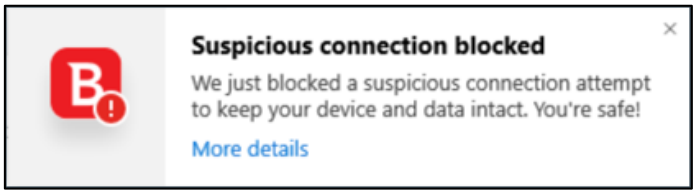
How to stop “Suspicious connection blocked” notifications



The “Suspicious connection blocked” notification is triggered by Bitdefender’s Online Threat Prevention module whenever there is an attempt to access an HTTPS domain that has security certificate issues. Unlike HTTP (Hypertext Transfer Protocol), HTTPS (safer HTTP Secure standard, HTTPS) is encrypted using Transport Layer Security (TLS), securing communications between your computer and the websites you visit.

HTTPS is indicated by the small lock symbol that appears in front of the address line whenever you visit a website. The padlock usually means the site has a valid HTTPS certificate, the site domain is verified to match the name on the certificate, and the connection to the website is encrypted. In other words, the information exchanged between you and that domain is not in clear text but encrypted. Unsafe domains are external links to websites that do not have a security certificate issued by a trusted certificate authority, have an unmatching or expired security certificate, and could contain phishing, malware, or unwanted software.

In this article, we will show you how to find out which website raises an alarm about “Suspicious connection blocked” and how to proceed if further action is needed.

Find out what triggers the “Suspicious connection blocked” notification

Notifications are an important tool in monitoring and managing your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if threats or vulnerabilities were found on your computer, etc. Additionally, you can take further action if needed or change actions taken by Bitdefender.

To find the site Bitdefender alerts you about, click on “More details” when the message “Suspicious connection blocked” is displayed in the corner of the screen.

If the message box flashes too quickly and you can’t open it in time, go to your notification log: access the Notifications log:

