Contents

1. ESET Endpoint Security 7 ................................................................. 8
  1.1 What's new in version 7 ................................................................. 8
  1.2 System requirements .................................................................. 8
  1.3 Prevention ................................................................................... 9

2. Documentation for endpoints managed by ESET Security Management Center ..................................................... 11
  2.1 Introduction to ESET Security Management Center ................................................. 11
  2.2 Introduction to ESET Cloud Administrator ......................................................... 11
  2.3 Password protected settings ........................................................................ 12
  2.4 What are policies .............................................................................. 13
    2.4.1 Merging policies .......................................................................... 13
  2.5 How flags work ................................................................................ 13

3. Using ESET Endpoint Security by itself ...................................................... 15
  3.1 Installation methods ........................................................................ 15
    3.1.1 Installation with ESET AV Remover ................................................. 15
    3.1.1.1 ESET AV Remover ................................................................ 16
    3.1.1.2 Uninstallation using ESET AV Remover ended with error .............. 18
    3.1.2 Installation (.exe) .......................................................................... 18
    3.1.2.1 Change installation folder (.exe) .................................................. 20
    3.1.3 Installation (.msi) ........................................................................... 21
    3.1.3.1 Advanced installation (.msi) .......................................................... 24
    3.1.4 Installation via ESET Security Management Center (command line) ... 25
    3.1.5 Deployment using GPO or SCCM .................................................... 25
    3.1.6 Upgrading to a more recent version ................................................ 25
    3.1.7 Common installation problems ....................................................... 26
    3.1.7.1 Activation failed ...................................................................... 26
  3.2 Product activation ............................................................................ 26
  3.3 Computer scan ................................................................................ 27
  3.4 Beginner’s guide ............................................................................... 27
    3.4.1 The user interface .......................................................................... 27
    3.4.2 Update setup ................................................................................ 31
    3.4.3 Zones setup .................................................................................. 33
    3.4.4 Web control tools ......................................................................... 33

4. Work with ESET Endpoint Security .......................................................... 34
  4.1 Computer ....................................................................................... 36
    4.1.1 Detection engine .......................................................................... 37
    4.1.1.1 An infiltration is detected ............................................................ 38
    4.1.2 Shared local cache ........................................................................ 40
    4.1.3 Real-time file system protection .................................................... 40
    4.1.3.1 Additional ThreatSense parameters ........................................... 41
    4.1.3.2 Cleaning levels .......................................................................... 41
    4.1.3.3 Checking real-time protection .................................................... 42
    4.1.3.4 When to modify real-time protection configuration .................... 42
    4.1.3.5 What to do if real-time protection does not work ....................... 42
    4.1.3.6 Processes exclusions ................................................................. 43
    4.1.3.6.1 Add or Edit processes exclusions ............................................ 44
    4.1.4 Computer scan ............................................................................. 45
    4.1.4.1 Custom scan launcher .............................................................. 46
4.1.12.1 File extensions excluded from scanning

4.1.10 Document protection

4.1.11 Exclusions

4.1.11.1 Add or Edit exclusion

4.1.11.2 Path exclusion format

4.1.12 ThreatSense parameters

4.1.12.1 File extensions excluded from scanning

4.2 Network

4.2.1 Firewall

4.2.1.1 Learning mode

4.2.2 Network attack protection

4.2.2.1 IDS exceptions

4.2.2.2 Allowed services and advanced options

4.2.2.3 Suspected threat blocked

4.2.2.4 Network protection troubleshooting

4.2.3 Connected networks

4.2.4 Known networks

4.2.4.1 Known networks editor

4.2.4.2 Network authentication - Server configuration

4.2.5 Firewall profiles

4.2.5.1 Profiles assigned to network adapters

4.2.6 Application modification detection

4.2.6.1 Applications excluded from modification detection

4.2.7 Configuring and using rules

4.2.7.1 Firewall rules

4.2.7.2 Working with rules

4.2.8 Temporary IP address blacklist

4.2.9 Trusted zone

4.2.10 Configuring zones

4.2.10.1 Firewall zones

4.2.9 Trusted zone

4.2.8 Temporary IP address blacklist
4.5 Updating the program

4.5.1 Update setup

4.5.1.1 Update rollback

4.5.1.2 Program component update

4.5.1.3 Connection options

4.5.1.4 Update mirror

4.5.1.4.1 HTTP Server

4.5.1.4.2 Updating from the Mirror

4.5.1.4.3 Troubleshooting Mirror update problems

4.5.2 How to create update tasks

4.5.3 Solving problems with protocol filtering

4.5.3.1 Web and email clients

4.5.3.2 Web protocols

4.5.3.3 URL addresses list

4.5.3.3.1 Create new URL address list

4.5.3.4 How to add URL mask

4.5.3.5 Anti-Phishing protection

4.5.4 Web control

4.5.4.1 Rules

4.5.4.1.1 Adding Web control rules

4.5.4.2 Category groups

4.5.4.3 URL groups

4.5.5 Updating the program

4.6 Tools

4.6.1 Log files

4.6.1.1 Log filtering
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6.1.2 Logging configuration</td>
<td>137</td>
</tr>
<tr>
<td>4.6.1.3 Audit logs</td>
<td>138</td>
</tr>
<tr>
<td>4.6.2 Scheduler</td>
<td>139</td>
</tr>
<tr>
<td>4.6.3 Protection statistics</td>
<td>140</td>
</tr>
<tr>
<td>4.6.4 Watch activity</td>
<td>141</td>
</tr>
<tr>
<td>4.6.5 ESET SysInspector</td>
<td>142</td>
</tr>
<tr>
<td>4.6.6 Cloud-based protection</td>
<td>142</td>
</tr>
<tr>
<td>4.6.7 Running processes</td>
<td>144</td>
</tr>
<tr>
<td>4.6.8 Security report</td>
<td>145</td>
</tr>
<tr>
<td>4.6.9 Network connections</td>
<td>146</td>
</tr>
<tr>
<td>4.6.10 ESET SysRescue Live</td>
<td>147</td>
</tr>
<tr>
<td>4.6.11 Submission of samples for analysis</td>
<td>147</td>
</tr>
<tr>
<td>4.6.12 Email notifications</td>
<td>148</td>
</tr>
<tr>
<td>4.6.13 Quarantine</td>
<td>150</td>
</tr>
<tr>
<td>4.6.14 Proxy server setup</td>
<td>151</td>
</tr>
<tr>
<td>4.6.15 Time slots</td>
<td>152</td>
</tr>
<tr>
<td>4.6.16 Microsoft Windows update</td>
<td>153</td>
</tr>
<tr>
<td>4.6.17 ESET CMD</td>
<td>153</td>
</tr>
<tr>
<td><strong>4.7 User interface</strong></td>
<td><strong>155</strong></td>
</tr>
<tr>
<td>4.7.1 User interface elements</td>
<td>155</td>
</tr>
<tr>
<td>4.7.2 Access setup</td>
<td>157</td>
</tr>
<tr>
<td>4.7.3 Alerts and message boxes</td>
<td>157</td>
</tr>
<tr>
<td>4.7.3.1 Confirmation messages</td>
<td>159</td>
</tr>
<tr>
<td>4.7.3.2 Advanced settings conflict error</td>
<td>159</td>
</tr>
<tr>
<td>4.7.4 Notifications</td>
<td>159</td>
</tr>
<tr>
<td>4.7.5 System tray icon</td>
<td>160</td>
</tr>
<tr>
<td>4.7.6 Context menu</td>
<td>161</td>
</tr>
<tr>
<td>4.7.7 Help and support</td>
<td>161</td>
</tr>
<tr>
<td>4.7.7.1 About ESET Endpoint Security</td>
<td>162</td>
</tr>
<tr>
<td>4.7.7.2 Submit system configuration data</td>
<td>163</td>
</tr>
<tr>
<td><strong>4.8 Advanced user</strong></td>
<td><strong>163</strong></td>
</tr>
<tr>
<td>4.8.1 Profile manager</td>
<td>163</td>
</tr>
<tr>
<td>4.8.2 Keyboard shortcuts</td>
<td>164</td>
</tr>
<tr>
<td>4.8.3 Diagnostics</td>
<td>164</td>
</tr>
<tr>
<td>4.8.4 Import and export settings</td>
<td>165</td>
</tr>
<tr>
<td>4.8.5 Command Line</td>
<td>166</td>
</tr>
<tr>
<td>4.8.6 Idle-state detection</td>
<td>167</td>
</tr>
<tr>
<td>4.8.7 Remote monitoring and management</td>
<td>168</td>
</tr>
<tr>
<td>4.8.7.1 RMM Command Line</td>
<td>169</td>
</tr>
<tr>
<td>4.8.7.2 List of JSON commands</td>
<td>171</td>
</tr>
<tr>
<td>4.8.7.2.1 get protection-status</td>
<td>171</td>
</tr>
<tr>
<td>4.8.7.2.2 get application-info</td>
<td>172</td>
</tr>
<tr>
<td>4.8.7.2.3 get license-info</td>
<td>175</td>
</tr>
<tr>
<td>4.8.7.2.4 get logs</td>
<td>176</td>
</tr>
<tr>
<td>4.8.7.2.5 get activation-status</td>
<td>177</td>
</tr>
<tr>
<td>4.8.7.2.6 get scan-info</td>
<td>178</td>
</tr>
<tr>
<td>4.8.7.2.7 get configuration</td>
<td>179</td>
</tr>
<tr>
<td>4.8.7.2.8 get update-status</td>
<td>180</td>
</tr>
<tr>
<td>4.8.7.2.9 start scan</td>
<td>181</td>
</tr>
<tr>
<td>4.8.7.2.10 start activation</td>
<td>182</td>
</tr>
<tr>
<td>4.8.7.2.11 start deactivation</td>
<td>183</td>
</tr>
</tbody>
</table>
## 5. Common Questions

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 How to update ESET Endpoint Security</td>
<td>186</td>
</tr>
<tr>
<td>5.2 How to activate ESET Endpoint Security</td>
<td>186</td>
</tr>
<tr>
<td>5.2.1 Login to ESET Business Account</td>
<td>186</td>
</tr>
<tr>
<td>5.3 How to use current credentials to activate a new product</td>
<td>187</td>
</tr>
<tr>
<td>5.4 How to remove a virus from my PC</td>
<td>187</td>
</tr>
<tr>
<td>5.5 How to allow communication for a certain application</td>
<td>188</td>
</tr>
<tr>
<td>5.6 How to create a new task in Scheduler</td>
<td>188</td>
</tr>
<tr>
<td>5.7 How to schedule a weekly computer scan</td>
<td>189</td>
</tr>
<tr>
<td>5.8 How to connect ESET Endpoint Security to ESET Security Management Center</td>
<td>189</td>
</tr>
<tr>
<td>5.9 How to configure a mirror</td>
<td>190</td>
</tr>
<tr>
<td>5.10 How do I upgrade to Windows 10 with ESET Endpoint Security</td>
<td>190</td>
</tr>
<tr>
<td>5.11 How to use Override mode</td>
<td>191</td>
</tr>
<tr>
<td>5.12 How to activate Remote monitoring and management</td>
<td>193</td>
</tr>
<tr>
<td>5.13 How to block the download of specific file types from the Internet</td>
<td>195</td>
</tr>
</tbody>
</table>
1. ESET Endpoint Security 7

ESET Endpoint Security 7 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine, combined with our custom Firewall and Antispam module, utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software endangering your computer.

ESET Endpoint Security 7 is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. The advanced technologies, based on artificial intelligence, are capable of proactively eliminating infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other Internet-borne attacks without hindering system performance or disrupting your computer.

ESET Endpoint Security 7 is primarily designed for use on workstations in a small business environment.

In the Using ESET Endpoint Security by itself section you can find help topics divided into several chapters and subchapters to provide orientation and context, including Installation and Activation.

Using ESET Endpoint Security with ESET Security Management Center in an enterprise environment allows you to easily manage any number of client workstations, apply policies and rules, monitor detections and remotely configure clients from any networked computer.

The Common Questions chapter covers some of the most frequently asked questions and problems encountered.

1.1 What's new in version 7

ESET Endpoint Security 7 has been released and is available to download. For more information about what's new in ESET Endpoint Security 7, see the following improvements or new features:

- New design of graphical user interface.
- Drag and drop files scan – You can scan a file or folder manually just by moving the file or folder to the marked area.
- Network attack protection is now available in ESET Endpoint Antivirus. For more information, see Network attack protection.
- In Protection status, quick action link can be disabled by ESET Security Management Center policy.
- Device control rules and Web control rules can be applied now for a certain time period. For more information, see Time slots.
- New type of logging from version 7.1 – Advanced type of logging is now available. For more information, see Audit logs.

1.2 System requirements

For seamless operation of ESET Endpoint Security, the system should meet the following hardware and software requirements (default product settings):

Processors Supported:
- 32-bit (x86) or 64-bit (x64) processor, 1 GHz or higher

Operating Systems:
Microsoft® Windows® 10/8.1/8/7/Vista
- An operating system and the required service pack supported by the chosen ESET product version installed
- System requirements of the operating system and other software installed on the computer are fulfilled
- 0.3 GB of free system memory (see Note 1)
- 1 GB of free disk space (see Note 2)
- Minimum display resolution 1024x768
- Internet connection or a local area network connection to a source (see Note 3) of product updates
- Windows XP is no longer supported for version 7

Although it might be possible to install and run the product on systems that do not meet these requirements, we recommend prior usability testing to be done based on performance requirements.

**Note**

(1): The product might use more memory if the memory would be otherwise unused on a heavily infected computer or when huge lists of data are being imported into the product (e.g. URL white lists).

(2): The disk space needed to download the installer, install the product and to keep a copy of the installation package in program data as well as backups of product updates to support the rollback feature. The product might use more disk space under different settings (e.g. when more product update backup versions are stored, memory dumps or huge amounts of log records are kept) or on an infected computer (e.g. due to the quarantine feature). We recommend to keep enough free disk space to support the updates of the operating system and for ESET product updates.

(3): Although not recommended, the product might be updated manually from a removable media.

### 1.3 Prevention

When you work with your computer, and especially when you browse the Internet, please keep in mind that no antivirus system in the world can completely eliminate the risk of **detections** and **remote attacks**. To provide maximum protection and convenience, it is essential that you use your antivirus solution correctly and adhere to several useful rules:

**Update regularly**

According to statistics from ESET LiveGrid®, thousands of new, unique infiltrations are created each day in order to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at the ESET Virus Lab analyze these threats on a daily basis and prepare and release updates in order to continually improve the level of protection for our users. To ensure the maximum effectiveness of these updates it is important that updates are configured properly on your system. For more information on how to configure updates, see the **Update setup** chapter.

**Download security patches**

The authors of malicious software often exploit various system vulnerabilities in order to increase the effectiveness of spreading malicious code. With this in mind, software companies watch closely for any vulnerabilities in their applications to appear and release security updates to eliminate potential threats on a regular basis. It is important to download these security updates as they are released. Microsoft Windows and web browsers such as Internet Explorer are two examples of programs for which security updates are released on a regular schedule.

**Back up important data**

Malware writers usually do not care about user’s needs, and the activity of malicious programs often leads to total malfunction of an operating system and the loss of of important data. It is important to regularly back up your important and sensitive data to an external source such as a DVD or external hard drive. This will make it far easier and faster to recover your data in the event of system failure.
Regularly scan your computer for viruses

Detection of more known and unknown viruses, worms, trojans and rootkits are handled by the Real-time file system protection module. This means that every time you access or open a file, it is scanned for a malware activity. We recommend that you run a full Computer scan at least once a month because malware signatures may vary and the detection engine updates itself each day.

Follow basic security rules

This is the most useful and most effective rule of all – always be cautious. Today, many infiltrations require user intervention in order to be executed and distributed. If you are cautious when opening new files, you will save considerable time and effort that would otherwise be spent cleaning infiltrations. Here are some useful guidelines:

- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe Internet websites.
- Be cautious when opening email attachments, particularly those from mass-mailed messages and messages from unknown senders.
- Don’t use an Administrator account for everyday work on your computer.
2. Documentation for endpoints managed by ESET Security Management Center

ESET Security Management Center (ESMC) is a new generation of remote management system that differs significantly from previous versions of ESET Security Management Center (ERA). Since the architecture is completely different, ESET Security Management Center 7 is only partially compatible with ERA 6 and there is no backward compatibility with ERA 5. However, compatibility with previous versions of ESET security products remains.

Together with new ESET Security Management Center, ESET has developed a new generation of security products with a new licensing system.

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed (Windows and Linux platforms):

- ESMC Server
- ESMC Web Console
- ESET Management Agent

The following supporting components are optional, we recommend that you install them for best performance of the application on the network:

- RD Sensor
- Apache HTTP Proxy
- Mobile Device Connector

More information
For more information please see the ESET Security Management Center Online user guide.

2.1 Introduction to ESET Security Management Center

ESET Security Management Center allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location. Using the ESET Security Management Center Web Console (ESMC Web Console), you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

- Read more about this in the ESET Security Management Center Online user guide

2.2 Introduction to ESET Cloud Administrator

ESET Cloud Administrator (ECA) allows you to manage ESET products on workstations and servers in a networked environment from one central location without the requirement to have a physical or virtual server like for ESMC. Using the (ECA Web Console), you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

- Read more about this in the ESET Cloud Administrator Online user guide
2.3 Password protected settings

To provide maximum security for your system, ESET Endpoint Security needs to be configured correctly. Any unqualified change or setting may result in lowering the client security and level of protection. To limit user access to advanced settings, an administrator can password protect the settings.

The administrator can create a policy to password protect the settings for ESET Endpoint Security on connected client computers. To create a new policy:

1. In the ESMC Web Console, click Policies in the left-hand main menu.
2. Click New Policy.
3. Name your new policy and optionally, give it a short description. Click the Continue button.
4. From the list of products, select ESET Endpoint for Windows.
5. Click User interface in the Settings list and expand Access setup.
6. According to a version of ESET Endpoint Security, click the slider bar to enable Password to protect settings. Note that ESET Endpoint products version 7 offers enhanced protection. If you have both version 7 and version 6 of Endpoint products in the network, set a different password for each. We recommend that you do not set the password only in the field for version 6 as it will lower the security on Endpoint products with version 7.
7. In the pop-up window, create a new password, confirm it and click OK. Click Continue.
8. Assign the policy to clients. Click Assign and select the computers or groups of computers to password protect. Click OK to confirm.
9. Check that all desired client computers are in the target list and click Continue.
10. Review the policy settings in the summary and click Finish to save your new policy.
2.4 What are policies

The administrator can push specific configurations to ESET products running on client computers using policies from the ESMC Web Console. A policy can be applied directly to individual computers as well as to groups of computers. You can also assign multiple policies to a computer or to a group.

A user must have the following permissions to create a new policy: Read permission to read the list of policies, Use permission to assign policies to target computers and Write permission to create, modify or edit policies.

Policies are applied in the order that Static Groups are arranged. This is not true for Dynamic Groups, where policies are applied to child Dynamic Groups first. This allows you to apply policies with greater impact to the top of the Group tree and apply more specific policies to subgroups. Using flags, an ESET Endpoint Security user with access to groups located higher in the tree can override the policies of lower groups. The algorithm is explained in ESMC Online user guide.

Assign more generic policies

We recommend that you assign more generic policies (for example, the update server policy) to groups that are higher within the group tree. More specific policies (for example, device control settings) should be assigned deeper in the group tree. The lower policy usually overrides the settings of the upper policies when merged (unless defined otherwise using policy flags).

2.4.1 Merging policies

A policy applied to a client is usually the result of multiple policies being merged into one final policy. Policies are merged one by one. When merging policies, the general rule is that the later policy always replaces the settings set by the former one. To change this behavior, you can use policy flags (Available for each setting).

When creating policies, you will notice that some settings have an additional rule (replace/append/prepend) that you can configure.

- **Replace** - the whole list is replaced, adds new values and removes all previous one.
- **Append** - items are added to the bottom of the currently applied list (must be another policy, the local list is always overwritten).
- **Prepend** - items are added to the top of the list (the local list is overwritten).

ESET Endpoint Security supports merging of local settings with the remote policies in a new way. If the setting is a list (for example a list of blocked websites) and remote policy conflicts with an existing local setting, the remote policy overwrites it. You can choose how to combine local and remote lists by selecting the different merging rules for:

- Merging settings for remote policies.
- Merging of remote and local policies - local settings with the resulting remote policy.

To learn more about merging policies, follow the ESMC Online user guide and see the example.

2.5 How flags work

The policy that is applied to a client computer is usually the result of multiple policies being merged into one final policy. When merging policies, you can adjust the expected behavior of the final policy, due to the order of applied policies, by using policy flags. Flags define how the policy will handle a specific setting.

For each setting, you can select one of the following flags:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not apply</td>
<td>Any setting with this flag is not set by the policy. Since the setting is not set by the policy, it can be changed by other policies applied later.</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td>Settings with the <strong>Apply</strong> flag will be applied to the client computer. However, when merging policies, it can be overwritten by other policies applied later. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer. Since the setting is not forced, it can still be changed by other policies applied later.</td>
</tr>
<tr>
<td><strong>Force</strong></td>
<td>Settings with the <strong>Force</strong> flag have priority and cannot be overwritten by any policy applied later (even if it also has a <strong>Force</strong> flag). This assures that other policies applied later won’t be able to change this setting during merging. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer.</td>
</tr>
</tbody>
</table>

---

**EXAMPLE:** Allow users to see all policies

**Scenario:** The **Administrator** wants to allow user **John** to create or edit policies in his home group and see all policies created by the **Administrator** including Policies that have a **Force** flag. The **Administrator** wants **John** to be able to see all policies, but not edit existing policies created by **Administrator**. **John** can only create or edit policies within his Home Group, San Diego.

**Solution:** **Administrator** has to follow these steps:

1. **Create custom static groups and permission sets**
   1. Create a new **Static Group** called **San Diego**.
   2. Create a new **Permission set** called **Policy - All John** with access to the Static Group **All** and with **Read** permission for **Policies**.
   3. Create a new **Permission set** called **Policy John** with access to Static Group **San Diego**, with functionality access **Write** permission for **Group & Computers** and **Policies**. This permission set allows **John** to create or edit policies in his Home Group **San Diego**.
   4. Create a new **user** **John** and in the **Permission Sets** section select **Policy - All John** and **Policy John**.

2. **Create policies**
   5. Create a new **policy** **All- Enable Firewall**, expand the **Settings** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall > Basic** and apply all settings by **Force** flag. Expand the **Assign** section and select the Static Group **All**.
   6. Create a new **policy** **John Group- Enable Firewall**, expand the **Setting** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall > Basic** and apply all settings by **Apply** flag. Expand the **Assign** section and select Static Group **San Diego**.

**Result**

The Policies created by **Administrator** will be applied first since **Force** flags were applied to the policy settings. Settings with the Force flag applied have priority and cannot be overwritten by another policy applied later. The policies that are created by user **John** will be applied after the policies created by the Administrator.

To see the final policy order, navigate to **More > Groups > San Diego**. Select the computer and select **Show details**. In the **Configuration** section, click **Applied policies**.
3. Using ESET Endpoint Security by itself

This section and the Work with ESET Endpoint Security section of this User Guide is intended for users who are using ESET Endpoint Security without ESET Security Management Center. All features and functionalities of ESET Endpoint Security are fully accessible depending on a user’s account rights.

3.1 Installation methods

There are several ESET Endpoint Security installation methods on a client workstation, unless you deploy ESET Endpoint Security remotely to client workstations via ESET Security Management Center or ESET Cloud Administrator.

<table>
<thead>
<tr>
<th>Method</th>
<th>Purpose</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation with ESET AV Remover</td>
<td>The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system before proceeding with installation.</td>
<td>Download 64-bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Download 32-bit</td>
</tr>
<tr>
<td>Installation (.exe)</td>
<td>Installation process without ESET AV Remover.</td>
<td>N/A</td>
</tr>
<tr>
<td>Installation (.msi)</td>
<td>In business environments, the .msi installer is the preferred installation package. This is mainly due to offline and remote deployments that use various tools such as ESET Security Management Center.</td>
<td>Download 64-bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Download 32-bit</td>
</tr>
<tr>
<td>Command-line installation</td>
<td>ESET Endpoint Security can be installed locally using command-line or remotely using a client task from ESET Security Management Center.</td>
<td>N/A</td>
</tr>
<tr>
<td>Deployment using GPO or SCCM</td>
<td>Use management tools such as GPO or SCCM to deploy ESET Management Agent and ESET Endpoint Security to client workstations.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

3.1.1 Installation with ESET AV Remover

Before you continue with the installation process, it is important that you uninstall any existing security application on the computer. Select the check box next to I want to uninstall unwanted antivirus applications using ESET AV Remover to have ESET AV Remover scan your system and remove any supported security applications. Leave the check box deselected and click Continue to install ESET Endpoint Security without running ESET AV Remover.
3.1.1.1 ESET AV Remover

The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system. Follow the instructions below to remove an existing antivirus program using ESET AV Remover:

1. To view a list of antivirus software that ESET AV Remover can remove, visit this ESET Knowledgebase article.

2. Read the End-User License Agreement and click Accept to acknowledge your acceptance. Clicking Decline will continue to installation of ESET Endpoint Security without removal of existing security application on the computer.

3. ESET AV Remover will begin searching your system for antivirus software.
4. Select any listed antivirus applications and click **Remove**. Removal may take a moment.

5. When removal is successful, click **Continue**.
6. Restart your computer to apply changes and continue with installation of ESET Endpoint Security. If uninstallation is unsuccessful, see the Uninstallation with ESET AV Remover ended with an error section of this guide.

3.1.1.2 Uninstallation using ESET AV Remover ended with error

If you are not able to remove an antivirus program using ESET AV Remover, you will receive a notification that the application you are trying to remove might not be supported by ESET AV Remover. Visit the list of supported products or uninstallers for common Windows antivirus software on ESET Knowledgebase to see if this specific program can be removed.

When the uninstallation of the security product was unsuccessful or some of its component was uninstalled partially, you are prompted to Restart and rescan. Confirm UAC after startup and continue with the scanning and uninstallation process.

If necessary, contact ESET Technical Support to open a support request and have the AppRemover.log file available to assist ESET Technicians. The AppRemover.log file is located in the eset folder. Browse to %TEMP% in Windows Explorer to access this folder. ESET Technical Support will respond as quickly as possible to help resolve your issue.

3.1.2 Installation (.exe)

Once you launch the .exe installer, the installation wizard will guide you through the installation process.

Important

Make sure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our knowledgebase article for a list of uninstaller tools for common antivirus software (available in English and several other languages).
1. Read the End-User License Agreement and click **I Accept** to acknowledge your acceptance of the End-User License Agreement. Click **Next** after you accept the terms to continue with installation.
2. Choose whether enable ESET LiveGrid® feedback system. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, which allows us to better protect our customers. The system allows you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the detection engine.

3. The next step in the installation process is to configure detection of Potentially unwanted applications. See the Potentially unwanted applications chapter for more details.

You can install ESET Endpoint Security to a specific folder by clicking Change installation folder.

5. The final step is to confirm installation by clicking Install. After installation is complete, you will be prompted to activate ESET Endpoint Security.

### 3.1.2.1 Change installation folder (.exe)

After selecting your preference for detection of potentially unwanted applications and clicking Change installation folder, you will be prompted to select a location for the installation ESET Endpoint Security folder. By default, the program installs to the following directory:

C:\Program Files\ESET\ESET Security\

You can specify a location for program modules and data. By default, they are installed to the following directories, respectfully:

C:\Program Files\ESET\ESET Security\Modules\
C:\ProgramData\ESET\ESET Security\

Click Browse to change these locations (not recommended).
Click **Continue** and then **Install** to start installation.

### 3.1.3 Installation (.msi)

Once you launch the .msi installer, the installation wizard will guide you through the installation process.

---

**Purpose of the .msi installer**

In business environments, the .msi installer is the preferred installation package. This is mainly due to offline and remote deployments that use various tools such as ESET Security Management Center.

---

**Important**

Make sure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our [knowledgebase article](#) for a list of uninstaller tools for common antivirus software (available in English and several other languages).
1. Click Next.

2. Read the End-User License Agreement and click I Accept the terms in the License Agreement to acknowledge your acceptance of the End-User License Agreement. Click Next after you accept the terms to continue with installation.

3. Select your preference for ESET LiveGrid® feedback system. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, which allows us to better protect our customers. The system allows you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the detection engine.
4. The next step in the installation process is to configure the detection of Potentially unwanted applications. See the [Potentially unwanted applications](#) chapter for more details.

Click [Advanced settings](#) if you wish to proceed with [Advanced installation (.msi)](#).

5. The final step is to confirm installation by clicking [Install](#). After installation is complete, you will be prompted to [activate ESET Endpoint Security](#).
3.1.3.1  Advanced installation (.msi)

Advanced installation allow you to customize a number of installation parameters not available when performing a
typical installation.

5. After selecting your preference for detection of Potentially unwanted applications and clicking Advanced
settings, you will be prompted to select a location for the installation ESET Endpoint Security folder. By default,
the program installs to the following directory:

C:\Program Files\ESET\ESET Security\

You can specify a location for program modules and data. By default, they are installed to the following directories,
respectfully:

C:\Program Files\ESET\ESET Security\Modules\nC:\ProgramData\ESET\ESET Security\

Click Browse to change these locations (not recommended).

6. Choose which product components will be installed. Product components in the Computer section include Real-
time file system protection, Computer scan, Document protection and Device control. Please note that the first
two components are mandatory for your security solution to work. The Network section offers the option to
install ESET firewall, which monitors all incoming and outgoing network traffic and applies rules for individual
network connections. Firewall also provides protection against attacks from remote computers. Network attack
protection (IDS) analyses the content of network traffic and protects from network attacks. Any traffic which is
considered harmful will be blocked. Components in the Web and email section are responsible for your
protection while you are browsing the Internet and communicating via email. The Update mirror component can
be used to update other computers on your network. Remote Monitoring and Management (RMM) is the process
of supervising and controlling software systems using a locally installed agent that can be accessed by a
management service provider.
7. The final step is to confirm installation by clicking **Install**.

### 3.1.4 Installation via ESET Security Management Center (command line)

ESET Endpoint Security can be installed locally via command-line or remotely using a client task from ESET Security Management Center.

- Read more about this type of installation in the ESET Security Management Center Online user guide

### 3.1.5 Deployment using GPO or SCCM

Apart from ESET Endpoint Security direct installation on a client workstation or remote deployment using a Server task in ESMC, you can also use management tools such as Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris or Puppet.

In this case, we install ESET Management Agent first, then deploy ESET Endpoint Security via ESET Security Management Center.

