

# Norton™ AntiVirus

Product Manual



# Norton™ AntiVirus Product Manual

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

Documentation version 22.20.1

Copyright © 2020 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Norton, Norton by Symantec, Norton Secured Logo, LifeLock, and the LockMan Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U. S. and other countries. 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, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
350 Ellis Street,  
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Contents

Chapter 1	Welcome to Norton .....	6
	System requirements for Norton AntiVirus .....	6
	FAQ: Norton account .....	7
	Find your product key, PIN, or renewal code .....	8
Chapter 2	Download and install Norton .....	11
	Download and install Norton .....	11
	Install Norton on additional devices .....	13
	Transfer your Norton license to a new device .....	15
	Troubleshoot with Norton Bootable Recovery Tool .....	16
Chapter 3	Understand and respond to threats .....	19
	What to do when your device is at risk .....	19
	Keep your Norton device security up to date .....	20
	View or fix device security threats that Norton detects .....	22
Chapter 4	Manage your security .....	24
	View your system activities .....	24
	View the Report Card .....	25
	Act on quarantined risks or threats .....	25
Chapter 5	Scan your computer .....	28
	Run Norton scans to check for threats on your PC .....	28
	Create your own custom Norton scans .....	31
	Schedule Norton scans .....	32
	Customize Real Time Protection settings .....	33
	View real-time threats that Norton SONAR protection detects .....	34
	Exclude files and folders from Norton Auto-Protect, SONAR, and Download Intelligence scans .....	36
	Exclude files with low-risk signatures from Norton scans .....	37
	Clear file IDs excluded during scans .....	37
	Turn on or turn off automatic tasks .....	38
	Run custom tasks .....	39

	Schedule security and performance scans .....	39
	Configure Data Protector to block malicious processes affecting your PC .....	40
	Set Norton to remove scripts that can be exploited in phishing attempts .....	43
	FAQs: Norton Script Control .....	45
Chapter 6	Keep secure on the Internet .....	48
	Turn on Browser Protection .....	48
	Intrusion Prevention exclusion list .....	49
	Set Norton to monitor applications and block malicious websites from accessing your computer .....	50
	Turn off or turn on AutoBlock .....	52
	Unblock AutoBlocked computers .....	53
	Add a device to Device Trust .....	53
	Turn off or turn on Download Intelligence .....	54
	Turn off or turn on spam filtering .....	55
	Define the Internet usage for Norton .....	56
	Turn off or turn on Network Cost Awareness .....	57
	Wi-Fi Security .....	57
	Protect your banking information using Norton Safe Web .....	58
Chapter 7	Secure your sensitive data .....	59
	Add the Norton browser extensions .....	59
	Turn off or turn on Norton Safe Web .....	63
	Search the web using Norton Safe Search .....	64
	Scam Insight .....	65
	Antiphishing .....	66
	Access Norton Password Manager .....	66
	Turn on or turn off Norton Password Manager .....	67
	Create Norton Password Manager cloud vault .....	68
	Delete your Norton Password Manager cloud vault .....	70
	Export your Norton Password Manager data .....	71
	Import your Norton Password Manager data .....	72
	Enable or disable the Norton Security toolbar .....	74
Chapter 8	Keep your PC tuned up .....	75
	Use Norton to optimize and improve computer performance .....	75
	View or change the Norton trust level of files that you use .....	79
	Set Norton to alert you about performance issues .....	80
	Run a Norton Diagnostic Report .....	81

	Set Norton to maximize your PC startup time .....	81
Chapter 9	Customize settings .....	84
	Configure Network Proxy Settings .....	84
	Set Norton to allow you to remotely manage your protected devices .....	85
	Protect Norton device security settings from unauthorized access .....	85
	Configure Norton for best battery use .....	86
	Set a shortcut key to search Norton device security for information .....	87
Chapter 10	Find additional solutions .....	88
	Find the version number of your product .....	88
	Upgrade your Norton product .....	88
	Uninstall your Norton product .....	89

# Welcome to Norton

This chapter includes the following topics:

- [System requirements for Norton AntiVirus](#)
- [FAQ: Norton account](#)
- [Find your product key, PIN, or renewal code](#)

## System requirements for Norton AntiVirus

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

### Windows

#### ◆ Operating systems

- Microsoft Windows® 10 (all versions)
- Microsoft Windows® 8.1 or later (32-bit and 64-bit)
- Microsoft Windows® 8 and Windows® 8 Pro (32-bit and 64-bit)
- Microsoft Windows® 7 (32-bit and 64-bit) with Service Pack 1 or later

### Hardware

#### ■ Processor

For Windows 10/8/7: 1 GHz

#### ■ RAM

For Windows 10: 2 GB (minimum of 512 MB RAM required for Recovery Tool)

For Windows 8/7: 1 GB (32-bit) (minimum of 512 MB RAM required for Recovery Tool)

#### ■ Hard disk space

300 MB of available hard disk space

### **Browser support for Vulnerability Protection**

The following browsers are supported for Vulnerability Protection.

- Microsoft Internet Explorer® 8.0 or higher (32-bit and 64-bit)<sup>1,2</sup>
- Mozilla Firefox® (32-bit and 64-bit)<sup>2</sup>
- Google Chrome™ (32-bit and 64-bit)<sup>2</sup>

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

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

- Microsoft Internet Explorer® 8.0 or higher (32-bit and 64-bit)<sup>1,2</sup>
- Microsoft Edge® (32-bit and 64-bit)<sup>1,2</sup>
- Mozilla Firefox® (32-bit and 64-bit)<sup>2</sup>
- Google Chrome™ (32-bit and 64-bit)<sup>2</sup>

---

**Note: Safe Search** feature is not available in Microsoft Edge browser.

---

### **Email clients**

Norton AntiVirus supports email scanning on all POP3 and SMTP compatible email clients.

<sup>1</sup> Some protection features are not available in Microsoft Internet Explorer 10.0 or later.

<sup>2</sup> As made available by Symantec within your service period.

## **FAQ: Norton account**

Sign in to your Norton account to do the following:

- Activate your product
- Access your backup
- Access or create your cloud Vault
- Manage your Norton subscriptions
- Reinstall Norton products by using your product keys stored in your account
- Buy storage to add more space for your online backup

### **How do I sign in to my Norton account?**

You access your Norton account from any device at <https://my.norton.com>.

To sign in, type the email address and password that you used when you created your Norton account.

---

**Note:** If you have opted for the Two-Step Verification to access your Norton account, you have to use the verification code in addition to your password.

---

## How do I recover my Norton account password?

- 1 On the Norton account sign in page, click **Forgot password?** link.
- 2 Type the email address that you used to purchase your Norton product or to create your Norton account.
- 3 Click **Continue**.
- 4 You will receive an email with reset password link from [norton@symantec.com](mailto:norton@symantec.com). Check your spam or junk folders if you do not see the email in your Inbox.

If clicking the link does not work, copy and paste this link directly into a web browser.

If you still cannot locate the email, make sure that the email address you enter is the same as the one that you used to make your Norton product purchase or to create your Norton account.

## I do not know if I have a Norton account

See the information below to help you find if you have a Norton account:

- If you have installed or activated a Norton product, you most likely have a Norton account. As part of the installation or activation process, you need to create one by providing your name, email address, and a password.
- If you purchased a product from the [Norton Online Store](#) or renewed a Norton product subscription you were asked to provide your name, email address and a password, and a Norton account was created for you.
- If you signed up for Norton Family, Norton Online Backup, or Norton Safe Web, you may have a Norton account. But, ensure that this account also has the Norton Security license associated with it.

## Find your product key, PIN, or renewal code

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

- **Product key:** A 25-character alphanumeric string shown in five groups of five characters each, separated by hyphens, that you need to activate or renew your Norton subscription.



- **Renewal code:** A 19-character alphanumeric code that you need to extend your Norton subscription.

## Find your product key

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

## Get the product key from Norton

- 1 [Sign in](#) to Norton.
  - 2 In the page that appears, click or hover the mouse on your profile, and then choose **My Subscriptions**.
  - 3 Go to the Norton product for which you want to see the product key.
  - 4 Write down or copy the product key.
- If you purchased your product from Hong Kong Online Store, refer to [How do I find the product key for the Norton product that I purchased from Hong Kong Norton Online Store](#) for detailed instructions.
  - If you obtained your Norton product by other means, see the section below.

## Other ways to find the product key

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

## Find your renewal code

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

## Get the renewal code from Norton

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

# Download and install Norton

This chapter includes the following topics:

- [Download and install Norton](#)
- [Install Norton on additional devices](#)
- [Transfer your Norton license to a new device](#)
- [Troubleshoot with Norton Bootable Recovery Tool](#)

## Download and install Norton

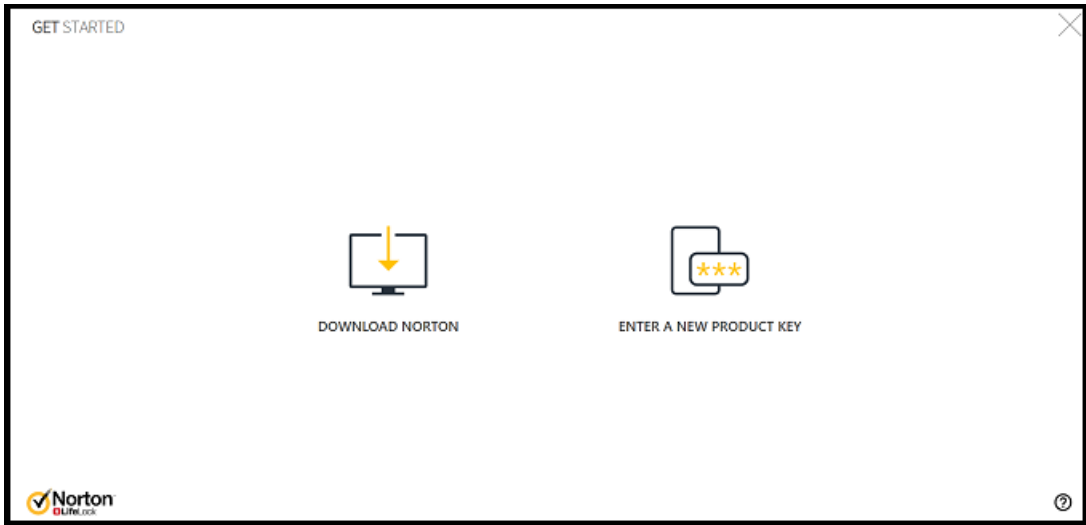
Protecting your devices and managing your Norton product is as easy as adding a new device to your Norton account.

**To download and install Norton on your computer**

- 1 [Sign in](#) to Norton.
- 2 If you are not signed in to your account, enter your email address and password, and then click **Sign in**.

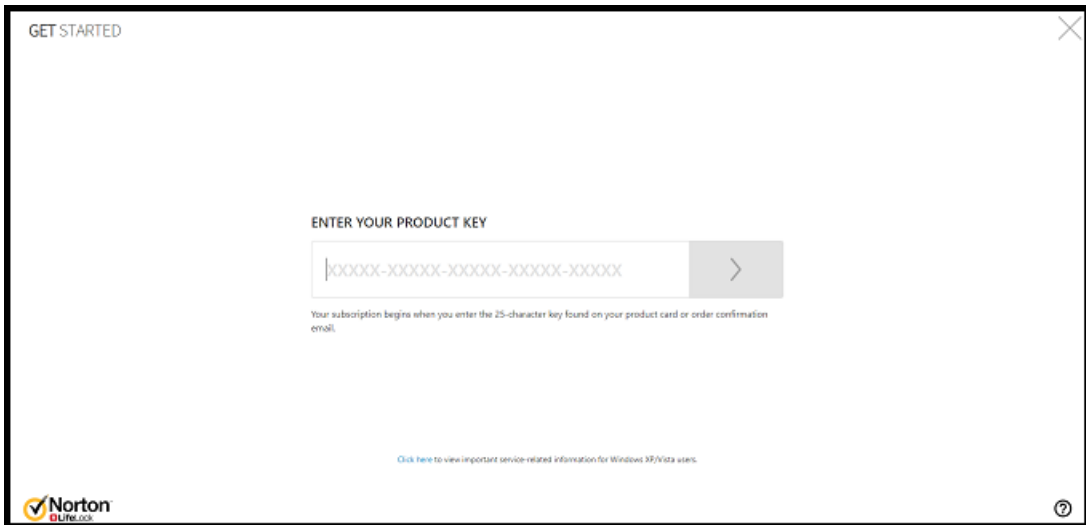
If you do not have an account, click **Create an Account**, and then complete the sign-up process.

