

ESET Endpoint Antivirus

Посібник користувача

[Натисніть тут щоб відкрити версію цього документа](#)

© ESET, spol. s r.o., 2024.

ESET Endpoint Antivirus розроблено компанією ESET, spol. s r.o.

Докладніше див. на сайті <https://www.eset.com>.

Усі права захищено. Без письмового дозволу автора жодну частину цього документа не можна відтворювати, зберігати в системі автоматичного пошуку або передавати в будь-якій формі чи будь-яким способом (електронним, механічним, фотокопіюванням, записуванням, скануванням тощо).

ESET, spol. s r.o. зберігає право вносити зміни до будь-якого описаного програмного забезпечення без попередження.

Служба технічної підтримки: <https://support.eset.com>

REV. 12.04.2024

1 ESET Endpoint Antivirus 9	1
1.1 Нові функції в цій версії?	2
1.2 Системні вимоги	3
1.2 Підтримувані мови	4
1.3 Запобігання зараженню комп'ютера	5
1.4 Довідкові сторінки	7
2 Документація для робочих станцій, якими керують віддалено	8
2.1 Загальний опис ESET PROTECT	9
2.2 Загальний опис ESET PROTECT Cloud	10
2.3 Параметри, захищені паролем	11
2.4 Що таке політики?	12
2.4 Об'єднання політик	13
2.5 Принцип дії прапорців	13
3 Самостійне використання ESET Endpoint Antivirus	14
3.1 Методи інсталяції	15
3.1 Інсталяція з використанням ESET AV Remover	15
3.1 ESET AV Remover	16
3.1 Помилка видалення програми за допомогою ESET AV Remover	18
3.1 Інсталяція (.exe)	19
3.1 Змінити папку інсталяції (.exe)	20
3.1 Інсталяція (.msi)	21
3.1 Розширена інсталяція (.msi)	23
3.1 Мінімальна інсталяція модулів	24
3.1 Інсталяція з використання командного рядка	25
3.1 Розгортання за допомогою об'єкта групової політики (GPO) або SCCM	30
3.1 Оновлення до останньої версії	32
3.1 Оновлення безпеки й стабільності	33
3.1 Поширені проблеми під час інсталяції	33
3.1 Помилка активації	33
3.2 Активація продукту	34
3.3 Сканування комп'ютера	34
3.4 Посібник для початківців	34
3.4 Інтерфейс користувача	35
3.4 Параметри оновлення	38
4 Робота з ESET Endpoint Antivirus	39
4.1 Комп'ютер	42
4.1 Ядро виявлення	43
4.1 Розширені параметри ядра виявлення	48
4.1 Дії в разі виявлення загрози	48
4.1 Захист файлової системи в режимі реального часу	51
4.1 Перевірка захисту в режимі реального часу	52
4.1 Можливі причини для змінення конфігурації захисту в режимі реального часу	53
4.1 Необхідні дії, коли не працює захист у режимі реального часу	53
4.1 Сканування комп'ютера	54
4.1 Модуль запуску вибіркового сканування	56
4.1 Хід сканування	58
4.1 Журнал сканування комп'ютера	59
4.1 Сканування шкідливого програмного забезпечення	59
4.1 Сканування в неактивному стані	60
4.1 Профілі сканування	60

4.1 Об'єкти сканування	61
4.1 Додаткові параметри сканування	62
4.1 Контроль пристроїв	62
4.1 Редактор правил контролю пристроїв	63
4.1 Виявлені пристрої	64
4.1 Групи пристроїв	65
4.1 Додавання правил контролю пристроїв	66
4.1 Система виявлення вторгнень (HIPS)	68
4.1 Інтерактивне вікно HIPS	71
4.1 Виявлено потенційно зловмисну програму, яка вимагає викуп	72
4.1 Керування правилами HIPS	72
4.1 Параметри правила HIPS	73
4.1 Додаткові параметри HIPS	76
4.1 Драйвери, які дозволено завжди завантажувати	76
4.1 Режим презентації	77
4.1 Сканування під час запуску	77
4.1 Автоматична перевірка файлів під час запуску системи	78
4.1 Захист документів	78
4.1 Виключення	79
4.1 Виключення в роботі	79
4.1 Додавання або зміна виключення в роботі	80
4.1 Формат виключення шляху	82
4.1 Виключення об'єктів виявлення	83
4.1 Додавання або зміна виключення об'єкта виявлення	86
4.1 Майстер створення виключень виявлених об'єктів	87
4.1 Виключення (7.1 і попередніх версій)	88
4.1 Виключення процесів	88
4.1 Додавання або зміна виключень процесів	89
4.1 Виключення HIPS	90
4.1 Параметри ThreatSense	90
4.1 Рівні очистки	93
4.1 Список розширень файлів, виключених із перевірки	94
4.1 Додаткові параметри ThreatSense	94
4.2 Мережа	95
4.2 Захист від мережових атак	96
4.2 Захист від атак повним перебором	96
4.2 Правила	96
4.2 Виключення	99
4.2 Розширені параметри фільтрації	99
4.2 Правила IDS	101
4.2 Заблоковано можливу загрозу	102
4.2 Майстер усунення помилок	103
4.2 Відомі мережі	103
4.2 Редактор відомих мереж	104
4.2 Автентифікація мережі – конфігурація сервера	106
4.2 Тимчасовий чорний список IP-адрес	107
4.2 Налаштування зон	107
4.2 Зони брандмауера	108
4.3 Інтернет і електронна пошта	108
4.3 Фільтрація протоколів	109
4.3 Виключені програми	110

4.3 Виключені IP-адреси	111
4.3 SSL/TLS	112
4.3 Сертифікати	113
4.3 Зашифрований мережевий трафік	114
4.3 Список відомих сертифікатів	115
4.3 Список програм, до яких застосовуються фільтри SSL/TLS	115
4.3 Захист поштового клієнта	116
4.3 Протоколи електронної пошти	118
4.3 Теги електронної пошти	119
4.3 Інтеграція з поштовими клієнтами	120
4.3 Панель інструментів Microsoft Outlook	120
4.3 Панель інструментів Outlook Express і Windows Mail	120
4.3 Діалогове вікно підтвердження	121
4.3 Повторне сканування повідомлень	121
4.3 Захист доступу до Інтернету	121
4.3 Розширене налаштування функції захисту доступу до Інтернету	124
4.3 Веб-протоколи	124
4.3 Управління URL-адресами	125
4.3 Список URL-адрес	126
4.3 Створення списку	127
4.3 Додавання маски URL-адреси	128
4.3 Захист від фішинг-атак	129
4.4 Оновлення програми	130
4.4 Параметри оновлення	134
4.4 Відкочування оновлення	137
4.4 Оновлення продукту	139
4.4 Параметри підключення	140
4.4 Дзеркало оновлень	142
4.4 HTTP-сервер і SSL для дзеркала	143
4.4 Оновлення із дзеркала	144
4.4 Виправлення неполадок під час оновлення із дзеркала	146
4.4 Створення завдань оновлення	146
4.5 Інструменти	147
4.5 Журнали	148
4.5 Фільтрація журналу	150
4.5 Налаштування ведення журналу	151
4.5 Журнали аудиту	152
4.5 Розклад	154
4.5 ESET SysInspector	156
4.5 Захист із використанням хмари	157
4.5 Фільтр виключень для хмарного захисту	160
4.5 Запущені процеси	161
4.5 Звіт про безпеку	162
4.5 ESET SysRescue Live	164
4.5 Відправлення зразків на аналіз	164
4.5 Вибір зразка для аналізу: підозрілий файл	165
4.5 Вибір зразка для аналізу: підозрілий сайт	165
4.5 Вибір зразка для аналізу: помилково розпізнаний файл	166
4.5 Вибір зразка для аналізу: помилково розпізнаний сайт	166
4.5 Вибір зразка для аналізу: інше	166
4.5 Карантин	166

4.5 Параметри проксі-сервера	168
4.5 Часові проміжки	170
4.5 Оновлення Microsoft Windows	171
4.5 Перевірка періоду ліцензування	172
4.6 Інтерфейс користувача	172
4.6 Елементи інтерфейсу користувача	172
4.6 Параметри доступу	174
4.6 Пароль для розділу	175
4.6 Піктограма в системному треї	176
4.6 Контекстне меню	177
4.6 Довідка та підтримка	178
4.6 Про продукт ESET Endpoint Antivirus	178
4.6 Надсилання даних про конфігурацію системи	179
4.6 Технічна підтримка	180
4.7 Сповіщення	180
4.7 Статуси програми	180
4.7 Сповіщення на робочому столі	181
4.7 Діалогове вікно: сповіщення на робочому столі	182
4.7 Налаштування сповіщень	182
4.7 Інтерактивні сповіщення	183
4.7 Список інтерактивних сповіщень	184
4.7 Повідомлення про підтвердження	185
4.7 Помилка через конфлікт додаткових параметрів	187
4.7 Знімні носії	187
4.7 Необхідно перезавантажити комп'ютер	188
4.7 Рекомендовано перезавантажити комп'ютер	189
4.7 Пересилання	190
4.7 Менеджер профілів	193
4.7 Сполучення клавіш	194
4.7 Діагностичні дані	194
4.7 Сканер командного рядку	196
4.7 ESET CMD	198
4.7 Виявлення неактивного стану	201
4.7 Імпорт і експорт параметрів	201
4.7 Відновлення всіх параметрів за замовчуванням	202
4.7 Відновлення всіх параметрів у поточному розділі	203
4.7 Помилка під час збереження конфігурації	203
4.7 Віддалений моніторинг і керування	203
4.7 Командний рядок ERMM	204
4.7 Список команд ERMM JSON	206
4.7 отримати стан захисту	206
4.7 отримати інформацію про програму	207
4.7 отримати інформацію про ліцензію	210
4.7 отримати журнали	210
4.7 отримати стан активації	211
4.7 отримати інформацію про сканування	212
4.7 отримати конфігурацію	213
4.7 отримати стан оновлення	214
4.7 запустити сканування	215
4.7 запустити активацію	215
4.7 запустити деактивацію	216

4.7 запуснути оновлення	217
4.7 застосувати конфігурацію	217
5 Поширені запитання	218
5.1 Запитання й відповіді щодо автоматичних оновлень	219
5.2 Оновлення ESET Endpoint Antivirus	222
5.3 Активація ESET Endpoint Antivirus	222
5.3 Введення ліцензійного ключа під час активації	223
5.3 Вхід до ESET Business Account	224
5.3 Використання попередніх облікових даних ліцензії для активації новішого продукту ESET Endpoint	224
5.4 Видалення вірусу з ПК	224
5.5 Створення нового запланованого завдання	224
5.5 Додавання до розкладу завдання щотижневого сканування комп'ютера	225
5.6 Підключення ESET Endpoint Antivirus до ESET PROTECT	226
5.6 Режим заміщення	226
5.6 Застосування рекомендованої політики для ESET Endpoint Antivirus	228
5.7 Налаштування дзеркала	231
5.8 Оновлення до ОС Windows 10 за допомогою ESET Endpoint Antivirus	231
5.9 Активація віддаленого моніторингу та керування	232
5.10 Блокування завантаження певних типів файлів з Інтернету	235
5.11 Згортання інтерфейсу користувача ESET Endpoint Antivirus	235
6 Ліцензійна угода з кінцевим користувачем	236
7 Політика конфіденційності	244

ESET Endpoint Antivirus 9

У продукті ESET Endpoint Antivirus 9 втілено новий підхід до розробки повністю інтегрованої системи безпеки комп'ютера. Робота останньої версії підсистеми сканування ESET LiveGrid® ґрунтується на принципах швидкості й точності для захисту вашого комп'ютера. Таким чином, кожен користувач отримує інтелектуальну систему, яка гарантує постійний захист від атак і зловмисного програмного забезпечення, що загрожують комп'ютеру.

ESET Endpoint Antivirus 9 — повноцінне рішення безпеки, яке стало результатом тривалої роботи, спрямованої на поєднання максимального захисту та використання мінімуму системних ресурсів. Передові технології на базі штучного інтелекту здатні проактивно блокувати проникнення вірусів, шпигунських і троянських програм, черв'яків, нав'язливої реклами, руткітів й інших атак з Інтернету, не зменшуючи продуктивності системи та не порушуючи роботу комп'ютера.

ESET Endpoint Antivirus 9 насамперед призначено для робочих станцій, які працюють у середовищі малих фірм.

Щоб вам було легше орієнтуватися в наданій інформації розділу [Самостійне використання ESET Endpoint Antivirus](#), теми довідки, зокрема [Завантаження](#), [Інсталяція](#) й [Активация](#), розділено на кілька розділів і підрозділів.

[Використання ESET Endpoint Antivirus і ESET PROTECT](#) у корпоративному середовищі дає змогу легко керувати будь-якою кількістю робочих станцій клієнтів, застосовувати політики та правила, стежити за виявленими об'єктами та віддалено налаштовувати клієнти з будь-якого комп'ютера в мережі.

У розділі [Поширені запитання](#) розглядаються питання та проблеми, які найчастіше виникають у користувачів.

Функції та переваги

Удосконалений інтерфейс користувача	У цій версії інтерфейс користувача було значно змінено та спрощено на основі результатів тестування зручності в користуванні. Усі формулювання в елементах графічного інтерфейсу та сповіщень ретельно відредаговано, а сам інтерфейс тепер підтримує мови із записом справа наліво, зокрема арабську й іврит. Онлайн-довідку тепер інтегровано в програму ESET Endpoint Antivirus. Її вміст постійно оновлюється.
Антивірус та антишпигун	Завчасне виявлення та видалення більшості зареєстрованих і невідомих вірусів, черв'яків, троянських програм і руткітів. Технологія розширеної евристики дає змогу визначати раніше не відомі шкідливі програми, гарантуючи захист від нових загроз і їх завчасне знешкодження. Захист доступу до Інтернету та Захист від фішингу здійснюється шляхом контролю зв'язків між веб-браузерами й віддаленими серверами (включно з протоколом SSL). Захист поштового клієнта забезпечує керування поштовими комунікаціями через протоколи POP3(S) та IMAP(S).

Регулярні оновлення	Регулярне оновлення обробника виявлення (попередня назва – "вірусна база даних") і модулів програми – найкращий спосіб гарантувати максимальний захист комп'ютера.
ESET LiveGrid® (репутація у хмарі)	Відстежуйте репутацію запущених процесів і файлів безпосередньо в ESET Endpoint Antivirus.
Віддалене керування	ESET PROTECT дозволяє керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях, які працюють у мережі, з єдиного центру. Веб-консоль ESET PROTECT (веб-консоль ESET PROTECT) дозволяє виконувати такі операції: розгортати рішення ESET, керувати завданнями, застосовувати політики безпеки, відстежувати стан системи й швидко реагувати на проблеми або загрози на віддалених комп'ютерах.
Захист від мережевих атак	Аналізує вміст мережевого трафіку й захищає від мережевих атак. Увесь трафік, який вважатиметься шкідливим, буде заблоковано.
Веб-контроль (тільки в ESET Endpoint Security)	Веб-контроль дає змогу блокувати веб-сторінки з потенційно образливими матеріалами. Крім того, керівники підприємств або системні адміністратори можуть заборонити доступ до певних попередньо визначених категорій (більше 27) і підкатегорій (більше 140) веб-сайтів.

Нові функції в цій версії?

Вийшов ESET Endpoint Antivirus версії 9, яка [доступна для завантаження](#).

Автоматичні оновлення

- гарантує, що ви завжди використовуєте найновішою версію продукту;
- [інтелектуальне рішення](#) для зменшення обслуговування ESET Endpoint Antivirus до необхідного мінімуму;
- увімкнено за замовчуванням і з використанням оновлення компонентів мікропрограми;
- не виконує повторну інсталяцію продукту зі всіма недоліками (видалення з реєстру системи під час виконання процесу, перенесення конфігурації);
- завантажує менше даних (різниці оновлення);
- має просте нагадування, або користувач може просто повністю приховати його; сумісний із керованими мережами;

Зміни у відповідній ліцензійній угоді з кінцевим користувачем

- нова ліцензійна угода з кінцевим користувачем презентується незалежно від процесу інсталяції з використанням інформаційного елемента на консолі або в інтерфейсі користувача ESET Endpoint Antivirus;
- спрощує процес автоматичного оновлення продукту й покращує роботу користувачів, оскільки більше не потрібно приймати ліцензійну угоду з кінцевим користувачем під час кожного оновлення продукту ESET до новішої версії.

Власна збірка ARM64

- у версії 9 доступна для вибору збірка ARM64.

У цьому випуску виправлена низка помилок і покращена робота.

Більш докладні відомості щодо нових функцій ESET Endpoint Antivirus, а також відповідні знімки екрана див. в цій статті бази знань ESET:

- [Нове в ESET Endpoint Antivirus 9](#)

Системні вимоги

Для нормальної роботи ESET Endpoint Antivirus система має відповідати наведеним нижче вимогам до апаратного та програмного забезпечення.


Підтримувані процесори


Процесор Intel або AMD, 32-розрядний (x86) із набором інструкцій SSE2 або 64-розрядний (x64), 1 ГБ або вище
процесор на базі ARM64, 1 ГГц або більше

Операційні системи

Microsoft® Windows® 11

Microsoft® Windows® 10


 Детальний список підтримуваних версій Microsoft® Windows® 10 у Microsoft® Windows® 11 див. в розділі [Windows Operating system support policy](#) (Політика підтримки операційної системи Windows).

 Щоб інсталювати або оновити продукти ESET, випущені з липня 2023 року, у всіх операційних системах Windows потрібно інсталювати модуль, що підтримує підписування коду Azure. [Додаткова інформація.](#)

Microsoft® Windows® 8.1


Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 з останніми оновленнями Windows (принаймні [KB4474419](#) і [KB4490628](#))

 ESET Endpoint Antivirus 9.1 — остання версія, яка підтримує Windows 7 і Windows 8.1. [Додаткова інформація.](#)

Windows XP та Windows Vista більше [не підтримуються](#).

 Завжди вчасно оновлюйте операційну систему.

 Інсталятор ESET Endpoint Antivirus, створений у ESET PROTECT 8.1 і новіших версій, підтримує Windows 10 Enterprise for Virtual Desktops і режим кількох сеансів у Windows 10.

Інше

- Відповідність усім системним вимогам, пов'язаним з операційною системою й іншим програмним забезпеченням, інстальованим на комп'ютері
- 0,3 ГБ вільної системної пам'яті (див. примітку 1)
- 1 ГБ вільного місця на диску (див. примітку 2)
- Мінімальна роздільна здатність екрана: 1024x768
- Підключення до джерела оновлень продукту через Інтернет або локальну мережу (див. примітку 3)
- Якщо дві антивірусні програми одночасно виконуються на одному пристрої, це спричиняє неминучі системні конфлікти ресурсів, наприклад уповільнення роботи системи аж до неможливості роботи з нею

Продукт можна інстальувати й запускати в системах, які не відповідають цим вимогам, однак рекомендується попередньо протестувати зручність використання продукту, беручи до уваги вимоги щодо продуктивності.

- (1).** Продукт може використовувати більше пам'яті, якщо в іншому разі вона не використовуватиметься на сильно інфікованому комп'ютері, а також коли у продукт імпортуються дуже великі списки даних (наприклад, білі списки URL-адрес).
- (2).** Місце на диску необхідне для завантаження інстальатора, інсталяції продукту та збереження копії інсталяційного пакета в даних програми, а також для збереження резервних копій оновлень продукту для підтримки функції відкочування. Продукт може використовувати більше місця на диску залежно від вибраних параметрів (наприклад, коли створюються резервні копії нових версій продукту, зберігаються дампи пам'яті або дуже велика кількість записів журналу), а також якщо комп'ютер інфіковано (зокрема через функцію карантину). Рекомендується залишати на диску достатньо вільного місця для підтримки оновлень операційної системи, а також для оновлень продуктів ESET.
- (3).** Продукт можна оновлювати вручну за допомогою знімного носія (не рекомендовано).

Підтримувані мови

Нижче наведено доступні мови для інсталяції й завантаження ESET Endpoint Antivirus.

Мова	Код мови	Код мови
Англійська (США)	en-US	1033
Арабська (Єгипет)	ar-EG	3073
Болгарська	bg-BG	1026
Китайська (спрощене письмо)	zh-CN	2052
Китайська (традиційне письмо)	zh-TW	1028
Хорватська	hr-HR	1050
Чеська	cs-CZ	1029
Естонська	et-EE	1061
Фінська	fi-FI	1035
Французька (Франція)	fr-FR	1036
Французька (Канада)	fr-CA	3084
Німецька (Німеччина)	de-DE	1031

Мова	Код мови	Код мови
Грецька	el-GR	1032
*Іврит	he-IL	1037
Угорська	hu-HU	1038
*Індонезійська	id-ID	1057
Італійська	it-IT	1040
Японська	ja-JP	1041
Казахська	kk-KZ	1087
Корейський	ko-KR	1042
*Латвійська	lv-LV	1062
Литовська	lt-LT	1063
Nederlands	nl-NL	1043
Норвезька	nb-NO	1044
Польська	pl-PL	1045
Португальська (Бразилія)	pt-BR	1046
Румунська	ro-RO	1048
Російська	ru-RU	1049
Іспанська (Чилі)	es-CL	13322
Іспанська (Іспанія)	es-ES	3082
Шведська (Швеція)	sv-SE	1053
Словацька	sk-SK	1051
Словенська	sl-SI	1060
Тайська	th-TH	1054
Турецька	tr-TR	1055
Українська (Україна)	uk-UA	1058
*В'єтнамська	vi-VN	1066

* Цією мовою доступний лише продукт ESET Endpoint Antivirus, а не онлайн-посібник користувача (виконуватиметься переспрямування на версію англійською).

Змінити мову цього онлайн-посібника можна в полі вибору мови (у правому верхньому куті).

Запобігання зараженню комп'ютера

Коли ви працюєте за комп'ютером (а особливо переглядаєте веб-сторінки в Інтернеті), пам'ятайте, що жодна антивірусна система у світі не зможе повністю усунути ризик, який несуть [інфіковані об'єкти](#) й [віддалені атаки](#). Щоб забезпечити максимальний захист і зручність під час роботи, важливо правильно користуватися рішеннями захисту від вірусів і дотримуватися кількох корисних правил.

Регулярне оновлення

Згідно зі статистичними даними від ESET LiveGrid® тисячі нових унікальних шкідливих кодів

створюються щодня. Їх мета – обійти наявні захисні бар'єри та принести прибуток своїм авторам. Щоб якомога краще захистити наших клієнтів, спеціалісти антивірусної лабораторії ESET щоденно аналізують ці загрози, а потім розробляють і випускають оновлення на основі отриманих даних. Максимальний рівень ефективності таких оновлень може гарантувати лише їхня належна конфігурація в системі. Щоб отримати додаткові відомості про спосіб налаштування оновлень, див. розділ [Параметри оновлення](#).

Завантаження оновлень для операційних систем та інших програм

Як правило, автори шкідливих програм використовують уразливість різних систем для збільшення дієвості поширення шкідливого коду. Тому компанії, що випускають програмне забезпечення, пильно слідкують за появою нових слабких місць у своїх програмах і регулярно випускають оновлення безпеки, які усувають потенційні загрози. Важливо завантажувати ці оновлення одразу після їх випуску. Microsoft Windows і веб-браузери, такі як Internet Explorer, – це дві програми, оновлення для яких випускаються на постійній основі.

Резервне копіювання важливих даних

Зловмисники, які створюють шкідливі програми, не переймаються потребами користувачів, а робота таких програм часто призводить до повної непрацездатності операційної системи та втрати важливих даних. Важливо регулярно створювати резервні копії важливих і конфіденційних даних на зовнішні носії, наприклад DVD- або зовнішній жорсткий диск. Так буде значно легше та швидше відновити дані у випадку збою системи.

Регулярне сканування комп'ютера на наявність вірусів

Модуль захисту файлової системи в режимі реального часу виявляє відомі й нові віруси, черв'яки, троянські програми та руткити. Тож під час кожного відкриття або переходу до файлу виконується його перевірка на наявність шкідливого коду. Рекомендується щонайменше раз на місяць виконувати повне сканування комп'ютера, оскільки шкідливі програми постійно змінюються, а обробник виявлення оновлюється кожного дня.

Дотримання основних правил безпеки

Будьте обережні – це найкорисніше й найефективніше з усіх правил. На сьогодні для виконання та поширення багатьох загроз потрібне втручання користувача. Будьте обережні, відкриваючи нові файли: це заощадить вам багато часу та зусиль, які інакше довелося б витратити на усунення проникнень. Нижче наведено деякі корисні правила:

- Не відвідуйте підозрілі веб-сайти з багатьма спливаючими вікнами та рекламою.
- Будьте обережні під час інсталяції безкоштовних програм, пакетів кодеків тощо. Користуйтеся тільки безпечними програмами й відвідуйте лише перевірені веб-сайти.
- Будьте обережні під час відкривання вкладених файлів електронних листів, зокрема в масово розісланих повідомленнях і повідомленнях від невідомих відправників.
- Не користуйтеся обліковим записом із правами адміністратора для повсякденної роботи на комп'ютері.

Довідкові сторінки

Ласкаво просимо до довідки ESET Endpoint Antivirus. Наведена тут інформація допоможе краще ознайомитися з продуктом і зробити роботу з комп'ютером безпечнішою.

Початок роботи

Перш ніж розпочати роботу з ESET Endpoint Antivirus, зверніть увагу, що наш продукт може застосовуватися [користувачами, які здійснили підключення через ESET PROTECT](#) або [за допомогою інших засобів](#). Ми також рекомендуємо докладніше ознайомитися з різними [типами виявлених об'єктів](#) і [віддалених атак](#), які можуть виникати під час використання комп'ютера.

Див. [нові функції](#), щоб дізнатися про функції, додані до цієї версії ESET Endpoint Antivirus. Ми також підготували посібник, який допоможе вам налаштувати основні параметри ESET Endpoint Antivirus.

Принципи використання довідкових сторінок ESET Endpoint Antivirus

Щоб вам було легше орієнтуватися в наданій інформації, теми довідки розділено на кілька розділів і підрозділів. Необхідну інформацію можна знайти, переглянувши структуру сторінок довідки.

Щоб дізнатися більше про будь-яке вікно програми, натисніть клавішу **F1**. Відкриється сторінка довідки, яка відноситься до поточного вікна.