- Read more about this type of installation in the ESET Security Management Center Online user guide

### 3.1.6 Upgrading to a more recent version

New versions of ESET Endpoint Security are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules. Upgrading to a more recent version can be accomplished in several ways:

1. Automatically, using ESET Security Management Center or ESET Cloud Administrator.
2. Manually, by downloading and installing a more recent version over the previous one.

#### Recommended upgrade scenarios

- **Upgrading remotely**

  If you manage more than 10 ESET Endpoint products, consider handling upgrades using ESET Security Management Center or ESET Cloud Administrator (ECA), please refer to the following documentation:

  - ESET Security Management Center | Infrastructure building and sizing
  - ESET Security Management Center | Upgrade, migration and reinstallation procedures
  - Introduction to ECA
Upgrading manually on a client workstation

If you plan to handle upgrades on individual client workstations manually, check the upgrade prerequisites first:

<table>
<thead>
<tr>
<th>Upgrade from</th>
<th>Upgrade to</th>
<th>Upgrade prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.x</td>
<td>7.x</td>
<td>• No prerequisites</td>
</tr>
</tbody>
</table>
| 5.x          | 7.x        | • Verify that your operating system is supported. For example, Windows XP is not supported for version 7.  
• Check if your versions of ESET endpoint products support upgrade from version 5.x. |
| 4.x          | 7.x        | • Verify that your operating system is supported.  

3.1.7 Common installation problems

If problems occur during installation, see our list of common installation errors and resolutions to find a solution to your problem.

3.1.7.1 Activation failed

In the case activation of ESET Endpoint Security was not successful, the most-common possible scenarios are:

• License key already in use
• Invalid License key. Product activation form error
• Additional information necessary for activation is missing or invalid
• Communication with the activation database failed. Please try to activate again in 15 minutes
• No or disabled connection to ESET activation servers, for more information see Ports and addresses required to use your ESET product with a third-party firewall

Make sure you have entered the proper License key or attached an Offline license and attempt to activate again.

If you are unable to activate, please read Resolve ACT or ECP errors during activation.

3.2 Product activation

After installation is complete, you will be prompted to activate your product.

Select one of the available methods to activate ESET Endpoint Security. See How to activate ESET Endpoint Security for more information.
3.3 Computer scan

We recommend that you perform regular computer scans, or schedule a regular scan, to check for threats. In the main program window, click Computer scan and then click Smart scan. For more information about computer scans, see Computer scan.

![Computer scan interface](image)

3.4 Beginner's guide

This chapter provides an initial overview of ESET Endpoint Security and its basic settings.

3.4.1 The user interface

The main program window of ESET Endpoint Security is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The following is a description of options within the main menu:

- **Protection status** – Provides information about the protection status of ESET Endpoint Security.
- **Computer scan** – This option allows you to configure and launch of Smart scan, Custom scan, or Removable media scan. You can also repeat the last scan that was run.
- **Update** – Displays information about the detection engine and allows to check for updates manually.
- **Setup** – Select this option to adjust your Computer, Network or Web and Email security settings.
- **Tools** – Provides access to Log files, Protection statistics, Watch activity, Running processes, Scheduler, Quarantine, Network connections, ESET SysInspector and ESET SysRescue to create a rescue CD. You can also submit a sample for analysis.
- **Help and support** – Provides access to help files, ESET Knowledgebase and the ESET company website. Also available are links to open a Technical Support support request, support tools, and information about product activation.
The **Protection status** screen informs you about the security and current protection level of your computer. The green **Maximum protection** status indicates that maximum protection is ensured.

The status window also displays quick links to frequently used features in ESET Endpoint Security and information about the last update.
What to do if the program doesn't work properly?

A green check mark will be displayed next to all program modules that are fully functional. A red exclamation point or orange notification icon is displayed if a module needs attention. Additional information about the module, including our recommendation about how to restore full functionality is shown in the upper part of the window. To change a module’s status, click **Setup** in the main menu and then click the desired module.
The red exclamation point (!) icon indicates that maximum protection of your computer is not ensured. You may encounter this type of notification in the following scenarios:

- **Antivirus and antispyware protection is paused** – Click Start all antivirus and antispyware protection modules to re-enable antivirus and antispyware protection in Protection status pane or Enable Antivirus and antispyware protection in Setup pane in the main program window.
- **Antivirus protection is non-functional** – Virus scanner initialization failed. Most ESET Endpoint Security modules will not function properly.
- **Anti-Phishing protection is non-functional** – This feature is not functional because other required program modules are not active.
- **The ESET Firewall is disabled** – This problem is indicated by a red icon and a security notification next to the Network item. Click Enable filtering mode to re-enable network protection.
- **Firewall initialization failed** – The firewall is disabled due to system integration issues. Restart your computer as soon as possible.
- **Detection engine is out of date** – You are using an outdated detection engine. Update the detection engine.
- **Product is not activated or License expired** – This is indicated by the Protection status icon turning red. The program is not able to update after the license expires. We recommend that you follow the instructions in the alert window to renew your license.
- **Host Intrusion Prevention System (HIPS) is disabled** – This problem is indicated when HIPS disabled from Advanced setup. Your computer is not protected against some types of threats and protection should be re-enabled immediately by clicking Enable HIPS.
- **ESET LiveGrid® is disabled** – This problem is indicated when ESET LiveGrid® disabled in Advanced setup.
- **No regular updates scheduled** – ESET Endpoint Security will not check for or receive important updates unless you schedule update task.
- **Anti-Stealth is disabled** – Click Enable Anti-Stealth to re-enable this functionality.
- **Real-time file system protection is paused** – Real-time protection was disabled by the user. Your computer is not protected against threats. Click Enable Real-time protection re-enable this functionality.

The orange "i" indicates that your ESET product requires attention for a non-critical problem. Possible reasons include:

- **Web access protection is disabled** – Click on the security notification to re-enable Web access protection and then click Enable Web access protection.
- **Your license will expire soon** – This is indicated by the protection status icon displaying an exclamation point. After your license expires, the program will not be able to update and the Protection status icon will turn red.
- **Botnet protection is paused** – Click Enable Botnet protection to re-enable this feature.
- **Network attack protection (IDS) is paused** – Click Enable Network attack protection (IDS) to re-enable this feature.
- **Antispam protection is paused** – Click Enable Antispam protection to re-enable this feature.
- **Web control is paused** – Click Enable Web control to re-enable this feature.
- **Policy override active** – The configuration set by the policy is temporarily overridden, possibly until troubleshooting is complete. Only authorized user can override the policy settings. For more information see How to use Override mode.
- **Device control is paused** – Click Enable Device control to re-enable this feature.

If you are unable to solve a problem by using the suggested solutions, click Help and support to access the help files or search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Technical Support request. ESET Technical Support will respond quickly to your questions and help find a resolution.

---

**Note**

If a status belongs to a feature that is blocked by ESMC policy, the link will not be clickable.
3.4.2 Update setup

Updating modules is an important part of maintaining complete protection against malicious code. Please pay careful attention to update configuration and operation. From the main menu, select **Update > Update now** to check for a newer module update.

If your **License Key** is not entered yet, you will be unable to receive new updates and will be prompted to activate your product.
The Advanced setup window (click Setup > Advanced setup from the main menu, or press F5 on your keyboard) contains additional update options. To configure advanced update options such as update mode, proxy server access, LAN connections and detection engine copy creation settings, click Update in the Advanced setup tree. If you experience problems with an update, click Clear to clear the temporary update cache. The Update server menu is set to AUTOSELECT by default. When using an ESET server, we recommend that you leave the Choose automatically option selected. If you do not want the system tray notification at the bottom right corner of the screen to appear, select Disable display notification about successful update.

For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct License key is entered in Help and support > Activate Product.

If you did not enter your License key after installation, you can do so at any time. For more detailed information about activation see How to activate ESET Endpoint Security and enter the credentials you received with your ESET security product in License details window.
3.4.3 Zones setup

It is necessary to configure Trusted zones to protect your computer in a network environment. You can allow other users to access your computer by configuring a Trusted zone to allow sharing. Click Advanced Setup (F5) > Firewall > Zones to access settings for Trusted zones.

Trusted zone detection occurs after ESET Endpoint Security installation and whenever your computer connects to a new network. Therefore, there is usually no need to define the Trusted zone. By default, a dialog window is displayed upon detection of a new zone which allows you to set the protection level for that zone.

---

Important

An incorrect trusted zone configuration may pose a security risk to your computer.

---

Note

By default, workstations from a Trusted zone are granted access to shared files and printers, have incoming RPC communication enabled and have remote desktop sharing available.

3.4.4 Web control tools

If you have already enabled Web control in ESET Endpoint Security, you must also configure Web control for your desired user accounts in order for Web control to function properly. Please refer to the Web control chapter for instructions on how to create specific restrictions for your client workstations to protect them from potentially offensive material.
4. Work with ESET Endpoint Security

The ESET Endpoint Security setup options allow you to adjust the level of protection for your computer, web, email and network.

Note

When creating a policy from ESET Security Management Center Web Console you can select the flag for each setting. Settings with the Force flag have priority and cannot be overwritten by a later policy (even if the later policy has a Force flag). This assures that this setting will not be changed (e.g. by user or by later policies during merging). For more information see Flags in ESMC Online Help.
The Setup menu contains the following sections:

- Computer
- Network
- Web and Email

**Computer** section allows you to enable or disable the following components:

- **Real-time file system protection** – All files are scanned for malicious code when they are opened, created or run on your computer.
- **Device control** – Provides automatic device (CD/DVD/USB/...) control. This module allows you to block or adjust extended filters/permissions and define a user's ability to access and work with a given device.
- **Host Intrusion Prevention System (HIPS)** – The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.
- **Advanced memory scanner** – Works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.
- **Exploit blocker** – Designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.
- **Ransomware shield** – It is another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.
- **Presentation mode** – A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.

The **Network** section allows you to have quick access to the following components or settings in Advanced setup:

- **Firewall** – Here you can adjust the filtering mode for the ESET Firewall. To access more detailed settings, click the gear wheel > Configure next to Firewall, or press F5 to access Advanced setup.
- **Network attack protection (IDS)** – Analyzes the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked. You can disable Network attack protection for a specific period of time by clicking .
- **Botnet protection** – Quickly and accurately identifies malware in the system. To disable Botnet protection for a specific period of time, click .
- **Connected networks** – Displays the networks to which network adapters are connected. After clicking the gear wheel, you will be prompted to select a protection type for the network you are connected to via your network adapter. In this window you can also see Network adapters in lower right corner. You can view each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.
- **Temporary IP address blacklist** – View a list of IP addresses that have been detected as the source of attacks and added to the blacklist to block connections for a certain period of time. For more information, click this option and press F1.
- **Troubleshooting wizard** – Helps you solve connectivity problems caused by ESET Firewall. For more detailed information see Troubleshooting wizard.

**Web and email** protection setup allows you to enable or disable the following components:

- **Web control** – Blocks web pages that may contain potentially offensive material. In addition, system administrators can specify access preferences for 27 pre-defined website categories.
- **Web access protection** – If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** – Monitors communication received through the POP3 and IMAP protocol.
- **Antispam protection** – Scans unsolicited email or spam.
- **Anti-Phishing protection** – Protects you from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites disguised as legitimate ones.
To temporarily disable individual modules, click the green switch next to the desired module. Note that this may decrease the protection level of your computer.

To re-enable the protection of a disabled security component, click the red switch to return a component to its enabled state.

When ESMC/ERA policy is applied, you will see the lock icon next to a specific component. The policy applied by ESET Security Management Center can be overridden locally after authentication by logged user (e.g. administrator). For more information see the ESMC Online Help.

**Note**

All protective measures disabled this way will be re-enabled after a computer restart.

To access detailed settings for a particular security component, click the gear wheel next to any component.

There are additional options at the bottom of the setup window. To load setup parameters using an .xml configuration file, or to save the current setup parameters to a configuration file, use Import/Export settings. Please see Import/Export settings for more detailed information.

For more detailed options, click Advanced Setup or press F5.

### 4.1 Computer

The **Computer** module can be found under Setup > Computer. It displays an overview of the protection modules described in the previous chapter. In this section, the following settings are available:

Click the gear wheel next to **Real-time file system protection** and click **Edit exclusions** to open the Exclusion setup window, which allows you to exclude files and folders from scanning.
Computer section allows you to enable or disable the following components:

- **Real-time file system protection** – All files are scanned for malicious code when they are opened, created or run on your computer.
- **Device control** – Provides automatic device (CD/DVD/USB/...) control. This module allows you to block or adjust extended filters/permissions and define a user's ability to access and work with a given device.
- **Host Intrusion Prevention System (HIPS)** – The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.
- **Advanced memory scanner** – Works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.
- **Exploit blocker** – Designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.
- **Ransomware shield** – It is another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.
- **Presentation mode** – A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.

**Pause Antivirus and antispyware protection** – Any time that you temporarily disable Antivirus and antispyware protection, you can select the period of time for which you want the selected component to be disabled using the drop-down menu and then click Apply to disable the security component. To re-enable protection, click Enable Antivirus and antispyware protection.

### 4.1.1 Detection engine

Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat is detected, the Antivirus module can eliminate it by first blocking it and then cleaning, deleting or moving it to quarantine.

To configure Antivirus module settings in detail, click Advanced Setup or press F5.

**Scanner options** for all protection modules (for example Real-time file system protection, Web access protection, ...) allows you to enable or disable detection of the following:

- **Potentially unwanted applications** – Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. It may however install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user. Read more about these types of applications in the glossary.

- **Potentially unsafe applications** refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default. Read more about these types of applications in the glossary.

- **Suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

**Anti-Stealth technology** is a sophisticated system that provides the detection of dangerous programs such as rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.

**Exclusions** enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude
an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan. To exclude an object from scanning see Exclusions.

Enable advanced scanning via AMSI – Microsoft Antimalware Scan Interface tool that allows application developers new malware defenses (Windows 10 only).

4.1.1.1 An infiltration is detected

Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, diskettes, etc.).

Standard behavior

As a general example of how infiltrations are handled by ESET Endpoint Security, infiltrations can be detected using:

- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

Each uses the standard cleaning level and will attempt to clean the file and move it to Quarantine or terminate the connection. A notification window is displayed in the notification area at the bottom right corner of the screen. For more information about cleaning levels and behavior, see Cleaning.
Cleaning and deleting

If there is no predefined action to take for Real-time file system protection, you will be prompted to select an option in the alert window. Usually the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, as this will leave infected files uncleaned. The exception to this is when you are sure that a file is harmless and has been detected by mistake.

![Alert window](image)

Apply cleaning if a file has been attacked by a virus that has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

If an infected file is “locked” or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

**Multiple threats**

If any infected files were not cleaned during Computer scan (or the **Cleaning level** was set to **No Cleaning**), an alert window prompting you to select action for those files is displayed.

**Deleting files in archives**

In Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a Strict cleaning scan, with Strict cleaning enabled an archive will be deleted if it contains at least one infected file regardless of the status of other files in the archive.

If your computer is showing signs of a malware infection, for example, it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Endpoint Security and click Computer scan
- Click **Smart scan** (for more information, see [Computer scan](#))
- After the scan has finished, review the log for the number of scanned, infected and cleaned files

If you only want to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.
4.1.2 Shared local cache

Shared local cache will boost performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. Turn on the **Caching option** switch to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET Endpoint Security will search for scanned files in the cache. If files match, they will be excluded from scanning.

The setup of **Cache server** contains the following:

- **Hostname** – Name or IP address of the computer where the cache is located.
- **Port** – Number of port used for communication (same as was set in Shared local cache).
- **Password** – Specify the ESET Shared local cache password if required.

4.1.3 Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. Real-time file system protection is launched at system startup.

By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging **Enable Real-time file system protection** in **Advanced setup** under **Real-time file system protection > Basic**.

**Media to scan**

By default, all types of media are scanned for potential threats:

- **Local drives** – Controls all system hard drives.
- **Removable media** – Controls CD/DVDs, USB storage, Bluetooth devices, etc.
- **Network drives** – Scans all mapped drives.

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.
Scan on

By default, all files are scanned upon opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open** – Enables or disables scanning when files are opened.
- **File creation** – Enables or disables scanning when files are created.
- **File execution** – Enables or disables scanning when files are run.
- **Removable media access** – Enables or disables scanning triggered by accessing particular removable media with storage space.

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in the ThreatSense engine parameter setup section), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each update of the detection engine. This behavior is controlled using Smart optimization. If this Smart optimization is disabled, all files are scanned each time they are accessed. To modify this setting, press F5 to open Advanced setup and expand Detection engine > Real-time file system protection. Click ThreatSense parameters > Other and select or deselect Enable Smart optimization.

### 4.1.3.1 Additional ThreatSense parameters

**Additional ThreatSense parameters for newly created and modified files** – The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the detection engine update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable Default archive scan settings.

To learn more about Runtime packers, Self-extracting archives and Advanced heuristics see ThreatSense engine parameters setup.

**Additional ThreatSense parameters for executed files** – By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid® enabled to mitigate impact on system performance.

### 4.1.3.2 Cleaning levels

Real-time protection has three cleaning levels (to access cleaning level settings, click ThreatSense engine parameter setup in the Real-time file system protection section and then click Cleaning).

**No cleaning** – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

**Normal cleaning** – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

**Strict cleaning** – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.
Warning

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive would be deleted if all the files it contains are infected files. In Strict cleaning mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

4.1.3.3 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file is available for download at http://www.eicar.org/download/eicar.com

Note

Before performing a real-time protection check, it is necessary to disable the firewall. If the firewall is enabled, it will detect the file and prevent test files from downloading. Make sure that you re-enable the firewall immediately following your check of real-time file system protection.

4.1.3.4 When to modify real-time protection configuration

Real-time file system protection is the most essential component for maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET Endpoint Security, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click next to each tab in the window (Advanced setup > Detection engine > Real-time file system protection).

4.1.3.5 What to do if real-time protection does not work

In this chapter, we describe problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to Setup in the main program window and click Real-time file system protection.

If real-time protection is not initiated at system startup, it is usually because Start Real-time file system protection automatically is deselected. To enable this option, navigate to Advanced setup (F5) and click Detection engine > Real-time file system protection > Basic. Make sure that the Start Real-time file system protection automatically switch is turned on.

If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system before installing ESET.

Real-time protection does not start

If real-time protection is not initiated at system startup (and Enable Real-time file system protection is enabled), it may be due to conflicts with other programs. For assistance resolving this issue, please contact ESET Technical Support.
4.1.3.6  Processes exclusions

The Processes exclusions feature allows you to exclude application processes from Real-time file system protection. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level malware protection are used during backup. Similar problems can occur when attempting live migrations of virtual machines. The only effective way to avoid both situations is to deactivate Anti-Malware software. By excluding specific process (for example those of the backup solution) all file operations attributed to such excluded process are ignored and considered safe, thus minimizing interference with the backup process. We recommend that you use caution when creating exclusions – a backup tool that has been excluded can access infected files without triggering an alert which is why extended permissions are only allowed in the real-time protection module.

Note
Do not be confused with Excluded file extensions or File/folder exclusions.

Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (.exe).

You can add executable files into the list of excluded processes via Advanced setup (F5) > Detection engine > Processes exclusions.

This feature was designed to exclude backup tools. Excluding the backup tool’s process from scanning not only ensures system stability, but it also does not affect backup performance as the backup is not slowed down while it is running.

Example
Click Edit to open the Processes exclusions management window, where you can Add exclusions and browse for executable file (for example Backup-tool.exe), which will be excluded from scanning.
As soon as the .exe file is added to the exclusions, activity of this process is not monitored by ESET Endpoint Security and no scanning is run on any file operations performed by this process.

Important
If you do not use browse function when selecting process executable, you need to manually enter a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also Edit existing processes or Delete them from exclusions.

Note
Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend you to create exclusions for web browsers.
4.1.3.6.1 Add or Edit processes exclusions

This dialog window enables you to add processes excluded from thread detection. Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (.exe).

Example

Select the file path of an excepted application by clicking … (for example C:\Program Files\Firefox\Firefox.exe). Do NOT enter the name of the application. As soon as the .exe file is added to the exclusions, activity of this process is not monitored by ESET Endpoint Security and no scanning is run on any file operations performed by this process.

Important

If you do not use browse function when selecting process executable, you need to manually enter a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also Edit existing processes or Delete them from exclusions.
4.1.4 Computer scan

The on-demand scanner is an important part of ESET Endpoint Security. It is used to perform scans of files and folders on your computer. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular (for example once a month) in-depth scans of your system to detect viruses not detected by Real-time file system protection. This can happen if Real-time file system protection was disabled at the time, if the detection engine was obsolete or if the file was not detected as a virus when it was saved to the disk.

Two types of Computer scan are available. Scan your computer quickly scans the system with no need for further configuration of the scan parameters. Custom scan allows you to select any of the predefined scan profiles and define specific scan targets.

See Scan progress for more information about the scanning process.

🔍 Scan your computer

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is that it is easy to operate and does not require detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see Cleaning.

🔍 Custom scan

Custom scan is an optimal solution if you want to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed using the same parameters.

To select scan targets, select Computer scan > Custom scan and select an option from the Scan targets drop-down menu, or select specific targets from the tree structure. A scan target can also be specified by entering the path of
the folder or file(s) you want to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. When performing a scan, you can choose from three cleaning levels by clicking **Setup... > ThreatSense parameters > Cleaning**.

Performing computer scans with Custom scan is suitable for advanced users with previous experience using antivirus programs.

You can also use the **Drag and drop scan** feature to scan a file or folder manually by clicking the file or folder, moving the mouse pointer to the marked area while keeping the mouse button pressed, and then releasing it. After that, the application is moved to the foreground.

**Removable media scan**

Similar to **Scan your computer** – quickly launch a scan of removable media (such as CD/DVD/USB) that are currently connected to the computer. This may be useful when you connect a USB flash drive to a computer and want to scan its content for malware and other potential threats.

This type of scan can be also initiated by clicking **Custom scan** and then selecting **Removable media** from the **Scan targets** drop-down menu and clicking **Scan**.

**Repeat last scan**

Allows you to quickly launch the previously performed scan using the same settings it was run with.

You can select **No action**, **Shutdown** or **Reboot** from **Action after scan** drop-down menu. The actions **Sleep** or **Hibernate** are available based on your computer Power & sleep operating system settings or your computer/laptop capabilities. The selected action will start after all of the running scans are finished. When **Shutdown** is selected, a shutdown confirmation dialog window will display a 30-second countdown (click **Cancel** to deactivate the requested shutdown). See **Advanced scan options** for more details.

**Note**

We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools > Scheduler**. **How do I schedule a weekly computer scan?**

### 4.1.4.1 Custom scan launcher

If only want to scan a specific target, you can use the Custom scan tool by clicking **Computer scan > Custom scan** and selecting an option from the **Scan targets** drop-down menu or selecting specific targets from the folder (tree) structure.

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets set in the selected scan profile.
- **Removable media** – Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** – Selects all system hard drives.
- **Network drives** – Selects all mapped network drives.
- **No selection** – Cancels all selections.

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list. This is only possible if no targets were selected in the tree structure and the **Scan targets** menu is set to **No selection**.
Infected items are not cleaned automatically. Scanning without cleaning can be used to obtain an overview of the current protection status. Furthermore, you can choose from three cleaning levels by clicking Advanced setup > Detection engine > On-demand scan > ThreatSense parameters > Cleaning. If you are only interested in scanning the system without additional cleaning actions, select Scan without cleaning. Scan history is saved to the scan log.

When Ignore exclusions is selected, files with extensions that were previously excluded from scanning will be scanned with no exception.

You can choose a profile from the Scan profile drop-down menu to be used for scanning chosen targets. The default profile is Smart scan. There are two more pre-defined scan profiles called In-depth scan and Context menu scan. These scan profiles use different ThreatSense parameters. The available options are described in Advanced setup > Detection engine > Malware scans > On-demand scan > ThreatSense parameters.

Click Scan to execute the scan using the custom parameters that you have set.

Scan as Administrator allows you to execute the scan under the Administrator account. Click this if the current user doesn't have privileges to access the appropriate files to be scanned. Note that this button is not available if the current user cannot call UAC operations as Administrator.

Note
You can view the computer scan log when a scan completes by clicking Show log.
4.1.4.2 Scan progress

The scan progress window shows the current status of the scan and information about the number of files found that contain malicious code.

**Note**

It is normal that some files, such as password protected files or files exclusively being used by the system (typically `pagefile.sys` and certain log files), cannot be scanned.

---

**Scan progress** – The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.

**Target** – The name of the currently scanned object and its location.

**Threats found** – Shows the total number of threats found during a scan.

**Pause** – Pauses a scan.

**Resume** – This option is visible when scan progress is paused. Click Resume to continue scanning.

**Stop** – Terminates the scan.

**Scroll scan log** – If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.
4.1.4.3 Computer scan log

The Computer scan log gives you general information about the scan such as:

- Date and time of scan
- Scanned disks, folders and files
- Number of scanned objects
- Number of threats found
- Time of completion
- Total scanning time

4.1.4.4 Malware scans

The Malware scans section is accessible in the Advanced setup menu. Press the F5 key, click Detection engine > Malware scans and provides options to select scanning parameters. This section includes the following options:

- **Selected profile** – A specific set of parameters used by the on-demand scanner. To create a new profile, click Edit next to List of profiles. See Scan profiles for more details.

- **Scan targets** – If you only want to scan a specific target, you can click Edit next to Scan targets and select an option from the drop-down menu or select specific targets from the folder (tree) structure. See Scan targets for more details.

- **ThreatSense parameters** – Advanced setup options, such as file extensions you want to control, detection methods used, etc. can be found in this section. Click to open a tab with advanced scanner options.
**4.1.4.4.1 Idle-state scan**

You can enable the idle-state scanner in **Advanced setup** under **Detection engine > Malware scans > Idle-state scan**.

**Idle-state scan**

Set the switch next to **Enable Idle-state scanning** to **On** to enable this feature. When the computer is in idle state, a silent computer scan is performed on all local drives.

By default, the idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting by activating the switch next to **Run even if computer is powered from battery** in Advanced setup.

Turn on the **Enable logging** switch in Advanced setup to record a computer scan output in the **Log files** section (from the main program window click **Tools > Log files**, and then select **Computer scan** from the **Log** drop-down menu).

**Idle-state detection**

See **Idle state detection triggers** for a full list of conditions that must be met in order to trigger the idle-state scanner.

Click **ThreatSense engine parameter setup** to modify scan parameters (for example, detection methods) for the Idle-state scanner.

---

**4.1.4.4.2 Scan profiles**

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced setup window (F5) and click **Detection engine > Malware scans > On-demand scan > List of profiles**. The **Profile manager** window includes the **Selected profile** drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see the **ThreatSense engine parameters setup** section for a description of each parameter of the scan setup.

---

**Note**

Suppose that you want to create your own scan profile and the **Scan your computer** configuration is partially suitable, but you do not want to scan **runtime packers** or **potentially unsafe applications** and you also want to apply **Strict cleaning**. Enter the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements, and then click **OK** to save your new profile.

---

**4.1.4.4.3 Scan targets**

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets set in the selected scan profile.
- **Removable media** – Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** – Selects all system hard drives.
- **Network drives** – Selects all mapped network drives.
- **No selection** – Cancels all selections.
4.1.4.4 Advanced scan options

In this window you can specify advanced options for a scheduled computer scan task. You can set an action to be performed automatically after a scan finishes using the drop-down menu:

- **Shut down** – The computer turns off after a scan finishes.
- **Reboot** – Closes all open programs, and restarts the computer after a scan finishes.
- **Sleep** – Saves your session and puts the computer in a low-power state so that you can quickly resume working.
- **Hibernate** – Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down, but will resume it's previous state the next time you start it.
- **No action** – After a scan finishes, no action will be performed.

**Note**

Please keep in mind that a sleeping computer is still a working computer. It is still running basic functions and using electricity when your computer is operating on battery power. To preserve battery life, for example when traveling outside of your office, we recommend using the Hibernate option.

Select **Action cannot be canceled by user** to deny non-privileged users the ability to stop actions taken after scanning.

Select **The scan may be paused by user for (min)** option if you want to allow the limited user to pause the computer scan for a specified time period.

See also the **Scan progress** chapter.

4.1.5 Device control

ESET Endpoint Security provides automatic device (CD/DVD/USB/...) control. This module allows you to block or adjust extended filters/permissions and define a user's ability to access and work with a given device. This may be useful if the computer administrator wants to prevent the use of devices containing unsolicited content.

**Supported external devices:**

- Disk storage (HDD, USB removable disk)
- CD/DVD
- USB printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device
- All device types

Device control setup options can be modified in **Advanced setup (F5) > Device control**.

Turning the switch on next to **Integrate into system** activates the Device control feature in ESET Endpoint Security; you will need to restart your computer for this change to take effect. Once Device control is enabled, the Rules will become active, allowing you to open the Rules editor window.

If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device will not be granted.
4.1.5.1 Device control rules editor

The **Device control rules editor** window displays existing rules and allows for precise control of external devices that users connect to the computer.

Specific devices can be allowed or blocked according to their user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, type of external device, action to perform after connecting an external device to your computer and log severity.

Click **Add** or **Edit** to manage a rule. Deselect the **Enabled** check box next to a rule to disable it until you want to use it in the future. Select one or more rules and click **Delete** to delete the rule(s) permanently.

**Copy** – Creates a new rule with predefined options used for another selected rule.

Click **Populate** to auto-populate removable media device parameters for devices connected to your computer.

Rules are listed in order of priority with higher-priority rules closer to the top. Rules can be moved by clicking **Top/Up/Down/Bottom** and can be moved individually or in groups.

The Device control log records all occurrences where Device control is triggered. Log entries can be viewed from the main program window of ESET Endpoint Security in **Tools > Log files**.

4.1.5.1.1 Detected devices

The **Populate** button provides an overview of all currently connected devices with information about: device type, about device vendor, model and serial number (if available).

If a device is selected (from the list of Detected devices) and **OK** is clicked, a rule editor window appears with predefined information (all settings can be adjusted).
4.1.5.2 Device groups

Warning
Device connected to your computer may pose a security risk.

The Device groups window is divided into two parts. The right part of the window contains a list of devices belonging to respective group and the left part of the window contains created groups. Select a group with a list of devices you want to display in the right pane.

When you open the Device groups window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file. Alternatively, you can click Populate button and all devices connected to your computer will be listed in the Detected devices window. Select a devices from the populated list to add it to the group by clicking OK.

Control elements

Add – You can add a group by entering its name, or a device to existing group (optionally, you can specify details such as vendor name, model and serial number) depending on which part of the window you clicked the button.

Edit – Lets you modify the name of selected group or device's parameters (vendor, model, serial number).

Delete – Deletes selected group or device depending on which part of the window you clicked on the button.

