Norton™ AntiVirus Plus
Norton™ 360
Norton™ 360 with LifeLock™
Norton™ 360 for Gamers

User Manual

Norton™ 360 with LifeLock™ User Manual

NortonLifeLock Inc.
60 East Rio Salado Parkway,
Suite 1000,
Tempe, AZ 85281

https://www.nortonlifelock.com

Contents

Chapter 1

Welcome to Norton LifeLock

This chapter includes the following topics:

System requirements for Norton 360

Norton Device Security entitlement only

- Norton™ AntiVirus Plus covers a single PC or Mac

Device Security and Norton Secure VPN entitlements

Supports devices running on Windows, Mac, Android, and iOS

- Norton™ 360 Standard covers a single device
- Norton™ 360 Deluxe covers up to 5 devices
- Norton™ 360 with LifeLock Select covers up to 5 devices
- Norton™ 360 with LifeLock Advantage covers up to 10 devices
- Norton™ 360 with LifeLock Ultimate Plus covers unlimited devices (Restrictions apply*)
- Norton™ 360 for Gamers covers up to 3 devices

Note: Not all NortonLifeLock protection offerings mentioned above are available in all regions or for all partners.

Device Security

Note: Not all features are available on all platforms.

Note: Parental Controls, Cloud Backup, and SafeCam are currently not supported on Mac OS.

Windows™ Operating Systems

- Microsoft Windows® 10 (all versions)
- Microsoft Windows® 10 in S mode (32-bit or 64-bit or ARM32) version 1803 and above
- Microsoft Windows® 8/8.1 (all versions)
  Some protection features are not available in Windows 8 Start screen browsers.
- Microsoft Windows® 7 (32-bit and 64-bit) with Service Pack 1 (SP 1) or later

Note: Norton AntiVirus Plus is not supported on Windows 10 in S mode.

Mac® Operating Systems

- Mac OS X 10.10.x or later with Norton product version 8.0 or later.

Note: Norton Family Parental Controls and Cloud Backup are currently not support on Mac OS.

Android™ Operating Systems

- Android 6.0 or later

  Must have Google Play app installed.

  Auto-scan of apps on Google Play is supported on Android 4.1 or later, except for Samsung devices. Samsung devices running Android 4.2 or later are supported. For earlier versions of Android, the Google Play “Share” function must be used to scan apps on Google Play.

iOS Operating Systems

- iPhones or iPads running the current and previous two versions of Apple iOS

System requirements for Norton™ Secure VPN

Available for Windows™ PC, Mac®, iOS and Android™ devices:

Norton Secure VPN is compatible with PCs, Macs, Android smartphones and tablets, iPads, and iPhones. Norton Secure VPN may be used on the specified number of devices – with unlimited use during the subscription term.

Windows™ Operating Systems

- Microsoft Windows® 10 (all versions except Windows 10 S)
- Microsoft Windows® 8/8.1 (all versions)

- Microsoft Windows® 7 (32-bit and 64-bit) with Service Pack 1 (SP 1) or later

150MB of available hard disk space.

Mac® Operating Systems

- Current and previous two versions of Mac OS.

300MB of available hard disk space.

Android™ Operating Systems

- Android 6.0 or later

Must have Google Play app installed.

iOS Operating Systems

- iPhones or iPads running the current and previous two versions of Apple iOS

Access your NortonLifeLock account

You manage subscription details, find your product key, activate subscription renewal, or access other services from your NortonLifeLock account.

Access your account

1. Go to my.Norton.com and click **Sign In**.
2. Type in your username/email address and password, and then click **Sign In**.
3. If you forgot your password, click **Forgot password?** and provide your email address.

If you see a message that your account is temporarily locked due to too many failed login attempts, we recommend that you wait for one hour and try signing in again.

Chapter 2

Set up your protection

This chapter includes the following topics:

Set up Device Security

To protect your device, you must install Norton Device Security. You can install Device Security on your Windows desktops and laptops, Mac computers, and mobile devices that run on Android and iOS.

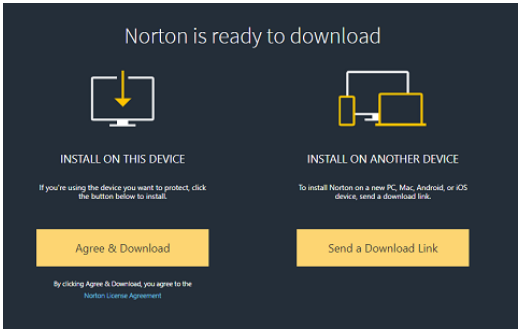
Download and install your Device Security

1. From each computer, laptop, and smart phone, open your browser and type the following URL:

   https://norton.com/setup

2. Sign in to your NortonLifeLock account.

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



4 Click on the area pointed by the on-screen arrow and follow the on-screen instructions.

Your service gets downloaded, installed, and activated automatically.

Note: If your download did not complete, or you see any error when you download your service, you can restart the download.

Set up Norton Password Manager

After you install Device Security your prompted to add browser extensions. In order for the features to work, you'll need to add the extensions to Internet Explorer, FireFox, and Chrome browsers.

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

Norton Safe Web	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.
Norton Safe Search	A secured search engine that uses Ask.com and Yahoo! to generate the search results. Norton Safe Search ranks the search results based upon the site safety status and Norton rating.
Norton Home Page	A website that uses the Norton Safe Search feature to enhance your web search experience. It provides the site safety status and Norton rating for each of the search result generated.

Norton Password Manager	A secure location where you can store all of your sensitive information such as logins, personal information, and financial information. You can use this information to log in to websites, automatically fill online forms, and online payments.

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**.

Google Chrome

Add Norton browser extensions in Google Chrome

Note: You must have the latest version of Norton 360 to install the browser extensions of Google Chrome. If you do not have the latest version, run LiveUpdate in your Norton product. We offer 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 Chrome by following the below instructions.

1. After you install Device Security 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.

Mozilla Firefox

Add Norton browser features in Mozilla Firefox

Note: You must have the latest version of Norton 360 to install the web-based standalone browser extensions of Mozilla Firefox. If you do not have the latest version, run LiveUpdate in your Norton product. We offer the following extensions for Firefox browser:

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

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

1 After you install Device Security 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 Device Security, 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.

Microsoft Edge

Add Norton browser extension in Microsoft Edge

Note: Norton Password Manager is an independent extension and does not require the installation of a Norton product in Microsoft Edge browser. The extension is compatible only with computers running Windows 10 Creators Update and later versions.