Пошук на сторінках довідки можна здійснювати за допомогою ключових слів або шляхом введення слів і фраз. Різниця між цими двома способами полягає в тому, що ключове слово може бути логічно пов'язане зі сторінками довідки, які не містять цього слова в тексті. Пошук за допомогою слів і фраз виконується у вмісті сторінок, відображаючи лише ті, які містять пошукове слово або фразу.

Щоб забезпечити узгодженість і уникнути плутанини, у цьому посібнику використовується термінологія на основі назв параметрів ESET Endpoint Antivirus. Щоб виділити важливі теми, ми також використовуємо стандартні набори символів.



Це лише коротке зауваження. Примітку можна пропустити, проте в ній зазначається цінна інформація, як-от про спеціальні функції або посилання на пов'язані теми.



Це повідомлення, на яке потрібно обов'язково звернути увагу. Зазвичай у ньому вказується некритична, але важлива інформація.



Це інформація, на яку потрібно звернути особливу увагу. Її розміщено для того, щоб застерегти користувача від потенційно небезпечних помилок. Уважно ознайомлюйтеся з попередженнями, оскільки в них подається інформація про надзвичайно важливі параметри системи або дії чи налаштування, пов'язані з ризиком.



Цей приклад використання допоможе зрозуміти, як можна застосовувати певну функцію чи опцію.

Позначення	Значення
Жирний текст	Назви елементів інтерфейсу, наприклад полів і кнопок опцій.
Текст курсивом	Поля, які користувач має заповнити даними. Наприклад, назва файлу або шлях означають, що необхідно ввести фактичну назву файлу або шлях.
Courier New	Зразки кодів і команд.
Гіперпосилання	Елемент для швидкого й легкого доступу до перехресних посилань і зовнішніх розташувань у мережі. Гіперпосилання виділені синім кольором і можуть бути підкреслені.
%ProgramFiles%	Системний каталог Windows, у якому зберігаються встановлені програми.

Інтерактивна довідка – основне джерело довідкової інформації. Найновіша версія інтерактивної довідки відображатиметься автоматично, якщо під час роботи у вас буде доступ до мережі.

Документація для робочих станцій, якими керують віддалено

На клієнтських робочих станціях, серверах і мобільних пристроях, які працюють у мережі, можна віддалено з єдиного центру керувати продуктами ESET для бізнесу, а також програмою ESET Endpoint Antivirus. Системні адміністратори, які керують більше ніж 10 клієнтськими робочими станціями, можуть розгорнути один з інструментів віддаленого керування ESET для розгортання рішень ESET, керування завданнями, примусового застосування [політик безпеки](#), відстежування статусу системи й швидкого реагування на проблеми чи загрози на віддалених комп'ютерах з єдиного центру.

Інструменти віддаленого керування ESET

Продуктом ESET Endpoint Antivirus можна віддалено керувати за допомогою ESET PROTECT або ESET Cloud Administrator.

- [Загальний опис ESET PROTECT](#)
- [Загальний опис ESET PROTECT Cloud](#)

Сторонні інструменти віддаленого керування

- [Віддалений моніторинг і керування \(RMM\)](#)

Рекомендації

- [Підключіть усі робочі станції з ESET Endpoint Antivirus до ESET PROTECT](#)
- Захистіть [додаткові параметри](#) на підключених клієнтських комп'ютерах, щоб унеможливити їх несанкціоновану зміну
- Застосуйте [рекомендовану політику](#) для примусового використання доступних функцій безпеки
- [Мінімізуйте інтерфейс користувача](#) , щоб зменшити або обмежити взаємодію користувача з ESET Endpoint Antivirus

Практичні керівництва

- [Режим заміщення](#)
- [Розгортання ESET Endpoint Antivirus за допомогою інструментів GPO або SCCM](#)

Загальний опис ESET PROTECT

ESET PROTECT дозволяє керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях, які працюють у мережі, з єдиного центру.

ESET PROTECT Web Console дозволяє розгортати рішення ESET, керувати завданнями, примусово застосовувати політики безпеки, відстежувати статус системи й швидко реагувати на проблеми або виявлені об'єкти на віддалених комп'ютерах. Докладніше див. в темах [Огляд архітектури й елементів інфраструктури ESET PROTECT](#), [Початок роботи з ESET PROTECT Web Console](#) і [Підтримувані середовища для підготовки робочих станцій](#).

До складу ESET PROTECT входять такі компоненти:

- [Сервер ESET PROTECT](#). Сервер ESET PROTECT можна інсталювати на серверах Windows, так само як і на серверах Linux; він також надається як віртуальний пристрій. Цей сервер керує обміном даними з агентами, а також збирає та зберігає дані програми в базі даних.
- [Веб-консоль ESET PROTECT](#). Веб-консоль ESET PROTECT є основним інтерфейсом, який дозволяє керувати клієнтськими комп'ютерами у вашому середовищі. У цій консолі відображається стан клієнтів у вашій мережі; вона дозволяє вам розгорнути рішення ESET на некеровані комп'ютери віддалено. Після інсталяції сервера ESET PROTECT веб-консоль можна відкрити у веб-браузері. Якщо ваш веб-сервер налаштовано таким чином, що він доступний через Інтернет, ESET PROTECT можна використовувати в будь-якому місці та (або) на будь-якому пристрої, на якому є підключення до Інтернету.
- [ESET Management Agent](#): ESET Management Agent забезпечує обмін даними між ESET PROTECT Server і клієнтськими комп'ютерами. Для встановлення зв'язку між комп'ютером і ESET PROTECT Server агент має бути інсталюваний на клієнтському комп'ютері. Оскільки ESET Management Agent розміщується на клієнтському комп'ютері, і він може зберігати декілька сценаріїв безпеки, його використання значно зменшує час реагування на нові виявлені об'єкти. На веб-консолі ESET PROTECT Web Console можна [розгорнути ESET Management Agent](#) на некерованих комп'ютерах, визначених Active Directory або ESET [RD Sensor](#). За потреби можна також [уручну інсталювати ESET Management Agent](#) на клієнтських комп'ютерах.
- [ESET Rogue Detection Sensor](#). ESET Rogue Detection (RD) Sensor виявляє у вашій мережі комп'ютери, які ще не контролюються, та надсилає їх дані на сервер ESET PROTECT. Це дозволяє вам легко додавати нові клієнтські комп'ютери в безпечну мережу. RD Sensor не надсилає однакову інформацію двічі, оскільки пам'ятає виявлені комп'ютери.
- [Проксі-сервер HTTP Apache](#). Служба, яку можна використовувати в комбінації з ESET PROTECT для:
 - Розповсюдження оновлень на клієнтські комп'ютери й інсталяції пакетів на агент ESET Management.
 - Переспрямування обміну даними з агентами ESET Management Agent на ESET PROTECT Server.
- [Mobile Device Connector](#). Цей компонент робить можливим керування мобільними пристроями за допомогою ESET PROTECT, дозволяючи керувати мобільними пристроями

(Android та iOS) і адмініструвати ESET Endpoint Security for Android.

- [Віртуальний притрій ESET PROTECT](#). Віртуальний пристрій ESET PROTECT призначений для користувачів, яким потрібно запускати ESET PROTECT у віртуалізованому середовищі.
- [ESET PROTECT Virtual Agent Host](#). Компонент ESET PROTECT віртуалізує об'єкти агента, дозволяючи керувати віртуальними машинами, на яких немає агента. Це рішення забезпечує автоматизацію, динамічне використання груп і рівень керування завданнями, ідентичний тому, який забезпечує агент ESET Management на фізичних комп'ютерах. Віртуальний агент збирає інформацію з віртуальних машин і надсилає її на сервер ESET PROTECT.
- [Інструмент "Дзеркало"](#): Цей інструмент потрібний для автономного оновлення модулів. Якщо на клієнтських комп'ютерах відсутнє підключення до Інтернету, інструмент "Дзеркало" дозволяє завантажити файли оновлення з серверів оновлення ESET і зберігати їх локально.
- [ESET Remote Deployment Tool](#). Цей інструмент дозволяє розгорнути комплексні пакети, створені у веб-консолі <%PRODUCT%>. Він забезпечує зручний спосіб розповсюдження агента ESET Management з продуктом ESET на комп'ютери в мережі.
- [ESET Business Account](#). Новий портал ліцензування для корпоративних продуктів ESET дозволяє керувати ліцензіями. Інструкції з активації вашого продукту див. у розділі [ESET Business Account](#) цього документа. Більш докладну інформацію щодо використання ESET Business Account див. у документі [Керівництво користувача ESET Business Account](#). Якщо ви вже маєте ім'я користувача і пароль від ESET, які вам потрібно перетворити в ліцензійний ключ, див. розділ [Перетворення облікових даних застарілої ліцензії](#).
- [ESET Inspect](#). Всеохоплююча система виявлення кінцевих точок і реагування, яка включає в себе такі функції, як виявлення інцидентів, керування інцидентами та реагування на них, збір даних, виявлення індикаторів компрометації, виявлення аномальної активності, виявлення поведінки і порушення політик.

Веб-консоль ESET PROTECT дозволяє розгортати рішення ESET, керувати задачами, примусово застосовувати [політики безпеки](#), відстежувати статус системи й швидко реагувати на проблеми чи загрози на віддалених комп'ютерах.

i Більш докладну інформацію див. в [онлайн посібнику користувача ESET PROTECT](#).

Загальний опис ESET PROTECT Cloud

ESET PROTECT Cloud дозволяє керувати продуктами ESET на робочих станціях і серверах, які працюють у мережі, з єдиного центру, нівелюючи потребу в фізичних або віртуальних серверах, таких як ESET PROTECT. Веб-консоль ESET PROTECT Cloud дозволяє виконувати такі операції: розгортати рішення ESET, керувати завданнями, застосовувати політики безпеки, відстежувати стан системи та швидко реагувати на проблеми або загрози на віддалених комп'ютерах.

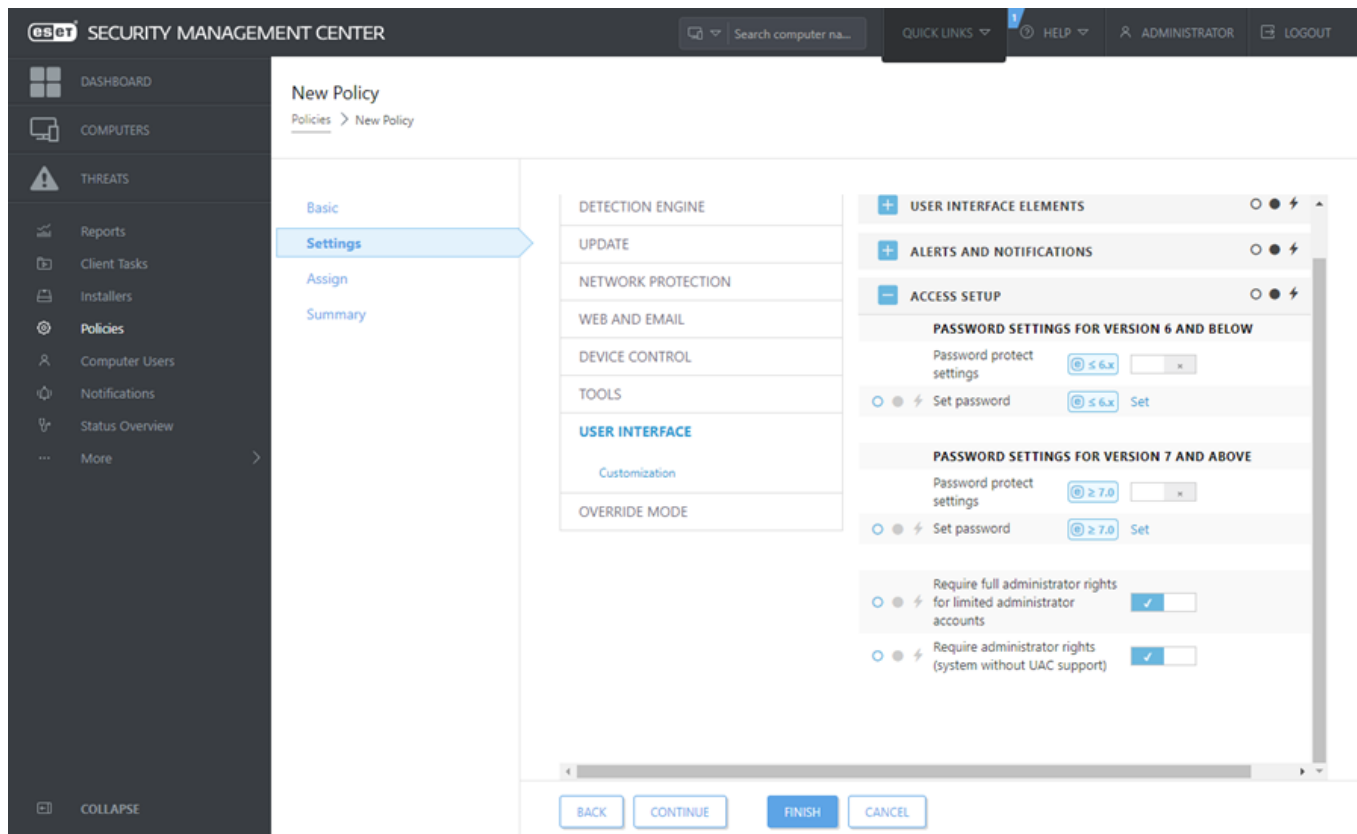
- [Більш докладну інформацію про це див. в онлайн-посібнику користувача ESET PROTECT Cloud](#)

Параметри, захищені паролем

Щоб забезпечити максимальну безпеку вашої системи, ESET Endpoint Antivirus необхідно налаштувати правильно. Будь-які некваліфіковані зміни або налаштування можуть призвести до погіршення безпеки клієнта та зниження рівня захисту. Щоб обмежити доступ користувачів до додаткових параметрів, адміністратор може захистити їх паролем.

Адміністратор може створити політику для захисту паролем налаштувань "Додаткові параметри" для ESET Endpoint Antivirus на підключених клієнтських комп'ютерах. Щоб створити нову політику, виконайте вказані нижче дії:

1. У ESET PROTECT Web Console клацніть **Політики** в основному меню ліворуч.
2. Клацніть **Створити політику**.
3. Вкажіть ім'я нової політики та введіть короткий опис (необов'язково). Натисніть кнопку **Продовжити**.
4. У списку продуктів виберіть **ESET Endpoint for Windows**.
5. Клацніть **Інтерфейс користувача** в списку **Налаштування** й розгорніть розділ **Параметри доступу**.
6. Відповідно до версії ESET Endpoint Antivirus клацніть повзунок, щоб увімкнути **Пароль для захисту параметрів**. Зверніть увагу, що продукти ESET Endpoint версії 7 і більш пізніх версій забезпечують покращений захист. Якщо ви маєте обидві версії продукту Endpoint (7 і більш пізніх версій та 6), рекомендується створити дві окремі політики з різними паролями для кожної з них.
7. У спливаючому вікні створіть новий пароль, підтвердьте його й натисніть кнопку **ОК**. Натисніть **Продовжити**.
8. Призначте політику клієнтам. Натисніть кнопку **Призначити** й виберіть комп'ютери або групи комп'ютерів, які необхідно захистити паролем. Натисніть кнопку **ОК** для підтвердження.
9. Перевірте, щоб всі бажані клієнтські комп'ютери були в цільовому списку та натисніть кнопку **Продовжити**.
10. Перегляньте параметри політики в розділі зведення та натисніть кнопку **Готово**, щоб зберегти нову політику.



Що таке політики?

Адміністратор може застосувати певні конфігурації до продуктів ESET, які виконуються на клієнтських комп'ютерах, за допомогою політик на веб-консолі ESET PROTECT. Політику можна застосувати безпосередньо до окремих комп'ютерів, а також до груп комп'ютерів. Можна також призначити декілька політик комп'ютеру або групі.

Користувачі можуть створювати нові політики, якщо вони мають такі дозволи: **Читання** для читання списку політик, **Використання** для призначення політик цільовим комп'ютерам, а також **Запис** для створення, зміни або редагування політик.

Політики застосовуються в тому порядку, в якому згруповані статичні групи. Це не так для динамічних груп, відносно яких політики застосовуються спочатку для дочірніх динамічних груп. Це дозволяє застосувати політики широкого впливу до верхньої частини дерева групи, а вузькоспрямовані політики — до підгруп. За допомогою [прапорців](#) користувач ESET Endpoint Antivirus з доступом до груп, розташованих вище в дереві, може перевизначити політики груп, що розташовані нижче. Відповідний алгоритм описаний в [онлайн-довідці ESET PROTECT](#).

i Рекомендуємо призначити більше загальних політик (наприклад, політику оновлення сервера) групам, що розташовані вище в дереві груп. Вузькоспрямовані політики (наприклад, параметри керування пристроєм) мають призначатися групам, розташованим на нижчих рівнях дерева групи. Під час злиття політики більш низького рівня зазвичай заміщують політики більш високого рівня (якщо інше не задано [прапорцями політики](#)).



Об'єднання політик

Політика, яка застосовується до клієнта, як правило, являє собою результат злиття декількох політик в одну. Політики об'єднуються одна за одною (по черзі). Під час об'єднання політик, як правило, більш пізня політика завжди заміщує параметри, задані більш ранньою. Щоб змінити цю поведінку, можна використовувати [прапорці політики](#) (доступні для кожного параметра).

Під час створення політик ви помітите, що деякі параметри мають додаткове правило (замінити/додати з кінця/додати з початку), яке можна налаштувати.

- **Замінити.** Замінюється весь список, додаються нові значення та видаляються всі попередні.
- **Додати з кінця.** Елементи додаються в нижню частину наразі застосованого списку (має бути інша політика, локальний список завжди перезаписується).
- **Додати з початку.** Елементи додаються у верхню частину списку (локальний список перезаписується).

ESET Endpoint Antivirus підтримує об'єднання локальних параметрів з віддаленими політиками по-новому. Якщо параметр є списком (наприклад, список заблокованих веб-сайтів), і локальна політика конфліктує з існуючим локальним параметром, останній перезаписується віддаленою політикою. Можна вибрати, як створювати локальні та віддалені списки, вибираючи різні правила об'єднання для:



-  Об'єднання параметрів для віддалених політик.
-  Об'єднання віддалених і локальних політик: локальні параметри з кінцевою віддаленою політикою.

Щоб дізнатися більше про об'єднання політик, див. [онлайн-посібник користувача ESET PROTECT](#), а також цей [приклад](#).

Принцип дії прапорців


Політика, яка застосовується до клієнтського комп'ютера, як правило, являє собою результат злиття декількох політик в одну. Під час об'єднання політик ви можете налаштувати бажану поведінку цільової політики, змінюючи порядок застосовуваних політик за допомогою прапорців політики. Прапорці визначають, яким чином політика буде керувати певними параметрами.

Для кожного параметра можна вибрати один із таких прапорців:

 Не застосовувати	Будь-який параметр із цим прапорцем не задається політикою. Оскільки параметр не задається політикою, він може бути змінений іншими політиками, які будуть застосовані пізніше.
 Застосувати	Параметри з прапорцем " Застосувати " будуть застосовані до клієнтського комп'ютера. Однак під час об'єднання політик ці налаштування можуть бути заміщені іншими політиками, які застосовані пізніше. Коли політика надсилається на клієнтський комп'ютер із параметрами, позначеними цим прапорцем, ці параметри змінять локальну конфігурацію клієнтського комп'ютера. Параметри, що не застосовуються примусово, можуть бути заміщені іншими політиками, які будуть застосовані пізніше.

Примусово

Параметри з прапорцем "**Примусово**" мають вищий пріоритет та не можуть бути заміщені будь-якою політикою, застосованою пізніше (навіть якщо для неї також встановлено прапорець "**Примусово**"). Це гарантує, що інші політики, які будуть застосовані пізніше, не зможуть змінити цей параметр під час об'єднання. Коли політика надсилається на клієнтський комп'ютер із параметрами, позначеними цим прапорцем, ці параметри змінять локальну конфігурацію клієнтського комп'ютера.



Сценарій. Адміністратор хоче дозволити користувачу *John* створювати або змінювати політики в його домашній групі та переглядати політики, створені адміністратором, включно з політиками, для яких встановлено прапорці  Примусово. Адміністратор хоче, щоб користувач *John* міг переглядати всі політики та не міг редагувати існуючі політики, створені адміністратором. *John* може тільки створювати або редагувати політики у власній домашній групі San Diego.

Рішення. Адміністратор має виконати такі кроки:


Створити статичні групи та набори дозволів

1. Створити нову [статичну групу](#) під назвою *San Diego*.
2. Створити новий [набір дозволів](#) під назвою *Policy - All John* з доступом до статичної групи Всі, а також із дозволом **Читання** для **політик**.
3. Створити новий [набір дозволів](#) під назвою *Policy John* з доступом до статичної групи *San Diego*, функціональним доступом із дозволом **Запис** по відношенню до **груп і комп'ютерів і Політик**. Цей набір дозволів дозволить користувачу *John* створювати або редагувати політики в його домашній групі *San Diego*.
4. Створити нового [користувача](#) *John* і в розділі **набори дозволів** вибрати *Policy - All John* і *Policy John*.

Створення політик

5. Створити нову [політику](#) *All- Enable Firewall*, розгорнути розділ **Параметри**, вибрати **ESET Endpoint for Windows**, потім послідовно вибрати пункти **Персональний брандмауер** > **Основне** і застосувати всі параметри за допомогою прапорця  **Примусово**. Розгорнути розділ **Призначити** і вибрати статичну групу Всі.
6. Створити нову [політику](#) *John Group- Enable Firewall*, розгорнути розділ **Параметри**, вибрати **ESET Endpoint for Windows**, потім послідовно вибрати пункти **Персональний брандмауер** > **Основне** і застосувати всі параметри за допомогою прапорця  **Застосувати**. Розгорнути розділ **Призначити** і вибрати статичну групу *San Diego*.

Результат

Політики, створені адміністратором, будуть застосовані вперше, оскільки до параметрів політики були застосовані прапорці  **Примусово**. Параметри з прапорцем "Примусово" мають вищий пріоритет та не можуть бути заміщені будь-якою політикою, застосованою пізніше. Політики, створені користувачем *John*, будуть застосовані після політик, створених адміністратором.

Щоб переглянути кінцевий порядок політик, послідовно виберіть пункти **Більше** > **Групи** > **San Diego**. Виберіть комп'ютер, потім виберіть пункт **Показати подробиці**. У розділі **Конфігурація** клацніть **Застосовані політики**.

Самостійне використання ESET Endpoint Antivirus

Цей розділ і розділ [Робота з ESET Endpoint Antivirus](#) посібника користувача призначені для тих, хто застосовує ESET Endpoint Antivirus без ESET PROTECT или ESET PROTECT Cloud. Усі функції ESET Endpoint Antivirus повністю доступні (залежно від прав облікового запису користувача).

Методи інсталяції

Є декілька методів інсталяції ESET Endpoint Antivirus версії 9.x на клієнтській робочій станції, якщо [ESET Endpoint Antivirus не розгорнуто віддалено на клієнтських робочих станціях за допомогою ESET PROTECT або ESET PROTECT Cloud](#).

Метод	Призначення	Посилання на завантаження
Інсталяція з використанням ESET AV Remover	На етапі підготовки до інсталяції інструмент ESET AV Remover допоможе видалити практично будь-яке антивірусне програмне забезпечення, інстальоване в системі раніше.	Завантажити 64-розрядну версію Завантажити 32-розрядну версію
*** Інсталяція (.exe)	Процес інсталяції без застосування ESET AV Remover.	N/A
Інсталяція (.msi)	У корпоративному середовищі рекомендується використовувати інсталятор MSI. Це обумовлено розгортаннями в режимі «офлайн» і віддаленими розгортаннями, для яких використовуються різні інструменти, наприклад ESET PROTECT.	Завантажити 64-розрядну версію Завантажити 32-розрядну версію
Інсталяція з використання командного рядка	ESET Endpoint Antivirus можна інсталювати локально за допомогою командного рядка або віддалено, використовуючи клієнтське завдання з ESET PROTECT.	N/A
Розгортання за допомогою об'єкта групової політики (GPO) або SCCM	Скористайтесь інструментами керування, наприклад об'єктом групової політики (GPO) або SCCM, для розгортання ESET Management Agent і ESET Endpoint Antivirus на робочих станціях клієнтів.	N/A
Розгортання з використанням інструментів RMM	Плагін ESET DEM для інструмента віддаленого моніторингу й керування (RMM) дозволяє розгорнути ESET Endpoint Antivirus на клієнтських робочих станціях.	N/A

ESET Endpoint Antivirus доступна [більш ніж 30 мовами](#).

Інсталяція з використанням ESET AV Remover

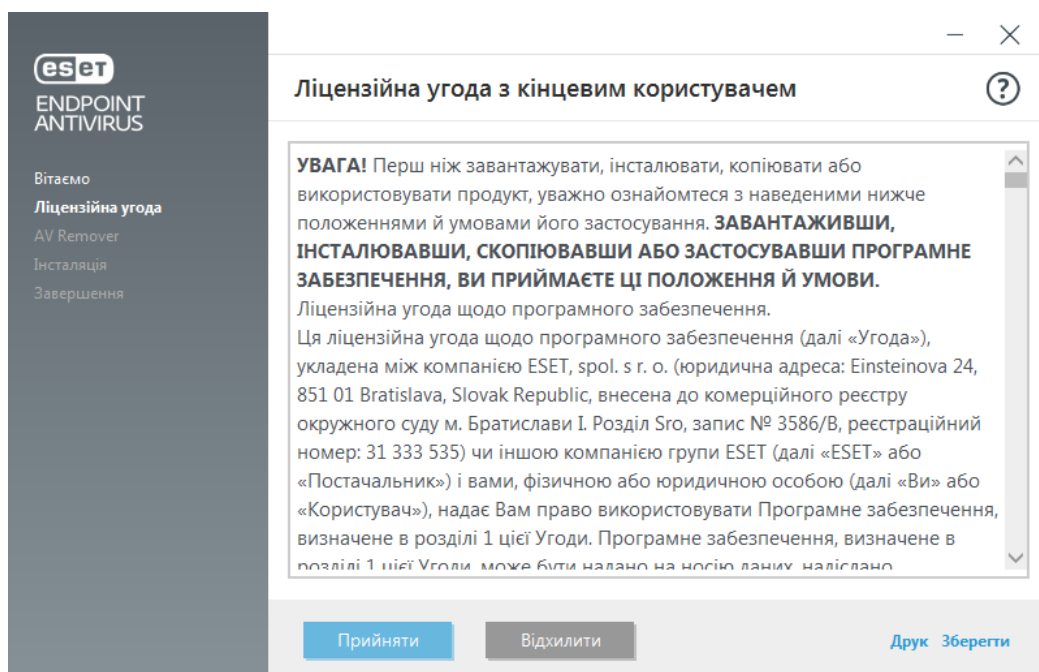
Перш ніж продовжувати інсталяцію, видаліть на комп'ютері всі програми для захисту. Установіть прапорець **Я хочу видалити непотрібні антивірусні програми за допомогою ESET AV Remover**. Після цього ESET AV Remover просканує вашу систему й вилучить усі [підтримувані програми для захисту](#). Щоб інсталювати ESET Endpoint Antivirus без запуску ESET AV Remover, натисніть **Продовжити** (прапорець має бути знято).



