A Guide to Bitdefender’s Cryptomining Protection

What is Cryptomining Protection?

Bitdefender’s Cryptomining Protection feature defends Windows computers against the growing threat of unauthorized crypto-mining activities, a malicious practice that exploits a user’s resources and electricity to generate revenue for attackers. This feature is built into Bitdefender security solutions for Windows, accessible through subscription plans:

- Bitdefender Total Security
- Bitdefender Premium Security
- Bitdefender Premium Security Plus
- Bitdefender Ultimate Security
- Bitdefender Ultimate Security Plus

Video

- Meet Cryptomining Protection: Stop Hidden Cryptocurrency Miners with Bitdefender

Prerequisites

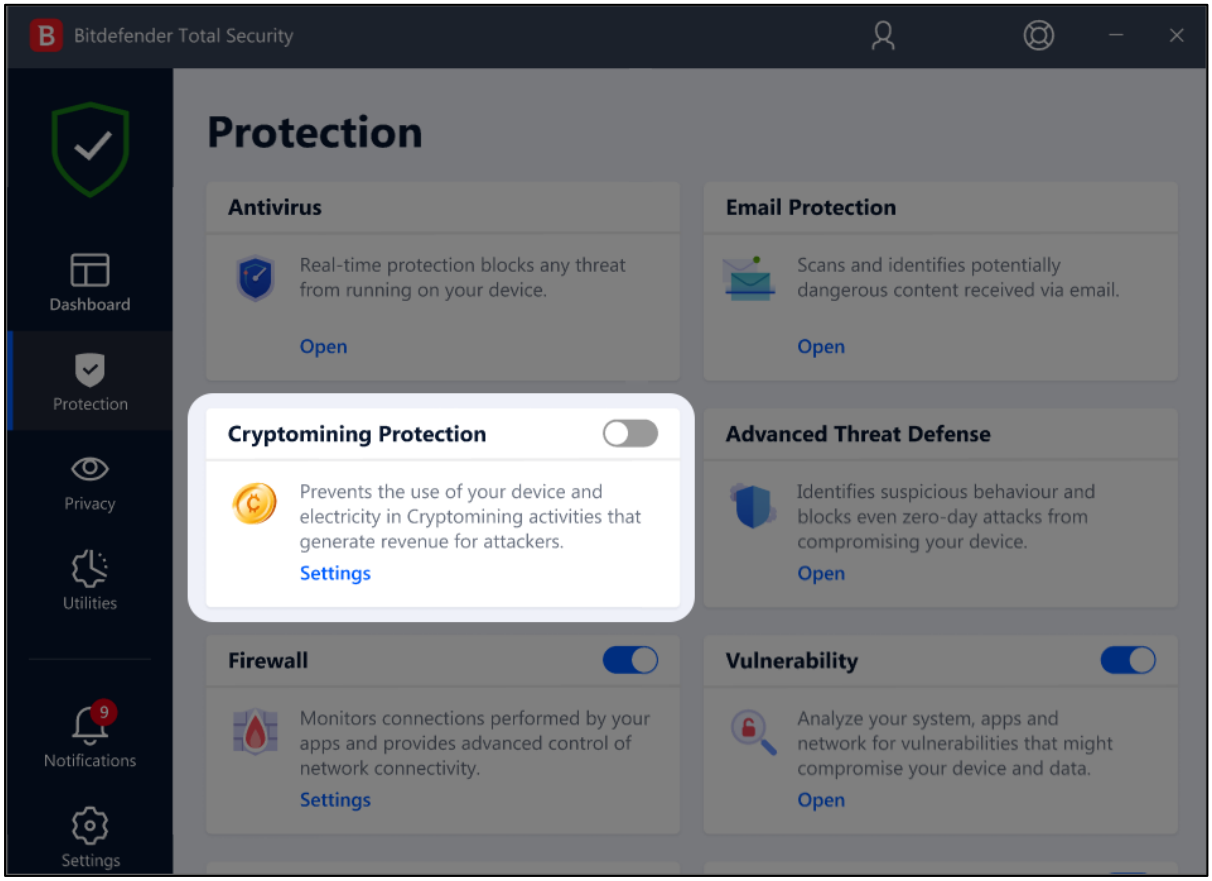
Cryptomining Protection relies on:

- **Bitdefender Shield** (Protection > Antivirus > Advanced > Bitdefender Shield)
- **Web Attack Prevention** (Protection > Online Threat Prevention > Web Attack Prevention)

Users are warned if either of these Bitdefender features is disabled, ensuring comprehensive protection.

Enabling Cryptomining Protection

Located within the **Protection** section, **Cryptomining Protection** is disabled by default, ensuring that users have control over its activation via the on/off switch.



Operating modes

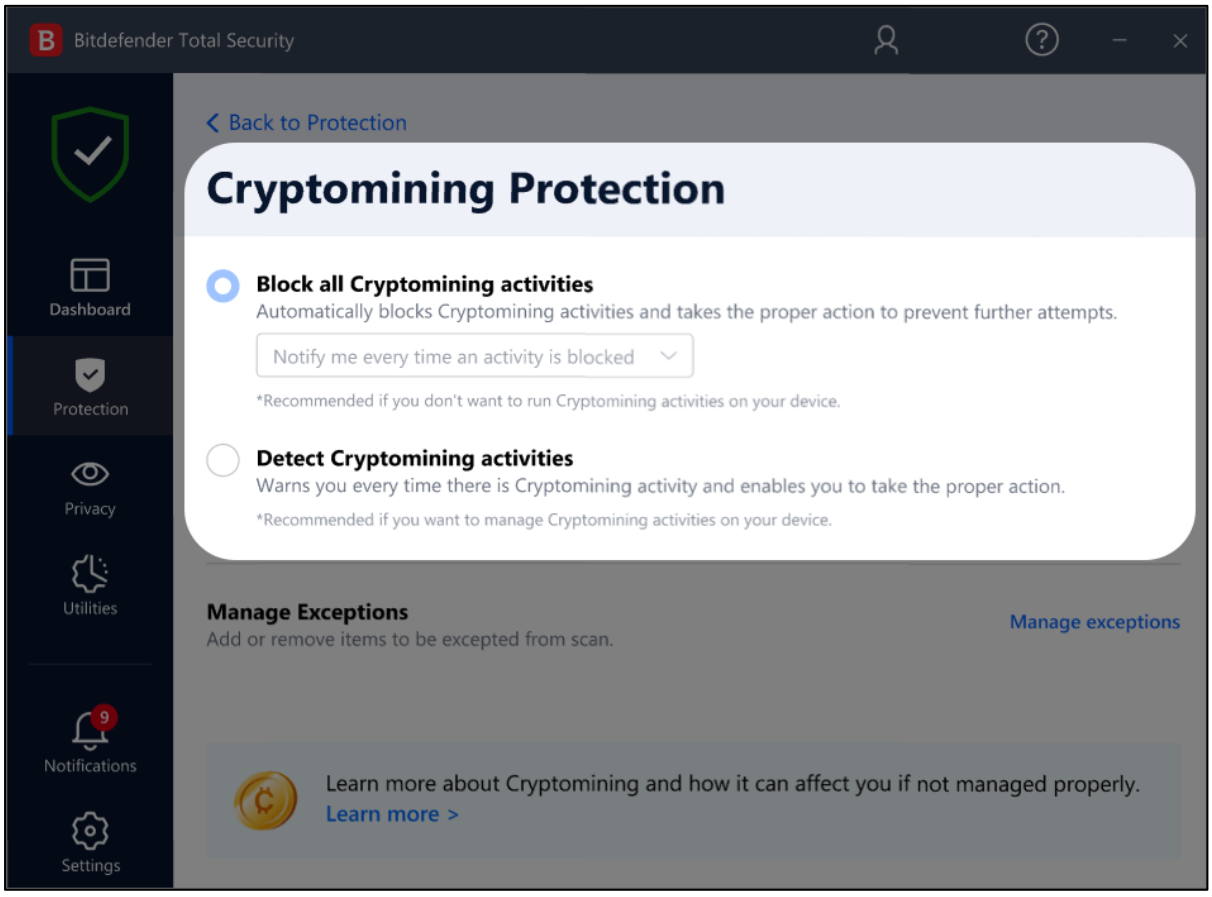
Once enabled, the Cryptomining Protection feature operates in 2 distinct states, each tailored to the user's preferences:

1. **Block all Cryptomining activities**

- Ideal for users who have no intention of engaging in crypto-mining activities.
- Bitdefender automatically blocks any crypto-mining activities and takes necessary actions to prevent further unauthorized attempts.
- Users can customize notification settings, choosing between receiving notifications for each detection or opting for a summary of detections.

2. **Detect Cryptomining activities**

- Suited for users actively involved in their own crypto-mining activities but wish to monitor and control any unauthorized attempts.
- Bitdefender issues alerts whenever a crypto-mining activity is detected and requires user input to determine the appropriate action.



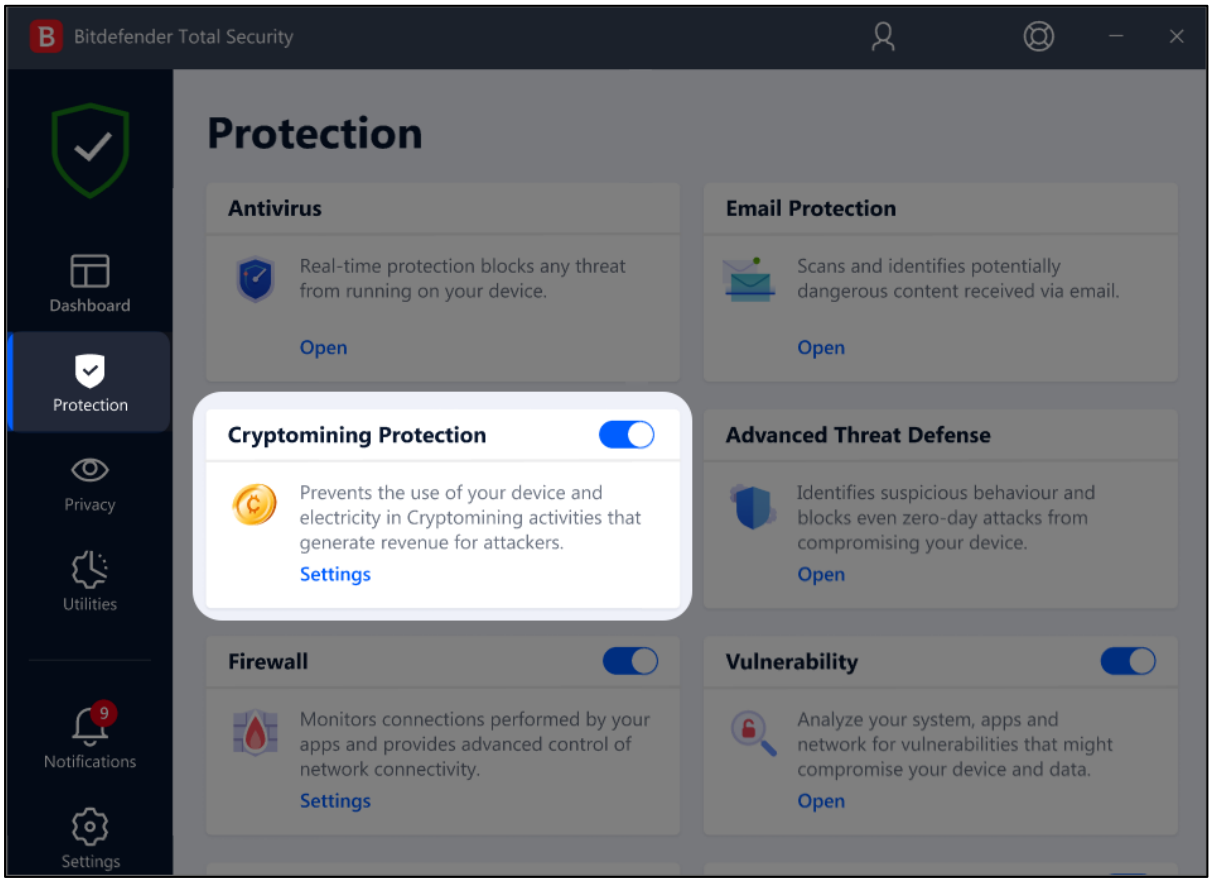
Exceptions

Users have the flexibility to create exceptions through a dedicated tab in the Exceptions area. These exceptions can be specified for applications, with the added capability of defining specific command lines. However, exceptions can also be established without the need for providing such detailed parameters, offering a balance between customization and simplicity.

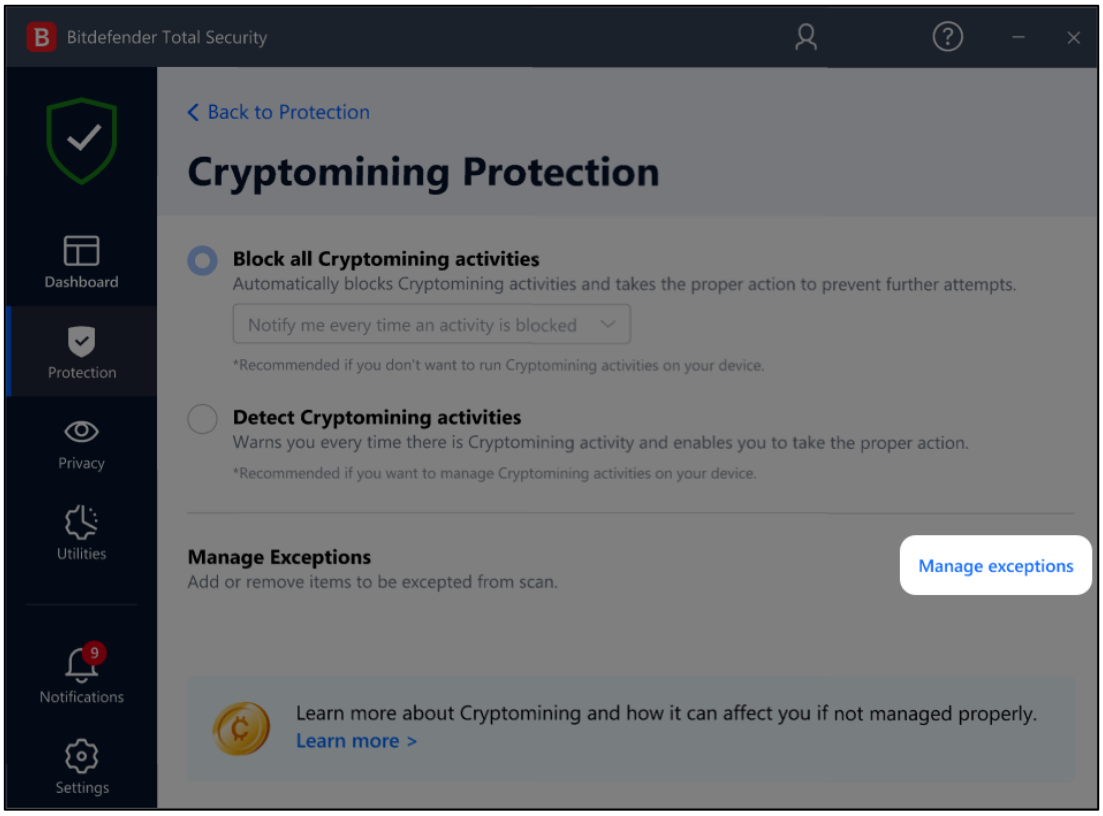
To add an exception:

1. Click **Protection** on the left-hand side menu on the Bitdefender interface.

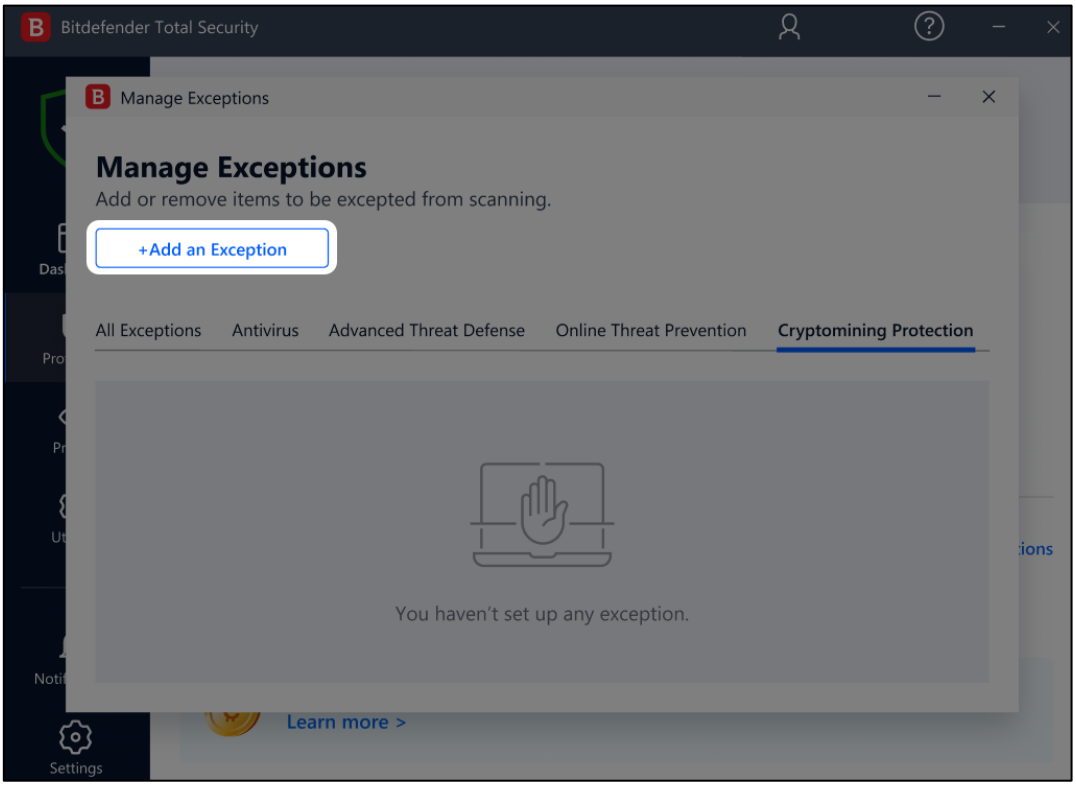
2. In the **Cryptomining Protection** pane, click **Settings**.



3. Click the **Manage exceptions** option.



4. Next, click the **Add an Exception** button.



5. A new window will open where you can manually exclude applications, URLs, and IP addresses.

Command line exception tips:

 • The “Add process command line” option becomes available after selecting or typing an app’s path.

• Multiple command lines can be added for the same process.

• The “Add new command line” option becomes active only when there is text in the input field above.

• When excluding multiple command lines for the same process (whether within the same exception session or in separate sessions), the cmd lines will be grouped under the same exception in the exceptions list.

6. Finally, click the **Save** button. The new rule is added to Cryptomining Protection exceptions list.

To remove an exception, simply click the trash can icon next to it.