Import – Imports a list of devices from a file.

The Populate button provides an overview of all currently connected devices with information about: device type, about device vendor, model and serial number (if available).

When you are done with customization click OK. Click Cancel if you want to leave the Device groups window without saving changes.

Example

You can create different groups of devices for which different rules will be applied. You can also create only one group of devices for which the rule with action Read/Write or Read only will be applied. This ensures blocking unrecognized devices by Device control when connected to your computer.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example Read Only is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).
4.1.5.3 Adding Device control rules

A Device control rule defines the action that will be taken when a device meeting the rule criteria is connected to the computer.

Enter a description of the rule into the Name field for better identification. Click the switch next to Rule enabled to disable or enable this rule; this can be useful if you don’t want to delete the rule permanently.

Apply during – Allows you to apply created rule during the certain time. From the drop-down menu, select created time slot. For more information click here.

Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). Device type information is collected from the operating system and can be seen in the system Device manager if a device is connected to the computer. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Smart card readers include all readers of smart cards with an embedded integrated circuit, such as SIM cards or authentication cards. Examples of imaging devices are scanners or cameras. Because these devices only provide information about their actions and do not provide information about users, they can only be blocked globally.

Note

The user list functionality is not available for the modem device type. The rule will be applied for all users and the current user list will be deleted.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices allow you to select one of the following rights settings:

- **Read/Write** – Full access to the device will be allowed.
- **Block** – Access to the device will be blocked.
- **Read Only** – Only read access to the device will be allowed.
- **Warn** – Each time that a device is connected, the user will be notified if it is allowed/blocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed upon subsequent connections of the same device.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example Read Only is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).

**Criteria type** – Select Device group or Device.

Additional parameters shown below can be used to fine-tune rules and tailor them to devices. All parameters are case-insensitive:

- **Vendor** – Filter by vendor name or ID.
- **Model** – The given name of the device.
- **Serial** – External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

*Note* If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

*Note* To view information about a device, create a rule for that type of device, connect the device to your computer and then check the device details in the Device control log.

**Logging Severity**

- **Always** – Logs all events.
- **Diagnostic** – Logs information needed to fine-tune the program.
- **Information** – Records informative messages, including successful update messages, plus all records above.
- **Warning** – Records critical errors and warning messages and sends them to ERA Server.
- **None** – No logs will be recorded.

Rules can be limited to certain users or user groups by adding them to the **User list**:

- **Add** – Opens the Object types: Users or Groups dialog window that allows you to select desired users.
- **Delete** – Removes the selected user from the filter.

*Note* Not all devices can be filtered by user rules, (for example imaging devices do not provide information about users, only about actions).
4.1.6 Removable media

ESET Endpoint Security provides automatic removable media (CD/DVD/USB/...) scanning. This module allows you to scan an inserted media. This may be useful if the computer administrator wishes to prevent the users from using removable media with unsolicited content.

**Action to take after inserting removable media** – Select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). If **Show scan options** is selected, a notification will display which allows you to choose a desired action:

- **Do not scan** – No action will be performed and the **New device detected** window will be closed.
- **Automatic device scan** – An on-demand computer scan of the inserted removable media device will be performed.
- **Show scan options** – Opens the Removable media setup section.

When a removable media is inserted, following dialog will shown:

![New device detected dialog](image)

**Scan now** – This will trigger scan of removable media.

**Scan later** – Scan of removable media will be postponed.

**Setup** – Opens the Advanced setup.

**Always use the selected option** – When selected, same action will be performed when a removable media is inserted another time.

In addition, ESET Endpoint Security features the Device control functionality, which allows you to define rules for the use of external devices on a given computer. More details on Device control can be found in the [Device control](#) section.

4.1.7 Host-based Intrusion Prevention System (HIPS)

**Warning**

Changes to HIPS settings should only be made by an experienced user. Incorrect configuration of HIPS settings can lead to system instability.

The **Host-based Intrusion Prevention System (HIPS)** protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

HIPS settings can be found in **Advanced setup** (F5) > **Detection engine** > **HIPS** > **Basic**. The HIPS state (enabled/disabled) is shown in the ESET Endpoint Security main program window, in the **Setup > Computer**.
Basic

Enable HIPS – HIPS is enabled by default in ESET Endpoint Security. Turning off HIPS will disable rest of the HIPS features like Exploit Blocker.

Enable Self-Defense – ESET Endpoint Security uses the built-in Self-defense technology as a part of HIPS to prevent malicious software from corrupting or disabling your antivirus and antispyware protection. Self-defense protects crucial system and ESET’s processes, registry keys and files from being tampered with.

Enable Protected Service – Enables kernel protection (this option is available in Windows 8.1 and Windows 10).

Enable Advanced memory scanner – works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.

Enable Exploit Blocker – designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.

Ransomware shield

Enable Ransomware shield – another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.

HIPS settings

Filtering mode can be performed in one of four modes:

- **Automatic mode** – Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.
- **Smart mode** – The user will only be notified about very suspicious events.
- **Interactive mode** – User will be prompted to confirm operations.
• **Policy-based mode** – Operations are blocked.

• **Learning mode** – Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select Learning mode from the HIPS Filtering mode drop down menu, the **Learning mode will end at** setting will become available. Select the time span that you want to engage learning mode for, the maximum duration is 14 days. When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

**Mode set after learning mode expiration** – Select the filtering mode that will be used after learning mode expires.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to those used by the Firewall. Click **Edit** next to **Rules** to open the HIPS rule management window. In the HIPS rules window you can select, add, edit or remove rules. More details on rule creation and HIPS operations can be found in **Edit a HIPS rule**.

### 4.1.7.1 HIPS interactive window

The HIPS notification window allows you to create a rule based on new actions that HIPS detects and then define the conditions under which to allow or deny that action.

Rules created from the notification window are considered to be equivalent to rules created manually. A rule created from a notification window can be less specific than the rule that triggered that dialog window. This means that after creating a rule in the dialog box, the same operation can trigger the same window. For more information see **Priority for HIPS rules**.

If the default action for a rule is set to **Ask every time**, a dialog window will be displayed each time that the rule is triggered. You can choose to **Deny** or **Allow** the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

**Remember until application quits** causes the action (**Allow/Deny**) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

The **Create rule and remember permanently** option will create a new HIPS rule which can be later altered in the **HIPS rule management** section (requires administration privileges).

Click **Details** on the bottom to see what application triggers the operation, what is the reputation of the file or what kind of operation you are asked to allow or deny.

Settings for the more detailed rule parameters can be accessed by clicking **Advanced options**. The options below are available if you select **Create rule and remember permanently**:

- **Create a rule valid only for this application** – If you deselect this check box, the rule will be created for all source applications.

- **Only for operation** – Select the rule file/application/registry operation(s). **See descriptions for all HIPS operations**.

- **Only for target** – Select the rule file/application/registry target(s).

---

Endless HIPS notifications?

To stop the notifications from appearing, change the filtering mode to **Automatic mode** in **Advanced setup (F5) > Detection engine > HIPS > Basic**.
4.1.7.1.1 Potential ransomware behavior detected

This interactive window will appear when potential ransomware behavior is detected. You can choose to Deny or Allow the operation.

Click Details to view specific detection parameters. The dialog window allows you Submit for analysis or Exclude from detection.
Important
ESET LiveGrid® must be enabled for Ransomware protection to function properly.

4.1.7.2 HIPS rule management
This is a list of user-defined and automatically-added rules in the HIPS system. More details about rule creation and HIPS operations can be found in the HIPS rules settings chapter. See also General principle of HIPS.

Columns
- **Rule** – User-defined or automatically chosen rule name.
- **Enabled** – Deactivate this option if you want to keep the rule in the list but do not want to use it.
- **Action** – The rule specifies an action – **Allow**, **Block** or **Ask** – that should be performed when the conditions are met.
- **Sources** – The rule will be used only if the event is triggered by an application(s).
- **Targets** – The rule will be used only if the operation is related to a specific file, application or registry entry.
- **Log** – If you activate this option, information about this rule will be written to the HIPS log.
- **Notify** – A small pop-up notification appears in the lower-right corner if an event is triggered.

Control elements
- **Add** – Creates a new rule.
- **Edit** – Enables you to edit selected entries.
- **Delete** – Removes selected entries.

Priority for HIPS rules
There are no options to adjust the priority level of HIPS rules using the top/bottom buttons (as for Firewall rules where rules are executed from top to bottom).

- All rules that you create have the same priority
- The more specific the rule, the higher the priority (for example, the rule for a specific application has higher priority than the rule for all applications)
- Internally, HIPS contains higher-priority rules that are not accessible to you (for example, you cannot override Self-defense defined rules)
- A rule you create that might freeze your operating system will not be applied (will have the lowest priority)

4.1.7.2.1 HIPS rule settings
See HIPS rule management as first.

- **Rule name** – User-defined or automatically chosen rule name.
- **Action** – Specifies an action – **Allow**, **Block** or **Ask** – that should be performed if conditions are met.
- **Operations affecting** – You must select the type of operation for which the rule will be applied. The rule will be used only for this type of operation and for the selected target.
- **Enabled** – Disable this switch if you want to keep the rule in the list but not apply it.
- **Log** – If you activate this option, information about this rule will be written to the HIPS log.
- **Notify user** – A small pop-up window appears in the lower-right corner if an event is triggered.
The rule consists of parts that describe the conditions triggering this rule:

**Source applications** – The rule will be used only if the event is triggered by this application(s). Select **Specific applications** from drop-down menu and click **Add** to add new files or you can select **All applications** from the drop-down menu to add all applications.

**Files** – The rule will be used only if the operation is related to this target. Select **Specific files** from drop-down menu and click **Add** to add new files or folders or you can select **All files** from the drop-down menu to add all applications.

**Applications** – The rule will be used only if the operation is related to this target. Select **Specific applications** from the drop-down menu and click **Add** to add new files or folders or you can select **All applications** from the drop-down menu to add all applications.

**Registry entries** – The rule will be used only if the operation is related to this target. Select **Specific entries** from the drop-down menu and click **Add** to add new files or folders, or you can select **All entries** from the drop-down menu to add all applications.

---

**Note**

Some operations of specific rules predefined by HIPS cannot be blocked and are allowed by default. In addition, not all system operations are monitored by HIPS. HIPS monitors operations that may be considered unsafe.

---

**Descriptions of important operations:**

**File operations**

- **Delete file** – Application is asking for permission to delete the target file.
- **Write to file** – Application is asking for permission to write to the target file.
- **Direct access to disk** – Application is trying to read from or write to the disk in a non-standard way that will circumvent common Windows procedures. This may result in files being modified without the application of corresponding rules. This operation may be caused by malware trying to evade detection, backup software trying to make an exact copy of a disk, or a partition manager trying to reorganize disk volumes.
- **Install global hook** – Refers to calling the `SetWindowsHookEx` function from the MSDN library.
- **Load driver** – Installation and loading of drivers onto the system.

**Application operations**

- **Debug another application** – Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified and its data can be accessed.
- **Intercept events from another application** – The source application is attempting to catch events targeted at a specific application (for example a keylogger trying to capture browser events).
- **Terminate/suspend another application** – Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes pane).
- **Start new application** – Starting of new applications or processes.
- **Modify state of another application** – The source application is attempting to write into the target applications’ memory or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

---

**Note**

It is not possible to intercept process operations on the 64-bit version of Windows XP.
Registry operations

- **Modify startup settings** – Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the *Run* key in the Windows Registry.
- **Delete from registry** – Deleting a registry key or its value.
- **Rename registry key** – Renaming registry keys.
- **Modify registry** – Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or group rights for registry keys.

**Note**

**Using wildcards in rules**

An asterisk in rules can only be used to substitute a particular key, e.g. “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\*\Start”. Other ways of using wildcards are not supported.

**Creating rules targeting HKEY_CURRENT_USER key**

This key is just a link to the appropriate subkey of HKEY_USERS specific to the user identified by SID (secure identifier). In order to create a rule only for the current user, instead of using a path to HKEY_CURRENT_USER, use a path pointing to HKEY_USERS\%SID%. As SID you can use an asterisk to make the rule applicable for all users.

**Warning**

If you create a very generic rule, the warning about this type of rule will be shown.

In the following example, we will demonstrate how to restrict unwanted behavior of a specific application:

1. Name the rule and select **Block** (or **Ask** if you prefer to choose later) from the **Action** drop-down menu.
2. Enable the **Notify user** switch to display a notification any time that a rule is applied.
3. Select **at least one operation** in the **Operations affecting** section for which the rule will be applied.
4. Click **Next**.
5. In the **Source applications** window, select **Specific applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.
6. Click **Add** and then ... to choose a path to a specific application and then press **OK**. Add more applications if you prefer.
   For example: `C:\Program Files (x86)\Untrusted application\application.exe`
7. Select the **Write to file** operation.
8. Select **All files** from the drop-down menu. This will block any attempts to write to any files by the selected application(s) from the previous step.
9. Click **Finish** to save your new rule.
4.1.7.3  HIPS advanced setup

The following options are useful for debugging and analyzing an application’s behavior:

**Drivers always allowed to load** – Selected drivers are always allowed to load regardless of configured filtering mode, unless explicitly blocked by user rule.

**Log all blocked operations** – All blocked operations will be written to the HIPS log.

**Notify when changes occur in Startup applications** – Displays a desktop notification each time an application is added to or removed from system startup.

4.1.7.3.1  Drivers always allowed to load

Drivers shown in this list will always be allowed to load regardless of HIPS filtering mode, unless explicitly blocked by user rule.

- **Add** – Adds a new driver.
- **Edit** – Edits a selected driver.
- **Remove** – Removes a driver from the list.
- **Reset** – Reloads a set of system drivers.

**Note**

Click **Reset** if you do not want drivers that you have added manually to be included. This can be useful if you have added several drivers and you cannot delete them from the list manually.
4.1.8 Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by antivirus activity. When enabled, all pop-up windows are disabled and scheduled tasks are not run. System protection still runs in the background, but does not require any user interaction.

Click Setup > Computer and then click the switch next to Presentation mode to enable presentation mode manually. In Advanced setup (F5), click Tools > Presentation mode, and then click the switch next to Enable Presentation mode when running applications in full-screen mode automatically to have ESET Endpoint Security engage Presentation mode automatically when full-screen applications are run. Enabling Presentation mode is a potential security risk, so the protection status icon in the taskbar will turn orange and display a warning. You will also see this warning in the main program window where you will see Presentation mode enabled in orange.

When Enable Presentation mode when running applications in full-screen automatically is engaged, Presentation mode will start whenever you initiate a full-screen application and will automatically stop after you exit the application. This is especially useful for starting Presentation mode immediately after starting a game, opening a full screen application or starting a presentation.

You can also select Disable Presentation mode automatically after to define the amount of time in minutes after which Presentation mode will automatically be disabled.

Note

If the firewall is in Interactive mode and Presentation mode is enabled, you might have trouble connecting to the Internet. This can be problematic if you start a game that connects to the Internet. Normally, you would be asked to confirm such an action (if no communication rules or exceptions have been defined), but user interaction is disabled in Presentation mode. The solution is to define a communication rule for every application that might be in conflict with this behavior or to use a different Filtering mode in the firewall. Keep in mind that if Presentation mode is enabled and you go to a webpage or an application that might be a security risk, it may be blocked but you will not see any explanation or warning because user interaction is disabled.

4.1.9 Startup scan

By default, the automatic startup file check will be performed on system startup and during modules updates. This scan is dependent upon the Scheduler configuration and tasks.

Startup scan options are a part of the System startup file check scheduler task. To modify Startup scan settings, navigate to Tools > Scheduler, click on Automatic startup file check and then click Edit. In the last step, the Automatic startup file check window will appear (see the following chapter for more details).

For detailed instructions about Scheduler task creation and management, see Creating new tasks.
4.1.9.1 Automatic startup file check

When creating a System startup file check scheduled task, you have several options to adjust the following parameters:

The **Scan target** drop-down menu specifies the scan depth for files run at system startup based on secret sophisticated algorithm. Files are arranged in descending order according to the following criteria:

- **All registered files** (most files scanned)
- **Rarely used files**
- **Commonly used files**
- **Frequently used files**
- **Only the most frequently used files** (least files scanned)

Two specific groups are also included:

- **Files run before user logon** – Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll’s, etc.).
- **Files run after user logon** - Contains files from locations that may only be accessed after a user has logged in (includes files that are only run by a specific user, typically files in `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Lists of files to be scanned are fixed for each aforementioned group.

**Scan priority** – The level of priority used to determine when a scan will start:

- **When idle** – the task will be performed only when the system is idle,
- **Lowest** – when the system load is the lowest possible,
- **Lower** – at a low system load,
- **Normal** – at an average system load.

4.1.10 Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that do not handle a high number of Microsoft Office documents.

To activate Document protection, open the **Advanced setup** window (press **F5**) > **Detection engine** > **Malware scans** > **Document protection** and click the **Integrate into system** switch.

**Note**

This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).
4.1.11 Exclusions

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. However, there are situations where you may need to exclude an object, for example large database entries that would slow your computer during a scan or software that conflicts with the scan.

You can add files and folder to be excluded from scanning into the list of exclusions via Advanced setup (F5) > Detection engine > Exclusions > Files and folders to be excluded from scanning > Edit.

**Note**
Do not be confused with Excluded file extensions or Processes exclusions.

To exclude an object (path, threat or hash) from scanning, click Add and enter the path to an object or select it in the tree structure. You can also Edit or Delete selected entries.

**Types of exclusions**

- **Path** – Path to excluded files and folders.
- **Threat** – If there is a name of a threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations and it can be created either in the threat alert window reporting the infiltration (click Show advanced options and then select Exclude from detection), or by clicking Tools > Quarantine and then right-clicking the quarantined file and selecting Restore and exclude from scanning from the context menu.
- **Hash** – Excludes a file based on specified hash (SHA1), regardless of the file type, location, name or its extension.

**Note**
A threat within a file will not be detected by the Real-time file system protection module or Computer scan module if a file meets the criteria for exclusion from scanning.
Control elements

Add – Excludes objects from detection.

Edit – Enables you to edit selected entries.

Delete – Removes selected entries (CTRL + click to select multiple entries).

4.1.11.1 Add or Edit exclusion
This dialog window enables you to add or edit exclusions. Choose the exclusion Type from the drop-down menu:

Exclude path
Excludes specific path (file or directory) for this computer. Choose an appropriate path by clicking ... in the Path field.

See more exclusion format examples below.

Exclude threat
A valid ESET detection / threat name should be provided. For a valid detection name, see Log files and then select Detections from the Log files drop-down menu. This is useful when a false positive sample is being detected in ESET Endpoint Security. Exclusions for real infiltrations are very dangerous, consider excluding only affected files / directories by clicking ... in the Path mask field and/or only for a temporary period of time. Exclusions apply also to Potentially unwanted applications, potentially unsafe applications and suspicious applications.

See also Threat exclusions example below.

Exclude hash
Excludes a file based on specified hash (SHA1), regardless of the file type, location, name or its extension.
You can use wildcards to exclude a group of files with a question mark or an asterisk. A question mark (?) represents a single character whereas an asterisk (*) represents a string of zero or more characters.

**Exclusion format**
- If you want to exclude all files in a folder, type the path to the folder and use the mask `*.*`
- To exclude an entire drive including all files and subfolders, use the mask `D:*`
- If you want to exclude doc files only, use the mask `*.doc`
- If the name of an executable file has a certain number of characters (with varying characters) and you only know the first one for sure (for example, “D”), use the following format: `D?????.exe` (question marks replace the missing / unknown characters)

**System variables in exclusions**
You can use system variables like `%PROGRAMFILES%` to define scan exclusions.
- To exclude the Program Files folder using this system variable, use the path `%PROGRAMFILES%` (make sure to add the backslash at the end of path when adding to exclusions)
- To exclude all files in a `%HOMEDRIVE%` subdirectory, use the path `%HOMEDRIVE%\Excluded_Directory\*.*`

Expand list of supported system variables

The following variables can be used in the path exclusion format:
- `%ALLUSERSPROFILE%`
- `%COMMONPROGRAMFILES%`
- `%COMMONPROGRAMFILES(X86)%`
- `%COMSPEC%`
- `%HOMEDRIVE%`
- `%HOMEPATH%`
- `%PROGRAMFILES%`
- `%PROGRAMFILES(X86)%`
- `%SystemDrive%`
- `%SystemRoot%`
- `%WINDIR%`
- `%PUBLIC%`

User-specific system variables (like `%TEMP%` or `%USERPROFILE%`) or environment variables (like `%PATH%`) are not supported.
Exclusions using an asterisk

A few more exclusion examples using an asterisk:

- C:\Tools - will be automatically converted to C:\Tools\*.*
- C:\Tools\*.dat - will exclude .dat files in the Tools folder
- C:\Tools\sg.dat - will exclude this particular file located in the exact path

When you select **Exclude path**, we recommend that you do not use wild cards in the middle of a path (for example C:\Tools\*\Data\file.dat) unless your system infrastructure requires it. See the following **Knowledgebase article** for more information.

When you select **Exclude threat**, there are no restrictions to using wildcards in the middle of a path.

Order of exclusions

- There are no options to adjust the priority level of exclusions using the top/bottom buttons (as for **Firewall rules** where rules are executed from top to bottom)
- When the first applicable rule is matched by the scanner, the second applicable rule will not be evaluated
- The fewer the rules, the better the scanning performance
- Avoid creating concurrent rules

Threat exclusions

If you want to exclude a threat, enter the valid detection name:

- **Win32/Adware.Optmedia**

You can also observe the following format when you exclude a detection from the ESET Endpoint Security alert window:

- @NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
- @NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
- @NAME=Win32/Bagle.D@TYPE=worm

4.1.11.2 Path exclusion format

You can use wildcards to exclude a group of files with a question mark or an asterisk. A question mark (?) represents a single character whereas an asterisk (*) represents a string of zero or more characters.

Exclusion format

- If you want to exclude all files in a folder, type the path to the folder and use the mask *.*
- To exclude an entire drive including all files and subfolders, use the mask D:\*.
- If you want to exclude doc files only, use the mask *.doc
- If the name of an executable file has a certain number of characters (with varying characters) and you only know the first one for sure (for example, “D”), use the following format: D?????.exe (question marks replace the missing / unknown characters)

System variables in exclusions

You can use system variables like `%PROGRAMFILES%` to define scan exclusions.
To exclude the Program Files folder using this system variable, use the path \%PROGRAMFILES\ (make sure to add the backslash at the end of path when adding to exclusions)

To exclude all files in a %HOMEDRIVE% subdirectory, use the path %HOMEDRIVE%\Excluded_Directory\*.*

Expand list of supported system variables

The following variables can be used in the path exclusion format:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %HOMEDRIVE%
- %HOME\PATH%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

User-specific system variables (like %TEMP% or %USERPROFILE%) or environment variables (like %PATH%) are not supported.

4.1.12 ThreatSense parameters

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click ThreatSense parameters in the Advanced setup window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.
Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI – Scans boot sectors for the presence of viruses in the master boot record. Read more about UEFI in the glossary.

Email files – The program supports the following extensions: DBX (Outlook Express) and EML.

Archives – The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS,RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives – Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers – After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics – A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not covered by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures – Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning:

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification in the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

Warning

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive would be deleted if all the files it contains are infected files. In Strict cleaning mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.
Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in Other section are also available:

Scan alternate data streams (ADS) – Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.

Enable Smart optimization – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

Preserve last access timestamp – Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.) – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: unlimited.

Archive scan setup

Archive nesting level – Specifies the maximum depth of archive scanning. Default value: 10.

Maximum size of file in archive – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: unlimited.

Note

We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.
4.1.12.1 File extensions excluded from scanning

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Note
Do not be confused with Processes exclusions or Exclusions.

By default, all files are scanned. Any extension can be added to the list of files excluded from scanning.

Excluding files is sometimes necessary if scanning certain file types prevents the program that is using certain extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

Example
To add a new extension to the list, click Add. Type the extension into the blank field (for example tmp) and click OK. When you select Enter multiple values, you can add multiple file extensions delimited by lines, commas or semicolons (for example, choose Semicolon from drop-down menu as a separator, and type edb; eml; tmp).

You can use a special symbol ? (question mark). The question mark represents any symbol (for example ?db).

Note
In order to see the exact extension (if any) of a file in a Windows operating system you have to uncheck the Hide extensions for known file types option at Control Panel > Folder Options > View (tab) and apply this change.
4.2 Network

The firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on your filtering rules. It provides protection against attacks from remote computers and blocks some potentially dangerous services. The firewall also provides IDS/IPS functionality by inspecting the content of allowed network traffic and blocking traffic that is deemed potentially harmful. ESET Endpoint Security will inform you when you connect to an unprotected wireless network or a network with weak protection.

The **Network** section allows you to have quick access to the following components or settings in Advanced setup:

- **Firewall** – Here you can adjust the filtering mode for the ESET Firewall. To access more detailed settings, click the gear wheel > **Configure** next to **Firewall**, or press F5 to access Advanced setup.
- **Network attack protection (IDS)** – Analyzes the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked. You can disable Network attack protection for a specific period of time by clicking .
- **Botnet protection** – Quickly and accurately identifies malware in the system. To disable Botnet protection for a specific period of time, click .
- **Connected networks** – Displays the networks to which network adapters are connected. After clicking the gear wheel, you will be prompted to select a protection type for the network you are connected to via your network adapter. In this window you can also see **Network adapters** in lower right corner. You can view each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.
- **Temporary IP address blacklist** – View a list of IP addresses that have been detected as the source of attacks and added to the blacklist to block connections for a certain period of time. For more information, click this option and press F1.
- **Troubleshooting wizard** – Helps you solve connectivity problems caused by ESET Firewall. For more detailed information see [Troubleshooting wizard](#).

Click the gear wheel next to Firewall to access the following settings:
• **Configure**... – Opens the firewall window in Advanced setup, where you can define how the firewall will handle network communication.

• **Block all traffic** – All inbound and outbound communication will be blocked by the firewall. Only use this option if you suspect a critical security risk that requires the system to be disconnected from the network. To restore the firewall to normal operation while Network traffic filtering is in the **Block all traffic** mode, click **Stop blocking all traffic**.

• **Pause firewall (allow all traffic)** – The opposite of blocking all network traffic. If selected, all firewall filtering options are turned off and all incoming and outgoing connections are permitted. To re-enable the firewall while Network traffic filtering is in this mode, click **Enable firewall**.

• **Automatic mode** – (when another filtering mode is enabled) – Click to change the filtering mode to automatic filtering mode (with user-defined rules).

• **Interactive mode** – (when another filtering mode is enabled) – Click to change the filtering mode to interactive filtering mode.

### 4.2.1 Firewall

The Firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and can block potentially threatening services.

#### Basic

**Enable Firewall**

We recommend that you leave this feature enabled to ensure the security of your system. With the firewall engaged, network traffic is scanned in both directions.

**Also evaluate rules from Windows firewall**

In automatic mode, allow also incoming traffic allowed by rules from Windows Firewall, unless explicitly blocked by ESET rules.

**Filtering mode**

The behavior of the firewall changes based on the filtering mode. Filtering modes also influence the level of user interaction required.

The following filtering modes are available for the ESET Endpoint Security Firewall:

<table>
<thead>
<tr>
<th>Filtering mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic mode</strong></td>
<td>The default mode. This mode is suitable for users who prefer easy and convenient use of the firewall without the need to define rules. Custom, user-defined rules can be created but are not required in <strong>Automatic mode</strong>. Automatic mode allows all outbound traffic for a given system and blocks most inbound traffic with the exception of some traffic from the Trusted Zone (as specified in <strong>IDS and advanced options/Allowed services</strong> and responses to recent outbound communications.</td>
</tr>
<tr>
<td><strong>Interactive mode</strong></td>
<td>Allows you to build a custom configuration for your Firewall. When a communication is detected and no existing rules apply to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option to allow or deny the communication, and the decision to allow or deny can be saved as a new rule for the Firewall. If you choose to create a new rule, all future connections of this type will be allowed or blocked according to that rule.</td>
</tr>
<tr>
<td><strong>Policy-based mode</strong></td>
<td>Blocks all connections that are not defined by a specific rule that allows them. This mode allows advanced users to define rules that permit only desired and secure connections. All other unspecified connections will be blocked by the Firewall.</td>
</tr>
</tbody>
</table>
Learning mode

Automatically creates and saves rules; this mode is best used for the initial configuration of the Firewall, but should not be left on for prolonged periods of time. No user interaction is required, because ESET Endpoint Security saves rules according to predefined parameters. Learning mode should only be used until all rules for required communications have been created to avoid security risks.

Profiles

Profiles can be used to customize the behavior of the ESET Endpoint Security Firewall by specifying different sets of rules in different situations.

Enable Connected Home Monitor

Protects computers from incoming network (Wi-Fi) threats.

Notify about newly discovered network devices

Notifies you when a new device is detected on your network.

Advanced

Rules

Here you can add rules and define how the Firewall handles network traffic.

Zones

Here you can create zones containing one or multiple secure IP addresses.

Note

You can create an IDS exception when a Botnet attacks your computer. An exception can be modified in Advanced setup (F5) > Network protection > Network attack protection > IDS exceptions by clicking Edit.
4.2.1.1 Learning mode

Learning mode automatically creates and saves a rule for each communication that has been established in the system. No user interaction is required, because ESET Endpoint Security saves rules according to the predefined parameters.

This mode can expose your system to risk, and is only recommended for initial configuration of the firewall. Activate Learning mode in Advanced setup (FS) > Firewall > Learning mode settings to display Learning mode options. This section includes the following items:

**Warning**

While in Learning mode, the firewall does not filter communication. All outgoing and incoming communications are allowed. In this mode, your computer is not fully protected by the firewall.

**Mode set after learning mode expiration** – Define which filtering mode the ESET Endpoint Security Firewall will revert to after the time period for learning mode ends. Read more about filtering modes.

**Communication type** – Select specific rule creation parameters for each type of communication. There are four types of communication:

- **Inbound traffic from the Trusted zone** – An example of an incoming connection within the trusted zone would be a remote computer from within the trusted zone attempting to establish communication with a local application running on your computer.

- **Outbound traffic to the Trusted zone** – A local application attempting to establish a connection to another computer within the local network, or within a network in the trusted zone.

- **Inbound Internet traffic** – A remote computer attempting to communicate with an application running on the computer.

- **Outbound Internet traffic** – A local application attempting to establish a connection to another computer.

Each section allows you to define parameters to be added to newly created rules:

**Add local port** – Includes the local port number of the network communication. For outgoing communications, random numbers are usually generated. For this reason, we recommend enabling this option only for incoming communications.

**Add application** – Includes the name of the local application. This option is suitable for future application-level rules (rules that define communication for an entire application). For example, you can enable communication only for a web browser or email client.