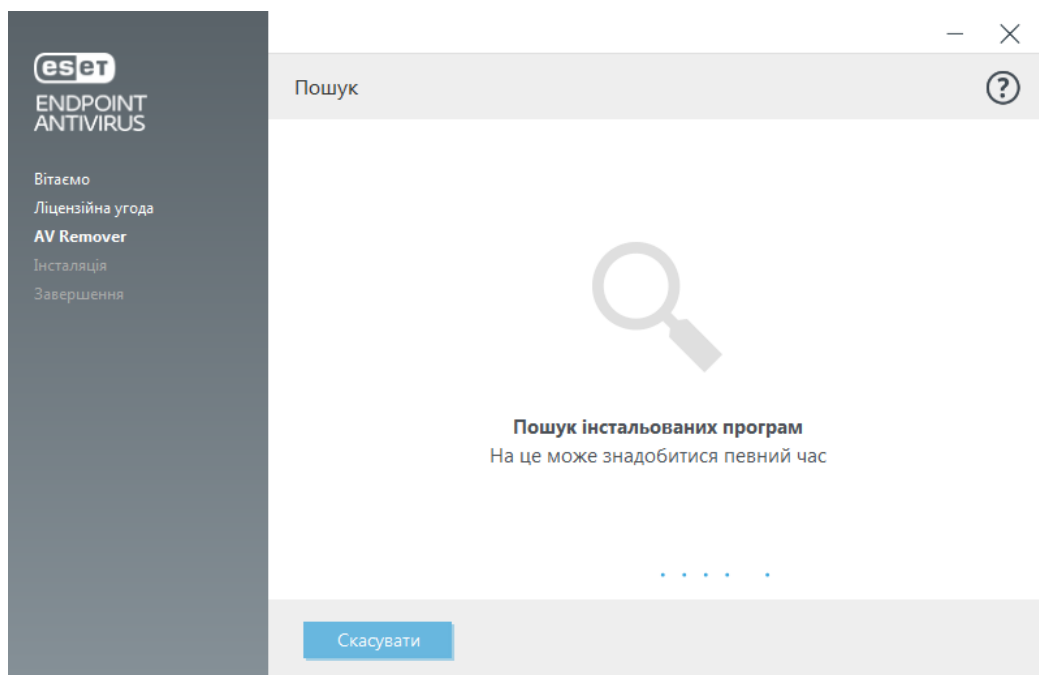
ESET AV Remover

Інструмент ESET AV Remover допоможе видалити практично будь-яке антивірусне програмне забезпечення, інстальоване в системі. Щоб видалити антивірусну програму за допомогою ESET AV Remover, дотримуйтесь інструкцій нижче.

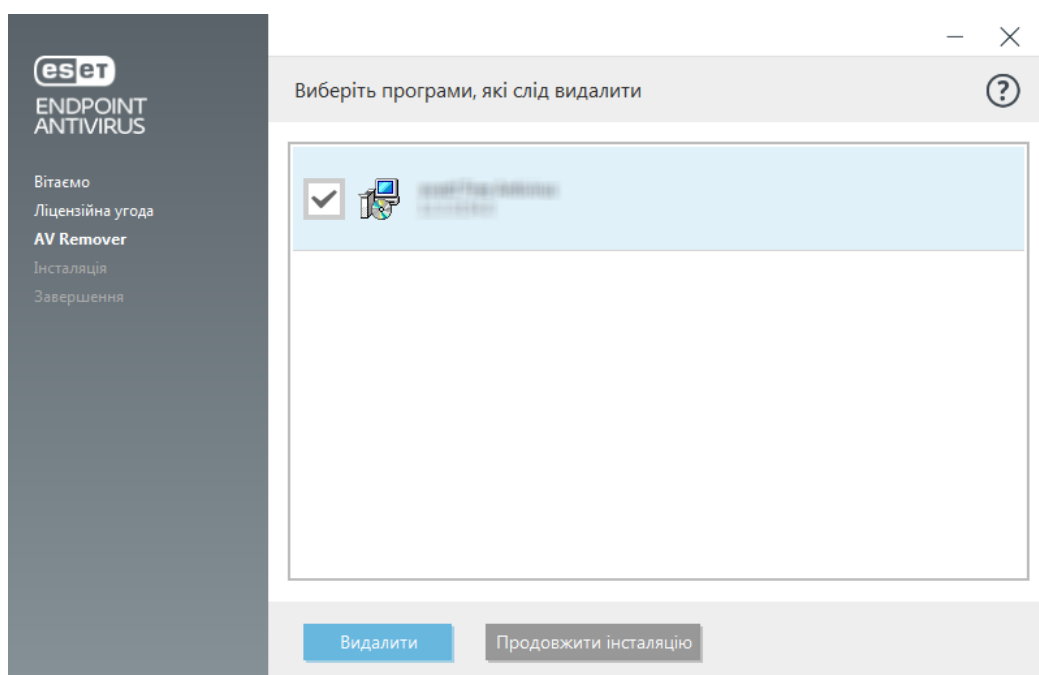
1. [Ознайомтеся зі статтею в базі знань ESET](#), щоб дізнатися, яке антивірусне програмне забезпечення можна видалити за допомогою ESET AV Remover.
2. Прочитайте Ліцензійну угоду з кінцевим користувачем і натисніть **Прийняти**, щоб засвідчити свою згоду з її умовами. Якщо натиснути **Відхилити**, інсталяцію ESET Endpoint Antivirus буде продовжено, однак програму для захисту на комп'ютері видалено не буде.



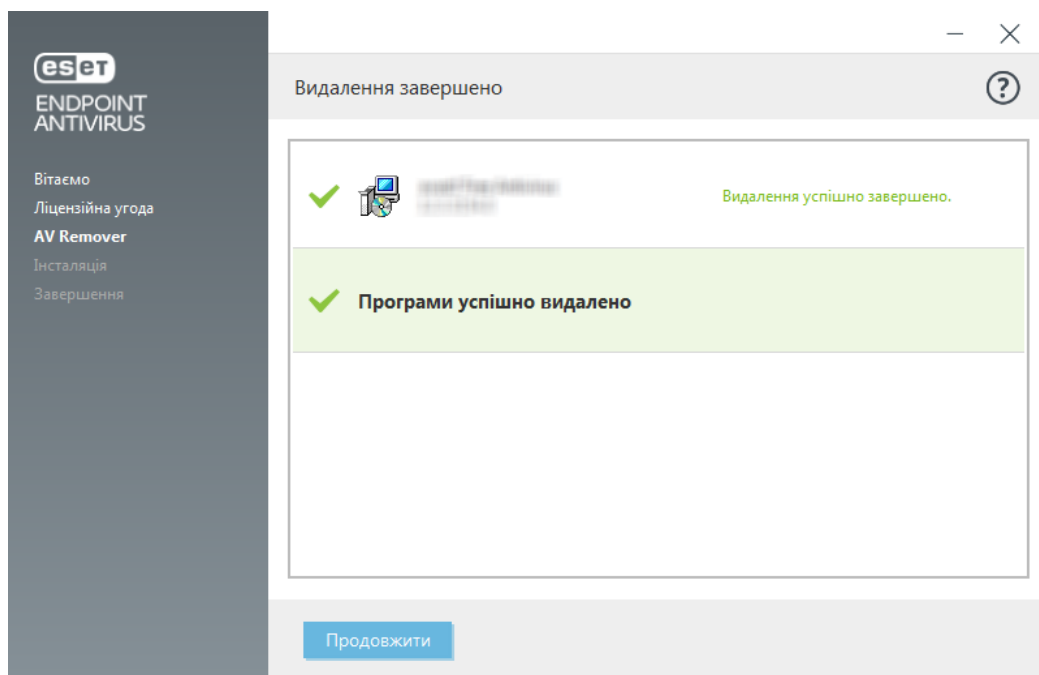
2. ESET AV Remover почне шукати у вашій системі антивірусне програмне забезпечення.



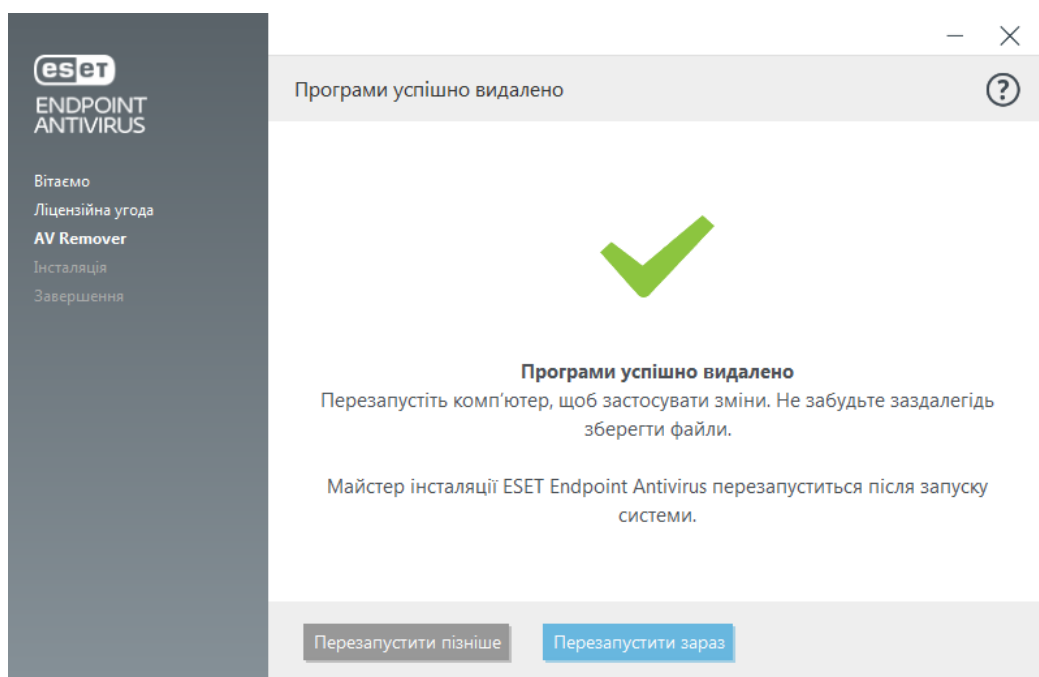
2. Виберіть будь-який знайдений варіант і натисніть **Видалити**. На це може знадобитися певний час.



2. Після видалення програми натисніть **Продовжити**.



6. Перезавантажте комп'ютер, щоб застосувати зміни та продовжити інсталяцію ESET Endpoint Antivirus. Якщо видалити програму не вдалося, перегляньте в цьому посібнику розділ [Помилка видалення програми за допомогою ESET AV Remover](#).



Помилка видалення програми за допомогою ESET AV Remover

Якщо вам не вдається видалити антивірусну програму за допомогою ESET AV Remover, ви отримаєте сповіщення про те, що ця програма не підтримується ESET AV Remover. Щоб дізнатися, чи можна видалити певну програму, перегляньте [список підтримуваних продуктів](#) або [засобів для видалення поширених антивірусних програм Windows](#) у базі знань ESET.

Якщо видалити продукт для захисту не вдалося або певний його компонент було видалено

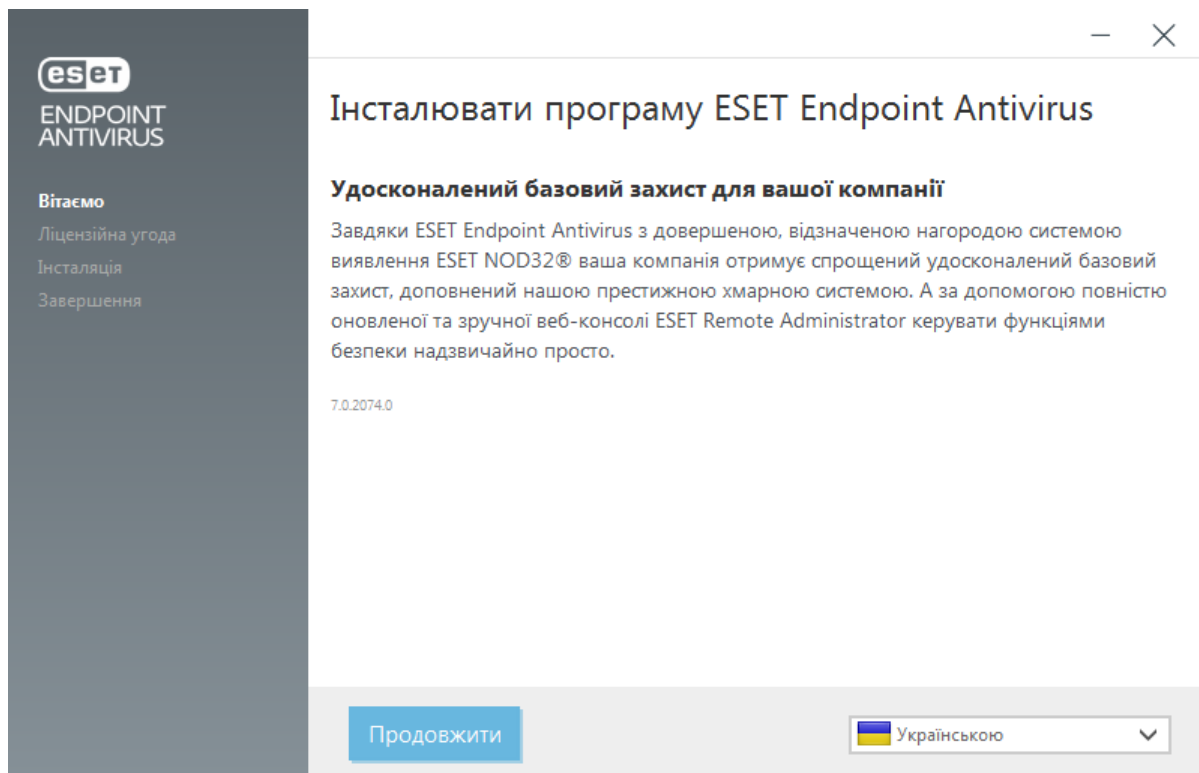
лише частково, з'явиться запит **Перезапустити та перевірити повторно**. Після запуску підтвердьте UAC та продовжте процес сканування й видалення.

За потреби зверніться до [служби технічної підтримки ESET](#), щоб створити відповідний запит і відкрити доступ до файлу **AppRemover.log** для технічних спеціалістів ESET. Файл **AppRemover.log** розташовано в папці **eset**. Щоб знайти її, відкрийте **%TEMP%** у Windows Explorer. Спеціалісти служби технічної підтримки ESET допоможуть вирішити проблему якнайшвидше.

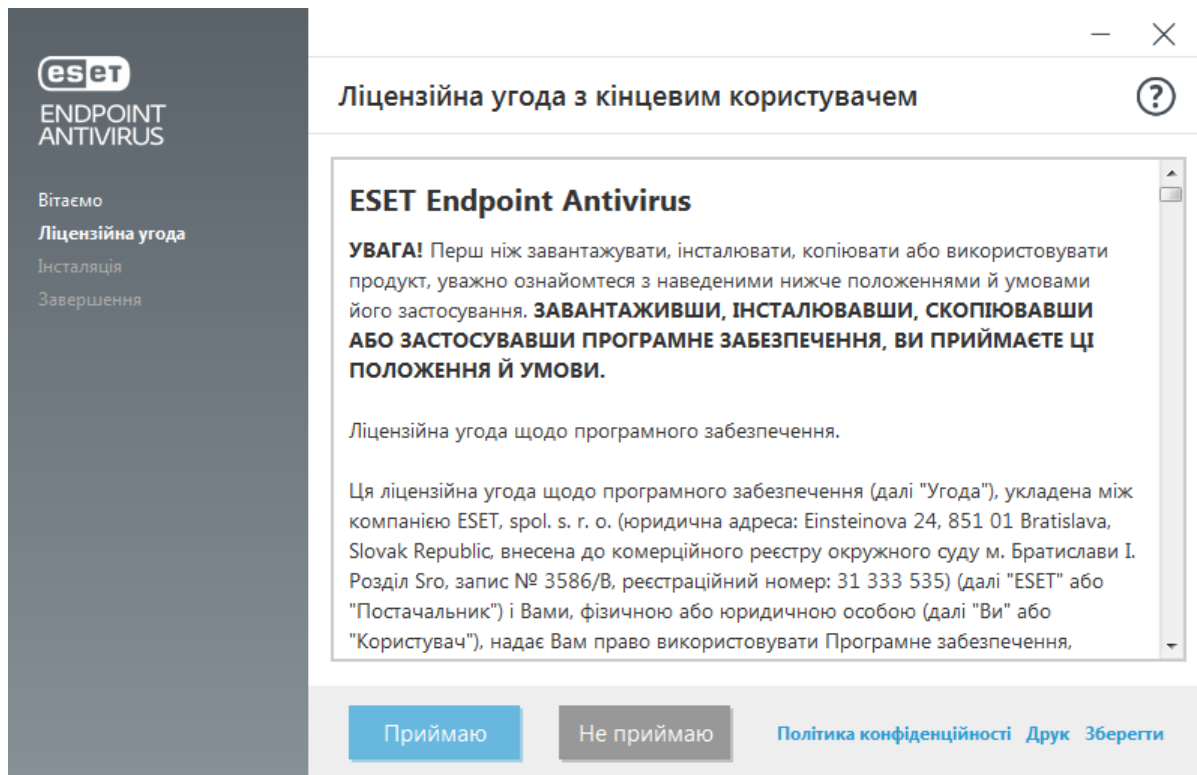
Інсталяція (.exe)

Після запуску інсталятора .exe майстер інсталяції надасть усі інструкції для виконання цього процесу.

⚠ Переконайтеся, що на комп'ютері не інстальовано іншої антивірусної програми. Якщо на комп'ютері інстальовано кілька антивірусних програм, вони можуть конфліктувати одна з одною. Рекомендується видалити із системи інші антивірусні програми. Див. [статтю бази знань](#), у якій представлено список засобів видалення типового антивірусного ПЗ (доступно англійською та кількома іншими мовами).



1. Ознайомтеся з текстом ліцензійної угоди з кінцевим користувачем. Клацніть **Дозволити все й продовжити**, щоб налаштувати виявлення [потенційно небажаних програм](#) і ввімкнути [систему зворотного зв'язку ESET LiveGrid®](#). За допомогою системи ESET LiveGrid® компанія ESET одразу та на постійній основі отримує сповіщення про всі нові загрози, що допомагає нам краще захищати наших клієнтів. Система дає змогу надсилати нові підозрілі файли в антивірусну лабораторію ESET, де вони аналізуються, обробляються та додаються до обробника виявлення. Клацніть **Продовжити**, щоб засвідчити свою згоду з умовами ліцензійної угоди з кінцевим користувачем. Можна інсталювати ESET Endpoint Antivirus в певну папку, клацнувши [Змінити папку інсталяції](#).



- Після завершення інсталяції з'явиться запит на [активацію ESET Endpoint Antivirus](#).

Змінити папку інсталяції (.exe)

Коли ви вкажете параметр для функції виявлення потенційно небажаних програм і натиснете **Потенційно небажані програми**, з'явиться запит на вибір папки для інсталяції продукту ESET Endpoint Antivirus. За замовчуванням програма інсталюється в таку папку:

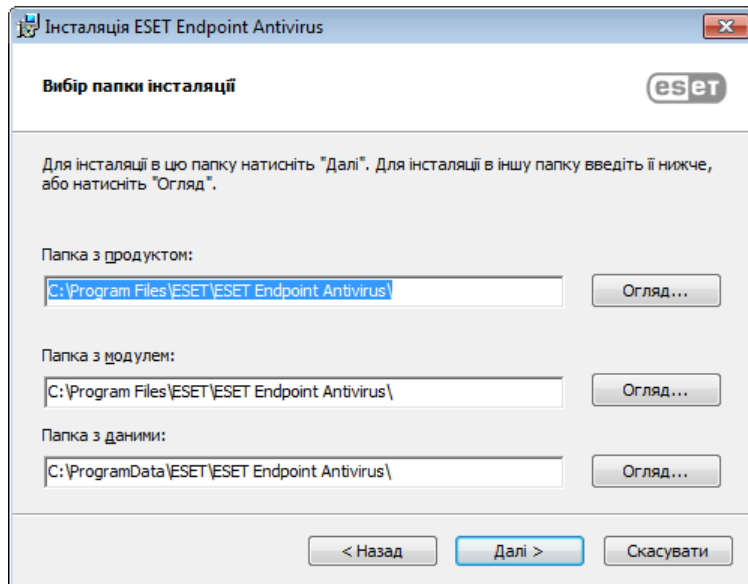
`C:\Program Files\ESET\ESET Security\`

Можна вказати розташування для модулів і даних програми. За замовчуванням ці компоненти інсталюються в такі папки відповідно:

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

`C:\ProgramData\ESET\ESET Security\`

Натисніть **Огляд**, щоб змінити розташування (не рекомендується).



Клацніть **Назад**, щоб продовжити інсталяцію.

Інсталяція (.msi)

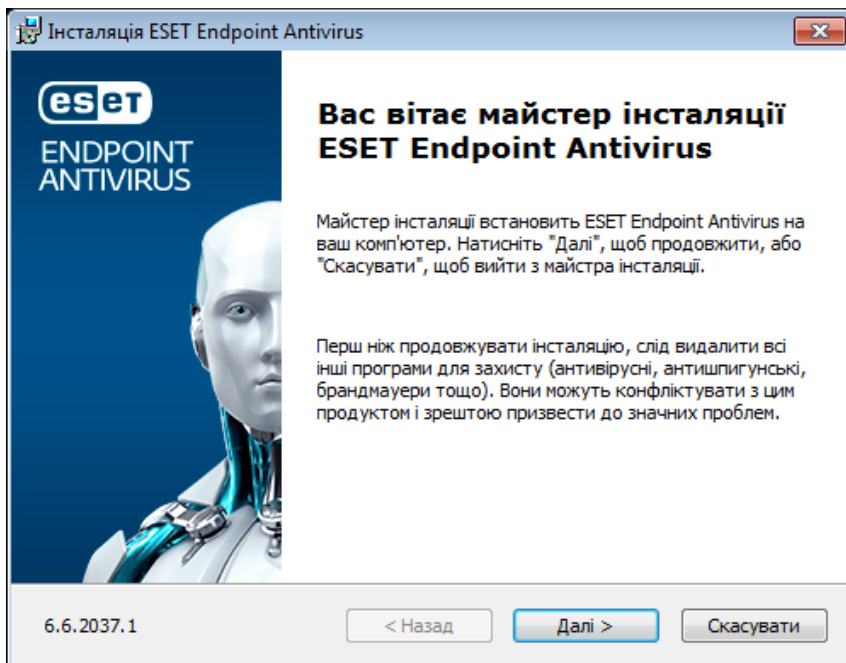
Після запуску інсталятора MSI майстер інсталяції надасть усі інструкції для виконання цього процесу.

✓ У корпоративному середовищі рекомендується використовувати інсталятор MSI. Це обумовлено розгортаннями в режимі «офлайн» і віддаленими розгортаннями, для яких використовуються різні інструменти, наприклад ESET PROTECT.

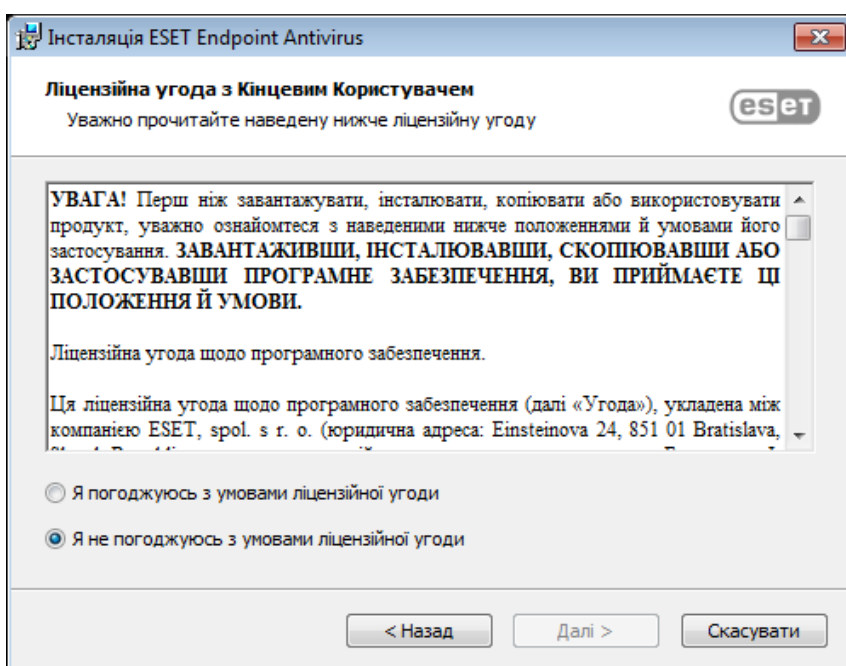
⚠ Переконайтеся, що на комп'ютері не інстальовано іншої антивірусної програми. Якщо на комп'ютері інстальовано кілька антивірусних програм, вони можуть конфліктувати одна з одною. Рекомендується видалити із системи інші антивірусні програми. Див. [статтю бази знань](#), у якій представлено список засобів видалення типового антивірусного ПЗ (доступно англійською та кількома іншими мовами).

i Інсталятор ESET Endpoint Antivirus, створений у ESET PROTECT 8.1 і новіших версій, підтримує Windows 10 Enterprise for Virtual Desktops і режим кількох сеансів у Windows 10.