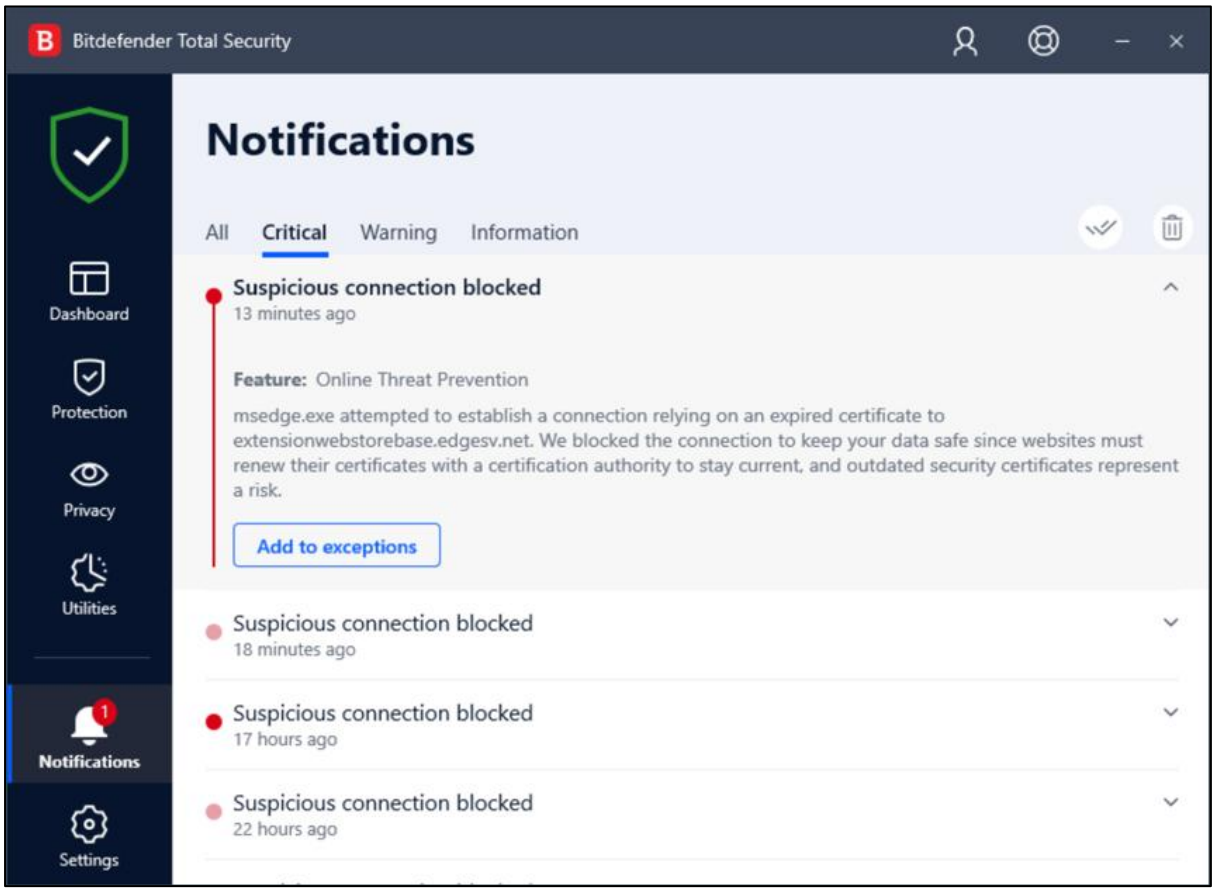
1. Click on Notifications 

in the menu on the left-hand side of the Bitdefender interface. Every time a critical event occurs, a counter can be noticed on the bell icon.

2. Depending on type and severity, Bitdefender notifications are grouped into three tabs Critical, Warning, and Information. Go to the Critical tab to find more details about the generated event.

3. Click to expand the latest notification entitled “Suspicious connection blocked”. A short description appears, listing the following information:

- Date of notification (e.g. 13 minutes ago)
- Bitdefender feature that blocked the connection (e.g. Online Threat Prevention)
- Name of the process trying to connect to the suspicious link (e.g. msedge.exe – Microsoft Edge)
- The reason why the connection was blocked (e.g. expired certificate)
- The URL blocked by Bitdefender due to certificate issues (e.g. *extensionwebstorebase.edgesv.net*)



In the example above, you will notice that Bitdefender’s Online Threat Prevention feature blocked 13 minutes ago a suspicious msedge.exe (Microsoft Edge process) connection to *extensionwebstorebase.edgesv.net*. The connection was blocked because the site certificate is expired.

That’s a simple method to find out which URL triggers the “Suspicious connection blocked” notification.

What to do when the “Suspicious connection blocked” notification appears

This alert appears when you try to visit a secured website (HTTPS) with an invalid security certificate. It tends to be websites with lots of ads, such as news websites, and analytics companies with an expired certificate trying to establish a connection. If you wish, you can check their SSL certificates at https://www.sslshopper.com/.

To avoid any security risk, it is advisable to exit right away the page you are about to visit. It’s that easy. No further action is required on your part.

Instead, if you do not navigate to the website indicated in Bitdefender notifications or if the site certificate appears to be valid, but you still get pop-ups about blocked suspicious connections, the problem might be your device. Try these preliminary steps:

1. Make sure your computer date and time are correct. If the PC’s clock is set so that the date/time is later than the expiry date of the web server’s SSL certificate, you will encounter security certificate errors.
2. Open your Bitdefender security solution and run a Full System Scan to check your PC for threats. Wait until the scan ends, then restart Windows.

If the situation remains unchanged, your browser most likely connects to these URLs either through allowed notifications or third-party toolbars/extensions. Here are the next steps:

Web Browser solution

To resolve this issue, uninstall any unknown programs and browser add-ons from your computer, revoke Web Push permissions for the sites allowed to display messages on your screen, reset your browser and install an ad blocker. For detailed instructions, read – Remove adware, pop-ups, and browser redirects from your PC.