---

1 Start the Microsoft Edge browser.

2 On the top-right corner, click the **More** button 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 and click **Norton Password Manager** from the results.

5 Click **Install**.

After the extension is installed, click **Launch**.

6 In the **You have a new extension** pop-up window, click **Turn it on**.

7 To display the Norton Password Manager icon on the address bar, click the **More** button on the top-right corner of the browser and click **Extensions**.

8 In the **Extension** window, select **Norton Password Manager**.

9 In the **Norton Password Manager** window, under **Show button next to the address bar**, move the slider to **On**.

Browser extensions for Microsoft Edge based on Chromium

Microsoft has launched a new version of Microsoft Edge based on the Chromium open source project. Norton offers the following browser extensions for this new browser version on the Microsoft Edge store.

- Norton Password Manager - Helps provide the tools you need to create, store, and manage your passwords, credit card and other sensitive information online more safely and securely
- Norton Safe Web - Provides protection from online threats while you browse the web.

The extensions are available for both Windows and Mac platforms.

Add Norton Safe Web extension in Microsoft Edge

1 Launch the Microsoft Edge browser.

2 Launch Norton Safe Web extension from the Microsoft Edge Addons page.

Note: You can click the settings icon > **Extensions** to check if the Norton Password Manager extension is already installed. In the **Extensions** page, move the Norton Safe Web slider to enable the extension.

---

3 In the Norton Safe Web Addons page, click **Get**.

4 Click **Add extension** in the **Add "Norton Safe Web" to Microsoft Edge** notification pop-up to install the Norton Safe Web extension.

Add Norton Password Manager extension in Microsoft Edge

1 Launch the Microsoft Edge browser.

2 Launch Norton Password Manager extension from the Microsoft Edge Addons page.

Note: You can click the settings icon > **Extensions** to check if the Norton Password Manager extension is already installed. In the **Extensions** page, move the Norton Password Manager slider to enable the extension.

---

3 In the Norton Password Addons page, click **Get**.

4 Click **Add extension** in the **Add "Norton Password Manager" to Microsoft Edge** notification to install the Norton Password Manager extension.

Set up Cloud Backup

Cloud Backup acts as a preventative measure to losing data due to ransomware, malware, or if you experience major hardware issues with your PC. Your subscription entitles you a specific amount of Norton Cloud Backup space. The volume of free cloud storage depends on the subscription you purchased.

Note: Norton Cloud Backup feature is only available on Windows.

Before running your first backup, you must activate Cloud Backup.

Note: To use Cloud Backup, you must set the **Network Cost Awareness** option in the **Firewall Settings** window to **No Limit**.

Activate Cloud Backup

1 Start Norton.

2 In the **My Norton** window, next to **Cloud Backup**, click **Set Up**.

3 In the window that appears, click **Activate Backup**.

4 When you see a sign-in prompt, type your NortonLifeLock account email address and password and click **Sign In**.

5 Click **Done**.

Set up LifeLock Identity Theft Protection

With LifeLock and Norton joining forces under one company, we now help protect your identity.

You can add the following personal information to LifeLock for monitoring†:

- Driver’s license
- Social security number, date of birth, mother’s maiden name
- 5 Insurance ID’s
- 5 addresses
- 5 phone numbers

- 10 bank accounts
- 10 credit cards*

You can add additional information for monitoring, such as additional phone numbers, email address or accounts.

The LifeLock Identity Alert System alerts you† when your identity is being used by someone. It can be people trying to obtain a cell phone account or an auto loan in your name.

Note: LifeLock Identity Theft Protection does not cover businesses. Our technology and service is designed to help protect individuals with social security numbers and other personal identifiable information, which businesses don't have.

*Major credit cards, such as Visa, MasterCard, American Express and Discover, can be added. Unfortunately at this time, other types of cards, such as retail store cards or gift cards, are not supported.

No one can prevent all identity theft or cybercrime.

†LifeLock does not monitor all transactions at all businesses.

Set up LifeLock Identity Theft Protection

1. Start Norton.
2. In the **My Norton** window, next to **Identity Theft Protection**, click **Set Up**.
3. In the **LifeLock Member Login** page, click **Sign In With Norton**.
4. Enter your account credentials and sign in.
5. Follow the on-screen instructions.

Install the LifeLock for Norton 360 app on Android

1. On your Android device, launch the **Play Store** app and search for **LifeLock Identity Theft Protection**.
2. Once you have located the app page in the Play Store, tap **Install**, and then tap **Accept**.
3. Open the app once installed and sign in with your account credentials.

Install the LifeLock for Norton 360 app on iOS

1. On your iOS device, launch the **App Store** app and search for **LifeLock Identity Theft Protection**.
2. Once you have located the app page in the App Store, tap **Get**, and then tap **Install**.
3. Open the app once installed and sign in with your account credentials.

Dark Web Monitoring powered by LifeLock**

What is Dark Web Monitoring?

We monitor for use of your personal information** on hard-to-find dark websites and forums. When we detect your information on the dark web, we notify you.

Why is it important?

Identity thieves can sell your personal information on hard-to-find dark web sites and forums.

What should you do?

If you find any of your information in the notification, refer to the steps below.

- **Debit/Credit Card Compromise**: If the card is closed no action needs to be taken. If the account is current, contact your credit/debit card company and request a new card. Keep a close eye on your statements.
- **Email Compromise**: Change your current email password. If you have any accounts with the same password, change those as well. If you have ongoing issues, you may want to open a new email account. Remember that changing your passwords every 30 days will help keep your accounts secure.
- **Social Security Number Compromise**: We recommend that you set fraud alerts with one of the three credit bureaus to further help protect your identity.
- **Name/Address/Phone Number Compromise**: Fortunately, more potentially damaging information such as your Social Security number hasn't been shared in this case. However, because some of your personal information is out there, we advise to keep a close eye on your credit report for any discrepancies.

We will continue to monitor the dark web for your personal information**. If we detect your information, we will send another email.

Note: No one can prevent all identity theft.

**Dark Web Monitoring in Norton 360 plans defaults to monitor your email address only. Please login to the portal to review if you can add additional information for monitoring purposes.