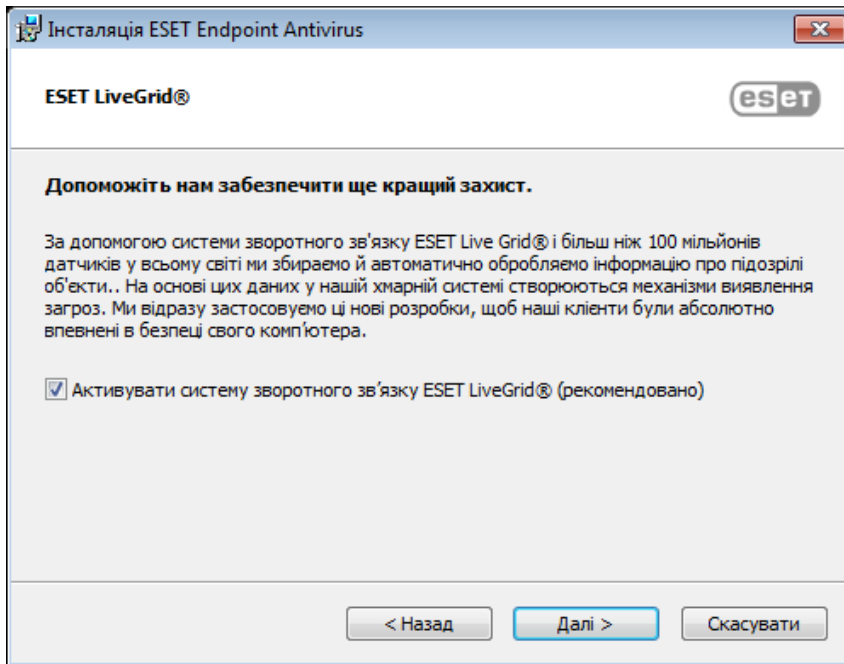
1. Виберіть потрібну мову й клацніть **Далі**.



2. Ознайомтеся з текстом ліцензійної угоди з кінцевим користувачем і натисніть **Я погоджуюсь з умовами ліцензійної угоди**, щоб засвідчити свою згоду з умовами ліцензійної угоди. Після цього натисніть **Далі**, щоб продовжити інсталяцію.



3. Виберіть налаштування для системи зворотного зв'язку [ESET LiveGrid®](#). За допомогою системи ESET LiveGrid® компанія ESET одразу та на постійній основі отримує сповіщення про всі нові загрози, що допомагає нам краще захищати наших клієнтів. Система дає змогу надсилати нові підозрілі файли в антивірусну лабораторію ESET, де вони аналізуються, обробляються та додаються до обробника виявлення. Щоб відкрити вікно [Розширена інсталяція \(.msi\)](#), клацніть **Додаткові параметри**.



5. Останній крок — підтвердити інсталяцію, натиснувши **Інсталювати**. Після завершення інсталяції з'явиться запит на [активацію ESET Endpoint Antivirus](#).

Розширена інсталяція (.msi)

Під час розширеної інсталяції можна налаштовувати певні параметри, не доступні під час типової інсталяції.

5. Коли ви вкажете параметр для функції виявлення [потенційно небажаних програм](#) і натиснете **Додаткові параметри**, з'явиться запит на вибір папки для інсталяції ESET Endpoint Antivirus. За замовчуванням програма інсталюється в таку папку:

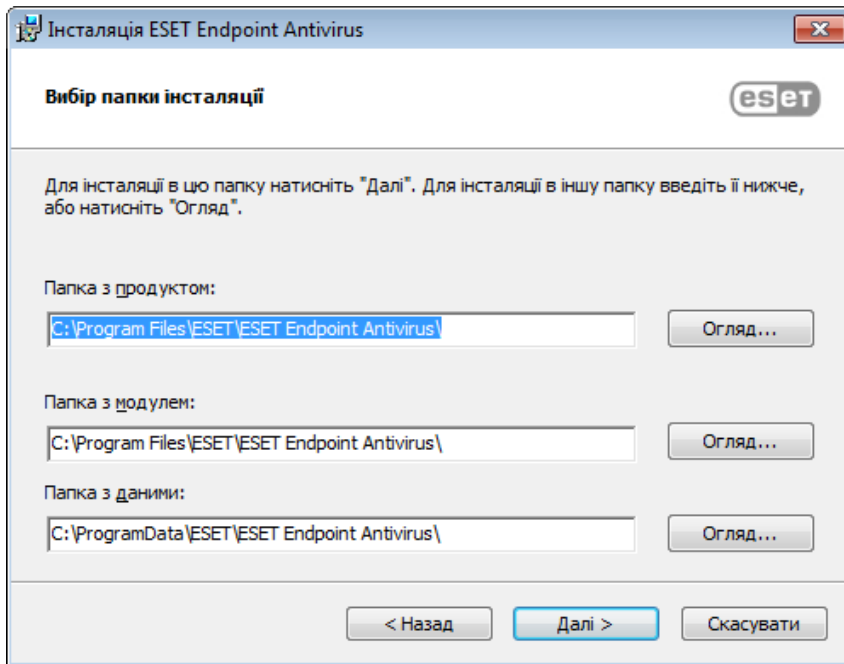
C:\Program Files\ESET\ESET Security

Можна вказати розташування для модулів і даних програми. За замовчуванням ці компоненти інсталюються в такі папки відповідно:

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

C:\ProgramData\ESET\ESET Security

Натисніть **Огляд**, щоб змінити розташування (не рекомендується).



7. Останній крок — підтвердити інсталяцію, натиснувши **Інсталювати**.

Мінімальна інсталяція модулів

Щоб зменшити мережевий трафік, що зумовлений великим розміром інсталювача, і зекономити ресурси, ESET надає можливість скористатися мінімальним інсталювачем модулів. Цей інсталювач містить лише важливі модулі, а всі інші модулі завантажуються під час першого оновлення модуля після активації продукту. Основна перевага полягає в тому, що розмір інсталювача значно менше, а ESET Endpoint Antivirus завантажує лише найновіші модулі програми під час активації продукту.

Мінімальний інсталювач модулів містить такі модулі:

- Модулі завантаження
- Модуль підтримки «Антируткіт»
- Модуль зв'язку для безпосереднього підключення до хмари
- Модуль підтримки перетворення
- Модуль конфігурації
- Модуль SSL

Після активації продукту відображатиметься статус **Ініціалізація захисту**, який сповіщатиме про ініціалізацію функцій.



Якщо під час завантаження модулів виникне проблема (наприклад, через налаштування проксі-сервера, відсутність зв'язку з мережею тощо), відобразиться статус попередження програми **Слід звернути увагу**. У головному вікні програми клацніть **Оновити > Перевірити наявність оновлень**, щоб знову запустити процес оновлення.

Після кількох невдалих спроб відображається червоний статус програми **Не вдалося налаштувати захист**.

✓ Якщо на клієнтських комп'ютерах немає підключення до Інтернету або ви працюєте в автономному режимі, скористуйтеся наведеними нижче способами, щоб завантажити файли оновлення із серверів оновлення ESET:

- [Оновлення із дзеркала](#)
- [Використання інструмента "Дзеркало"](#)

i Якщо не вдається ініціалізувати процес і завантажити модулі, завантажте повні інсталятори MSI [за цим посиланням](#).

Інсталяція з використання командного рядка

ESET Endpoint Antivirus можна інсталювати локально з використанням командного рядка або віддалено з використанням клієнтського завдання з ESET PROTECT.

Підтримувані параметри

APPDIR=<path>

- Path – дійсний шлях до каталогу.
- Каталог для інсталяції програми.

APPDATADIR=<path>

- Path – дійсний шлях до каталогу.
- Каталог для інсталяції даних програми.

MODULEDIR=<path>

- Path – дійсний шлях до каталогу.
- Каталог для інсталяції модуля.

ADDLOCAL=<list>

- Інсталяція компонентів – список необов'язкових функцій, які потрібно інсталювати локально.
- Використання з пакетами .msi ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Докладнішу інформацію про властивість **ADDLOCAL** можна переглянути на сторінці <http://msdn.microsoft.com/uk-ua/library/aa367536%28v=vs.85%29.aspx>.

ADDEXCLUDE=<list>

- ADDEXCLUDE — це список (із роздільниками-комами) з іменами всіх функцій, які не потрібно інсталювати. Цей список тепер використовується замість REMOVE.
- Під час вибору функції, яку не потрібно інсталювати, у списку необхідно явним чином вказати повний шлях (з усіма його підфункціями), а також пов'язані невидимі функції.
- Використання з пакетами .msi ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

i ADDEXCLUDE не можна використовувати разом з **ADDLOCAL**.

Відповідні параметри командного рядка можна переглянути в [документації](#) для використовуваної версії **msiexec**.

Правила

- Список **ADDLOCAL** – це список імен усіх функцій для інсталяції (імена розділено комами).
- Вибираючи функцію, яку потрібно інсталювати, додайте у список увесь шлях (усі батьківські функції).
- Щоб зробити все як слід, перегляньте додаткові правила.

Компоненти й функції



Параметри ADDLOCAL/ADDEXCLUDE не працюють для установки компонентів у програмі ESET Endpoint Antivirus.

Функції розподілено за чотирма такими категоріями:

- **Обов'язкові:** такі функції інсталюються завжди.
- **Необов'язкові:** інсталяцію цих функцій можна скасувати.
- **Невидима:** логічна функція, необхідна для належної роботи інших функцій.
- **Показчик місця заповнення:** функція, яка ніяк не впливає на продукт, однак її слід зазначити з підфункціями.

Нижче наведено набір функцій ESET Endpoint Antivirus:

Опис	Ім'я функції	Батьківська функція	Категорія
Базові компоненти програми	Computer		Показчик місця заповнення
Ядро виявлення	Antivirus	Computer	Обов'язкова
Ядро виявлення / сканування на наявність шкідливого програмного забезпечення	Scan	Computer	Обов'язкова
Ядро виявлення / захист файлової системи в режимі реального часу	RealtimeProtection	Computer	Обов'язкова
Ядро виявлення / сканування на наявність шкідливого програмного забезпечення / захист документів	DocumentProtection	Antivirus	Необов'язкова
Контроль пристроїв	DeviceControl	Computer	Необов'язкова
Захист мережі	Network		Показчик місця заповнення
Захист мережі / брандмауер	Firewall	Network	Необов'язкова
Захист мережі / захист від мережеских атак / ...	IdsAndBotnetProtection	Network	Необов'язкова
Захищений браузер	OnlinePaymentProtection	WebAndEmail	Необов'язкова

Опис	Ім'я функції	Батьківська функція	Категорія
Інтернет і електронна пошта	WebAndEmail		Показчик місця заповнення
Інтернет і електронна пошта / фільтрація протоколів	ProtocolFiltering	WebAndEmail	Невидима
Інтернет і електронна пошта / Захист доступу до Інтернету	WebAccessProtection	WebAndEmail	Необов'язкова
Інтернет і електронна пошта / Захист поштового клієнта	EmailClientProtection	WebAndEmail	Необов'язкова
Інтернет і електронна пошта / захист поштового клієнта / поштові клієнти	MailPlugins	EmailClientProtection	Невидима
Інтернет і електронна пошта / Захист поштового клієнта / Антиспам	Antispam	EmailClientProtection	Необов'язкова
Інтернет і електронна пошта/Веб-контроль	WebControl	WebAndEmail	Необов'язкова
Інструменти / ESET RMM	Rmm		Необов'язкова
Оновлення / профілі / дзеркало оновлення	UpdateMirror		Необов'язкова
Плагін ESET Inspect	EnterpriseInspector		Невидима

Груповий набір функцій:

Опис	Ім'я функції	Тип функції
Усі обов'язкові функції	_Base	Невидима
Усі доступні функції	ALL	Невидима

Додаткові правила

- Якщо будь-яка функція **WebAndEmail** вибрана для інсталяції, невидиму функцію **ProtocolFiltering** необхідно внести до списку.
- Імена всіх функцій указуються з урахуванням регістру, наприклад ім'я UpdateMirror не тотожне до імені UPDTEMIRROR.

Список властивостей конфігурації

Властивість	Значення	Функція
CFG_POTENTIALLYUNWANTED_ENABLED=	0 — вимкнено 1 — увімкнено	Виявлення потенційно небажаних програм
CFG_LIVEGRID_ENABLED=	Див. нижче	Див. тему Властивість LiveGrid нижче
FIRSTSCAN_ENABLE=	0 — вимкнено 1 — увімкнено	Планування й виконання сканування комп'ютера після інсталяції

Властивість	Значення	Функція
CFG_PROXY_ENABLED=	0 — вимкнено 1 — увімкнено	Параметри проксі-сервера
CFG_PROXY_ADDRESS=	<ip>	IP-адреса проксі-сервера
CFG_PROXY_PORT=	<port>	Номер порту проксі-сервера
CFG_PROXY_USERNAME=	<username>	Ім'я користувача для автентифікації
CFG_PROXY_PASSWORD=	<password>	Пароль для автентифікації
ACTIVATION_DATA=	Див. нижче	Активация продукту, ліцензійний ключ або автономний файл ліцензії
ACTIVATION_DLG_SUPPRESS=	0 — вимкнено 1 — увімкнено	Якщо задано значення "1", діалогове вікно активації продукту не відображається після першого запуску
ADMINCFG=	<path>	Шлях до експортованої конфігурації в файлі XML (за замовчуванням використовується файл <i>cfg.xml</i>)

Властивість [LiveGrid®](#)

Після інсталяції ESET Endpoint Antivirus з CFG_LIVEGRID_ENABLED, його поведінку описано нижче:

Функція	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Система репутації ESET LiveGrid® (рекомендується)	Увімкнено	Увімкнено
Система зворотного зв'язку ESET LiveGrid®	Вимкнено	Увімкнено
Надіслати анонімну статистику	Вимкнено	Увімкнено

Властивість ACTIVATION_DATA

Формат	Метод
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Активация з використанням ліцензійного ключа ESET (підключення до Інтернету має бути активним)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Активация з використанням автономного ліцензійного файлу

Властивості мови

ESET Endpoint Antivirus (необхідно вказати обидві властивості).

Властивість	Значення
PRODUCT_LANG=	Код мови (код локалізації), наприклад 1033 для англійської (США). Список код мов див. за цим посиланням .
PRODUCT_LANG_CODE=	Рядок коду мови (мова й регіональні параметри) в нижньому регістрі, наприклад "en-us" для англійської (США). Список код мов див. за цим посиланням .

Властивості перезавантаження

Укажіть наведені нижче параметри, щоб перезавантажити комп'ютер після інсталяції:

Властивість	Значення	Функція
REBOOT_WHEN_NEEDED=	0 — вимкнено 1 — увімкнено	Якщо цей параметр увімкнено, після інсталяції комп'ютер перезавантажиться.
REBOOT_CANCELABLE=	0 — вимкнено 1 — увімкнено	Якщо цей параметр увімкнено, користувач може скасувати перезавантаження комп'ютера.
REBOOT_POSTPONE=	значення в секундах	Максимальний час у секундах, протягом якого користувач може відкласти перезавантаження комп'ютера.



REBOOT_CANCELABLE і REBOOT_POSTPONE доступні, тільки якщо ввімкнено REBOOT_WHEN_NEEDED.

Приклади інсталяції з використанням командного рядка



Перш ніж запускати інсталяцію, необхідно ознайомитися з [ліцензійною угодою](#) й мати права адміністратора.



Виключіть розділ **NetworkProtection** з інсталяції (необхідно також указати всі дочірні функції):

```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```



Щоб продукт ESET Endpoint Antivirus автоматично налаштувався після інсталяції, можна вказати основні параметри конфігурації в команді інсталяції.

Інсталяція ESET Endpoint Antivirus з увімкненою системою ESET LiveGrid®:

```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```



Інсталяція в інший каталог, ніж [установлений за замовчуванням](#).

```
msiexec /qn /i ees_nt64_eni.msi APPDIR=C:\ESET\
```



Інсталяція й активація ESET Endpoint Antivirus з використанням ліцензійного ключа ESET.

```
msiexec /qn /i ees_nt64_eni.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```



Автоматична інсталяція з докладним журналюванням (стане в пригоді для виправлення неполадок) і RMM тільки з обов'язковими компонентами:

```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```



Примусова автоматична повна інсталяція з [указаною мовою](#).

```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Параметри командного рядка, які застосовуються після інсталяції

- [ESET CMD](#) : імпорт конфігурації .xml або увімкнення/вимкнення функції захисту
- [Сканер командного рядка](#) : запуск сканування комп'ютера в командному рядку

Розгортання за допомогою об'єкта групової політики (GPO) або SCCM

Окрім [інсталяції ESET Endpoint Antivirus безпосередньо на робочу станцію клієнта](#), можна також скористатися інструментами керування "Об'єкт групової політики (GPO)" (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris або Puppet.

Кероване (рекомендовано)

Для керованих комп'ютерів спочатку потрібно інсталювати агент ESET Management, потім розгорнути ESET Endpoint Antivirus в ESET PROTECT. ESET PROTECT необхідно інсталювати у вашій мережі.

1. Завантажте [автономний інстальатор](#) для агента ESET Management.
2. [Підготуйте сценарій віддаленого розгортання за допомогою інструментів "Об'єкт групової політики \(GPO\)"/SCCM](#).
3. Розгорніть агент ESET Management за допомогою GPO або SCCM.
4. Переконайтеся, що [комп'ютери клієнта](#) додано в ESET PROTECT.
5. [Розгорніть і активуйте ESET Endpoint Antivirus на клієнтських комп'ютерах](#).

i Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Розгортання ESET Management Agent за допомогою SCCM або GPO](#)
- [Розгортання ESET Management Agent за допомогою об'єкта групової політики \(GPO\)](#)

Некерована процедура

Для некерованих комп'ютерів ESET Endpoint Antivirus можна розгорнути безпосередньо на робочих станціях клієнта. Таке розгортання не рекомендується, оскільки ви не зможете відстежувати й примусово застосовувати політики для всіх продуктів ESET Endpoint на робочих станціях.

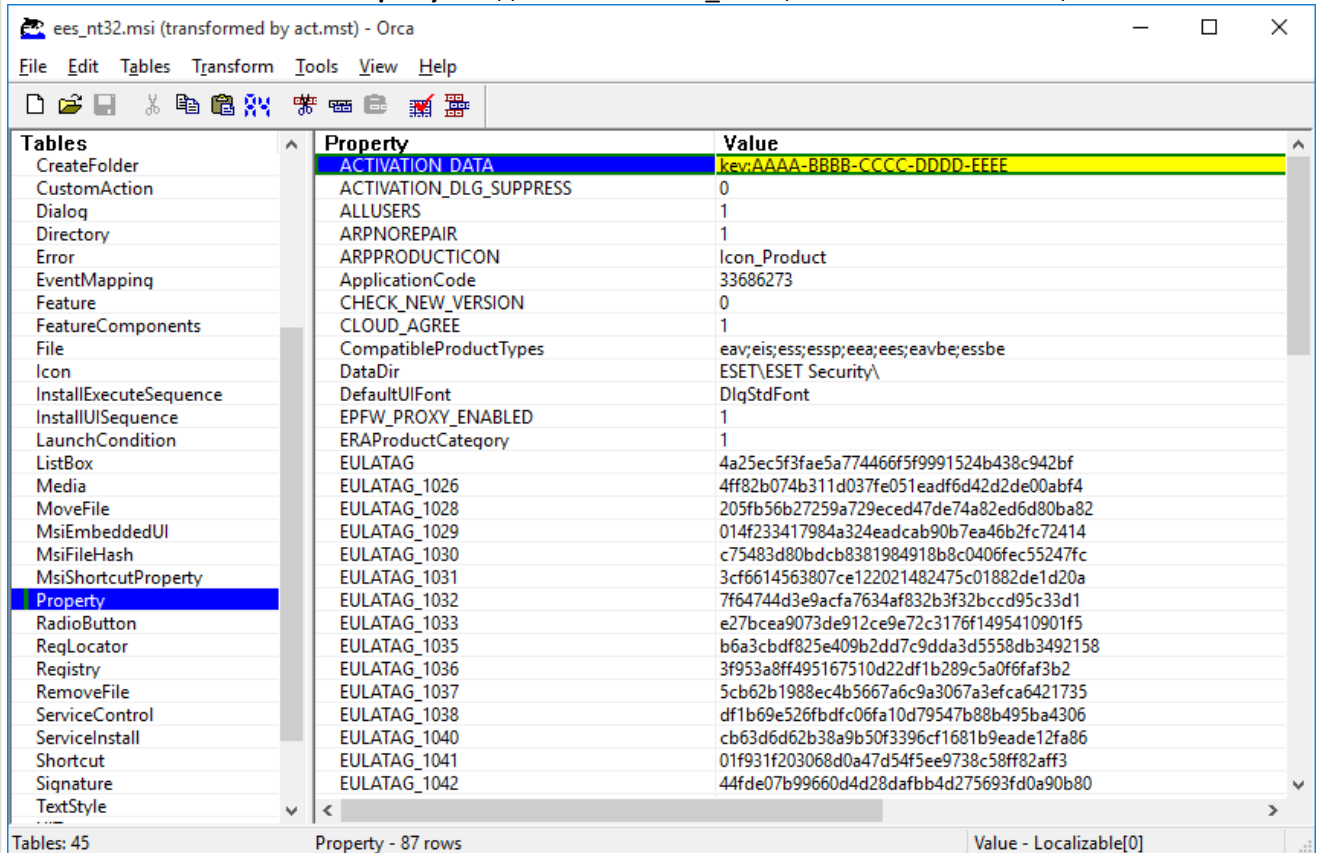
За замовчуванням ESET Endpoint Antivirus не активується після інсталяції, а відтак він не працює.

Варіант 1 (інсталяція програми)

1. [Завантажте MSI-файл інстальатора](#) для ESET Endpoint Antivirus.
2. Створіть пакет перетворення .mst з файлу .msi (наприклад, за допомогою редактора Orca для файлів .msi), включивши до нього властивість активації продукту (див. таблицю ACTIVATION_DATA в темі [Інсталяція з використання командного рядка](#)).

☐ [Показати покрокову інструкцію зі створення пакета .mst в Orca](#)

1. Відкрити Orca.
2. Завантажте інсталятор .msi. Для цього клацніть **File > Open**.
3. Клацніть **Transform > New Transform**.
4. Клацніть **Property** в розділі **Tables**, а потім виберіть **Tables > Add row**.
5. У вікні **Add Row** в полі **Property** введіть **ACTIVATION_DATA**, а в полі **Value** — ліцензійний ключ.



6. Збережіть файл .mst. Для цього клацніть **Перетворення > Сформувати перетворення**.

1. Необов'язкова: Для [імпорту](#) налаштовуваного файлу конфігурації .xml продукту ESET Endpoint Antivirus (наприклад, якщо потрібно увімкнути RMM або налаштувати параметри проксі-сервера), помістіть файл cfg.xml в одному місці з інсталятором .msi.
2. Віддалено розгорніть інсталятор .msi із файлом .mst за допомогою GPO (інсталяція програми) або SCCM.

Варіант 2 (із використанням запланованого завдання)

1. [Завантажте MSI-файл інсталятора](#) для ESET Endpoint Antivirus.
2. Додайте властивість активації продукту в сценарій [Інсталяція з використанням командного рядка](#) (див. таблицю **ACTIVATION_DATA**).
3. Зробіть інсталятор .msi і сценарій .cmd доступними в мережі для всіх робочих станцій.
4. Необов'язкова: Для [імпорту](#) налаштовуваного файлу конфігурації .xml продукту ESET Endpoint Antivirus (наприклад, якщо потрібно увімкнути RMM або налаштувати параметри проксі-сервера), помістіть файл cfg.xml в одному місці з інсталятором .msi.
5. Застосуйте підготовлений сценарій командного рядка за допомогою GPO або SCCM.
 - Якщо використовується інструмент "Об'єкт групової політики (GPO)", виберіть "Group Policy Preferences (Налаштування групової політики)" > "Group Policy Schedule Tasks (Завдання розкладу групової політики)" > "Immediate task (Негайне завдання)"

i Якщо ви не бажаєте використовувати ESET PROTECT для віддаленого керування продуктами ESET Endpoint, у ESET Endpoint Antivirus є плагін ESET для RMM, який дозволяє здійснювати нагляд за програмними системами й контролювати їх у локально інстальованому агенті, який доступний для постачальника служби керування.

- [Пошук більш докладних відомостей](#)

Оновлення до останньої версії

Нові версії ESET Endpoint Antivirus містять програмні вдосконалення й виправлення помилок, які не можна усунути під час автоматичного оновлення програмних модулів.

Оновити програму до новішої версії можна кількома способами:

1. Автоматично за допомогою ESET PROTECT або ESET PROTECT Cloud. Продуктом ESET Endpoint Antivirus версії 9 не можна керувати за допомогою ESET Remote Administrator.
2. Автоматично [за допомогою об'єкта групової політики \(GPO\) або SCCM](#).
3. Автоматично, за допомогою оновлення програми.
Оновлення програми надсилаються всім без винятку користувачам і можуть впливати на певні системні конфігурації. Тому оновлення стають доступними лише після тривалого тестування: це гарантує, що програма належним чином працюватиме з усіма можливими системними конфігураціями. Якщо ви хочете інстальувати новішу версію відразу після її випуску, скористайтесь одним із наведених нижче методів.
Переконайтеся, що **режим оновлення** ввімкнено в розділі **Додаткові параметри (F5) > Оновити > Профілі > Оновлення продукту**.
4. Уручну, завантаживши й [інстальовавши новішу версію](#) поверх попередньої.

Рекомендовані сценарії оновлення

Я керую або хочу керувати продуктами ESET віддалено

Якщо під вашим керування більше 10 продуктів ESET Endpoint, рекомендується працювати з оновленнями за допомогою ESET PROTECT, ESET PROTECT Cloud.

Більш докладну інформацію див. в наведеній нижче документації:

- [ESET PROTECT | Оновлення програмних продуктів ESET із використанням завдання клієнта](#)
- [ESET PROTECT | Посібник для організацій малого й середнього бізнесу, які керують продуктами ESET Endpoint для Windows у кількості до 250](#)
- [Загальний опис ESET PROTECT Cloud](#)

Ручне оновлення на робочій станції клієнта

Не інстальуйте версію 9 поверх версії 4.x або старого/неробочого продукту ESET Endpoint Antivirus версії 5.x або 6.x.

Якщо ви плануєте працювати з оновленнями на окремих клієнтських робочих станціях уручну.

1. Перевірте, чи ваша операційна система [підтримується](#) (Windows Vista і Windows XP не підтримується для версії).

2. Завантажте й [інсталюйте більш актуальну версію](#), ніж попередня.

Щоб максимально підвищити ймовірність успішного оновлення до [останньої версії 9.x](#), виконайте оновлення з однієї з таких версій ESET Endpoint Antivirus:



- 5.0.2272.x
- 6.5.2132.x
- 7.3.2044.x

В іншому разі спочатку видаліть ESET Endpoint Antivirus. Додаткову інформацію про оновлення ESET Endpoint Antivirus на робочій станції клієнта див. у цій [статті бази знань ESET](#).

Оновлення безпеки й стабільності

Оновлення ESET Endpoint Antivirus — це важлива складова для забезпечення повного захисту від шкідливого програмного коду. У кожній новій версії ESET Endpoint Antivirus є низка вдосконалень або виправлень помилок. Наполегливо рекомендуємо періодично оновлювати ESET Endpoint Antivirus, щоб забезпечити захист від загроз. Продукт ESET Endpoint Antivirus є на певному етапі життєвого циклу (як і інші продукти ESET).

Докладніше про:



[Політика щодо життєвого циклу \(продукти для бізнесу\)](#)

[Оновлення продукту](#)

[Поточні виправлення безпеки й стабільності](#)

Додаткову інформацію про зміни в ESET Endpoint Antivirus див. в [статті бази знань ESET](#).



Автоматичні оновлення забезпечують максимальну безпеку й стабільність роботи вашого продукту. Неможливо вимкнути оновлення безпеки й стабільності.

Поширені проблеми під час інсталяції

Якщо під час інсталяції виникають проблеми, шукайте спосіб їх вирішення у списку [поширених проблем під час інсталяції та їх рішень](#).

Помилка активації

Якщо не вдалося активувати продукт ESET Endpoint Antivirus, скористайтеся одним із таких найбільш поширених сценаріїв:

- Ліцензійний ключ уже використовується.
- Недійсний ліцензійний ключ. Помилка форми активації продукту.
- Додаткова інформація, потрібна для активації, відсутня або недійсна.
- Помилка зв'язку з базою даних активації. Повторіть спробу через 15 хвилин.
- Відсутнє або вимкнене підключення до серверів активації ESET

Переконайтеся, що ви ввели правильний ліцензійний ключ або додали дійсну автономну ліцензію. Після цього повторіть пробу.

Якщо вам не вдається активувати продукт, у нашому інформаційному пакеті ви знайдете докладні відомості щодо поширених проблем, помилок, проблем з активацією й ліцензуванням

(пакет доступний англійською й деякими іншими мовами).

- [Запустити виправлення неполадок продукту ESET](#)

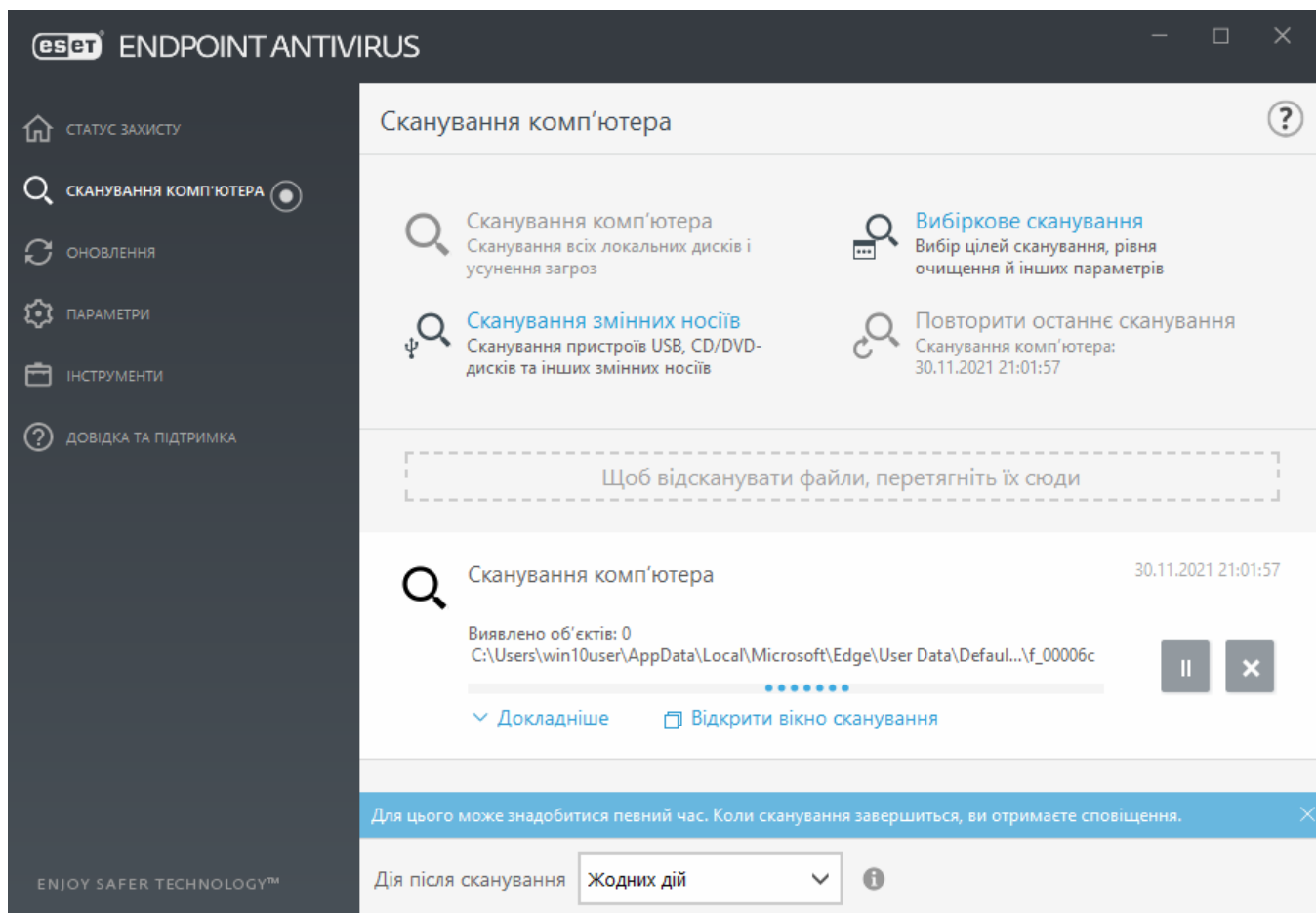
Активация продукту

Після завершення інсталяції з'явиться запит на активацію продукту.

Виберіть один із доступних способів, щоб активувати ESET Endpoint Antivirus. Докладніше див. у розділі [Активация ESET Endpoint Antivirus](#).

Сканування комп'ютера

Рекомендується вручну виконувати регулярне сканування комп'ютера або [запланувати регулярне сканування](#) на наявність загроз. У головному меню програми натисніть **Сканування комп'ютера**, після чого натисніть **Сканування комп'ютера**. Докладніші відомості про сканування комп'ютера див. у розділі [Сканування комп'ютера](#).



Посібник для початківців

У цьому розділі наведено загальний опис продукту ESET Endpoint Antivirus та його основних параметрів.

Інтерфейс користувача

Головне вікно ESET Endpoint Antivirus розділено на дві основні частини. В основному вікні, що праворуч, відображається інформація, яка відповідає вибраній у головному меню зліва опції.

Нижче наведено опис опцій головного меню.

Статус захисту: надає інформацію про статус захисту ESET Endpoint Antivirus.

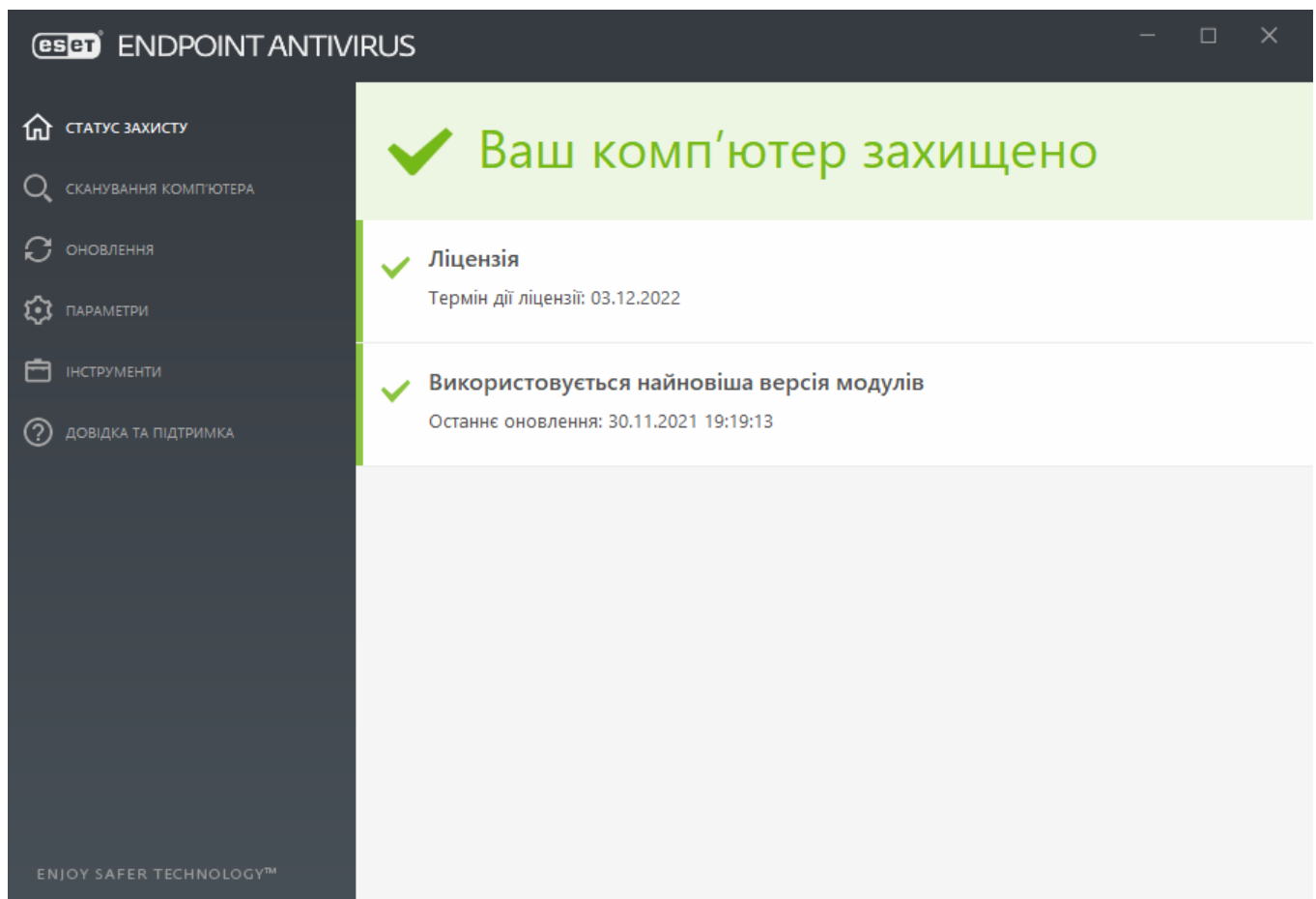
Сканування комп'ютера: за допомогою цього параметра можна налаштувати й запустити сканування комп'ютера, налаштувати вибіркове сканування або сканування змінних носіїв. Також можна повторити останнє сканування, що виконувалося.

Оновлення: відображає інформацію про обробник виявлення й дозволяє вручну перевірити наявність оновлень.

Параметри: скористайтеся цією опцією, щоб налаштувати захист комп'ютера або доступу до Інтернету й електронної пошти.

Інструменти: надає доступ до розділів "Файли журналу", "Статистика захисту", "Перегляд активності", "Запущені процеси", "Розклад", "Карантин", ESET SysInspector та ESET SysRescue для створення відновлювального компакт-диска. Також можна надіслати файл на аналіз.

Довідка та підтримка: надає доступ до файлів довідки, [бази знань ESET](#) і веб-сайту компанії ESET. Також доступні посилання на створення запиту до служби технічної підтримки, інструменти підтримки й інформацію щодо активації продукту.

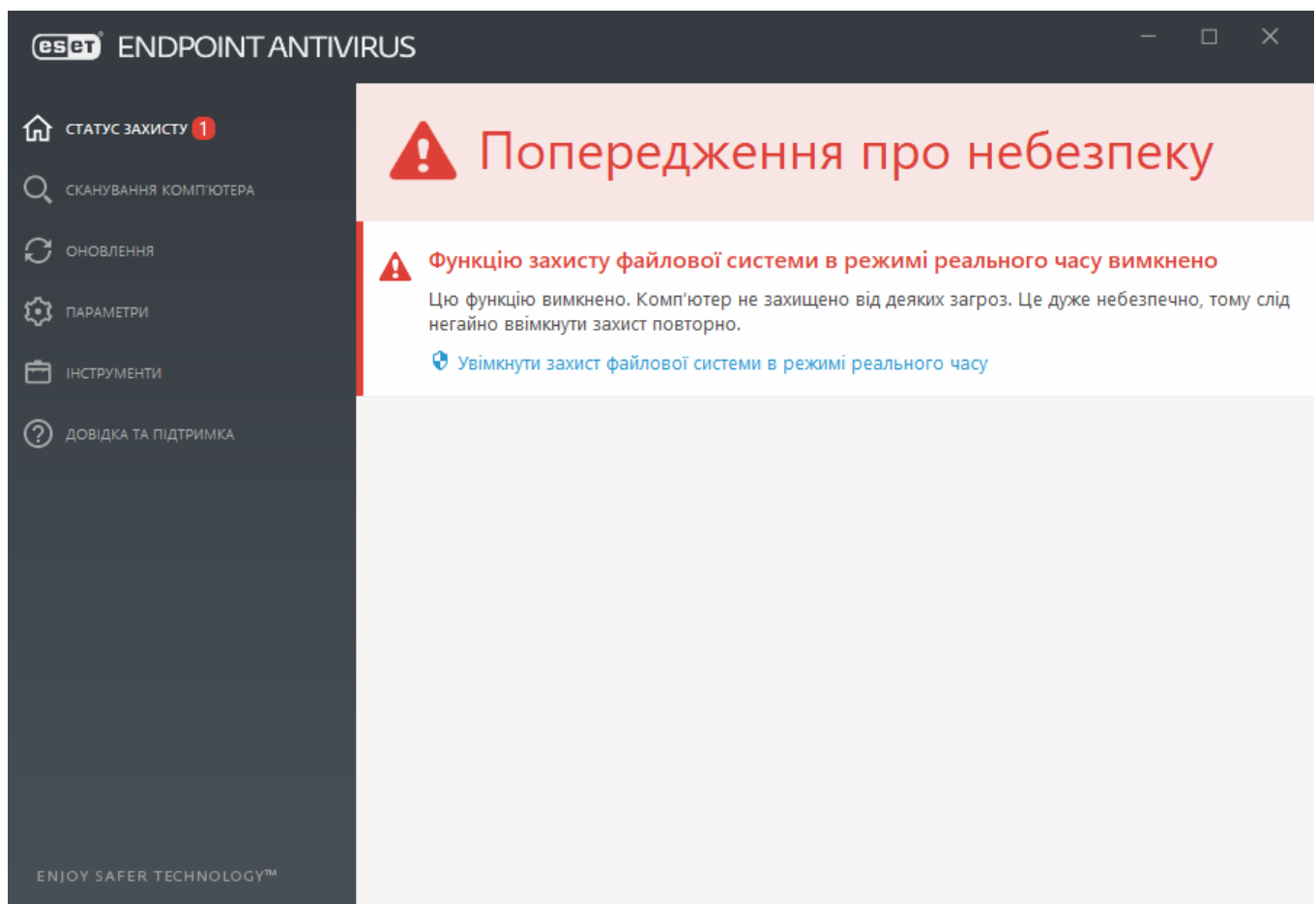


На сторінці **Статус захисту** міститься інформація про рівень безпеки та поточний захист комп'ютера. Зелений статус **Максимальний захист** указує на те, що система максимально захищена.

Вікно статусу також містить короткі посилання на часто використовувані функції програми ESET Endpoint Antivirus й інформацію про останнє оновлення.

Якщо програма не працює належним чином

Поруч з усіма повністю функціональними модулями програми відображатиметься зелена позначка. Якщо на модуль потрібно звернути увагу, ви побачите червоний знак оклику або оранжеву піктограму сповіщення. Додаткову інформацію про модуль, включно з нашими рекомендаціями щодо відновлення його повної функціональності, наведено вгорі вікна. Щоб змінити статус модуля, натисніть **Параметри** в головному меню, після чого виберіть потрібний модуль.



Червоний знак оклику (!) указує на те, що максимальний захист вашого комп'ютера не гарантовано. Цей тип сповіщення може відображатися в наведених нижче випадках.

- **Роботу функції захисту від вірусів і шпигунських програм призупинено:** натисніть **Запустити всі модулі захисту від вірусів і шпигунських програм** на панелі **Статус захисту** або **Увімкнути захист від вірусів і шпигунських програм** на панелі **Параметри** в головному вікні програми.
- Антивірус не працює: не вдалося запустити антивірусний сканер. Більшість модулів ESET Endpoint Antivirus працюватиме з помилками.
- **Функція захисту від фішинг-атак не працює:** це пов'язано з тим, що інші необхідні

модулі програми не активовано.

- **Ядро виявлення застаріле:** ця помилка відображається після кількох невдалих спроб оновити ядро виявлення (раніше мало назву "вірусна база даних"). Рекомендується перевірити параметри оновлення. Найпоширеніша причина помилки – неправильно введені [дані автентифікації](#) чи неналежним чином налаштовані [параметри підключення](#).
- **Продукт не активовано або термін дії ліцензії завершився:** на цю проблему вказує червона піктограма статусу захисту. Після завершення терміну дії ліцензії програма не оновлюватиметься. Щоб оновити ліцензію, дотримуйтесь інструкцій, наведених у вікні тривоги.
- **Систему виявлення вторгнень (HIPS) вимкнено:** сповіщення про цю проблему з'являється, якщо вимкнути систему HIPS у меню "Додаткові параметри". негайно відновіть захист, натиснувши **Увімкнути HIPS**.
- **ESET LiveGrid® вимкнено:** сповіщення про цю проблему з'являється, якщо вимкнути ESET LiveGrid® у меню "Додаткові параметри".
- **Регулярні оновлення не заплановано:** ESET Endpoint Antivirus не перевірятиме доступність важливих оновлень і не отримуватиме їх, доки ви не заплануєте завдання оновлення.
- **Антируткіт вимкнено:** натисніть **Увімкнути антируткіт**, щоб відновити роботу функції.
- **Доступ до мережі заблоковано:** відображається в разі виклику клієнтського завдання **Ізолювати комп'ютер від мережі** цієї робочої станції з ESET PROTECT. За додатковою інформацією зверніться до системного адміністратора.
- **Функцію захисту файлової системи в режимі реального часу призупинено:** захист у режимі реального часу вимкнено користувачем. Ваш комп'ютер не захищено від загроз. Натисніть **Увімкнути захист** у режимі реального часу, щоб відновити дію функції.



Оранжева літера "i" указує на необхідність втручання користувача для вирішення некритичної проблеми. Можливі причини:

- **Функцію захисту доступу до Інтернету вимкнено:** її можна повторно активувати, натиснувши сповіщення безпеки й вибравши параметр **Увімкнути захист доступу до Інтернету**.
- **Термін дії ліцензії завершується:** на цю проблему вказує піктограма статусу захисту зі знаком оклику. Після завершення терміну дії ліцензії програма не оновлюватиметься, а піктограма статусу захисту стане червоною.
- **Роботу функції захисту від антиспаму призупинено:** натисніть **Увімкнути захист від антиспаму**, щоб відновити дію функції.
- **Роботу функції веб-контролю призупинено:** натисніть **Увімкнути веб-контроль, щоб відновити дію функції**.
- **Заміщення політики активовано:** конфігурацію, установлену політикою, тимчасово заміщено (можливо, доки не буде виправлено неполадки). Лише авторизований користувач може замістити параметри політики. Докладнішу інформацію наведено в розділі [Режим заміщення](#).
- **Роботу функції контролю пристроїв призупинено:** натисніть **Увімкнути контроль пристроїв**, щоб відновити дію функції.

Інформацію щодо налаштування внутрішніх статусів видимості на першій вкладці ESET Endpoint Antivirus див. в розділі [Статуси програм](#).

Якщо вирішити проблему за допомогою наведених рекомендацій не вдається, клацніть **Довідка та підтримка**, щоб перейти до файлів довідки, або виконайте пошук у [базі знань](#)

[ESET](#). Якщо вам усе одно потрібна допомога, зверніться до служби підтримки. Спеціалісти служби технічної підтримки ESET швидко нададуть відповідь на ваші запитання й допоможуть знайти спосіб вирішення проблеми.

