

ESET Tech Center

Knowledgebase > Endpoint Solutions > Disable ESET Outlook Plug-in on an endpoint computer in ESET PROTECT (Cloud)

Disable ESET Outlook Plug-in on an endpoint computer in ESET PROTECT (Cloud)

Steef | ESET Nederland - 2022-11-22 - Comments (0) - Endpoint Solutions

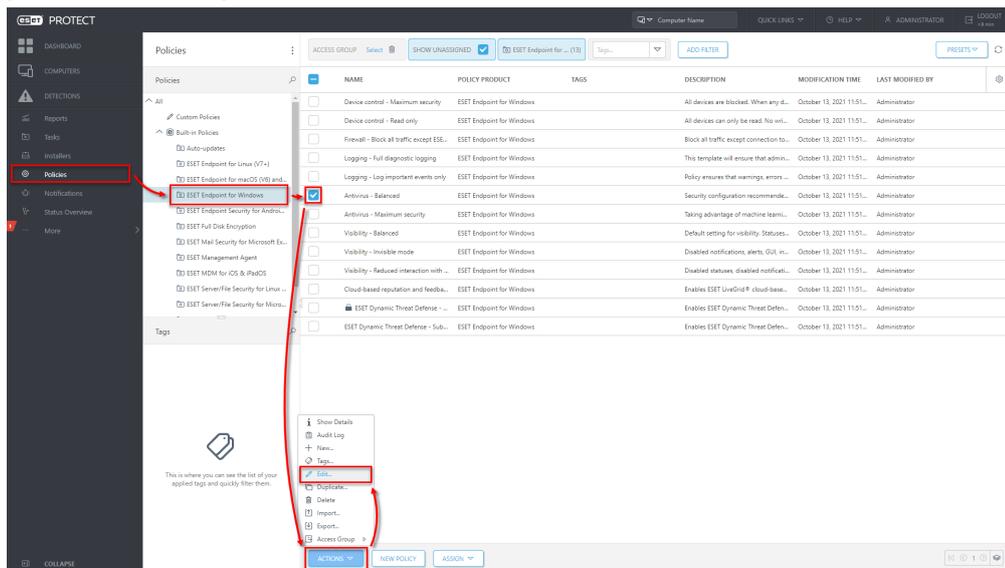
Issue

- You receive the following error message when starting Microsoft Outlook on an endpoint: "The Add-in 'ESET Outlook Plugin' (C:\PROGRA~1\ESET\ESETNO~1\EPLGOU~1.DLL) cannot be loaded and has been disabled by Outlook. If no update is available, please uninstall the Add-in."
- The error message above may occur on a computer with multiple user profiles after an upgrade, reinstall, or a failed uninstall of ESET security product
- Performance issues in outlook, unstable email client, compatibility issues with other plugins
- Duplicate emails in mailbox
- Disable the ESET Outlook Add-in

Always upgrade to the latest Endpoint version first before disabling the outlook integration and test if latest version solves Outlook related issues!

Solution

1. Open the ESET PROTECT (Cloud) Web Console in your web browser and log in.
2. Click **Policies**, select the check box next to the policy (baseline or customer policy) you want to modify, and click **Actions** → **Edit**.



3. Click **Settings**, expand **Web and Email** (1) and click **Email client protection** (2).
4. In the **Email Clients Integration** section, click the slider bar next to **integrate into**

Microsoft Outlook (3) to disable it.

- In the **Email Clients** section, click the slider bar next to **Enable email protection by client plugin (4)** to disable it.
- In the **Email Protocols** section, click the slider bar next to **Enable email protection by protocol filtering (5)** to disable it.
- In the **Antispam protection** section, click the slider bar next to **Enable email client antispam protection (6)** to disable it.

The screenshot displays the Microsoft Defender for Endpoint console interface. On the left, a navigation pane shows 'WEB AND EMAIL' selected, with 'Email client protection' highlighted. The main content area is divided into several sections:

- EMAIL CLIENT INTEGRATION:** The 'Integrate into Microsoft Outlook' option is selected, indicated by a red circle with the number 3.
- SPECIAL SETTINGS:** Includes 'Attachment handling optimization' and 'Advanced email client processing', both with version indicators (≥ 9.1) and checkmarks.
- EMAIL CLIENTS:** The 'Enable email protection by client plugins' option is selected, indicated by a red circle with the number 4.
- EMAIL TO SCAN:** Lists 'Received email', 'Sent email', 'Read email', and 'Modified email', each with a checkmark.
- ACTION TO BE PERFORMED ON EMAILS WITH DETECTIONS:** Includes 'Action' (set to 'Move email to folder') and 'Folder' (set to 'Detected Items').
- EMAIL PROTOCOLS:** The 'Enable email protection by protocol filtering' option is selected, indicated by a red circle with the number 5.
- IMAP SCANNER SETUP:** Includes 'Enable IMAP protocol checking' (checked) and 'Ports used by IMAP protocol' (set to 143).
- IMAPS SCANNER SETUP:** Includes 'Enable IMAPS checking' (checked) and 'Ports used by IMAPS protocol' (set to 585, 993).
- POP3 SCANNER SETUP:** Includes 'Enable POP3 protocol checking' (checked).
- ANTISPAM PROTECTION:** The 'Enable email client antispam protection' option is selected, indicated by a red circle with the number 6.
- MESSAGE PROCESSING:** Includes 'Add text to email subject' (checked), 'Text' (set to '[SPAM]'), 'Move messages to spam folder' (checked), 'Use the folder' (set to a dropdown), 'Folder' (set to a text input), 'Mark spam messages as read' (set to a dropdown), 'Mark reclassified messages as unread' (checked), and 'Spam score logging' (set to 'None').
- ANTISPAM ADDRESS LISTS:** A section at the bottom with a plus icon and a refresh icon.

- Click **Finish** to save your changes.

These settings will result in a disabled Outlook plugin and no warnings will be shown in the protection status of the Endpoint.