3 In the **Get Started** window, click **Download Norton**.



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

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



4 Click **Agree & Download**.

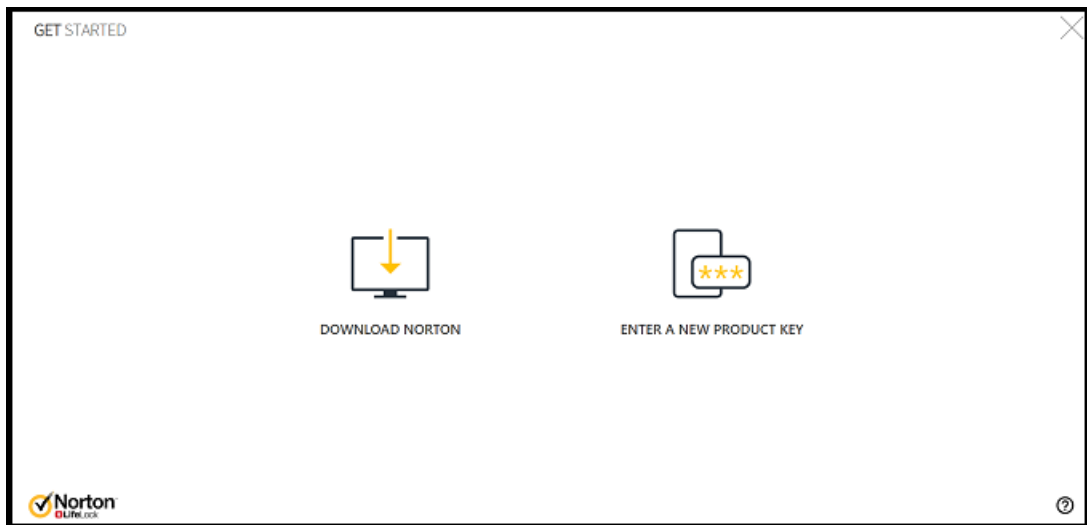
- 5 Click the area pointed by the on-screen blue arrow and follow the on-screen instructions.
  - For Internet Explorer or Microsoft Edge browser: Click **Run**.
  - For Firefox or Safari: On the top-right corner of the browser, click the **Download** option to view the downloaded files, and double-click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

## Install Norton on additional devices

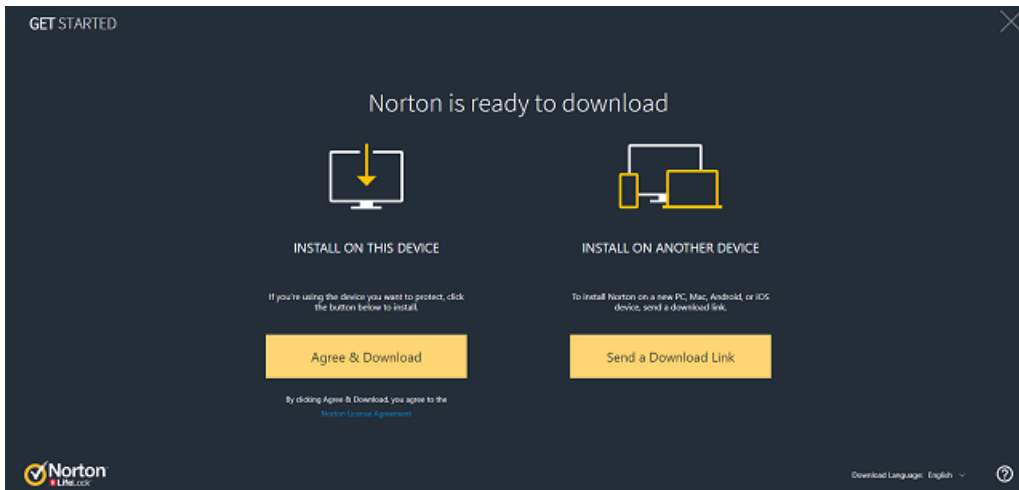
From your Norton account, you can send emails to additional devices and install Norton on the devices. The email contains the install link and instructions to install Norton.

### To install Norton on a different device

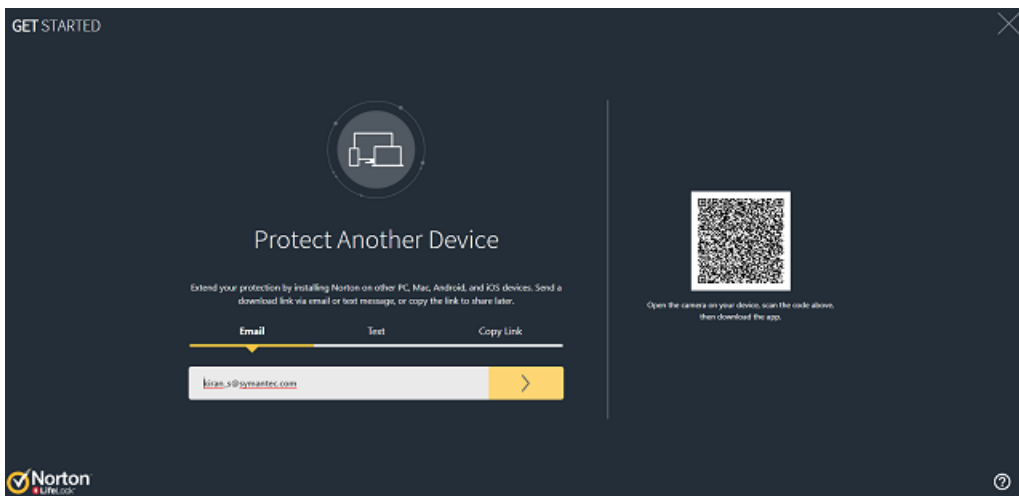
- 1 [Sign in](#) to Norton.
- 2 If you are not signed in to your Norton account, enter your email address and click **Sign In**.
- 3 In the **Get Started** window, click **Download Norton**.



- 4 In the page that appears, click **Send a Download Link**.



- 5 Enter an email address that you can access on your additional device and click the send button, and then click **Done**.



An email is sent to the email address with instructions to install the Norton product.

- 6 On the device where you want to download Norton, locate and open the email that you received from **The Norton Team**.
- 7 Click **Download Now**.

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

## Transfer your Norton license to a new device

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

### Transfer the Norton license

- 1 [Sign in](#) to your Norton account.
- 2 In the **Devices** page, identify the device that you no longer want to protect.

---

**Note:** The device must appear with a green status. If the device that you no longer use appears with a red or an orange status, you can remove the device from your Norton account and free a license.

---

- 3 Click the ellipse icon available below the device.
- 4 In the menu that appears, click **Manage License**.
- 5 In the **Manage Device** page, do the following:
  - Click on the device name.
  - Under **What would you like to do**, click **Remove Norton**.
  - Click **Next**.
- 6 In the **Remove Norton** window that appears, click **Yes**.
- 7 In the page that appears, click **Install Now**.
- 8 In the **Install on New Device** page, select one of the following:
  - To install Norton on the current device, click **Download**.
  - To install Norton on a different device, click **Send Link**.
- 9 Click **Next**.
- 10 Follow the on-screen instructions to complete the installation.

# Troubleshoot with Norton Bootable Recovery Tool

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

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

---

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

---

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

To download the ISO file

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

## Step 2: Create a Norton Bootable Recovery Tool bootable media

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

---

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

---

---

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

---

## Step 3: Launch Norton Bootable Recovery Tool

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



### To launch Norton Bootable Recovery Tool

- 1 Insert the Norton Bootable Recovery Tool DVD or USB drive that you created.
- 2 Turn on or restart the infected computer, then enter the BIOS mode by pressing the key that appears on the screen immediately after your computer restarts.
- 3 Select the DVD or the USB drive on which you created Norton Bootable Recovery Tool, and then press **Enter**. If you use a UEFI-enabled computer, select the recovery media under the **Legacy Boot** option instead of the **UEFI Boot** option. The recovery media is the Norton Bootable Recovery Tool DVD or USB drive.
- 4 In the **Welcome to NBRT** page, select the **Boot** option. If the booting fails, then select **Boot (Basic Video)** option.
- 5 In the **Select Language** drop-down list, select your preferred language, and then click **OK**.
- 6 Read the Norton license agreement and then click **Agree** to launch the tool.

### Step 4: Scan and resolve threats

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

#### To scan and resolve threats

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

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

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

---

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

---

- 4 Click **Fix**.
- 5 In the confirmation dialog box, click **OK**.
- 6 The **Remediation window** displays the status of each threat under the **Action** column.

7 Click **Continue**.

8 In the **Reboot your computer** window, click **Reboot** to restart your computer.

If you want to run the scan again, click **Scan Again**.

Norton Bootable Recovery Tool automatically downloads and updates the latest virus definitions from the Symantec servers when you initiate the scan and are connected to the Internet. The latest virus definitions helps you secure your computer from the latest viruses and security threats.

# Understand and respond to threats

This chapter includes the following topics:

- [What to do when your device is at risk](#)
- [Keep your Norton device security up to date](#)
- [View or fix device security threats that Norton detects](#)

## What to do when your device is at risk

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

- **Green:** You have protection.
- **Orange:** Your computer needs attention.
- **Red:** Your computer is at risk.

---

**Note:** The backup category is available only with Deluxe, Premium, and Norton 360 subscriptions.

---

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

### Respond to Attention or At Risk status indicators

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, click the red or orange tile of the category that indicates **At Risk** or **Attention**.

- 3 Click **Fix Now** and follow the on-screen instructions.

If you still have issues, click **Help > Get Support** to run the diagnostic tool.

You can also try using [Norton Rescue Tools](#) if you think your computer is severely infected.

## Keep your Norton device security up to date

If you turned off Automatic LiveUpdate or have been offline, you can check when you last received Norton device security updates and run LiveUpdate, if necessary, to assure that you have the latest

- virus definitions that help protect your device against malware, unauthorized network access, spam emails, and much more.
- program updates that extend operating system or hardware compatibility, adjust performance issues, or fix program errors.

While your subscription is current, Norton makes it easy to automatically receive updates that help protect you from emerging threats.

### Check when Norton was last updated

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

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

- 3 Under the security status indicator, check the date next to **Protection Updates**.

- 4 If the date is older than a day or two, run LiveUpdate.

### Run LiveUpdate to get the latest Norton updates

---

**Note:** Make sure that you are connected to the Internet.

---

1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

2 In the Norton main window, double-click **Security**, and then click **LiveUpdate**.

3 In the **Norton LiveUpdate** window, when LiveUpdate completes, click **OK**.

If LiveUpdate has failed due to some reasons, you can run Intelligent Updater to get the latest updates.