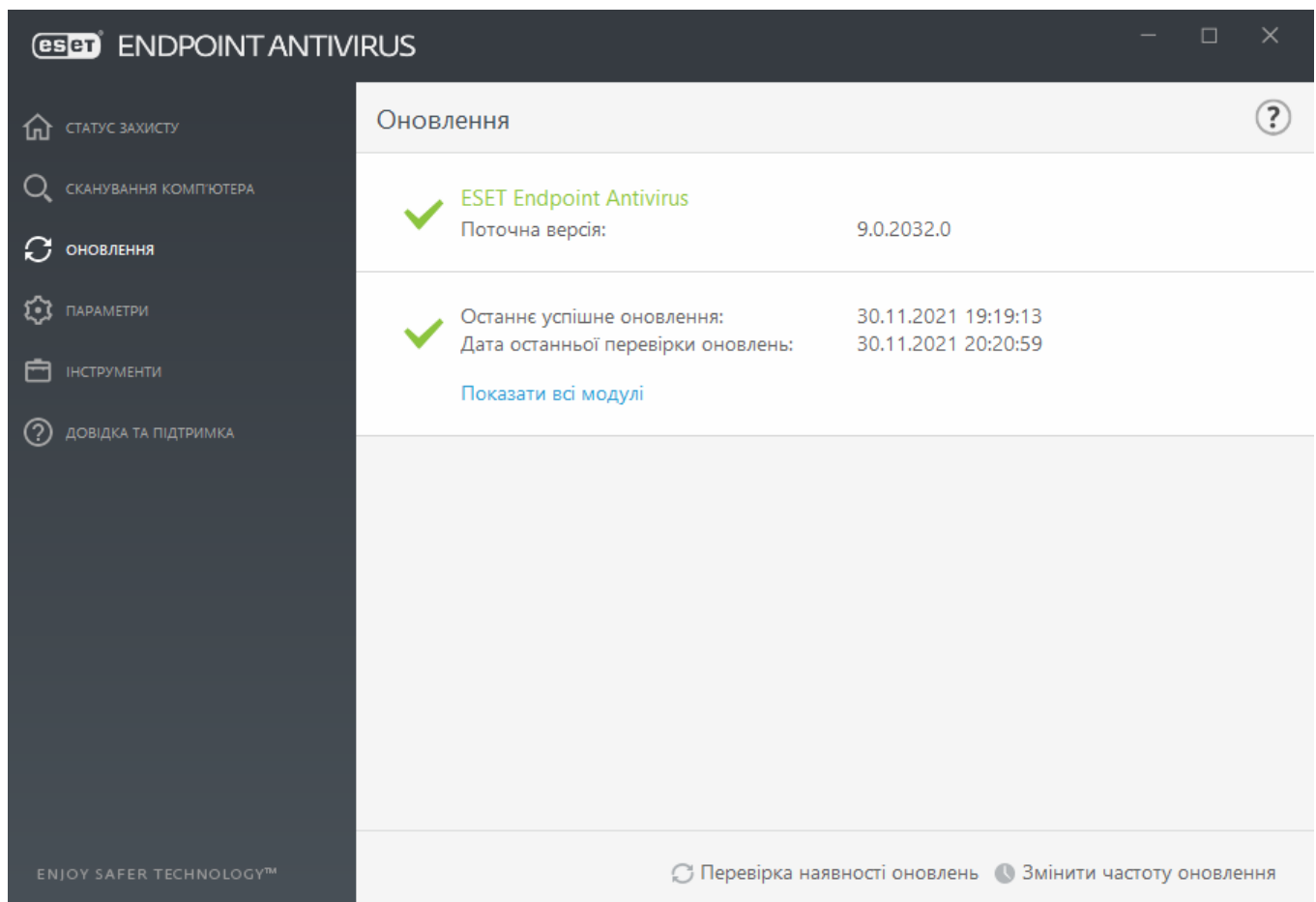
i Якщо статус стосується функції, яку заблоковано політикою ESET PROTECT, посилання не можна буде натиснути.

Параметри оновлення

Своєчасне оновлення модулів є важливим фактором для ефективного захисту від шкідливого коду. Особливу увагу слід приділити оновленню конфігурації та роботі цієї функції. Щоб перевірити наявність оновлень для модулів, у головному меню виберіть **Оновлення** >

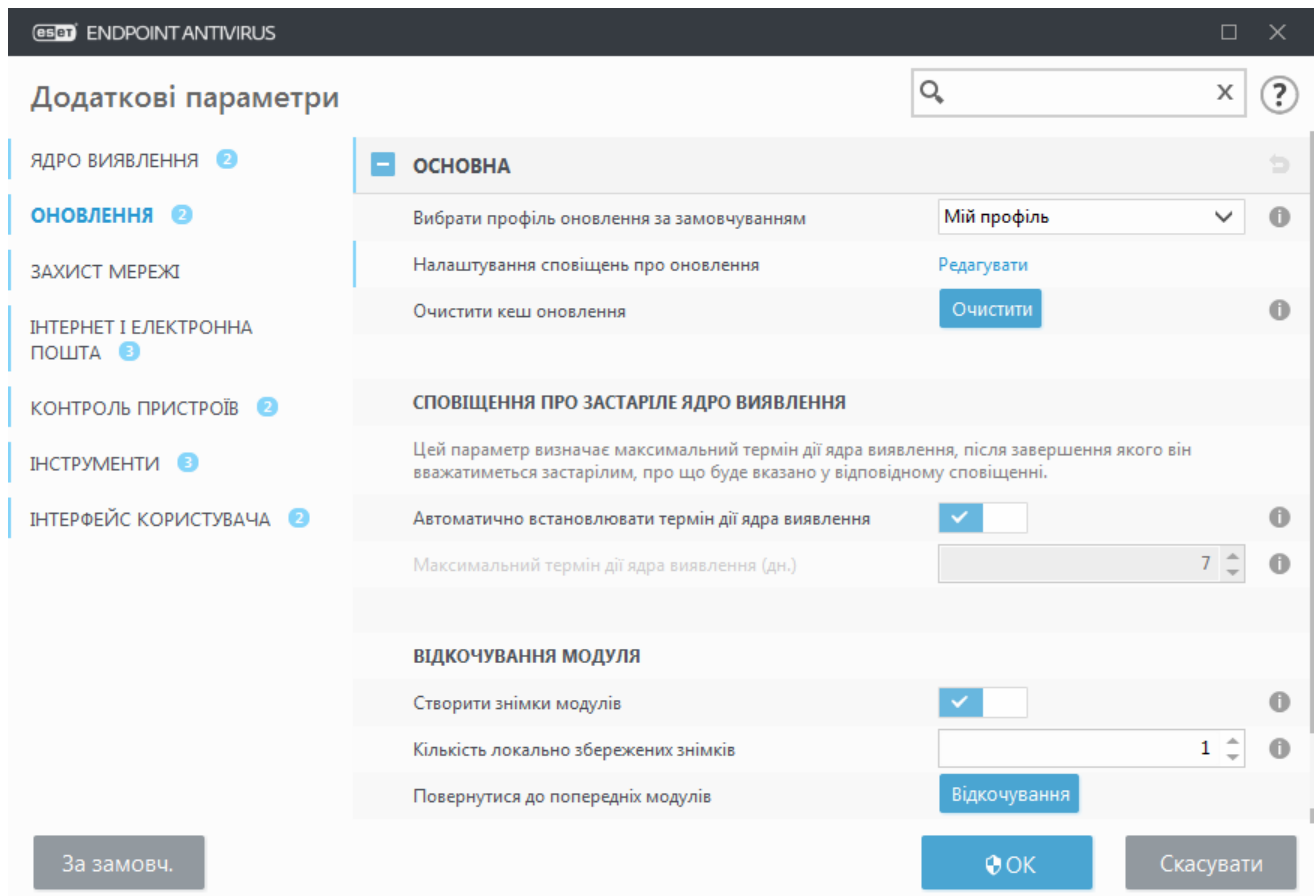
Перевірити наявність оновлень.

Якщо **Ліцензійний ключ** ще не введено, ви не отримуватимете оновлення, доки не активуєте продукт за відповідним запитом.



Вікно "Додаткові параметри" (в головному меню виберіть **Параметри** > **Додаткові параметри** або натисніть **F5** на клавіатурі) містить додаткові параметри оновлення. Щоб налаштувати їх (наприклад, режим оновлення, доступ до проксі-сервера, підключення до локальної мережі, параметри створення копії ядра виявлення тощо), у дереві "Додаткові параметри" клацніть **Оновити**.

- Якщо виникнуть проблеми з оновленням, клацніть **Очистити** й видалить усі тимчасові файли кешу оновлення.



- За замовчуванням у меню **Профілі > Оновлення > Оновлення модулів** вибрано параметр **Автоматичний вибір**. Якщо оновлення отримуються із сервера оновлень ESET, рекомендуємо не змінювати це налаштування за замовчуванням.
- Щоб у системному треї в нижньому правому куті екрана не відображалися сповіщення про успішне оновлення, розгорніть меню **Профілі > Оновлення**, клацніть **Редагувати** біля параметра **Вибрати отримані сповіщення про оновлення** й установіть потрібні прапорці для сповіщення **Ядро виявлення успішно оновлено**.

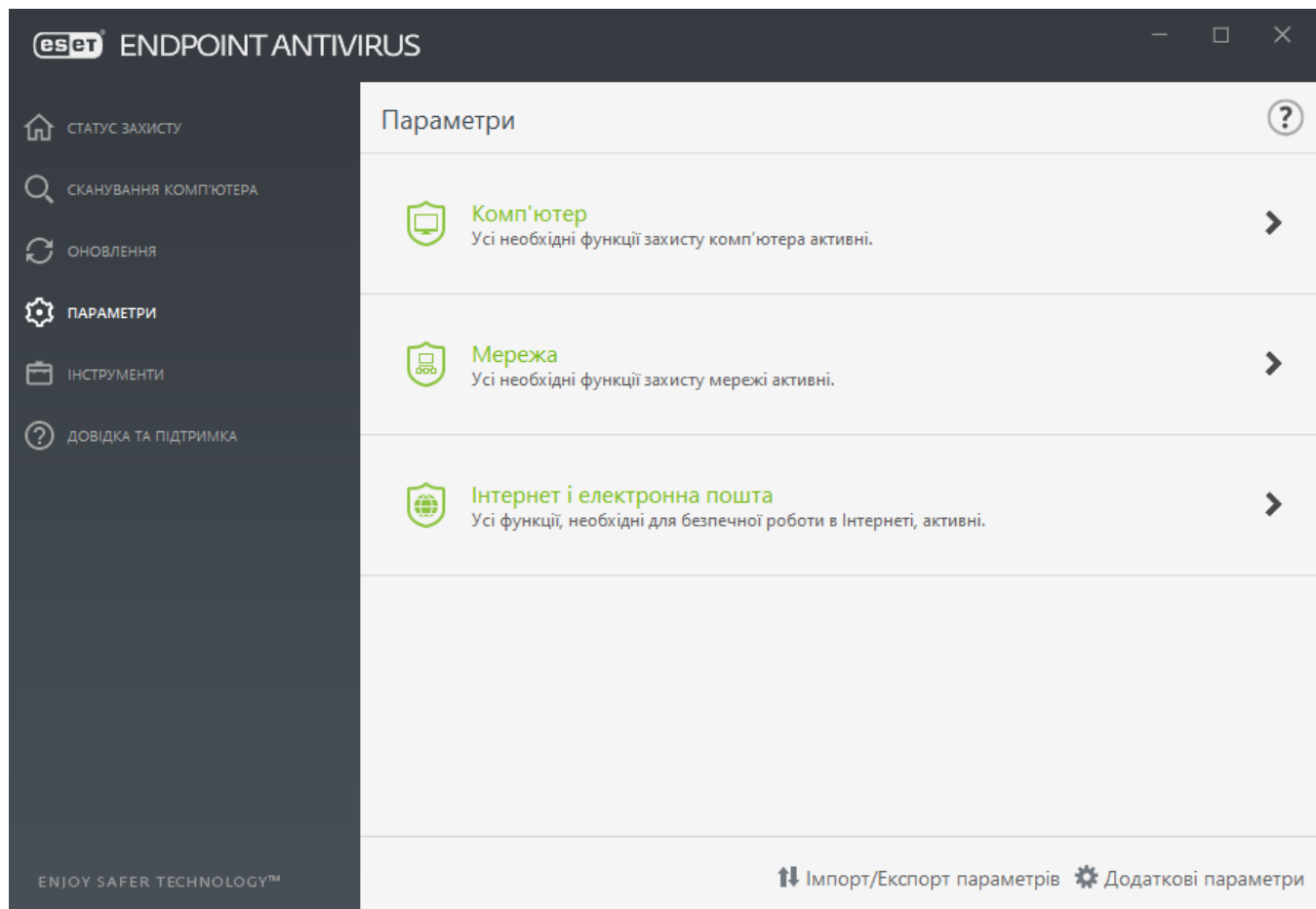
Для оптимальної роботи програми важливо, щоб вона автоматично оновлювалася. Це можливо, якщо ввести правильний **Ліцензійний ключ** у меню **Довідка та підтримка > Активувати продукт**.

Ліцензійний ключ можна ввести відразу після інсталяції або пізніше. Докладнішу інформацію див. у розділі [Активация ESET Endpoint Antivirus](#). Дані для активації, отримані із продуктом ESET, потрібно ввести у вікні **Дані ліцензії**.

Робота з ESET Endpoint Antivirus

Параметри ESET Endpoint Antivirus дають можливість відрегулювати рівень захисту комп'ютера, доступу до Інтернету й електронної пошти.

i Під час створення політики з веб-консолі ESET PROTECT можна встановити прапорець для кожного параметра. Параметри з прапорцем "Примусово" мають пріоритет, і їх не може замінити новіша політика, навіть якщо для неї також встановлено такий самий прапорець. Це гарантує, що параметр не буде змінено користувачем або замінено новішою політикою під час об'єднання. Докладнішу інформацію можна переглянути в розділі ["Прапорці" в інтерактивній довідці ESET PROTECT](#).



Меню **Параметри** містить такі опції:

- **Комп'ютер**
- **Мережа**
- **Інтернет і електронна пошта**

За допомогою параметрів захисту в розділі Комп'ютер можна ввімкнути або вимкнути такі компоненти:

- **Захист файлової системи в режимі реального часу:** усі файли перевіряються на наявність шкідливого коду під час відкриття, створення або запуску.
- **Контроль пристроїв:** дає змогу автоматично [керувати](#) носіями (CD/DVD/USB тощо). За допомогою цього модуля можна блокувати й налаштовувати розширені фільтри чи дозволи, а також контролювати доступ користувачів до пристрою та роботу з ним.
- **Host Intrusion Prevention System (HIPS):** модуль [HIPS](#) стежить за подіями в середовищі операційної системи й реагує на них відповідно до спеціально визначеного набору правил.
- **Удосконалений сканер пам'яті:** працює разом із засобом захисту від експлойтів. Він


посилює захист від зловмисного ПЗ, призначеного для обходу захисних продуктів за допомогою обфускації або шифрування. Удосконалений сканер пам'яті ввімкнено за замовчуванням. Докладніше про цей тип захисту див. в [глосарії](#).


- **Увімкнути захист від експлойтів:** служить для захисту програм, які зазвичай використовуються для зараження системи, зокрема веб-браузерів, засобів читання PDF, клієнтів електронної пошти й компонентів MS Office. Захист від експлойтів увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [глосарії](#).
- **Захист від програм-вимагачів:** це ще один засіб захисту, який включено до системи HIPS. Щоб такий тип захисту працював, потрібно мати систему перевірки репутації ESET LiveGrid®. [Докладніше про цей тип захисту можна прочитати тут](#).
- **Режим презентації:** це функція для користувачів, які не хочуть переривати робочий процес, відволікатися на спливаючі вікна й надмірно навантажувати процесор. Після ввімкнення [режиму презентації](#) відобразиться попередження (потенційна загроза для безпеки), а колір головного вікна зміниться на оранжевий.


У розділі **Мережа** можна налаштувати модуль "Захист від мережевих атак (IDS)" і модуль [захисту від ботнет-вірусів](#).


За допомогою параметрів захисту **Інтернету й електронної пошти** можна увімкнути або вимкнути наведені нижче компоненти.


- **Захист доступу до Інтернету:** якщо ввімкнено, увесь трафік, який проходить через протокол HTTP або HTTPS, сканується на наявність шкідливого програмного забезпечення.
- **Захист поштового клієнта:** контролює обмін даними через протоколи POP3 та IMAP.
- **Захист від фішинг-атак:** захищає від спроб отримання паролів, банківських даних, а також іншої конфіденційної інформації за допомогою зловмисних веб-сайтів, замаскованих під надійні.

Щоб тимчасово вимкнути окремі модулі, натисніть поруч із ними зелений перемикач . Слід пам'ятати, що це може зменшити рівень захисту комп'ютера.

Щоб повторно активувати вимкнений компонент системи безпеки, натисніть червоний перемикач .

Якщо застосовується політика ESET PROTECT, поруч з окремим компонентом відображатиметься значок замка . Після автентифікації користувач, який увійшов у систему (наприклад, адміністратор), може локально замінити політику, яку застосував ESET PROTECT. Докладніші відомості можна переглянути в [інтерактивній довідці ESET PROTECT](#).

 Усі захисні засоби, вимкнені в такий спосіб, будуть повторно активовані після перезавантаження комп'ютера.


Щоб відкрити меню додаткових параметрів певного компонента системи безпеки, клацніть значок шестерні  поруч із будь-яким компонентом.

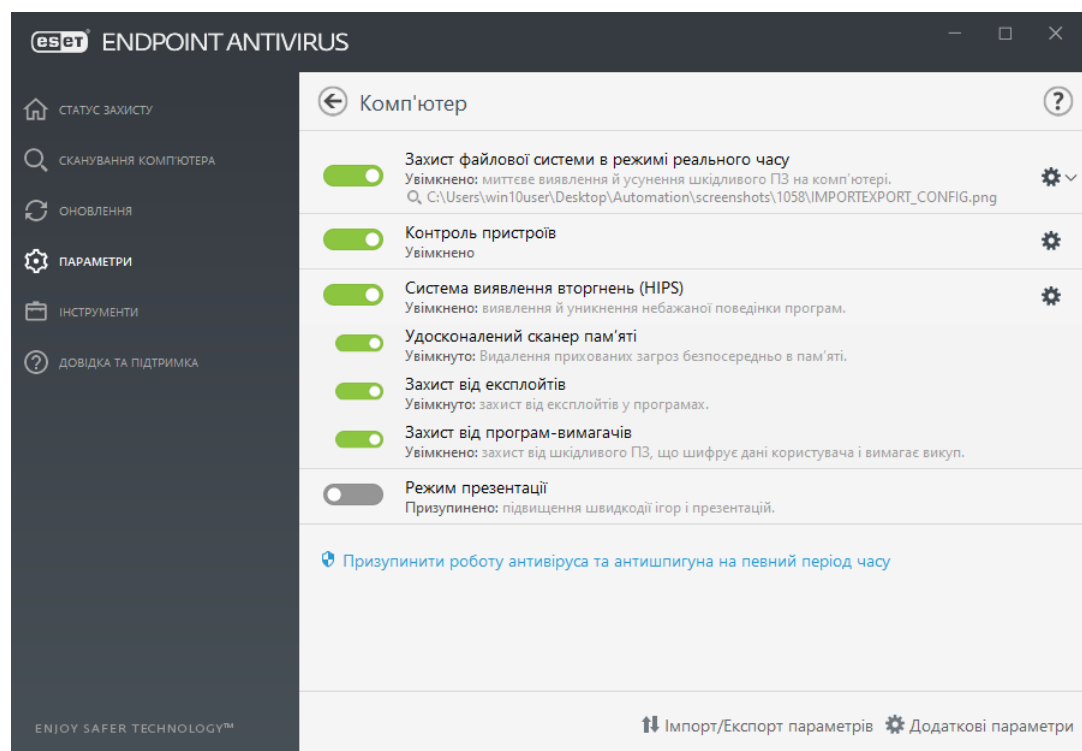
У нижній частині вікна параметрів доступні додаткові опції. Щоб завантажити параметри з файлу конфігурації у форматі *.xml* або зберегти поточні параметри в такий файл, використовуйте опцію **Параметри імпорту/експорту**. Докладнішу інформацію наведено в розділі [Параметри імпорту/експорту](#).

Розширені параметри доступні в меню **Додаткові параметри (F5)**.

Комп'ютер

Модуль **Комп'ютер** доступний у меню **Параметри > Комп'ютер**. У ньому відображаються короткі відомості про модулі захисту, описані в [попередньому розділі](#). У цьому розділі доступні наведені нижче параметри.

Натисніть значок шестерні  поруч з елементом **Захист файлової системи в режимі реального часу** й виберіть **Змінити виключення**, щоб відкрити [вікно параметрів виключень](#), у якому можна виключати файли й папки з перевірки. Щоб відкрити додаткові параметри модуля **Захист файлової системи в режимі реального часу**, натисніть **Налаштувати**.



За допомогою параметрів захисту в розділі **Комп'ютер** можна увімкнути або вимкнути такі компоненти:

- **Захист файлової системи в режимі реального часу:** усі файли перевіряються на наявність шкідливого коду під час відкриття, створення або запуску на комп'ютері.
- **Контроль пристроїв:** дає змогу автоматично [керувати](#) носіями (CD/DVD/USB тощо). За допомогою цього модуля можна блокувати й налаштовувати розширені фільтри чи дозволи, а також контролювати доступ користувачів до пристрою та роботу з ним.
- **Host Intrusion Prevention System (HIPS):** модуль [HIPS](#) стежить за подіями в середовищі операційної системи й реагує на них відповідно до спеціально визначеного набору правил.
- **Удосконалений сканер пам'яті:** працює разом із засобом захисту від експлойтів. Він посилює захист від зловмисного ПЗ, призначеного для обходу захисних продуктів за допомогою обфускації або шифрування. Удосконалений сканер пам'яті увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).
- **Увімкнути захист від експлойтів:** служить для захисту програм, які зазвичай використовуються для зараження системи, зокрема веб-браузерів, засобів читання PDF, клієнтів електронної пошти й компонентів MS Office. Захист від експлойтів увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).

- **Захист від програм-вимагачів:** це ще один засіб захисту, який включено до системи HIPS. Щоб такий тип захисту працював, потрібно мати систему перевірки репутації ESET LiveGrid®. [Докладніше про цей тип захисту можна прочитати тут](#).
- **Режим презентації:** це функція для користувачів, які не хочуть переривати робочий процес, відволікатися на спливаючі вікна й надмірно навантажувати процесор. Після увімкнення [режиму презентації](#) відобразиться попередження (потенційна загроза для безпеки), а колір головного вікна зміниться на оранжевий.

Тимчасово вимкнути антивірус та антишпигун: щоразу, коли ви тимчасово вимикаєте антивірус й антишпигун, можна вказати період часу, протягом якого вибраний компонент має бути неактивним. Для цього виберіть потрібний параметр у розкритому меню й натисніть кнопку **Застосувати**. Щоб повторно активувати захист, натисніть **Активувати антивірус та антишпигун**.

Ядро виявлення

Ядро виявлення захищає систему від зловмисних атак шляхом контролю файлів, повідомлень електронної пошти й обміну даними в Інтернеті. Наприклад, якщо об'єкт класифіковано як шкідливе програмне забезпечення, запускається його виправлення. Ядро виявлення може знешкодити його: спочатку він блокується, потім очищається, видаляється або переміщується до карантину.

Щоб налаштувати параметри ядра виявлення, клацніть **Додаткові параметри** або натисніть клавішу **F5**.

У цьому розділі:

- [Категорії захисту в режимі реального часу й за допомогою машинного навчання](#)
- [Сканування шкідливого програмного забезпечення](#)
- [Налаштування звітування](#)
- [Налаштування захисту](#)
- [Рекомендації](#)

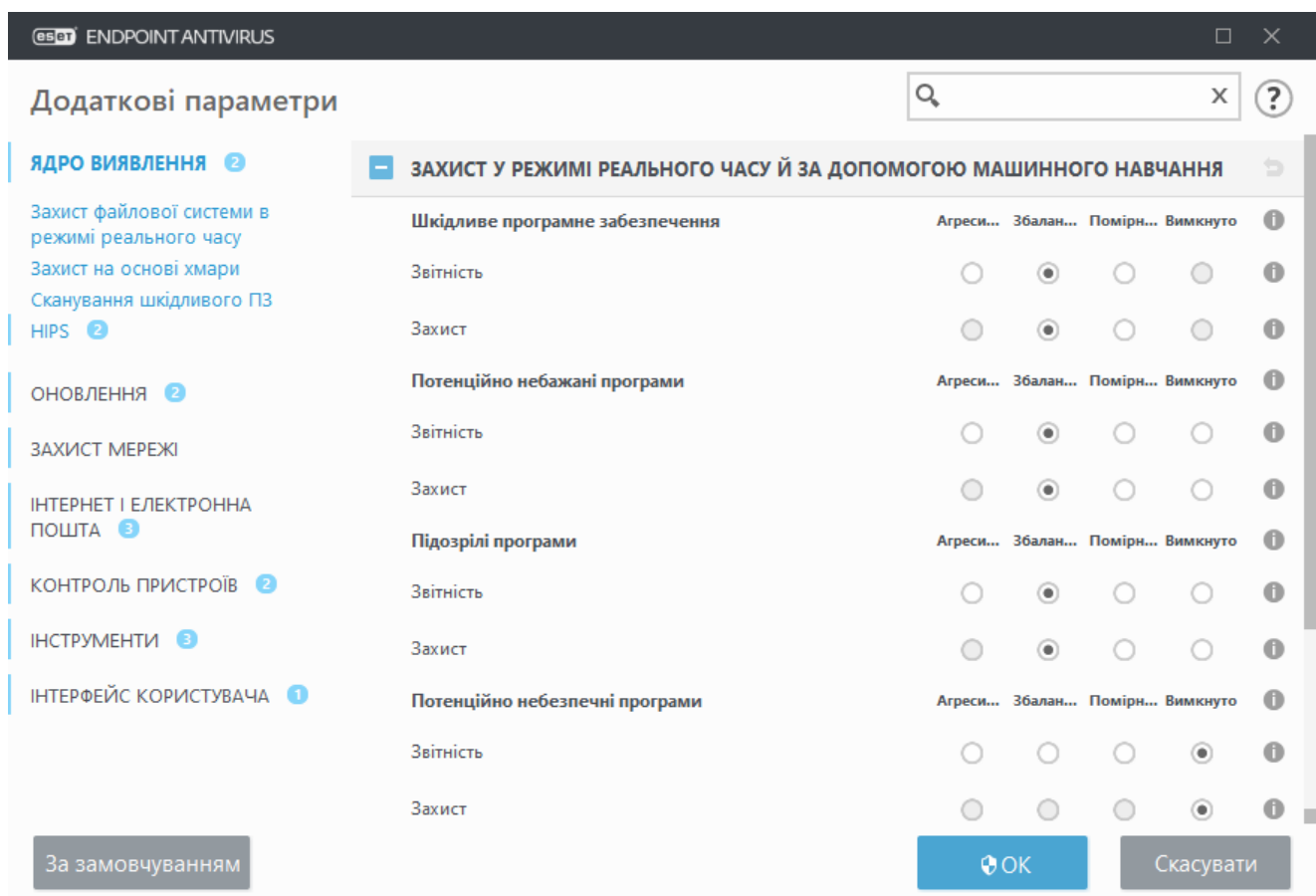


Починаючи з версії 7.2, у розділі "Ядро виявлення" більше немає перемикачів увімкнення й вимкнення, [як це було у версії 7.1 і попередніх](#). Замість кнопок увімкнення й вимкнення користувачі мають чотири порогових рівня "Агресивний", "Збалансований", "Помірний" і "Вимкнено".

Категорії захисту в режимі реального часу й за допомогою машинного навчання

Захист у реальному часі й за допомогою машинного навчання для всіх модулів захисту (наприклад, "Захист файлової системи в режимі реального часу", "Захист доступу до інтернету" тощо) дозволяє налаштувати рівні звітування й захисту для наведених нижче категорій:

- **Шкідливе програмне забезпечення** (вірус) — це певний шкідливий код, який додається на початок або кінець коду наявних файлів на комп'ютері. Проте, термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення (шкідливі програми)". Виявлення шкідливого програмного забезпечення здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Докладніше про ці типи програм див. в [гlossарії](#).
- **Потенційно небажані програми**: умовно шкідливе ПО або потенційно небажані програми (PUA, Potentially Unwanted Application) — це широка категорія програмного забезпечення, яке не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни. Ці програми можуть інсталиувати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним. Докладніше про ці типи програм див. в [гlossарії](#).
- **Потенційно небезпечні програми** – комерційне легальне програмне забезпечення, що може використовуватися для зловмисних цілей. До потенційно небезпечних програм належать інструменти віддаленого доступу, програми для зламу паролів і клавіатурні шпигуни (програми, які записують кожне натискання клавіш, зроблене користувачем). Докладніше про ці типи програм див. в [гlossарії](#).
- **Підозрілі програми** – це програми, стиснуті [пакувальниками](#) або протекторами. Зловмисники часто використовують такі типи захисту, щоб запобігти виявленню шкідливого програмного забезпечення.



i У ядрі виявлення тепер впроваджено розширене машинне навчання — удосконалений рівень захисту, який покращує виявлення на основі машинного навчання. Докладніше про цей тип захисту див. в [гlossарії](#).

Сканування шкідливого програмного забезпечення

Параметри сканера можна налаштувати окремо від параметрів сканування в реальному часі й [сканування за вимогою](#). За замовчуванням увімкнено параметр **Використовувати параметри захисту в режимі реального часу**. Коли цей параметр увімкнено, відповідні параметри сканування за вимогою успадковуються з розділу **Захист у реальному часі й на основі машинного навчання**.

Налаштування звітування

Коли виявлено певний об'єкт (наприклад, знайдено загрозу, класифіковану як шкідливе програмне забезпечення), інформація про це записується в [журнал виявлених об'єктів](#), а на робочому столі з'являються [сповіщення](#), якщо це налаштовано в ESET Endpoint Antivirus.

Пороговий рівень звітування налаштовується для кожної з таких категорій (далі — КАТЕГОРІЯ):

1. Шкідливе програмне забезпечення
2. Потенційно небажані програми
3. Потенційно небезпечні програми
4. Підозрілі програми

Операції звітування виконуються ядром виявлення, зокрема й компонентом машинного навчання. Можна задати більш високий поріг звітування, ніж поточний поріг [захисту](#). Ці параметри звітування не впливають на блокування, [очищення](#) чи видалення [об'єктів](#).

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) звітування для КАТЕГОРІЇ:

Поріг	Пояснення
Агресивний	Для звітування про КАТЕГОРІЮ налаштована максимальна чутливість. Програма буде повідомляти про більшу кількість виявлених об'єктів. Використання параметрів рівня Агресивний може призвести до помилкового визначення об'єктів як таких, що належать до КАТЕГОРІЇ.
Збалансований	Для звітування про КАТЕГОРІЮ налаштовано збалансований рівень. Цей параметр дає змогу збалансувати продуктивність і точність виявлення й кількість помилково визначених об'єктів.
Помірний	Для звітування про КАТЕГОРІЮ налаштовано мінімізацію кількості помилково визначених об'єктів зі збереженням достатнього рівня захисту. Об'єкти реєструються тільки тоді, коли ймовірність очевидна й відповідає поведінці КАТЕГОРІЇ.

Поріг	Пояснення
Вимкнено	Звітування про КАТЕГОРІЮ не активовано. Пошук (очищення) об'єктів цього типу не виконується. У результаті цей параметр вимикає захист від об'єктів цього типу. Параметр "Вимкнено" недоступний для звітування про шкідливе програмне забезпечення; його встановлено за замовчуванням для потенційно небезпечних програм.

Доступність модулів захисту ESET Endpoint Antivirus

Нижче наведено інформацію про доступність модуля захисту (увімкнено або вимкнено) модуля захисту для вибраного порога КАТЕГОРІЇ:

	Агресивний	Збалансований	Помірний	Вимкнено**
Модуль розширеного машинного навчання*	✓ (агресивний режим)	✓ (консервативний режим)	X	X
модуль ядра виявлення	✓	✓	✓	X
Інші модулі захисту	✓	✓	✓	X

* Доступно в ESET Endpoint Antivirus версії 7.2 й новіших.

** Не рекомендовано

Визначення версії продукту, версій модуля продукту й дат збірки

1. Клацніть **Довідка та підтримка > Про програму ESET Endpoint Antivirus**.
2. На екрані **Про програму** в першому рядку тексту відображається номер версії вашого продукту ESET.
3. Клацніть **Показати модулі**, щоб отримати доступ до інформації про певні модулі.

Тези

Наводимо кілька тез щодо налаштування відповідного порогового рівня для вашого середовища:

- Поріг **Збалансований** рекомендується для більшості налаштувань.
- Поріг **Помірний** відповідає рівню захисту в попередніх версіях ESET Endpoint Antivirus (7.1 і попередніх версій). Він рекомендується для тих середовищ, де пріоритетом є мінімізація хибно виявлених об'єктів програми безпеки.
