service, or port.

Norton Security provides enhanced security and protects your Mac in the following ways:

- Automatically detects and removes viruses.
- Scans and cleans downloaded files and email attachments.
- Protects against the attacks that target software vulnerabilities.
- Checks for security risks every time you use a program on your Mac, insert removable media, or access the Internet.
- Monitors your computer for any unusual symptoms that may indicate an active threat.
- Prevents identity thefts and phishing attempts.
- Protects sensitive information from malicious programs. Monitors the network activity and blocks unauthorized access attempts.



Symantec does not collect or store any of your personal information. Your information remains encrypted and secure on your Mac.

The following table lists the important features that are available in Norton Security:

<b>Automatic Scans</b>	<p>Automatically detects and removes spyware, viruses, Trojan horses, bots, and Internet worms.</p> <p>Norton Security provides enhanced security and protects your Mac in the following ways:</p> <ul style="list-style-type: none"><li>■ Checks for security risks every time you use a program on your computer, insert removable media, and access the Internet.</li><li>■ Monitors your computer for any unusual symptoms that may indicate an active threat.</li></ul> <p>You can use the Automatic Scans options to customize the protection of your computer.</p> <p>See <a href="#">“About Automatic Scans settings”</a> on page 63.</p>
------------------------	---

**Firewall**

Monitors the network activity of your Mac and manages the incoming and the outgoing access attempts.

The Connection Blocking settings contain the rules that specify the access settings for the applications, services, and ports in your Mac. It also contains access settings for the IP addresses in the network to which your Mac is currently connected. Based on the firewall rules, Norton Security allows or blocks the incoming or the outgoing connections that use a particular application, service, or port.

**Vulnerability Protection**

Blocks any network attacks that can steal your information or take control of your Mac.

See [“About Vulnerability Protection”](#) on page 54.

## Scans

Lets you perform the following types of scans:

### ■ Quick Scan

Lets you scan the home folders on your Mac.

### ■ Full Scan

Lets you select and scan multiple disks to remove viruses and other security threats.

### ■ File Scan

Lets you scan a particular file or folder on your Mac to know if it is infected.

### ■ Scan Facebook Wall

Lets you scan News Feeds on your Facebook wall periodically to protect you from malicious links.

See [“About Norton Security scans”](#) on page 47.

## LiveUpdate

Automatically downloads the latest virus definitions and program updates to safeguard your Mac. The virus definitions protect your Mac from the latest viruses and security threats.

<b>Safe Web</b>	<p>Lets you enable or disable the different Safe Web options that protect you from visiting unsafe websites.</p> <p>You can enable or disable the following Safe Web options:</p> <ul style="list-style-type: none"><li>■ Safe Web</li><li>■ Norton Phishing Protection</li></ul> <p>See <a href="#">“About Safe Web”</a> on page 32.</p>
<b>File Guard</b>	<p>Lets you protect the specific files that contain sensitive information from being opened, moved, copied, or deleted without your permission.</p> <p>See <a href="#">“About File Guard”</a> on page 42.</p>
<b>Activity</b>	<p>Lets you monitor the tasks that your product performs in the background. In addition, you can view the statistics of the access attempts and the statuses of different features of Norton Security.</p>

What to do if Norton Security quits unexpectedly?  
FAQs on Norton Automatic Renewal Service

## About the Norton product main window

Your Norton product delivers today's fast and light all-in-one solution to protect your Mac and all your online activities.

Your Norton product main window provides you a centralized location for the various activities that you can perform using the product. You can access the main features of the product from the main window and manage the performance of your Mac.



You cannot access Norton account if you are a Norton Small Business user.

You can use the following options to perform the important tasks in your Norton product:

### Security

Lets you view the overall protection status of your computer.

When your system status is **Secure**, your computer is fully protected. When your system status is at **Attention** state, ensure that you fix all the issues. When your system status is at **At Risk** state, you must take immediate actions to fix the issues.

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

## Scans

Lets you access different types of scans to protect your computer and your sensitive data.

You can use the **Scans** option and run the following types of scans:

- **Quick Scan:** Scans the home folders on your Mac.
- **Full Scan:** Scans selected disks to remove viruses and other security threats.
- **File Scan:** Scans a particular file or folder on your Mac and removes any security threats.
- **Scan Facebook Wall:** Lets you scan News Feeds on your Facebook wall periodically to protect you from malicious links.
- **Scheduled Scan:** Lets you configure a scheduled scan. Norton Security automatically scans your Mac on the day and time that you specify.

### LiveUpdate

Lets you run LiveUpdate to download the latest virus definitions and program updates.

Norton Security uses the latest virus definitions from Symantec servers to detect and remove latest security threats.

What to do if I get a LiveUpdate error?

### Advanced

Lets you access the **Advanced** window.

You can do the following tasks in the **Advanced** window:

- Configure and schedule different scans.
- Change the Firewall settings.
- Configure Norton Safe Web for browsers.
- Safeguard the files that have your sensitive data.
- View Security History.
- View the quarantined items in the **Security History** window.
- View Network Activity history.
- Turn on Silent Mode and Error Reporting features.

In addition, you can choose to turn on or turn off the protection features from this window.




### Add Devices

Lets you install the latest version of Norton Security on other devices.

This ensures that your Mac and other devices are protected by Norton.

You can use the **Get Started** option to access your Norton account. You can use your Norton account login credentials to sign in to Norton.

After logging in, you can use the **Install on another device** option and follow the on-screen instructions to install the product on another device.

 Access to Norton account may not be available in some versions of Norton Security.

Your Norton product also provides you quick links at the top of the main window to the most frequent tasks. You can use the **Account** link to access your Norton account. You can use the **Help** link to do the following:

- Access your Norton account
- Access the online Help and support options
- Take a product tour
- Check your subscription status
- Add devices
- Enter a product key
- View product information such as version number, serial number, Third-Party notice, etc.

Your activation status or subscription status appears at the bottom of the main window. You can use the

**Activate Now** or **Renew Now** option to activate or renew your Norton product subscription.

FAQs on Norton Automatic Renewal Service

How to find your product key

## Opening and closing Norton Security on Mac

After you install Norton Security, the product automatically protects you from all types of malware and safeguards your sensitive data. If Norton Security detects a threat that requires your attention, an alert appears to help you resolve it. By default, all the protection features are enabled and Norton Security monitors your computer.

You can access Norton Security from the following areas:

- **Applications** folder
- **Norton QuickMenu**



You cannot close Norton Security if any of the Norton Security dialogs or alerts is open.

### To open Norton Security

- ❖ To open Norton Security, do one of the following:
  - In the **Applications** folder, click **Norton Security**.
  - On the Mac menu bar, click the Symantec icon, and then click **Open Norton Security**.

### To close Norton Security

- 1 If any of the Norton Security dialogs or alerts is open, close them.
- 2 To close Norton Security, do one of the following:
  - Click close on the Norton Security main window.
  - Right-click the **Norton Security** icon in the Dock, choose **Quit**.
  - Press **⌘Q**.

## About the Norton Security menu

The Norton Security menu appears on the top-left corner of the Mac menu bar when you launch Norton Security.

You can use the **Norton Security** option from the Norton Security menu to view the different menu options. You can access the following options from the Norton Security menu:

<b>About Norton Security</b>	Displays the general information of Norton Security.  You can view details such as the build number, layout, product serial number, endpoint ID, and SKU information.
<b>Services</b>	Lets you access the Mac OS X services settings.
<b>Hide Norton Security</b>	Lets you hide the Norton Security application.
<b>Hide others</b>	Lets you hide the other active applications on your Mac.
<b>Show All</b>	Displays all the active programs on your Mac.  This option is available only if you have used the <b>Hide Norton Security</b> option or the <b>Hide Others</b> option.

<b>Uninstall Norton Security</b>	Lets you uninstall Norton Security.  You need to have a user account with administrator privileges to uninstall Norton Security.
<b>Quit Norton Security</b>	Lets you close Norton Security.

You can use the **Export** option under the **File** menu to export your network location settings. You can export your network location settings in a .npfx file format. See [“Exporting the connection blocking settings for a network location”](#) on page 114.

## About the Norton Security shortcut menu

The Norton Security shortcut menu lets you easily access the Norton Security application and explore its features. You can access the Norton Security shortcut menu by control-clicking or right-clicking the Norton Security icon in the **Dock**.

You can perform the following activities using the shortcut menu:

- Open the Norton Security main window, the **Scans** window, the **LiveUpdate** window, and the **Advanced** window.
- Lets you install the latest version of Norton Security on other devices.
- Keep or remove the Norton Security icon from the **Dock**.
- Open Norton Security automatically each time you log on to your Mac.
- View the Norton Security application in the **Applications** folder.
- Show or hide Norton Security.

- Quit Norton Security.

## How to check your Mac user account type

A user account defines the actions a user can perform on a Mac. You can create the following types of user accounts on your Mac:

- Administrator account
- Standard account
- Managed account

Each account has different privileges. An administrator account gives you access to all areas of the Mac, install and update software, create and maintain other user accounts.

If you do not know your user account type, you can check it in **System Preferences**.

### To check your Mac user account type

- 1 On the **Apple** menu, click **System Preferences**.
- 2 Click **Users & Groups**.
- 3 On the left side of the **Users & Groups** window, view your account name and account type.

## Viewing recent activities

The **Security History** window lets you view all the recent tasks that your product performs in the background.

You can view the information about the recent activities under the following categories in the **Security History** window:

### General

Lets you view all the recent activities that Norton Security performed.

### Firewall

Lets you view the following:

- Applications that were allowed or blocked.
- Connection attempts that were allowed or blocked.
- Change in the network location of your Mac.
- Vulnerability attacks that were allowed or blocked.

### Safe Web & File Guard

Lets you view the list of activities that the Safe Web feature had performed and the unauthorized access attempts to your guarded files.

### Protect My Mac

Lets you view the following:

- List of detected viruses and the action that was taken against the virus to protect your Mac.
- List of virus scans that Norton Security performed on your Mac.
- List of quarantined files.

### To view the recent activities

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Activity**.
- 3 In the **Security History** row, click the view icon.
- 4 In the **Security History** window, select the category for which you want to view the recent activities.
- 5 View the recent activities and click **Done**.

## Viewing network activities

You can view the incoming and the outgoing network connection details in the **Network Activity** window.

You can also search for a particular type of application, service, port, or IP address that runs on your Mac and view its network connection details in the **Network Activity** window. You can view the information about the recent activities under the following categories:

### Connections

Lets you view the network connection details based on the type of connection.

Your options are:

#### ■ Into my Mac

Displays a list of all incoming connections to your Mac.

#### ■ Out of my Mac

Displays a list of all outgoing connections from your Mac.

#### ■ Listening

Displays a list of all of the applications that are on open ports for incoming traffic.

### **Search For**

Lets you view the network connection details based on the applications, services, or ports that run on your Mac.

Your options are:

#### **■ Applications**

Searches for and displays a list of the applications that are currently running on your Mac.

#### **■ Services & Ports**

Searches for and displays a list of the services and ports that run on your Mac.

### **To view the network connections**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Activity**.
- 3 In the **Network Activity** row, click the view icon.
- 4 In the **Network Activity** window, select an application, service, or port to view the details of the current network connections.
- 5 Click **Done**.



# Activating your product

# 2

This chapter includes the following topics:

- [Activation protects you](#)
- [Activating your Norton product on Mac](#)
- [Where to find your product key](#)

## Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software. It protects you by limiting the use of a product to those users who have acquired the product legitimately. Product activation requires a product key for each installation of a product. You must activate the product within a limited time period after you install it.

If you are connected to the Internet, the Norton product prompts you to enter your Norton account credentials. You can use your existing Norton account or register for a new Norton account. After signing in to your Norton account, your Norton product is automatically activated and registered to your Norton account.



You cannot access Norton account if you are a Norton Small Business user.

If you are not connected to the Internet, you can close the **Subscription** window to start your product. The **Subscription** window is displayed every time you start your product until you activate your product. If you

choose not to activate at that time, you receive an alert that reminds you to activate the product. You can also activate your product from the Norton Security main window.



If you do not activate the product within the time period that the alert specifies, the product stops working. You can activate it after the time period has elapsed, but you are not protected until you activate the product.

## Activating your Norton product on Mac

If you did not activate your product after installation, you receive a Subscription alert regularly until you activate the product.