**Add remote port** – Includes the remote port number of the network communication. For example you can allow or deny a specific service associated with a standard port number (HTTP – 80, POP3 – 110, etc.).

**Add remote IP address/Trusted zone** – A remote IP address or zone can be used as a parameter for new rules defining all network connections between the local system and that remote address / zone. This option is suitable if you want to define actions for a certain computer or a group of networked computers.

**Maximum number of different rules for an application** – If an application communicates through different ports to various IP addresses, etc., the firewall in learning mode creates appropriate count of rules for this application. This option allows you to limit the number of rules that can be created for one application.
4.2.2 Network attack protection

Enable Network attack protection (IDS) – Analyses the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked.

Enable Botnet protection – Detects and blocks communication with malicious command and control servers based on typical patterns when the computer is infected and a bot is attempting to communicate. Read more about Botnet protection in the glossary.

IDS exceptions – This option allows you to configure advanced filtering options to detect several types of attacks and exploits that might be used to harm your computer.

4.2.2.1 IDS exceptions

IDS exceptions allows you to configure advanced filtering options to detect several types of attacks and exploits that might be used to harm your computer.

Illustrated instructions

The following ESET Knowledgebase articles may only be available in English:

- Create IDS exclusions on client workstations in ESET Endpoint Security
- Create IDS exclusions for client workstations in ESET Security Management Center

Columns

- **Alert** – Type of alert.
- **Application** – Select the file path of an excepted application by clicking ... (for example C:\Program Files\Firefox\Firefox.exe). Do NOT enter the name of the application.
- **Remote IP** – A list of remote IPv4 or IPv6 address / ranges / subnets. Multiple addresses must be separated by a comma.
- **Block** – Each system process has its own default behavior and assigned action (block or allow). To override the default behavior for ESET Endpoint Security you can choose to block or allow it using the drop-down menu.
- **Notify** – Select Yes to display Desktop notifications on your computer. Select No if you do not want desktop notifications. The available values are Default/Yes/No.
- **Log** – Select Yes to log events to ESET Endpoint Security log files. Select No if you do not want to log events. The available values are Default/Yes/No.
Managing IDS exceptions

- **Add** – Click to create a new IDS exception.
- **Edit** – Click to edit an existing IDS exception.
- **Delete** – Select and click if you want to remove an existing exception from the list of IDS exceptions.
- **Top/Up/Down/Bottom** – Allows you to adjust the priority level of exceptions (exceptions are evaluated from top to bottom).
Example

You want to display a notification and collect a log each time the event occurs:

1. Click Add to add a new IDS exception.
2. Select particular alert from the Alert drop-down menu.
3. Click ... and select the file path of the application to which you want to apply the notification.
4. Leave Default in the Block drop-down menu. This will inherit the default action applied by ESET Endpoint Security.
5. Set both the Notify and Log drop-down menus to Yes.
6. Click OK to save this notification.

Example

You want to remove recurring notifications for a type of alert you do not consider to be a threat:

1. Click Add to add a new IDS exception.
2. Select particular alert from the Alert drop-down menu, for example SMB session without security extensions or TCP Port Scanning attack.
3. Select In from the direction drop-down menu in case it is from an inbound communication.
4. Set the Notify drop-down menu to No.
5. Set the Log drop-down menu to Yes.
7. If the communication is not coming from a particular IP address, leave Remote IP addresses blank.
8. Click OK to save this notification.

4.2.2.2 Allowed services and advanced options

The Allowed services options section allows you to configure access to some of the services running on your computer from the Trusted zone and enable/disable detection of several types of attacks and exploits that might be used to harm your computer.

Note

In some cases you will not receive a threat notification about blocked communications. Please consult the Logging and creating rules or exceptions from log section for instructions to view all blocked communications in the firewall log.

Important

The availability of particular options in this window may vary depending on the type or version of your ESET product network attack protection and/or firewall module, as well as the version of your operating system. Some of them may be available only for ESET Endpoint Security.

Allowed services

Settings in this group are meant to simplify the configuration of access to this computer’s services from the trusted zone. Many of them enable/disable predefined firewall rules.

- Allow file and printer sharing in the Trusted zone – Allows remote computers in the Trusted zone to access your shared files and printers.
- **Allow UPNP for system services in the Trusted zone** – Allows incoming and outgoing requests of UPnP protocols for system services. UPnP (Universal Plug and Play also known as Microsoft Network Discovery) is used in Windows Vista and later operating systems.

- **Allow incoming RPC communication in the Trusted zone** – Enables TCP connections from the Trusted zone allowing access to the MS RPC Portmapper and RPC/DCOM services.

- **Allow remote desktop in the Trusted zone** – Enables connections via Microsoft Remote Desktop Protocol (RDP) and allows computers in the Trusted zone to access your computer using a program that uses RDP (for example, Remote Desktop Connection).

- **Enable logging into multicast groups through IGMP** – Allows incoming/outgoing IGMP and incoming UDP multicast streams, for example video streams generated by applications using the IGMP protocol (Internet Group Management Protocol).

- **Allow communication for bridged connections** – Select this option to avoid terminating bridged connections.

- **Allow Metro applications** – Communication of Windows Store applications that are running in the Metro environment is allowed according to the Metro application manifest. This option will override all rules and exceptions for Metro applications regardless of whether you have selected Interactive mode or Policy-based mode in ESET Firewall settings.

- **Allow automatic Web Services Discovery (WSD) for system services in the Trusted zone** – Allows incoming Web Services Discovery requests from Trusted zones through the firewall. WSD is the protocol used to locate services on a local network.

- **Allow multicast addresses resolution in the Trusted zone (LLMNR)** – The LLMNR (Link-local Multicast Name Resolution) is a DNS packet based protocol that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link without requiring a DNS server or DNS client configuration. This option allows incoming multicast DNS requests from the Trusted zone through the firewall.

- **Windows HomeGroup support** – Enables HomeGroup support for Windows 7 and later operating systems. A HomeGroup is able to share files and printers on a home network. To configure a Homegroup, navigate to Start > Control Panel > Network and Internet > HomeGroup.

### Intrusion detection

- **Protocol SMB** – Detects and blocks various security problems in SMB protocol, namely:
  - **Rogue server challenge attack authentication detection** – Protects against an attack that uses a rogue challenge during authentication in order to obtain user credentials.
  - **IDS evasion during named pipe opening detection** – Detection of known evasion techniques used for opening MSRPCS named pipes in SMB protocol.
  - **CVE detections** (Common Vulnerabilities and Exposures) – Implemented detection methods of various attacks, forms, security holes and exploits over SMB protocol. Please see the [CVE website at cve.mitre.org](http://cve.mitre.org) to search and obtain more detailed info about CVE identifiers (CVEs).

- **Protocol RPC** – Detects and blocks various CVEs in the remote procedure call system developed for the Distributed Computing Environment (DCE).

- **Protocol RDP** – Detects and blocks various CVEs in the RDP protocol (see above).

- **ARP Poisoning attack detection** – Detection of ARP poisoning attacks triggered by man in the middle attacks or detection of sniffing at network switch. ARP (Address Resolution Protocol) is used by the network application or device to determine the Ethernet address.

- **Allow response to ARP requests from outside the Trusted zone** – Select this option if you want the system to respond to ARP requests with IP addresses that are not from the Trusted zone. ARP (Address Resolution Protocol) is used by the network application to determine the Ethernet address.
• **DNS Poisoning attack detection** – Detection of DNS poisoning – relieving a fake answer to a DNS request (sent by an attacker) which can point you to fake and malicious websites. DNS (Domain name systems) are distributed database systems that translate between human-friendly domain names and numeric IP addresses and allow users to refer to a website simply by using its domain name. Read more about this type of attack in the glossary.

• **TCP/UDP Port Scanning attack detection** – Detects attacks of port scanning software – application designed to probe a host for open ports by sending client requests to a range of port addresses with the goal of finding active ports and exploiting the vulnerability of the service. Read more about this type of attack in the glossary.

• **Block unsafe address after attack detection** – IP addresses that have been detected as sources of attacks are added to the Blacklist to prevent connection for a certain period of time.

• **Display notification after attack detection** – Turns on the system tray notification at the bottom right corner of the screen.

• **Display notifications also for incoming attacks against security holes** – Alerts you if attacks against security holes are detected or if an attempt is made by a threat to enter the system this way.

### Packet inspection

• ** Allow incoming connection to admin shares in SMB protocol** - The administrative shares (admin shares) are the default network shares that share hard drive partitions (C$, D$, ...) in the system together with the system folder (ADMIN$). Disabling connection to admin shares should mitigate many security risks. For example, the Conficker worm performs dictionary attacks in order to connect to admin shares.

• **Deny old (unsupported) SMB dialects** – Deny SMB sessions that use an old SMB dialect unsupported by IDS. Modern Windows operating systems support old SMB dialects due to backward compatibility with old operating systems such as Windows 95. The attacker can use an old dialect in an SMB session in order to evade traffic inspection. Deny old SMB dialects if your computer does not need to share files (or use SMB communication in general) with a computer with an old version of Windows.

• **Deny SMB sessions without extended security** – Extended security can be used during the SMB session negotiation in order to provide a more secure authentication mechanism than LAN Manager Challenge/Response (LM) authentication. The LM scheme is considered weak and is not recommended for use.

• **Deny opening of executable files on a server outside the Trusted zone in SMB protocol** – Drops connection when you are trying to open an executable file (.exe, .dll, ...) from a shared folder on the server that does not belong to the Trusted zone in firewall. Note that copying executable files from trusted sources can be legitimate, however this detection should mitigate risks from the unwanted opening of a file on a malicious server (for example, a file opened by clicking a hyperlink to a shared malicious executable file).

• **Deny NTLM authentication in SMB protocol for connecting a server in/outside the Trusted zone** – Protocols that use NTLM (both versions) authentication schemes are subject to a credentials forwarding attack (known as an SMB Relay attack in the case of SMB protocol). Denying NTLM authentication with a server outside the Trusted zone should mitigate risks from forwarding credentials by a malicious server outside the Trusted zone. Similarly, you can deny NTLM authentication with servers in the Trusted zone.

• **Allow communication with the Security Account Manager service** – For more information about this service see [MS-SAMR].

• **Allow communication with the Local Security Authority service** – For more information about this service see [MS-LSAD] and [MS-LSAT].

• **Allow communication with the Remote Registry service** – For more information about this service see [MS-RRP].

• **Allow communication with the Service Control Manager service** – For more information about this service see [MS-SCMR].

• **Allow communication with the Server service** – For information about this service see [MS-SRVS].

• **Allow communication with the other services** – Other MSRPC services. MSRPC is the Microsoft implementation of the DCE RPC mechanism. Moreover, MSRPC can use named pipes carried into the SMB (network file sharing)
protocol for transport (ncacn_np transport). MSRPC services provide interfaces for accessing and managing
windows systems remotely. Several security vulnerabilities have been discovered and exploited in the wild in the
Windows MSRPC system (for example, Conficker worm, Sasser worm,...). Disable communication with MSRPC
services that you do not need to provide to mitigate many security risks (such as remote code execution or service
failure attacks).

- **Check TCP connection status** – Checks to see if all TCP packets belong to an existing connection. If a packet does
  not exist in a connection, it will be dropped.

- **Maintain inactive TCP connections** – In order to function, some applications require that the TCP connection that
  they establish is maintained even though the TCP connection may be inactive. Select this option to avoid
  terminating inactive TCP connections.

- **TCP protocol overload detection** – The principle of this method involves exposing the computer/server to
  multiple requests – also see DoS (Denial of service attacks).

- **ICMP protocol message checking** – Prevents attacks that exploit the weaknesses of the ICMP protocol, which
  could lead to computer unresponsiveness - also see DoS (Denial of service attacks).

- **Covert data in ICMP protocol detection** – Checks to see if the ICMP protocol is used for data transfer. Many
  malicious techniques use the ICMP protocol to bypass the firewall.

Please see this ESET Knowledgebase article for an updated version of this help page.

### 4.2.2.3 Suspected threat blocked

This situation can occur when an application on your computer is trying to transmit malicious traffic to another
computer on the network, exploiting a security hole or if someone is trying to scan ports on your network.

- **Threat** – Name of the threat.
- **Source** – Source network address.
- **Target** – Target network address.
- **Stop blocking** – Creates an IDS exception for the suspected threat with settings to allow communication.
- **Keep blocking** – Blocks the detected threat. To create an IDS exception with settings to block communication for this
  threat, select Do not notify me again.

**Note**

Information shown in this notification window may vary depending on the type of threat detected.

For more information about threats and other related terms see Types of remote attacks or Types of
detections.

### 4.2.2.4 Network protection troubleshooting

The Troubleshooting wizard helps you resolve connectivity problems caused by the ESET Firewall. From the drop-
down menu, select a period of time during which communication has been blocked. A list of recently blocked
communications gives you an overview about the type of application or device, reputation and total number of
application and devices blocked during that time period. For more details about blocked communication, click
Details. The next step is to unblock the application or device on which you are experiencing connectivity problems.

When you click Unblock, the previously blocked communication will be allowed. If you continue to experience
problems with an application, or your device does not work as expected, click The application still doesn't work and
all communications previously blocked for that device will now be allowed. If the issue persist, restart the
computer.

Click Show changes to see rules created by the wizard. Additionally, you can see rules created by the wizard
Advanced setup > Network protection > Firewall > Basic > Rules.
Click **Unblock another** to troubleshoot communications issues with a different device or application.

### 4.2.3 Connected networks

The Connected network section is accessible from the main program window of ESET Endpoint Security by clicking **Setup > Network > Connected networks**.

It shows the networks to which network adapters are connected. After clicking the link below the network name, you will be prompted to select a protection type (strict or allowed) for the network you are connected to via your network adapter, or you can click the gear wheel 🔄 to change this selection in Advanced setup. This setting defines how accessible your computer is to other computers on the network.

Clicking the **Network adapters** in lower right corner of the window allows you to view each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.

### 4.2.4 Known networks

When using a computer that frequently connects to public networks or networks outside of your normal work network, we recommend that you verify the network credibility of new networks that you are connecting to. Once networks are defined, ESET Endpoint Security can recognize trusted (Home/office) networks using various network parameters configured in **Network Identification**. Computers often enter networks with IP addresses that are similar to the trusted network. In such cases, ESET Endpoint Security may consider an unknown network to be trusted (Home/office). We recommend that you use **Network authentication** to avoid this type of situation.

When a network adapter is connected to a network or its network settings are reconfigured, ESET Endpoint Security will search the known network list for a record that matches the new network. If **Network identification** and **Network authentication** (optional) match, the network will be marked connected in this interface. When no known network is found, network identification configuration will create a new network connection to identify the network the next time that you connect to it. By default, the new network connection uses the **Public network** protection type. The **New Network Connection Detected** dialog window will prompt you to choose between the **Public network, Home or office network** or **Use Windows setting** protection type. If a network adapter is connected to a known network and that network is marked as **Home or office network**, local subnets of the adapter will be added to the Trusted zone.

**Protection type of new networks** – Select which of the following options: **Use Windows setting**, **Ask user** or **Mark as public** is used by default for new networks.

#### Note

When you select **Use Windows setting** a dialog will not appear and the network you are connected to will automatically be marked according to your Windows settings. This will cause certain features (for example file sharing and remote desktop) to become accessible from new networks.

Known networks can be configured manually in the **Known networks editor** window.

### 4.2.4.1 Known networks editor

Known networks can be configured manually in **Advanced setup > Network protection > Firewall > Known Networks** by clicking **Edit** next to **Known networks**.

**Columns**

- **Name** – Name of known network.
- **Protection type** – Shows if the network is set to **Home or office network**, **Public** or **Use Windows setting**.
- **Firewall profile** – Select a profile from the **Display rules used in the profile** drop-down menu to display the profiles rules filter.
- **Update profile** – Allows you to apply created update profile when connected to this network.
Control elements

Add – Creates a new known network.

Edit – Click to edit an existing known network.

Delete – Select a network and click Delete to remove it from the list of known networks.

Top/Up/Down/Bottom – Allows you to adjust the priority level of known networks (networks are evaluated from top to bottom).

Network configuration settings are arranged in the following tabs:

Network

Here you can define the **Network name** and select the **Protection type** (Public network, Home or office network or Use Windows setting) for the network. Use the **Firewall profile** drop-down menu to select the profile for this network. If the network uses the **Home or office network** protection type, all directly connected network subnets are considered trusted. For example, if a network adapter is connected to this network with the IP address 192.168.1.5 and the subnet mask 255.255.255.0, the subnet 192.168.1.0/24 is added to that adapter’s trusted zone. If the adapter has more addresses/subnets, all of them will be trusted, regardless of the **Network Identification** configuration of the known network.

Additionally, addresses added under **Additional trusted addresses** are always added to the trusted zone of adapters connected to this network (regardless of the network’s protection type).

**Warn about weak WiFi encryption** – ESET Endpoint Security will inform you when you connect to an unprotected wireless network or network with weak protection.

**Firewall profile** – Select firewall profile that will be used when connected to this network.

**Update profile** – Select update profile that will be used when connected to this network.

The following conditions must be met for a network to be marked as connected in the list of connected networks:

- Network identification – All filled in parameters must match active connection parameters.
- Network authentication – if authentication server is selected, successful authentication with the ESET Authentication Server must take place.

**Network identification**

Network identification is performed based on the local network adapter’s parameters. All selected parameters are compared against the actual parameters of active network connections. IPv4 and IPv6 addresses are allowed.
Network authentication

Network authentication searches for a specific server in the network and uses asymmetric encryption (RSA) to authenticate that server. The name of the network being authenticated must match the zone name set in authentication server settings. The name is case sensitive. Specify a server name, server listening port and a public key that corresponds to the private server key (see Network authentication – Server configuration). The server name can be entered in the form of an IP address, DNS or NetBios name and can be followed by a path specifying the location of the key on the server (for example, server_name_/directory1/directory2/authentication). You can specify alternate servers to use by appending them to the path, separated by semicolons.

Download the ESET Authentication Server.

The public key can be imported using any of the following file types:

- PEM encrypted public key (.pem), this key can be generated using the ESET Authentication Server (see Network authentication – Server configuration).
- Encrypted public key
- Public key certificate (.crt)
Click **Test** to test your settings. If authentication is successful, *Server authentication was successful* will be displayed. If authentication is not configured properly, one of the following error messages will be displayed:

- **Server authentication failed. Invalid or mismatched signature.**
  
  Server signature does not match the public key entered.

- **Server authentication failed. Network name doesn’t match.**
  
  The configured network name does not correspond with the authentication server zone name. Review both names and ensure they are identical.

- **Server authentication failed. Invalid or no response from server.**
  
  No response is received if the server is not running or is inaccessible. An invalid response may be received if another HTTP server is running on the specified address.

- **Invalid public key entered.**
  
  Verify that the public key file you have entered is not corrupted.

### 4.2.4.2 Network authentication - Server configuration

The authentication process can be executed by any computer/server connected to the network that is to be authenticated. The ESET Authentication Server application needs to be installed on a computer/server that is always accessible for authentication whenever a client attempts to connect to the network. The installation file for the ESET Authentication Server application is available for download on ESET’s website.

After you install the ESET Authentication Server application, a dialog window will appear (you can access the application by clicking **Start > Programs > ESET > ESET Authentication Server**).

To configure the authentication server, enter the authentication network name, the server listening port (default is 80) as well as the location to store the public and private key pair. Next, generate the public and private key that will be used in the authentication process. The private key will remain on the server while the public key needs to be imported on the client side in the Network authentication section when setting up a network in the firewall setup.
4.2.5  Firewall profiles

Global default profile – If there is no profile from network nor from network adapter configuration, the global default profile is used.

List of profiles – Profiles can be used to control the behavior of the ESET Endpoint Security Firewall. When creating or editing a firewall rule, you can assign it to a specific profile, or have it apply to every profile. When a profile is active on a network interface, only the global rules (rules with no profile specified) and the rules that have been assigned to that profile are applied to it. You can create multiple profiles with different rules assigned to network adapters or assigned to networks to easily alter firewall behavior.

Profiles assigned to network adapters – A network adapter can be set up to use a profile configured for a specific network when it is connected to that network.

You can also assign a specific profile to use when on a given network in Advanced setup (FS) > Firewall > Known networks. Select a network from the list of Known networks and click Edit to assign a firewall profile to the specific network from the Firewall profile drop-down menu. If that network has no assigned profile, then the adapter’s default profile will be used. If the adapter is set up not to use the network’s profile, its default profile will be used regardless of which network it is connected to. If there is no profile for a network or for adapter configuration, the global default profile is used. To assign a profile to a network adapter, select the network adapter, click Edit next to Profiles assigned to network adapters, select the profile from Default firewall profile drop-down menu and then click OK.

When the firewall switches to another profile, a notification will appear in the lower right corner by the system clock.

4.2.5.1  Profiles assigned to network adapters

By switching profiles you can quickly make multiple changes to firewall behavior. Custom rules can be set and applied for particular profiles. Network adapter entries for all adapters present on the machine are added to the list of Network adapters automatically.

Columns

- **Name** – Name of the network adapter.
- **Default firewall profile** – The default profile is used when the network you are connected to has no configured profile, or your network adapter is set not to use a network profile.
- **Prefer network’s profile** – Network adapter can use firewall profile configured for the connected known network. If that network has no configured profile, or network adapter is set up not to use the network’s profile, then adapter’s default profile is used.

Control elements

- **Add** – Adds a new network adapter.
- **Edit** – Allows you to edit an existing network adapter.
- **Delete** – Select a network adapter and click Delete if you want to remove a network adapter from the list.
- **OK/Cancel** – Click OK if you want to save changes or click Cancel to leave without any changes.
4.2.6 Application modification detection

The application modification detection feature displays notifications if modified applications, for which a firewall rule exists, attempt to establish connections. This is useful to avoid abusing rules configured for some application by another application by temporarily or permanently replacing the original application’s executable file with the other applications executable file, or by maliciously modifying the original application’s executable file.

Please be aware that this feature is not meant to detect modifications to any application in general. The goal is to avoid abusing existing firewall rules, and only applications for which specific firewall rules exist are monitored.

**Enable detection of application modifications** – If selected, the program will monitor applications for changes (updates, infections, other modifications). When a modified application attempts to establish a connection, you will be notified by the firewall.

**Allow modification of signed (trusted) applications** – Don’t notify if the application has the same valid digital signature before and after the modification.

**List of applications excluded from checking** – This window allows you add or remove individual applications for which modifications are allowed without notification.

4.2.6.1 Applications excluded from modification detection

The firewall in ESET Endpoint Security detects changes to applications for which rules exist (see Application modification detection).

In certain cases you may not want to use this functionality for some applications if you want to exclude them from checking by the firewall.

**Add** – Opens a window where you can select an application to add to the list of applications excluded from modification detection.

**Edit** – Opens a window where you can change the location of an application that is on the list of applications excluded from modification detection.

**Delete** – Removes entries from the list of applications excluded from modification detection.

4.2.7 Configuring and using rules

Rules represent a set of conditions used to test all network connections and all actions assigned to these conditions. Using a firewall rules, you can define the action that is taken when different types of network connections are established. To access rule filtering setup, navigate to **Advanced setup (F5) > Network protection > Firewall > Advanced**. Some of predefined rules are bound to the check boxes from **allowed services** (Allowed services and advanced options) and they can not be turned off directly, instead you can use those related check boxes to do it.

Unlike the previous version of ESET Endpoint Security, rules are evaluated from top to bottom. The action of the first matching rule is used for each network connection being evaluated. This is an important behavioral change from the previous version, in which the priority of rules was automatic and more specific rules had higher priority then more general ones.

Connections can be divided into incoming and outgoing connections. Incoming connections are initiated by a remote computer attempting to establish a connection with the local system. Outgoing connections work the opposite way – the local system contacts a remote computer.

If a new unknown communication is detected, consider carefully whether to allow or deny it. Unsolicited, unsecured or unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay particular attention to the remote computer and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data, or download other malicious applications to host workstations. The firewall allows you to detect and terminate such connections.
4.2.7.1 Firewall rules

Click Edit next to Rules in the Advanced tab section to display the Firewall rules window, where the list of all rules is displayed. Add, Edit, and Delete allow you to add, configure or delete rules. You can adjust the priority level of a rule by selecting a rule(s) and clicking Top/Up/Down/Bottom.

Note
Click the icon to search for rule(s) by name, protocol or port.

Columns

Name – Name of rule.

Enabled – Shows if rule is enabled or disabled; the corresponding check box must be selected to activate a rule.

Protocol – The protocol this rule is valid for.

Profile – Shows the firewall profile this rule is valid for.

Action – Shows the status of communication (block/allow/ask).

Direction – Direction of communication (incoming/outgoing/both).

Local – IP address and port of local computer.

Remote – IP address and port of remote computer.

Applications – The application to which the rule applies.

Control elements

Add – Creates a new rule.

Edit – Edit an existing rule.

Delete – Remove an existing rule.

Copy - Create a copy of a selected rule.

Show built in (predefined) rules – Rules predefined by ESET Endpoint Security which allow or deny specific communications. You can disable these rules, but you cannot delete a predefined rule.
Top/Up/Down/Bottom – Allows you to adjust the priority level of rules (rules are executed from top to bottom).

4.2.7.2 Working with rules
Modification is required each time that monitored parameters are changed. If changes are made such that a rule cannot fulfill the conditions and the specified action cannot be applied, the given connection may be refused. This can lead to problems with the operation of the application affected by a rule. An example is a change of network address or port number for the remote side.

The upper part of the window contains three tabs:

- **General** – Specify a rule name, the direction of the connection, the action (Allow, Deny, Ask), the protocol and the profile to which the rule will apply.
- **Local** – Displays information about the local side of the connection, including the number of the local port or port range and the name of the communicating application. Also allows you to add a predefined or created zone with a range of IP addresses here by clicking Add.
- **Remote** – This tab contains information about the remote port (port range). It allows you to define a list of remote IP addresses or zones for a given rule. You can also add a predefined or created zone with range of IP addresses here by clicking Add.

When creating a new rule, you must enter a name for the rule in the Name field. Select the direction to which the rule applies from the Direction drop-down menu and the action to be executed when a communication meets the rule from the Action drop-down menu.

**Protocol** represents the transfer protocol used for the rule. Select which protocol to use for a given rule from the drop-down menu.

**ICMP Type/Code** represents an ICMP message identified by a number (for example; 0 represents "Echo Reply").

All rules are enabled for Any profile by default. Alternatively, select a custom firewall profile using the Profiles drop-down menu.

If you enable Log, the activity connected with the rule will be recorded in a log. Notify user displays a notification when the rule is applied.

**Note**
Logs with Warning status can be collected by ESET Remote Administrator.

Below is an example in which we create a new rule to allow the web browser application to access the network. In this example, the following must be configured:

- In the **General** tab, enable outgoing communication via the TCP and UDP protocol.
- Add your browser application (for Internet Explorer it is iexplore.exe) in the **Local** tab.
- In the **Remote** tab, enable port number 80 if you want to allow standard Internet browsing.

**Note**
Please be aware that predefined rules can be modified in limited way.
4.2.8  Temporary IP address blacklist
To view IP addresses that have been detected as sources of attacks are added to the blacklist to block connection for a certain period of time, from ESET Endpoint Security navigate to Setup > Network protection > Temporary IP address blacklist.

Columns
- **IP address** – shows an IP address that has been blocked.
- **Block reason** – shows type of attack that has been prevented from the address (for example TCP Port Scanning attack).
- **Timeout** – shows time and date when the address will expire from the black list.

Control elements
- **Remove** – click to remove an address from the blacklist before it will expire.
- **Remove all** – click to remove all addresses from the blacklist immediately.
- **Add exception** – click to add an firewall exception into IDS filtering.

4.2.9  Trusted zone
The trusted zone represents a group of network addresses from which the firewall allows some inbound traffic using default settings. Settings for features like file sharing and remote desktop inside of the trusted zone are determined in Allowed services and advanced options.

The actual trusted zone is computed dynamically and separately for each network adapter based on what network the computer is currently connected to. Addresses defined as inside of the trusted zone in the Zones editor are always trusted. If a network adapter is connected to a known network, then the Additional trusted addresses configured for that network are added to the adapter's trusted zone. If a network has the Home/office protection type, all directly connected subnets are included in the trusted zone. The actual trusted zone for each network adapter can be viewed from the Setup window under Network > Network adapters.

**Note**
Per-interface trusted zone is not supported on Windows XP operating systems. For these operating systems, all adapters have the same trusted zone, and this is also visible in the Network adapters page.

4.2.10  Configuring zones
A zone represents a collection of network addresses that create one logical group of IP addresses, useful when you need to reuse the same set of addresses in multiple rules. Each address in a given group is assigned similar rules defined centrally for the whole group. One example of such a group is a Trusted zone. A Trusted zone represents a group of network addresses that are not blocked by the Firewall in any way. These zones can be configured in Advanced setup > Network protection> Firewall > Advanced, by clicking Edit next to Zones. To add a new zone click Add, enter a Name for the zone, a Description and add a remote IP address into the Remote computer address (IPv4/IPv6, range, mask) field.

In the Firewall zones setup window, you can specify a zone name, description, network address list (see also Known networks editor).
4.2.10.1 Firewall zones

For more information about zones, see the section Configuring zones.

Columns

- **Name** – Name of a group of remote computers.
- **IP addresses** – Remote IP addresses that belong to a zone.

Control elements

When you add or edit a zone, the following fields are available:

- **Name** – Name of a group of remote computers.
- **Description** – A general description of the group.
- **Remote computer address (IPv4, IPv6, range, mask)** – Allows you to add a remote address, address range or subnet.
- **Delete** – Removes a zone from the list.

**Note**

Please be aware that predefined zones cannot be removed.

4.2.11 Firewall log

The ESET Endpoint Security Firewall saves all important events in a log file, which can be viewed directly from the main menu. Click **Tools > Log files**, and then select **Firewall** from the **Log** drop-down menu. To enable firewall logging, navigate to **Advanced setup > Tools > Log files** and set the minimum logging verbosity to **Diagnostic**. All denied connections will be recorded.

Log files can be used to detect errors and reveal intrusions on your system. The ESET Firewall logs contain the following data:

- **Time** – Date and time of event.
- **Event** – Name of event.
- **Source** – Source network address.
- **Target** – Target network address.
- **Protocol** – Network communication protocol.
- **Rule/worm name** – Rule applied, or name of worm, if identified.
- **Application** – Application involved.
- **User** – Name of the user logged in at the time the infiltration was detected.