- Що вище рівень звітування, то вище частота виявлення й імовірність хибно ідентифікувати об'єкти.
- Фактично не існує гарантії виявлення 100 % шкідливих об'єктів, як і гарантії повного уникнення неправильної категоризації нешкідливих об'єктів як шкідливих.
- [Своєчасно оновлюйте ESET Endpoint Antivirus і його модулі](#), щоб забезпечити максимально оптимальний баланс між продуктивністю й точністю виявлення та кількістю хибно виявлених об'єктів.

Налаштування захисту

Якщо повідомляється про об'єкт, віднесений до КАТЕГОРІЇ, програма захисту блокує його, а

потім [очищає](#), видаляє або переміщує його в [карантин](#).

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для захисту КАТЕГОРІЇ:

Поріг	Пояснення
Агресивний	Об'єкти, виявлені із застосуванням агресивного (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення). Цей параметр рекомендований, якщо всі кінцеві точки проскановані з використанням параметрів агресивного рівня, а помилково визначені об'єкти додані в список виключень.
Збалансований	Об'єкти, виявлені із застосуванням збалансованого (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).
Помірний	Об'єкти, виявлені із застосуванням помірного рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).
Вимкнено	Корисно для ідентифікації й виключення помилково визначених об'єктів. Параметр "Вимкнено" недоступний для захисту від шкідливого програмного забезпечення; його встановлено за замовчуванням для потенційно небезпечних програм.

☐ [Таблиця відповідності політик ESET PROTECT для ESET Endpoint Antivirus 7.1 і попередніх версій](#)

Редактор політик ESET PROTECT більше не містить перемикачів увімкнення/вимкнення для кожної категорії. У таблиці нижче наведено інформацію про відповідність порогового рівня захисту й кінцевого стану [перемикача в ESET Endpoint Antivirus 7.1 і попередніх версій](#).

Стан порогу КАТЕГОРІЇ	Агресивний	Збалансований	Помірний	Вимкнено
Застосований перемикач КАТЕГОРІЇ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> x

Після оновлення з версій 7.1 і попередніх до версії 7.2 й новіших новий стан порогових рівнів буде таким:

Перемикач категорії до оновлення	<input checked="" type="checkbox"/>	<input type="checkbox"/> x
Новий поріг КАТЕГОРІЇ після оновлення	Збалансований	Вимкнено

Рекомендації

НЕКЕРОВАНЕ СЕРЕДОВИЩЕ (окрема клієнтська робоча станція)

Не змінюйте рекомендовані значення за замовчуванням.

КЕРОВАНЕ СЕРЕДОВИЩЕ

Зазвичай ці параметри застосовуються до робочих станцій через [політику](#).

1. Початковий етап

Цей етап може тривати тиждень.

- Установіть для всіх порогів **Звітування** значення **Збалансований**.

ПРИМІТКА: За потреби встановіть значення **Агресивний**.

- Для політики **Захист** для шкідливого програмного забезпечення встановіть або збережіть рівень **Збалансований**.
- Для інших КАТЕГОРІЙ для політики **Захист** установіть значення **Помірний**.
ПРИМІТКА: На цьому етапі не рекомендується задавати політиці **Захист** пороговий рівень **Агресивний**, оскільки в цьому разі всі виявлені об'єкти (зокрема й хибно виявлені) будуть виправлені.
- Визначте хибно виявлені об'єкти в журналі [виявлень](#) і спочатку додайте їх у список [Виключення об'єктів виявлення](#).

2. Перехідний етап

- Виконайте процедури етапу впровадження на певних робочих станціях (не для всіх робочих станцій у мережі).

3. Етап упровадження

- Для всіх політик **Захист** установіть рівень **Збалансований**.
- Якщо керування здійснюється віддалено, використовуйте відповідну [попередньо визначену політику](#) антивірусу для ESET Endpoint Antivirus.
- Якщо потрібний максимально високий ступінь виявлення, а кількість хибно виявлених об'єктів не є пріоритетом, установіть рівень захисту **Агресивний**.
- Перевірте, чи всі виявлені об'єкти є в [журналі виявлення](#) або звітах ESET PROTECT.

Розширені параметри ядра виявлення

Технологія Антируткіт – це найсучасніша система виявлення небезпечних програм, наприклад [руткітів](#), здатних приховувати свою присутність у системі. Це означає, що їх неможливо виявити за допомогою звичайних методів перевірки.

Увімкнути розширену перевірку за допомогою AMSI: активувати інструмент перевірки Microsoft Antimalware Scan Interface, який надає розробникам нові засоби захисту від шкідливих програм (лише для ОС Windows 10, 11).

Дії в разі виявлення загрози

Загрози можуть проникати в систему через різні точки входу, наприклад [веб-сторінки](#), спільні папки, електронну пошту або [знімні пристрої](#) (USB, зовнішні диски, CD-диски, DVD-диски, тощо).

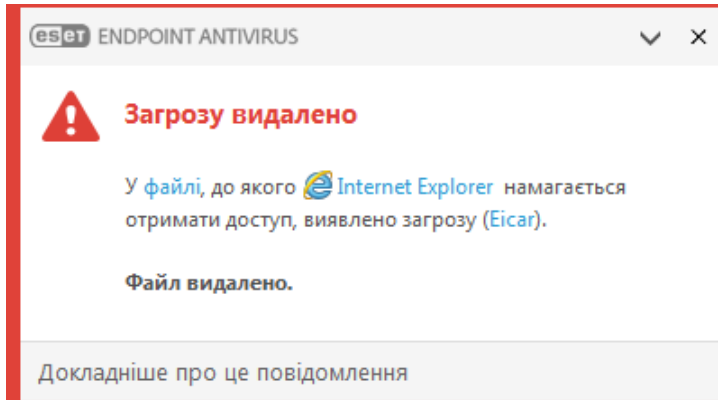
Стандартна поведінка

ESET Endpoint Antivirus захищає систему, виявляючи загрози за допомогою наведених нижче методів.

- [Захист файлової системи в режимі реального часу](#)

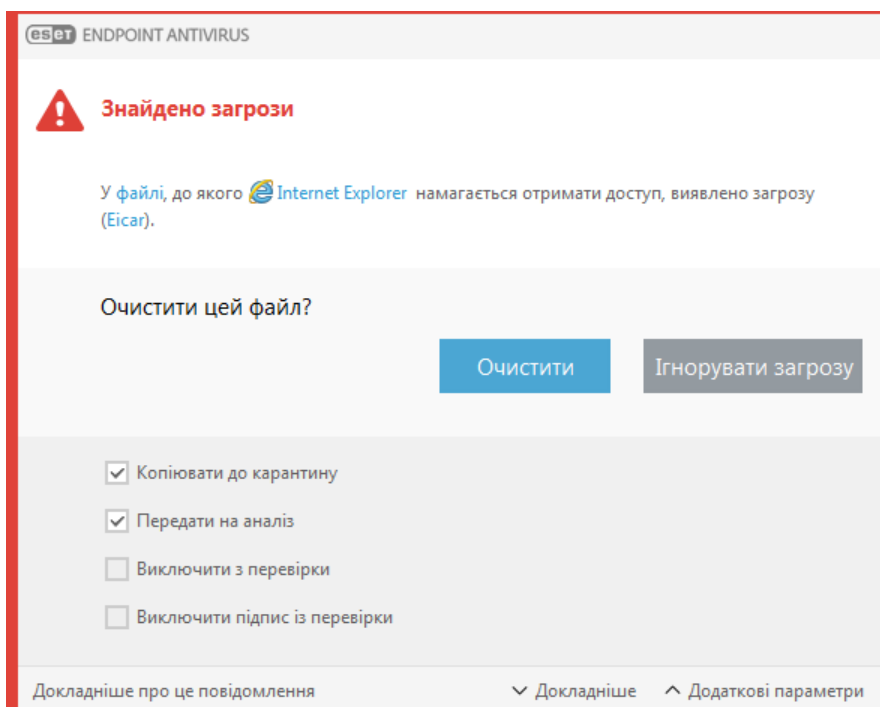
- [Захист доступу до Інтернету](#)
- [Захист поштового клієнта](#)
- [Сканування комп'ютера за вимогою](#)

Для кожного з цих параметрів використовується стандартний рівень очистки й виконується спроба видалити файл і перемістити його до [карантину](#) або перервати підключення. В області сповіщень у нижньому правому куті екрана відображається вікно сповіщень. Більш докладні відомості про виявлені/очищені об'єкти див. в розділі [Файли журналу](#). Більш докладні відомості про рівні очистки й поведінку див. в розділі [Очистка](#).



Очистка та видалення

Якщо попередньо визначеної дії для модуля захисту файлової системи в режимі реального часу немає, на екрані відобразиться вікно тривоги, у якому вам буде запропоновано вибрати дію самостійно. Зазвичай у цьому вікні доступні такі дії: **Очистити**, **Видалити** та **Пропустити**. Не рекомендується вибирати опцію **Пропустити**, оскільки в такому разі інфіковані файли залишатимуться неочищеними. Винятком є випадки, коли ви впевнені, що файл безпечний і його виявлено помилково.



Очистку слід виконувати, якщо файл атаковано вірусом, який додав до нього шкідливий код. У цьому разі спершу потрібно спробувати очистити файл, щоб повернути його до початкового

стану. Якщо файл складається виключно зі шкідливого коду, файл видаляється.

Якщо інфікований файл "заблоковано" або він використовується системним процесом, його буде видалено лише після розблокування (зазвичай після перезапуску системи).

Відновлення з карантину

Щоб відкрити карантин, у головному вікні програми ESET Endpoint Antivirus натисніть **Інструменти > Карантин**.

Файли з карантину також можна відновити й повернути до початкових місць розташування.

- Для цього натисніть правою кнопкою файл у карантині та виберіть опцію **Відновити** в контекстному меню.
- Якщо файл позначено як [потенційно небажану програму](#), доступна опція **Відновити та виключити з перевірки**. Також див. [Виключення](#).
- У контекстному меню також доступна опція **Відновити в**, за допомогою якої користувач може відновити файли в інше місце, а не туди, звідки їх було видалено.
- У деяких випадках функція відновлення недоступна, наприклад, якщо файли знаходилися на мережевому диску, доступному лише для читання.

Кілька загроз

Якщо якісь інфіковані файли не вдалось очистити під час сканування комп'ютера (або для [рівня очистки](#) вибрано значення **Без очищення**), відкривається вікно з пропозицією вибрати для них дію.

Видалення файлів з архівів

У режимі очистки за замовчуванням архів буде видалятися повністю лише в тому випадку, якщо містить виключно інфіковані файли й жодного чистого. Іншими словами, якщо архів також містить безпечні файли, він не видалятиметься. Будьте обережні, запускаючи сканування з ретельною очисткою. У ході цієї процедури архів видалятиметься, якщо в ньому виявлено принаймні один інфікований файл, незалежно від стану інших.

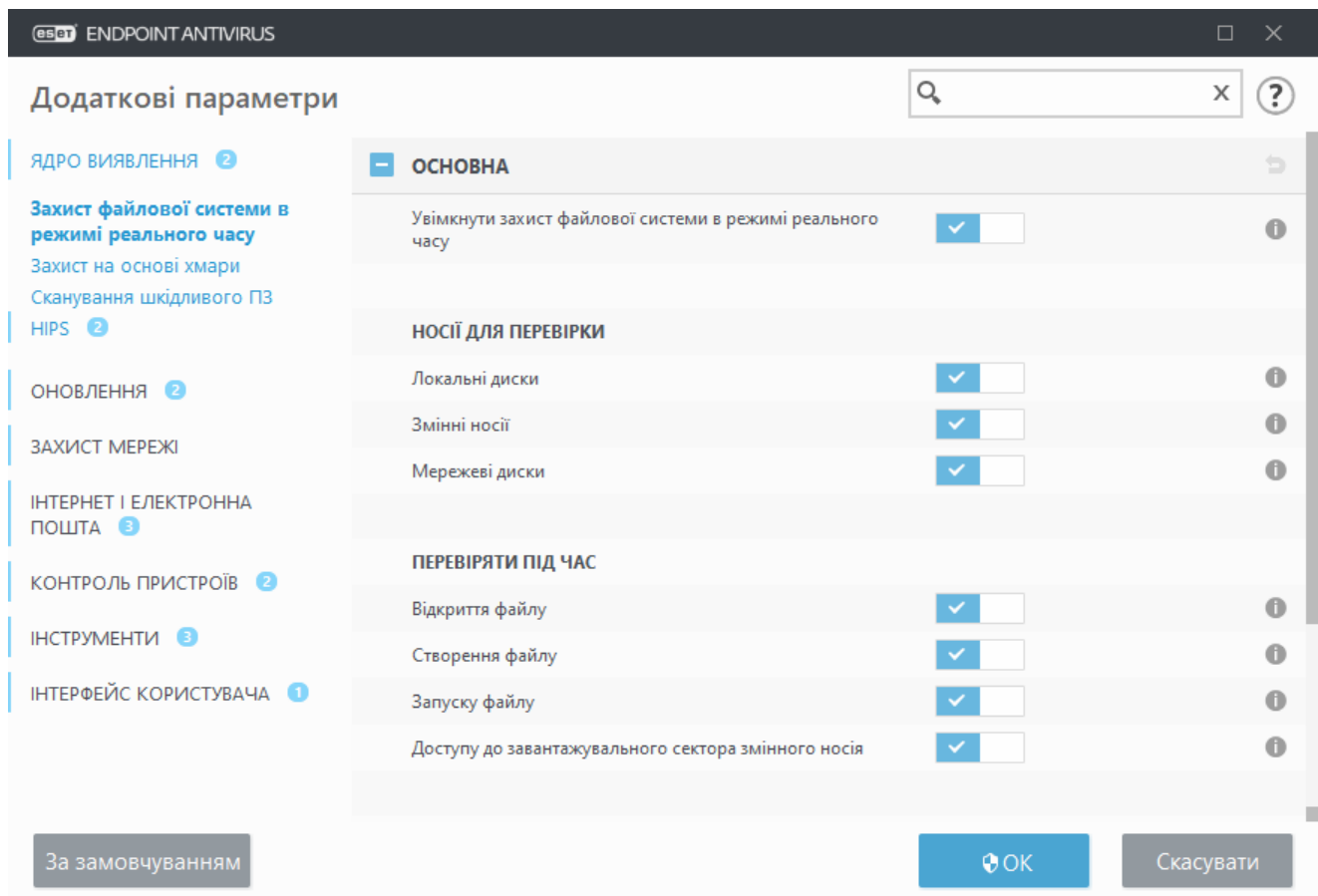
Якщо на комп'ютері спостерігаються ознаки діяльності шкідливих програм (наприклад, система працює повільніше, ніж звичайно, часто зависає тощо), рекомендується виконати наведені нижче дії.

- Відкрийте ESET Endpoint Antivirus і натисніть "Сканування комп'ютера".
- Натисніть **Smart-сканування** (докладніші відомості див. у розділі [Сканування комп'ютера](#)).
- Після завершення сканування перегляньте в журналі кількість перевірених, інфікованих і очищених файлів.

Якщо необхідно перевірити лише певну частину диска, натисніть **Вибіркова перевірка** та виберіть об'єкти для сканування на наявність вірусів.

Захист файлової системи в режимі реального часу

Функція "Захист файлової системи в режимі реального часу" контролює всі файли в системі на наявність шкідливого коду під час їх відкриття, створення або запуску.



За замовчуванням модуль захисту файлової системи в режимі реального часу запускається разом із системою та виконує безперервне сканування. Не рекомендуємо вимикати параметр **Увімкнути захист файлової системи в режимі реального часу** в меню **Додаткові параметри** (Ядро виявлення > **Захист файлової системи в режимі реального часу** > Базові).

Перевірка носіїв

За замовчуванням усі типи носіїв скануються на наявність потенційних загроз:

- **Локальні диски:** скануються всі системні й незмінні жорсткі диски (наприклад, C:\, D:\).
- **Змінний носій:** скануються CD/DVD-диски, USB-пристрої, карти пам'яті тощо
- **Мережеві диски:** скануються всі підключені мережеві диски (наприклад, H:\ як \\store04) або мережеві диски з безпосереднім доступом (наприклад, \\store08).

Рекомендується використовувати параметри за замовчуванням і змінювати їх лише у крайньому разі, наприклад, коли сканування певних носіїв значно сповільнює передачу даних.

Період перевірки

За замовчуванням усі файли скануються під час відкриття, створення або запуску. Рекомендується використовувати параметри за замовчуванням, оскільки вони забезпечують максимальний рівень захисту комп'ютера в режимі реального часу.

- **Відкриття файлу:** файли скануються під час відкриття.
- **Створення файлу:** скануються створені або змінені файли.
- **Запуск файлу:** файли скануються під час виконання або запуску.
- **Доступ до завантажувального сектора змінного носія:** під час підключення змінного носія із завантажувальним сектором до пристрою завантажувальний сектор відразу ж сканується. Цей параметр не вмикає сканування файлів на змінному носії. Щоб увімкнути сканування файлів на змінному носії, виберіть **Перевірка носіїв > Змінний носій**. Для належної роботи **доступу до завантажувального сектора на змінному носії** не вимикайте **Завантажувальні сектори/UEFI** в параметрах ThreatSense.

Процеси, виключені з перевірки : дізнайтеся більше про цей тип виключень у розділі [Виключення процесів](#).

Модуль захисту файлової системи в режимі реального часу перевіряє всі типи носіїв. Його активують різноманітні системні події, наприклад відкриття файлу. Методи виявлення загроз, які використовуються в технології ThreatSense (див. розділ [Налаштування параметрів підсистеми ThreatSense](#)), дають змогу налаштувати модуль захисту файлової системи в режимі реального часу так, щоб він діяв по-різному відносно новостворених і вже наявних файлів. Наприклад, модуль може більш ретельно аналізувати новостворені файли.

Щоб зменшити споживання системних ресурсів, уже проскановані файли повторно не перевіряються (якщо їх не було змінено). Файли скануються повторно після кожного оновлення обробника виявлення. Виконання цієї процедури контролюється за допомогою функції **Smart-оптимізація**. Якщо **Smart-оптимізацію** вимкнено, усі файли скануються щоразу, коли користувач до них звертається. Щоб змінити цей параметр, натисніть клавішу **F5** і відкрийте вікно додаткових параметрів, потім розгорніть меню **Обробник виявлення > Захист файлової системи в режимі реального часу**. Натисніть **Параметри ThreatSense > Інше** й установіть або зніміть прапорець **Увімкнути Smart-оптимізацію**.


Перевірка захисту в режимі реального часу

Щоб переконатися, що захист у режимі реального часу працює й виявляє віруси, скористайтесь тестовим файлом із сайту eicar.com. Це безпечний файл, який виявляється всіма антивірусними програмами. Файл було створено Європейським інститутом комп'ютерних антивірусних досліджень (EICAR) для тестування функціональності антивірусних програм.

Цей файл можна завантажити за посиланням <http://www.eicar.org/download/eicar.com>. Після вводу цієї URL-адреси в браузер, відкриється повідомлення про те, що загрозу було видалено.

Можливі причини для змінення конфігурації захисту в режимі реального часу

Захист файлової системи в режимі реального часу – це найголовніший модуль, від якого залежить загальна безпека системи. Змінювати його параметри завжди слід дуже обережно. Зміни до параметрів рекомендується вносити лише у виключних випадках.

Після інсталяції ESET Endpoint Antivirus усі параметри оптимізовано таким чином, щоб досягти максимального рівня безпеки користувацької системи. Щоб відновити налаштування за замовчуванням, натисніть  поруч із кожною вкладкою у вікні (**Додаткові параметри > Обробник виявлення > Захист файлової системи в режимі реального часу**).

Необхідні дії, коли не працює захист у режимі реального часу

У цьому розділі описуються проблеми, які можуть виникнути під час використання захисту в режимі реального часу, і способи їх усунення.

Захист у режимі реального часу вимкнено

Якщо захист у режимі реального часу випадково вимкнено користувачем, знову ввімкніть його. Щоб повторно активувати захист у режимі реального часу, перейдіть у меню **Параметри** в головному вікні програми й натисніть **Захист комп'ютера > Захист файлової системи в режимі реального часу**.

Якщо модуль захисту в режимі реального часу не запускається під час запуску системи, можливо, параметр **Увімкнути захист файлової системи в режимі реального часу** вимкнено. Щоб переконатися, що цю опцію ввімкнуто, перейдіть у меню **Додаткові параметри (F5)** і натисніть **Обробник виявлення > Захист файлової системи в режимі реального часу**.

Захист у режимі реального часу не виявляє й не усуває загрози

Переконайтеся, що на комп'ютері не інстальовано жодної іншої антивірусної програми. Якщо на комп'ютері інстальовано дві антивірусні програми, вони можуть конфліктувати між собою. Перш ніж установлювати ESET, рекомендується видалити із системи інші антивірусні програми.

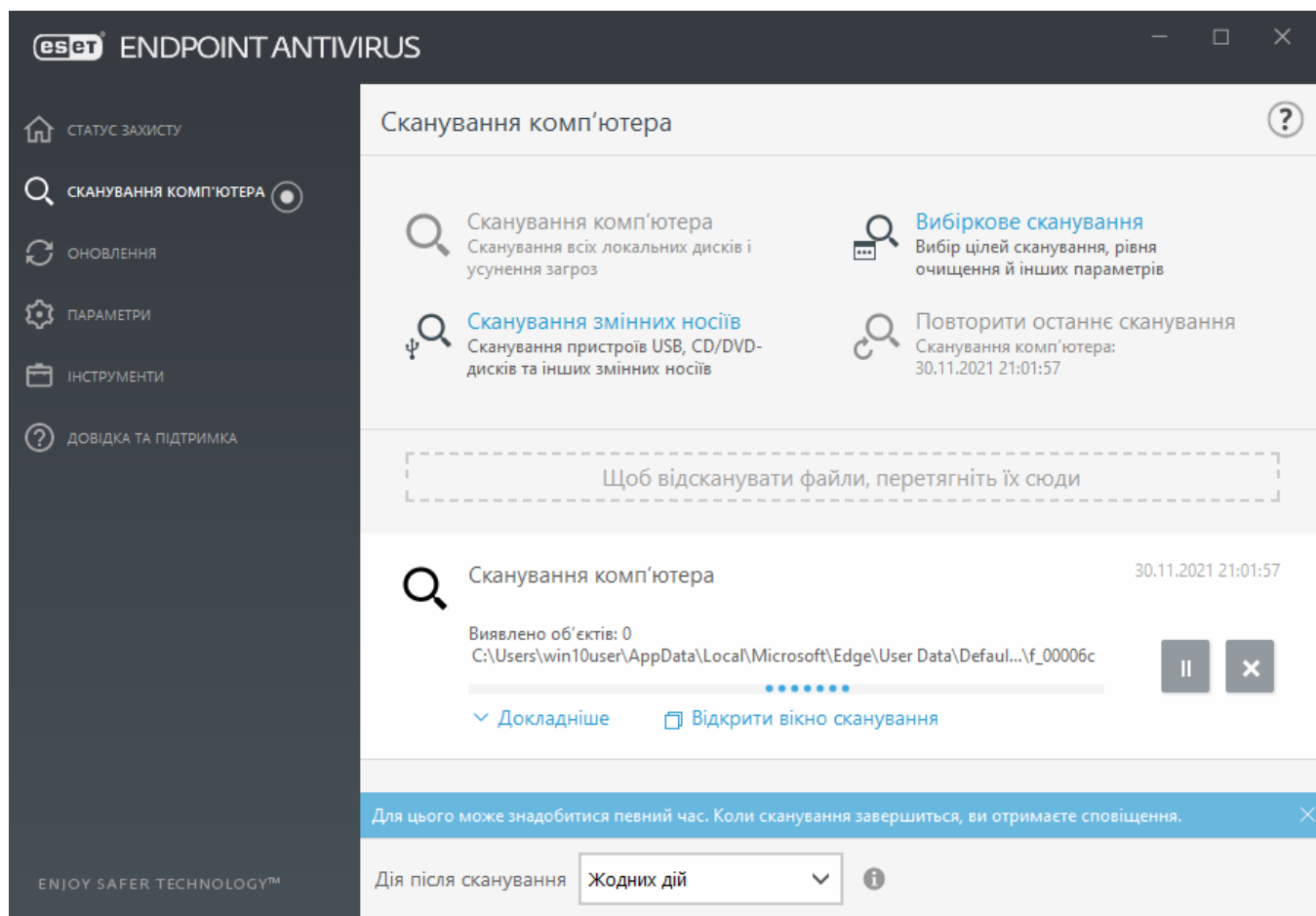
Модуль захисту в режимі реального часу не запускається

Якщо захист у режимі реального часу не активується під час запуску системи, а параметр **Увімкнути захист файлової системи в режимі реального часу** ввімкнено, можливо, має місце конфлікт з іншими програмами. Щоб отримати допомогу з вирішення цієї проблеми, зверніться до служби технічної підтримки ESET. Щоб допомогти нам у вирішенні проблеми,

створіть журнал ESET SysInspector та надішліть його до технічної підтримки ESET на аналіз. Докладніші відомості див. в [цій статті бази знань ESET](#).

Сканування комп'ютера

Сканер за вимогою – це важлива частина програми ESET Endpoint Antivirus. Він використовується для сканування файлів і папок на комп'ютері. З точки зору безпеки важливо перевіряти комп'ютер не лише в разі підозри на наявність зараження, а й регулярно в рамках превентивних заходів захисту. Рекомендується регулярно (наприклад, раз на місяць) виконувати ретельне сканування системи, щоб виявити віруси, які могли бути пропущені модулем [захисту файлової системи в режимі реального часу](#). Це могло статися, якщо в той час захист файлової системи в режимі реального часу було вимкнено, обробник виявлення застарів або файл не було класифіковано як вірус під час збереження на диск.



Доступні два типи **Сканування комп'ютера**. **Сканування комп'ютера** дозволяє швидко просканувати комп'ютер без додаткового налаштування параметрів. **Розширена перевірка** дає змогу вибрати один із попередньо заданих профілів сканування, а також конкретні об'єкти для сканування.

Додаткову інформацію про процедуру сканування див. у розділі [Хід сканування](#).