Set up your Secure VPN

Public Wi-Fi is everywhere: airports, coffee shops, malls, and hotels. Free 'hotspots' are so widespread and convenient that people may connect to them without thinking twice. But reading emails, checking your bank account, or performing any activity that requires a logon can be risky when you use public Wi-Fi. If you use public Wi-Fi, your online activities can be monitored.

Cybercriminals can steal personal information like your usernames, passwords, location, chats, emails, or account numbers.

Secure VPN helps secure your connection when you use a public wireless connection. It creates a virtual private network (VPN) that encrypts your sensitive data.

Secure VPN helps protect the data you send and receive when using public Wi-Fi in the following ways:

- Adds bank-grade encryption to protect your connection while on public Wi-Fi hotspots.
- Lets you browse the web anonymously so your online privacy is protected.
- Allows access to your favorite apps and content anywhere you go, as if you were at home.
- Encrypts your data with a no-log virtual private network that doesn't track or store your activity.
- Offers world-class customer support from Norton LifeLock, a leader in consumer online security.

Note: The Secure VPN feature is not available with all subscriptions.

Follow the below instructions to set up Secure VPN.

Set up Secure VPN

1. Start Norton.
2. In the **My Norton** window, next to **Secure VPN**, click **Set Up**.
3. In the web page that appears, click **Sign In**.
4. Enter your account credentials and sign in.
5. If you get a prompt to download, click **Download**.
6. Follow the on-screen instructions.

Join the discussion with other desktop users here Norton Community.

Set up Parental Controls

You can now set up Parental Controls to help your kids enjoy the Internet safely. It is easy and takes only three steps.

Parental Controls provide what you need to protect your family's online activities from Internet dangers and inappropriate content. It even helps you keep your children from passing along confidential information online.

Sign in to your NortonLifeLock account

1. Start Norton.
2. In the **My Norton** window, next to **Parental Controls**, click **Set Up**.
3. If prompted to sign in, enter your account credentials and sign in.
4. In the page that appears, click **Family** tab.
5. Read the **Terms of Service** and click **Agree & Continue** to set up your family.
6. Follow the on-screen instructions.

Add a child to your account

As you add each child, Parental Control applies pre-defined house rules based on the child's age. You can customize the house rules at any time to better suit each child's maturity level.

Note: You can add up to 15 children to your account. You can add or remove a child from your Norton Family account at any time.

---

1. In the **Child Name** box, type the child's name.

   Note: The name must not contain special characters such as &, #, or $.

   ---

2. Select the child's year of birth.

   House rules are applied based on the child's age.

3. Choose **Select an Avatar** or **Upload Photo** to set a profile picture for your child.

   Note: You can add more children to your account after you complete the set up for the first child.

   ---

4. Click **Next**.

Install Norton Family on your child's device

Install Norton Family on each device that your child uses. If you are not on your child's device, click **No** to send a download link in an email. Open this email on the device on which you want to install Norton Family.

To install Norton Family on Windows

1. Under **Does your child use this device?**, click **Yes** and then click **Next**.
2. Click or run the downloaded installer file.

3 Norton Download Manager will automatically install Norton Family on the device.

4 Read the User License Agreement and then click **Agree & Install**.

The device gets automatically linked to your account.

5 Click **Continue**.

6 In the assign device window, click **Edit** next to the child to whom you want to assign this device.

7 Click **signs in as** and choose the account that the child uses to log on to this device. If your child uses multiple user accounts, choose the child on all those user accounts.

8 Click **Save** > **OK**.

To install Norton Family app on Android

1 In the **INSTALL Norton Family** window, tap **Yes**, and then tap **Continue**.

2 Tap **Download Norton Family app**.

3 If prompted, complete the action using **Play Store**.

4 Tap **Install** and follow the on screen instructions.

5 Open the Norton Family parental control app.

6 Read the **Norton License Agreement** and then tap **Agree & Continue** > **Get Started**.

7 Click **Sign In** and enter your account credentials.

8 Tap **Child** to get into child mode and then tap **Continue**.

Child mode allows you to add child and assign house rules to this device.

9 To add a child, tap **Add a child**, and in the **PROFILE** window, enter the details of your child.

Choose an avatar for your child profile by tapping the avatar image. You can choose an image from your gallery or take instant photo for your child's profile.

10 Tap **Continue**, and then tap **Save**.

Norton Family has set default house rules based on your child's year of birth. You can tap **House Rules** to review the rules assigned to your child.

11 Choose the child whom you want to assign this device, give a name that helps you identify this device, and then tap **Done**.

12 If prompted, turn on **App Usage** and **Accessibility** options.

13 In the alert that appears, tap **Activate** to set Norton Family as the device administrator.

To install Norton Family app on iOS

1. In the **INSTALL Norton Family** window, tap **Yes**, and then tap **Continue**.
2. Tap **Download Norton Family app**.
3. Tap and install **Norton Family** application.
4. Tap **Open**.
5. Tap **OK** to allow Norton Family to send you the notifications.
6. Read the **Norton Licence Agreement** and **Privacy Policy**, and then tap **Agree & Continue**.
7. Sign in with your account credentials.
8. In the **Add child** screen, enter the details of your child and then tap **Add**.

   To add another child, tap **Add a new child**, and in the **Add Child** window, enter the details of your child and then tap **Add**.

   Choose an avatar for your child profile by tapping the avatar image. You can choose an image from your gallery or take instant photo for your child's profile.
9. Choose the child whom you want to assign this device and give a name that helps you identify this device.
10. Tap **Assign**.
11. Tap **Install** and follow the on-screen instructions to install a profile.

    Profile installation is required for instant lock and other features to work on your child's device.
12. Follow the on-screen instructions to set up restrictions.

Install Norton Family on a parent device

After you complete the setup, you must download and install the following mobile app on your device:

- Android device: install the **Norton Family parental control** app
- iOS device: install the **Norton Family for Parents** app

Download and install Norton Family parental control app on Android

1. Open the Play Store app and search for **Norton Family parental control**.
2. Select **Norton Family parental control app** and then tap **Install**.
3. Open the app once installed.
4. Read the **Norton License Agreement** and other policies and then tap **Continue**.

5 Sign in with your account credentials.

6 Tap **Parent device**. If you share the device with your child, switch to **Child mode** before you hand over the device to your child.

Download and install Norton Family for Parents app on iOS

1 Open the App Store app and search for **Norton Family for Parents**.

2 Select **Norton Family for parents** and then tap **Get**.

3 Open the app once installed.

4 Read the **Norton License Agreement** and other policies and then tap **Continue**.

5 Sign in with your account credentials.

Discuss with your family

Communication is the key to online family safety. Therefore, you can initiate a discussion with your child explaining the importance of responsible use of the Internet.

