

ESET Micro Updates

User guide

[Click here to display the online version of this document](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Micro Updates was developed by ESET, spol. s r.o.

For more information visit <https://www.eset.com>.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Technical Support: <https://support.eset.com>

REV. 4/15/2024

1 Introduction	1
2 Requirements	1
3 Setup and maintenance	2
4 Download Micro update packages	3
5 Alternatives to ESET Micro Updates	4
6 Help and support	5
7 Terms and conditions	6

Introduction

ESET Micro Updates is intended for customers who manage ESET products in closed networks without the internet connection or with a limited internet connection. By default, ESET client workstations check for updates on an hourly basis. ESET Micro Updates provide a user with an option to manually download and distribute updates across the whole network. The client workstations can either obtain these updates over the internet directly from ESET's update servers, or from a locally managed update source.

ESET Micro Updates is suitable for industries with insufficient internet access (GPRS, satellite, radio) as well as those with strict update policies. In such environments, it is still important to keep security updates, and detection engine with the newest algorithms up-to-date, while balancing the cost and availability of an internet connection.

Limited modules availability



To save bandwidth ESET Micro Updates does not provide updates for all modules, only detection engine (em000 – em005; loader, perseus, engine, archives, heuristics, cleaner). It does not contain an update of any other modules to save as much bandwidth as possible. This means incomplete protection and may cause security warnings from ESET products.

How to use

1. Download the PDF version of this user guide if needed.
2. Verify the [Requirements](#).
3. Proceed with [Setup and maintenance](#).

For more information, read about [Alternatives to ESET Micro Updates](#). If you need additional assistance, see [Help and support](#).

Requirements

License requirements

- Valid ESET license (not expired)
- [Legacy license credentials](#) to access Micro update packages (ESET-issued Username and Password)
- ESET Micro Updates must be enabled on your ESET license. [Request the activation of ESET Micro Updates for your ESET license](#).

More information about licensing



To buy ESET license [visit the ESET Store page](#).

For more information on ESET licensing, visit [Licensing FAQ](#).

To recover lost license details, type your email address in [License management support site](#).

ESET products supported

- ESET Micro Updates are currently supported for all ESET server and endpoint desktop products, however, ESET product versions receiving Micro update packages should be supported. See [ESET End of Life policy \(Business products\)](#) for more information.