A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and allow you to minimize their impact. Some examples of potential threat indicators include frequent connections from unknown locations, multiple attempts to establish connections and unknown applications communicating or unusual port numbers being used.
4.2.12 Establishing connection - detection

The firewall detects each newly-created network connection. The active firewall mode determines which actions are performed for the new connection. If **Automatic mode** or **Policy-based mode** is activated, the firewall will perform predefined actions with no user interaction.

Interactive mode displays an informational window that reports detection of a new network connection, supplemented with detailed information about the connection. You can opt to allow the connection or refuse (block) it. If you repeatedly allow the same connection in the dialog window, we recommend that you create a new rule for the connection. To do this, select **Remember action (create rule)** and save the action as a new rule for the firewall. If the firewall recognizes the same connection in the future, it will apply the existing rule without requiring user interaction.

**Temporarily remember action for the process** causes an action (Allow/Deny) to be used until application restart, a change of rules or filtering modes, a Firewall module update or a system restart. After any of these actions, temporary rules will be deleted.

![Inbound network traffic](image)

Please be careful when creating new rules and only allow connections that you know are secure. If all connections are allowed, then the firewall fails to accomplish its purpose. These are the important parameters for connections:

- **Remote side** – Only allow connections to trusted and known addresses.
- **Local application** – It is not advisable to allow connections for unknown applications and processes.
- **Port number** – Communication on common ports (for example, web traffic – port number 80) should be allowed under normal circumstances.

In order to proliferate, computer infiltrations often use the Internet and hidden connections to help them infect remote systems. If rules are configured correctly, a firewall becomes a useful tool for protection against a variety of malicious code attacks.
4.2.13 Solving problems with ESET Firewall

If you experience connectivity problems with ESET Endpoint Security installed, there are several ways to tell if the ESET Firewall is causing the issue. Moreover, ESET Firewall can help you create new rules or exceptions to resolve connectivity problems.

See the following topics for help resolving problems with the ESET Firewall:

- Troubleshooting wizard
- Logging and creating rules or exceptions from log
- Creating exceptions from firewall notifications
- Advanced PCAP logging
- Solving problems with protocol filtering

4.2.13.1 Troubleshooting wizard

The troubleshooting wizard silently monitors all blocked connections, and will guide you through the troubleshooting process to correct firewall issues with specific applications or devices. Next, the wizard will suggest a new set of rules to be applied if you approve them. **Troubleshooting wizard** can be found in the main menu under **Setup > Network**.

4.2.13.2 Logging and creating rules or exceptions from log

By default, the ESET Firewall does not log all blocked connections. If you want to see what was blocked by the firewall, enable Network protection advanced logging in the **Diagnostics** section of **Advanced setup** under **Tools > Diagnostics**. If you see something in the log that you do not want the firewall to block, you can create a rule or an IDS exception for it by right-clicking on that item and selecting **Don’t block similar events in the future**. Please note that the log of all blocked connections can contain thousands of items and it might be difficult to find a specific connection in this log. You can turn logging off after you have resolved your issue.

For more information about the log see **Log files**.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use logging to see the order in which the firewall blocked specific connections. Moreover, creating rules from the log allows you to create rules that do exactly what you want.</td>
</tr>
</tbody>
</table>

4.2.13.2.1 Create rule from log

The new version of ESET Endpoint Security allows you to create a rule from the log. From the main menu click **Tools > Log files**. Choose **Network protection** from drop-down menu, right-click your desired log entry and select **Don’t block similar events in the future** from the context menu. A notification window will display your new rule.

To allow for the creation of new rules from the log, ESET Endpoint Security must be configured with the following settings:

- set the minimum logging verbosity to **Diagnostic** in **Advanced setup (F5) > Tools > Log files**,
- enable **Display notifications also for incoming attacks against security holes** in **Advanced setup (F5) > Network protection > Network attack protection > Advanced options > Intrusion detection**.
4.2.13.3 Creating exceptions from firewall notifications

When ESET Firewall detects malicious network activity, a notification window describing the event will be displayed. This notification contains a link that will allow you to learn more about the event and set up an exception for this event if you want.

**Note**
If a network application or device does not implement network standards correctly it can trigger repetitive firewall IDS notifications. You can create an exception directly from the notification to keep the ESET Firewall from detecting this application or device.

4.2.13.4 Advanced PCAP logging

This feature is intended to provide more complex log files for ESET customer support. Use this feature only when requested to by ESET customer support, as it might generate a huge log file and slow down your computer.

1. Navigate to Advanced setup > Tools > Diagnostics and enable Enable Protocol filtering advanced logging.
2. Attempt to reproduce the problem you are experiencing.
3. Disable advanced PCAP logging.
4. The PCAP log file can be found in the same directory where diagnostic memory dumps are generated:
   - Microsoft Windows Vista or newer
     \ProgramData\ESET\ESET Security\Diagnostics\n   - Microsoft Windows XP
     \Documents and Settings\All Users... \n
4.2.13.5 Solving problems with protocol filtering

If you experience problems with your browser or email client, the first step is to determine if protocol filtering is responsible. To do that, try temporarily disabling application protocol filtering in the advanced setup (remember to turn it back on after you’re finished, otherwise your browser and email client will remain unprotected). If your problem disappears after turning it off, here is a list of common problems and a way to solve them:

**Update or secure communication problems**

If your application complains about the inability to update or that a communication channel is not secure:

- If you have SSL protocol filtering enabled, try temporarily turning it off. If that helps, you can keep using SSL filtering and make the update work by excluding the problematic communication:
  Switch SSL protocol filtering mode to interactive. Rerun the update. There should be a dialog informing you about encrypted network traffic. Make sure the application matches the one you’re troubleshooting and the certificate looks like coming from the server it is updating from. Then choose to remember action for this certificate and click ignore. If no more relevant dialogs are show, you can switch the filtering mode back to automatic and the problem should be solved.

- If the application in question is not a browser or email client, you can completely exclude it from protocol filtering (doing this for browser or email client would leave you exposed). Any application that had its communication filtered in the past should already be in the list provided to you when adding exception, so manually adding one shouldn’t be necessary.
Problem accessing a device on your network

If you are unable to use any functionality of a device on your network (this could mean opening a webpage of your webcam or playing video on a home media player), try adding its IPv4 and IPv6 addresses to the list of excluded addresses.

Problems with a particular website

You can exclude specific websites from protocol filtering using URL address management. For example if you can’t access https://www.gmail.com/intl/en/mail/help/about.html, try adding *gmail.com* to the list of excluded addresses.

Error "Some of the applications capable of importing the root certificate are still running“

When you enable SSL protocol filtering, ESET Endpoint Security makes sure that installed applications trust the way it filters SSL protocol by importing a certificate to their certificate store. For some applications this is not possible while they are running. This includes Firefox and Opera. Make sure none of them are running (the best way to do this is to open Task Manager and make sure there is no firefox.exe or opera.exe under Processes tab), then hit retry.

Error about untrusted issuer or invalid signature

This most likely means that the import described above failed. First make sure that none of the mentioned applications are running. Then disable SSL protocol filtering and enable it back on. This reruns the import.

4.3 Web and email

Web and email configuration can be found under Setup > Web and email. From here you can access more detailed program settings.

The Web control module allows you to configure settings that provide administrators with automated tools to help protect their workstations and set restrictions for internet browsing. The aim of the Web control functionality is to prevent access to pages with inappropriate or harmful content. See Web control for more information.
Internet connectivity is a standard feature for personal computers. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection.

**Email client protection** provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in program for your email client, ESET Endpoint Security provides control of all communications from the email client (POP3, IMAP, HTTP, MAPI).

**Antispam protection** filters unsolicited email messages.

When you click the gear wheel next to Antispam protection the following options are available:

- **Configure...** — Opens advanced settings for Email client antispam protection.

- **User's Whitelist/Blacklist/Exceptions list** — Opens a dialog window where you can add, edit or delete email addresses that are considered safe or unsafe. According to rules defined here, email from these addresses will not be scanned or will be treated as spam. Click **User’s Exceptions list** to open a dialog where you can add, edit or delete email addresses that may be spoofed and used for sending spam. Email messages received from addresses listed in the Exception list will always be scanned for spam.

**Anti-Phishing protection** is another layer of protection that provides increased defense from illegitimate websites that attempt to acquire passwords and other sensitive information. Anti-Phishing protection can be found in the Setup pane under Web and email. See Anti-Phishing protection for more information.

**Disable** — Click the switch to disengage web/email/antispam protection for web browsers and email clients.

### 4.3.1 Protocol filtering

Antivirus protection for application protocols is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. To edit encrypted (SSL) settings, go to Web and email > SSL.

**Enable application protocol content filtering** — Can be used to disable protocol filtering. Note that many ESET Endpoint Security components (Web access protection, Email protocols protection, Anti-Phishing, Web control) depend on this and will be non-functional without it.

**Excluded applications** — Allows you to exclude specific applications from protocol filtering. Useful when protocol filtering causes compatibility issues.

**Excluded IP addresses** — Allows you to exclude specific remote addresses from protocol filtering. Useful when protocol filtering causes compatibility issues.

#### 4.3.1.1 Web and email clients

Starting with Windows Vista Service Pack 1 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since WFP technology uses special monitoring techniques, the Web and email clients section is not available.

Because of the enormous amount of malicious code circulating the Internet, safe Internet browsing is a very important aspect of computer protection. Web browser vulnerabilities and fraudulent links help malicious code enter the system unnoticed which is why ESET Endpoint Security focuses on web browser security. Each application accessing the network can be marked as an Internet browser. Applications that already used protocols for communication or application from selected path can be entered to the list of Web and email clients.
4.3.1.2 Excluded applications

To exclude communications for specific network-aware applications from protocol filtering, add them to this list. HTTP/POP3/IMAP communication for the selected applications will not be checked for threats. We recommend that you only use this technique in cases where applications do not function properly with protocol filtering enabled.

Applications and services that were already affected by protocol filtering will be automatically displayed after clicking **Add**.

**Edit** – Edit selected entries from the list.

**Delete** – Remove selected entries from the list.
4.3.1.3 Excluded IP addresses

IP addresses in this list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Add – Click to add an IP address/address range/subnet of a remote point to which a rule is applied.

Edit – Edit selected entries from the list.

Delete – Remove selected entries from the list.

4.3.1.4 SSL/TLS

ESET Endpoint Security is capable of checking for threats in communications that use the SSL protocol. You can use various scanning modes to examine SSL protected communications with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering – Protocol filtering is enabled by default. You can disable SSL/TLS protocol filtering in Advanced setup > Web and email > SSL/TLS or via policy. If protocol filtering is disabled, the program will not scan communications over SSL.

SSL/TLS protocol filtering mode is available in following options:

Automatic mode – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

Interactive mode – If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL certificates that will be excluded from scanning.

Policy mode – All SSL/TLS protected sites are filtered, except configured exclusions. Either applications or server certificates can be excluded.

The List of SSL/TLS filtered applications can be used to customize ESET Endpoint Security behavior for specific applications.

List of known certificates allows you to customize ESET Endpoint Security behavior for specific SSL certificates.

Exclude communication with trusted domains – Domain trustiness is determined by builtin whitelist.
Block encrypted communication utilizing the obsolete protocol SSL v2 – Communication using the earlier version of the SSL protocol will automatically be blocked.

**Note**

Addresses will not be filtered if the setting *Exclude communication with trusted domains* is enabled and the domain is considered trusted.

**Root certificate**

*Root certificate* – For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). *Add the root certificate to known browsers* should be enabled. Select this option to automatically add the ESET root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

To apply the certificate to unsupported browsers, click *View Certificate > Details > Copy to File...* and manually import it into the browser.

**Certificate validity**

*If the certificate cannot be verified using the TRCA certificate store* – In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store. This means that the certificate is signed by someone (for example, the administrator of a web server or a small business) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by the TRCA. If *Ask about certificate validity* is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. You can select *Block communication that uses the certificate* to always terminate encrypted connections to sites with unverified certificates.

*If the certificate is invalid or corrupt* – This means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave *Block communication that uses the certificate* selected.

4.3.1.4.1 Encrypted SSL communication

If your system is configured to use SSL protocol scanning, a dialog window prompting you to choose an action will be displayed in two situations:

First, if a website uses an unverifiable or invalid certificate, and ESET Endpoint Security is configured to ask the user in such cases (by default yes for unverifiable certificates, no for invalid ones), a dialog box will ask you whether to Allow or Block the connection.

Second, if SSL protocol filtering mode is set to Interactive mode, a dialog box for each website will ask whether to Scan or Ignore the traffic. Some applications verify that their SSL traffic is not modified nor inspected by anyone, in such cases ESET Endpoint Security must Ignore that traffic to keep the application working.

In both cases, the user can choose to remember the selected action. Saved actions are stored in the *List of known certificates*.

4.3.1.4.2 List of known certificates

The *List of known certificates* can be used to customize ESET Endpoint Security behavior for specific SSL certificates, and to remember actions chosen if Interactive mode is selected in SSL/TLS protocol filtering mode. The list can be viewed and edited in Advanced setup (FS) > Web and email > SSL/TLS > List of known certificates.

The *List of known certificates* window consists of:

**Columns**

- **Name** – Name of the certificate.
- **Certificate issuer** – Name of the certificate creator.
Certificate subject – The subject field identifies the entity associated with the public key stored in the subject public key field.

Access – Select Allow or Block as the Access action to allow/block communication secured by this certificate regardless of its trustworthiness. Select Auto to allow trusted certificates and ask for untrusted ones. Select Ask to always ask user what to do.

Scan – Select Scan or Ignore as the Scan action to scan or ignore communication secured by this certificate. Select Auto to scan in automatic mode and ask in interactive mode. Select Ask to always ask the user what to do.

Control elements

Add – A certificate can be loaded manually as a file with the extension .cer, .crt or .pem. Click File to upload a local certificate or click URL to specify the location of a certificate online.

Edit – Select the certificate that you want to configure and click Edit.

Delete – Select the certificate that you want to delete and click Remove.

OK/Cancel – Click OK if you want to save changes or click Cancel if you want to exit without saving.

4.3.1.4.3 List of SSL/TLS filtered applications

The List of SSL/TLS filtered applications can be used to customize ESET Endpoint Security behavior for specific applications, and to remember actions chosen if Interactive mode is selected in SSL/TLS protocol filtering mode. The list can be viewed and edited in Advanced setup (F5) > Web and email > SSL/TLS > List of SSL/TLS filtered applications.

The List of SSL/TLS filtered applications window consists of:

Columns

Application – Name of the application.

Scan action – Select Scan or Ignore to scan or ignore communication. Select Auto to scan in automatic mode and ask in interactive mode. Select Ask to always ask the user what to do.

Control elements

Add – Add filtered application.

Edit – Select the certificate that you want to configure and click Edit.

Delete – Select the certificate that you want to delete and click Delete.

OK/Cancel – Click OK if you want to save changes or click Cancel if you want to exit without saving.

4.3.2 Email client protection

Integration of ESET Endpoint Security with your email client increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET Endpoint Security. When integrated into your email client, the ESET Endpoint Security toolbar is inserted directly into the email client (the toolbar for newer versions of Windows Live Mail is not inserted), for more efficient email protection. Integration settings are located under Advanced setup (F5) > Web and email > Email client protection > Email clients.

Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.
Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

Turn on **Disable checking upon inbox content change** if you experience system slowdown when working with Microsoft Outlook. This can occur when retrieving email from the Kerio Outlook Connector store.

**Email to scan**

- **Enable email protection by client plugins** – When email client protection by email client is disabled, email client protection by protocol filtering will be still enabled.
- **Received email** – Toggles checking of received messages.
- **Sent email** – Toggles checking of sent messages.
- **Read email** – Toggles checking of read messages.

**Action to be performed on infected email**

- **No action** – If enabled, the program will identify infected attachments, but will leave emails without taking any action.
- **Delete email** – The program will notify the user about infiltration(s) and delete the message.
- **Move email to the Deleted items folder** – Infected emails will be moved automatically to the Deleted items folder.
- **Move email to folder** (default action) – Infected emails will be moved automatically to the specified folder.
- **Folder** – Specify the custom folder where you want to move infected emails when detected.
- **Repeat scan after update** – Toggles rescanning after a detection engine update.
- **Accept scan results from other modules** – If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

**Note**

We recommend that you enable **Enable email protection by client plugins** and **Enable email protection by protocol filtering**. These settings are located under **Advanced setup (F5) > Web and email > Email client protection > Email protocols**.

### 4.3.2.1 Email protocols

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another Internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET Endpoint Security provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client.

The protection module providing this control is automatically initiated at system startup and is then active in memory. IMAP protocol control is performed automatically without the need to reconfigure the email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

You can configure IMAP/IMAPS and POP3/POP3S protocol checking in Advanced setup. To access this setting, expand **Web and email > Email client protection > Email protocols**.

**Enable Email protection by protocol filtering** – Enables checking of email protocols.

In Windows Vista and later, IMAP and POP3 protocols are automatically detected and scanned on all ports. In Windows XP, only the configured **Ports used by the IMAP/POP3 protocol** are scanned for all applications, and all ports are scanned for applications marked as **Web and email clients**.

ESET Endpoint Security also supports the scanning of IMAPS and POP3S protocols, which use an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL
(Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by IMAPS/POP3S protocol**, regardless of operating system version.

Encrypted communication will be scanned by default. To view the scanner setup, navigate to **SSL/TLS** in the Advanced setup section, click **Web and email > SSL/TLS**, and enable the **Enable SSL/TLS protocol filtering** option.

### 4.3.2.2 Email alerts and notifications

The options for this functionality are available in **Advanced setup** under **Web and email > Email client protection > Alerts and notifications**.

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read mail**, **Append note to the subject of received and read infected email** or **Append tag messages to sent mail**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The available options are:

- **Never** – No tag messages will be added at all.
- **To infected email only** – Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** – The program will append messages to all scanned email.

**Append note to the subject of sent infected email** – Disable this if you do not want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient and if an infiltration is detected, provides valuable information about the threat level of a given email or sender.

**Template added to the subject of infected email** – Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject "Hello" to the following format: "[virus DETECTION NAME] Hello". The variable %VIRUSNAME% represents the detection.
4.3.2.3 Antispam protection

Unsolicited email, called spam, ranks among the greatest problems of electronic communication. Spam represents up to 80 percent of all email communication. Antispam protection serves to protect against this problem. Combining several email security principles, the Antispam module provides superior filtering to keep your inbox clean.

One important principle for spam detection is the ability to recognize unsolicited email based on predefined trusted addresses (whitelist) and spam addresses (blacklist). All addresses from your contact list are automatically added to the whitelist, as well as all other addresses you mark as safe.

The primary method used to detect spam is the scanning of email message properties. Received messages are scanned for basic Antispam criteria (message definitions, statistical heuristics, recognizing algorithms and other unique methods) and the resulting index value determines whether a message is spam or not.

**Start email client antispam protection automatically** – When enabled, antispam protection will be activated automatically on system startup.

**Allow advanced antispam scan** – Additional antispam data will be downloaded periodically, increasing antispam capabilities and producing better results.

Antispam protection in ESET Endpoint Security allows you to set different parameters to work with mailing lists. Options are as follows:

**Message processing**

**Add text to email subject** – Enables you to add a custom prefix string to the subject line of messages that have been classified as spam. The default is "[SPAM]".

**Move messages to spam folder** – When enabled, spam messages will be moved to the default junk email folder and also messages reclassified as not spam will be moved to inbox. When you right-click an email message and select ESET Endpoint Security from the context menu, you can choose from applicable options.

**Use the folder** – This option moves spam to a user-defined folder.

**Mark spam messages as read** – Enable this to automatically mark spam as read. It will help you to focus your attention on "clean" messages.
Mark reclassified messages as unread – Messages originally classified as spam, but later marked as “clean” will be displayed as unread.

Spam score logging – The ESET Endpoint Security Antispam engine assigns a spam score to every scanned message. The message will be recorded in the antispam log (ESET Endpoint Security > Tools > Log files > Antispam protection).

- None – The score from antispam scanning will not be logged.
- Reclassified and marked as spam – Select this if you want to record a spam score for messages marked as SPAM.
- All – All messages will be recorded to the log with a spam score.

Note
When you click a message in junk email folder, you can choose Reclassify selected messages as NOT spam and the message will be moved to inbox. When you click a message you consider spam in inbox, select Reclassify messages as spam and the message will be moved to junk email folder. You can select multiple messages and perform the action on all of them at the same time.

Note
ESET Endpoint Security supports Antispam protection for Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail.

4.3.2.3.1 Antispam address books
The Antispam feature in ESET Endpoint Security allows you to configure various parameters for address lists.

Address books
Allow user address list – Enable this option to activate the address book created by a user within their own email client.

Allow global address lists – Enable this option to activate the global address book shared by all users, the directory service within the email system. The GAL (Global Address List) contains information for all email users, distribution groups and resources.

User’s Whitelist – List of contacts where you can add, edit or delete addresses that are considered safe and from whom the user wants to receive messages.

User’s Blacklist – List of contacts where you can add, edit or delete addresses that are considered unsafe and from whom the user does not want to receive messages.

User’s Exception list – This list of contacts contains email addresses that may be spoofed and used for sending spam. See also Exception list.

Global Whitelist/Blacklist/Exception list – These lists are used for applying global antispam policies to all workstations in the network.

Add to user’s Whitelist automatically
Add addresses from address book – Add addresses from your contact list to the Whitelist.

Add recipient addresses from outgoing messages – Add recipient addresses from sent messages to the Whitelist.

Add addresses from messages reclassified as NOT spam – Add sender addresses from messages reclassified as NOT spam to the Whitelist.

Add to user’s Exception list automatically
Add addresses from own accounts – Add your addresses from existing email client accounts to the Exception list.
4.3.2.3.2 Blacklist/Whitelist/Exceptions list

To provide protection against unsolicited emails, ESET Endpoint Security allows you to classify email addresses using specialized lists. The Whitelist contains email addresses you consider to be safe. Messages from users on the Whitelist are always available in the incoming mail folder. The Blacklist contains email addresses classified as spam, and all messages from senders on the Blacklist are marked accordingly. The exception list contains email addresses that are always checked for spam but may also contain addresses from unsolicited email messages that might not be recognized as spam initially.

All lists can be edited from main program window of ESET Endpoint Security in Advanced Setup > Web and email > Email client protection > Antispam address books using the Add, Edit and Delete buttons in each list's dialog window, or from Setup > Web and email after you click the gear wheel next to Antispam protection.

![User’s Whitelist dialog](image)

By default, ESET Endpoint Security adds all addresses from the address book of supported email clients to the Whitelist. The Blacklist is empty by default. The Exception list only contains user’s own email addresses by default.

4.3.2.3.2.1 Add/Edit Blacklist/Whitelist/Exceptions address

This window allows you to add or edit entries in the Whitelist or Blacklist.

Email address – The email address to add/edit.

Name – The name of the entry.

Whole domain – Select this option for the entry to be applied to the whole domain of the contact (not only to the address specified in the Email address field, but all email addresses at the address.info domain).

Lower level domains – Select this option for the entry to be applied to the lower level domains of the contact (The address.info represents domain, while my.address.info represents a subdomain).
4.3.3 Web access protection

Internet connectivity is a standard feature on most personal computers. Unfortunately, it has also become the main medium for transferring malicious code. Web access protection works by monitoring communication between web browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules.

Access to web pages known to contain malicious content is blocked before content is downloaded. All other webpages are scanned by the ThreatSense scanning engine when they are loaded and blocked if malicious content is detected. Web access protection offers two level of protection, blocking by blacklist and blocking by content.

We strongly recommend that you leave Web access protection enabled. This option can be accessed from the main program window of ESET Endpoint Security by navigating to Setup > Web and email > Web access protection.

The following options are available in Advanced setup (F5) > Web and email > Web access protection:

- **Web protocols** – enables you to configure monitoring for these standard protocols which are used by most Internet browsers.

- **URL address management** – enables you to specify HTTP addresses to block, allow or exclude from checking.

- **ThreatSense parameters** – Advanced virus scanner setup – enables you to configure settings such as types of objects to scan (emails, archives, etc.), detection methods for Web access protection etc.

4.3.3.1 Basic

Enable Web access protection – When disabled, Web access protection and Anti-Phishing protection will not run.

Enable advanced scanning of browser scripts – When enabled, all JavaScript programs executed by internet browsers will be checked by antivirus scanner.

Note

We strongly recommend you leave Web access protection enabled.
4.3.3.2  Web protocols
By default, ESET Endpoint Security is configured to monitor the HTTP protocol used by most Internet browsers.

HTTP Scanner setup
In Windows Vista and later, HTTP traffic is always monitored on all ports for all applications. In Windows XP, you can modify the Ports used by HTTP protocol in Advanced setup (F5) > Web and email > Web access protection > Web protocols > HTTP scanner setup. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

HTTPS Scanner setup
ESET Endpoint Security also supports HTTPS protocol checking. HTTPS communication uses an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in Ports used by HTTPS protocol, regardless of operating system version.

Encrypted communication will be scanned by default. To view the scanner setup, navigate to SSL/TLS in the Advanced setup section, click Web and email > SSL/TLS, and enable the Enable SSL/TLS protocol filtering option.

4.3.3.3  URL address management
The URL address management section allows you to specify HTTP addresses to block, allow or exclude from checking.

Websites in the List of blocked addresses will not be accessible unless they are also included in the List of allowed addresses. Websites in the List of addresses excluded from checking are not scanned for malicious code when accessed.

Enable SSL protocol filtering must be selected if you want to filter HTTPS addresses in addition to HTTP web pages. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk represents any number or character, while the question mark represents any one character. Particular care should be taken when specifying excluded addresses because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. See Add HTTP address / domain mask for how a whole domain including all subdomains can be matched safely. To activate a list, enable the List active option. If you want to be notified when entering an address from the current list, enable Notify when applying.

If you want to block all HTTP addresses except addresses present in the active List of allowed addresses, add * to the active List of blocked addresses.

Note
Addresses will not be filtered if the setting Exclude communication with trusted domains is enabled and the domain is considered trusted.
Add – Creates a new list in addition to the predefined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from some external public blacklist, and a second one may contain your own blacklist, which makes it easier to update the external list while keeping yours intact.

Edit – Modifies existing lists. Use this to add or remove addresses from the lists.

Delete – Deletes existing list. Only possible for lists created with Add, not for the default ones.

4.3.3.3.1 URL addresses list

In this section you can specify lists of HTTP addresses that will be blocked, allowed or excluded from checking.

By default, the following three lists are available:

- List of addresses excluded from content scan – No checking for malicious code will be performed for any address added to this list.
- List of allowed addresses – If allow access only to HTTP addresses in the list of allowed addresses is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they are included in the list of blocked addresses.
- List of blocked addresses – The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.

Click Add to create a new list. To delete selected lists, click Delete.
4.3.3.3.2 Create new URL address list

This section allows you to specify lists of URL addresses/masks that will be blocked, allowed or excluded from checking.

When creating a new list, the following options are available to configure:

- **Address list type** – Three predefined list types are available:
  - **Excluded from checking** – No checking for malicious code will be performed for any address added to this list.
  - **Blocked** – The user will not be allowed to access addresses specified in this list.
  - **Allowed** – If your policy is configured to use this feature and the wildcard (*) value is added to this list, you will be allowed to access addresses in this list even if those addresses are also present in the blocked list.

- **List name** – Specify the name of the list. This field will be unavailable if you are editing one of the three predefined lists.

- **List description** – Type a short description for the list (optional). This field will be unavailable if you are editing one of the three predefined lists.

- **List active** – Select the slider bar to activate the list.

- **Notify when applying** – Select the slider bar if you want to be notified when this list is used to evaluate an HTTP site that you visited. For example, a notification will be issued when a website is either blocked or allowed because the website is included in the list of blocked or allowed addresses. The notification will display the list name for the list that specifies the website.

- **Logging severity** – Select the Logging severity from the drop-down menu. Records with Warning verbosity can be collected by Remote Administrator.

**Control elements**

- **Add** – Add a new URL address to the list (enter multiple values with separator).

- **Edit** – Modifies existing address in the list. Only possible for addresses created with **Add**.

- **Delete** – Deletes existing addresses in the list. Only possible for addresses created with **Add**.

- **Import** – Import a file with URL addresses (separate values with a line break, for example *.txt using encoding UTF-8).
4.3.3.3 How to add URL mask

Please refer to the instructions in this dialog before you enter the desired address/domain mask.

ESET Endpoint Security enables user to block access to specified websites and prevent the Internet browser from displaying their content. Furthermore, it allows user to specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wishes to specify a whole group of remote servers, so called masks can be used to identify such a group. The masks include the symbols “?” and “*”:

- use ? to substitute a symbol
- use * to substitute a text string.

For example * .c?m applies to all addresses, where the last part begins with the letter c, ends with the letter m and contains an unknown symbol in between them (.com, .cam, etc.).

A leading "* ." sequence is treated specially if used at the beginning of domain name. First, the * wildcard does not match the slash character ('/') in this case. This is to avoid circumventing the mask, for example the mask * .domain.com will not match http://anydomain.com/anypath#.domain.com (such suffix can be appended to any URL without affecting the download). And second, the "* ." also matches an empty string in this special case. This is to allow matching whole domain including any subdomains using a single mask. For example the mask * .domain.com also matches http://domain.com. Using *domain.com would be incorrect, as that would also match http://anotherdomain.com.

4.3.4 Anti-Phishing protection

The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET Endpoint Security includes anti-phishing protection, which blocks web pages known to distribute this type of content.

We strongly recommend that you enable Anti-Phishing in ESET Endpoint Security. To do so, open Advanced setup (F5) and navigate to Web and email > Anti-Phishing protection.

Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET Endpoint Security.

Accessing a phishing website

When you access a recognized phishing website, the following dialog will be displayed in your web browser. If you still want to access the website, click Proceed to the site (not recommended).
Note
Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool. From Advanced setup (F5) expand Web and email > Web access protection > URL address management > Address list, click Edit and then add the website that you want to edit to the list.

Phishing site reporting
The Report link enables you to report a phishing/malicious website to ESET for analysis.

Note
Before submitting a website to ESET, make sure it meets one or more of the following criteria:
- the website is not detected at all,
- the website is incorrectly detected as a threat. In this case, you can Report a false-positive phishing site.

Alternatively, you can submit the website by email. Send your email to samples@eset.com. Remember to use a descriptive subject and enclose as much information about the website as possible (for example, the website that referred you there, how you learned of this website, etc.).
4.4 Web control

The Web control section allows you to configure settings that protect your company from risk of legal liability. Web control can regulate access to websites that violate intellectual property rights. The goal is to prevent employees from accessing pages with inappropriate or harmful content, or pages that may have a negative impact on productivity.

Web control lets you block webpages that may contain potentially offensive material. In addition, employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories.