**Run Intelligent Updater if LiveUpdate has failed**

1 Go to the [Intelligent Updater](#) downloads page.

2 Depending on your version of Windows, do one of the following:

- For Windows 8.1/8/7/Vista/XP 32-bit: Click the first file in the list under Filename. The file name starts with the year and ends with v5i32.exe. For example, 20130528-017-v5i32.exe
- For Windows 8.1/8/7/Vista 64-bit: Go to the 64-bit Platforms section, and click the first file in the list under Filename. The file name starts with the year and ends with v5i64.exe. For example, 20130528-017-v5i64.exe

3 Save the file to the Windows desktop.

4 On the desktop, double-click the file that you saved.

**Make sure that Norton Automatic LiveUpdate is turned on**

1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

2 In the Norton product main window, click **Settings**.

3 In the **Settings** window, click **Antivirus**.

4 In the **Antivirus** settings window, click the **Updates** tab.

5 In the **Automatic LiveUpdate** row, move the switch to **On**.

6 Click **Apply**.

7 In the **Settings** window, click **Close**.

**Set Norton to apply updates without restarting your device**

---

**Note:** On Windows 7/8.1 or later devices, you can apply updates without restarting your computer.

---

- 1 Start Norton.  
 If you see the **My Norton** window, next to Device Security, click Open.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 In the **Antivirus** settings window, click the **Updates** tab.
- 5 In the **Apply updates only on reboot** row, do one of the following:
  - To receive LiveUpdate notifications asking if you want to apply updates without restarting, move the switch to **Off**. This is the default setting.
  - To apply updates only after you restart your computer, move the switch to **On**.
- 6 In the **Settings** window, click **Apply**, and then click **Close**.

## View or fix device security threats that Norton detects

When Norton detects a threat, it automatically removes it, unless it requires your input to understand how you want to resolve the threat. If you do need to provide input, Norton displays a Threats Detected alert or Security Risk alert with suggestions on how to respond to the threat.

### View risks that were automatically resolved during a scan

View risks automatically resolved during a scan

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In the **Security History** window, in the **Show** drop-down list, select **Resolved Security Risks**.
- 4 Select a risk in the list, then in the **Details** pane, view the action that was taken.

### Fix unresolved risks detected during a scan

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

Fix unresolved risks detected during a scan

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.

- 3 In the **Security History** window, in the **Show** drop-down list, select **Unresolved Security Risks**.
- 4 Select a risk in the list if there are unresolved risks displayed.
- 5 Follow the **Recommended Action** in the **Details** pane.

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

Run Norton Power Eraser if you think your system is infected. Norton Power Eraser is a powerful malware removal tool that eliminates the security risks that are difficult to remove. For more information, See ["Run Norton scans to check for threats on your PC"](#) on page 28.

---

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

---

## Restore a file that was mistakenly identified as a security risk

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

### Restore a file from Quarantine

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

---

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

---

# Manage your security

This chapter includes the following topics:

- [View your system activities](#)
- [View the Report Card](#)
- [Act on quarantined risks or threats](#)

## View your system activities

Norton provides information about the important system activities that you performed over a period of the last three months.

Norton monitors your computer's performance. If it detects an increased usage of system resources by any program or process, it notifies you with performance alerts.

### View details of your system activities

1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

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

3 In the **Graphs** window, click the tab for a month to view the details.

4 In the Events graph, move the mouse pointer over the icon or the stripe for an activity.

5 In the pop-up that appears, view the details of the activity.

6 If the **View Details** option appears in the pop-up, click **View Details** to view additional details in the **Security History** window.



## View the Report Card

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

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

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

### Turn off Report Card

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 In the **Report Card** row, move the **On/Off** switch to **Off**.

### How do I manually view the Report Card?

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

## Act on quarantined risks or threats

Quarantined items are isolated from the rest of your computer so that they cannot spread or infect your computer. If you have an item that you think is infected, but is not identified as a risk by Norton, you can manually put the item in Quarantine. You can also restore an item from quarantine if you think it is a low risk. Norton does not repair the item that you restore. However, Norton can disinfect the restored items during the subsequent scans.

### Restore an item from quarantine

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In **Security History** window, in the **Show** drop-down list, select the **Quarantine** category.
- 4 Select an item that you want to manage.

- 5 In the **Details** pane, click **Options**.

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

- 6 In the **Threat Detected** window, choose one of the following options:

- **Restore**: Returns the item to the original location on your computer. This option is available only for manually quarantined items.
- **Restore & Exclude this file**: Returns the item to its original location without repairing it and excludes the item from being detected in the future scans. This option is available for the detected viral and non-viral threats.
- **Remove from history**: Removes the selected item from the **Security History** log.

- 7 If you choose to restore, in the **Quarantine Restore** window, click **Yes**.

- 8 In the **Browse for Folder** dialog, select the folder or drive where you want to restore the file and then click **OK**.

## Submit an item for Symantec's evaluation

You can contribute to the effectiveness of your Norton product by submitting files that you think is a security risk. Symantec Security Response analyzes the file and if it is a risk, adds it to the future protection definitions.

---

**Note:** Personally identifiable information is never included in submissions.

---

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In **Security History** window, in the **Show** drop-down list, select the **Quarantine** category.
- 4 Select an item that you want to manage.
- 5 In the **Details** pane, click **Options**.

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

- 6 In the **Threat Detected** window, click **Submit to Symantec**.
- 7 In the screen that appears, click **OK**.

#### Quarantine an item manually

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In **Security History** window, in the **Show** drop-down list, select the **Quarantine** category.
- 4 Click **Add to Quarantine**.
- 5 In the **Manual Quarantine** window, add the file that you want to quarantine and enter a description for your reference.

---

**Note:** If you quarantine a file that is associated with any running processes, the processes get terminated. So, close all open files and running processes before adding a file to quarantine.

---

# Scan your computer

This chapter includes the following topics:

- [Run Norton scans to check for threats on your PC](#)
- [Create your own custom Norton scans](#)
- [Schedule Norton scans](#)
- [Customize Real Time Protection settings](#)
- [View real-time threats that Norton SONAR protection detects](#)
- [Exclude files and folders from Norton Auto-Protect, SONAR, and Download Intelligence scans](#)
- [Exclude files with low-risk signatures from Norton scans](#)
- [Clear file IDs excluded during scans](#)
- [Turn on or turn off automatic tasks](#)
- [Run custom tasks](#)
- [Schedule security and performance scans](#)
- [Configure Data Protector to block malicious processes affecting your PC](#)
- [Set Norton to remove scripts that can be exploited in phishing attempts](#)
- [FAQs: Norton Script Control](#)

## Run Norton scans to check for threats on your PC

Norton automatically updates virus definitions and regularly scans your PC for a range of threats. If you have been offline, or suspect that you have a virus, you can manually run the following:

- **Quick Scan** to analyze areas of your computer that are most vulnerable to threats.
- **Full System Scan** to analyze your entire system including less vulnerable applications, files, and running processes than those checked during a Quick Scan.
- **Custom Scan** to analyze individual files, folders, or drives if you suspect that they are at risk.

---

**Note:** After you install Norton, the first scan may take an hour or more to analyze your entire system.

---

### Run a Quick Scan, Full System Scan, or Custom Scan

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, next to **Scans and Tasks**, select one of the following:
  - **Quick Scan > Go**
  - **Full System Scan > Go**
  - **Custom Scan > Go**, then click **Run** next to **Drive Scan**, **Folder Scan**, or **File Scan** to navigate to the components that you want to scan.
- 4 In the **Results Summary** window, click **Finish**.  
If there are items that require attention, review the risks in the **Threats Detected** window.

### Full System Scan

Full System Scan performs a deep scan of your computer to remove viruses and other security threats. It checks all boot records, files, and running processes to which the user has access. This scans your computer thoroughly and takes longer time.

---

**Note:** When you run a Full System Scan with administrator privileges, it scans more files than when you run it without administrator privileges.

---

### Run a Full System Scan

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.

- 3 In the **Scans** window, under **Scans and Tasks**, click **Full System Scan**.
- 4 Click **Go**.

## Custom Scan

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

### Scan individual elements

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
- 4 Click **Go**.
- 5 In the **Scans** window, do one of the following:
  - To scan specific drives, click **Run** next to **Drive Scan**, select the drives that you want to scan, and then click **Scan**.
  - To scan specific folders, click **Run** next to **Folder Scan**, select the folders that you want to scan, and then click **Scan**.
  - To scan specific files, click **Run** next to **File Scan**, select the files that you want to scan, and then click **Add**. You can also press **Ctrl**, and select multiple files to scan.
- 6 In the **Results Summary** window, click **Finish**.  
If any items require attention, review them and take the recommended action.

## Norton Power Eraser scan

Norton Power Eraser is a powerful malware removal tool that can help you clean up the security risks that are difficult to remove. Norton Power Eraser uses aggressive techniques than normal scan process; sometimes there is a risk that Norton Power Eraser flags a legitimate program for removal. Review scan results carefully before removing any files using Norton Power Eraser.

### Scan using Norton Power Eraser

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, double-click **Security**, and then click **Scans**.

- 3 In the **Scans** window, under **Norton Power Eraser**, click **Norton Power Eraser**.
- 4 Click **Go**.
- 5 In the **Norton Power Eraser** window, click **OK**.
- 6 In the **Norton Power Eraser** main window, click **Advanced Scans**.
- 7 Click **System Scan**.
- 8 Review the scan results and follow the on-screen instructions to fix the security risks detected.

## Create your own custom Norton scans

While the default Norton automated scan settings work well for most users, some users may want to customize options to scan specific drives, folders, or files on a schedule that they choose.

### Create a custom scan

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**, and then click **Go**.
- 4 In the **Scans** window, click **Create Scan**.
- 5 In the **New Scan** window, next to **Scan Name**, type a name for your custom scan and add the settings as follows:
  - On the **Scan Items** tab, click **Add Drives**, **Add Folders**, or **Add Files** to navigate to the components that you want to include in the scan.
  - On the **Schedule Scan** tab, under When do you want the scan to run, select an interval, and then select the timing options.  
Under **Run the scan**, select from the options. For most users, it's best to keep all boxes checked. This assures that scans run only when you are not using your computer or when you are not using battery power, and it prevents your computer from going to sleep during a scan.
  - On the **Scan Options** tab, move the switches to customize behaviors for compressed files or low risk threats during the scan.
- 6 Click **Save**.

## Edit or delete a Norton custom scan

You can edit a custom scan that you created to rename the scan, add or remove files, or change the schedule. If you no longer need to run the scan, you can delete it.

### Edit or delete a custom scan

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**, and then click **Go**.
- 4 In the **Scans** window, in the **Edit Scan** column, next to the custom scan that you want to modify, do one of the following:
  - Click the edit icon, and then in the **Edit Scan** window, move the switches to turn the scan options on or off. For most users, the default settings work well. Click **Use Defaults** to remove custom settings.
  - Click the trash icon, and then click **Yes** to confirm that you want to delete the custom scan.
- 5 Click **Save**.

## Schedule Norton scans

Norton detects when you are away from your computer and automatically runs scans to assure that your system is regularly monitored for threats. You can also schedule your own Quick Scan, Full System Scan, or Custom Scan to run on times of your choosing.

### Schedule a Norton Quick Scan, Full System Scan, or Custom Scan

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, under **Scans and Tasks**, click **Custom Scan**.
- 4 Click **Go**.
- 5 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to Quick Scan, Full System Scan, or a Custom Scan that you previously created.
- 6 In the **Edit Scan** window, on the **Scan Schedule** tab:
  - Under **When do you want the scan to run**, select an interval, and then select the timing options.



- Under **Run the scan**, select from the options. For most users, it's best to keep all boxes checked. This assures that scans run only when you are not using your computer or when you are not using battery power, and it prevents your computer from going to sleep during a scan.
- 7 Click **Next**.
  - 8 In the **Scan Options** window, click **Save**.

## Customize Real Time Protection settings

Real Time Protection detects unknown security risks on your computer and lets you determine what action to take if it finds a risk.