Product activation reduces software piracy and ensures that you use authentic Symantec software. Activation provides you with a specified period of subscription to your Norton product.



You must activate your product within the time period that the alert specifies, or your product stops working. To activate, you need to use the product key that was included with this product.

You need a Norton account to activate your product. You can use your existing Norton account or register for a new Norton account. After signing in to your Norton account, you can enter the product key to activate your Norton product and register the product key to your Norton account. Your Norton account lets you view the details, such as the product key, the product registration date, and recent product updates.



You cannot access Norton account if you are a Norton Small Business user.

### To activate your Norton product

- 1 Do one of the following:
  - In the Activation alert, click **Activate Now**.
  - In the Norton Security main window, click **Activate Now**.

- 2 On the **Subscription** window, enter your Norton account credentials, and click **Sign In**. If you do not have a Norton account, click **Create a new Norton account** to register for an account.
- 3 You can activate your product in one of the following ways:
  - **Use a product key**  
To activate your product using a retail version of the product key that you purchased, click **Enter a Key**.
  - **Buy a new subscription**  
To purchase a product subscription online, click **Buy a Subscription**.
  - **Use existing subscription**  
After you sign in to your Norton account, the **Subscription** window displays the list of product licenses registered to your Norton account and the subscription details for the registered licenses. To use an existing subscription to activate your product, select the subscription, and then click **Next**.
- 4 Follow the on-screen instructions to complete the activation of your Norton product.

## Where to find your product key

The product key is a unique key that helps you to install and activate the Symantec 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. The location of the product key varies depending on how you acquired the product.

The locations of the product key are as follows:

If you downloaded the product from the Symantec Store

The product key is stored on your computer as part of the download process and is included in the confirmation email from the Symantec Store.

If your computer came with the product already installed

The product key is provided as part of the activation process. Be sure to save your product key by creating or signing in to your Norton account, or by printing the key. You may need the product key if you ever want to reinstall your product.

If you received a product key card

The product key is printed on the card along with instructions on how to use it. Be sure to save your product key by creating or signing in to your Norton account. You need the product key if you ever want to reinstall the product.

If you are still unable to locate your product key, you can recover it using Norton account

To recover or access your product key log on to <https://manage.norton.com>. If you are not registered, register for Norton account. If you are already registered, you can find the product key on the **Services** page.

🔒 You cannot access Norton account if you are a Norton Small Business user.


If you purchased a Norton card from a retail store

The product key is printed at the back of the Norton card.

Go to the following webpage and enter your product key:

<https://manage.norton.com/setup>

Norton validates the product key that you entered and prompts you to log in using a Norton account. After logging in using your Norton account, you can use the **Agree & Download** option to download and install your Norton product.



This chapter includes the following topics:

- [Creating a Norton account](#)
- [Accessing your Norton account](#)

## Creating a Norton account

With a Norton account, you can manage all of your Norton products in one place. Your Norton account stores the product key and the billing information of your product. You can also register your product with the Norton account.



You cannot access Norton account if you are a Norton Small Business user.

In addition, Norton account helps you to do the following:

- Access the product key and other product information when you need it.
- Reinstall your Norton product.
- Buy additional product keys for your home or office.
- Save online orders and update billing information.
- Disable the Automatic Renewal feature.



Symantec products that are older than 2006 do not appear in your Norton account.

It takes only a few moments to create your Norton account. You must be connected to the Internet to create a Norton account.

### To create a Norton account

- 1 Open your browser and go to the following URL:  
<https://manage.norton.com>
- 2 In the **Norton** webpage that appears, click **Create an Account**.
- 3 In the page that appears, click **Create account**.
- 4 In the **Create an account** webpage, provide the details of your account information, and then click **Sign Up**.

## Accessing your Norton account

The product key for each Norton product is conveniently stored in your Norton account. After you have created your Norton account successfully, you can access your account from anywhere in the world.



You cannot access Norton account if you are a Norton Small Business user.

You can log in to your Norton account any time by visiting the following URL:

<https://manage.norton.com>

You can easily find and update your account, product, and billing information from your Norton account. You can also change your Norton account password, if required. Your computer must be connected to the Internet to access your Norton account.



Symantec products that are older than 2006 do not appear in your Norton account.

### To access Norton account

- 1 Open Norton Security.
- 2 In the Norton Security main window, click **Account > Sign In**.
- 3 In the Norton account webpage, click **Sign In**.
- 4 Type your email address and password, and click **Sign In**.

# Identifying fraudulent websites

# 4

This chapter includes the following topics:

- [About Safe Web](#)
- [Disabling or enabling Safe Web](#)
- [About Norton Safe Web](#)
- [About Norton Phishing Protection](#)
- [Disabling or enabling Norton Phishing Protection](#)
- [About Norton toolbar](#)

## About Safe Web

Safe Web monitors your Internet activities and protects you from visiting unsafe websites. Safe Web includes the following features:

- Norton Safe Web
- Norton Phishing Protection
- Norton toolbar

Norton Safe Web provides you a safe search environment by displaying the site-rating icons next to every search result. Phishing Protection analyzes the security levels of the websites you visit and provides a safety rating for each website.



When **Safe Web** is enabled, Norton Security analyzes the security statuses of the websites and alerts you if you visit fraudulent or phishing websites.



The Norton browser extensions get added to your web browser when you launch the Firefox or Safari browser for the first time after you install Norton Security. The Safari browser prompts you for a confirmation before it adds the extension. You can also choose to add the **Norton Safe Search** box to the Norton toolbar when you launch your browser for the first time.

The following are the different options that you can configure under the Safe Web feature:

<b>Enhance search engine results</b>	Lets you configure Norton Safe Web to display the site-rating icons next to each search result.
<b>Block harmful websites</b>	Lets you configure Norton Safe Web to block harmful or malicious websites.
<b>Show a warning when visiting a harmful website</b>	Lets you configure Norton Safe Web to display a warning message when you visit harmful or malicious websites.
<b>Enable Norton Phishing Protection</b>	Lets you enable or disable Norton Phishing Protection.  The Phishing Protection analyzes the security levels of the websites you visit and displays the safety rating in the Norton toolbar.
<b>Submit full URL when a suspicious website is detected</b>	Let you submit the URL of the suspicious website to Symantec.

## Disabling or enabling Safe Web

You can disable or enable Safe Web from the Advanced window.

### To disable or enable the Safe Web

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the **Norton Security** main window, click **Advanced**.
- 3 On the left pane, click **Safe Web**, and do one of the following:
  - To disable Safe Web, move the **Safe Web** switch to the **Off** position.
  - To enable Safe Web, move the **Safe Web** switch to the **On** position.

## About Norton Safe Web

Norton Safe Web is a free service from Norton that helps you surf, search, and shop more safely.

By using Norton Safe Web, you can check if a website is malicious even before you visit it. Norton Safe Web analyzes websites and detects if any viruses, spyware, malware, other security threats exist on a website. Based on the analysis, Norton Safe Web provides safety ratings for all websites.

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

If you own a website and your website is not Norton rated, you can register your website for Norton safety ratings. Based on the analysis, Symantec provides a reputation rating for your website. The ratings are available on the Norton Rating report. These ratings help millions of Norton users to decide whether to visit your website.

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

The following are the options that you can use to configure Norton Safe Web:

**Enhance search engine results**

Lets you configure Norton Safe Web to display the site-rating icons next to each search result.

When you search the Internet using search engines like Google or Yahoo, Norton Safe Web displays the site-rating icons next to each search result.

**Show a warning when visiting a harmful website**

Lets you configure Norton Safe Web to display a warning message when you visit harmful websites.

When you select this option Norton Security displays a warning message when you visit harmful websites. Symantec recommends that you do not visit such websites.

**Block harmful websites**

Lets you configure Norton Safe Web to block harmful websites.

When you select this option Norton Security displays the **Website Blocked** page when you visit harmful websites. Symantec recommends that you do not visit such websites.

## About Norton Phishing Protection

Phishing Protection protects you from visiting unsafe websites. When Phishing Protection is turned on, the Antiphishing component analyzes the security level of the websites that you visit. It then displays the safety rating of the websites in the Norton toolbar. Antiphishing also blocks navigation to the websites that are confirmed to be fraudulent.

The **Norton Site Safety** indicator in the web browser lets you know if the website that you visit is safe.



The Norton browser extensions get added to your web browsers when you launch the Firefox or Safari browser for the first time after you install Norton Security. You can also choose to add the **Norton Safe Search** box to the Norton toolbar when you launch your browser for the first time.

The **Norton Site Safety** indicator displays all Norton Authenticated webpages as **Norton Secured**. Website hackers often mimic company websites to create fraudulent websites. Norton Security identifies these fraudulent websites. The authenticated websites are categorized as **Site Approved** websites. These websites usually belong to large financial institutions or shopping websites, with the pages that request personal information.

Symantec analyzes the pages of these websites 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.

If you think that the Symantec security status rating is incorrect, you can report the website to Symantec for re-evaluation. For example, you may visit a website that you shop with regularly, and Phishing Protection rates the website as unsafe. You can report the website to Symantec for re-evaluation.

You can select the **Submit full URL when a suspicious website is detected** option in the **Safe Web** window to submit the full URL of the suspicious website to Symantec.

Even when you disable the **Enable Norton Phishing Protection** option, Norton Security protects you from Internet threats through its **Norton Safe Web** feature. But you cannot submit the evaluation of the webpage to Symantec.

The Norton Phishing Protection feature is supported on Firefox and Safari web browsers.

The Norton toolbar displays the following safety ratings:

- **Site is Safe**
- **Site is Unsafe**
- **Use Caution**
- **Site Untested**
- **Norton Secured**
- **Not Licensed**

## Disabling or enabling Norton Phishing Protection

Phishing Protection protects you from visiting unsafe websites. It analyzes the security level of all the websites that you visit and displays the safety rating in the Norton

toolbar of your browser. Phishing Protection also blocks navigation on a fraudulent website.

You can disable or enable Phishing Protection from the **Safe Web** window.

#### To disable or enable Norton Phishing Protection

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the **Norton Security** main window, click **Advanced**.
- 3 On the left pane, click **Safe Web**.
- 4 In the **Safe Web** row, click the settings icon.
- 5 In the **Safe Web** window, do one of the following:
  - To disable Norton Phishing Protection, deselect the **Enable Norton Phishing Protection** check box.
  - To enable Norton Phishing Protection, select the **Enable Norton Phishing Protection** check box.

## About Norton toolbar

When you install Norton Security, it adds the Norton toolbar to the supported web browsers.

The Norton toolbar is supported on Firefox and Safari web browsers.

Norton toolbar has the following features:

**Norton menu**

Lets you do the following:

- **Open Norton Security**
- **Hide Norton Toolbar**
- **Disable Safe Search**
- **Norton Community Buzz**
- **Norton Safe Web Site**
- **My Norton account**

⏻ The **Disable Safe Search** option appears only if you added the **Norton Safe Search** box to your Norton toolbar when you first launched your browser after you installed Norton Security.

**Norton Site Safety indicator**

Lets you know if the website that you visit is safe.

Norton Safe Web analyzes the websites that you visit and provides a safety rating for each website.

The Norton toolbar gives you the following visual indicators of the potential fraud that exists on a website that you visit:

- The toolbar displays a security status of the website.
- The toolbar changes color to indicate the safety of the website.

The following table describes the different security statuses of the Norton toolbar:

**Monitoring**

Indicates that Norton Security is analyzing the website.

**Norton Secured**

Indicates that the website is verified by Symantec.

Symantec analyzed this website and found that the website is VeriSign trusted. The website has a Secure Socket Layer (SSL) certificate provided by VeriSign. VeriSign trusted websites are virus free and are safe. Symantec categorizes the shopping websites that are VeriSign trusted as Norton Secured websites. You can enter your personal information and perform online transactions on this website.

**Site is Safe**

Indicates that Symantec has analyzed this website and determined that there is no indication of threat. Norton Safe Web has also determined that this webpage offers a safe shopping experience.





**Site is Unsafe**

Indicates Symantec has analyzed this website and determined that the website is unsafe to visit. This website may attempt to install malicious software on your computer. The website that you visit may have **Computer Threats, Identity Threats, and Annoyance Factors.**

Symantec recommends that you do not visit this website.