Email app solution

If you use an email client such as Microsoft Outlook or Mozilla Thunderbird, clean up your inbox by deleting emails from unknown senders. Delete all SPAM/Junk as well. Finally, empty the trash on your email account.

Add to Bitdefender exceptions

Alternatively, if you wish to access a website with a problematic SSL certificate at your own risk, you can add an exception for that address in Bitdefender. For detailed instructions, read – Whitelist a safe website on Windows.

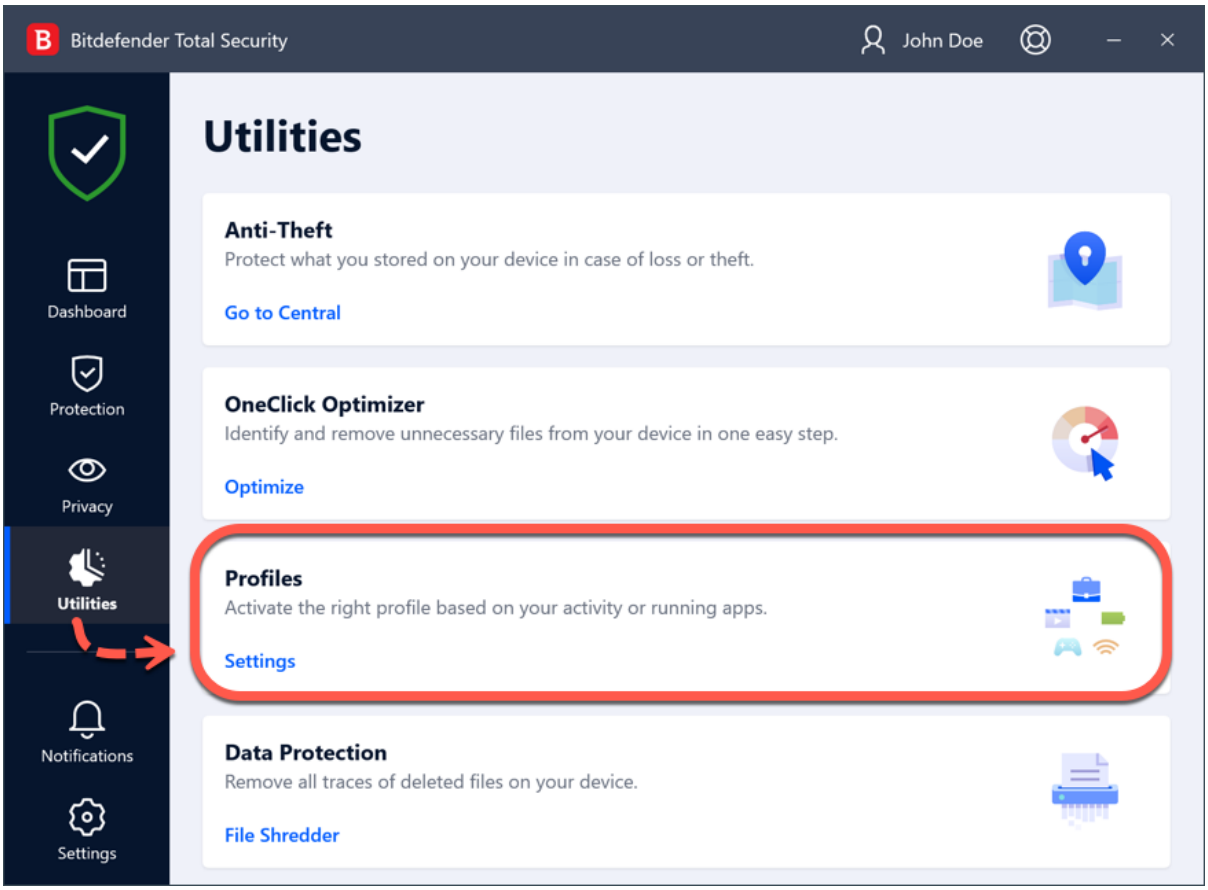
Turn off “Suspicious connection blocked” notifications