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**.

Chapter 3

Manage your Device Security

This chapter includes the following topics:

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.

Run LiveUpdate

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

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

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

Run LiveUpdate manually

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 **LiveUpdate**.

3. In the **Norton LiveUpdate** window, when the LiveUpdate is completed successfully, click **OK**.

View or fix device security risks that Norton detects

When Norton detects a security risk, it automatically removes it, unless it requires your input to understand how you want to resolve the risk. 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 security risk.

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.

Note: Sometimes, you may need to restart your computer after Norton removes a security risk. If Norton prompts you to restart your computer, you should save any open files, and then restart your computer.

Note: 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 31.

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**.

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

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.

---

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**.

Submit an item for Norton's evaluation

You can contribute to the effectiveness of your Norton product by submitting files that you think is a security risk. Norton 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 NortonLifeLock**.

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.

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 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.

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.

Download Norton Power Eraser and run a scan (on Windows 10/8/7)

1 Download Norton Power Eraser.

2 Press **Ctrl** + **J** key, to open the **Downloads** window in your browser, and double-click the **NPE.exe** file.

If the User Account Control window prompts, click **Yes** or **Continue**.

3 Read the license agreement and click **Agree**.

If you have already accepted the license agreement, you will not be prompted again.

Norton Power Eraser checks for and automatically downloads the new version if available.

4 In the Norton Power Eraser window, select **Full System Scan**, and click **Run Now**.

5 If you want to include the Rootkit scan, click **Settings**, and under **Scan and Log Settings**, toggle the option **Include Rootkit scan (requires a computer restart)** and click **Apply**.

6 When you see a prompt to restart the computer, click **Restart**.

Wait for the scan to complete. Follow the on-screen instructions.

Download Norton Power Eraser and run a scan (on Windows XP/Vista)

1 Download Norton Power Eraser.

2 Press **Ctrl** + **J** key, to open the **Downloads** window in your browser, and double-click the **NPE.exe** file.

If the User Account Control window prompts, click **Yes** or **Continue**.

3 Read the license agreement, and click **Accept**.

Norton Power Eraser checks for and prompts to download the new version if available.

4 In the **Norton Power Eraser** window, click the **Scan for Risks** icon.

5 By default, Norton Power Eraser performs a Rootkit scan and requires a system restart. When you see a prompt to restart the computer, click **Restart**.

If you do not want to include the Rootkit scan, go to **Settings**, and uncheck the option **Include Rootkit scan (requires a computer restart)**.

6 Wait for the scan to complete. Follow the on-screen instructions.

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**.

View real-time threats detected by Norton SONAR

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.

Note: SONAR Protection should be kept turned on always. When Auto-Protect is turned off, SONAR Protection is also disabled and your computer is not protected against emerging threats.

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.

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 to **On**.

5 Click **Apply**.

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

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**.

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. NortonLifeLock 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. 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, 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 uncommon 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.

In addition, Norton blocks programs with embedded scripts from running if it detects any uncommon behavior with the embedded scripts. However, you can configure how you want Norton to handle programs with embedded scripts.

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 37. 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 or program 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 or programs 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**, and then click **Apply**.

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, and click **OK**.

6 In the **Block scripts when opening documents** row, move the **On/Off** switch to **On** or **Off**, and then click **Apply**.

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, and click **OK**.

7 In the **Settings** window, 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 and programs 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 PDF documents.

10 In the **Block scripts with uncommon behavior** row, select the action you want Norton to perform for programs with embedded scripts.

Your options are:

- **Block**
- **Allow**

- **Ask Me**

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

Learn more about Norton Script Control

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, etc.

Script Control helps protect you from malware that you download or receive as attachments in phishing emails.

It removes unsafe 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.

The following sections help you with configuring the Script Control settings.

Restore the original file with embedded scripts

You can restore the original files by replacing the sanitized files. You should restore the original files only if you are confident that they do not have any malicious content.

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**.

Configure Norton to handle documents and programs 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 PDF documents.

10 In the **Block scripts with uncommon behavior** row, select the action you want Norton to perform for programs with embedded scripts.

Your options are:

- **Block**
- **Allow**
- **Ask Me**

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

Turn off Script Control

Note: Turning off Script Control reduces your protection and should be done only if you have a specific need. Script Control provides an extra layer of security by removing scripts and sanitizing documents. NortonLifeLock recommends that you keep Script Control turned on at all times as it provides an extra layer of security.

---

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 **Off**.

6 In the **Block scripts when opening documents** row, move the **On/Off** switch to **Off**.

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

8 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 feature, and then click **OK**.

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

Protect your device from exploits, hackers, and zero-day attacks

A zero-day exploit is a technique that hackers use to take advantage of vulnerabilities in a program in order to perform malicious actions on your computer. Besides slowing down your computer or causing programs to fail, these exploits can expose your personal data and confidential information to hackers.

The Exploit Prevention feature in your Norton product protects applications and files that are prone to exploit attacks. By default, Norton Exploit Prevention is turned on and blocks attacks against vulnerable programs by closing those programs. Norton sends an Attack Blocked notification when it shuts down a program and provides links to information about the attack.

Turn off or turn on Exploit Prevention

Note: When **Exploit Prevention** is turned off, your computer is vulnerable to zero-day and other exploits.

---

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 **Exploit Prevention**.

4 In the Exploit Prevention row, move the **On/Off** switch to **Off** or **On**.

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

Exploit Prevention Techniques

Norton uses proactive exploit prevention techniques to protect your computer from the latest zero-day attacks. You can turn individual techniques on or off from the **Settings** window. By default, all techniques are turned on.

Note: Norton recommends that you keep all individual Exploit Prevention techniques turned on to protect against the widest range of exploits.