**Use Caution**

Indicates the Symantec has analyzed this page and determined that this page provides annoying results. The site can spam your email address or change your browser settings without any confirmation. The website that you visit may have **Computer Threats, Identity Threats, and Annoyance Factors.**

Symantec recommends that you do not visit this website.



This chapter includes the following topics:

- [About File Guard](#)
- [Disabling or enabling File Guard](#)
- [Adding files to File Guard](#)
- [Removing files from File Guard](#)
- [Granting access to guarded files for Mac OS X applications](#)
- [Turn on or turn off guarded file access notification](#)

## About File Guard

You can use the **File Guard** feature of Norton Security to safeguard the files that have your sensitive data. File Guard prevents the files on your Mac from the malicious programs that access your sensitive data without your permission. When a malicious program tries to open, copy, rename, move, or delete the file in the **Guarded File** list, Norton Security notifies you.

The following are limitations for using the File Guard feature:

- You cannot add an entire folder to File Guard at once. You can add multiple files at once by using **Command-click** or **Shift-click**.

- A guarded file must be located on a local disk. It cannot be in the root folder of the local disk or in the System folder.
- The maximum number of files you can protect is 250.

## Disabling or enabling File Guard

When you disable the File Guard feature, it stops protecting your files that you have added to the **Guarded Files** list. The files that you have added in the **Guarded Files** list are not deleted. If you enable the File Guard feature again, the files that you have added to the **Guarded Files** list are protected.

You can disable or enable the **File Guard** feature from the **Advanced** window.

The **File Guard** feature is turned off by default after you install your Norton product. However, Symantec recommends that you keep the **File Guard** feature enabled to prevent your sensitive data from identity theft.

### To disable or enable File Guard

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the **Norton Security** main window, click **Advanced**.
- 3 On the left pane, click **File Guard**, and then do one of the following:
  - To disable File Guard, move the **File Guard** switch to the **Off** position.
  - To enable File Guard, move the **File Guard** switch to the **On** position.

## Adding files to File Guard

File Guard helps you protect your files in which you store your sensitive data including your credit card information and social security number. File Guard protects the sensitive information from unauthorized access. You

must enable the File Guard feature to add files to the **Guarded Files** list.

You can use the **File Guard** window to do the following:

- Add the files that you want to protect against unauthorized access.
- Remove the files that are already protected.
- Enable or disable access to your guarded files by Mac OS X programs such as **Finder** and **Spotlight**.
- Disable or enable the notifications when an access to a guarded file is blocked.

#### To add files to File Guard

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the **Norton Security** main window, click **Advanced**.
- 3 On the left pane, click **File Guard**.
- 4 In the **File Guard** row, click the settings icon.
- 5 In the **File Guard** window, do one of the following:
  - Drag and drop individual files to the **Guarded Files** list.
  - Click **Add File(s)**, and then select individual files or folders.
- 6 Click **Done**.

## Removing files from File Guard

You can remove the files that you added to the **Guarded Files** list at any time. If you remove the guarded files, File Guard stops protecting the files that have your sensitive information from unauthorized access. You can then add the files to the **Guarded Files** list to protect them again.

#### To remove files from File Guard

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the **Norton Security** main window, click **Advanced**.

## Granting access to guarded files for Mac OS X applications

- 3 On the left pane, click **File Guard**.
- 4 In the File Guard row, click the settings icon.
- 5 In the **Guarded Files** list, select the files that you want to remove.  
To select multiple items, use **Shift-click** or **Command-click**.
- 6 Click **Remove File(s)**.
- 7 Click **Done**.

## Granting access to guarded files for Mac OS X applications

You can enable the **Allow Mac OS X to access my guarded files** option to enable the Mac OS X applications such as **Finder** and **Spotlight** to gain access to your guarded files without notification. This option enables you to copy, move, rename, or delete the guarded files using applications such as **Finder** and **Spotlight**.

When you enable the **Allow Mac OS X to access my guarded files** option, the Mac operating system processes that run in the background can also access your guarded files without notification.

### To grant access to guarded files for Mac OS X applications

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **File Guard**.
- 3 In the **File Guard** row, click the settings icon.
- 4 In the **File Guard** window, check **Allow Mac OS X to access my guarded files**.
- 5 Click **Done**.

## Turn on or turn off guarded file access notification

When there is an unauthorized access to the guarded files, the File Guard feature notifies you. You must enable the **Notify me when access to a guarded file is automatically blocked** option to get a notification.

### To turn on or turn off guarded file access notification

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **File Guard**.
- 3 In the File Guard row, click the settings icon.
- 4 In the **File Guard** window, do one of the following:
  - To turn on notification, check **Notify me when access to a guarded file is automatically blocked**.
  - To turn off notification, uncheck **Notify me when access to a guarded file is automatically blocked**.
- 5 Click **Done**.

# Scanning your Mac manually

# 6

This chapter includes the following topics:

- [About Norton Security scans](#)
- [Running a Quick Scan](#)
- [Running a full system scan](#)
- [Scanning a specific file or folder](#)
- [About Scan Facebook Wall](#)
- [Scanning your Facebook wall](#)
- [Running scans from the command line](#)

## About Norton Security scans

Norton Security lets you perform manual virus scans.

The Automatic Scans feature monitors your Mac for viruses in the following ways:

- Scans all the files when they are created, copied, or modified.
- Scans the disks and removable media.

However, Automatic Scans might not detect the following viruses:

- Viruses that were on your Mac before you installed Norton Security.

- Viruses in the files that are excluded from the Automatic Scans.

In this case, you can use Norton Security to scan a particular file, folder, or drive on your Mac.

You can perform the following types of manual virus scans:

<b>Quick Scan</b>	Scans the important locations of your Mac that the viruses and other security threats often target. Quick Scan takes less time because this scan does not scan your entire Mac.
<b>Full Scan</b>	Scans your entire Mac for all types of viruses and security threats.
<b>File Scan</b>	Scans the selected files or folders for all types of viruses and security threats.

## Running a Quick Scan

Quick Scan helps you to scan the areas of your computer that the viruses and other security risks often target. Quick Scan does not scan your entire computer.

### To run a Quick Scan

- 1 In the Norton Security main window, click **Scans**.



- 2 On the left pane, click **Quick Scan**, and then click **Start a Quick Scan**.  
You can use the following options when the scan is in process:

<b>Pause</b>	Suspends the scan temporarily.  You must click the <b>Resume</b> option to continue the scan.
<b>Cancel</b>	Terminates the scan.

## Running a full system scan

You can run a full system scan on your Mac. A full system scan thoroughly examines your entire computer for viruses, spyware, and different security vulnerabilities.

### To run a full system scan

- 1 In the Norton Security main window, click **Scans**.
- 2 On the left pane, click **Full Scan**, and then click **Start a Full Scan**.  
You can use the following options when the scan is in process:

<b>Pause</b>	Suspends the scan temporarily.  You must click the <b>Resume</b> option to continue the scan.
<b>Cancel</b>	Terminates the scan.

## Scanning a specific file or folder

By using Norton Security, you can scan a specific file or a folder. For example, if you have received a compressed file in an email message and if you suspect a virus, you can use the File Scan option to scan that file.

### To scan a specific file or folder

- 1 In the Norton Security main window, click **Scans**.
- 2 On the left pane, click **File Scan**.
- 3 Click **Select a file** and navigate to the file or folder location.
- 4 Select the folder or file that you want to scan and then click **Scan**.

You can also drag and drop the folder or file.

## About Scan Facebook Wall

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 check if a URL is safe or unsafe and then share the URL with your friends on Facebook. Norton Safe Web scans the URL that you post on Facebook wall and gives you the safety status for the URL. This way, you are not only protected from unsafe websites but you also let other Facebook users know the security status of any website.

You can also use the **Scan Facebook Wall** option in the Norton Security to scan your Facebook wall. Norton Security takes you to the Facebook login webpage. After you log in to your Facebook profile, Norton Safe Web asks for your permission to access your Facebook wall. You can use the **Allow** option to view the **Additional Permissions Required** page. The **Please grant us permission to access your News Feed and Wall**

option on this page lets you give permission to Norton Safe Web to access your Facebook wall.

The auto-scan feature in the Norton Safe Web application page helps you protect your Facebook wall. Norton Safe Web scans the News Feed on your Facebook wall periodically and protects you from malicious links. When Norton Safe Web detects a malicious link, it notifies you. To activate Norton Auto-Scan, go to your **Norton Safe Web** webpage on Facebook, and then click **Auto-Scan On**.

To remove the malicious link from your Facebook wall, go to your profile and remove the malicious link. If your friend has posted the malicious link, you can use the **Warn Your Friends** option to alert your Facebook friend. 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 every week notifying that your Facebook wall is safe.

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

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

**Safe**

Indicates that the website is safe to visit and Norton Trusted.

The websites with this rating do not harm your computer and so you can visit this site.

<b>Warning</b>	Indicates that the website has security risks.  The websites with this rating may install malicious software on your computer. Symantec recommends that you do not visit this site.
<b>Untested</b>	Indicates that Norton Safe Web has not yet tested this site and it does not have sufficient information about this website.
<b>Caution</b>	Indicates that the site may have security threats. Symantec recommends you to be cautious while you visit such websites.

## Scanning your Facebook wall

The Norton Safe Web feature scans your Facebook wall and analyzes the security levels of all the available links on your Facebook wall. It then displays the security status of the scanned URLs. However, Norton Safe Web requires your permission to scan your Facebook wall.

### To scan your Facebook wall

- 1 In the Norton Security main window, click **Scans**.
- 2 On the left pane, click **Scan Facebook Wall**, and then click **Scan my Facebook wall**.
- 3 In the Facebook login webpage, log in to your Facebook profile.
- 4 Follow the on-screen instructions.

## Running scans from the command line

Norton Security lets you perform multiple scans from the command line interface. The Norton Scanner feature in Norton Security provides this power user feature. Symantec recommends that you use this feature only if you are an advanced user.

You can launch the command line interface by navigating to **Finder > Applications > Utilities > Terminal**.

### To run a Quick Scan

- ❖ In the command line, type

```
/usr/bin/nortonscanner quickscan.
```

### To run a full system scan

- ❖ In the command line, type

```
/usr/bin/nortonscanner systemscan.
```

### To scan a specific file

- ❖ In the command line, type

```
/usr/bin/nortonscanner -a <file path>.
```

### To scan a compressed file

- ❖ In the command line, type

```
/usr/bin/nortonscanner -c <file path>.
```

### To scan the Quarantine

- ❖ In the command line, type

```
/usr/bin/nortonscanner quarantine.
```

# Keeping secure on the Internet

# 7

This chapter includes the following topics:

- [About Vulnerability Protection](#)
- [Turning off or turning on Vulnerability Protection](#)
- [Excluding or including attack signatures](#)
- [Getting information about attack signatures](#)
- [Enabling or disabling notifications for blocked attack signatures](#)
- [Configuring the port scan sensitivity](#)

## About Vulnerability Protection

Vulnerability Protection feature helps you in detecting and preventing intrusions through the Internet. Vulnerability Protection provides information about the susceptibility of the programs that may be on your Mac against malicious attacks. It also provides information about the known attacks.

Vulnerabilities are flaws in your programs or your operating system that can create weaknesses in the overall security of your Mac. Improper Mac configurations or security configurations also create vulnerabilities. External attackers exploit these vulnerabilities and perform malicious actions on your Mac. Examples of such malicious attacks are active desktop monitoring, keylogging, and hacking. Such

attacks can slow down the performance of your Mac, cause program failure, or expose your personal data and confidential information to the hackers.

Norton Security provides the signature-based solutions to protect your Mac from the most common Internet attacks. Attack signatures contain the information that identifies an attacker's attempt to exploit a known vulnerability in your operating system or your Mac programs. The Intrusion Prevention feature of Norton Security uses an extensive list of attack signatures to detect and block suspicious network activity.

## Turning off or turning on Vulnerability Protection

You can choose whether you want to protect your Mac from the threats that can affect your Mac vulnerabilities.

By default, the Vulnerability Protection option is turned on. Symantec recommends that you keep the Vulnerability Protection option turned on to protect your Mac from any malicious attacks.

### To turn off or turn on Vulnerability Protection

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, do one of the following:
  - To turn off the Vulnerability Protection feature, move the switch to the **Off** position.
  - To turn on the Vulnerability Protection feature, move the switch to the **On** position.