Notifications can appear whenever other vulnerabilities or malware is detected, to alert the user of potential threats. If a notification is critical to the security of the system, it cannot be disabled, but the source of the notification can be investigated by the support team, to determine what is causing it and to what extent it can be mitigated.

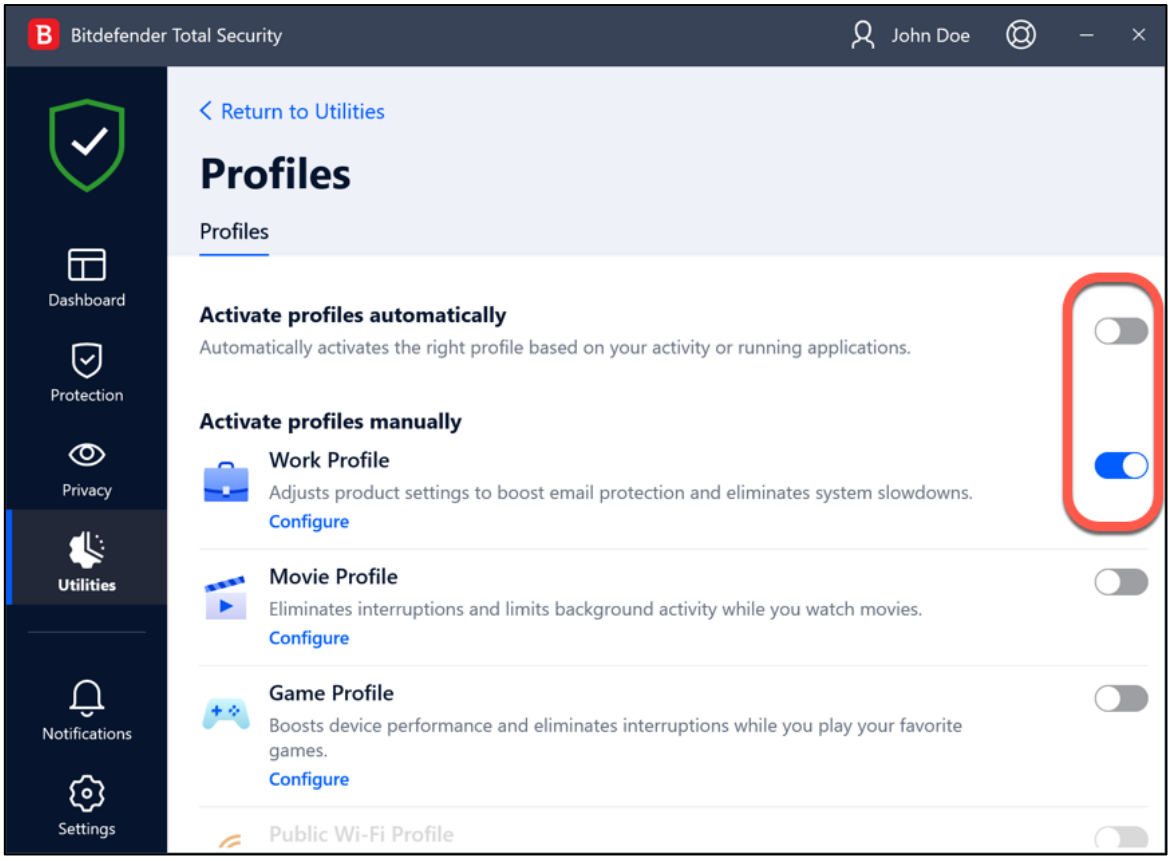
If you are only trying to hide the “Suspicious connection blocked” notifications and nothing more, you may want to activate a Bitdefender Profile: Work, Movie, or Game. While in use, profiles also stop all notifications from being displayed on the screen – including Bitdefender notifications.