Exploit Prevention techniques include:

- **Java Process Protection**
  Prevents remote hackers from using malicious code through java processes and allows only trusted java processes to run.
- **Structured Exception Handler Overwrite Protection**
  Protects against structured exception handling exploits, which compromise an application by overwriting the pointer of an exception handler with an attacker controlled address.
- **Stack Pivot Detection**
  Block exploit attacks that changes the stack pointer with attacker's controlled memory to execute its Return Oriented Programming (ROP) crafted attack code.
- **Data Execution Prevention Enforcement**
  Blocks attackers from executing malicious code from stack or heap memory of your computer.
- **Memory Layout Randomization Enforcement**
  Enforces dynamically loaded application DLLs or modules to be always loaded in random locations to protect them from attackers.
- **Heap Spray Protection**
  Protects commonly targeted memory locations where exploits or attackers allocate their shellcode using heap spray attack techniques.
- **Memory Layout Randomization Enhancement**
  Improves the ASLR (Address Space Layout Randomization) behavior of the operating system when allocating critical memory locations of the application. This makes those memory locations less predictable from attackers.
- **Null Page Protection**
  Pre-allocates the null memory location which will help in preventing attacks on null pointer dereference vulnerabilities.
- **Remote DLL Injection Detection**
  Prevents remote hackers from inserting malicious executable code over external networks such as public IP addresses or domains.
- **Stack Execution Prevention**, **Suspicious API Invocation Detection**, and **Heap Payload Detection** techniques protect your computer against Return-Oriented Programming (ROP)

attacks that bypass the Address Space Layout Randomization and Data Execution Prevention exploit mitigation techniques.

Turn Norton Firewall on or off

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

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

Turn Norton Firewall 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 **Firewall**.
4. On the **General Settings** tab, in the **Smart Firewall** row, move the **On/Off** switch to **Off** or **On**.
5. Click **Apply**.
6. If prompted, select the duration until when you want the Firewall feature to be turned off, and click **OK**.

Disable or enable Norton Firewall from the Windows notification area

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

Customize Program Rules to change access settings for programs

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

Customize Program Rules

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 **Program Control** tab, in the **Program** column, select the program that you want to change.

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

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

6 Click **Apply**.

Change the order of firewall rules

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

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

Change the order of Traffic rules

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 **Traffic Rules** tab, select the rule that you want to move.

5 Do one of the following:

- To move this rule before the rule above it, click **Move Up**.
- To move this rule after the rule below it, click **Move Down**.

6 When you are done moving the rules, click **Apply**.

Change the order of Program rules

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 **Program Control** tab, select the program that contains the rule that you want to move.

5 Click **Modify**.

6 In the **Rules** window, select the rule that you want to move.

7 Do one of the following:

- To move this rule before the rule above it, click **Move Up**.
- To move this rule after the rule below it, click **Move Down**.

8 When you are done moving the rules, click **OK**.

9 In the **Firewall** settings window, click **Apply**.

Turn off a Traffic rule temporarily

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

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

Turn off a Traffic rule temporarily

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 **Traffic Rules** tab, uncheck the box next to the rule that you want to turn off.

5 Click **Apply**.

Allow Internet access for a blocked program

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

Allow Internet access for a blocked program

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 **Program Control** tab, select the program that you want to allow access to the Internet.
5. In the **Access** drop-down list for the program entry, click **Allow**.
6. Click **Apply**.

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

However, Norton lets you can manually configure the Internet access settings for your programs.

Configure Internet access settings for your programs

Turn off Automatic Program Control

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. In the **Firewall** settings window, click **Advanced Program Control**.
5. In the **Automatic Program Control** row, move the **On/Off** switch to **Off**.
6. In the confirmation window, click **Yes**.
7. In the **Settings** window, click **Apply**, and then click **Close**.

Configure the Internet access settings for a program

1. Start your program.

   When the program tries to access the Internet, Norton prompts you with a firewall alert.
2. In the **Firewall Alert** window, in the **Options** drop-down list, select an action.

   You can allow, block, or manually create a program rule.
3. Click **OK**.

Turn Firewall Block Notification off

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

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

Turn Firewall Block Notification 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 **Firewall**.
4. On the **Advanced Program Control** tab, move the **Show Firewall Block Notification** switch to **Off**.

Learn more about 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.

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**.

Turn Browser Protection on

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**.

Set Norton Firewall to stop or start notifying you when it blocks an attack

You can choose whether you want to receive notifications when Norton Intrusion Prevention blocks suspected attacks.

If you chose not to receive notifications, you can still view attacks that Norton blocked in your security history.

Turn off or turn on Intrusion Prevention notifications

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 **Notifications** row, move the **On/Off** switch to **Off** or **On**.

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

Turn off or turn on an individual Intrusion Prevention notification

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 Signatures** row, click **Configure**.

6 In the **Intrusion Signatures** window, uncheck or check **Notify me** corresponding to the individual signature.

7 Click **OK**.

8 In the **Intrusion Signatures** window, click **Apply**, and then click **OK**.

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

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 computers that are blocked by Norton AutoBlock

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:

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

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**.

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.

Get started using Norton Cloud Backup

Cloud Backup stores and protect important files and documents as a preventative measure to data loss due to hard drive failures, stolen devices and even ransomware.

Note: Norton Cloud Backup is available only on Windows.

Before running Norton Cloud Backup, create a backup set that specifies what files you want to back up. You can also specify where you want the files to be backed up and when you want the backup to run. You can backup files to the cloud using Norton Cloud Backup or to your own external drives.

Note: The first time you run a backup, Norton may take some time to examine and copy all the files on your computer. If your Internet connection is slow, the process may take longer.

Norton does not back up your files automatically if the backup destination is Local Backup. Backing up to local storage devices needs your intervention.

Create a backup set

1. Start Norton.

   If you see the **My Norton** window, next to **Device Security**, click **Open**.
2. In the Norton main window, double-click **Backup**, and then click **Backup Sets**.
3. In the **Backup Settings** window, click **Create New Set**.
4. In the window that appears, type a name for your backup set, and then click **OK**.
5. On the **What** tab, under **File Types**, turn on one or more file categories that you want to back up.
6. On the **Where** tab, in the **Destination** column, select **Secure Cloud Storage**.

   If you have not activated cloud backup, click the **Activate for free** link and follow the instructions.
7. On the **When** tab, use the **Schedule** list to select the backup schedule that best suits your needs.
8. Click **Save Settings**.

Run Norton Cloud Backup

Note: Norton may prompt you to enter your account credentials for authentication when you run backup for the first time.

1. Start Norton.

   If you see the **My Norton** window, next to **Device Security**, click **Open**.
2. In the Norton main window, double-click **Backup**, and then click **Run Backup**.
3. In the **Run Backup** window, follow the on-screen instructions.
4. Click **Close**.

   Note: If the backup does not complete, Norton suggests possible causes such as inadequate storage capacity or speed limitations. Always check that you are connected to the Internet when running a backup and that storage devices are connected and turned on.