## Excluding or including attack signatures

Norton Security performs scans by comparing the signature of the files against the known attack signatures to identify threats on your Mac. An attack signature is

used to identify an attacker's attempt to exploit a known operating system or application vulnerability.

You can choose whether you want to protect your Mac from all the attack signatures or only from the selected signatures. In some cases, benign network activity can appear to be similar to an attack signature. You might receive repeated notifications about possible attacks. If you know that the attacks that trigger these notifications are safe, you can create an exclusion list for the signature that matches the benign activity.

If you want protection against vulnerabilities, but you do not want to receive notifications about blocked attacks, you can stop Vulnerability Protection from displaying notifications. Unless you have a good reason to disable a signature, you should leave the signatures turned on. If you disable a signature, your computer may be vulnerable to attack.

#### To enable or disable attack signatures

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, click the **Signatures** tab.
- 5 In the **Signatures** list, select a signature, and do one of the following:
  - To disable the detection of the attack signature, uncheck **Enable this signature**
  - To enable the detection of the attack signature, check **Enable this signature**
- 6 Click **Done**.



## Getting information about attack signatures

Vulnerability Protection uses a frequently updated list of signatures to detect known attacks. You can view the list of signatures or get information on a specific signature from the Symantec Security Response website.

A web browser opens to display information about the signature from the Symantec website.

### To get information about a signature

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the setting icon.
- 4 In the **Vulnerability Protection** window, click the **Signatures** tab.
- 5 In the **Signatures** list, select the signature for which you want to get more information.
- 6 Click **Learn More**.  
The information about the selected signature appears in a separate webpage.

## Enabling or disabling notifications for blocked attack signatures

You can choose whether you want to receive notifications when Vulnerability Protection blocks suspected attacks.

The notification message lets you do the following:

- To view the details of the blocked attack.
- To report a wrongly detected attack.

All of the Vulnerability Protection activities are recorded in the **Security History** window. The entries include

## Enabling or disabling notifications for blocked attack signatures

information about the unauthorized accesses attempts and other details.

You can enable or disable notification for all blocked attacks or for individual attack signatures.

### To enable or disable notifications for all blocked attacks

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, click the **Advanced** tab.
- 5 In the **Advanced** tab, do one of the following:
  - To disable the notifications for all blocked attacks, deselect **Notify me when Vulnerability Protection automatically blocks an attack**.
  - To enable the notifications for all blocked attacks, select **Notify me when Vulnerability Protection automatically blocks an attack**.
- 6 Click **Done**.

### To enable or disable notifications for individual attack signatures

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, click the **Signatures** tab.
- 5 In the **Signature** list, do one of the following:
  - To disable the notifications, deselect **Show notifications for this signature**.
  - To enable the notifications, select **Show notifications for this signature**.
- 6 Click **Done**.

## Configuring the port scan sensitivity

Port scanner is an application that randomly searches for vulnerable areas of the computers that are connected on a network. When you use the Internet, port scanners might try to infect through the vulnerabilities of your Mac. The Vulnerability Protection feature monitors your Mac for port scans and blocks the connection from unauthorized or unknown computers.

Port scans are also used for legitimate purposes. For example, network administrators perform port scans to find and solve any potential problem in your Mac. You can adjust the sensitivity of Vulnerability Protection against the port scan.

Norton Security notifies you each time it blocks a port scan. The number of notifications varies based on the sensitivity level that you configure for port scans. For example, if you configure the **Most secure** option, Norton Security displays more notifications. Norton Security port scan detection does not work when the built-in Mac OS X firewall is turned on.

### To configure the port scan sensitivity

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, click the **Advanced** tab.

5 Under **Sensitivity**, select any one of the following sensitivity level:

**Most secure**

When you set this level, Norton Security is more sensitive to port scan. It blocks any application from accessing your Mac and notifies you with alerts. You can set this option when you use a public wireless network to provide the maximum protection for your Mac.

**Moderate secure**

When you set this level, Norton Security is moderately sensitive to port scans and blocks any unknown or any unwanted application from accessing your Mac.

By default, this option is selected.

**Less secure**

When you set this level, Norton Security is less sensitive to port scans and allows applications to access your Mac. However, Norton Security scans all the application that attempts to access your Mac and notifies you about the details of the applications.

6 Click **Done**.

# Customizing settings

# 8

This chapter includes the following topics:

- [About Automatic Scans settings](#)
- [Turning off or turning on Automatic Scans](#)
- [Including files for Automatic Scans](#)
- [Excluding files from Automatic Scans](#)
- [Removing files from the Automatic Scans exclusion list](#)
- [Removing files from Automatic Scans list](#)
- [About Scheduled Scans](#)
- [Turning on or turning off Scheduled Scans](#)
- [Customizing Scheduled Scans settings](#)
- [About Idle Scans](#)
- [Turning off or turning on Idle Scans](#)
- [Customizing Idle Scans settings](#)
- [About Firewall settings](#)
- [About Connection Blocking settings](#)
- [Configuring Connection Blocking settings](#)
- [About access settings for an application](#)

- [Configuring the access settings for an application](#)
- [Customizing the specific access settings for an application](#)
- [Editing the access settings of an application](#)
- [Removing access settings for an application](#)
- [About access settings for a service](#)
- [Configuring the access settings for services](#)
- [Customizing the specific access settings for a service](#)
- [Editing the access settings for a service](#)
- [Removing the access settings for a service](#)
- [About firewall rule for IP addresses](#)
- [Configuring firewall rules for an IP address](#)
- [Modifying firewall rules for an IP address](#)
- [Removing firewall rule for an IP address](#)
- [About configuring firewall for an application](#)
- [Setting up firewall rules for an application](#)
- [Customizing the firewall rule for an application](#)
- [Removing the firewall rule for an application](#)
- [About Location Awareness settings](#)
- [Disabling or enabling Location Awareness](#)
- [Viewing Location Awareness settings](#)
- [Exporting the connection blocking settings for a network location](#)
- [About advanced protection](#)

- [Disabling or enabling advanced protection features](#)
- [Configuring Norton DeepSight Community Download](#)
- [Configuring Norton DeepSight Community Submission](#)
- [Configuring AutoBlock settings](#)
- [Managing Excluded IP addresses](#)
- [Configuring Signatures settings](#)

## About Automatic Scans settings

Automatic Scans provide enhanced security from the time you start your Mac. This feature ensures better protection by running all the necessary components that are required.

Automatic Scans protect your Mac in the following ways:

- Scans the files when they are created, copied, or modified.
- Scans the disks and removable media when they are first accessed by your Mac.
- Scans all the traffic through Internet to your Mac.



If your Mac is configured with more than one user account, these settings apply to all the user accounts.

You can configure Automatic Scans settings in the **Protect My Mac** section of the **Advanced** window. The Automatic Scans settings are:

- **Scan everything**

Scans all the files on your Mac during Automatic Scans.

**Scan everything** provides better protection when compared to other type of scans. By default, **Scan everything** is selected.

- **Scan only these folders**

Lets you specify the folders that you want to be scanned automatically.

■ **Don't scan these folders**

Lets you exclude specific folders from Automatic Scans.

■ **Scan files in compressed archives (Recommended)**

Lets you enable or disable Norton Security to scan the files within the compressed files available on your Mac. For example, files with .zip or .rar file extension with the maximum size limit of 1 MB.

■ **Scan files on external drives on access**

Lets you enable or disable Norton Security to scan the files available on an external drive that is connected to your Mac.

■ **Reset to Defaults**

Lets you reset configuration to default level.

## Turning off or turning on Automatic Scans

If you turn on the Automatic Scans, Norton Security automatically performs the following activities each time you turn on your Mac:

- Downloads the most up-to-date virus definitions.
- Scans entire Mac and removes viruses from infected files.
- Monitors all the incoming and outgoing traffic on your Mac.

Norton Security displays a message if there is an issue that requires your attention. For example, if there is a security risk, Norton Security pop-ups a warning message with a list of options. You can choose an option and take appropriate action on the unresolved risk. You can open Norton Security at any time to see the status of your Mac or to view the protection details.



### To turn off or turn on Automatic Scans

- 1 In the Norton Security main window, in the left pane, click **Advanced**.
- 2 On the left pane, click **Protect My Mac**.
- 3 In the **Automatic Scans** row, do one of the following:
  - Turn off Automatic Scans, move the switch to the **Off** position.
  - Turn on Automatic Scans, move the switch to the **On** position.

## Including files for Automatic Scans

If you think that any file or application on your Mac is vulnerable, you can add it for Automatic Scans.

For example, if you think the Downloads folder in your Mac that you use frequently to download files from the Internet is vulnerable, you can add the Downloads folder to Automatic Scans. Norton Security scans this folder when it is modified and ensures that your Mac is not infected.

You can use the **Scan only these folders** option and customize Automatic Scans to scan only the selected files.

### To include a file for Automatic Scans

- 1 In the **Norton Security** main window, click **Advanced**.
- 2 On the left pane, click **Protect My Mac**
- 3 In the **Automatic Scans** row, click the settings icon.
- 4 In the **Automatic Scans** window, click **Scan only these folders**.
- 5 Click **+**.
- 6 Browse for the folder that you want to scan automatically.
- 7 Click **Add**.
- 8 Click **Save**.

## Excluding files from Automatic Scans

By default, Norton Security scans all the files and folders on your Mac. However, you can configure it not to scan certain files or directories. You can exclude some frequently used applications from Automatic Scans to reduce the scanning time.

### To exclude a file from Automatic Scans

- 1 In the **Norton Security** main window, click **Advanced**.
- 2 On the left pane, click **Protect My Mac**
- 3 In the **Automatic Scans** row, click the settings icon.
- 4 In the **Automatic Scans** window, click **Don't scan these folders**.
- 5 Click **+**.
- 6 Browse for the folder that you do not want Norton Security to scan automatically.
- 7 Click **Exclude**.
- 8 Click **Save**.

## Removing files from the Automatic Scans exclusion list

If you think any of the files that are excluded from Automatic Scans are vulnerable, you can remove the file from the list. The removed files are automatically added for Automatic Scans.

### To remove a file from the Automatic Scans exclusion list

- 1 In the **Norton Security** main window, click **Advanced**.
- 2 On the left pane, click **Protect My Mac**
- 3 In the **Automatic Scans** row, click the settings icon.
- 4 In the **Automatic Scans** window, click **Don't scan these folders**.

- 5 Select the folder that you want to remove from the exclusion list and click -.
- 6 Click **Save**.

## Removing files from Automatic Scans list

The files that are included for Automatic Scans are listed in the **Scan only these folders** list. If you think that scanning a file that you included previously is not necessary, you can remove it from the Automatic Scans list.

### To remove a file from the Automatic Scans list

- 1 In the **Norton Security** main window, click **Advanced**.
- 2 On the left pane, click **Protect My Mac**
- 3 In the **Automatic Scans** row, click the settings icon.
- 4 In the **Automatic Scans** window, click **Scan only these folders**.
- 5 Select the folder that you want to remove from the list and click -.
- 6 Click **Save**.

## About Scheduled Scans

Norton Security automatically detects the idle state of your Mac and runs an idle scan.

However, you can schedule a scan according to your preferences. You can schedule a scan to run automatically on a specific day and time. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work.



The scheduled scan settings do not change when a different user uses the Mac. Norton Security runs the scheduled scan at the scheduled time with the settings already configured.

Norton Security displays the scan results on your computer when the scheduled scan is complete.

You can use the **Reset to Defaults** option to reset the **Scheduled Scans** settings to default.

## Turning on or turning off Scheduled Scans

You can configure Norton Security to run a scheduled scan. Norton Security runs the scan on a specific day and time.

If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work. You need to turn on the Scheduled Scans feature to let Norton Security scan your computer. By default, the Scheduled Scans feature is turned off.

### To turn on or turn off Scheduled Scans

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Protect my Mac**.
- 3 In the **Scheduled Scans** row, do one of the following:
  - To turn on Scheduled Scans, move the switch to the **On** position.
  - To turn off Scheduled Scans, move the switch to the **Off** position.

## Customizing Scheduled Scans settings

You can configure Norton Security to run a scheduled scan. Norton Security runs the scan on a specific day and time. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work. Norton Security lets you customize the settings for the scheduled scan.

Norton Security displays the scan results on your computer when the scheduled scan is complete.



The scheduled scan settings do not change when a different user uses the Mac. Norton Security runs the scheduled scan at the scheduled time with the settings already configured.