For instance, to enable the work profile and to customize it so that it does not interfere with other background processes such as Windows updates:

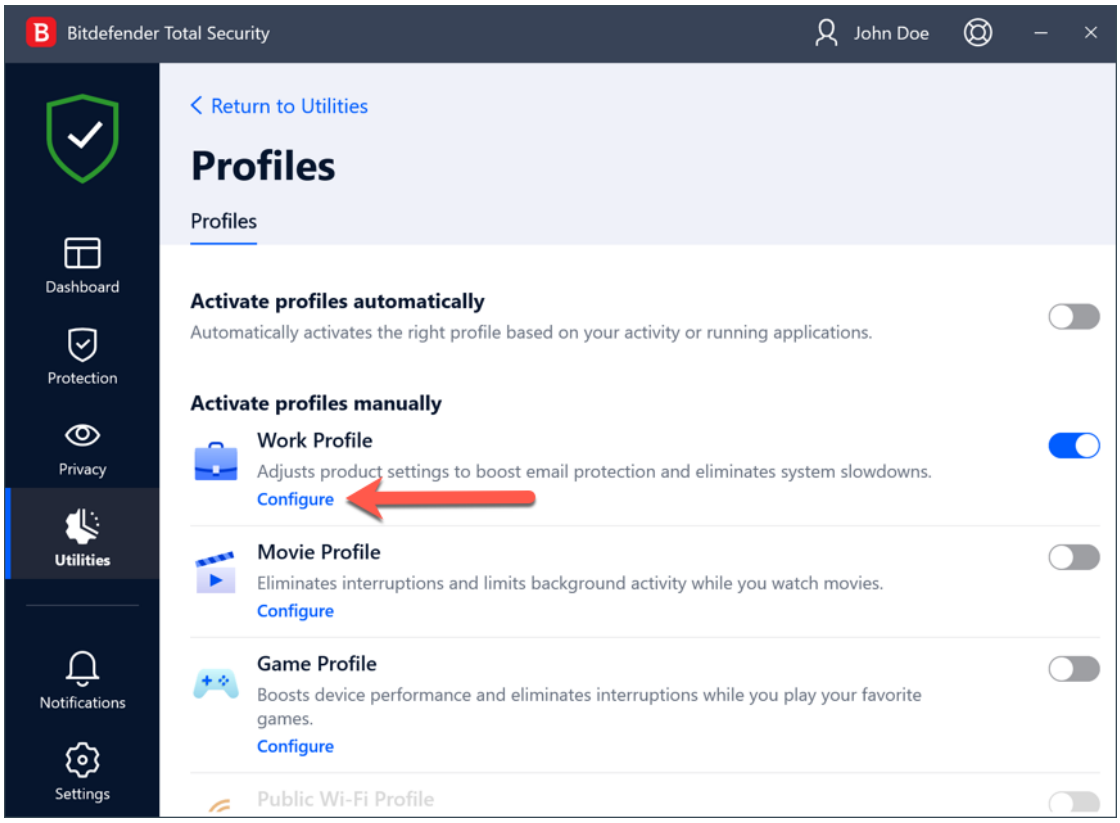
1. Bring up Bitdefender and click on “Utilities” on the left-hand side menu. In the Profiles pane, click on Settings.



2. In the Profiles tab, set:
   - Activate profiles automatically to OFF
   - Work Profile to ON



3. Next, click on “Configure” in the Work Profile panel to start customizing its settings.



4. Uncheck all available boxes in the pop-up window, then press the “Save” button:
    - Optimize product settings for Work profile
    - Postpone background programs and maintenance tasks
    - Postpone Windows Automatic Updates