Minimal modules installer not compatible

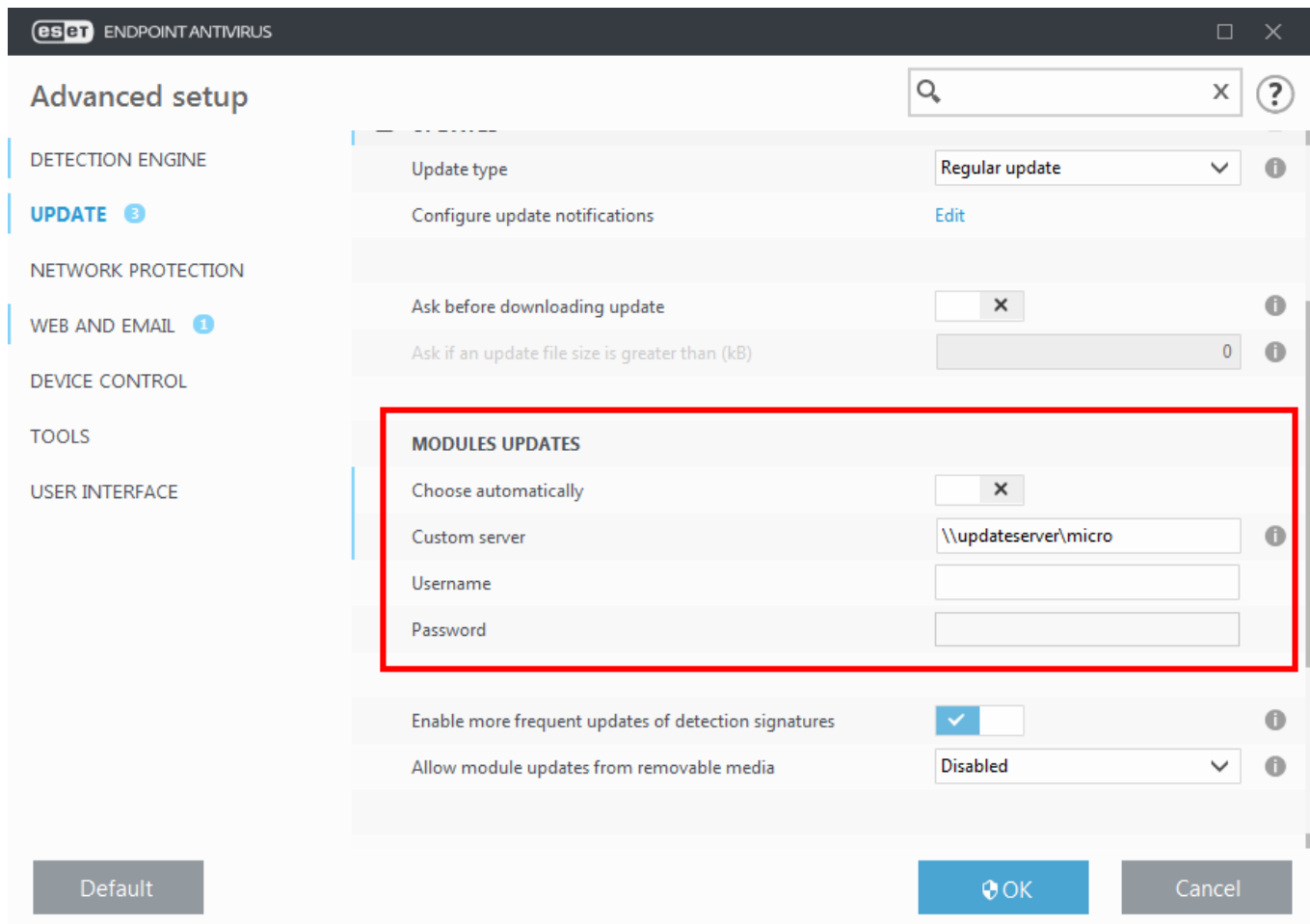


ESET endpoint products for Windows (9.x and later) come with a minimal modules installer. Applying Micro update packages will work after the initial successful update from ESET update servers or with [full MSI installers](#).

Setup and maintenance

Initial setup

1. At first, you will need to download a package with a full update of the detection engine and scanner modules. Open the [Download Micro update packages](#) section and according to the version of your product and bit version of your system, download a full Micro update package.
2. On a server in a local network, that will not always be connected to the internet, configure a shared network folder `\\updateserver\micro`. The folder should be empty. Note the UNC path format for shared folders.
Alternatively, use a local network address like `http://updateserver.local/micro/`.
3. Extract the contents of downloaded full Micro update package to folder `\\updateserver\micro`. Preserve the folder structure in the archive and do not create any new folders or files.
4. After extraction, shared folder should look like `\\updateserver\micro\dll*.nup` and `\\updateserver\micro\dll\update.ver`
5. On a client computer connected to the same network, configure the update profile for ESET endpoint products to update from `\\updateserver\micro`.
 - [ESET endpoint products for Windows \(7.3 and later\)](#)
 - [ESET Endpoint Antivirus for macOS 7.x](#)
 - [ESET endpoint products for Mac 6.x](#)
 - [ESET Endpoint Antivirus for Linux \(7.x and later\)](#)



6. After you apply new update profile, run an update on ESET product. The product is now updated with the latest detection engine and scanner modules.
7. For the following week, continue with steps in **Weekly maintenance**.

Weekly maintenance

1. Download a package with an incremental update of detection engine and scanner modules. Open the [Download](#) section of this manual and according to the version of your product and bit version of your system, download a weekly Micro update package.
2. Navigate to network folder `\\updateserver\\micro` and remove all of its contents. The folder is empty now.
3. Extract the contents of the downloaded weekly Micro update package to the folder. Preserve the folder structure as in the archive and do not create any new folders or files.
4. Check for updates in ESET products.
5. For the following week, repeat the Weekly maintenance.

Download Micro update packages

Before downloading, ensure all [Requirements](#) are met.

Missed weeks?

- ✓ If an update is missed for three weeks, you need to install three weekly updates consecutively. In case of an update is missed for ten weeks, you need to install two 4-week updates and two weekly updates consecutively. After that, you can download regular weekly updates as usual.



First use

Before the weekly Micro updates can be used, the full Micro updates package must be applied first.

ESET Micro Updates are generated every Friday as differential updates containing detection engine updates changed from last week. If you miss two consecutive updates for any reason, and thus regular weekly differential update would not be possible, you need to install two missing weekly updates before installing the latest update. There is still a possibility to download a 4-week differential update (~13 MB). A 4-week update package consists of four weekly updates but has usually smaller size than four weekly update packages, so it is less demanding on the internet connection.

ESET Windows products (64-bit)

- [Download weekly Micro update package](#) - Incremental update of detection engine. (Size: ~1 MB)
- [Download 4-week Micro update package](#) - Incremental update of detection engine. (Size: ~13 MB)
- [Download full Micro update package](#) - Full update of detection engine. (Size: ~75 MB)

ESET Windows products (32-bit)

- [Download weekly Micro update package](#) - Incremental update of detection engine. (Size: ~1 MB)
- [Download 4-week Micro update package](#) - Incremental update of detection engine. (Size: ~13 MB)
- [Download full Micro update package](#) - Full update of detection engine. (Size: ~75 MB)

ESET Linux products (64-bit)

- [Download weekly Micro update package](#) - Incremental update of detection engine. (Size: ~1 MB)
- [Download 4-week Micro update package](#) - Incremental update of detection engine. (Size: ~2 MB)
- [Download full Micro update package](#) - Full update of detection engine. (Size: ~75 MB)