Add or exclude files and folders in your backup sets

Norton lets you back up different file types, like picture, music, or video files, to your backup sets. You can specify files or folders that contain file types normally included in your backup sets and exclude them from backups.

You can also add or remove file extensions that are normally part of the default file types. For more information, See "View or change the default file types or file extensions that Norton includes in backups" on page 68.

Add or exclude files and folders in backup set

1. Start Norton.

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

2. In the Norton main window, double-click **Backup**, and then click **Backup Sets**.
3. In the **Backup Settings** window, in the **Backup Set** drop-down list, select the backup set that you want to configure.
4. On the **What** tab, click **Add or exclude files or folders**.
5. In the window that appears, do the following:
   - To add a file to the backup set, click **Include File** and navigate to the file you want to add.
   - To add a folder to the backup set, click **Include Folder** and navigate to the folder you want to add.
   - To remove a file from the backup set, click **Exclude File** and navigate to the file you want to remove.
   - To remove a folder from the backup set, click **Exclude Folder** and navigate to the folder you want to remove.
6. In the **Backup Settings** window, click **Save Settings**.

Note: You can also right-click a file or folder and select **Norton Security > Add to Backup/Exclude from Backup** from the shortcut menu.

The **Add to Backup** and **Exclude from Backup** options appear in the shortcut menu only after you configure your backup and when the **Backup Settings** and the **Restore Files** windows are closed.

View or change the default file types or file extensions that Norton includes in backups

By default, Norton Backup looks for files that belong to certain file types, like pictures, music, or video, before running a backup. The default file types ensure that the data most users consider important gets backed up automatically once they create a backup set and run a backup. You can change the backup file type defaults, or the extensions included in each file type, if you want to include or exclude data from your backups.

View or change default file types or file extensions included in backups

1. Start Norton.

   If you see the **My Norton** window, next to **Device Security**, click **Open**.
2. In the Norton main window, double-click **Backup**, and then click **Backup Sets**.
3. In the **Backup Settings** window, in the **Backup Set** drop-down list, select the backup set that you want to configure.
4. On the **What** tab, check **Edit File Type** to change the extensions included in file types for picture, music, video and other file types.
5. Under **File Types**, click **Configure** next to a file type.
6. In the window that appears, do the following, and click **Save**.
   - To remove a file extension, select the file extension in the list and click **Remove**.
   - To add additional extensions to the list, click **Add New**.
7. In the **Backup Settings** window, click **Save Settings**.

Restore pictures, music, or other important files from Norton backup sets

You can easily restore your Norton Backup data if you are the victim of ransomware or other malware or if you experience unrecoverable hardware issues. You can choose to restore entire backup sets or specific files in a backup set. You can also determine where to restore backed up files.

Note: Restore happens as per the configured backup set. If you restore to a new device, you cannot expect Norton to restore your files as per your desired folder structure of your old device.

Restore Norton backup files or entire backup sets

1. Start Norton.

   If you see the **My Norton** window, next to **Device Security**, click **Open**.
2. In the Norton main window, double-click **Backup**, and then click **Restore Files**.
3. In the **Restore Files** window, under **Restore From**, click **View All**.

   Click a backup set, and then click **OK**.
4. In the **Restore Files** window, under **Files**, click **Browse for Files and Folders**.

   Select the files that you want to restore, and then click **OK**.
5. In the **Restore Files** window, under **Restore To**, click **Original Location**.

   Click **Change** and follow the instructions if you don't want to restore to the original location.
6. Click **Restore Files** and then click **Close**.

Download files from Cloud Backup

1. Go to https://my.Norton.com.
2. Click **Sign In**.
3. Enter your NortonLifeLock account email address and password and click **Sign In**.
4. In the **My Norton** page, in the **Cloud Backup** tile, click **View Backup Sets**.
5. Select the backup set that has the file you want to download.
6. Navigate to the file you want to download.

   If you know the file name, you can use the search functionality to search for the particular file.

   Use the **Filter** option to filter out the pictures and documents.
7. Move the mouse pointer over the file name and click **Download**.

Delete backup set and files from Cloud Backup

You can delete a backup set if it is no longer needed. You cannot delete a backup set if only one backup set is available. However, you can create a new backup set before you delete the old backup set.

Note: Sometimes, a back-end service outage or server maintenance can stop you from deleting your backup data. In such cases, try deleting after some time. To identify if there is a service outage, check the Norton Service Status page.

When a backup set is deleted, the Backup details of the files that are included in that backup set also change. For example, the icon overlays and the **Backup** tab in the file properties of the file no longer appear.

Deleting a backup set is particularly helpful if you want to free some space on your Secure Cloud Storage.

Note: To delete a backup set from your cloud backup, you must set the **Network Cost Awareness** option in the **Firewall Settings** window to **No Limit**.

For more information, See "Define the Internet usage for Norton" on page 62.

Delete a backup set

1. Start Norton.

   If you see the **My Norton** window, next to **Device Security**, click **Open**.
2. In the Norton main window, double-click **Backup**, and then click **Backup Sets**.
3. In the **Backup Settings** window, in the **Backup Set** drop-down list, select the backup set that you want to delete.
4. Click **Delete**.
5. In the **Delete Backup Set** window, do one of the following:
   - To delete the current backup set, select **Delete backup set**.
   - To delete the current backup set and purge the files already backed up, select **Delete backup set and files**.
6. Click **Yes**.

Delete backup set from your account

1. Sign in to your account.
2. In the **My Norton** page, click **Cloud Backup**.

   The existing backup sets that are in use are displayed.
3. To delete a backup set, click the trash icon of the backup set that you want to delete.
4. In the **Delete Backup Set** confirmation window, click **Delete**.

   Click **Cancel** to display the backup page without deleting the backup set.

Customize your Norton product settings

In the **Settings** window, you can turn on or turn off the following **Quick Controls** services:

- **Silent Mode**
- **Backup**
- **Backup Status Overlays**
- **Automatic LiveUpdate**
- **Smart Firewall**
- **Norton Tamper Protection**

You should leave all of the services turned on except Silent Mode.

Turn on or turn off Quick Controls services

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, under **Quick Controls**, do one of the following:
   - To turn on a service, check its check box.
   - To turn off a service, uncheck its check box.
     If an alert or a message appears, select the duration from the drop-down menu, and then click **OK**.