---

**Note:** Default settings are recommended for most users. If you want to turn off a feature temporarily, turn it on as soon as possible. If you want low-risk items removed automatically, configure SONAR Advanced mode. Auto-Protect checks for viruses and other security risks every time that you run programs on your computer. Always keep Auto-Protect on.

---

### Set Auto-Protect to scan removable media

Removable Media Scan checks for viruses when you insert any removable media and takes a few seconds to complete. After the removable media has been scanned, it is not scanned until it is reinserted or formatted. If you still suspect your removable media is infected, turn on Auto-Protect, insert the removable media, and open it in Windows Explorer for Auto-Protect to rescan it. You can also scan the removable media manually.

#### Customize Automatic Protection settings

- 1 Start Norton.
  - If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 Under **Removable Media Scan**, set the slider to **On**.

### Set SONAR to remove threats automatically

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

### Set SONAR to remove threats automatically

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 Under **Remove Risks Automatically**, set the slider to **Always**.
- 5 Under **Remove Risks if I Am Away**, set the slider to **Always**.
- 6 Click **Apply**.

### Set Auto-Protect to exclude known good files from Norton scans

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

#### Exclude files from Norton scans

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 In the Antivirus settings window, click the **Scans and Risks** tab.
- 5 Under **Exclusions / Low Risks**, do one of the following:
  - In the **Items to Exclude from Scans** row, click **Configure**.
  - In the **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection** row, click **Configure**.
- 6 In the window that appears, click **Add Folders** or **Add Files**.
- 7 In the **Add Item** dialog box, click the browse icon. In the dialog box that appears, select the item that you want to exclude from scans.
- 8 Click **OK**.

## View real-time threats that Norton SONAR protection detects

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks. SONAR identifies emerging threats based on the behavior of applications, which is quicker than the traditional

signature-based threat detection. It helps protect you against malicious code even before virus definitions are available through LiveUpdate.

You should keep SONAR Protection turned on at all times.

---

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

---

#### Make sure that SONAR Protection is on

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 On the **Automatic Protection** tab, under **Real Time Protection**, move the **SONAR Protection** switch, make sure that the switch is to **Off** or **On**.  
If you turn the switch off, even for a short duration, real-time protection features are disabled, and your computer may be vulnerable.
- 5 Click **Apply**.
- 6 If you turned the switch off, select how long you want SONAR to be disabled, and click **OK**.
- 7 In the **Settings** window, click **Close**.

#### View risks detected by SONAR

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In the **Security History** window, in the drop-down list, select **SONAR Activity**.
- 4 Select a risk in the list if there are risks displayed.
- 5 Follow the **Recommended Action** in the **Details** pane.

This category also lists any activity that modifies the configuration or the settings of your computer. The **More Details** option of this category provides details about the resources that the activity affects.

# Exclude files and folders from Norton Auto-Protect, SONAR, and Download Intelligence scans

You can configure Norton to exclude certain programs from the Auto-Protect scans and SONAR scans. You can use **Scan Exclusions** window and **Real Time Exclusions** window to exclude viruses and other high-risk security threats from scanning. When you add a file or folder to the exclusions list, Norton ignores the file or folder when it scans for security risks.

To exclude a file from Download Intelligence, you must select a folder and download the file to the selected folder. For example, when you download an unsafe executable file to this folder, Norton lets you download the file and does not remove it from your computer. You must create a new folder specific for Download Intelligence exclusions.

---

**Note:** Excluding a file from the Norton scans reduce the level of protection of your computer and should be used only if you have a specific need. You should only exclude items if you are confident that they are not infected.

---

## Exclude high-risk security threats from scanning

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 In the **Antivirus** settings window, click the **Scans and Risks** tab.
- 5 Under **Exclusions / Low Risks**, do one of the following:
  - In the **Items to Exclude from Scans** row, click **Configure**.
  - In the **Items to Exclude from Auto-Protect, Script Control, SONAR and Download Intelligence Detection** row, click **Configure**.
- 6 In the window that appears, click **Add Folders** or **Add Files**.  
You can assign exclusions to local drives, folders, groups of files, single files, or network drives. However, Norton does not support exclusions for files on a network. If you add a network drive to the exclusion list, make sure that the drive is connected to your computer.
- 7 In the **Add Item** dialog box, click the browse icon.
- 8 In the dialog box that appears, select the item that you want to exclude from the scan.  
When you add folders, you can specify whether to include or exclude subfolders.
- 9 Click **OK**.

- 10 In the **Add Item** dialog box, click **OK**.
- 11 In the window that appears, click **Apply**, and then click **OK**.

## Exclude files with low-risk signatures from Norton scans

Norton Signature Exclusions let you select specific known security risks to exclude from Norton scans. For example, if a legitimate app, like a free game, relies on another program, like adware, to function, you might decide to keep the adware, even if it exposes you to risk. You might also decide not to be notified about the program in future scans.

---

**Note:** Exclusions reduce your protection and should be used only if you have a specific need and fully understand the potential risk of excluding known threats from Norton scans.

---

### Add a low-risk signature to the Signature Exclusions

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

## Clear file IDs excluded during scans

When you run a scan, Norton excludes the files that are added to Scan Exclusions. If you want Norton to scan all the files on your computer, you have to clear the file IDs.

### Clear IDs of the files that are excluded during scans

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.

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

## Turn on or turn off automatic tasks

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

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

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

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

### Turn on or turn off automatic tasks

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Tasks Scheduling**.
- 4 In the **Task Scheduling** window, on the **Automatic Tasks** tab, do the following:
  - Check the feature that you want to run automatically.  
Check the **Tasks** check box to check all the features at once.
  - Uncheck the feature that you do not want to run automatically.  
Uncheck the **Tasks** check box to uncheck all the features at once.
- 5 Click **Apply**, and then click **Close**.

## Run custom tasks

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

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

### Run custom tasks

**1** Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

**2** In the Norton main window, double-click **Security**, and then click **Scans**.

**3** In the **Scans** window, under **Scans and Tasks**, click **Custom Task**, and then click **Go**.

**4** In the **Custom Tasks** window, check the tasks that you want to run.

To select all the tasks, check **Tasks**.

**5** Click **Go**.

## Schedule security and performance scans

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

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

### **Automatic (Recommended)**

Examine your PC for security and performance issues whenever your PC is idle.

This setting provides the maximum protection.

### **Weekly**

Examine your PC one or more times each week for security and performance issues.

You can pick the days of the week and the time of day on which the scan performs.

### **Monthly**

Examine your PC once each month for security and performance issues.

You can pick the day of the month and the time of day on which the scan performs.

**Manual Schedule**

Do not perform a scheduled security or performance scan of your PC.

If you choose this option, you should perform manual security and performance scans of your PC periodically to maintain protection.

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

**Schedule security and performance scans**

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

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

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

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

## Configure Data Protector to block malicious processes affecting your PC

Data Protector protects your PC from malicious processes that intend to destabilize your PC, corrupt and/or steal your data, and propagate the malicious nature to other good processes. It uses Norton reputation technology to identify a process as safe, malicious, or unknown. Based on the identification, it blocks malicious processes from performing any action on your PC. It is more aggressive in protecting your files that even safe processes are blocked if a malicious file is injected into it during runtime. By default, Data Protector is turned on and protects preset folders and extensions. Depending on your situation, you can add more folders and/or extensions and can also exclude processes for scanning and protection.

---

**Warning:** Turning off this feature reduces your PC protection. So, we recommend you to keep this feature turned on always. However, if you wish to turn it off, do that temporarily and ensure that it is turned on again.

---



### Turn off or turn on Data Protector

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings > Antivirus**.
- 3 In the **Antivirus** window, click the **Data Protector** tab.
- 4 In the **Data Protector** row, move the **On/Off** switch to **On** or **Off**.
- 5 In the **Show Notifications** row, do one of the following:
  - Move the switch to **On** to notify you every time Data Protector blocks a threat.
  - Move the switch to **Off** to suppress notifications. However, you can see the details of blocked threats in the **Security History** window.  
To access the **Security History** window, in the Norton main window, double-click **Security** and then click **History > Data Protector**.
- 6 Click **Apply**.
- 7 If prompted, select the duration until when you want the Data Protector feature to be turned off, and click **OK**.

### Add or edit a folder for Data Protector protection

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings > Antivirus**.
- 3 In the **Antivirus** window, click the **Data Protector** tab.
- 4 In the **Data Protector** row, move the **On/Off** switch to **On**.
- 5 To add or edit a folder, do the following:
  - Next to **Protected Folders**, click **Configure**.
  - In the **Protected Folders** window, do the following:
    - To include a new item, click **Add**.
    - To change an existing item, choose the item and then click **Edit** to modify it.

---

**Note:** You cannot edit a preset folder.

---

- In the **Add Item** or **Edit Item** window, click



to browse and select the folder.

- Click the check box to include the subfolders.
- Click **OK**.

6 Click **Apply** and then click **OK**.

#### Add an extension for Data Protector protection

1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

2 In the Norton product main window, click **Settings > Antivirus**.

3 In the **Antivirus** window, click the **Data Protector** tab.

4 In the **Data Protector** row, move the **On/Off** switch to **On**.

5 To add an extension, do the following:

- Next to **Protected File Types**, click **Configure**.
- In the **Protected File Types** window, click **Add**.
- In the **Add Item** window, type the extension that you want to protect. For example, if you want to protect executable files, type .exe in the box. All files with the .exe extension, anywhere on the PC, are protected.
- Click **OK**.

6 Click **Apply** and then click **OK**.

#### Remove a folder or an extension from Data Protector

1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

2 In the Norton product main window, click **Settings > Antivirus**.

3 In the **Antivirus** window, click the **Data Protector** tab.

4 In the **Data Protector** row, move the **On/Off** switch to **On**.

5 Next to **Protected Folders** or **Protected File Types**, click **Configure**.

6 On the **Protected Folders** or **Protected File Types** window, choose the item that you want to remove.

---

**Note:** You cannot remove a preset folder or extension.

---

7 Click **Remove**.

8 Click **Apply** and then click **OK**.

### Add or remove a process from Data Protector exclusion

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings > Antivirus**.
- 3 In the **Antivirus** window, click the **Data Protector** tab.
- 4 In the **Data Protector** row, move the **On/Off** switch to **On**.
- 5 On the **Process Exclusion** row, click **Configure** and do the following:
  - To add a process for Data Protector exclusion, click **Add** and then choose the process.
  - To remove a process from Data Protector exclusion, click the process and then click **Remove**.
- 6 Click **Apply** and then click **OK**.

## Set Norton to remove scripts that can be exploited in phishing attempts

Script Control helps protect you from malware that you download or receive as attachments in phishing emails. It removes suspicious scripts from files and sanitizes the files, by default\*\*. However, you can restore the original files with the script, and configure how you want Norton to handle documents with embedded scripts.

---

**Note:** \*\*For Chrome, Edge, and Internet Explorer browsers, this feature is supported from Windows 10 RS2 and later versions.

---

Scripts are used to make documents dynamic and interactive. Although the primary objective of scripts is to improve the document experience, cybercriminals can use them to sneak malware on your computer. Scripts are generally not important to the function of a document and many software programs disable them by default.

You can set Norton to exclude specific files from Script Control if you are confident that they do not contain malicious content. For more information, See [“Exclude files and folders from Norton Auto-Protect, SONAR, and Download Intelligence scans”](#) on page 36. You can restore the original files by replacing the sanitized files. You should exclude files only if you are confident that they do not have any malicious content.

Script Control identifies potential threats based on the behavior of files. If Norton detects any potentially dangerous activity when you open a document with embedded script, it blocks the application from running the script. You can configure how you want Norton to handle the scripts when you open documents with embedded scripts.