By default, Web control is disabled. To activate Web control:

1. Press F5 to enter Advanced setup and expand Web and email > Web control.
2. Select Integrate into system to activate Web control in ESET Endpoint Security.
3. To configure access to specific webpages, click Edit next to Rules to access the Web control rules editor window.

Blocked webpage message and Block webpage graphic fields allow you to easily customize the displayed message when a website is blocked.

This is the default message and design of in-browser notification when a user tries to access a blocked website:
An example of a blocked webpage message would be *The webpage was blocked because it is considered inappropriate or with harmful content. Please contact your administrator for details* and you can enter a web address or network path with custom image for example http://test.com/test.jpg. The custom image size is set automatically to 90 x 30; images will automatically be scaled to this size if they are not already.

In case you want to block all webpages and leave only certain available, use [URL address management](#).

### 4.4.1 Rules

The **Rules** editor window displays existing URL-based or Category-based rules.

The list of rules contains several descriptions of rules such as name, type of blocking, action to perform after matching a Web control rule and log severity.

Click **Add** or **Edit** to manage a rule. Click **Copy** to create a new rule with predefined options used for another selected rule. By pressing **Ctrl** and clicking, you can select multiple rules and delete all selected rules. The **Enabled** check box disables or enables a rule; this can be useful if you don't want to delete a rule permanently because it
might be used in the future.

Rules are sorted in the order determining their priority, with higher priority rules on top. Evaluation of rules based on URL always has higher priority than evaluation based on category. For example, if a rule based on a URL is under a rule based on category in the list of rules, the URL-based rule has higher priority and will be evaluated first.

For more information on creating rules click here.

4.4.1.1 Adding Web control rules

The Web control rules window allows you to manually create or modify an existing Web control filtering rule.

Name

Enter a description of the rule into the Name field for better identification.

Enabled

Click the Enabled switch to disable or enable the rule; this can be useful if you do not want to delete the rule permanently.

Action

Choose between URL-based Action or Category-based Action:

- **URL-based Action**

  For rules that control access to a given website, enter the URL in the URL field.

  The special symbols * (asterisk) and ? (question mark) cannot be used in the URL address list. When creating a URL group that contains a website with multiple top-level-domains (TLDs), each TLD must be added separately. If you add a domain to the group, all content located on this domain and all subdomains (for example, sub.examplepage.com) will be blocked or allowed based on your choice of URL-based action.

  **URL or Use URL Group** – Uses the URL link or URL group of links to allow, block or warn the user when one of these URLs are detected.

- **Category-based Action**

  When this is selected, set the website category for your action using the drop-down menu.

  **URL Category** or **Use Group** – Uses the website category or Category groups of categories to allow, block or warn the user when one of these groups are detected.
Access rights
- **Allow** – Access to the URL address/category will be granted.
- **Warn** – Warns the user about the URL address/category.
- **Block** – Blocks the URL address/category.

Apply during
Allows you to apply created rule during the certain time. From the drop-down menu, select created time slot.
- [More information about Time slots](#)

Logging severity
- **Always** – Logs all online communications.
- **Diagnostic** – Logs information needed to fine-tune the program.
- **Information** – Records informative messages, including successful update messages, plus all records above.
- **Warning** – Records critical errors and warning messages.
- **None** – No logs will be created.

**Note**
The Logging severity can be configured separately for each list. Logs with **Warning** status can be collected by ESET Security Management Center.

User list
- **Add** – Opens the **Select Users or Groups** dialog window, which allows you to select desired users. When no user is entered the rule is applied for all users.
- **Delete** – Removes the selected user from the filter.
4.4.2 Category groups

The Category groups window is divided into two parts. The right part of the window contains a list of categories and subcategories. Select a category in the Category list to display its subcategories.

Each group contains adult and/or generally inappropriate subcategories as well as categories considered generally acceptable. When you open the Category groups window and click on first group, you can add or remove categories/subcategories from the list of appropriate groups (for example Violence or Weapons). Web pages with inappropriate content can be blocked, or users can be informed after a rule with predefined actions is created.

Select the check box to add or remove a subcategory to a particular group.

Here are some examples of categories that users might not be familiar with:

**Miscellaneous** – Usually private (local) IP addresses such as intranet, 192.168.0.0/16, etc. When you get a 403 or 404 error code, the website will also match this category.

**Not resolved** – This category includes web pages that are not resolved because of an error when connecting to the Web control database engine.

**Not categorized** – Unknown web pages that are not yet in the Web control database.

**Proxies** – Web pages such as anonymizers, redirectors or public proxy servers can be used to obtain (anonymous) access to web pages that are usually prohibited by the Web control filter.

**File sharing** – These web pages contain large amounts of data such as photos, videos or e-books. There is a risk that these sites contain potentially offensive material or adult content.

**Note**

A subcategory can belong to any group. There are some subcategories that are not included in predefined groups (for example, Games). In order to match a desired subcategory using Web control filter, add it to your desired group.
4.4.3 URL groups

URL groups allow you to create a group that contains several URL links for which you want to create a rule (allow/disallow a particular website).

To create a new URL group click Add. Select a URL group and click Add in the bottom right of the window to add a new URL address to the list, or click Import to import a file with a list of URL addresses (separate values with a line break, for example *.txt using encoding UTF-8). If you want to set an action to be performed for a specific URL group, open the Web control rules editor, select your URL group using the drop-down menu, adjust other parameters and then click OK.

Note

Blocking or allowing a specific web page can be more accurate than blocking or allowing a whole category of web pages. Be careful when changing these settings and adding a category/web page to the list.

4.5 Updating the program

Regularly updating ESET Endpoint Security is the best method to obtain the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways, by updating the detection engine and by updating system components. Updates are automatic by default when the program is activated.

By clicking Update in the main program window, you can find the current update status including the date and time of the last successful update and if an update is needed. You can also click the Show all modules link to open the list of installed modules and check the version and the last update of a module.

In addition, the option to manually begin the update process, Check for updates is available. Updating the detection engine and updating program components are important parts of maintaining complete protection against malicious code. Please pay attention to their configuration and operation. If you did not enter your License details during installation, you can enter your license key by clicking Activate product when updating to access ESET’s update servers.

If you activate ESET Endpoint Security with Offline license file without Username and Password and try to update, the red information Modules update failed signals you can download updates from the mirror only.

Note

Your license key is provided by ESET after purchasing ESET Endpoint Security.
**Current version** – The ESET Endpoint Security build number.

**Last successful update** – The date and time of the last successful update. Make sure it refers to a recent date, which means that the detection engine is current.

**Last successful check for updates** – The date and time of the last successful attempt to update modules.

**Show all modules** – Click the link to open the list of installed modules and check the version and the last update of a module.
Update process

After clicking **Check for updates**, the download process begins. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Cancel update**.

---

**Important**

Under normal circumstances the modules updates several times a day. If this is not the case, the program is out of date and more vulnerable to infection. Please update the modules as soon as possible.

**Detection engine out of date** – This error will appear after several unsuccessful attempts to update modules. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured [connection settings](#).
The previous notification is related to the following two **Modules update failed** messages about unsuccessful updates:

1. **Invalid license** – The license key has been incorrectly entered in update setup. We recommend that you check your authentication data. The Advanced setup window (click **Setup** from the main menu and then click **Advanced setup**, or press F5 on your keyboard) contains additional update options. Click **Help and support > Change license** from the main menu to enter a new license key.
2. **An error occurred while downloading update files** – A possible cause of the error is incorrect [Internet connection settings](#). We recommend that you check your Internet connectivity (by opening any website in your web browser). If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.

![ESET ENDPOINT SECURITY](image)

**Note**

For more information please visit this [ESET Knowledgebase article](#).

### 4.5.1 Update setup

Update setup options are available in the **Advanced setup** tree (FS) under **Update**. This section specifies update source information like the update servers being used and authentication data for these servers.

**Adjust update settings correctly**

For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the Internet (for example, HTTPS communication).

**Basic**

The update profile that is currently in use is displayed in the **Select default update profile** drop-down menu.

To create a new profile, see the **Update profiles** section.

If you are experiencing difficulty when attempting to download modules updates, click **Clear** next to **Clear update cache** to clear the temporary update files/cache.
Outdated detection engine alerts

Set maximum detection engine age automatically – Allows to set maximum time (in days) after which the detection engine will be reported as out of date. Default value of Maximum detection engine age (days) is 7.

Module Rollback

If you suspect that a new update of the detection engine and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time.

Profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users who need an alternative profile for Internet connection properties that regularly change.

The Select profile to edit drop-down menu displays the currently selected profile and is set to My profile by default.

To create a new profile, click Edit next to List of profiles, enter your own Profile name and then click Add.

Updates

By default, the Update type is set to Regular update to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the Pre-release update option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required. Delayed update allows updating from special update servers providing new versions of virus databases with a delay of at least X hours (i.e. databases tested in a real environment and therefore considered as stable).

Select received update notifications – Click Edit to select what application notifications are displayed. You can choose if the notifications Show on a desktop and/or are Send by email.
Ask before downloading update – The program will display a notification where you can choose to confirm or decline update file downloads. If the update file size is greater than the value specified in the Ask if an update file is greater than (kB) field, the program will display a notification.

Modules updates

The Choose automatically option is enabled by default. The Custom server option is the location where updates are stored. If you use an ESET update server, we recommend that you leave the default option selected.

Enable more frequent updates of detection signatures – Detection signatures will be updated in shorter interval. Disabling this setting may negatively impact detection rate.

Update from removable media – Allows you to update from removable media if contains created mirror. When Automatic selected, update will run on background. If you want to show update dialogs select Always ask.

When using a local HTTP server – also known as a Mirror – the update server should be set as follows:
http://computer_name_or_its_IP_address:2221

When using a local HTTP server with SSL – the update server should be set as follows:
https://computer_name_or_its_IP_address:2221

When using a local shared folder – the update server should be set as follows:
\\computer_name_or_its_IP_address\shared_folder

HTTP server port number

HTTP server port number specified in the examples above depends on what port your HTTP/HTTPS server listens.

Program component update

See Program component update.

Update mirror

See Update mirror.
**4.5.1.1 Update rollback**

If you suspect that a new update of the detection engine and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET Endpoint Security records snapshots of detection engine and program modules for use with the *rollback* feature. In order to create virus database snapshots, leave the **Create snapshots of modules** switch enabled. The **Number of locally stored snapshots** field defines the number of previous detection engine snapshots stored.

If you click **Rollback** (*Advanced setup* (F5) > **Update** > **Basic** > **Module rollback**), you have to select a time interval from the drop-down menu that represents the period of time that the detection engine and program module updates will be paused.

Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. Because it represents a potential security risk, we do not recommend selecting this option.

The detection engine version is downgraded to the oldest available and stored as a snapshot in the local computer file system.

---

**Note**

Let the number 10646 be the most recent version of detection engine. 10645 and 10643 are stored as a detection engine snapshots. Note that 10644 is not available because, for example, the computer was turned off and a more recent update was made available before 10644 was downloaded. If the **Number of locally stored snapshots** field is set to 2 and you click **Rollback**, the detection engine (including program modules) will be restored to version number 10643. This process may take some time. Check whether the detection engine version has downgraded from the main program window of ESET Endpoint Security in the **Update** section.

---

**4.5.1.2 Program component update**

The **Program component update** section contains options related to the program component update. The program enables you to predefine its behavior when a new program component upgrade is available.

Program component updates brings new features or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required.

In the **Update mode** drop-down menu, three options are available:

- **Ask before update** – The default option. You will be prompted to confirm or refuse program component updates when they are available.
- **Auto-update** – A program component update will be downloaded and installed automatically. Please remember that a computer restart may be required.
- **Never update** – Program component updates will not be performed at all. This option is suitable for server installations, since servers can usually be restarted only when they are undergoing maintenance.
By default, program component updates are downloaded from ESET repository servers. In large or offline environments, the traffic can be distributed to allow internal caching of the program component files.

Define custom server for program component updates

1. Define the path to the program component update in the **Custom server** field. It can be an HTTP(S) link, SMB network share path, a local disk drive or a removable media path. For network drives, use the UNC path instead of a mapped drive letter.

2. Leave **Username** and **Password** blank if not required.
   If required, define the appropriate credentials here for HTTP authentication on the custom web server.

3. Confirm the changes and test the presence of a program component update using a standard ESET Endpoint Security update.

**Note**

Selecting the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers – for example, restarting the server automatically after a program update could cause serious damage.

4.5.1.3  **Connection options**

To access the proxy server setup options for a given update profile, click **Update** in the **Advanced setup** tree (F5) and then click **Profiles > Updates > Connection options**.

**Proxy server**

Click the **Proxy mode** drop-down menu and select one of the three following options:

- Do not use proxy server
- Connection through a proxy server
- Use global proxy server settings

Select **Use global proxy server settings** to use the proxy server configuration options already specified in the **Tools > Proxy server** branch of the Advanced setup tree.

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET Endpoint Security.

**Connection through a proxy server** option should be selected if:

- A different proxy server than the one defined in **Tools > Proxy server** is used to update ESET Endpoint Security. In this configuration, information for the new proxy should be specified under **Proxy server** address, communication **Port** (3128 by default), and **Username** and **Password** for the proxy server if required.
- Proxy server settings are not set globally, but ESET Endpoint Security will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. Settings are taken from Internet Explorer during program installation, but if they are changed (for example, if you change your ISP), please make sure the proxy settings listed in this window are correct. Otherwise the program will not be able to connect to update servers.

The default setting for the proxy server is **Use global proxy server settings**.

**Use direct connection if proxy is not available** – Proxy will be bypassed during update if it is unreachable.

**Windows shares**

When updating from a local server with a version of the Windows NT operating system, authentication for each network connection is required by default.

To configure such an account, select from the **Connect to LAN as** drop-down menu:
System account (default),
Current user,
Specified user.

Select System account (default) to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select Current user. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select Specified user if you want the program to use a specific user account for authentication. Use this method when the default system account connection fails. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

Username and Password settings are optional.

**Warning**

When either Current user or Specified user is selected, an error may occur when changing the identity of the program to the desired user. We recommend entering the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: domain_name\user (if it is a workgroup, enter workgroup_name\name) and password. When updating from the HTTP version of the local server, no authentication is required.

Select Disconnect from server after update to force a disconnection if a connection to the server remains active even after updates have been downloaded.
4.5.1.4 Update mirror

ESET Endpoint Security allows you to create copies of update files that can be used to update other workstations on the network. The use of a "mirror" – a copy of the update files in the LAN environment is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each workstation. Updates are downloaded to the local mirror server and then distributed to all workstations to avoid the risk of network traffic overload. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are located in Advanced setup under Update. To access this section press F5 to access Advanced setup, click Update > Profiles and select the Update mirror tab.

To create a mirror on a client workstation, enable Create update mirror. Enabling this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

Access to update files

Enable HTTP server – If enabled, update files can be accessed through HTTP, no credentials are required.

Methods to access the Mirror server are described in detail in Updating from the Mirror. There are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder, or clients can access the mirror located on an HTTP server.

The folder dedicated to storing update files for the Mirror is defined under Folder to store mirrored files. To choose a different folder click Clear to delete predefined folder C:\ProgramData\ESET\ESET Endpoint Security\mirror and click Edit to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be entered in the Username and Password fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder. The username and password should be entered in the format Domain/User or Workgroup/User. Please remember to supply the corresponding passwords.
Program component update

Files – When configuring the Mirror you can specify the language versions of updates you want to download. Languages selected must be supported by the mirror server configured by the user.

Update components automatically – Allows for the installation of new features and updates to existing features. An update can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required.

Update components now – Updates your program components to the latest version.

4.5.1.4.1 HTTP Server

Server port – By default, the Server port is set to 2221.

Authentication – Defines the method of authentication used for accessing update files. The following options are available: None, Basic and NTLM. Select Basic to use base64 encoding with basic username and password authentication. The NTLM option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is None, which grants access to the update files with no need for authentication.

Append your Certificate chain file, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: ASN, PEM and PFX. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. The Private key type option is set to Integrated by default (and therefore the Private key file option is disabled by default). This means that the private key is a part of the selected certificate chain file.

Note

Authentication data such as Username and Password is intended for accessing the proxy server. Complete these fields only if a username and password are required. Please note that these fields are not for your Username/Password for ESET Endpoint Security, and should only be completed if you know you need a password to access the internet via a proxy server.
4.5.1.4.2 Updating from the Mirror

There are two basic methods to configure a Mirror, which is essentially a repository where clients can download update files. The folder with update files can be presented as a shared network folder or as an HTTP server.

Accessing the Mirror using an internal HTTP server

This is the default configuration specified in the predefined program configuration. To allow access to the Mirror using the HTTP server, navigate to Advanced setup > Update > Profiles > Mirror and select Create update mirror.

In the HTTP Server section of the Mirror tab you can specify the Server port where the HTTP server will listen as well as the type of Authentication used by the HTTP server. By default, the Server port is set to 2221. The Authentication option defines the method of authentication used for accessing the update files. The following options are available: None, Basic, and NTLM. Select Basic to use base64 encoding with basic username and password authentication. The NTLM option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is None, which grants access to the update files with no need for authentication.

Warning

If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Endpoint Security instance creating it.

SSL for HTTP Server

Append your Certificate chain file, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: PEM, PFX and ASN. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. Private key type is set to Integrated by default, which means that the private key is a part of the selected certificate chain file.

Note

An error Invalid Username and/or Password will appear in the Update pane from the main menu after several unsuccessful attempts to update the detection engine from the Mirror. We recommend that you navigate to Advanced setup > Update > Profiles > Mirror and check the Username and Password. The most common reason for this error is incorrectly entered authentication data.
After your Mirror server is configured, you must add the new update server on client workstations. To do this, follow the steps below:

- Access **Advanced setup** (F5) and click **Update > Profiles > Basic**.
- Disengage **Choose automatically** and add a new server to the **Update server** field using one of the following formats:
  - http://IP_address_of_your_server:2221
  - https://IP_address_of_your_server:2221 (if SSL is used)

**Accessing the Mirror via system shares**

First, a shared folder should be created on a local or network device. When creating the folder for the Mirror, you must provide “write” access for the user who will save update files to the folder and “read” access for all users who will update ESET Endpoint Security from the Mirror folder.

Next, configure access to the Mirror in **Advanced setup > Update > Profiles > Mirror** tab by disabling **Provide update files via internal HTTP server**. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must enter authentication data to access the other computer. To enter authentication data, open ESET Endpoint Security **Advanced setup** (F5) and click **Update > Profiles > Connect to LAN as**. This is the same setting used for updating, as described in the **Connect to LAN as** section.

To access the mirror folder, this needs to be done under the same account as the one used for logging into the computer the mirror is created on. In case the computer is in a domain, "domain\user" username should be used. In case the computer is not in a domain, "IP_address_of_your_server\user" or "hostname\user" should be used.

After the Mirror configuration is complete, on client workstations set `\\UNC\PATH` as the update server using the steps below:

1. Open ESET Endpoint Security **Advanced setup** and click **Update > Profiles > Updates**.
2. Disengage **Choose automatically** next to **Module updates** and a new server to the **Update server** field using the `\\UNC\PATH` format.
The last section controls program components (PCUs). By default, downloaded program components are prepared to copy to the local mirror. If **Program component update** is activated, there is no need to click **Update**, because files are copied to the local mirror automatically when they are available. See **Update mode** for more information about program component updates.

### 4.5.1.4.3 Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

**ESET Endpoint Security reports an error connecting to Mirror server** – Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, enter the folder name and click **OK**. The contents of the folder should be displayed.

**ESET Endpoint Security requires a username and password** – Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, **Domain/Username**, or **Workgroup/Username**, plus the corresponding Passwords. If the Mirror server is accessible to “Everyone”, please be aware that this does not mean that any user is granted access. “Everyone” does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to “Everyone”, a domain username and password will still need to be entered in the update setup section.

**ESET Endpoint Security reports an error connecting to the Mirror server** – Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

**ESET Endpoint Security reports an error while downloading update files** – Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates.

### 4.5.2 How to create update tasks

Updates can be triggered manually by clicking **Check for updates** in the primary window displayed after clicking **Update** from the main menu.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools > Scheduler**. By default, the following tasks are activated in ESET Endpoint Security:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see **Scheduler**.

4.6 Tools

The Tools menu includes modules that help simplify program administration and offers additional options for advanced users.

This menu includes the following tools:

- **Log files**
- **Running processes** (if ESET LiveGrid® is enabled in ESET Endpoint Security)
- **Protection statistics**
- **Watch activity**
- **Scheduler**
- **Network connections** (if Firewall is enabled in ESET Endpoint Security)
- **ESET SysInspector**
- **ESET SysRescue Live** – Redirects you to the ESET SysRescue Live website, where you can download the ESET SysRescue Live .iso CD/DVD image.
- **Quarantine**
- **Submit sample for analysis** – Allows you to submit a suspicious file for analysis to the ESET Research Lab. The dialog window displayed after clicking this option is described in this section.
4.6.1 Log files

Log files contain information about all important program events that have occurred and provide an overview of detected threats. Logs are an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view text messages and logs directly from the ESET Endpoint Security environment. It is also possible to archive log files.

Log files are accessible from the main program window by clicking **Tools > Log files**. Select the desired log type from the Log drop-down menu. The following logs are available:

- **Detections** – This log offers detailed information about detections and infiltrations detected by ESET Endpoint Security modules. The information includes the time of detection, name of detection, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window. Not-cleaned infiltrations are always marked with red text on light red background, cleaned infiltrations are marked with yellow text on white background. Not-cleaned PUAs or Potentially unsafe applications are marked with yellow text on white background.

- **Events** – All important actions performed by ESET Endpoint Security are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed to help system administrators and users resolve problems. Often the information found here can help you find a solution for a problem occurring in the program.

- **Computer scan** – All scan results are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.

- **Blocked files** – Contains records of files that were blocked and could not be accessible. The protocol shows the reason and the source module that blocked the file, as well as the application and user that executed the file.

- **Sent files** – Contains records of files that were sent to ESET LiveGrid® or ESET Dynamic Threat Defense for analysis.

- **Audit logs** – Each log contains information about the date and time when the change was performed, type of change, description, source and user. See **Audit logs** for more details.

- **HIPS** – Contains records of specific rules that are marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the name of the rule created.

- **Network protection** – The firewall log displays all remote attacks detected by Network attack protection or Firewall. Here you will find information about any attacks on your computer. The Event column lists the detected attacks. The Source column informs you more about the attacker. The Protocol column reveals the communication protocol used for the attack. Analysis of the network protection log may help you to detect system infiltration attempts in time to prevent unauthorized access to your system. For more details on particular network attacks, see **IDS and advanced options**.

- **Filtered websites** – This list is useful if you want to view a list of websites that were blocked by Web access protection or Web control. In these logs you can see the time, URL, user and application that opened a connection to the particular website.

- **Antispam protection** – Contains records related to email messages that were marked as spam.

- **Web control** – Shows blocked or allowed URL addresses and details about how they are categorized. The Action performed column tells you how filtering rules were applied.

- **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).

Select the contents of any log and press **Ctrl + C** to copy it to the clipboard. Hold **Ctrl + Shift** to select multiple entries.

Click **Filtering** to open the **Log filtering window** where you can define the filtering criteria.
Right-click a specific record to open the context menu. The following options are available in the context menu:

- **Show** – Shows more detailed information about the selected log in a new window.
- **Filter same records** – After activating this filter, you will only see records of the same type (diagnostics, warnings, ...).
- **Filter.../Find...** – After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** – Activates filter settings.
- **Disable filter** – Clears all filter settings (as described above).
- **Copy/Copy all** – Copies information about all the records in the window.
- **Delete/Delete all** – Deletes the selected record(s) or all the records displayed – this action requires administrator privileges.
- **Export...** – Exports information about the record(s) in XML format.
- **Export all...** – Export information about all records in XML format.
- **Find/Find next/Find previous** – After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.

### 4.6.1.1 Log filtering

Click **Filtering** in **Tools > Log files** to define filtering criteria.

The log filtering feature will help you find the information you are looking for, especially when there are many records. It lets you narrow down log records, for example, if you are looking for a specific type of event, status or time period. You can filter log records by specifying certain search options, only records that are relevant (according to those search options) will be displayed in the Log files window.

Type the keyword you are searching for into the **Find text** field. Use the **Search in columns** drop-down menu to refine your search. Choose one or more record from the **Record log types** drop-down menu. Define the **Time period** from which you want the results to be displayed. You can also use further search options, such as **Match whole words only** or **Case sensitive**.

**Find text**

Type a string (word, or part of a word). Only records that contain this string will be shown. Other records will be omitted.

**Search in columns**

Select what columns will be taken into account when searching. You can check one or more columns to be used for searching.

**Record types**

Choose one or more log record types from the drop-down menu:

- **Diagnostic** - Logs information needed to fine-tune the program and all records above.
- **Informative** - Records informative messages, including successful update messages, plus all records above.
- **Warnings** - Records critical errors and warning messages.
- **Errors** - Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** - Logs only critical errors (error starting antivirus protection).

**Time period**

Define the time period from which you want the results to be displayed:

- **Not specified** (default) - Does not search within time period, searches the whole log.
- **Last day**
- **Last week**
- **Last month**
- **Time period** - You can specify the exact time period (From: and To:) to filter only the records of the specified time period.
4.6.1.2 Logging configuration

The Logging configuration of ESET Endpoint Security is accessible from the main program window. Click Setup > Advanced Setup > Tools > Log files. The logs section is used to define how the logs will be managed. The program automatically deletes older logs in order to save hard disk space. You can specify the following options for log files:

**Minimum logging verbosity** – Specifies the minimum verbosity level of events to be logged:

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting antivirus protection, built-in firewall, etc...).

**Note**

All blocked connections will be recorded when you select the Diagnostic verbosity level.

Log entries older than the specified number of days in the Automatically delete records older than (days) field will automatically be deleted.

**Optimize log files automatically** – When engaged, log files will automatically be defragmented if fragmentation percentage is higher than value specified in the If the number of unused records exceeds (%) field.

Click Optimize to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed particularly when the logs contain a large number of entries.

**Enable text protocol** enables the storage of logs in another file format separate from Log files:

- **Target directory** – Select the directory where log files will be stored (only applies to Text/CSV). You can copy the path or select another directory by clicking Clear. Each log section has its own file with a predefined file name (for example, virlog.txt for the Detected threats section of log files, if you use a plain text file format to store logs).

- **Type** – If you select the Text file format, logs will be stored in a text file and data will be separated into tabs. The same applies to the comma-separated CSV file format. If you choose Event, logs will be stored in the Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to the file.

- **Delete all logs files** – Erases all stored logs currently selected in the Type drop-down menu. A notification about successful deletion of the logs will be shown.

**Audit log** – Informs you about each configuration change. To see the Audit log, click Tools in the main menu and then click Log files and select Audit logs from the drop-down menu.
Note

In order to help resolve issues more quickly, ESET may ask you to provide logs from your computer. ESET Log Collector makes it easy for you to collect the information needed. For more information about ESET Log Collector please visit our ESET Knowledgebase article.

4.6.1.3 Audit logs

In an enterprise environment there are usually multiple users with access rights defined for configuring endpoints. Since the modification of the product configuration might dramatically affect how the product operates it is essential that administrators would like to trace the changes done by users to help administrators quickly identify, resolve, and also to prevent occurring of the same or similar problems in the future.

The Audit log is a new type of logging from ESET Endpoint Security version 7.1 and solution for the identification of the origin of the problem. Audit log tracks changes in configuration or protection state and records snapshots for later reference.

The Audit log contains information about:

- Time - when the change was performed
- Type - what type of setting or feature was changed
- Description - what exactly was changed and which part of setting has been changed together with number of changed settings
- Source - where is the source of the change
- User - who made the change

Right-click any Settings changed type of audit log in the Log files window and select Show changes from the context menu to display detailed information about the performed change. Besides, you can restore setting change by clicking Restore from the context menu. If you select Delete all from the context menu, the log with information about this action will be created.
If **Optimize log files automatically** enabled in **Advanced setup > Tools > Log files**, the Audit logs will automatically be defragmented as other logs.

If **Automatically delete records older than (days)** enabled in **Advanced setup > Tools > Log files**, log entries older than the specified number of days will automatically be deleted.

### 4.6.2 Scheduler

Scheduler manages and launches scheduled tasks with predefined configuration and properties.

The Scheduler can be accessed from the ESET Endpoint Security main program window by clicking **Tools > Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time and scanning profile used.

The Scheduler serves to schedule the following tasks: detection engine update, scanning task, system startup file check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add task** or **Delete** at the bottom). Right click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, and delete an existing task. Use the checkboxes at the beginning of each entry to activate/deactivate the tasks.

By default, the following scheduled tasks are displayed in **Scheduler**:

- Log maintenance
- Regular automatic update
- Automatic update after dial-up connection
- Automatic update after user logon
- Automatic startup file check (after user logon)
- Automatic startup file check (after successful module update)

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit**... or select the task you wish to modify and click the **Edit** button.

#### Add a new task

1. Click **Add task** at the bottom of the window.
2. Enter a name of the task.
3. Select the desired task from the drop-down menu:
   - **Run external application** – Schedules the execution of an external application.
   - **Log maintenance** – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
   - **System startup file check** – Checks files that are allowed to run at system startup or logon.
   - **Create a computer status snapshot** – Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
   - **On-demand computer scan** – Performs a computer scan of files and folders on your computer.
   - **Update** – Schedules an Update task by updating the detection engine and program modules.
4. Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting checkbox in the list of scheduled tasks), click **Next** and select one of the timing options:
   - **Once** – The task will be performed at the predefined date and time.
   - **Repeatedly** – The task will be performed at the specified time interval.
   - **Daily** – The task will run repeatedly each day at the specified time.
   - **Weekly** – The task will be run on the selected day and time.
   - **Event triggered** – The task will be performed on a specified event.
5. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. If the task could not be run at the predefined time, you can specify when it will be performed again:

- At the next scheduled time
- As soon as possible
- Immediately, if the time since the last run exceeds a specified value (the interval can be defined using the **Time since last run** scroll box)

You can review scheduled task when right click and click **Show task details**.

![Scheduler - ESET Endpoint Security](image)

### 4.6.3 Protection statistics

To view a graph of statistical data related to ESET Endpoint Security's protection modules, click **Tools > Protection statistics**. Select the desired protection module from the **Statistics** drop-down menu to see the corresponding graph and legend. If you mouse over an item in the legend, only the data for that item will display in the graph.

The following statistic graphs are available:

- **Antivirus and Antispyware protection** – Displays the number of infected and cleaned objects.
- **File system protection** – Only displays objects that were read or written to the file system.
- **Email client protection** – Only displays objects that were sent or received by email clients.
- **Web access and Anti-Phishing protection** – Only displays objects downloaded by web browsers.
- **Email client antispam protection** – Displays the history of antispam statistics since the last startup.