Archive of earlier Micro update packages

- Archive links can be used if you do not want to apply the full Micro update package again. The archive link is in the following format, but only for each Friday starting from April 2019:
YYYYMMDD/weekly_(eav64|dll32|dll64)_(nanos|nanos4|levels).rar
- For example, 4-week dlls 32-bit for Friday, February 17, 2023:
https://download.eset.com/download/engine/archive/20230217/weekly_dll32_nanos4.rar
- For example, weekly dlls 64-bit for Friday, February 17, 2023:
https://download.eset.com/download/engine/archive/20230217/weekly_dll64_nanos4.rar
- Update packages for Linux products version 7 and later were added in March 2021.



Provision of ESET Micro Updates is subject to the End of Life policy, which is available on https://go.eset.com/eol_business. Updates might not be provided after the ESET product or any of its features reach the End of Life date defined in the End of Life policy.

Alternatives to ESET Micro Updates

Apart from using ESET Micro Updates to receive module updates, the following alternatives are available:

ESET Bridge (recommended)

Useful when internet connection is available and there are a lot of endpoints with ESET installed in the network.

ESET Bridge (replacing Apache HTTP Proxy, as a component of ESET PROTECT) downloads and caches:

- Detection engine updates
- Activation tasks - communication with activation servers and caching of license requests
- ESET PROTECT repository data
- Product component updates


Cached data is distributed to endpoint clients on your network. Caching can significantly decrease internet traffic on your network.

- [More information and setup](#)

Mirror Tool

The [Mirror Tool](#) is necessary for offline detection engine updates but initial download takes more than 1 GB.

When to start using Mirror Tool?

 If you have an offline environment, meaning the computers in your network do not connect to the internet for a prolonged period of time (months, a year) the Mirror Tool is the only way to distribute product module updates, because it downloads all available Level and Nano updates after each new update request if there is a new update available.

- [More information and comparison with Apache HTTP Proxy](#)

To set up an update mirror using Mirror Tool and configure clients in your network to distribute the update across your network follow instructions in our Knowledgebase and Online Help articles:

1. Create update mirror:

- [ESET PROTECT \(8.x and later\)](#)
- [ESET endpoint products for Windows \(7.x and later\)](#)

2. Configure clients to access update mirror:

- [ESET endpoint products for Windows \(7.x and later\)](#)
- [ESET endpoint products for Mac](#)

Help and support

The [ESET Knowledgebase](#) is a searchable repository of support articles designed to help you resolve issues and answer questions.

The [ESET user Forum](#) is monitored by ESET staff and allows ESET users to share issues they are having and find solutions.

The [ESET Knowledgebase video channel](#) contains video walkthroughs of common procedures for ESET products.

Visit [ESET Support News](#) and Customer Advisories for the latest announcements about ESET product features and upgrades.

[Stay informed about new product releases](#) by visiting our Changelogs page.

You can [open a case with ESET Technical Support](#) at any time if you are not able to resolve an issue or find the answer to your question.

Terms and conditions for minimal weekly updates for ESET products

IMPORTANT



Please read the terms and conditions set out below carefully prior to enabling minimal weekly updates functionality. **THROUGH ENABLING MINIMAL WEEKLY UPDATES FUNCTIONALITY YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS.**

Under the terms and conditions executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, Business Registration Number: 31333532 or another company from the ESET Group (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use minimal weekly updates functionality for ESET products licensed to You.

1. The terms not defined herein shall have the meaning assigned to them in the End User License Agreement.
2. Minimal weekly updates are Updates designated to minimize the size of download via expensive satellite internet connection. As such, minimal weekly updates are compromise between keeping the most important part of Software as up-to-date as practical and not updating the Software at all.
3. Minimal weekly updates are designed to maintain only the most important functionalities of the Software and in no case replace the regular Updates.
4. Minimal weekly updates could be enabled only by End User and are downloaded from dedicated servers.
5. With minimal weekly updates enabled, the performance of Software could not be optimal and does not offer the best protection which fully updated Software can offer.
6. It shall be explicitly understand that Software with minimal weekly updates enabled could not be able to detect some Infiltrations which would be detected with regular Updates enabled. In such computer system on which the Software is installed could be eventually compromised by Infiltration.
7. End User is advised to update the Software from default set of update servers to receive regular Updates as soon as possible. Only such Update ensures standard functionality of Software. After update from regular update server full scan of the computer system is strongly recommended.
8. **END USER DECLARATIONS.** AS THE END USER YOU ACKNOWLEDGE THAT THE MINIMAL WEEKLY UPDATES ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE MINIMAL WEEKLY UPDATES WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE MINIMAL WEEKLY UPDATES WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE OPTING FOR MINIMAL WEEKLY UPDATES TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE USE AND RESULTS OBTAINED FROM IT.