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

Checks for boot viruses when you access removable media. After the removable media has been scanned for boot viruses, it is not scanned again until it is reinserted or formatted. If you still suspect that a boot virus infects your removable media, ensure that Auto-Protect is turned on to rescan the removable media. You then insert the removable media and open it from My

Computer for Auto-Protect to rescan it. You can also scan it manually to verify that the removable media is not infected.

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

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**.

Learn more about Scans and Risks settings

Scans and Risks settings let you customize the scans that Norton performs on your computer. You can configure a scan based on the digital signature and trust level of the files on your computer. You can define how Norton should behave when it scans email messages.

You can use the following **Scans and Risks** settings:

Computer Scans

You can run different types of scans to detect and prevent any virus infection on your computer. The scans are Quick Scan, Full System Scan, and customized scans. You can use the various **Computer Scans** options to customize the scans that Norton performs on your computer. You can also specify scanning of compressed files.

The **Computer Scans** options also let you specify scans to detect rootkits, other stealth items, tracking cookies, and unknown security threats. Your options are:

- **Compressed File Scan**
  Scans and repairs the files inside compressed files.
  When you turn on this feature, Norton scans and detects viruses and other security risks in the files within compressed files and removes the compressed files.
- **Rootkits and Stealth Items Scan**
  Scans for rootkits and other security risks that might be hidden on your computer.
- **Network Drives Scan**
  Scans the network drives that are connected to your computer.
  Norton performs a **Network Drives Scan** during **Full System Scan** and **Custom Scan**. By default, the **Network Drives Scan** option is turned on. If you turn off this option, Norton does not scan network drives.
- **Heuristic Protection**
  Scans your computer to protect against unknown security threats.
  Norton uses heuristic technology to check suspicious characteristics of a file to categorize it as infected. It compares the characteristics of a file to a known infected file. If the file has sufficient suspicious characteristics, then Norton identifies the file as infected with a threat.

- **Tracking Cookies Scan**
  Scans for the small files that programs might place on your computer to track your computing activities.
- **Full System Scan**
  A Full System Scan thoroughly examines your entire computer for viruses, spyware, and different security vulnerabilities. You can use the **Configure** option to schedule the Full System Scan.

Protected Ports

Protected Ports settings protect the POP3 and SMTP ports of your email program.

You can use this option to manually configure your POP3 and SMTP email ports for email protection. If the SMTP and POP3 port numbers that your Internet service provider (ISP) has provided for your email program is different from the default SMTP and POP3 port numbers, you must configure Norton to protect the ports.

Email Antivirus Scan

Email Antivirus Scan protects you from the threats that are sent or received in email attachments.

You can use the Email Antivirus Scan options to define how Norton should behave when it scans email messages. Based on the options you choose, Norton automatically scans the email messages that you send or receive.

Exclusions / Low Risks

Exclusions options specify the items such as folders, files, and drives that you exclude from Norton scans. Scan signatures and low-risk items are some items that you can exclude from scanning.

Exclusions options also let you choose which categories of risks you want Norton to detect. Your options are:

- **Low Risks**
  Lets you manage the low-risk items that are found in your computer.
  You can specify how you want Norton to respond to low-risk items.
- **Items to Exclude from Scans**
  Lets you determine which disks, folders, or files you want to exclude from risk scanning.
  You can add new exclusion items or edit the added items in the excluded-items list. You can also remove items from the excluded-items list.
- **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection**
  Lets you determine which disks, folders, or files you want to exclude from Auto-Protect scans and SONAR scans.

You can add the new items that need to be excluded or modify the items that you already excluded. You can also remove items from the excluded-items list.

- **Signatures to Exclude from All Detections**
  Lets you select known risks by name and remove a risk name from the excluded-items list
  You can also view the risk impact that is based on the performance, privacy, removal, and stealth impact.
- **Clear file IDs excluded during scans**
  Lets you remove the reputation information of the files that are excluded from scanning.
  You can use the **Clear All** option to clear the reputation information of the files that are excluded from scanning.

Note: Exclusions reduce your level of protection and should be used only if you have a specific need.

Learn more about Intrusion and Browser Protection settings

Intrusion Prevention scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects your computer against most common Internet attacks.

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. The Norton product runs LiveUpdate automatically to keep your list of attack signatures up to date. If you do not use Automatic LiveUpdate, you should run LiveUpdate once a week.

The Norton product also provides the Browser Protection feature to protect your browser from malicious programs.

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

With increasing Internet use, your browser is prone to attack by malicious websites. These websites detect and exploit the vulnerability of your browser to download malware programs to your system without your consent or knowledge. These malware programs are also called drive-by downloads. The Norton product protects your browser against drive-by downloads from malicious websites.

The **Intrusion and Browser Protection** settings also include the **Download Intelligence** option to protect your computer against any unsafe file that you download. Download Intelligence provides information about the reputation level of any executable file that you download using the browser. Download Intelligence supports only downloads using the HTTPS protocol, Internet Explorer 6.0 browser or later, Edge 40.15063 browser or later, Chrome 10.0 browser or later, and Firefox 3.6 browser or later. The reputation details that Download Intelligence provides indicate whether the downloaded file is safe to install. You can use these details to decide whether you want to install the executable file.

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.

Set a shortcut key to search Norton device security for information

When you search using the search icon in the Norton device security app, you can find Norton features 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**.

Optimize your computer for gaming with Game Optimizer

Game Optimizer[1] is patented technology for multi-core CPU PCs. It provides an immersive game experience by reducing performance interruptions while still maintaining your computer's security. By isolating non-essential apps to a single CPU core, it allows the rest of the CPUs to be allocated to game.

Note: Your computer's processor must be minimum four cores for Game Optimizer to work.

Game Optimizer helps improve your gaming experience by doing the following:

- Optimizes CPU performance for smoother gaming
- Isolates non-essential applications to a single CPU core so that the rest of the CPU can be allocated to game for better performance
- Automatically detects games[2]
- Lets you add games or select games you do not want to optimize
- Increases frames per second (FPS) and reduces latency
- Eliminates the need to turn off antivirus protection by dedicating the CPU need for optimal gaming performance
- By dedicating CPU cores to the game, it reduces random CPU spikes which can slow down the game

For more information, see See "Learn more about Game Optimizer" on page 79..

Note: All critical Norton protection features that are involved in protecting your computer from viruses and other security threats run in the background without interrupting your gaming experience.