## Restore the original file

- 1 Start Norton.  
If you see the **My Norton** window, in the **Device Security** row, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In the **Security History** window, from the **Show** drop-down list, select **Script Control**.
- 4 In the **Script Control** view, select the item that you want to restore.
- 5 On the right pane, under **Details**, click **Restore**.
- 6 In the **Script Control Restore** window, click **Yes**.
- 7 In the prompt that appears, select **Yes**.
- 8 In the **Security History** window, click **Close**.

## Turn on or turn off Script Control

- 1 Start Norton.  
If you see the **My Norton** window, in the **Device Security** row, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 In the **Antivirus** settings window, click the **Script Control** tab.
- 5 In the **Remove scripts when downloading documents** row, move the **On/Off** switch to **On** or **Off**.

If you turn off, do the following:

- In the **Security Request** window, in the **Select the duration** drop-down list, select the amount of time that you want to turn off the option.
- 6 In the **Block scripts when opening documents** row, move the **On/Off** switch to **On** or **Off**.

If you turn off, do the following:

- In the **Security Request** window, in the **Select the duration** drop-down list, select the amount of time that you want to turn off the option.
- 7 In the **Settings** window, click **Apply**, and then click **Close**.

## Permanently delete all the Script Control items

- 1 Start Norton.  
If you see the **My Norton** window, in the **Device Security** row, click **Open**.
- 2 In the Norton main window, click **Settings**.

- 3 In the **Security History** window, from the **Show** drop-down list, select **Script Control**.
- 4 In the **Script Control** view, click **Clear Entries**.
- 5 In the **Clear Entries** window, click **Yes**.
- 6 In the confirmation dialog box, click **Yes**.
- 7 In the **Security History** window, click **Close**.

## Configure how Norton should handle documents with embedded script

- 1 Start Norton.  
If you see the **My Norton** window, in the **Device Security** row, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Antivirus**.
- 4 In the **Antivirus** settings window, click the **Script Control** tab.
- 5 Under **Block scripts when opening documents**, in the **Microsoft Office** row, click **Configure**.
- 6 In the **Microsoft Office Preferences** window, under **Actions**, select the action you want Norton to perform for each application.  
Your options are:
  - **Block**
  - **Allow**
  - **Ask Me**You can choose a different action for each application.
- 7 In the confirmation window that appears, click **OK**.
- 8 In the **Microsoft Office Preferences** window, click **Apply** and then click **OK**.
- 9 In the **Adobe Document** row, select the action you want Norton to perform for Adobe documents.
- 10 In the **Settings** window, click **Apply**, and then click **Close**.

## FAQs: Norton Script Control

### What are scripts and why does Norton remove them?

Scripts are used to make documents dynamic and interactive. They can also add functionality by automating certain tasks.

Scripts can include:

- ActiveX controls
- Add-ins
- Data connections
- Macros
- Linked object linking and embedded OLE files
- Color-theme files

Although the primary objective of scripts is to improve the document experience, cybercriminals can use them in phishing attempts to sneak malware on your computer. Scripts are generally not important to the function of a document and many software programs disable them by default.

### Can removing scripts cause problems?

It depends. If a document relies on scripts to provide interactivity or to download additional content, then that functionality will not work if the script is removed.

### Am I still protected even if I turn off Script Control?

Norton detects when malware attempts to execute in a document, including malware embedded by scripts, so you would be protected. Script Control provides an extra layer of security by removing scripts and sanitizing documents.

### How do I get back the original file?

- 1 Start Norton.  
If you see the **My Norton** window, in the **Device Security** row, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In the **Security History** window, from the **Show** drop-down list, select **Script Control**.
- 4 In the **Script Control** view, select the active content item that you want to restore.
- 5 On the right pane, under **Details**, click **Restore**.
- 6 In the **Script Control Restore** window, click **Yes**.
- 7 In the prompt that appears, select **Yes**.
- 8 In the **Security History** window, click **Close**.

### What applications does Norton block if it detects potential threat?

Norton blocks the following applications from opening if it detects any potentially dangerous activity:

- Microsoft Excel

- Microsoft PowerPoint
- Microsoft Word

In addition to these applications, Norton detects and blocks scripts from Adobe documents, common developer utilities, Windows Management Instrumentation (WMI) tools, command-line interfaces, and scripting interfaces.

### **Blocking scripts when downloading documents vs. opening documents: what's the difference?**

When you download a document with embedded script, Script Control uses **Auto-Protect** to detect suspicious scripts. **Auto-Protect** uses the threat signatures that Norton receives during virus definition updates and other security updates to determine the safety of any file that you download.

When you open a document with embedded script, Script Control uses **SONAR Protection** to detect any potentially dangerous activity. It identifies potential threats based on the behavior of files and blocks the application from running the script.

---

**Note:** For Chrome, Edge, and Internet Explorer browsers, the **Remove scripts when downloading documents** option is available only from Windows 10 RS2 and later versions.

---

Norton recommends that you keep both the Script Control options always turned on.

# Keep secure on the Internet

This chapter includes the following topics:

- [Turn on Browser Protection](#)
- [Intrusion Prevention exclusion list](#)
- [Set Norton to monitor applications and block malicious websites from accessing your computer](#)
- [Turn off or turn on AutoBlock](#)
- [Unblock AutoBlocked computers](#)
- [Add a device to Device Trust](#)
- [Turn off or turn on Download Intelligence](#)
- [Turn off or turn on spam filtering](#)
- [Define the Internet usage for Norton](#)
- [Turn off or turn on Network Cost Awareness](#)
- [Wi-Fi Security](#)
- [Protect your banking information using Norton Safe Web](#)

## Turn on Browser Protection

Malicious websites detect and exploit browser vulnerabilities to download malware. When you turn on Browser Protection, Norton blocks malware before it can attack. It helps protect your sensitive information and prevents attackers from accessing your computer.

By default, Browser Protection is turned on. Keep Browser Protection turned on to ensure protection against malicious websites.



---

**Note:** The Browser Protection feature is available for Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Microsoft Edge browsers.

---

## How do I turn on Browser Protection?

To protect your browser from malicious websites, the Browser Protection feature is turned on by default. However, if you had turned it off for any reason, you can turn it back on.

### Turn on Browser Protection

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the Settings window, click **Firewall** or **Network**.
- 4 Click the **Intrusion and Browser Protection** tab.
- 5 In the Browser Protection row, move the **On/Off** switch to **On**.
- 6 Click **Apply**.
- 7 In the **Settings** window, click **Close**.

## Intrusion Prevention exclusion list

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. You can configure the trust level of a device using the Device Trust under Network Settings. You can exclude these trusted devices from Intrusion Prevention scan. Excluding Full Trust devices from the Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a device that is set to Full Trust, your Norton product does not scan any information that is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

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

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

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

## How do I remove all devices from Intrusion Prevention exclusion list?

Remove all the devices from the Intrusion Prevention exclusion list

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the Settings window, click **Firewall**.
- 4 Click the **Intrusion and Browser Protection** tab.
- 5 Under Intrusion Prevention, in the Exclusion List row, click **Purge**.
- 6 In the confirmation dialog box, click **Yes**.
- 7 In the Settings window, click **Close**.

## Set Norton to monitor applications and block malicious websites from accessing your computer

A few malicious websites may attempt to gain unauthorized access to your device information when you install and open any freeware or shareware applications. Malicious websites detect and exploit vulnerabilities to download malware such as **crypto mining** malware that can expose your device information to cybercriminals.

With **App URL Monitoring** turned on, Norton monitors all applications that are installed on your computer and block the malicious websites from accessing your computer. Norton alerts you when it blocks a malicious website and you can view the information about the attack using the Security History window.

---

**Note:** **App URL Monitoring** does not monitor the browser applications. To protect your browser application from malicious websites, you need to add Norton browser extensions.

---

### Turn on App URL Monitoring to block malicious websites

By default, **App URL Monitoring** is turned on. Keep App URL Monitoring turned on to ensure protection against malicious websites.

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the Settings window, click **Firewall** or **Network**.

- 4 Click the **Intrusion and Browser Protection** tab.
- 5 Under **Intrusion Prevention**, in the **App URL Monitoring** row, move the On/Off switch to On.

## Exclude a URL or domain from monitoring

Intrusion Prevention uses an extensive list of attack signatures to detect and block suspicious websites. In some cases, benign websites may be identified as suspicious, because it has a similar attack signature. If you receive notifications about a possible attack, and you know that the website or domain that triggers the notification is safe, you can exclude the signature from monitoring.

### Exclude a URL or domain from the alert notification

- 1 On the alert notification, click **View Details**.
- 2 In the **Security History - Advanced Details** window, click **Unblock URL**.

### Exclude a URL or domain using your Norton

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall** or **Network**.
- 4 Click the **Intrusion and Browser Protection** tab.
- 5 Under **Intrusion Prevention**, in the **App URL Monitoring Exclusions** row, click **Configure**.
- 6 Click the **Add** button and enter the URL or the domain name that you want to exclude from monitoring.
- 7 If you want to edit or remove a URL or domain, do the following:
  - Select a URL or domain from the list and click the **Edit** button. Modify the URL or the domain name.
  - Select a URL or domain that you want to remove and click the **Remove** button.

## View information about the blocked URL

### View information in the alert notification

- 1 On the alert notification, click **View Details**.
- 2 In the **Security History - Advanced Details** window, you can view more details about the blocked URL.

### View information using the Security History window

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, double-click **Security**, and then click **History**.
- 3 In **Security History** window, in the **Show** drop-down list, select **Intrusion Prevention** from the list.
- 4 Click a row to view the details for that item.
- 5 Double-click a row, or click **More Options**, to open the Security History Advanced Details to view more details about the activity and take an action on an activity if required.

## Turn off or turn on AutoBlock

Norton AutoBlock stops all traffic between a device in your network and any other computer that attempts to exploit that device. Since this includes traffic that may not be malicious, AutoBlock only stops the connection for a limited time after it detects a threat. You can specify the period for which you want your Norton product to block the connections from attacking computers. By default, your Norton product blocks all traffic between your computer and the attacking computer for a period of 30 minutes.

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

### Turn off or turn on AutoBlock

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall** or **Network**.
- 4 Click the **Intrusion and Browser Protection** tab.
- 5 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
- 6 In the **Intrusion AutoBlock** window, under **AutoBlock**, do one of the following:
  - To turn off Intrusion AutoBlock, click **Off**.
  - To turn on Intrusion AutoBlock, click **On (Recommended)**, and then in the **AutoBlock attacking computers for** drop-down list, select how long you want to turn on AutoBlock.
- 7 In the **Intrusion AutoBlock** window, click **OK**.
- 8 In the **Settings** window, click **Close**.

# Unblock AutoBlocked computers

If Norton Firewall stops network traffic to a computer that you know is safe, you can restore connections to the computer by removing it from the AutoBlock list in Norton Firewall settings.

## Unblock an AutoBlocked computer

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall** or **Network**.
- 4 Click the **Intrusion and Browser Protection** tab.
- 5 Under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
- 6 In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, select the IP address of the computer.
- 7 Under the **Action** column, select **Unblock** from the drop-down list.
- 8 In the Intrusion AutoBlock window, click **OK**.
- 9 In the **Settings** window, click **Close**.

# Add a device to Device Trust

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

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

---

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

---

## Add a device to Device Trust

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall**.
- 4 On the **General Settings** tab, in the **Device Trust** row, click **Configure**.
- 5 In the **Device Trust** window, click **Add**.

- 6 In the **Add Device** window, in the **Name** box, type the name of the device that you want to add to your network.

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

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

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

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

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

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

<b>Full Trust</b>	Adds a device to the Full Trust list.  Full Trust devices are monitored only for known attacks and infections. You should select this setting only when you are sure that the device is completely safe.
<b>Restricted</b>	Adds a device to the Restricted list.  Restricted devices do not have access to your computer.