**To customize Scheduled Scans settings**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Protect my Mac**.
- 3 In the **Scheduled Scans** row, click the settings icon.

4 In the **Scheduled Scans** window, configure your scan settings.

Your options are:

**When to Scan**

Lets you specify the day and time at which you want Norton Security to run the scan.

**What to Scan**

Lets you specify the area that you want Norton Security to scan.

Your options are:

■ **Startup Disk**

Performs a scan on the startup (boot) disk of your Mac.

■ **All User Folders**

Performs a scan on all of the home folders on your Mac.

■ **Entire System**

Performs a scan on all the available disks of your Mac.

**Scan files in compressed archives (Recommended)**

Lets you enable or disable Norton Security to scan the files within the compressed files.

**Show Scheduled Scan Results**

Lets you specify when you want Norton Security to notify you about the Scheduled Scan results.

Your options are:

■ **Only when infections are found**

Select this option if you want to be notified when a security threat is detected.

■ **Always**

Select this option if you want to receive notification for activities of Norton Security during the scheduled scan. You can receive notifications for activities such as completed scans or scans that are canceled because of system activity.

**Reset to Defaults**

Lets you set the **Scheduled Scans** settings to the recommended settings.

5 Click **Save**.

## About Idle Scans

Norton Security keeps your Mac secure from latest security threats by automatically running scans on your computer using the **Idle Scans** feature. Idle scan detects the time when you do not use your Mac and intelligently runs the scan.

The **Idle Scans** option is automatically turned on when you install Norton Security. Even though idle scan automatically runs the scan, you can still customize the settings of idle scan. Norton Security decides when to run idle scan depending on your settings and a few other predefined parameters.



The idle scan settings do not change when a different user uses the Mac. Norton Security detects the idle time of the Mac and runs the idle scan with the settings already configured.

Norton Security discontinues any idle scan that it started during idle time if you begin to use your Mac again. However, it resumes the scan when your Mac is idle again. You should always keep the **Idle Scans** option turned on to let Norton Security scan your Mac when it becomes idle.

You can use the **Reset to Defaults** option to reset the **Idle Scans** settings to default.

## Turning off or turning on Idle Scans

Your Norton product keeps your Mac secure from latest security threats by automatically running scans on your computer using the **Idle Scans** feature. Your Norton product detect the time when you do not use your Mac and intelligently runs the scan.

You should always keep the **Idle Scans** option turned on to let your Norton product scan your computer when it becomes idle.

### To turn off or turn on Idle Scans

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Protect my Mac**.
- 3 In the **Idle Scans** row, do one of the following:
  - To turn off idle scans, move the switch to the **Off** position.
  - To turn on idle scans, move the switch to the **On** position.



## Customizing Idle Scans settings

Norton Security keeps your Mac secure from latest security threats by automatically running scans on your computer using the **Idle Scans** feature. **Idle Scans** detect the time when you do not use your Mac and intelligently run the scan.



The idle scan settings do not change when a different user uses the Mac. Norton Security detects the idle time of the Mac and runs the idle scan with the settings already configured.

### To customize Idle Scans settings

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Protect my Mac**.
- 3 In the **Idle Scans** row, click the settings icon.

**4** In the **Idle Scans** window, customize your scan settings.

You can customize the scan in the following ways:

**What to Scan**

Lets you specify the area that you want Norton Security to scan. Your options are:

■ **Startup Disk**

Performs an idle scan on the startup (boot) disk of your Mac.

■ **All User Folders**

Performs an idle scan on all of the home folders on your Mac.

■ **Entire System**

Performs an idle scan on all the available disks of your Mac.

**Scan files in compressed archives (Recommended)**

Lets you enable or disable Norton Security to scan the files within the compressed files.

**Show Idle Scan Results**

Lets you view the idle scan results in the **Security History** window. Your options are:

■ **Only when infections are found**

Select this option if you want to view the scan results when a security threat is detected.

■ **Always**

Select this option if you want to view the activities of Norton Security during the idle scan. You can view activities such as completed scans or scans that are canceled because of system activity.

**Reset to Defaults**

Lets you set the **Scheduled Scans** settings to the recommended settings.

## About Firewall settings

Firewall settings let you customize how firewall should monitor and respond to the inbound and the outbound network communications. Firewall settings contain the access settings for the applications, services, and ports on your Mac. They also contain access settings for connections to or from the other computers in the network to which your Mac is connected.

You can use the **Firewall** window to customize the following firewall settings:

<b>Application Blocking</b>	<p>Lets you configure firewall rules for the applications that run on your Mac to connect to the Internet.</p> <p>The Application Blocking settings determine whether to allow or deny an application, such as a Web browser or iTunes, from connecting to the Internet.</p> <p>Application Blocking settings are not specific to a particular network location. The Application Blocking settings do not change when you change to a different network location.</p> <p>You can use the <b>Configure</b> option under <b>Application Blocking</b> to set Internet access for applications on your Mac.</p> <p>⚙ Whenever an overlap exists in the settings between Connection Blocking and Application Blocking, the Connection Blocking settings take precedence over the Application Blocking settings.</p>
-----------------------------	--

### Connection Blocking

Lets you allow or block the applications, ports, services, and IP addresses that:

- Connect to your Mac.
- Connect to a network.

The Connection Blocking settings determine whether to allow or deny the incoming or the outgoing connections that use a specific service, application, or a port. You can also configure firewall to allow or block a specific IP address on the network.

Connection blocking settings apply only to a particular location.

You can use the settings icon in the **Connection Blocking** row to set connections for applications and services on your Mac.

### Vulnerability Protection

Helps you in detecting and preventing Intrusions through the Internet. Vulnerability Protection monitors all the incoming and the outgoing traffic on your Mac and blocks any unauthorized access.

It provides information about the susceptibility of the programs that may be on your Mac against malicious attacks. It also provides information about the known attacks. You can manage the list of signatures for Vulnerability Protection.

<b>Location Awareness</b>	<p>Lets you configure the firewall settings based on the network location to which your Mac is connected.</p> <p>The firewall settings that you configure contains the connection blocking settings for the application and services that run on your Mac. When you connect your portable Mac to a new network location, Norton Security prompts you to select a new firewall setting for the network location.</p>
---------------------------	---



<p><b>DeepSight</b></p>	<p>Lets you access and configure the Norton DeepSight Community Download and Norton DeepSight Community Submission features.</p> <p>Your options are:</p> <ul style="list-style-type: none"> <li> <p>■ <b>Norton DeepSight Community Download</b></p> <p>This feature lets you obtain the updated list of IP addresses that Symantec identifies as attackers. You can enable the Norton DeepSight Community Download feature to obtain the updated list of IP addresses from Symantec servers.</p> </li> <li> <p>■ <b>Norton DeepSight Community Submission</b></p> <p>This feature helps you identify new security risks by submitting selected security and application data to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. You can enable or disable the Norton DeepSight Community Submission feature in the Advanced Protection window to allow or block the security risks information submission.</p> </li> </ul>
-------------------------	--

## About Connection Blocking settings

You can configure the Connection Blocking settings for an application, a service, or an IP address. Based on the Connection Blocking settings, the firewall allows, or blocks the incoming and the outgoing network connections.

The Connection Blocking settings that you configure are specific to the selected network location. The settings apply only when your Mac connects to the specified network location.

You can configure the Connection Blocking settings for the following:

<b>Applications</b>	Lets you specify access settings for the applications that run on your Mac.
<b>Services/Ports</b>	Lets you specify access settings for the services and ports that run on your Mac.
<b>Zones</b>	Lets you specify the IP address to or from which you want to allow or block connections.
<b>All, in order of precedence</b>	Lets you view the entire access settings for a firewall setting that you select.  Whenever the settings overlap, settings at the top of the list take precedence over the settings in the bottom of the list.



# Configuring Connection Blocking settings

Connection Blocking settings apply to the incoming and the outgoing connections that use a specific application, service, port, or IP address.

You can use the **Connection Blocking** window to configure whether an application or a service that is allowed to connect to the Internet or to the local network. You can select the required network location from the **Editing settings** menu and configure the Connection Blocking settings.



You can configure the Connection Blocking settings only if the **Connection Blocking** option is turned on in the **Advanced** window.




You must have a user account that has administrator privileges to perform this task.

## To configure Connection Blocking settings

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to configure the connection blocking settings.

- 5 Select an option in the **View** menu.  
The options that appear in the **View** menu vary depending on the network location that you select in the **Editing settings** menu.  
Your options are:

<b>Applications</b>	Lets you specify the Connection Blocking settings for the applications that run on your Mac.
<b>Services/Ports</b>	Lets you specify the Connection Blocking settings for the services and ports that run on your Mac.
<b>Zones</b>	Lets you specify the IP address to or from which firewall allows or blocks connections.
<b>All, in order of precedence</b>	Lets you specify the current Connection Blocking settings for the Applications, services, ports, and zones in the order of precedence.



6 Select one of the following tabs:

**Incoming**

Lets you specify the access settings for the incoming connections that use an application or a service that runs on your Mac.


**Outgoing**

Lets you specify the access settings for the outgoing connections that use an application or a service that runs on your Mac.

**Incoming & Outgoing**

Lets you configure the access settings for connections to and from the IP addresses that you specify.

This tab appears only when you select **Zones** in the **View** menu.



- 7 Use the **Action pop-up** menu at the bottom of the **Connection Blocking** window to specify other connection blocking preferences. Your options are:

<b>Logging and notification settings</b>	Lets you specify the type of access attempts for which Norton Security must maintain records.  You can also specify the type of access attempts about which Norton Security must notify you.
<b>Advanced settings</b>	Lets you specify the advanced firewall options.
<b>Reset to defaults</b>	Lets you reset configuration to default level.

- 8 Click **Done**.

## About access settings for an application

You can use the **Connection Blocking** window to specify the access settings of applications to connect to a network. You can customize the firewall to allow or block network connections to or from applications like iTunes.

You can also configure the default and specific access settings for an application. The default access settings apply to all the incoming and the outgoing connections within your network. The specific access settings let you allow or block connections to specific computers.

You can perform the following activities for an application using the **Connection Blocking** window:

- Configure the access settings
- Customize the specific access settings

## Configuring the access settings for an application

- Edit the access settings
- Remove the access settings

# Configuring the access settings for an application

Norton Security lets you configure the access settings for the applications that run on your Mac. Based on the settings that you configure and the network location of your Mac, the firewall allows or blocks the incoming and the outgoing connections.

When you configure the access settings for an application, the name of the application appears in the **View** pane of the **Connection Blocking** window. You can also view the default access setting for the selected application under the application name.

Norton Security creates the **<All other applications>** access setting by default. This access setting includes all applications that run on your Mac.

### To configure the access settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to configure the access settings.
- 5 In the **View** menu, select **Applications**.

**Configuring the access settings for an application**

6 Select one of the following tabs:

**Incoming** Lets you specify the access settings for the incoming connections for the application.

**Outgoing** Lets you specify the access settings for the outgoing connections for the application.

7 Click **Add application**.

8 In the **Choose Application** dialog, select the required application.

If the application that you want does not appear in the list, click **Other** to search for the application.

9 In the menu at the top of the dialog, select one of the following default access setting:

**Allow** Allows the network connections for the application.

**Block** Blocks the network connections for the application.

**Ask** Set up the firewall notify you when a program attempts to access the Internet.

10 Click **Choose**.

The name of the application that you have added appears in the **View** pane in the **Connection Blocking** window.

**Customizing the specific access settings for an application**

11 Use the **Action** drop-down menu at the bottom of the **Connection Blocking** window to specify the advanced firewall preferences. Your options are:

<b>Logging and notification settings</b>	Lets you specify the type of access attempts for which Norton Security must maintain records.
<b>Advanced settings</b>	Lets you specify the advanced firewall options.
<b>Reset to defaults</b>	Lets you reset configuration to default level.

12 Click **Done**.

## Customizing the specific access settings for an application

Norton Security lets you customize the incoming and outgoing network connections settings for each application on your Mac. You can specify the IP addresses from which you want to allow or deny connection attempts. The specific access settings that you specify appear in the row under the application name with a minus (-) and plus (+) sign.



You can add any number of specific access settings for an application. For example, you can add a specific access setting for an application to allow connection from all the computers on your network. You can also add another specific access setting for the same application to block connection from a single computer.