Configure Norton for optimal gaming experience

1. Start Norton.
2. In the **My Norton** window, in the center pane, click the lightening icon.
3. In the **Gaming Dashboard**, click **Manage Optimization**.
4. In the **Game Optimizer** window, configure the following settings:
   - **Restrict resource usage for user processes**: Turn on this option to restrict CPU usage for all user-initiated processes.

- **Restrict resource usage for system processes**: Turn on this option to restrict CPU usage for all operating system-initiated processes.
- **Automatically set power plan to Max Performance**: Turn on this option to switch to the high performance power plan setting on Windows. Game Optimizer creates a custom Windows power plan settings to maximize gaming performance. This power plan is available only when the gaming session is in progress. After the gaming session ends, the power plan defaults to the original setting.
  Norton recommends that you keep this option turned on for better gaming experience.
- **Optimized Games**: Lists the games that are optimized by Game Optimizer.

Turn off Game Optimizer

By default, Game Optimizer is turned on. You can turn off Game Optimizer if you do not want it to enhance your gaming experience. Norton recommends that you keep this feature turned on for better gaming experience.

Turn Game Optimizer off or on

1. Start Norton.
2. In the **My Norton** window, on the left pane, slide the **Game Optimizer** switch to enable or disable the feature.

Turn Game Optimizer off or on from notification area

- In the notification area on the Windows taskbar, right-click the Norton icon, and do one of the following:
  - To turn off Game Optimizer, click **Turn off Game Optimizer**.
  - To turn on Game Optimizer, click **Turn on Game Optimizer**.

[1]Game Optimizer is only available on Windows (excluding Windows 10 in S mode, Windows running on ARM processor) with four or more core processors.

[2]Automatically detects games based on Full-Screen Detection mode with high CPU usage, as well as use of a game launcher[3], if the user adds a game manually, or if it has been detected previously.

[3]Game Launchers we currently monitor for as of April 2021 are: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Learn more about Game Optimizer

Game Optimizer[1] is patented technology for multi-core CPU PCs. It provides an immersive game experience by reducing performance interruptions while still maintaining your computer's security. By isolating non-essential applications to a single CPU core, it allows the rest of the CPUs to be allocated to game.

Game Optimizer helps improve your gaming experience by doing the following:

- Optimizes CPU performance for smoother gaming
- Isolates non-essential applications to a single CPU core so that the rest of the CPU can be allocated to game for better performance
- Automatically detects games[2]
- Lets you add games or select games you do not want to optimize
- Increases frames per second (FPS) and reduces latency
- Eliminates the need to turn off antivirus protection by dedicating the CPU need for optimal gaming performance
- By dedicating CPU cores to the game, it reduces random CPU spikes which can slow down the game

The minimum background activities also ensure higher performance of your computer which is ideal for gaming. After you end your gaming session, Norton 360 for Gamers resumes all the suspended activities to run in the background.

Note: Your computer's processor must be minimum four cores for Game Optimizer to work.

Game Optimizer starts the optimization when you start a gaming application and continues until you exit the game. Optimization is paused if you exit the full screen mode when the gaming session is active. For example, if you press **Alt + Tab** to access any other running program, it exits game optimization and removes the restrictions. However, when you get back to gaming, it continues the game optimization and restricted programs do not get access to CPU usage.

Note: All critical Norton protection features that are involved in protecting your computer from viruses and other security threats run in the background without interrupting your gaming experience.

You can verify the status of Game Optimizer in the notification area of the taskbar. The Norton product icon in the notification area displays a green lightening icon when Game Optimizer is enabled. When you turn off Game Optimizer, the color changes to gray.

The Gamer Dashboard displays the status of Game Optimizer, optimization status of recently played games, and access to the Game Optimizer settings. You can use the toggle switch to enable or disable optimization for the recently-played games.

Note: The Game Optimizer feature is available only in Norton 360 for Gamers.

---

[1]Game Optimizer is only available on Windows (excluding Windows 10 in S mode, Windows running on ARM processor) with four or more core processors.

[2]Automatically detects games based on Full-Screen Detection mode with high CPU usage, as well as use of a game launcher[3], if the user adds a game manually, or if it has been detected previously.

[3]Game Launchers we currently monitor for as of April 2021 are: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Manually add games to the Optimized Games list

Game Optimizer[1] is patented technology for multi-core CPU PCs. It provides an immersive game experience by reducing performance interruptions while still maintaining your computer's security. By isolating non-essential apps to a single CPU core, it allows the rest of the CPUs to be allocated to game. It automatically checks the internal list of known games to detect gaming applications.[1,2] However, if it has not automatically detected a specific game, you can manually add the game to the **Optimized Games** list.

In addition, you can also remove games from the **Optimized Games** list if you do not want Norton 360 for Gamers to enhance the performance for those games.

Note: When you remove a specific game from the **Optimized Games** list, the game is no longer optimized and can impact your gaming experience with that game.

Add a game to the Optimized Games list

1. Start Norton.
2. In the **My Norton** window, in the center pane, click the lightening icon.
3. In the **Gaming Dashboard**, click **Manage Optimization**.
4. In the **Game Optimizer** window, next to **Optimized Games**, click **Add**.
5. Navigate and select the gaming program you want Norton to optimize.

Remove a game from the Optimized Games list

1. Start Norton.
2. In the **My Norton** window, in the center pane, click the lightening icon.
3. In the **Gaming Dashboard**, click **Manage Optimization**.
4. In the **Game Optimizer** window, under **Optimized Games**, disable the switch next to the gaming program you want to remove.

[1]Game Optimizer is only available on Windows (excluding Windows 10 in S mode, Windows running on ARM processor) with four or more core processors.

[2]Automatically detects games based on Full-Screen Detection mode with high CPU usage, as well as use of a game launcher[3], if the user adds a game manually, or if it has been detected previously.

[3]Game Launchers we currently monitor for as of April 2021 are: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

Chapter 4

Find additional solutions

This chapter includes the following topics:

Uninstall Device Security on Windows

Follow the instructions below to uninstall your Device Security app from your computer.

Uninstall Device Security from Windows

1. Press the **Windows + R** keys to open the **Run** dialog box.
2. Type `appwiz.cpl` and press **Enter**.
3. In the list of currently installed programs, select your Norton product, and then click **Uninstall/Change**.
4. Follow the on-screen instructions.

   Device Security is not fully uninstalled until you restart your computer.

Disclaimers