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

## Turn off or turn on Download Intelligence

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

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

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

#### Turn off or turn on Download Intelligence

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

## Turn off or turn on spam filtering

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

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

---

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

---

#### Turn off or turn on spam filtering

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **AntiSpam**.
- 4 On the **Filter** tab, in the **AntiSpam** row, move the **On/Off** switch to **Off** or **On**.
- 5 If you turn spam filtering off, do the following:

- In the **Security Request** window, in the **Select the duration** drop-down list, select the amount of time that you want to turn off spam filtering.
- 6 Click **Apply**.
  - 7 Click **OK**.
  - 8 In the **Settings** window, click **Close**.

## Define the Internet usage for Norton

**Network Cost Awareness** lets you control the bandwidth that Norton uses. By default, Network Cost Awareness is turned on and set to Auto. In Windows 7 or earlier, the default setting is **No Limit**. If you have a slow Internet connection, you can reduce the bandwidth that Norton uses. You can also set communication policies for all network connections that your computer uses by changing Network Cost Awareness settings.

### Define the Internet usage for Norton

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

---

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

---

- **No Limit** Allows Norton to use the required network bandwidth to receive all product and virus definition updates. If you use Windows 7 or earlier, the default policy is **No Limit**.
- **Economy** Allows Norton to access the Internet only to receive critical product updates and virus definitions. If you have a limited Internet connection, **Economy** ensures you are protected from critical security threats.



- **No Traffic** Blocks Norton from connecting to the Internet. If you choose this policy, Norton cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.
- 7 Click **Apply**, and then click **OK**.
  - 8 In the **Settings** window, click **Close**.

## Turn off or turn on Network Cost Awareness

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

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

### Turn off or turn on Network Cost Awareness

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall**.  
If you have Norton AntiVirus, click **Network**.
- 4 On the **General Settings** tab, in the **Network Cost Awareness** row, move the **On/Off** switch to **Off** or **On**.
- 5 In the **Settings** window, click **Apply**, and then click **Close**.

## Wi-Fi Security

Wi-Fi Security feature protects you from MITM attacks, SSL strip attacks, content tampering attacks, ARP spoofing attacks, and DNS spoofing attacks.

Public Wi-Fi connections are vulnerable to man-in-the-middle (MITM) attacks. MITM attack is a setup where an attacker places himself between you and the Wi-Fi provider. You might think that you are connected to your trusted Wi-Fi provider but you would be connecting to a malicious tool which is recording all your keystrokes and passwords.

What if Norton identifies a network you trust as an MITM attack.

If you think Norton identifies a known trusted network as an MITM attack, you can add the network to trusted networks list. Norton notifies you when it identifies MITM attack like behavior. If you click Trust in the alert, you will not get a notification the next time you access the network.

If you accidentally clicked Disconnect, you can add it back to trusted networks using Security History. To trust a network Norton blocked earlier.

#### To trust a network Norton blocked earlier

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **History**.
- 3 In **Security History** window, in the drop-down list, select **Wi-Fi Security**.
- 4 Select the specific activity and click **More Options**.
- 5 In the **Security History – Advanced Details** window, click **Trust This Network**.

## Protect your banking information using Norton Safe Web

Banking Protection in Norton Safe Web provides increased security when you transact with banking websites. When you access a banking website using Google Chrome, Mozilla Firefox, or Microsoft Edge browser, you receive a notification to install or enable the Norton Safe Web extension. Click **Install** or **Enable** in the notification and follow the on-screen instructions to install or enable the Norton Safe Web extension.

You can turn off the Banking Protection Notification alert by clicking **Don't Show Me Again** in the notification or by going to the **Settings** window.

#### Turn off or turn on Banking Protection Notifications

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **Firewall**.
- 4 Under the **Intrusion and Browser Protection** tab, in the **Banking Protection Notifications** row, move the **On/Off** slider to **Off** or **On**.
- 5 In the **Settings** window, click **Apply**, and then click **Close**.

# Secure your sensitive data

This chapter includes the following topics:

- [Add the Norton browser extensions](#)
- [Turn off or turn on Norton Safe Web](#)
- [Search the web using Norton Safe Search](#)
- [Scam Insight](#)
- [Antiphishing](#)
- [Access Norton Password Manager](#)
- [Turn on or turn off Norton Password Manager](#)
- [Create Norton Password Manager cloud vault](#)
- [Delete your Norton Password Manager cloud vault](#)
- [Export your Norton Password Manager data](#)
- [Import your Norton Password Manager data](#)
- [Enable or disable the Norton Security toolbar](#)

## Add the Norton browser extensions

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

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

Norton Safe Web	<p>A secure search experience that helps you to surf, search, and shop safely online. It analyzes websites that you visit and detects if there are any viruses, spyware, malware, or other threats.</p> <p>See <a href="#">“Turn off or turn on Norton Safe Web”</a> on page 63.</p>
Norton Safe Search	<p>A secured search engine that generates search results and ranks them based on the site safety status and Norton rating.</p>
Norton Home Page	<p>A webpage that uses the Norton Safe Search feature to enhance your web search experience. It provides the site safety status and Norton rating for each of the search result generated.</p>
Norton Password Manager	<p>A secure online location where you can store all of your sensitive information such as logins, personal information, and financial information. You can use this information to log in to websites, automatically fill online forms, and online payments.</p>

## Internet Explorer

### Add Norton browser extension in Internet Explorer

- 1 After you install Norton for the first time, the **Browser Protection** page automatically opens in a new window on launching a new Internet Explorer session.
- 2 In the **Browser Protection** page, click the **Enable** option of **Norton Security Toolbar**.
- 3 In the extensions pop-up that appears, click **Add Extension**.
- 4 After you have enable Norton Security toolbar, you can enable Norton Safe Search, Norton Home Page and Norton Password Manager extensions for your browser.

You can use the **Click to Add** option and follow the on-screen instructions to enable these features.

- 5 If you have not installed any one of the extensions, the **Internet Explorer Protection Alert** notification appears when you launch Internet Explorer after a week.

Click **Install Now** and follow the on-screen instructions to install the extensions.

---

**Note:** If you want to enable the Norton extension at a later time, click **Remind Me Later**. If you do not want the notification alert to appear, click **Don't ask me again**.

---

---

**Note:** You must have the latest version of Norton to install the browser extensions of Internet Explorer.

---

## Google Chrome

### Add Norton browser extensions in Google Chrome

Norton offers the following extensions for Google Chrome browser:

- Norton Safe Web
- Norton Password Manager
- Norton Safe Search
- Norton Home Page

You can install the browser extensions for Google Chrome by following the below instructions.

- 1 After you install Norton for the first time, the **Browser Protection** page automatically opens in a new window on launching a new Google Chrome session.  
  
You can also launch the **Browser Protection** page by clicking the **Set Up Now** option in the **Internet Security** pillar.
- 2 In the **Browser Protection** page, click the **Click to Add** option of **Norton Safe Web**.
- 3 In the extensions pop-up that appears, click **Add Extension**.
- 4 After you enable Norton Safe Web, you can enable Norton Safe Search, Norton Home Page and Norton Password Manager extensions for your browser. You can use the **Click to Add** option and follow the on-screen instructions to enable these extensions.  
  
To enable all the Norton extensions in Google Chrome, click **Add All Norton Extensions for Free** and follow the on-screen instructions.
  - If you have not installed the Norton Safe Web extension, the **Chrome Protection Removed** alert notification appears when you launch Google Chrome after a week.
  - If you have not installed any one of the extensions, the **Google Chrome Protection Alert** notification appears when you launch Google Chrome after a week.
- 5 Click **Install Now** and follow the on-screen instructions to install the extensions.

---

**Note:** If you want to enable the Norton extension at a later time, click **Remind Me Later**. Click **Do not ask me again** if you do not want the notification alert to appear.

---

---

**Note:** You must have the latest version of Norton to install the browser extensions of Internet Explorer.

---

## Mozilla Firefox

### Add Norton browser features in Mozilla Firefox

Norton offers the following extensions for Mozilla Firefox browser:

- Norton Safe Web
- Norton Safe Search
- Norton Home Page
- Norton Password Manager

You can install or upgrade the browser extensions for Mozilla Firefox by following the below instructions.

- 1 After you install Norton for the first time, the **Browser Protection** page automatically opens in a new window/tab on launching a new Mozilla Firefox session.

If you have upgraded Norton, click **OK** on the **Browser Protection** alert window to display the extensions page.

---

**Note:** You can also launch the **Browser Protection** page by clicking the **Set Up Now** option in the **Internet Security** pillar.

---

- 2 In the **Browser Protection** page, click the **Enable** option of **Norton Safe Web**.
- 3 In the extensions pop-up that appears, click **Allow**.

After you enable Norton Safe Web, you can enable Norton Safe Search, Norton Home Page and Norton Password Manager features for your browser. You can use the **Enable** option and follow the on-screen instructions to enable these features.

To enable all the Norton extensions in Firefox, click **Add All Norton Extensions for Free** and follow the on-screen instructions.

If you have not installed the extensions, the **Firefox Protection Alert** notification alert appears when you launch Firefox after a week. If you want to enable the Norton extension at a later time, click **Remind Me Later**. If you do not want the notification alert to appear, click **Do not ask me again**. If you choose **Remind Me Later**, Firefox displays a Protection Alert notification after a week. You can click the **Install Now** option in the notification and follow the on-screen instructions to install the extensions.

---

**Note:** You must have the latest version of Norton to install the browser extensions of Internet Explorer.

---

## Turn off or turn on Norton Safe Web

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

### Turn off or turn on Norton Safe Web from extensions page in Google Chrome

- 1 Start Google Chrome.
- 2 On the top-right corner, click **Settings**.
- 3 In the **Settings** option, navigate to **More Tools** and click **Extensions**.
- 4 In the **Extensions** page, if Norton Safe Web is enabled, uncheck the **Enabled** box.  
If Norton Safe Web is disabled, check the **Enabled** box.
- 5 Restart Google Chrome.

### Turn off or turn on Norton Safe Web from Add-ons page in Mozilla Firefox

- 1 Start Mozilla Firefox.
- 2 On the Firefox menu, click **Add-ons**.
- 3 On the **Extensions** tab, click **Enable**.  
If Norton Safe Web is not grayed out, click **Disable**.
- 4 Restart Mozilla Firefox.

### Turn off or turn on Norton Safe Web from Extensions page in Safari

- 1 Start Safari.
- 2 On the **Safari** menu, click **Safari**, and then click **Preferences**.
- 3 Click **Extensions**.
- 4 On the left pane, if Norton Safe Search is enabled, uncheck the **Enabled** box.  
If Norton Safe Search is disabled, check the **Enabled** box.

### Turn off or turn on Norton Safe Web from Extensions page in Microsoft Edge

- 1 Start Microsoft Edge.
- 2 On the top-right corner, click **More**



and select **Extensions**.

- 3 In the **Extensions** window, click **Get extensions from the store**.
- 4 In the **Store** window, type Norton in the Search box.
- 5 In the results, click **Norton Safe Web** and click **Install**.
- 6 After the extension is installed, click **Launch**.
- 7 In the **You have a new extension** pop-up window, click **Turn it on**.

If you miss the pop-up window, on the top-right corner of Microsoft Edge, click **More**



, and select **Extensions**.

- 8 In the **Norton Safe Web** window, under **Norton Safe Web**, move the slider to **On**.  
To turn off the Norton Safe Web extension, move the slider to **Off**.

## Search the web using Norton Safe Search

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

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

---

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

---

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



---

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

---

### Search the web using Norton Safe Search

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

### Enable Norton Safe Search Box on Toolbar

---

**Note:** This feature is available only for Internet Explorer.

---

When you install Norton, it adds the Norton Security toolbar to Internet Explorer. When you open Internet Explorer, you are prompted to enable the **Norton Safe Search** box on your toolbar.