### To customize the specific access settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.

## Customizing the specific access settings for an application

- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to configure the specific access settings for an application.
- 5 In the **View** menu, select **Applications**.
- 6 Select one of the following tabs:

**Incoming** Lets you specify the access settings for the incoming connections that use the application.

**Outgoing** Lets you specify the access settings for the outgoing connections that use the application.

- 7 In the **View** pane, click the **+** sign next to the application name.
- 8 In the **Edit address** window, use the following options to select the type of access for the connections:

<b>Allow</b>	Allows the connections to or from an IP address.
<b>Block</b>	Blocks the connections to or from an IP address.



9 Select the one of the following option to customize the specific access settings:

**All computers on my current network** Lets you allow or block connections to or from all computers on your network.

**A single computer** Allow or block connections to or from the computer with the IP address that you specify.

**All IP addresses beginning with** Allow or block connections to or from computers with the base address that you specify.

**All IP addresses on a network** Allow or block connections to or from computers on a local network that share the base address and the mask address that you specify.

10 Click **Save**.

11 Click **Done**.

## Editing the access settings of an application

You can edit the following access settings for an application:

- Logging and Notifications settings
- Specific access settings
- Default access settings that you configured for the application

### To edit the Logging and Notifications settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location that you want to edit.
- 5 In the **View** menu, select **Applications**.
- 6 Select an application that you want to edit.
- 7 In the **View** pane, select the row that contains the application name, and then click **Edit**.

8 In the **Edit application** window, edit the logging settings. Your options are:

**Override global logging settings**

Select the **Override global logging settings** check box to select the logging options

**Log allowed inbound connections**

Maintains a record of all the allowed incoming connections that use the application.

**Log allowed outbound connections**

Maintains a record of all the allowed outgoing connections that use the application.

**Log blocked inbound connections**

Maintains a record of all the blocked incoming connections that use the application.

**Log blocked outbound connections**

Maintains a record of all the blocked outgoing connections that use the application.

- 9 In the **Edit application** window, edit the notifications settings. Your options are:

**Override global notifications settings** Select the **Override global notifications settings** check box to select the notification options

**Notify me of allowed inbound connections** Displays an alert for all of the allowed incoming connections that use the application.

**Notify me of allowed outbound connections** Displays an alert for all of the allowed outgoing connections that use the application.

**Notify me of blocked inbound connections** Displays an alert for all of the blocked incoming connections that use the application.

**Notify me of blocked outbound connections** Displays an alert for all of the blocked outgoing connections that use the application.

- 10 Click **Save**.

#### To edit the specific access settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to edit the specific access settings.
- 5 In the **View** menu, select **Applications**.

- 6 Select an application for which you want to edit the specific access settings.
- 7 In the **View** pane, select the row that contains the specific access settings for the application, and then click **Edit**.
- 8 In the **Edit address** window, edit the required option.
- 9 Click **Save**.

**To edit the default access settings for an application**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to edit the default access settings.
- 5 In the **View** menu, select **Applications**.
- 6 Select the row that contains the default access settings for the application in the **View** pane.
- 7 Click **Edit**.
- 8 In the window that appears, select one of the following options:

<b>Allow</b>	Allows the network connections for the application.
<b>Block</b>	Blocks the network connections for the application.
<b>Ask</b>	Prompts you with a notification window.  You can select whether the firewall must allow or block the network connections using the application.

- 9 Click **Save**.

## Removing access settings for an application

You can use the **Connection Blocking** window to remove the following access settings that you have configured for an application:

- Access settings for an application
- Specific access setting for an application

However, you cannot remove the default Connection Blocking setting that appears in the list.

### To remove access settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to remove access settings.
- 5 In the **View** menu, click **Applications**.
- 6 In the **View** pane, select the application name, and do one of the following:
  - Click **Remove**.
  - Click the - sign next to the application name.
- 7 In the confirmation window, click **Remove**.

### To remove specific access settings for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to remove access settings.

5 In the **View** menu, click **Applications**.

6 Select one of the following tabs:

**Incoming** Lets you specify the access settings for the incoming connections that use the application.

**Outgoing** Lets you specify the access settings for the outgoing connections that use the application.

7 Select the row that contains the specific access settings and do one of the following:

- Click **Remove**.
- Click the - sign next to the specific access setting for the application.

8 In the confirmation window, click **Remove**.

## About access settings for a service

You can use the **Connection Blocking** window to specify access settings for the services that are running on your Mac. For example, you can customize the access settings for the file transfer protocol (FTP) service that allows access to the shared folders on your Mac using the port 21. You can customize the firewall for FTP to allow or block the incoming and the outgoing connections.

When you add an existing service, Norton Security displays the port through which the service communicates the incoming and the outgoing connections.

You also can specify default and specific access settings for a service. The default access setting applies to all connections to or from the computers that use the

## Configuring the access settings for services

service. The specific access settings let you allow or block connections to specific computers.

You can perform the following activities for a service using the **Connection Blocking** window:

- Configure the access settings
- Customize the specific access settings
- Edit the access settings
- Remove the access settings

## Configuring the access settings for services

Norton Security lets you specify the access settings for the services that run on your Mac. Based on the access settings that you specify and the current network location of your Mac, firewall allows or blocks the network connections that use the service.

The access settings that you configure are specific to the selected network location. It applies to your Mac only when it connects to the network location for which your Connection Blocking setting is configured.

When you add a service, the name of the service appears in the **View** pane of the **Connection Blocking** window. In addition, you can view the default access setting for the service under the service name.

By default, Norton Security creates the **<All other services>** access setting. This access setting includes all services that run on your Mac.

### To specify access settings for a service

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to configure the access settings.
- 5 In the **View** menu, select **Services/Ports**.



6 Select one of the following tabs:

**Incoming** Lets you specify the access settings for the incoming connections that use the service.

**Outgoing** Lets you specify the access settings for the outgoing connections that use the service.

7 Click **Add service**.

8 In the **New Service** dialog that appears, select the default access setting option that you want to apply for the service. Your options are:

**Allow** Allows the network connections for the service.

**Block** Blocks the network connections for the service.

9 Select the required service from the **Service name** menu.

If the service is not listed in the **Service name** menu, enter the name of the new service in the **Service name** menu. You can also enter a description for the service in the **Description** field.

10 Configure the following tabs as required:

<b>Ports</b>	<p>Lists the ports in the firewall that the service can open.</p> <p>You can use the <b>Add</b>, <b>Edit</b>, and <b>Remove</b> options only when you add a new service.</p> <p>You can use these options to add or modify the port numbers that you add.</p>
<b>Logging</b>	<p>Lists the types of connections that Norton Security must log.</p>
<b>Notifications</b>	<p>Lists the types of connections for which Norton Security should notify you when it makes a connection attempt.</p> <p>You can select whether the firewall must allow or block the connection attempts that use the service.</p>

11 Click **Save**.

## Customizing the specific access settings for a service

12 In the **Action** drop-down menu at the bottom of the **Connection Blocking** window, specify the advanced firewall preferences. Your options are:

<b>Logging and notification settings</b>	Lets you specify the type of access attempts for which you want Norton Security to maintain records.  You can also specify the type of access attempts about which you want Norton Security to notify you.
<b>Advanced settings</b>	Lets you specify the advanced firewall options.
<b>Reset to Defaults</b>	Lets you reset configuration to default level.

13 Click **Done**.

## Customizing the specific access settings for a service

Norton Security lets you customize the incoming and outgoing network connections settings for each service on your Mac. You can specify the IP addresses from which you want to allow or block connection attempts. The specific access settings that you specify appear in the row under the application name with a minus (-) and plus (+) sign.



You can add any number of specific access settings for a service. For example, you can add a specific access setting for a service to allow connection from all the computers on your network. You can also add another specific access setting for the same service to block connection from a single computer.

## Customizing the specific access settings for a service

**To customize the specific access settings for a service**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to specify the specific access settings.
- 5 In the **View** menu, click **Services/Ports**.
- 6 Select one of the following tabs:

**Incoming**

Lets you specify the access settings for the incoming connections that use the service.

**Outgoing**

Lets you specify the access settings for the outgoing connections that use the service.

- 7 In the **View** pane, click the **+** sign next to the service name.
- 8 In the **Edit address** dialog, select the type of access for the connections. Your options are:

**Allow**

Lets you allow the connections to or from an IP address.

**Block**

Lets you block the connections to or from an IP address.

9 Select the one of the following option to customize the specific access settings:

**All computers on my current network** Lets you allow or block connections to or from all computers on your network.

**A single computer** Lets you allow or block connections to or from the computer with the IP address that you specify.

**All IP addresses beginning with** Lets you allow or block connections to or from computers with the base address that you specify.

**All IP addresses on a network** Lets you allow or block connections to or from computers on a local network.

10 Click **Save**.

## Editing the access settings for a service

You can edit the following access settings for a service:

- Access settings
- Specific the access settings
- Default access setting

### To edit the access settings for a service

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.

- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to edit the Connection Blocking settings.
- 5 In the **View** menu, select **Services/Ports**.
- 6 Select one of the following tabs:

<b>Incoming</b>	Lets you specify the access settings for the incoming connections that use the service.
-----------------	---

<b>Outgoing</b>	Lets you specify the access settings for the outgoing connections that use the service.
-----------------	---

- 7 In the **View** pane, select the row that contains the service name, and then click **Edit**.
- 8 In the **Edit Service** dialog, make the changes as required.
- 9 Click **Save**.

#### To edit the specific access settings for a service

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to edit the Connection Blocking settings.
- 5 In the **View** menu, select **Services/Ports**.
- 6 On the **Incoming** or the **Outgoing** tab, select a service for which you want to edit the specific access settings.
- 7 In the **View** pane, select the row that contains the specific access settings for the application, and then click **Edit**.

- 8 In the **Edit Service** window, make the changes as required.
- 9 Click **Save**.

**To edit the default access settings for a service**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to edit the Connection Blocking settings.
- 5 In the **View** menu, select **Services/Ports**.
- 6 On the **Incoming** or the **Outgoing** tab, select the row that contains the default access settings for the service in the **View** pane, and then click **Edit**.
- 7 In the **Default action for <Service Name>** window, that appears select one of the following options:

<b>Allow</b>	Allows the network connections for the service.
<b>Block</b>	Blocks the network connections for the service.

- 8 Click **Save**.

## Removing the access settings for a service

You can use the **Connection Blocking** window to remove the access settings and the specific access settings that you have configured for a service.

However, you cannot remove the default Connection Blocking setting that appears in the list.

**To remove all access settings for a service**

- 1 In the Norton Security main window, click **Advanced**.

- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to remove the Connection Blocking settings.
- 5 In the **View** menu, select **Services/Ports**.
- 6 Select one of the following tabs:

<b>Incoming</b>	Lets you specify the access settings for the incoming connections that use the service.
-----------------	---

<b>Outgoing</b>	Lets you specify the access settings for the outgoing connections that use the service.
-----------------	---

- 7 Select the required service from the **View** pane and do one of the following:
  - Click **Remove**.
  - Click the - sign next to the service name.
- 8 In the confirmation window, click **Remove**.

**To remove an individual access setting for a service**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location for which you want to remove the Connection Blocking settings.
- 5 In the **View** menu, select **Services/Ports**.



6 Select one of the following tabs:

**Incoming**

Lets you specify the access settings for the incoming connections that use the service.

**Outgoing**

Lets you specify the access settings for the outgoing connections that use the service.

7 In the **View** pane, select the row that contains the specific access settings for a service and do one of the following:

- Click **Remove**.
- Click the - sign next to the service name.

8 In the confirmation window, click **Remove**.

## About firewall rule for IP addresses

You can use the **Connection Blocking** window to configure the firewall for zones in the network to which your Mac is connected. You can configure the zone access settings to specify IP addresses to which you want to allow or block connections.

The **Trust Zone** in the **View** pane shows the IP addresses to or from which you allowed access attempts for a network location. The **Block Zone** in the **View** pane shows the IP address to or from which you blocked access attempts of a network location.

You can perform the following activities for a zone from the **Connection Blocking** window:

- Configure the access settings for an IP address
- Edit the access settings for an IP address
- Remove the access settings for an IP address

## Configuring firewall rules for an IP address

You can specify the firewall rules of the IP address that is specific to a network location setting.