Next to the statistics graphs, you can see the number of all scanned objects, number of infected objects, number of cleaned objects and the number of clean objects. Click **Reset** to clear statistics information or click **Reset all** to clear and remove all the existing data.
4.6.4 Watch activity

To see the current File system activity in graph form, click Tools > Watch activity. At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. To change the time span, select from Refresh rate drop-down menu.

The following options are available:

- **Step: 1 second** – The graph refreshes every second and the timeline covers the last 10 minutes.
- **Step: 1 minute (last 24 hours)** – The graph is refreshed every minute and the timeline covers the last 24 hours.
- **Step: 1 hour (last month)** – The graph is refreshed every hour and the timeline covers the last month.
- **Step: 1 hour (selected month)** – The graph is refreshed every hour and the timeline covers the last X selected months.

The vertical axis of the File system activity graph represents the amount of read data (blue color) and the amount of written data (turquoise color). Both values are given in kB (kilobytes)/MB/GB. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

You can also select Network activity from the drop-down menu. The graph display and options for File system activity and Network activity are the same except that the latter displays the amount of received data (blue color) and amount of sent data (turquoise color).
4.6.5 ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components such as drivers and applications, network connections or important registry entries and assesses the risk level of each component. This information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection. See also Online user guide for ESET SysInspector.

The SysInspector window displays the following information about created logs:

- **Time** – The time of log creation.
- **Comment** – A short comment.
- **User** – The name of the user who created the log.
- **Status** – The status of log creation.

The following actions are available:

- **Show** – Opens created log. You can also right-click a given log file and select Show from the context menu.
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as Created) before attempting to access the log.
- **Delete** – Removes the selected log(s) from the list.

The following items are available from the context menu when one or more log files are selected:

- **Show** – Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as Created) before attempting to access the log.
- **Delete** – Deletes selected log.
- **Delete all** – Deletes all logs.
- **Export...** – Exports the log to a .xml file or zipped .xml.

4.6.6 Cloud-based protection

ESET LiveGrid® (built on the ESET ThreatSense.Net advanced early warning system) utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to needs of our customers and keep ESET responsive to the latest threats.

A user can check the reputation of Running processes and files directly from the program’s interface or contextual menu with additional information available from ESET LiveGrid®. There are two options:

1. You can choose not to enable ESET LiveGrid®. You will not lose any functionality in the software, but in some cases, ESET Endpoint Security may respond faster to new threats than detection engine update when ESET LiveGrid® is enabled.
2. You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its detection capabilities.

ESET LiveGrid® will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer’s operating system.

By default, ESET Endpoint Security is configured to submit suspicious files for detailed analysis to the ESET Virus Lab. Files with certain extensions such as .doc or .xls are always excluded. You can also add other extensions if there are particular files that you or your organization want to avoid sending.
The ESET LiveGrid® reputation system provides cloud-based whitelisting and blacklisting. To access settings for ESET LiveGrid®, press F5 to enter Advanced setup and expand Detection Engine > Cloud-based Protection.

**Cloud-based protection in Advanced setup**

**Enable ESET LiveGrid® reputation system (recommended)** – The ESET LiveGrid® reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

**Enable ESET LiveGrid® feedback system** – Data will be sent to the ESET Research Lab for further analysis.

**Submit crash reports and diagnostics data** – Submit data such as crash reports, modules memory dumps.

**Submit anonymous statistics** – Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, product version, and configuration including information about your system.

**Contact email (optional)** – Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

**Submission of samples**

**Automatic submissions of infected samples**

This will submit all infected samples to ESET for analysis and to improve future detection. The following options are available:

- All infected samples
- All samples except documents
- Do not submit

**Automatic submissions of suspicious samples**

- **Executables** – Includes files like .exe, .dll, .sys.
- **Archives** – Includes filetypes like .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts** – Includes filetypes like .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Other** – Includes filetypes like .jar, .reg, .msi, .sfw, .lnk.
- **Possible Spam emails** – This will allow sending possible spam parts or whole possible spam emails with attachment to ESET for further analysis. Enabling this option improve Global detection of spam including improvements to future spam detection for you.
- **Documents** – Include Microsoft Office documents or PDFs with active content.

**Exclusions**

The Exclusion filter allows you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.
If you have used ESET LiveGrid® before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. Once all current information is sent, no further packages will be created.

### 4.6.7 Running processes

Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET Endpoint Security provides detailed information on running processes to protect users with ESET LiveGrid® technology enabled.

Reputation – In most cases, ESET Endpoint Security and ESET LiveGrid® technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a reputation level from 9 – Best reputation (green) to 0 – Worst reputation (red).

Process – Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing **Ctrl+Shift+Esc** on your keyboard.

PID – Is an ID of processes running in Windows operating systems.

---

**Note**

Known applications marked green are definitely clean (white-listed) and will be excluded from scanning, as this will improve the scanning speed of on-demand computer scan or Real-time file system protection on your computer.

Number of users – The number of users that use a given application. This information is gathered by ESET LiveGrid® technology.

Time of discovery – Period of time since the application was discovered by ESET LiveGrid® technology.
When an application is marked as Unknown (orange) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the submit file for analysis feature to send the file to the ESET Virus Lab. If the file turns out to be a malicious application, its detection will be added to one of the upcoming detection engine updates.

Application name – The given name of a program or process.

By clicking a given application at the bottom, the following information will appear at the bottom of the window:

- **Path** – Location of an application on your computer.
- **Size** – File size either in kB (kilobytes) or MB (megabytes).
- **Description** – File characteristics based on the description from the operating system.
- **Company** – Name of the vendor or application process.
- **Version** – Information from the application publisher.
- **Product** – Application name and/or business name.
- **Created on** – Date and time when an application was created.
- **Modified on** – Last date and time when an application was modified.

Reputation can also be checked on files that do not act as running programs/processes - mark files you want to check, right-click on them and from the context menu select Advanced options > Check File Reputation using ESET LiveGrid®.

### 4.6.8 Security report

This feature gives an overview of the statistics for the following categories:

- **Documents scanned** – Displays the number of scanned document objects.
- **Applications scanned** – Displays the number of scanned executable objects.
- **Other objects scanned** – Displays the number of other scanned objects.
- **Web pages objects scanned** – Displays the number of scanned web page objects.

The order of these categories is based on the numeric value from the highest to the lowest. The categories with zero values are not displayed. Click Show more to expand and display hidden categories.

Below the categories, you can see the actual virus situation with the map of the world. The presence of virus in each country is indicated with color (the darker the color, the higher the number). Countries without data are grayed. Hover mouse over the country displays data for the selected country. You can select the specific continent and it will be automatically zoomed.

Click the gear wheel in the upper right corner you can Enable/Disable Security report notifications or select whether the data will be displayed for the last 30 days or since the product was activated. If ESET Endpoint Security is installed less than 30 days, then only the number of days from installation can be selected. The period of 30 days is set by default.

Reset data will clear all statistics and remove the existing data for Security report. This action has to be confirmed except the case that you deselect the Ask before resetting statistics option in Advanced setup > User interface > Alerts and notifications > Confirmation messages.
4.6.9 Network connections

In the Network connections section, you can see a list of active and pending connections. This helps you control all applications establishing outgoing connections.

The first line displays the name of the application and its data transfer speed. To see the list of connections made by the application (and also more detailed information), click +.

Columns

- **Application/Local IP** – Name of application, local IP addresses and communication ports.
- **Remote IP** – IP address and port number of the particular remote computer.
- **Protocol** – Transfer protocol used.
- **Up-Speed/Down-Speed** – The current speed of outgoing and incoming data.
- **Sent/Received** – Amount of data exchanged within the connection.
- **Show details** – Choose this option to display detailed information about the selected connection.

Select an application or IP address in the Network connections screen and right-click on it will show context menu with following structure:

- **Resolve host names** – If possible, all network addresses are displayed in DNS format, not in the numeral IP address format.
- **Show only TCP connections** – The list only displays connections which belong to the TCP protocol suite.
- **Show listening connections** – Select this option to only display connections, where no communication is currently established, but the system has opened a port and is waiting for a connection.
- **Show connections within the computer** – Select this option to only show connections, where the remote side is a local system – so-called localhost connections.
Right-click on a connection to see additional options that include:

**Deny communication for the connection** – Terminates the established communication. This option is available only after clicking on an active connection.

**Refresh speed** – Choose the frequency to refresh the active connections.

**Refresh now** – Reloads the Network connections window.

The following options are available only after clicking on an application or process, not an active connection:

**Temporarily deny communication for the process** – Rejects current connections for the given application. If a new connection is established, the firewall uses a predefined rule. A description of the settings can be found in the [Rules and zones](#) section.

**Temporarily allow communication for the process** – Permits current connections for the given application. If a new connection is established, the firewall uses a predefined rule. A description of the settings can be found in the [Rules and zones](#) section.

### 4.6.10 ESET SysRescue Live

ESET SysRescue Live is a free utility that allows you to create a bootable rescue CD/DVD or USB drive. You can boot an infected computer from your rescue media, and then scan for malware and clean infected files.

The main advantage of ESET SysRescue Live is the fact that it runs independent of the host operating system, but has direct access to the disk and file system. This makes it possible to remove threats that under normal operating conditions might be impossible to delete (for example, when the operating system is running, etc.).

- [Online Help for ESET SysRescue Live](#)

### 4.6.11 Submission of samples for analysis

If you find a suspiciously behaving file on your computer or suspicious site on the Internet, you can submit it to the ESET Research Lab for analysis.

Before submitting samples to ESET

Do not submit a sample unless it meets at least one of the following criteria:

- The sample is not detected by your ESET product at all
- The sample is incorrectly detected as a threat
- We do not accept your personal files (that you would like to scan for malware by ESET) as samples (ESET Research Lab does not perform on-demand scans for users)
- Use a descriptive subject line and enclose as much information about the file as possible (for example, a screenshot or the website you downloaded it from)

Sample submission enables you to send a file or a site to ESET for analysis using one of these methods:

1. Using the sample submission dialog can be found in **Tools > Submit sample for analysis**.

2. Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected", and send it to [samples@eset.com](mailto:samples@eset.com).

3. To report spam, spam false positives or miscategorized websites by the Parental control module, please refer to our [ESET Knowledgebase article](#).

With **Select sample for analysis** opened, select the description from the **Reason for submitting the sample** drop-down menu that best fits your message:
• Suspicious file
• Suspicious site (a website that is infected by any malware)
• False positive file (file that is detected as an infection but are not infected)
• False positive site
• Other

File/Site – The path to the file or website you intend to submit.

Contact email – This contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional, select Submit anonymously to leave it empty.

You may not get a response from ESET

You will not get a response from ESET unless more information is required from you. Each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.

If the sample turns out to be a malicious application or website, its detection will be added to an upcoming ESET update.

4.6.12 Email notifications

ESET Endpoint Security can automatically send notification emails if an event with the selected verbosity level occurs. Enable Send event notifications by email to activate email notifications.

SMTP server

SMTP server – The SMTP server used for sending notifications (e.g. smtp.provider.com:587, predefined port is 25).

Note

SMTP servers with TLS encryption are supported by ESET Endpoint Security.
Username and password – If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.

Sender address – This field specifies the sender address that will be displayed in the header of notification emails.

Recipient addresses – This field specifies the recipient addresses that will be displayed in the header of notification emails. Use a semi-colon ";" to separate multiple email addresses.

From the Minimum verbosity for notifications drop-down menu, you can select the starting severity level of notifications to be sent.

- Diagnostic – Logs information needed to fine-tune the program and all records above.
- Informative – Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- Warnings – Records critical errors and warning messages (Antistealth is not running properly or update failed).
- Errors – Errors (document protection not started) and critical errors will be recorded.
- Critical – Logs only critical errors error starting antivirus protection or infected system.

Enable TLS – Enable sending alert and notification messages supported by TLS encryption.

Interval after which new notification emails will be sent (min) – Interval in minutes after which new notifications will be sent to email. If you set this value to 0, the notifications will be sent immediately.

Sent each notification in a separate email – When enabled, the recipient will receive a new email for each individual notification. This may result in large number of emails being received in a short period of time.

Message format

Communications between the program and a remote user or system administrator are done via emails or LAN messages (using the Windows messaging service). The default format of the alert messages and notifications will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

Format of event messages – Format of event messages that are displayed on remote computers.

Format of threat warning messages – Threat alert and notification messages have a predefined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Charset – Converts an email message to the ANSI character encoding based upon Windows Regional settings (for example, windows-1250), Unicode (UTF-8), ASCII 7-bit (for example "á" will be changed to "a" and an unknown symbol to ")") or Japanese (ISO-2022-JP).

Use Quoted-printable encoding – The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

Keywords (strings separated by % signs) are replaced in the message by the actual information as specified. The following keywords are available:

- %ComputerName% - Name of the computer where the alert occurred.
- %ProgramName% - Program that generated the alert.
- %TimeStamp% - Date and time of the event.
- %InfectedObject% - Name of infected file, message, etc.
- %VirusName% - Identification of the infection.
- %ErrorDescription% - Description of a non-virus event.
- %Scanner% - Module concerned.

The keywords %InfectedObject% and %VirusName% are only used in threat warning messages, and %ErrorDescription% is only used in event messages.
4.6.13 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET Endpoint Security.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.

Files stored in the quarantine folder can be viewed in a table that displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (for example, object added by user), and number of detections.

Quarantining files

ESET Endpoint Security automatically quarantines deleted files (if you have not disabled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Move to quarantine**. The original file will be removed from its original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine file**.

Restoring from Quarantine

Quarantined files can also be restored to their original location. To restore a quarantined file, right-click it in the Quarantine window and select **Restore** from the context menu. If a file is marked as a **potentially unwanted application**, **Restore and exclude from scanning** will also be available. The context menu also contains the **Restore to...** option, which allows you to restore a file to a location other than the one from which it was deleted.

Deleting from Quarantine – Right-click on a given item and select **Delete from Quarantine**, or select the item you want to delete and press **Delete** on your keyboard. You can also select multiple items and delete them together.
If the program has quarantined a harmless file by mistake, exclude the file from scanning after restoring it and send the file to ESET Technical Support.

**Submitting a file from the Quarantine**

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly detected as a threat and subsequently quarantined, please send the file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

### 4.6.14 Proxy server setup

In large LAN networks, communication between your computer and the internet can be mediated by a proxy server. Using this configuration, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET Endpoint Security, proxy server setup is available from two different sections of the Advanced setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Endpoint Security. Parameters here will be used by all modules that require a connection to the Internet.

To specify proxy server settings for this level, select **Use proxy server** and enter the address of the proxy server into the **Proxy server** field along with the **Port** number of the proxy server.

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and enter a valid **Username** and **Password** into the respective fields. Click **Detect proxy server** to automatically detect and populate proxy server settings. The parameters specified in Internet options for Internet Explorer or Google Chrome will be copied.

**Note**

You must manually enter your Username and Password in **Proxy server** settings.

**Use direct connection if proxy is not available** – If ESET Endpoint Security is configured to connect via proxy and the proxy is unreachable, ESET Endpoint Security will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be established from Advanced update setup (**Advanced setup > Update > Profiles > Updates > Connection options**) by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu. This setting applies for the given update profile and is recommended for laptops that often receive detection engine updates from remote locations. For more information about this setting, see **Advanced update setup**.
4.6.15 Time slots

Time slots can be created and then assigned to rules for Device control and Web control. The Time slots setting can be found in Advanced setup > Tools. This lets you define commonly used time slots (e.g. work time, weekend, etc.) and reuse them easily without redefining the time ranges for every rule. Time slot is applicable to any relevant type of rule that supports time-based control.

To create a time slot, complete the following:
1. Click **Edit > Add**.
2. Type the name and **description** of the time slot and click **Add**.
3. Specify the day and start/end time for the time slot or select **All day**.
4. Click **OK** to confirm.

A single time slot can be defined with one or more time ranges based on days and times. When the time slot is created, it will show in the **Apply during** drop-down menu in the **Device control rules editor window** or **Web control rules editor window**.

### 4.6.16   Microsoft Windows update

The Windows update feature is an important component of protecting users from malicious software. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET Endpoint Security notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** – No system updates will be offered for download.
- **Optional updates** – Updates marked as low priority and higher will be offered for download.
- **Recommended updates** – Updates marked as common and higher will be offered for download.
- **Important updates** – Updates marked as important and higher will be offered for download.
- **Critical updates** – Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Accordingly, the system update information may not be immediately available after saving changes.

### 4.6.17   ESET CMD

This is a feature that enables advanced ecmd commands. It gives you the possibility to export and import settings using command line (ecmd.exe). Until now, it was possible to export and import settings using **GUI** only. ESET Endpoint Security configuration can be exported to `.xml` file.

When you have enabled ESET CMD, there are two authorization methods available:

- **None** - no authorization. We do not recommend you this method because it allows import of any unsigned configuration which is a potential risk.
- **Advanced setup password** - uses password protection. When importing configuration from an `.xml` file, this file must be signed (see signing `.xml` configuration file further down). This authorization method verifies password during configuration import to make sure it matches the password specified in **Access Setup**. If you do not have access setup enabled, password does not match or `.xml` configuration file is not signed, configuration will not be imported.

Once ESET CMD is enabled, you can start using command line for exporting/importing ESET Endpoint Security configuration. You can do it manually or create a script for the purpose of automation.

---

**Important**

To use advanced ecmd commands, you need to run them with administrator privileges, or open Windows Command Prompt (cmd) using **Run as administrator**. Otherwise, you'll get **Error executing command** message. Also, when exporting configuration, destination folder must exist.

---

**Note**

Advanced ecmd commands can only be run locally. Executing a client task **Run command** using ERA will not work.
Example

Export settings command:
ecmd /getcfg c:\config\settings.xml

Import settings command:
ecmd /setcfg c:\config\settings.xml

Signing .xml configuration file:
1. Download XmlSignTool from [ESET Tools and Utilities download page](#) and extract it. This tool was developed specifically for signing eset .xml configuration files.
2. Open Windows Command Prompt (cmd) using Run as administrator.
3. Navigate to a location with XmlSignTool.exe.
4. Execute a command to sign .xml configuration file, usage: XmlSignTool <xml_file_path>
5. Enter and Re-enter Advanced Setup Password as asked by the XmlSignTool. Your .xml configuration file is now signed and can be used for import on another instance of ESET Endpoint Security with ESET CMD using Advanced setup password authorization method.

**Warning**

Enabling ESET CMD without an authorization is not recommended, since this will allow the import of any unsigned configuration. Set the password in Advanced setup > User interface > Access setup to prevent from unauthorized modification by users.

List of ecmd commands

Individual security features can be enabled and temporarily disabled with the ERA Client Task Run command. The commands do not override policy settings and any paused settings will revert back to its original state after the command has executed or after a device reboot. To utilize this feature, specify the command line to run in the field of the same name.

Review the list of commands for each security feature below:

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Temporary Pause command</th>
<th>Enable Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time file system protection</td>
<td>ecmd /setfeature onaccess pause</td>
<td>ecmd /setfeature onaccess enable</td>
</tr>
<tr>
<td>Document protection</td>
<td>ecmd /setfeature document pause</td>
<td>ecmd /setfeature document enable</td>
</tr>
<tr>
<td>Device control</td>
<td>ecmd /setfeature devcontrol pause</td>
<td>ecmd /setfeature devcontrol enable</td>
</tr>
<tr>
<td>Presentation mode</td>
<td>ecmd /setfeature presentation pause</td>
<td>ecmd /setfeature presentation enable</td>
</tr>
<tr>
<td>Anti-Stealth technology</td>
<td>ecmd /setfeature antistealth pause</td>
<td>ecmd /setfeature antistealth enable</td>
</tr>
<tr>
<td>Personal firewall</td>
<td>ecmd /setfeature firewall pause</td>
<td>ecmd /setfeature firewall enable</td>
</tr>
<tr>
<td>Network attack protection (IDS)</td>
<td>ecmd /setfeature ids pause</td>
<td>ecmd /setfeature ids enable</td>
</tr>
<tr>
<td>Botnet protection</td>
<td>ecmd /setfeature botnet pause</td>
<td>ecmd /setfeature botnet enable</td>
</tr>
<tr>
<td>Web Control</td>
<td>ecmd /setfeature webcontrol pause</td>
<td>ecmd /setfeature webcontrol enable</td>
</tr>
<tr>
<td>Function</td>
<td>Command</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Web access protection</td>
<td><code>ecmd /setfeature webaccess pause</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ecmd /setfeature webaccess enable</code></td>
<td></td>
</tr>
<tr>
<td>Email client protection</td>
<td><code>ecmd /setfeature email pause</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ecmd /setfeature email enable</code></td>
<td></td>
</tr>
<tr>
<td>Antispam protection</td>
<td><code>ecmd /setfeature antispam pause</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ecmd /setfeature antispam enable</code></td>
<td></td>
</tr>
<tr>
<td>Anti-Phishing protection</td>
<td><code>ecmd /setfeature antiphishing pause</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ecmd /setfeature antiphishing enable</code></td>
<td></td>
</tr>
</tbody>
</table>

### 4.7 User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI).

Using the **User Interface elements** tool, you can adjust the program's visual appearance and effects used.

To provide maximum security of your security software, you can prevent any unauthorized changes using the **Access setup** tool.

By configuring **Alerts and notifications**, you can change the behavior of detection alerts and system notifications. These can be customized to fit your needs.

If you choose not to display some notifications, they will be displayed in **User interface elements > Application statuses**. Here you can check their status or alternatively prevent to display these notifications.

The **Context menu integration** is displayed after right-clicking on the selected object. Use this tool to integrate the ESET Endpoint Security control elements into the context menu.

**Presentation mode** is useful for users, who want to work with an application and not be interrupted by pop-up windows, scheduled tasks and any components that could load the processor and RAM.

#### 4.7.1 User interface elements

User interface configuration options in ESET Endpoint Security allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface > User interface elements** branch of the ESET Endpoint Security Advanced setup tree.

In the **User interface elements** section, you can adjust the working environment. Use the **Start mode** drop-down menu to select from the following Graphical user interface (GUI) start modes:

- **Full** – The complete GUI will be displayed.
- **Minimal** – The GUI is running, but only notifications are displayed to the user.
- **Manual** – The GUI is not started automatically on logon. Any user may start it manually.
- **Silent** – No notifications or alerts will be displayed. The GUI can only be started by the Administrator. This mode can be useful in situations where you need to preserve system resources.

**Note**

Once the Minimal GUI start mode is selected and your computer is restarted, notifications will be displayed but the graphical interface will not. To revert to full graphical user interface mode, run the GUI from the Start menu under **All Programs > ESET > ESET Endpoint Security** as an administrator, or you can do this via ESET Security Management Center using a policy.

If you want to deactivate the ESET Endpoint Security splash-screen, deselect **Show splash-screen at startup**.

To have ESET Endpoint Security play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select **Use sound signal**.

**Integrate into the context menu** – Integrate the ESET Endpoint Security control elements into the context menu.

**Statuses**
Application statuses – Click Edit button to manage (disable) statuses that are displayed in the Protection status pane in main menu.

License information

Show license information – When disabled, the license expiration date on Protection status and Help and support screen will not be displayed.

Show license messages and notifications – When disabled, the notifications and messages will only be displayed when the license expired.

Note

License information settings are applied but not accessible for ESET Endpoint Security activated with MSP license.
4.7.2 Access setup

In order to provide maximum security for your system, it is essential that ESET Endpoint Security is correctly configured. Any unqualified change may result in a loss of important data. To avoid unauthorized modifications, the setup parameters of ESET Endpoint Security can be password protected. Configuration settings for password protection are located in Advanced setup (F5) under User interface > Access setup.

Password protect settings – Indicate password settings. Click to open the Password setup window.

To set or change a password to protect setup parameters, click Set.

Require full administrator rights for limited administrator accounts – Leave this option active to prompt the current user (if he or she does not have administrator rights) to enter the administrator username and password when modifying certain system parameters (similar to the UAC in Windows Vista). The modifications include disabling protection modules or turning off the firewall.

For Windows XP only:

Require administrator rights (system without UAC support) – Enable this option to have ESET Endpoint Security prompt for administrator credentials.

4.7.3 Alerts and message boxes

Looking for information about common alerts and notifications?

- Threat found
- Address has been blocked
- Product not activated
- Update is available
- Troubleshooting for "Modules update failed" message
- Network threat blocked
The **Alerts and message boxes** section under **User interface** allows you to configure how threat alerts and system notifications (for example, successful update messages) are handled by ESET Endpoint Security. You can also set the display time and transparency of system tray notifications (this applies only on systems that support system tray notifications).

### Alert windows

Disabling **Display alerts** will cancel all alert windows, and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left in its default setting (enabled).

### Desktop notifications

Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select **Display notifications on desktop**. Turn the **Do not display notifications when running applications in full-screen mode** switch on to suppress all non-interactive notifications. More detailed options, such as notification display time and window transparency can be modified below.

The **Minimum verbosity of events to display** drop-down menu allows you to select the severity level of alerts and notifications to be displayed. The following options are available:

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting antivirus protection, built-in firewall, etc...).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies which user will receive system and other notifications on systems allowing multiple users to connect at the same time. Normally, this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.
Message boxes
To close pop-up windows automatically after a certain period of time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time period elapses.

**Confirmation messages** – Shows you a list of confirmation messages that you can select to display or not to display.

**4.7.3.1 Confirmation messages**
This dialog window displays confirmation messages that ESET Endpoint Security will display before any action is performed. Select or deselect the check box next to each confirmation message to allow or disable it.

**4.7.3.2 Advanced settings conflict error**
This error may occur if some component (e.g. HIPS or Firewall) and user create the rules in interactive or learning mode at the same time.

---

**Important**
We recommend to change the filtering mode into the default **Automatic mode** if you want to create your own rules. Read more about [ESET Firewall Learning mode](#). Read more about [HIPS and HIPS filtering modes](#).

---

**4.7.4 Notifications**
In this window you can customize the messaging used in notifications.

**Default notification message** – A default message to be shown in the footer of notification.

**Threats**
Enable **Do not close malware notifications automatically** to have malware notifications stay on screen until they are closed manually.

Disable **Use default message** and enter your own message in the **Threat notification message** field to use customized notification messaging.
4.7.5 System tray icon

Some of the most important setup options and features are available by right-clicking the system tray icon.

Pause protection – Displays the confirmation dialog box that disables Detection engine, which guards against attacks by controlling file, web and email communication.

The Time interval drop-down menu represents the period of time that the protection will be disabled for.

Pause firewall (allow all traffic) – Switches the firewall to an inactive state. See Network for more information.

Block all network traffic – Firewall will block all outgoing / incoming network and internet traffic. You can re-enable it by clicking Stop blocking all network traffic.

Advanced setup – Select this option to enter the Advanced setup tree. You can also access Advanced setup by pressing the F5 key or navigating to Setup > Advanced setup.

Log files – Log files contain information about all important program events that have occurred and provide an overview of detections.

Open ESET Endpoint Security – Opens the ESET Endpoint Security main program window from the tray icon.

Reset window layout – Resets the ESET Endpoint Security window to its default size and position on the screen.

Check for updates... – Starts updating the program modules to ensure your level of protection against malicious code.
4.7.6 Context menu

The context menu is displayed after right-clicking an object (file). The menu lists all of the actions that you can perform on an object.

It is possible to integrate ESET Endpoint Security control elements into the context menu. Setup option for this functionality are available in the Advanced setup tree under **User interface > User interface elements**.

Integrate into the context menu – Integrate the ESET Endpoint Security control elements into the context menu.

4.7.7 Help and support

ESET Endpoint Security contains troubleshooting tools and support information that will help you solve issues that you may encounter.

Help

Search ESET Knowledgebase – The **ESET Knowledgebase** contains answers to the most frequently asked questions as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various problems.

Open help – Click this link to launch the ESET Endpoint Security help pages.

Find quick solution – Click this link to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting Technical Support.

Technical Support

Submit support request – If you could not find an answer to your problem, you can use this form located on the ESET website to quickly contact our Technical Support department.

Details for Technical Support – When prompted, you can copy and send information to ESET Technical Support (such as product name, product version, operating system and processor type).

Support Tools

Threat encyclopedia – Links to the ESET Threat Encyclopedia, which contains information about the dangers and symptoms of different types of infiltration.

Detection Engine history – Links to ESET Virus radar, which contains information about each version of the ESET detection database (previously known as "virus signature database").

ESET Log Collector – Links to the **ESET Knowledgebase article**, where you can download ESET Log Collector, application that automatically collects information and logs from a computer in order to help resolve issues more quickly. For more information see the **ESET Log Collector online user guide**.

ESET Specialized Cleaner – Removal tools for common malware infections, for more information please visit this **ESET Knowledgebase article**.

Activate Product/Change License – Click to launch the activation window and activate your product.

4.7.7.1 About ESET Endpoint Security

This window provides details about installed version of ESET Endpoint Security, your operating system and system resources.

Click Installed components to see information about the list of installed program modules. You can copy information about modules to the clipboard by clicking Copy. This may be useful during troubleshooting or when contacting Technical Support.
4.7.7.2 Submit system configuration data

In order to provide assistance as quickly and accurately as possible, ESET requires information about ESET Endpoint Security configuration, detailed system information and running processes (ESET SysInspector log file) and registry data. ESET will use this data only for providing technical assistance to the customer.

When submit the web form, your system configuration data will be submitted to ESET. Select Always submit this information if you want to remember this action for this process. To submit the form without sending any data click Don’t submit data and you can contact ESET Technical Support using the online support form.

This setting can also be configured in Advanced setup > Tools > Diagnostics > Technical Support.

Note

If you have decided to submit system data it is needed to fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.

4.8 Advanced user

4.8.1 Profile manager

Profile manager is used in two places within ESET Endpoint Security – in the On-demand computer scan section and in the Update section.

On-demand computer scan

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced setup window (F5) and click Antivirus > On-demand computer scan and then Edit next to List of profiles. The Update profile drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Note

Suppose that you want to create your own scan profile and the Scan your computer configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply Strict cleaning. Enter the name of your new profile in the Profile manager window and click Add. Select your new profile from the Selected profile drop-down menu and adjust the remaining parameters to meet your requirements, and then click OK to save your new profile.

Update

The profile editor in the Update setup section allows users to create new update profiles. Create and use your own custom profiles (other than the default My profile) only if your computer uses multiple means to connect to update servers.

For example, a laptop that normally connects to a local server (Mirror) in the local network but downloads updates directly from ESET update servers when disconnected from the local network (business trip) might use two profiles: the first one for connecting to the local server; the other one for connecting to ESET servers. Once these profiles are configured, navigate to Tools > Scheduler and edit the update task parameters. Designate one profile as primary and the other as secondary.