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

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

To disable the Norton Safe Search box, do the following:

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

## Scam Insight

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

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

## Antiphishing

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

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

## Access Norton Password Manager

You can access Password Manager from the following areas:

- From the **Internet Security** section in the product main window on Windows
- From the Norton Password Manager extension
- From the Norton Password Manager app on Android and iOS

You can use the **Logins** and **Cards** options in the **Web Protection** pane to access **Manage Logins** window and **Manage Cards** window respectively.

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

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

---

**Note:** You must be signed in to Password Manager to access the Password Manager features. The Password Manager features are supported in Internet Explorer, Firefox, Safari, and Chrome browsers.

---

### Download and install the Norton Password Manager app on Android or iOS

- 1 Do one of the following:

- On Android, go to **Play Store**. If you open Play Store for the first time, the Terms of Service screen appears. Tap **Accept** to continue.
  - On iOS, tap the **App Store** icon on your home screen.
- 2 Search and select Norton Password Manager app.
  - 3 Do one of the following:
    - On Android, on the application details screen, tap **Install**, and tap **Accept & download**.
    - On iOS, tap **Free** and then tap **INSTALL APP**. In the **Apple ID Password** screen, type your Apple account password.

## Turn on or turn off Norton Password Manager

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

You can turn off or turn on the Password Manager from the Extensions page in Google Chrome or from the Add-ons page in Mozilla Firefox.

### Turn on Password Manager from Extensions page in Google Chrome

- 1 Start Google Chrome.
- 2 On the top-right corner, click **Settings**.
- 3 In the **Settings** option, navigate to **More tools** and click **Extensions**.
- 4 In the **Extensions** page, if **Norton Password Manager** is disabled, check the **Enabled** box.
- 5 Restart Google Chrome

### Turn on Password Manager from Add-ons page in Mozilla Firefox

- 1 Start Mozilla Firefox.
- 2 On the **Firefox** menu, click **Add-ons**.
- 3 On the **Extensions** tab, click **Norton Password Manager**.
- 4 If **Norton Password Manager** is not grayed out, click **Enable**.
- 5 Restart Mozilla Firefox.

### Turn on Norton Password Manager from Extensions page in Safari

- 1 Start Safari.
- 2 On the **Safari** menu, click **Safari**, and then click **Preferences**.

- 3 Click **Extensions**.
- 4 On the left pane, if Norton Password Manager is disabled, check the **Enabled** box.

#### Turn off Password Manager from Extensions page in Google Chrome

- 1 Start Google Chrome.
- 2 On the top-right corner, click **Settings**.
- 3 In the **Settings** option, navigate to **More tools** and click **Extensions**.
- 4 In the **Extensions** page, if **Norton Password Manager** is enabled, uncheck the **Enabled** box.
- 5 Restart Google Chrome

#### Turn off Password Manager from Add-ons page in Mozilla Firefox

- 1 Start Mozilla Firefox.
- 2 On the **Firefox** menu, click **Add-ons**.
- 3 On the **Extensions** tab, click **Norton Password Manager**.
- 4 If **Norton Password Manager** is grayed out, click **Enable**.
- 5 Restart Mozilla Firefox.

#### Turn off Norton Password Manager from Extensions page in Safari

- 1 Start Safari.
- 2 On the **Safari** menu, click **Safari**, and then click **Preferences**.
- 3 Click **Extensions**.
- 4 On the left pane, if Norton Password Manager is enabled, uncheck the **Enabled** box.

## Create Norton Password Manager cloud vault

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

You can access the Norton Password Manager cloud vault from any computer that is connected to the Internet.

### Create cloud vault from browser

- 1 Open your browser.
- 2 Click **Norton Password Manager** on the top-right corner of the browser.
- 3 In the Norton Password Manager sign in screen, click **Sign In**.
- 4 In the **Welcome to Norton** window that appears, click **Create an Account**.
- 5 In the **Create an Account** tab, fill in the details, and click **Create Account**.
- 6 In the **No Vault detected** window, click **Create Vault**.
- 7 In the **Create your vault** window, type your password, and click **Next**.  
The password must satisfy all the mentioned criteria to be accepted.
- 8 Type in your password again and click **Next**.
- 9 Type in a hint to remind you of the password and click **Create Vault**.
- 10 In the **Setup complete** window, click **Go to vault**.

### Create cloud vault from Norton

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

### Create cloud vault in Android or iOS

- 1 Log on to the **Norton Password Manager** app.
- 2 In the **Sign in** window, type your Norton account email address and password.
- 3 Tap **Sign in** and follow the on-screen instructions.

## Delete your Norton Password Manager cloud vault

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

---

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

---

### Delete your cloud vault from browser

- 1 Open your browser.
- 2 Click **Norton Password Manager** on the top-right corner of the browser.
- 3 In the pop-up that appears, click **Open vault**.
- 4 In the **Unlock your vault** window, type your vault password and click **Open vault**.
- 5 Click the Norton Password Manager extension icon and click **Vault**.
- 6 In the Norton Password Manager window, click the



symbol to launch the **Settings** page.

- 7 Click **Delete Vault**.
- 8 In the Norton sign-in page, enter your login credentials and click **Sign in**.
- 9 In the **Delete vault** page, click **Yes, Delete vault**.

### Delete your cloud vault from Norton

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Internet Security**, and then click **Password Manager**.

- 3 In the **Vault Closed** window, type your password incorrectly for three times.
- 4 Click the **Click here** link next to the **Need to delete your Vault?** option.
- 5 In the **Delete Vault** window, click **Yes, Delete my vault**.
- 6 In the warning dialog box, click **Yes**.
- 7 Type your Norton account password to validate and click **Sign In**.
- 8 In the confirmation window, click **OK**.

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

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

## Export your Norton Password Manager data

You can export your Password Manager data for security purposes, data recovery, or when you transfer your Password Manager data to a new computer. Your vault password cannot be reset. So, Symantec recommends that you back up your vault data periodically. When you enable automatic backup feature, backups of your vault are automatically created and stored locally on your device.

You can retrieve Password Manager data when your product expires.

---

**Note:** Norton Password Manager does not allow the export of Norton Password Manager (.NPM) files.

---

#### Export your Norton Password manager data from browser

- 1 Open your browser.
- 2 Click **Norton Password Manager** on the top-right corner of the browser.
- 3 In the pop-up that appears, click **Open vault**.
- 4 In the **Unlock your vault** window, type your vault password and click **Open vault**.
- 5 Click the Norton Password Manager extension icon and click **Vault**.

- 6 In the Norton Password Manager window, click



and click **Export vault**.

- 7 In the **Protected vault Action** window, enter your vault password to export the Norton Password Manager data.

#### Export your Norton Password Manager data from Norton

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Internet Security**, and then click **Password Manager**.
- 3 In the **Norton Password Manager** window, click the **Settings** icon available at the bottom of the window.
- 4 Click the **Import/Export** tab.
- 5 In the **Export** pane, select the file format.

You can select one of the following:

- **Password Manager Backup Format – DAT File**  
If you want to back up your data with a password for more security, type and confirm the password.
- **Plain Text – CSV file (Logins & Notes only)**

You can access your vault backups at **My Documents\Norton Password Manager Backups\<Norton account name>**.

- 6 Click **Export**.
- 7 In the **Validate Password for Password Manager** window, type your vault password to export your Password Manager data.
- 8 In the confirmation dialog box, click **OK**.

## Import your Norton Password Manager data

You can import your Password Manager data from the file that was previously backed up. Vault auto backup happens only when auto backup feature is enabled. Default location of auto backup folder is C:\Documents\Norton Password Manager.

The Merge imported data with existing data and Replace existing data with imported data options appear when you import Norton Password Manager data from a backup file. You can



merge the imported data with the vault that you are currently signed in or replace the existing data stored in your vault

---

**Note:** When you import, the file size must not be more than 15 MB for .CSV files. Also, Norton Password Manager does not allow the import of Norton Password Manager (.NPM) files.

---

### Import your Norton Password Manager data from Norton

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Internet Security**, and then click **Password Manager**.
- 3 In the **Norton Password Manager** window, click the **Settings** icon available at the bottom of the window.
- 4 Click the **Import/Export** tab.
- 5 In the **Import** row, click **Import**.
- 6 In the **Vault Import** window, select one of the following options:
  - **Merge imported data with existing data**
  - **Replace existing data with imported data**
- 7 Click **Import**.
- 8 Browse to the location of the file that you want to import.  
You can access your vault backups at **My Documents\Norton Password Manager Backups\<Norton account name>**.
- 9 Select the file, and then click **Open**.
- 10 If you have different passwords for the logins that you stored in the currently using vault and the importing vault, Norton displays a confirmation message. Select one of the following:
  - Click **Keep Existing Password** to retain the password that is stored in the cloud vault.
  - Click **Keep Imported Password** to overwrite the password that is stored in the cloud vault with the password stored in the importing vault.
- 11 In the confirmation dialog box, click **OK**.

## Enable or disable the Norton Security toolbar

When the Norton Security toolbar is enabled, Norton Password Manager displays the Norton Safe Web pop-up window and a security ranking for websites that you visit. When the toolbar is disabled, Norton Password Manager does not display the Norton Safe Web pop-up window, but still notifies you about suspicious and fraudulent websites.

### Enable or disable the Norton Security toolbar

- ◆ Open your preferred browser:
  - On Internet Explorer, right-click the menu bar, check or uncheck **Norton Security Toolbar** to enable or disable it, and then follow the on-screen instructions.
  - On Safari, click **View > Customize Toolbar**, and then drag and drop the Norton Security toolbar extensions that you want to enable or disable.

# Keep your PC tuned up

This chapter includes the following topics:

- [Use Norton to optimize and improve computer performance](#)
- [View or change the Norton trust level of files that you use](#)
- [Set Norton to alert you about performance issues](#)
- [Run a Norton Diagnostic Report](#)
- [Set Norton to maximize your PC startup time](#)

## Use Norton to optimize and improve computer performance

We know how frustrating it is when your computer slows down and simple tasks take forever. It is the perception of some users that their computer performance degrades after installing Norton. But the fact is that Norton is streamlined to provide a world-class protection without sacrificing performance.

Norton can also boost your computer speed with performance management and optimization tools that make everyday tasks go more quickly.

### Speed up my computer startup time

Many applications are configured to launch when you start your computer. These include programs that you never use, rarely use, or never knew that you had. The more programs that launch when you start your computer, the longer it takes. **Norton Startup Manager** lets you disable or delay startup programs to get you up and running faster.

### Disable or delay startup items

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Startup Manager**.
- 3 In the **Startup Manager** window, do the following:
  - In the **On/Off** column, uncheck programs that you don't use to prevent them from launching when your computer starts.
  - In the **Delay Start** column, select programs that you want to load only after startup completes.
- 4 Click **Apply**, and then click **Close**.

### Improve the time it takes programs and files to load

The **Optimize Disk** tool rearranges file fragments, which get dispersed over your computer with time. It improves the computer performance so that you work more efficiently.

#### Run Optimize Disk

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Optimize Disk**.
- 3 When it completes, click **Close**.

### Remove temporary files and folders that make my computer run slow

Every time you browse or download files, your computer stores temporary files. Even though you don't need to keep them, they collect over time and can slow you down. The File Cleanup tool removes the clutter to make your computer run faster.

#### Remove temporary files and folders

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **File Cleanup**.
- 3 When it completes, click **Close**.

### Optimize your computer

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

You can run Disk optimization only when disk has more than 15 percent of free space. During the disk optimization process, solid-state drives (SSD) are defragmented only in Windows 8 or later operating systems.

### Optimize your permanent disks

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

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

### Optimize your boot volume

Optimization of your boot volume maximizes the usable free space by rearranging file fragments into adjacent and contiguous clusters. When the drive head of your hard disk accesses all of the file data in one location, the file is read into the memory faster.