The **Trust Zone** in the **View** pane shows the IP addresses to or from which you allowed access attempts for a network location. The **Block Zone** in the **View** pane shows the IP addresses to or from which you blocked access attempts of a network location.

### To configure firewall rules for an IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing settings** menu, select the network location.
- 5 In the **View** menu, click **Zones**.
- 6 Click **Add IP address**.  
You can also use the **+** sign next to the **Block Zone** or **Trust Zone** row to specify access settings for the IP address.
- 7 In the **Edit address** window, select the default access setting option. Your options are:

<b>Allow</b>	Lets you allow the connections to or from all computers that exist on your network.
<b>Block</b>	Lets you block the connections to or from the computer with the IP address that you specify.

- 8 In the address menu, select an option to specify the IP addresses of computers to which you want to apply the access settings. Your options are:

**All computers on my current network** Lets you allow or block connections to or from all computers on your network.

**A single computer** Lets you allow or block connections to or from the computer with the IP address that you specify.

**All IP addresses beginning with** Lets you allow or block connections to or from computers with the base address that you specify.

**All IP addresses on a network** Lets you allow or block connections to or from computers on a local network.

- 9 Click **Logging and notification settings** to configure Norton Security to maintain records and notify you about access attempts.

- 10 Click **Save**.

## Modifying firewall rules for an IP address

You can edit the firewall rules of IP address, which is specific to a network location setting.

### To modify firewall rules for an IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.

- 4 In the **Connection Blocking** window, in the **Editing Settings** menu, select the Connection Blocking setting for which you want to change the settings of an IP address.
- 5 In the **View** menu, click **Zones** and select a row that contains the access settings for an IP address that you want to modify.
- 6 Click **Edit**.
- 7 In the **Edit address** window, make the necessary changes.
- 8 Click **Save**.

## Removing firewall rule for an IP address

You can remove the firewall rule for an IP address, which is specific to a network location.

### To remove firewall rule for an IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Connection Blocking** row, click the settings icon.
- 4 In the **Connection Blocking** window, in the **Editing Settings** menu, select a Connection Blocking setting.
- 5 In the **View** menu, click **Zones**.
- 6 In the **View** pane, select the row that contains the access settings of an IP address and do one of the following:
  - Click **Remove**, and in the confirmation window, click **Remove** again.
  - Click the - option that appears next to the IP address that you want to remove, and in the confirmation window, click **Remove** again.

## About configuring firewall for an application

The Application Blocking settings let you configure the firewall rules for the different applications that run on your Mac. Based on these settings, the firewall allows or blocks connections to the Internet from an application.



You cannot specify the firewall settings for applications based on the network to which your Mac is connected. The Application Blocking settings remain the same regardless of the network location. Application Blocking does not let you allow or block connections to a specific IP address.

When an application for which you have not specified Internet access tries to connect to the Internet, Norton Security prompts you with a notification dialog. You can choose whether you want the firewall to allow or block the application from accessing the Internet.

In addition to setting Internet access for applications, you can select the following options for the application in the **Application Blocking** window:

<b>Search icon</b>	Lets you locate an application in the <b>Settings</b> list.
<b>Add application</b>	Lets you add an application and configure the Internet access manually.
<b>Remove</b>	Lets you remove a selected application from the <b>Settings</b> list.

<b>Allow applications that are signed by Apple</b>	Lets you automatically allow the applications that are signed by Apple to access the Internet.
<b>Notify me when a blocked application tries to use the Internet</b>	Lets you configure Norton Security to notify you whenever a blocked application attempts to access the Internet.
<b>Log all applications that use the Internet</b>	Lets you keep record of the applications that access the Internet.  This information is viewable in the <b>Security History</b> window.
<b>Reset to defaults</b>	Lets you reset configuration to default level.

## Setting up firewall rules for an application

Applications that run on your Mac connect to the Internet to download updates or to send information about a program. For example, when you open Apple iTunes, it connects to the Internet to get the latest Store information of iTunes. If you trust the application, you can allow the application to connect to the Internet.

In some cases, you may want to deny Internet access for some applications. For example, Norton Security notifies you about an application that tries to connect to the Internet. You can block the Internet connection for the application to prevent it from sending or receiving any malicious information.

You can use the **Application Blocking** window to configure the Internet access for an application. The

selected application appears in the **Settings** list in the **Application Blocking** window. The application name and the firewall setting that you select appear in the **Settings** list in the **Application Blocking** window.

#### To set up firewall rules for an application

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Application Blocking** row, click the settings icon.
- 4 In the **Application Blocking** window, click **Add application**.  
If the application that you want to choose does not appear in the list, click **Other** to search for the application.
- 5 In the **Choose Application** dialog, select the required application.
- 6 Click **Choose**.  
The name of the application that you have added appears in the **Settings** list in the **Application Blocking** window.
- 7 Click **Done**.

## Customizing the firewall rule for an application

A firewall is a security system that uses rules to block or allow connections and data transmission between your Mac and the Internet. Firewall rules controls and protects your Mac from malicious programs and unauthorized access. The firewall automatically checks all traffic that comes in or out of your Mac against these rules.

You can use the **Application Blocking** window to customize the firewall rule for an application. You can use the up arrow and the down arrow next to the name of the application to allow or block Internet access for the application.

**To customize the firewall rule for an application**

- 1 In the **Application Blocking** window, select the application name row.
- 2 Click the up arrow or the down arrow next to the name of the application and do one of the following:
  - To allow the application to access Internet, choose **allow**.
  - To block the application to access Internet, choose **block**.
- 3 Click **Done**.

## Removing the firewall rule for an application

You can use the **Application Blocking** window to remove some of the firewall rules if necessary.



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 Mac.

**To remove the firewall rule for an application**

- 1 In the **Application Blocking** window, select the application name row.
- 2 Click **Remove**.
- 3 In the confirmation window, click **Remove**.
- 4 Click **Done**.

## About Location Awareness settings

Location Awareness settings lets you configure the firewall settings based on the network location to which your Mac is connected. The firewall settings that you configure contains the connection blocking settings for the application and services that run on your Mac. When you connect your portable Mac to a new network



location, Norton Security prompts you to select a new firewall setting for the network location.

You can use the **Location Awareness** window to do the following:

- Turn on or turn off the Location Awareness feature.
- View the current network location to which your Mac is connected.

## Disabling or enabling Location Awareness

The **Location Awareness** feature lets you set the **Connection Blocking** settings for every network that your Mac connects to. By default, the network to which your Mac is connected when you install your Norton product is categorized as **Trusted**. When you connect your Mac to weaker or vulnerable networks, your Norton product categorizes those networks as **Untrusted**. However, if you think a network is safe and trustworthy, you can change the network category to **Trusted**.

You can disable or enable the **Location Awareness** feature from the **Advanced** window.

### To disable or enable Location Awareness

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 In the Norton Security main window, click **Advanced**.
- 3 On the left pane, click **Firewall**.
- 4 In the **Location Awareness** row, do one of the following:
  - To disable **Location Awareness**, move the **Location Awareness** switch to the **Off** position.
  - To enable **Location Awareness**, move the **Location Awareness** switch to the **On** position.

## Viewing Location Awareness settings

You can view the current network location to which your Mac is connected and the Location Awareness setting

## Exporting the connection blocking settings for a network location

using the **Location Awareness** window. You can also view the history of network locations to which your Mac was connected and the connection blocking settings.

### To view Location Awareness settings

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Location Awareness** row, click the settings icon.

The **Location Awareness** window displays the current network location to which your Mac is connected.

## Exporting the connection blocking settings for a network location

You can export the network location settings using the **Export** window. You can use the **Export** option present under the **File** menu in the Norton Security menu bar. Norton Security exports the network location settings as .npfx file format.

You can use the following options to export the network locations settings:

### Export all settings

Lets you export all of the settings of the selected network location

<b>Export only these settings</b>	Lets you export only the required settings of the selected network location Your options are: <ul style="list-style-type: none"><li>■ Application Blocking</li><li>■ Connection Blocking</li><li>■ Applications</li><li>■ Services &amp; Ports</li><li>■ Zones</li><li>■ Vulnerability Protection</li><li>■ Norton DeepSight™ Community Download</li></ul>
-----------------------------------	---

<b>Password protect the exported settings</b>	Lets you add a password to protect the exported file.
---	---



You can use the **Password protect the exported settings** check box to protect the exported network location settings.

You can import the saved settings later to view it or apply to another computer that has Norton Security.

#### To export the connection blocking settings for a network location

- 1 In the Norton QuickMenu, click **Norton Security**.
- 2 On the Norton Security menu bar, click **File > Export**.
- 3 In the **Export** window, select the export option as required.
- 4 Click **Export**.

## About advanced protection

The **Advanced** window lets you configure the advanced protection features for Norton Security.

The following are the different advanced protection features:

**Norton DeepSight  
Community Download**

Lets you configure Norton Security to automatically obtain the updated list of IP addresses of computers that Symantec identifies as attackers.

**Norton DeepSight  
Community Submission**

Lets you configure Norton Security to automatically submit any suspicious network activity to Symantec for evaluation.

Symantec saves only the geographic location of the computer that submits the event. It does not save the IP address of the computer.

**Vulnerability Protection**

Lets you configure Norton Security to scan all of the network traffic that enters and exits your Mac and compare this information against a set of attack signatures.

The attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability.

## Disabling or enabling advanced protection features

The **Advanced** window lets you disable or enable the following advanced protection features of Norton Security:

- **Norton DeepSight Community Download**
- **Norton DeepSight Community Submission**
- **Vulnerability Protection**

By default, the advanced protection features are enabled. Symantec recommends that you do not disable any of the advanced firewall features.

### To disable or enable Norton DeepSight Community Download

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **DeepSight** row, click the settings icon.
- 4 In the **Norton DeepSight Settings** window, on the **Downloads** tab, do one of the following:
  - To disable **Norton DeepSight Community Download**, select **Off**.
  - To enable **Norton DeepSight Community Download**, select **On**.
- 5 Click **Done**.

### To disable or enable Norton DeepSight Community Submission

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **DeepSight** row, click the settings icon.
- 4 In the **Norton DeepSight Settings** window, on the **Submission** tab, do one of the following:
  - To disable **Norton DeepSight Community Submissions**, select **Off**.
  - To enable **Norton DeepSight Community Submissions**, select **On**.

### To disable or enable Vulnerability Protection

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, do one of the following:
  - To disable **Vulnerability Protection**, move the switch to the **Off** position.
  - To enable **Vulnerability Protection**, move the switch to the **On** position.

## Configuring Norton DeepSight Community Download

The **Norton DeepSight Community Download** feature lets you obtain the updated list of IP addresses that Symantec identifies as attackers.

You can turn on the **Norton DeepSight Community Download** feature to obtain the updated list of IP addresses from Symantec servers.

You can turn on or turn off the **Norton DeepSight Community Download** feature in the **Advanced** window to allow or deny the information to be downloaded from Symantec servers.

### To configure Norton DeepSight Community Download

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **DeepSight** row, click the settings icon. The **Norton DeepSight Settings** window displays a list of IP addresses that Symantec identifies as attackers.

**Configuring Norton DeepSight Community Submission**

- 4 On the **Downloads** tab, select the required option to set connections for all of the IP addresses in the list.

Your options are:

<b>Block all connections</b>	Lets you block the incoming and the outgoing connections from all the IP addresses in the list.
<b>Block only incoming connections</b>	Lets you block only the incoming connections from the IP addresses in the list.

- 5 Click **Done**.

## Configuring Norton DeepSight Community Submission

Norton DeepSight Community Submission helps you identify new security risks by submitting selected security and application data to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. You can enable or disable the Norton DeepSight Community Submission feature in the Advanced Protection window to allow or block the security risks information submission.



Norton DeepSight Community Submission 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.

### To configure Norton DeepSight Community Submission

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **DeepSight** row, click the settings icon.

- 4 In the **Norton DeepSight Settings** window, on the **Submissions** tab, do one of the following:
  - To disable **Norton DeepSight Community Submission**, select **Off**.
  - To enable **Norton DeepSight Community Submission**, select **On**.

## Configuring AutoBlock settings

You can use the **AutoBlock** tab in the **Vulnerability Protection** window to automatically block the IP addresses of computers that Symantec identifies as attackers. When you turn on the **AutoBlock** option, Norton Security adds the IP addresses of the attackers to the **Addresses currently blocked by AutoBlock** list. You can use the **Addresses should remain in the list for** menu to specify a time period for which Norton Security must block any connections from the attacker's IP address.