Update profile – The currently used update profile. To change it, choose a profile from the drop-down menu.
List of profiles – Create new or remove existing update profiles.

4.8.2 Keyboard shortcuts

For better navigation in ESET Endpoint Security, the following keyboard shortcuts can be used:

<table>
<thead>
<tr>
<th>Keyboard shortcut</th>
<th>Action taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>opens help pages</td>
</tr>
<tr>
<td>F5</td>
<td>opens Advanced setup</td>
</tr>
<tr>
<td>Up/Down</td>
<td>navigation in product through items</td>
</tr>
<tr>
<td>TAB</td>
<td>moves the cursor in a window</td>
</tr>
<tr>
<td>Esc</td>
<td>closes the active dialog window</td>
</tr>
<tr>
<td>Ctrl+U</td>
<td>shows information about ESET license and your computer (Details for Technical Support)</td>
</tr>
<tr>
<td>Ctrl+R</td>
<td>resets product window to its default size and position on the screen</td>
</tr>
</tbody>
</table>

4.8.3 Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, `ekrn`). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET Endpoint Security problems.

Click the drop-down menu next to Dump type and select one of three available options:

- Select Disable to disable this feature.
- Mini (default) – Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited, however because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- Full – Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

Target directory – Directory where the dump during the crash will be generated.

Open diagnostics folder – Click Open to open this directory in a new Windows explorer window.

Create diagnostic dump – Click Create to create diagnostic dump files in the Target directory.

Advanced logging

Enable Antispam engine advanced logging – Record all events that occur during antispam scanning. This can help developers to diagnose and fix problems related to ESET Antispam engine.

Enable Device control advanced logging – Record all events that occur in Device control. This can help developers diagnose and fix problems related to Device control.

Enable Licensing advanced logging – Record all product communication with ESET activation and ESET Business Account servers.

Enable Network protection advanced logging – Record all network data passing through Firewall in PCAP format in order to help developers diagnose and fix problems related to Firewall.

Enable Operating System advanced logging – Additional information about Operating system such as running processes, CPU activity, disc operations will be gathered. This can help developers to diagnose and fix problems related to ESET product running on your operating system (available for Windows 10).

Enable Protocol filtering advanced logging – Record all data passing through the Protocol filtering engine in PCAP format in order to help the developers diagnose and fix the problems related to Protocol filtering.

Enable Update engine advanced logging – Record all events that occur during update process. This can help developers diagnose and fix problems related to the Update engine.
**Enable Web control advanced logging** – Record all events that occur in Parental control. This can help developers diagnose and fix problems related to Parental control.

### Log files location

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Log files directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Vista and later</td>
<td>C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics\</td>
</tr>
<tr>
<td>Earlier versions of Windows</td>
<td>C:\Documents and Settings\All Users...</td>
</tr>
</tbody>
</table>

#### 4.8.4 Import and export settings

You can import or export your customized ESET Endpoint Security .xml configuration file from the **Setup** menu.

Importing and exporting of configuration files is useful if you need to backup your current configuration of ESET Endpoint Security for use at a later time. The export settings option is also convenient for users who want to use their preferred configuration on multiple systems, they can easily import an .xml file to transfer these settings.

Importing a configuration is very easy. In the main program window click **Setup > Import/Export settings**, and then select **Import settings**. Enter the file name of the configuration file or click the ... button to browse for the configuration file you want to import.

The steps to export a configuration are very similar. In the main program window, click **Setup > Import/Export settings**. Select **Export settings** and enter the file name of the configuration file (i.e. *export.xml*). Use the browser to select a location on your computer to save the configuration file.

**Note**

You may encounter an error while exporting settings if you do not have enough rights to write the exported file to specified directory.
4.8.5 Command Line

ESET Endpoint Security's antivirus module can be launched via the command line – manually (with the “ecls” command) or with a batch (“bat”) file. ESET Command-line scanner usage:

ecls [OPTIONS..] FILES..

The following parameters and switches can be used while running the on-demand scanner from the command line:

Options

/base-dir=FOLDER load modules from FOLDER
/quar-dir=FOLDER quarantine FOLDER
/exclude=MASK exclude files matching MASK from scanning
/subdir scan subfolders (default)
/no-subdir do not scan subfolders
/max-subdir-level=LEVEL maximum sub-level of folders within folders to scan
/symlink follow symbolic links (default)
/no-symlink skip symbolic links
/ads scan ADS (default)
/no-ads do not scan ADS
/log-file=FILE log output to FILE
/log-rewrite overwrite output file (default – append)
/log-console log output to console (default)
/no-log-console do not log output to console
/log-all also log clean files
/no-log-all do not log clean files (default)
/aind show activity indicator
/auto scan and automatically clean all local disks

Scanner options

/files scan files (default)
/no-files do not scan files
/memory scan memory
/boots scan boot sectors
/no-boots do not scan boot sectors (default)
/arch scan archives (default)
/no-arch do not scan archives
/max-obj-size=SIZE only scan files smaller than SIZE megabytes (default 0 = unlimited)
/max-arch-level=LEVEL maximum sub-level of archives within archives (nested archives) to scan
/scan-timeout=LIMIT scan archives for LIMIT seconds at maximum
/max-arch-size=SIZE only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited)
/max-sfx-size=SIZE only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited)
/mail scan email files (default)
/no-mail do not scan email files
/mailbox scan mailboxes (default)
/no-mailbox do not scan mailboxes
/sfx scan self-extracting archives (default)
/no-sfx do not scan self-extracting archives
/rtp scan runtime packers (default)
/no-rtp do not scan runtime packers
/unsafe scan for potentially unsafe applications
/no-unsafe do not scan for potentially unsafe applications (default)
/unwanted scan for potentially unwanted applications
/no-unwanted do not scan for potentially unwanted applications (default)
/suspicious scan for suspicious applications (default)
The following options are available:

- none – No automatic cleaning will occur.
- standard (default) – ecls.exe will attempt to automatically clean or delete infected files.
- strict – ecls.exe will attempt to automatically clean or delete infected files without user intervention (you will not be prompted before files are deleted).
- rigorous – ecls.exe will delete files without attempting to clean regardless of what the file is.
- delete – ecls.exe will delete files without attempting to clean, but will refrain from deleting sensitive files such as Windows system files.

/quarantine copy infected files (if cleaned) to Quarantine (supplements the action carried out while cleaning)
/no-quarantine do not copy infected files to Quarantine

**General options**

/help show help and quit
/version show version information and quit
/preserve-time preserve last access timestamp

**Exit codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>no threat found</td>
</tr>
<tr>
<td>1</td>
<td>threat found and cleaned</td>
</tr>
<tr>
<td>10</td>
<td>some files could not be scanned (may be threats)</td>
</tr>
<tr>
<td>50</td>
<td>threat found</td>
</tr>
<tr>
<td>100</td>
<td>error</td>
</tr>
</tbody>
</table>

**Note**
Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

### 4.8.6 Idle-state detection

Idle state detection settings can be configured in **Advanced setup** under **Detection engine > Malware scans > Idle-state scanning > Idle state detection**. These settings specify a trigger for **Idle-state scanning**, when:

- the screen saver is running,
- the computer is locked,
- a user logs off.

Use the switches for each respective state to enable or disable the different idle state detection triggers.
4.8.7 Remote monitoring and management

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider.

The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory C:\Program Files\ESET\ESET Security\ermm.exe.

ermm.exe is a command line utility designed to facilitate the management of endpoint products and communications with any RMM plugin. ermm.exe exchanges data with the RMM Plugin, which communicates with the RMM Agent linked to an RMM Server. By default, the ESET RMM tool is disabled.

For more information, see How to activate Remote monitoring and management.
4.8.7.1 RMM Command Line

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file `ermm.exe` located in the Endpoint application within the directory `c:\Program Files\ESET\ESET Security`.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a `cmd.exe` into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.

`ermm.exe` uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.
<table>
<thead>
<tr>
<th>Context</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>application-info</td>
<td>Get information about product</td>
</tr>
<tr>
<td></td>
<td>license-info</td>
<td>Get information about license</td>
</tr>
<tr>
<td></td>
<td>protection-status</td>
<td>Get protection status</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>Get logs</td>
</tr>
<tr>
<td></td>
<td>scan-info</td>
<td>Get information about running scan</td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td>Get product configuration</td>
</tr>
<tr>
<td></td>
<td>update-status</td>
<td>Get information about update</td>
</tr>
<tr>
<td></td>
<td>activation-status</td>
<td>Get information about last activation</td>
</tr>
<tr>
<td>start</td>
<td>scan</td>
<td>Start on demand scan</td>
</tr>
<tr>
<td></td>
<td>activation</td>
<td>Start activation of product</td>
</tr>
<tr>
<td></td>
<td>deactivation</td>
<td>Start deactivation of product</td>
</tr>
<tr>
<td></td>
<td>update</td>
<td>Start update of product</td>
</tr>
<tr>
<td>set</td>
<td>configuration</td>
<td>Set configuration to product</td>
</tr>
</tbody>
</table>

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Command node not present</td>
<td>&quot;Command&quot; node not present in input json</td>
</tr>
<tr>
<td>2</td>
<td>Command not supported</td>
<td>Particular command is not supported</td>
</tr>
<tr>
<td>3</td>
<td>General error executing the command</td>
<td>Error during execution of command</td>
</tr>
<tr>
<td>4</td>
<td>Task already running</td>
<td>Requested task is already running and has not been started</td>
</tr>
<tr>
<td>5</td>
<td>Invalid parameter for command</td>
<td>Bad user input</td>
</tr>
<tr>
<td>6</td>
<td>Command not executed because it's disabled</td>
<td>RMM isn't enabled in advanced settings or isn't started as an administrator</td>
</tr>
</tbody>
</table>
4.8.7.2 List of JSON commands

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

4.8.7.2.1 get protection-status

Get the list of application statuses and the global application status

Command line

ermm.exe get protection-status

Parameters

None

Example

call

```json
{
  "command":"get_protection_status",
  "id":1,
  "version":"1"
}
```

result

```json
{
  "id":1,
  "result":{
    "statuses":[]
  }
}
```
"description":"Product not activated"}

"status":2,
"description":"Security alert"
},
"error":null
}

4.8.7.2.2  get application-info

Get information about the installed application

Command line
ermm.exe get application-info

Parameters
None

Example

call
{
  "command":"get_application_info",
  "id":1,
  "version":"1"
}

result
{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":{
      "id":"SCANNER32",
      "description":"Detection engine"}
{"version": "15117",
"date": "2017-03-20"
},
{"id": "PEGASUS32",
"description": "Rapid Response module",
"version": "9734",
"date": "2017-03-20"
},
{"id": "LOADER32",
"description": "Update module",
"version": "1009",
"date": "2016-12-05"
},
{"id": "PERSEUS32",
"description": "Antivirus and antispyware scanner module",
"version": "1513",
"date": "2017-03-06"
},
{"id": "ADVHEUR32",
"description": "Advanced heuristics module",
"version": "1176",
"date": "2017-01-16"
},
{"id": "ARCHIVER32",
"description": "Archive support module",
"version": "1261",
"date": "2017-02-22"
},
{"id": "CLEANER32",
"description": "Cleaner module",
"version": "1132",
"date": "2017-03-15"
},
{"id": "ANTISTEALTH32",
"description": "Anti-Stealth support module",
"version": "1106",
"date": "2016-10-17"}
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},
"id":"SAURON32"
4.8.7.2.3  get license-info

Get information about the license of the product

Command line

ermm.exe get license-info

Parameters

None

Example

call

{
  "command":"get_license_info",
  "id":1,
  "version":"1"
}

result

{
  "id":1,
  "result":{
    "type":"NFR",
    "description":"Rootkit detection and cleaning module",
    "version":"1006",
    "date":"2016-07-15"
  }

  {
    "id":"SSL32",
    "description":"Cryptographic protocol support module",
    "version":"1009",
    "date":"2016-12-02"
  }

  "error":null
}
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}

4.8.7.2.4  get logs

Get logs of the product

Command line

ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>{ all, virlog, warnlog, scanlog, blocked, hipslog, urlog, devctrllog } : log to retrieve</td>
</tr>
<tr>
<td>start-date</td>
<td>start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])</td>
</tr>
<tr>
<td>end-date</td>
<td>end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])</td>
</tr>
</tbody>
</table>

Example

```
call
{
  "command":"get_logs",
  "id":1,
  "version":"1",
  "params":{
    "name":"warnlog",
    "start_date":"2017-04-04 06-00-00",
    "end_date":"2017-04-04 12-00-00"
  }
}
```
```json
result
{
  "id":1,
  "result":{
    "warnlog":{
      "display_name":"Events",
      "logs":[
        {
          "Time":"2017-04-04 06-05-59",
          "Severity":"Info",
          "PluginId":"ESET Kernel",
          "Code":"Malware database was successfully updated to version 15198 (20170404)",
          "UserData":"
        },
        {
          "Time":"2017-04-04 11-12-59",
          "Severity":"Info",
          "PluginId":"ESET Kernel",
          "Code":"Malware database was successfully updated to version 15199 (20170404)",
          "UserData":"
        }
      ]
    }
  },
  "error":null
}
```

### 4.8.7.2.5 get activation-status

Get information about the last activation. Result of status can be `{ success, error }`

**Command line**

ermm.exe get activation-status

**Parameters**

None

**Example**

call
{
```
4.8.7.2.6  get scan-info

Get information about running scan.

Command line

ermm.exe get scan-info

Parameters

None

Example

call

{  
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}

result

{
  "id": 1,
  "result": {  
    "scan-info": {
      "error": null
    }
  }
}
"scans": [{
    "scan_id": 65536,
    "timestamp": 272,
    "state": "finished",
    "pause_scheduled_allowed": false,
    "pause_time_remain": 0,
    "start_time": "2017-06-20T12:20:33Z",
    "elapsed_tickcount": 328,
    "exit_code": 0,
    "progress_filename": "Operating memory",
    "progress_arch_filename": "",
    "total_object_count": 268,
    "infected_object_count": 0,
    "cleaned_object_count": 0,
    "log_timestamp": 268,
    "log_count": 0,
    "log_path": "C:\ProgramData\ESET\ESET Security\Logs\eScan\ndl31494.dat",
    "username": "test-PC\test",
    "process_id": 3616,
    "thread_id": 3992,
    "task_type": 2
  }],
  "pause_scheduled_active": false
},
"error": null

4.8.7.2.7  get configuration

Get the product configuration. Result of status may be { success, error }

Command line

ermm.exe get configuration --file C:\tmp\conf.xml --format xml

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>the path where the configuration file will be saved</td>
</tr>
</tbody>
</table>
Example

call

```json
{
    "command": "get_configuration",
    "id": 1,
    "version": "1",
    "params": {
        "format": "xml",
        "file": "C:\\tmp\\conf.xml"
    }
}
```

result

```json
{
    "id": 1,
    "result": {
        "configuration": "PD94bWwgdmVyc2lvbj0iMS4wIiBvbmx5PSIuMSIgaGVpZ2h0PSIxIiBwaG90b3Nob3AgbnVzaGVyIHRvIGZyb20gc2l0IGxheW91ciB0aGlzIG5ld25ldCB3b3JsZCBzcm9tIHN0cmluZw=="
    },
    "error": null
}
```

4.8.7.2.8 get update-status

Get information about the update. Result of status may be { success, error }

Command line

```shell
ermm.exe get update-status
```

Parameters

None

Example

call

```json
{
```

```
"command":"get_update_status",
"id":1,
"version":"1"
}

result
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}

4.8.7.2.9 start scan
Start scan with the product

Command line
ermm.exe start scan --profile "profile name" --target "path"

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile</td>
<td>Profile name of On-demand computer scan defined in product</td>
</tr>
<tr>
<td>target</td>
<td>Path to be scanned</td>
</tr>
</tbody>
</table>

Example
call
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{

4.8.7.2.10 start activation

Start activation of product

Command line

ermm.exe start activation --key "activation key" | --offline "path to offline file"

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Activation key</td>
</tr>
<tr>
<td>offline</td>
<td>Path to offline file</td>
</tr>
<tr>
<td>token</td>
<td>Activation token</td>
</tr>
</tbody>
</table>

Example

call

```json
{
    "command":"start_activation",
    "id":1,
    "version":"1",
    "params":{
        "key":"XXXX-XXXX-XXXX-XXXX-XXXX"
    }
}
```
4.8.7.2.11  start deactivation

Start deactivation of the product

Command line
ermm.exe start deactivation

Parameters
None

Example

call

{
  "command":"start_deactivation",
  "id":1,
  "version":"1"
}

result

{
  "id":1,
  "result":{
  },
  "error":null
}
4.8.7.2.12  start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line
ermm.exe start update

Parameters
None

Example

call

{  
  "command":"start_update", 
  "id":1, 
  "version":"1" 
}

result

{  
  "id":1, 
  "result":{}, 
  "error":{   
    "id":4, 
    "text":"Task already running." 
  } 
}
4.8.7.2.13  set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>the path where the configuration file will be saved</td>
</tr>
<tr>
<td>password</td>
<td>password for configuration</td>
</tr>
<tr>
<td>value</td>
<td>configuration data from the argument (encoded in base64)</td>
</tr>
</tbody>
</table>

Example

call

{
    "command":"set_configuration",
    "id":1,
    "version":"1",
    "params":{
        "format":"xml",
        "file":"C:\tmp\conf.xml",
        "password": "pass"
    }
}

result

{
    "id":1,
    "result":{
    },
    "error":null
}
5. Common Questions

This chapter covers some of the most frequently asked questions and problems encountered. Click a topic title to find out how to solve your problem:

- How to update ESET Endpoint Security
- How to activate ESET Endpoint Security
- How to use current credentials to activate a new product
- How to remove a virus from my PC
- How to allow communication for a certain application
- How to create a new task in Scheduler
- How to schedule a weekly computer scan
- How to connect my product to ESET Security Management Center
- How to configure a mirror

If your problem is not included in the help pages listed above, try searching by keyword or phrase describing your problem in the ESET Endpoint Security Help pages.

If you cannot find the solution to your problem/question in the Help pages, visit the ESET Knowledgebase where answers to common questions and issues are available.

- Best practices to protect against Filecoder (ransomware) malware
- ESET Endpoint Security and ESET Endpoint Antivirus 7 FAQ
- What addresses and ports on my third-party firewall should I open to allow full functionality for my ESET product?

If necessary, you can contact our online technical support center with your questions or problems. The link to our online contact form can be found in the Help and Support pane in the main program window.

5.1 How to update ESET Endpoint Security

Updating ESET Endpoint Security can be performed either manually or automatically. To trigger the update, click Update now in the Update section in main menu.

The default installation settings create an automatic update task which is performed on an hourly basis. To change the interval, navigate to Tools > Scheduler (for more information on Scheduler, click here).

5.2 How to activate ESET Endpoint Security

After installation is complete, you will be prompted to activate your product.

There are several methods for activating your product. Availability of a particular activation scenario in the activation window may vary depending on the country, as well as the means of distribution (ESET web page, installer type .msi or .exe, etc.).

To activate your copy of ESET Endpoint Security directly from the program, click the system tray icon and select Activate product license from the menu. You can also activate your product from the main menu under Help and support > Activate product or Protection status > Activate product.

You can use any of the following methods to activate ESET Endpoint Security:

- Enter a License Key – A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and for activation of the license.
- ESET Business Account – An account created on the ESET Business Account portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- Offline License – An automatically generated file that will be transferred to the ESET product to provide license information. If a license allows you to download an offline license file (.lf) that file can be used to perform
offline activation. The number of offline licenses will be subtracted from the total number of available licenses. For more details about generation of an offline file see the ESET Business Account Online user guide.

Click **Activate later** if your computer is a member of managed network and your administrator will perform remote activation via ESET Security Management Center. You can also use this option if you would like to activate this client at a later time.

If you have a Username and Password used for activation of older ESET products and do not know how to activate ESET Endpoint Security, **convert your legacy credentials to a License key**.

You can change your product license at any time. To do so, click **Help and support > Change license** in the main program window. You will see the public license ID used to identify your license to ESET Support. The Username under which your computer is registered is stored in the **About** section, which you can view by right-clicking the system tray icon.

---

**Note**

ESET Security Management Center can activate client computers silently using licenses made available by the administrator. For instructions to do so, see the ESET Security Management Center Online help.

---

### 5.2.1 Login to ESET Business Account

The Security Admin account is an account created on the ESET Business Account portal with your **Email address** and **Password**, which is able to see all seat authorizations. A Security Admin account allows you to manage multiple licenses. If you do not have a Security Admin account click **Create account** and you will be redirected to the ESET Business Account portal where you can register with your credentials.

If you have forgotten your password click **I forgot my password** and you will be redirected to the ESET Business Account portal. Enter your email address and click **Sign in** to confirm. After that you will obtain a message with instructions how to reset your password.

### 5.3 How to use current credentials to activate a new product

If you already have your Username and Password and would like to receive a License Key, visit the ESET Business Account portal, where you can convert your credentials to a new License Key.

### 5.4 How to remove a virus from my PC

If your computer is showing symptoms of malware infection, for example it is slower, often freezes, we recommend that you do the following:

1. In the main program window, click **Computer scan**.
2. Click **Smart scan** to begin scanning your system.
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.
4. If you want to only scan a certain part of your disk click **Custom scan** and select targets to be scanned for viruses.

For additional information please see our regularly updated ESET Knowledgebase article.
5.5 How to allow communication for a certain application

If a new connection is detected in interactive mode and if there is no matching rule, you will be prompted to allow or deny the connection. If you want ESET Endpoint Security to perform the same action every time the application attempts to establish a connection, select the Remember action (create rule) check box.

You can create new firewall rules for applications before they are detected by ESET Endpoint Security in the firewall setup window, located under Advanced setup > Firewall > Basic > Rules by clicking Edit.

Click Add to add the rule. In the General tab, enter the name, direction and communication protocol for the rule. This window allows you to define the action to be taken when the rule is applied.

Enter the path to the application's executable and the local communication port in the Local tab. Click the Remote tab to enter the remote address and port (if applicable). The newly-created rule will be applied as soon as the application tries to communicate again.

5.6 How to create a new task in Scheduler

To create a new task in Tools > Scheduler, click Add task or right-click and select Add... from the context menu. Five types of scheduled tasks are available:

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** - Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** — Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** – Performs a computer scan of files and folders on your computer.
- **Update** – Schedules an Update task by updating modules.

Since Update is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:
From the Scheduled task drop-down menu, select **Update**. Enter the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if time since last exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

### 5.7 How to schedule a weekly computer scan

To schedule a regular task, open the main program window and click **Tools > Scheduler**. Below is a short guide on how to schedule a task that will scan your local drives every week. See our [Knowledgebase article](#) for more detailed instructions.

To schedule a scan task:

1. Click **Add** in the main Scheduler screen.
2. Select **On-demand computer scan** from the drop-down menu.
3. Enter a name for the task and select **Weekly** for the task frequency.
4. Set the day and time the task will execute.
5. Select **Run the task as soon as possible** to perform the task later if the scheduled task does not run for any reason (for example, if the computer was turned off).
6. Review the summary of the scheduled task and click **Finish**.
7. From the **Targets** drop-down menu, select **Local drives**.
8. Click **Finish** to apply the task.

### 5.8 How to connect ESET Endpoint Security to ESET Security Management Center

When you have installed ESET Endpoint Security on your computer and you want to connect via ESET Security Management Center, make sure that you have also installed ESMC Agent on your client workstation. ESMC Agent is an essential part of every client solution that communicates with ESMC Server. ESET Security Management Center uses the RD Sensor tool to search for computers on the network. Every computer on your network that is detected by RD Sensor is displayed in the Web Console.

Once the Agent is deployed, you can perform remote installation of ESET security products on your client computer. The exact steps for remote installation are described in the [ESET Security Management Center User Guide](#).
5.9 How to configure a mirror

ESET Endpoint Security can be configured to store copies of detection engine update files and distribute updates to other workstations that are running ESET Endpoint Security or ESET Endpoint Antivirus.

Configuring ESET Endpoint Security as a Mirror server to provide updates via an internal HTTP server
1. Press F5 to access Advanced setup and expand Update > Profiles > Update Mirror.
2. Expand Updates and make sure the Choose automatically option under Modules updates is enabled.
3. Expand Update mirror and enable Create update mirror and Enable HTTP server.
For more information see Update mirror.

Configuring a Mirror server to provide updates via a shared network folder
1. Create a shared folder on a local or network device. This folder must be readable by all users running ESET security solutions and writable from the local SYSTEM account.
2. Activate Create update mirror under Advanced setup > Update > Profiles > Update Mirror.
3. Choose an appropriate Storage folder by clicking Clear and then Edit. Browse and select the created shared folder.

Note
If you do not want to provide module updates via internal HTTP server disengage Create update mirror.

5.10 How do I upgrade to Windows 10 with ESET Endpoint Security

Warning
We highly recommend that you upgrade to the latest version of your ESET product, then download the latest module updates, before upgrading to Windows 10. This will ensure maximum protection and preserve your program settings and license information during the upgrade to Windows 10.

Version 7.x:
Click the appropriate link below to download and install the latest version to prepare for your upgrade to Microsoft Windows 10:

Download ESET Endpoint Security 7 32-bit  Download ESET Endpoint Antivirus 7 32-bit
Download ESET Endpoint Security 7 64-bit  Download ESET Endpoint Antivirus 7 64-bit

Version 5.x:
Click the appropriate link below to download and install the latest version to prepare for your upgrade to Microsoft Windows 10:

Download ESET Endpoint Security 5 32-bit  Download ESET Endpoint Antivirus 5 32-bit
Download ESET Endpoint Security 5 64-bit  Download ESET Endpoint Antivirus 5 64-bit

Other language versions:
If you are looking for another language version of your ESET endpoint product, please visit our download page.
5.11 How to use Override mode

Users with ESET Endpoint products (version 6.5 and above) for Windows installed on their machine can use the Override feature. Override mode allows users on the client-computer level to change settings in the installed ESET product, even if there is a policy applied over these settings. Override mode can be enabled for certain AD users, or it can be password-protected. The function can not be enabled for more than four hours at once.

Warning

- Override mode can not be stopped from the ESMC Web Console once it is enabled. Override is disabled only after the time of override expires, or after it is turned off on the client itself.
- Override mode can not be assigned to an Active directory group.

To set the Override mode:

1. Navigate to Admin > Policies > New Policy.
2. In the Basic section, type in a Name and Description for this policy.
3. In the Settings section, select ESET Endpoint for Windows.
4. Click Override mode and configure rules for override mode.
5. In the Assign section, select the computer or group of computers on which this policy will be applied.
6. Review the settings in the Summary section and click Finish to apply the policy.
Example

If John has a problem with his endpoint settings blocking some important functionality or web access on his machine, the Administrator can allow John to override his existing endpoint policy and tweak the settings manually on his machine. Afterward, these new settings can be requested by ESMC so the Administrator can create a new policy out of them.

To do so, follow the steps below:

1. Navigate to Admin > Polices > New Policy.
2. Complete the Name and Description fields. In the Settings section, select ESET Endpoint for Windows.
3. Click Override mode, enable the override mode for one hour and select John as the AD user.
4. Assign the policy to John’s computer and click Finish to save the policy.
5. John has to enable the Override mode on his ESET endpoint and change the settings manually on his machine.
6. On the ESMC Web Console, navigate to Computers, select John’s computer and click Show Details.
7. In the Configuration section, click Request configuration to schedule a client task to get the configuration from the client ASAP.
8. After short time, the new configuration will appear. Click on the product which settings you want to save and then click Open Configuration.
9. You can review settings and then click Convert to policy.
10. Complete the Name and Description fields.
11. In the Settings section, you can modify the settings if needed.
12. In the Assign section, you can assign this policy to John’s computer (or others).
13. Click Finish to save the settings.
14. Do not forget to remove the override policy once it is no longer needed.
5.12 How to activate Remote monitoring and management

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems (such as those on desktops, servers and mobile devices) using a locally installed agent that can be accessed by a management service provider. ESET Endpoint Security can be managed by RMM from the version 6.6.2028.0.

By default, ESET RMM is disabled. To enable ESET RMM, press F5 to access Advanced setup, click Tools, expand ESET RMM and turn on the switch next to Enable RMM.

Working mode – Select Safe operations only if you want to enable RMM interface for safe and read only operations. Select All operations if you want to enable RMM interface for all operations.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Mode Safe operations only</th>
<th>Mode All operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get application info</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Get configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Get license info</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Get logs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Get protection status</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Get update status</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Set configuration</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Start activation</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Start scan</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Start update</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Authorization method – Set the RMM authorization method. To use authorization, select Application path from the drop-down menu, otherwise select None.
Warning
RMM should always use authorization to prevent malicious software from disabling or circumventing ESET Endpoint protection.

Application paths – Specific application which is allowed to run RMM. If you have selected Application path as an authorization method, click Edit to open the Allowed RMM application paths configuration window.

Add – Create a new allowed RMM application path. Enter the path or click the … button to select an executable.
Edit – Modify an existing allowed path. Use Edit if the location of the executable has changed to another folder.
Delete – Delete an existing allowed path.

Default ESET Endpoint Security installation contains file ermm.exe located in Endpoint application directory (default path c:\Program Files\ESET\ESET Security). The file ermm.exe exchange data with RMM Plugin, which communicates with RMM Agent, linked to a RMM Server.

- ermm.exe – command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.
- RMM Plugin is a third party application running locally on Endpoint Windows system. The plugin was designed to communicate with specific RMM Agent (e.g. Kaseya only) and with ermm.exe.
- RMM Agent is a third party application (e.g. from Kaseya) running locally on Endpoint Windows system. Agent communicates with RMM Plugin and with RMM Server.

Note
RMM Server is running as a service on a third party server. Supported RMM systems are by Kaseya, Labtech, Autotask, Max Focus and Solarwinds N-able.
5.13 How to block the download of specific file types from the Internet

If you do not want to allow downloading of specific file types (e.g., .exe, .pdf, or .zip) from the internet, use URL Address management with a combination of wildcards. Press the F5 key to access Advanced setup. Click Web and Email > Web access protection and expand URL Address Management. Click Edit next to Address list.

In the Address list window, select List of blocked addresses and click Edit, or click Add to create a new list. A new window opens. If you are creating a new list, select Blocked from the Address list type drop-down menu and name the list. If you want to be notified when accessing a file type from the current list, enable the Notify when applying slider bar. Select the Logging severity from the drop-down menu. Remote Administrator can collect records with Warning verbosity.

Click Add to enter a mask that specifies file types you want to block from downloading. Enter the full URL if you want to block the download of a specific file from a specific website, for example, http://example.com/file.exe. You can use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters. For example, the mask */*.zip blocks all zip compressed files to be downloaded.