#### Optimize your boot volume

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

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

### Improve performance when I play games or watch movies

Ever played a game or watched a movie when your security software started running and your screen froze at the worst moment? You can set the **Full Screen Detection** tool to sense when you're running a program that shouldn't be interrupted. Norton then waits until you're done with the app before running background tasks that keep you protected.

#### Make sure that Full Screen Detection is on

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.

- 4 Under **Silent Mode Settings**, in the **Full Screen Detection** row, move the switch to **On**.
- 5 Click **Apply**, and then click **Close**.

## Stop interruptions when I use my favorite apps

If you think that Norton is slowing down your favorite programs, **Quiet Mode** settings stop Norton from running while you use them. Norton waits until you're done using these programs before starting background tasks that keep you protected.

### Run my favorite programs in Quiet Mode

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 Under **Silent Mode Settings**, in the **User-Specified Programs** row, click **Configure**.
- 5 In the **Quiet Mode Programs** window, click **Add**.
- 6 In the **Add Program** dialog box, navigate to your program.
- 7 Select the file, click **Open**, and then click **OK**.

## Show me programs that consume resources and slow me down

Norton monitors your computer and can alert you if a program or process seems to use an unusual amount of resources. You can shut these programs down to improve performance if you're not using them.

### Identify processes that consume resources

- 1 Start Norton.  
 If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Graphs**.
- 3 In the **Graphs** window, on the left pane, click **Usage**.
- 4 Do one of the following:
  - To view the CPU graph, click the **CPU** tab.

- To view the memory graph, click the **Memory** tab.
- 5 Click at any point on the graph to obtain a list of resource-consuming processes.  
Click the name of a process to obtain additional information about the process in the **File Insight** window.

## View or change the Norton trust level of files that you use

**Norton Insight** whitelists files or apps based on reputation and shows the trust level of your files and the percentage of trusted files on your computer. The higher the percentage of trusted files, the quicker scans run, since Norton excludes trusted files from scans.

**Norton Insight** shows files that have high Norton Community usage and known good and known bad files in the Norton Network. File Insight gives more detail including the file's signature, install date, resource usage, and source. If Norton gives a poor trust rating to a file that you believe is safe, you can, though not recommended, set Norton to trust the file.

### View or change the Norton trust level of files you use

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, select **Norton Insight**, and then click **Go**.
- 4 In the **Norton Insight** window, on the **Trust Level** tab, select an option from the **Show** drop-down list to view a category of files.  
You may need to scroll down to view all the files that are listed in the details area.
- 5 Click any file in the list to see more information, like file signature or install date, or to change the trust level.  
You can also click **Check a Specific File**, then browse to a file.
- 6 In the **File Insight** window:
  - On the **Details** tab, click **Locate** to find where the file is on your computer.  
If Norton does not give the file a Trusted rating, you may see an option to trust the file.
  - On the **Origin** tab, view information about the file source.
  - On the **Activity** tab, select an item from the **Show** drop down to view performance issues including average resource, CPU, or memory usage.
- 7 Click **Close**.

# Set Norton to alert you about performance issues

Norton monitors your system performance. If it detects an increase in system resources used by any program or process, it notifies you with performance alerts.

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

## Set Norton to alert you about performance issues

- 1 Start Norton.

If you see the **My Norton** window, next to **Device Security**, click **Open**.

- 2 In the Norton main window, click **Settings**.

- 3 In the **Settings** window, click **Administrative Settings**.

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

### Off

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

### On

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

### Log Only

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

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

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

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

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



By default, this option is turned off.

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

## Configure resource threshold profile

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

### Configure the resource threshold profile

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 Under **Performance Monitoring**, in the **Resource Threshold Profile for Alerting** row, select one of the options.
- 5 Click **Apply**, and then click **Close**.

## Run a Norton Diagnostic Report

Diagnostic Report gathers information about your computer, including the operating system, programs, and hardware. You can use this report to find and fix the issues. The Diagnostic Report is a real-time report with a timestamp. Norton does not generate this report automatically.

If Norton finds any issues on your computer, you can use the **Fix Now** option to resolve the issues. You can save, email, or print the report when needed for review.

### Run Diagnostic Report

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Security**, and then click **Scans**.
- 3 In the **Scans** window, select **Diagnostic Report**, and then click **Go**.

## Set Norton to maximize your PC startup time

When you start your computer, some programs, called startup items, automatically run and increase the time it takes your computer to start. Norton Startup Manager helps you manage startup items. If you do not want a program to automatically start when you turn on your computer, you can disable the program using Startup Manager.

To reduce the start time of your computer and improve the performance, you can delay the start of some of the programs when you turn on your computer. Norton delays the start of the delayed programs by five minutes. Every subsequent delayed program starts with a further delay of ten seconds.

## Delay startup items

### Delay startup items

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Startup Manager**.
- 3 In the **Startup Manager** window, in the **Delay Start** column, select the program that you want to delay.
- 4 Click **Apply**.
- 5 Click **Close**.

## Run delayed startup items manually

### Run delayed startup items manually

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Startup Manager**.
- 3 In the **Startup Manager** window, click **Run Delayed Items Now**.
- 4 Wait for the program to start, and then in the **Startup Manager** window, click **Close**.

## Disable startup items

### Disable startup items

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Startup Manager**.
- 3 In the **On/Off** column, uncheck a program that you do not want to automatically start when you turn on your computer.

- 4 Click **Apply** to save the changes.
- 5 Click **Close**.

## Enable startup items

### Enable startup items

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, double-click **Performance**, and then click **Startup Manager**.
- 3 In the **On/Off** column, check a program that you want to automatically start when you turn on your computer.
- 4 Click **Apply** to save the changes.
- 5 Click **Close**.

# Customize settings

This chapter includes the following topics:

- [Configure Network Proxy Settings](#)
- [Set Norton to allow you to remotely manage your protected devices](#)
- [Protect Norton device security settings from unauthorized access](#)
- [Configure Norton for best battery use](#)
- [Set a shortcut key to search Norton device security for information](#)

## Configure Network Proxy Settings

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

### Configure Network Proxy Settings

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 In the **Network Proxy Settings** row, click **Configure**.
- 5 In the **Network Proxy Settings** window, do the following:
  - If you want your browser to automatically detect network connection settings, under **Automatic Configuration**, check **Automatically detect settings**.

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

## Set Norton to allow you to remotely manage your protected devices

Norton **Remote Management** sends the health status of your device and other information to Norton Studio app for Windows. You can use this app to view, manage, or explore Norton products and fix some protection issues with your device remotely. By default, Remote Management is turned off.

### Turn on Remote Management

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 In the **Remote Management** row, move the switch to **On**.
- 5 Click **Apply**, and then click **Close**.

## Protect Norton device security settings from unauthorized access

To prevent unauthorized changes to your Norton device security settings turn on **Settings Password Protection** and **Norton Tamper Protection**.

- **Settings Password Protection** lets you set a password to view or change device security settings.

- **Norton Tamper Protection** checks for modifications to your settings by unknown or suspicious apps.

#### Turn on or off Settings Password Protection and Norton Tamper Protection

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 Under **Product Security**:
  - In the **Settings Password Protection** row, move the switch to **On** or **Off**.
  - In the **Norton Tamper Protection** row, move the switch to **On** or **Off**.  
If prompted, select how long you want the feature off, and click **OK**.
- 5 Click **Apply**.
- 6 If you see the **Set Password** window, type a password and confirm. You need to set a password each time you turn this feature off and on.
- 7 Click **OK**.
- 8 In the **Settings** window, click **Close**.

### Reset a lost or forgotten password for Norton Settings Password Protection

You must reinstall your Norton to access the settings and set a new password.

## Configure Norton for best battery use

When your computer runs on battery power, active software programs should consume minimum resources. This assures that your computer maximizes battery life and is more energy efficient. You can configure a low threshold profile for battery use. When a program or a process exceeds the low threshold limit, Norton notifies you with a performance alert. You can choose to close the program or the process manually and free the resource. If the **Use Low Resource Profile On Battery Power** option in the **Administrative Settings** window is turned on, Norton automatically changes the threshold profile to low when your computer runs on battery power. By default, this option is turned on.

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

**Turn the Use Low Resource Profile On Battery Power option on or off**

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to **Off** or **On**.
- 5 Click **Apply**, and then click **Close**.

## Set a shortcut key to search Norton device security for information

When you search using the



icon in the Norton device security app, you can find Norton feature and support information as well as general topics online. You can use the default keyboard shortcut **Ctrl + F** to launch search more quickly or set a shortcut.

**Set up a Search Shortcut Key**

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton product main window, click **Settings**.
- 3 In the **Settings** window, click **Administrative Settings**.
- 4 In the **Search Shortcut Key** row, move the switch to **On**.
- 5 Click the arrow and then choose a key that you want to assign for in-product search.
- 6 Do one of the following:
  - For the shortcut key to work only when your Norton product has focus, **uncheck** the **Global** option.
  - For the shortcut key to work even when your Norton product has **no** focus, **check** the **Global** option.
- 7 Click **Apply**, and then click **Close**.

# Find additional solutions

This chapter includes the following topics:

- [Find the version number of your product](#)
- [Upgrade your Norton product](#)
- [Uninstall your Norton product](#)

## Find the version number of your product

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

### Find the version number of your product

- 1 Start Norton.  
If you see the **My Norton** window, next to **Device Security**, click **Open**.
- 2 In the Norton main window, click **Help**.
- 3 In the **Help Center** window, under **General Information**, click **About**.

## Upgrade your Norton product

If you have an active subscription, you can upgrade your current Norton product to the latest version without any cost.

To check for the availability of new version, on the Norton product main window, click **Help > New Version Check**. If a new version is available, follow the on-screen instructions to download the new product. Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats.



After successful download, your Norton product prompts you for seamless installation. Ensure that you have saved all your important data such as pictures and financial records before you install the new version of the product.

On the completion of upgrade, your subscription status remains the same as your previous version of product. For example, you have 200 days of subscription left with your current version of product and you upgrade your product to the latest version. In this case, the subscription status of your upgraded product remains 200 days only.

---

**Note:** The upgrade process might not work if your browser is incompatible to communicate with the Symantec servers. The supported browsers are Internet Explorer 11 or later, Chrome 30 or later, Firefox 27 or later, Safari 7 or later, and Opera 17 or later.

---

Product upgrade is different from the protection updates that are processed by LiveUpdate. The main differences are as follows:

- Product upgrade lets you download and install a new version of the entire product.
- Protection updates are the files that keep your Norton product up to date with the latest antithreat technology.

Even if you have the latest version, always ensure that you have all the latest protection updates. LiveUpdate automates the process of obtaining and installing protection updates. You can run **LiveUpdate** or turn on **Automatic LiveUpdate** to obtain the latest updates.

## Uninstall your Norton product

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

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

---

**Note:** You should print out this help topic before continuing with the uninstallation. You cannot access online Help during uninstallation.

---

### Uninstall your Norton product from Windows Control Panel

- 1 Do one of the following:
  - On the Windows Taskbar, click **Start > Control Panel**.
  - In Windows 8, go to **Apps**, and under **Windows System**, click **Control Panel**.

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

4 Follow the on-screen instructions.

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

**Uninstall your Norton product from the Start menu**

- 1 On the Windows taskbar, click **Start > All Programs/All apps > Norton Security > Uninstall Norton Security**.
- 2 If you do not want to keep Norton Home Page as your default home page and Norton Safe Search as your default search provider, select the check box that appears at the bottom.
- 3 Follow the on-screen instructions.

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

**Uninstall your Norton product from the Start screen in Windows 8/8.1**

- 1 On the **Start** screen, right-click your Norton product, and then click **Uninstall**.
- 2 In the list of currently installed programs, click your Norton product, and then click **Uninstall/Change**.
- 3 Follow the on-screen instructions.

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