You can remove an IP address from the **Addresses currently blocked by AutoBlock** list using the **Remove** option.

You can also use the **Excluded addresses** option to create exceptions for IP addresses that you trust. Norton Security allows connections from an excluded address and does not include the address in the **Addresses currently blocked by AutoBlock** list.

### To configure AutoBlock settings

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, select the **AutoBlock** tab.
- 5 Click the **On** option to turn on AutoBlock.



- 6 View the list of IP addresses blocked by the Vulnerability Protection feature in the **Addresses currently blocked by AutoBlock** list.
- 7 Set the time period for which Norton Security must block any connections in the **Addresses should remain in the list for** list.  
 The default value is 30 minutes.
- 8 Click **Done**.

## Managing Excluded IP addresses

You can use the **Excluded addresses** option in the **AutoBlock** tab in the **Vulnerability Protection** window to create exceptions for IP addresses that you trust. Norton Security allows connections from an excluded address and does not include the address in the **Addresses currently blocked by AutoBlock** list.

You can use the **Excluded IP addresses** dialog to add the IP addresses you trust.

Your options are:

- |  |   |
|--|---|
| <b>All computers on my current network</b> | Lets you allow connections to or from all the computers that are connected on the network to which your Mac is connected. |
| <b>A single computer</b>                   | Lets you allow connections to or from the IP address of the computer that you specify.                                    |
| <b>All IP addresses beginning with</b>     | Lets you allow connections to or from the computers whose IP addresses begin with the IP address that you specify.        |

<b>All IP addresses on a network</b>	Lets you allow connections to or from all the computers on a local network that share the base address and mask address that you specify.
--------------------------------------	---

You can use the **Exclude IP addresses** window to do the following:

- Add the IP addresses you trust.
- Edit the IP addresses in the excluded IP address list.
- Remove the IP address from the excluded IP address list.

#### To add an excluded IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, select the **AutoBlock** tab.
- 5 Click the **On** option to turn on AutoBlock.
- 6 Click the **Excluded addresses** option.
- 7 In the **Excluded IP addresses** dialog, click **Add**.
- 8 In the **New AutoBlock excluded address** dialog, select the required option from the menu to add an excluded IP address.
- 9 Type the base address and click **Save**.

#### To edit an excluded IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, select the **AutoBlock** tab.
- 5 Click the **Excluded addresses** option.

- 6 In the **Excluded IP addresses** dialog, select the excluded IP address, and click **Edit**.
- 7 In the **Edit AutoBlock excluded address** dialog, make the changes as required.
- 8 Click **Save**.

#### To remove an excluded IP address

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, select the **AutoBlock** tab.
- 5 Click the **On** option to turn on AutoBlock.
- 6 Click the **Excluded addresses** option.
- 7 In the **Excluded IP addresses** dialog, select the IP address that you want to remove.
- 8 Click **Remove**.
- 9 Click **Save**.

## Configuring Signatures settings

Vulnerability Protection uses a frequently updated list of signatures to detect known attacks. You can view the list of signatures in the **Signatures** list.

You can receive alerts when an access attempt that matches a signature occurs using the **Enabled** option and the **Notify** option next to a signature in the **Signatures** list. By default, all the signatures are enabled and selected for notification.

You must not disable any signatures in the **Signatures** list. If you disable a signature, **Vulnerability Protection** feature cannot protect you from the threat that is related to the signature.

You can also enable the **Notify me when Vulnerability Protection automatically blocks an attack alerts** to

receive an alert whenever Vulnerability Protection blocks an attack.

**To configure the Signature settings**

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Firewall**.
- 3 In the **Vulnerability Protection** row, click the settings icon.
- 4 In the **Vulnerability Protection** window, select the **Signatures** tab.
- 5 Under the **Signatures** list, disable or enable the required options for any signature.
- 6 Click **Done**.

# Managing items in Quarantine

# 9

This chapter includes the following topics:

- [About Norton Security Quarantine](#)
- [Repairing an item in the Quarantine](#)
- [Restoring an item from the Quarantine](#)
- [Deleting an item from the Quarantine](#)

## About Norton Security Quarantine

Sometimes Norton Security detects an unknown virus that cannot be eliminated with the current set of virus definitions. Norton Security quarantines it automatically. The files that are in Quarantine are removed from their original locations on your Mac and are isolated, so that they cannot spread or infect your Mac. You cannot view the file in the Finder or use the file while it is in Quarantine. As a result, you cannot accidentally open the file and spread the virus.

## Repairing an item in the Quarantine

If an infected file is detected, Norton Security attempts to repair the file. If it cannot be repaired, it is quarantined. Symantec frequently updates the virus definition. Hence, if new virus definition is received after the file has been quarantined, you can attempt to repair the quarantined

item. New virus definitions might repair the file that could not be repaired previously.

#### To repair an item from the Quarantine

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Activity**.
- 3 In the **Security History** row, click the view icon.
- 4 In the **Security History** window, under **Protect my Mac**, click **Quarantine**.
- 5 In the quarantined items list, select the file item that you want to repair.
- 6 Click the **Actions** icon on the top-left corner, and then click **Repair**.
- 7 Click **Done**.

## 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 a safe location on your Mac. This way, Norton Security lets you restore any file to regain the functionality of a program.

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 from the Quarantine.

Some quarantined items are successfully disinfected after Norton Security 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, click **Advanced**.
- 2 On the left pane, click **Activity**.

- 3 In the **Security History** row, click the view icon.
- 4 In the **Security History** window, under **Protect my Mac**, click **Quarantine**.
- 5 In the quarantined items list, select the item that you want to restore.
- 6 Click the **Actions** icon on the top-left corner, and then click **Restore**.
- 7 Click **Done**.

## Deleting an item from the Quarantine

You can delete an item from the Quarantine at any time. When you delete an item from the Quarantine, it is removed permanently from your Mac. You can delete a quarantined item only if you are sure that you no longer need it.

### To delete an item from the Quarantine

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Activity**.
- 3 In the **Security History** row, click the view icon.
- 4 In the **Security History** window, under **Protect my Mac**, click **Quarantine**.
- 5 In the quarantined items list, select the item that you want to delete.
- 6 Click the **Actions** icon on the top-left corner, and then click **Delete**.
- 7 Click **Done**.

# Protecting against new threats

# 10

This chapter includes the following topics:

- [About LiveUpdate](#)
- [About program updates and definition updates](#)
- [Checking for updates manually](#)

## About LiveUpdate

Using your Internet connection, Norton Security automatically downloads the latest definition updates and program updates regularly from Symantec servers. The definition updates protect your computer from the latest viruses and unknown security risks.

Norton Security takes little time to download and process the definition updates and program updates. To ensure that your Mac is updated with latest program and definition updates, Norton Security automatically runs LiveUpdate every 2 hours.

## About program updates and definition updates

Norton Security obtains program updates and definition updates for all the Symantec products that you installed on your Mac.



Program updates are improvements for all the Symantec products that you installed on your Mac. Program updates differ from product upgrades, which are newer versions of the product. Program updates are usually created to improve the product's compatibility with the operating system or hardware, adjust a performance issue, or fix program errors.

Norton Security automates the process of downloading and installing program updates. It locates and downloads files regularly from Symantec servers. Norton Security uses your Internet connection to download these updates. Norton Security then installs the downloaded files and deletes the leftover files from your computer.



Some program updates may require that you restart your computer after you install them.

Definition updates are the files that keep your Symantec products up to date with the latest antithreat technology.

The types of definition updates that your Norton product receives are as follows:

- Virus definition service updates, which provide access to the latest virus signatures, attack signatures, and other technology from Symantec.
- Information about known good and fraudulent websites.
- Latest versions of the product and protection-related files.

## Checking for updates manually

Norton Security downloads the latest definition updates and program updates regularly from Symantec servers. The definition updates protect your computer from the latest viruses and security threats. Symantec products obtain and install these updates by using the Norton Security technology.

By default, Norton Security automatically downloads and installs the latest definition updates and program

updates regularly from Symantec servers. However, you can manually download the updates from Symantec servers using Norton Security.



Some program updates may require that you restart your computer after you install them.

**To check for updates manually**

- ❖ In the Norton Security main window, click **LiveUpdate**.

# Finding additional solutions

# 11

This chapter includes the following topics:

- [Checking for virus names and definitions](#)
- [Uninstalling Norton Security on Mac](#)

## Checking for virus names and definitions

The **Virus Definitions** window lists the names of viruses and their details. To know if your Mac is protected from a particular virus, you can search for the virus name. By default, Norton Security automatically updates virus definitions on a regular basis.

You can select each of the viruses and click the impact icon to see how severe the virus might affect your mac, when infected. You can click **Learn More** to read the summary. The summary of each virus is displayed on a separate webpage.

### To look up virus names

- 1 In the Norton Security main window, click **Advanced**.
- 2 On the left pane, click **Protect my Mac**.
- 3 In the **Virus Definitions** row, click the settings icon.
- 4 In the **Virus Definitions** window, type the name or part of the name of the virus in the search field. Norton Security displays all the related viruses. You can click on the virus for which you want to know more information.
- 5 Click **Done**.

## Uninstalling Norton Security on Mac

To uninstall Norton Security, you must know the Administrator account user name and password.

You must restart your Mac after uninstalling the product.



To ensure continuous protection, Symantec recommends you to keep Norton Security installed on your Mac.

### To uninstall Norton Security

- 1 On the Mac menu bar, click the **Symantec** icon.
- 2 In the Norton Security menu, click **Norton Security > Uninstall Norton Security**.
- 3 In the window that appears, click **Uninstall**.
- 4 Type your Administrator password when prompted.
- 5 Click **Restart Now** when prompted to restart your Mac.

You can also uninstall Norton Security by dragging and dropping the Norton Security application from the **Applications** folder to the **Trash**.

This chapter includes the following topics:

- [About support](#)
- [About Self Help](#)
- [Contact Support](#)
- [Support Policy](#)
- [Keeping your subscription current](#)

## About 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 Self Help

The Symantec website contains answers to the most common customer questions. From our website you can:

- Find help with your subscription, download, product activation, or other nontechnical issues.
- Search our Support Resources for help with technical issues, such as installing, configuring, or troubleshooting errors with your Norton products.
- Find information about the latest virus threats and removal tools.

You can access the Symantec Support website at:  
[www.norton.com/macsupport](http://www.norton.com/macsupport)

## Contact Support

In addition to using our Self Help options, you can contact a support representative by chat, email, or phone.



Availability of support varies by region. Regular telephone and Internet connection fees apply in certain countries. For full support details, please visit:

[www.norton.com/macsupport](http://www.norton.com/macsupport)

Following is an overview of our support offerings:

Chat	Chat in real time with a support representative.
Email	Submit your question on our website and receive a response by email. Email support has a slower response time when compared to phone. Email support is free.

Phone	Speak to a support representative in real time.
-------	---

To contact a support representative, please visit the Symantec support website at the following URL:

[www.norton.com/macsupport](http://www.norton.com/macsupport)

The online support option is displayed along with the **Contact Us** link where you can select the type of support you prefer.

## Support Policy

Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats. In case of older versions, complimentary support is offered for a minimum of two years. However, technical information on these products may still be available through the support website at the following address:

[www.norton.com/macsupport](http://www.norton.com/macsupport)

Symantec reserves the right to change its support policies at any time without notice. You can view the latest version of the support policy at the following URL:

[www.symantec.com/supportpolicy](http://www.symantec.com/supportpolicy)

## Keeping your subscription current

This renewable service includes protection updates and new product features as available throughout the service period. Please note that features may be added, modified, or removed during the subscription period.

Service period lengths vary by Symantec product. After your initial subscription period ends, you must renew your subscription before you can update and use your protection. When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe



for a nominal charge. Follow the instructions on the screen to renew.

The subscription renewal alert is not displayed if you opted for the Automatic Renewal service when you purchased your Norton product. Your product is automatically renewed before it expires. If Automatic Renewal fails, the subscription renewal alert is displayed.



Norton from Symantec products protect consumers from traditional threats with antivirus, antispyware, 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](#) | [Antispyware](#) | [Spyware Protection](#) | [Online Backup](#)

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, Norton, and the Norton Logo are trademarks or registered trademarks of Symantec Corporation and its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.