🔍 Сканування комп'ютера

Smart-сканування дає можливість швидко запустити процес сканування комп'ютера й очистити інфіковані файли без втручання користувача. Перевага Smart-сканування – простота у

використанні й відсутність необхідності визначати детальні параметри цього процесу. Під час Smart-сканування перевіряються всі файли на локальних дисках, а виявлені загрози автоматично очищаються чи видаляються. Для рівня очистки автоматично вибирається параметр за замовчуванням. Докладніше про типи очистки можна прочитати в розділі [Очистка](#).

Вибіркове сканування

Вибіркове сканування – оптимальне рішення, якщо потрібно вказати необхідні параметри сканування (наприклад, об'єкти та методи). Перевага розширеної перевірки полягає в тому, що користувач може детально настроїти всі параметри. Конфігурації можна зберегти в користувацьких профілях сканування. Такий метод ефективний, якщо сканування регулярно виконується з однаковими параметрами.

Щоб вибрати об'єкти сканування, натисніть **Сканування комп'ютера > Розширена перевірка**, після чого виберіть потрібний параметр у розкритому меню **Об'єкти сканування** або конкретні об'єкти в дереві. Об'єкт сканування можна визначити, ввівши шлях до папки чи файлу, які потрібно включити до списку сканування. Якщо потрібно лише просканувати систему, не виконуючи очистки, виберіть **Сканувати без очищення**. Під час сканування можна вибрати три рівні очистки, натиснувши **Параметри... > Параметри ThreatSense > Очистка**.

Сканування комп'ютера з використанням розширеної перевірки розраховане на досвідчених користувачів, які мають практичні навички використання антивірусних програм.

Також можна скористатися функцією **Сканування перетягуванням**. Щоб просканувати файл або папку вручну, натисніть відповідний елемент і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку. після цього програма переміститься на передній план.

Сканування змінних носіїв

Цей тип сканування схожий на функцію "**Сканування комп'ютера**", оскільки виконується швидкий запуск перевірки змінних носіїв (наприклад, компакт-/DVD-диск/USB), наразі під'єднаних до комп'ютера. Такий тип сканування може знадобитися, коли ви під'єднуєте до комп'ютера флеш-пам'ять USB, і вам потрібно перевірити її на відсутність шкідливого ПЗ й інших загроз.

Цей тип сканування також можна запустити, якщо вибрати параметр **Розширена перевірка**, а потім пункт – **Знімні носії** в спадному меню **Об'єкти сканування** й натиснути **Сканувати**.

Повторити останнє сканування


Дає змогу швидко запустити сканування з налаштуваннями, які застосовувалися під час останнього сканування.

У розкритому меню **Дія після сканування** виберіть **Пропустити**, **Вимкнути**, **Перезавантажити**, **Перезавантажити за потреби**, **Примусово перезавантажити за потреби** або **Примусово перезавантажити**. Дії **Сон** або **Глибокий сон** доступні залежно від налаштувань живлення та режиму сну в операційній системі або можливостей комп'ютера чи

ноутбука. Вибрана дія запуститься після завершення всіх виконуваних процесів сканування. Якщо вибрано параметр **Завершити роботу**, у діалоговому вікні підтвердження вимкнення відображатиметься 30-секундний відлік (натисніть **Скасувати**, щоб відмінити вимкнення за запитом). Щоб дізнатися більше, перегляньте розділ [Додаткові параметри сканування](#).

i Сканування комп'ютера рекомендується виконувати принаймні раз на місяць. Сканування можна налаштувати як заплановане завдання в меню **Інструменти > Планувальник. Додавання до розкладу завдання щотижневого сканування комп'ютера**

Модуль запуску вибіркового сканування

Для сканування певних об'єктів скористайтесь інструментом розширеної перевірки, вибравши його в меню **Сканування комп'ютера > Розширена перевірка**. Далі в спадному меню  **Об'єкти сканування** вкажіть потрібний параметр або окремі об'єкти в структурі папок (дерева).

У вікні об'єктів сканування можна визначити об'єкти (пам'ять, диски, сектори, файли й папки), які скануватимуться на наявність інфікувань.

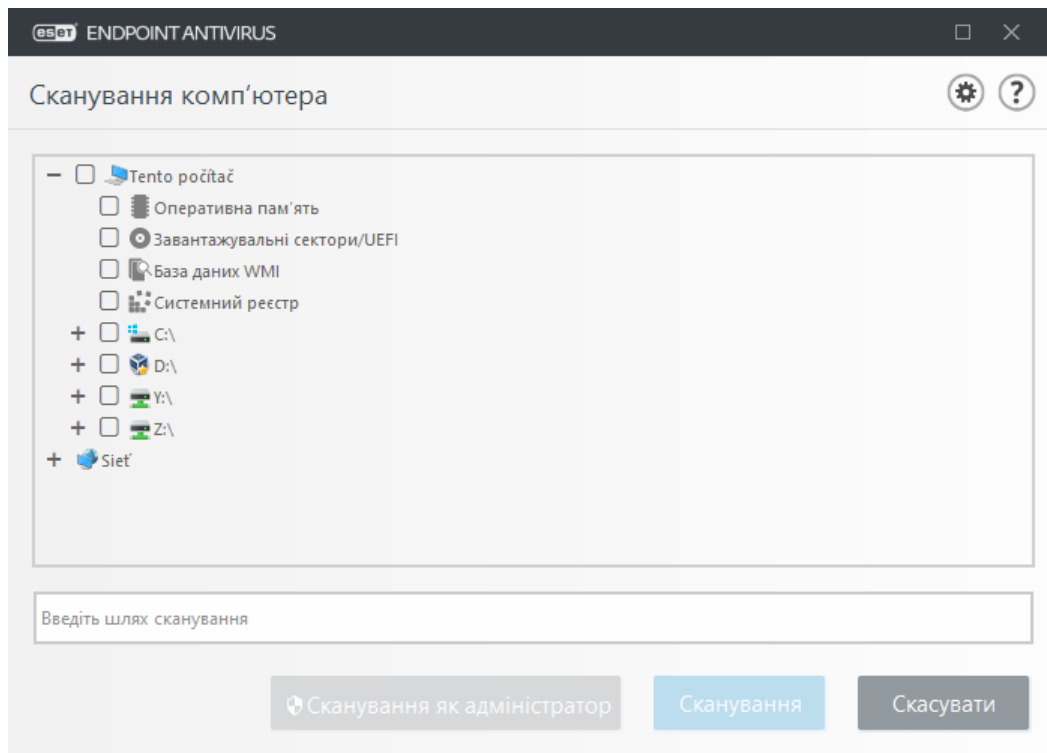
У розкритому меню **Об'єкти сканування** можна вибрати попередньо визначені набори об'єктів.

- **За параметрами профілю** – вибір об'єктів, зазначених у відповідному профілі сканування.
- **Змінні носії**: вибір дискет, запам'ятовуючих пристроїв USB, компакт-/DVD-дисків.
- **Локальні диски**: вибір усіх жорстких дисків системи.
- **Мережеві диски**: вибір усіх підключених мережевих дисків.
- **Налаштований вибір**: скасування вибору для всіх раніше вибраних об'єктів.

Структура папки (дерево) також містить певні об'єкти сканування.

- **Оперативна пам'ять**: сканування всіх процесів і даних, які наразі використовуються оперативною пам'яттю.
- **Завантажувальні сектори/UEFI**: сканування завантажувальних секторів і UEFI на наявність шкідливого програмного забезпечення. Більш докладну інформацію про сканер UEFI див. [в глосарії](#).
- **База даних WMI**: сканування всієї бази даних Windows Management Instrumentation (WMI), усіх областей імен, екземплярів класів і властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних.
- **Системний реєстр**: сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних. Після очищення реєстру посилання залишатиметься в ньому, що вбезпечить користувачів від втрати важливих даних.

Щоб швидко перейти до об'єкта сканування (файлу або папки), введіть шлях у текстове поле під структурою дерева. Шлях чутливий до регістру. Щоб додати об'єкт до сканування, установіть відповідний прапорець у структурі дерева.



Інфіковані елементи не очищаються автоматично. Сканування без очистки використовують для отримання інформації про поточний статус системи безпеки. Крім того, можна вибрати один із трьох рівнів очистки, натиснувши **Додаткові параметри > Обробник виявлення > Сканування за вимогою > Параметри ThreatSense > Очистка**. Якщо потрібно лише просканувати систему, не виконуючи очистку, виберіть **Сканувати без очищення**. Історія сканування зберігається в однойменний журнал.

Якщо вибрано параметр **Ігнорувати виключення**, усі файли з розширеннями, які раніше було виключено зі сканування, перевірятимуться без винятку.

У розкритому меню **Профіль сканування** можна вибрати профіль, що використовуватиметься для перевірки вибраних об'єктів. За замовчуванням використовується профіль **Інтелектуальне сканування**. Інші три попередньо визначених профілі — **Сканування контекстного меню**, **Детальне сканування** й **Сканування комп'ютера**. Вони використовують різні [параметри ThreatSense](#). Доступні настройки наведено в розділі **Додаткові параметри > Ядро виявлення > Сканування шкідливого програмного забезпечення > Сканування за вимогою > Параметри ThreatSense.**

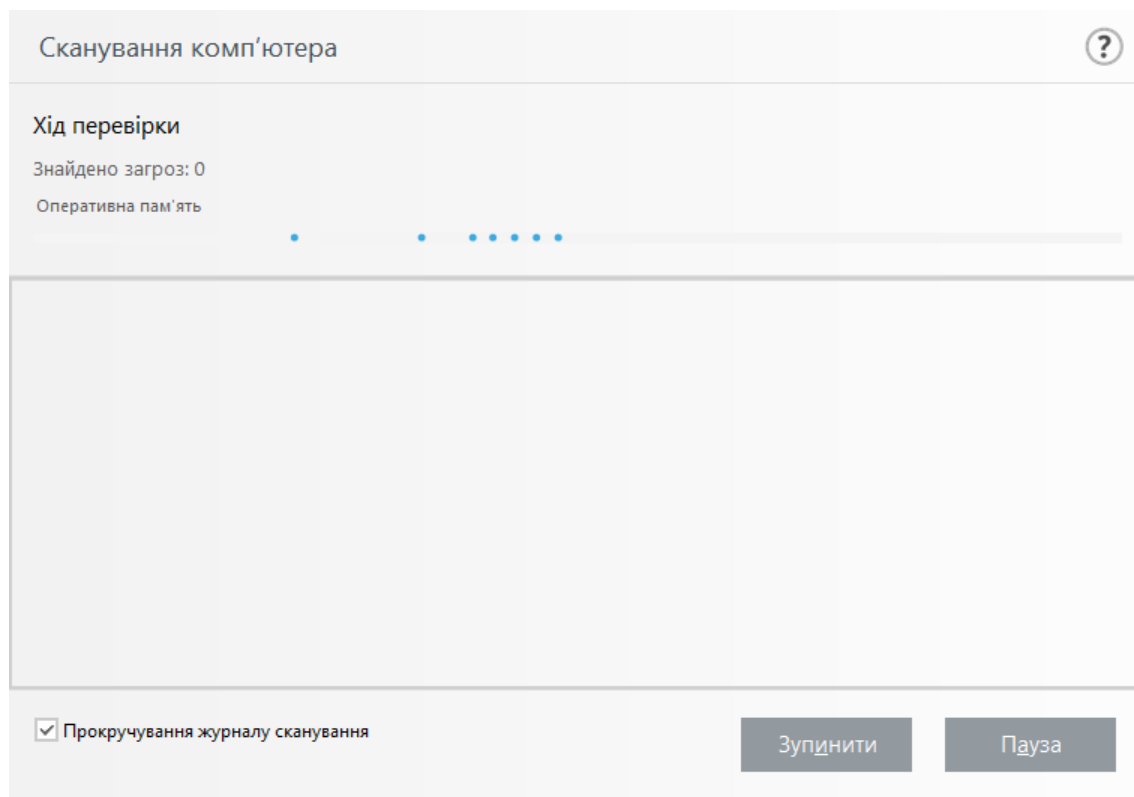
Натисніть **Сканувати**, щоб виконати перевірку на основі встановлених спеціальних параметрів.

Кнопка **Виконати сканування як адміністратор** запускає сканування від імені облікового запису адміністратора. Натисніть цю кнопку, якщо в поточного користувача немає прав доступу до файлів, які потрібно просканувати. Примітка. Ця кнопка не доступна, якщо користувач, що наразі ввійшов у систему, не може виконувати дії УАС як адміністратор.

i Щоб переглянути журнал, коли сканування завершиться, натисніть посилання [Показати журнал](#).

Хід сканування

У вікні ходу сканування відображається поточний стан процесу сканування, а також інформація про те, скільки файлів містять шкідливий код.



Деякі файли, наприклад захищені паролем або ті, що ексклюзивно використовуються системою (зазвичай *pagefile.sys* і певні журнали), просканувати неможливо. Це явище не є неполадкою.

Хід сканування[^] індикатор стану виконання процедури відображає, скільки об'єктів уже проскановано та скільки ще потрібно просканувати. Цей показник вираховується на основі загальної кількості об'єктів, доданих до списку сканування.

Ціль: ім'я об'єкта, який наразі сканується, а також шлях до нього.

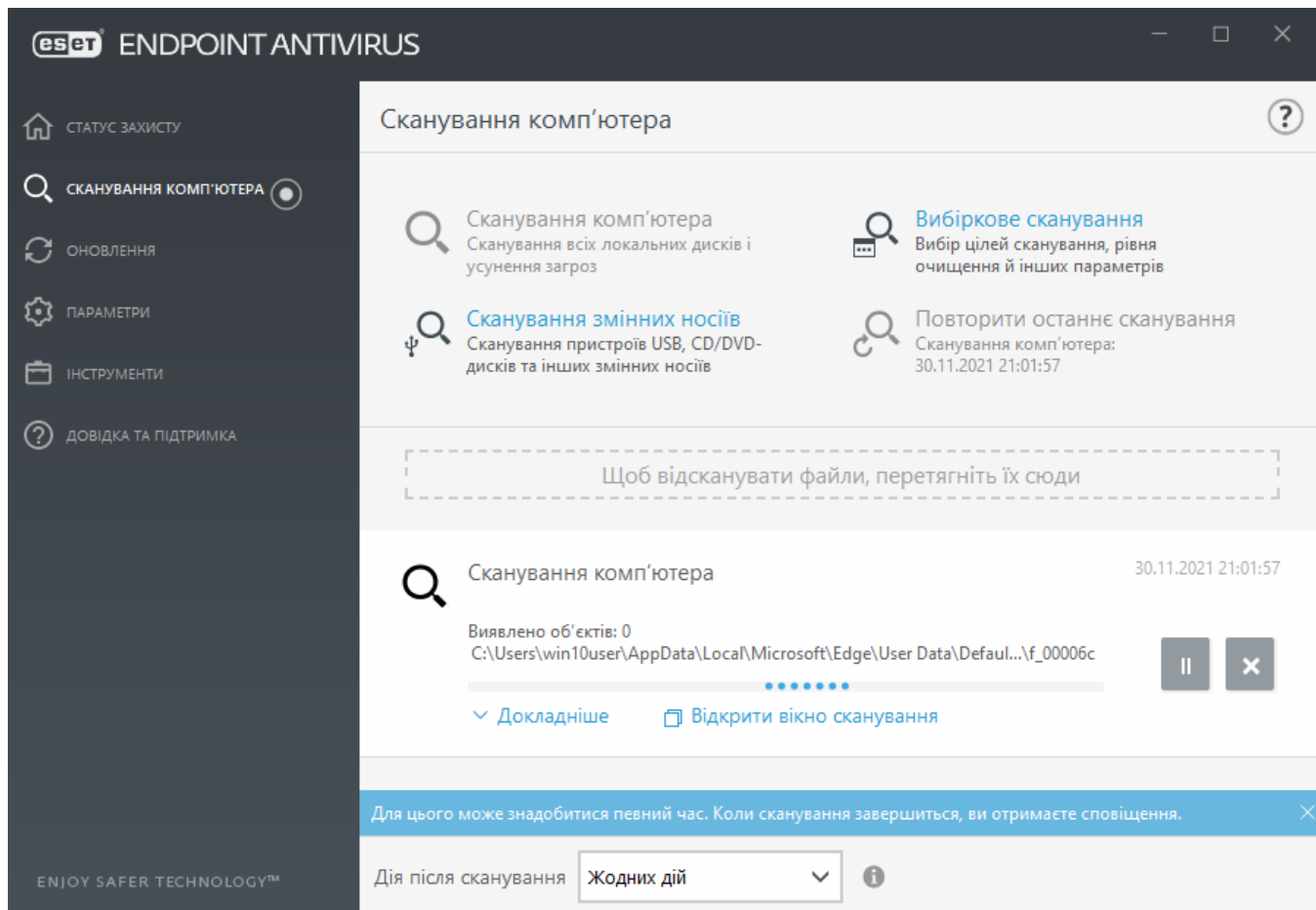
Знайдено загрози: загальна кількість загроз, виявлених у процесі сканування.

Пауза: призупинення процедури сканування.

Продовжити: цей параметр доступний у режимі паузи. Натисніть **Продовжити**, щоб відновити сканування.

Зупинити: зупинення сканування.

Прокручування журналу перевірки: якщо вибрано цей параметр, журнал перевірки буде прокручуватися автоматично під час додавання нових записів, щоб останні з них були постійно видимі.



Журнал сканування комп'ютера

У [журналі сканування комп'ютера](#) наводяться загальні відомості, зокрема:

- дата й час сканування;
- проскановані диски, папки та файли;
- кількість просканованих об'єктів;
- кількість знайдених загроз;
- час виконання;
- загальний час сканування.

Сканування шкідливого програмного забезпечення

Розділ **Сканування шкідливого ПЗ** доступний у меню «Додаткові параметри». Натисніть клавішу **F5**, клацніть **Ядро виявлення** > **Сканування шкідливого ПЗ** й виберіть параметри сканування. У цьому розділі також є такі параметри:

- **Вибраний профіль:** особливий набір параметрів, які використовуються під час сканування за вимогою.
Щоб створити новий профіль, клацніть Змінити поруч з елементом Список профілів. Більш докладну інформацію див. в розділі [Профілі сканування](#).
- **Захист за вимогою й за допомогою машинного навчання:** див. розділ [Ядро виявлення](#)

[\(7.2 й новіших версій\).](#)

- **Об'єкти сканування:** щоб просканувати лише певний об'єкт, клацніть **Змінити** поруч з елементом **Об'єкти сканування** й виберіть потрібну опцію в розкритому меню або виберіть певні цільові об'єкти в структурі папок (дереві). Більш докладну інформацію див. в розділі [Об'єкти сканування](#).
- **Параметри ThreatSense:** у цьому розділі можна знайти додаткові параметри, наприклад розширення файлів, які бажано перевіряти, використовувані методи виявлення тощо. Натисніть, щоб відкрити вкладку додаткових параметрів сканера.

Сканування в неактивному стані

Сканування в неактивному стані можна увімкнути в розділі **Додаткові параметри**. Для цього виберіть **Ядро виявлення > Сканування шкідливого ПЗ > Сканування в неактивному стані**.

Сканування в неактивному стані

Щоб увімкнути цю функцію, установіть перемикач **Увімкнути сканування в неактивному стані** в положення **Увімк.**. Коли комп'ютер не використовуватиметься, програма виконуватиме сканування всіх локальних дисків без виводу даних на екран.

За замовчуванням сканування в неактивному стані не здійснюється, якщо комп'ютер (портативний комп'ютер) працює від батареї. Цей параметр можна змінити, активувавши перемикач біля пункту **Запускати, навіть якщо комп'ютер живиться від батареї** в розділі додаткових параметрів.

Увімкніть перемикач **Вести журнал** у розділі додаткових параметрів, щоб вихідні дані перевірки комп'ютера реєструвалися в розділі [Журнали](#) (натисніть у головному вікні програми **Інструменти > Журнали**, після чого виберіть **Сканування комп'ютера** в розкритому меню **Журнал**).

Виявлення неактивного стану

Повний перелік умов, обов'язкових для запуску сканування в неактивному стані, наведено в розділі [Умови ініціювання виявлення неактивного стану](#).

Натисніть [Налаштування параметрів підсистеми ThreatSense](#), щоб змінити параметри сканування (наприклад, методи виявлення) для неактивного стану.

Профілі сканування

У ESET Endpoint Antivirus є чотири попередньо визначених профіля сканування:

- **Інтелектуальне сканування** – цей профіль розширеного сканування використовується за замовчуванням. Профіль "Інтелектуальне сканування" використовує технологію Smart-оптимізації, що виключає зі сканування файли, які в процесі попереднього сканування визначені як непошкоджені й з цього моменту не змінювалися. Це дозволяє знизити час сканування з мінімальним впливом на безпеку системи.
- **Сканування з контекстного меню** – у контекстному меню можна запустити сканування

за вимогою для будь-якого файлу. Профіль сканування з контекстного меню дозволяє визначити конфігурацію сканування, яка буде використовуватися в разі запуску такого сканування.

- **Детальне сканування** – профіль детального сканування за замовчуванням не використовує технологію Smart-оптимізації, тому за умови використання цього профілю жоден файл не виключається зі сканування.
- **Сканування комп'ютера** – цей профіль використовується за замовчуванням під час стандартного сканування комп'ютера.

Потрібні параметри сканування можна зберегти для майбутнього використання. Рекомендується створити окремі профілі (з різними об'єктами сканування, способами сканування та іншими параметрами) для кожного типу сканування, які регулярно застосовуються.

Щоб створити новий профіль, відкрийте вікно додаткових параметрів (F5) і натисніть **Обробник виявлення > Сканування на шкідливе ПЗ > Сканування комп'ютера за вимогою > Список профілів**. У вікні **Менеджер профілів** міститься розкриття меню **Вибраний профіль** зі списком наявних профілів перевірки й опцією для створення нового. Щоб створити профіль, який точно відповідатиме вашим вимогам, ознайомтесь із вмістом розділу [Налаштування параметрів підсистеми ThreatSense](#), у якому окремо описуються функції кожного параметра сканування.

і Припустімо, що вам потрібно створити власний профіль сканування, для якого частково підходить конфігурація функції **Сканування комп'ютера**, але ви не бажаєте сканувати [упаковані](#) або [потенційно небезпечні програми](#) й додатково хочете застосувати параметр **Ретельна очистка**. Введіть ім'я нового профілю у вікні **Менеджер профілів** і натисніть **Додати**. Виберіть новий профіль у розкритому меню **Вибраний профіль** і відкоригуйте решту параметрів відповідно до своїх потреб. Потім натисніть **ОК**, щоб зберегти свій новий профіль.

Об'єкти сканування

У вікні об'єктів сканування можна визначити об'єкти (пам'ять, диски, сектори, файли й папки), які скануватимуться на наявність інфікувань.

У розкритому меню **Об'єкти сканування** можна вибрати попередньо визначені набори об'єктів.

- **За параметрами профілю** – вибір об'єктів, зазначених у відповідному профілі сканування.
- **Змінні носії**: вибір дискет, запам'ятовуючих пристроїв USB, компакт-/DVD-дисків.
- **Локальні диски**: вибір усіх жорстких дисків системи.
- **Мережеві диски**: вибір усіх підключених мережевих дисків.
- **Налаштований вибір**: скасування вибору для всіх раніше вибраних об'єктів.

Структура папки (дерево) також містить певні об'єкти сканування.

- **Оперативна пам'ять**: сканування всіх процесів і даних, які наразі використовуються оперативною пам'яттю.
- **Завантажувальні сектори/UEFI**: сканування завантажувальних секторів і UEFI на наявність шкідливого програмного забезпечення. Більш докладну інформацію про сканер

UEFI див. [в глосарії](#).

- **База даних WMI:** сканування всієї бази даних Windows Management Instrumentation (WMI), усіх областей імен, екземплярів класів і властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних.
- **Системний реєстр:** сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних. Після очищення реєстру посилання залишатиметься в ньому, що вбереже користувачів від втрати важливих даних.

Щоб швидко перейти до об'єкта сканування (файлу або папки), введіть шлях у текстове поле під структурою дерева. Шлях чутливий до регістру. Щоб додати об'єкт до сканування, установіть відповідний прапорець у структурі дерева.

Додаткові параметри сканування

У цьому вікні можна вказати розширені параметри для запланованої перевірки комп'ютера. У розкривному меню можна вибрати дію, що виконуватиметься автоматично після завершення сканування:

- **Завершити роботу:** комп'ютер вимикається після завершення сканування.
- **Перезавантажити:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується.
- **Перезавантажити за потреби:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується, якщо цього вимагає сканування.
- **Режим сну:** сеанс зберігається, а комп'ютер переводиться в режим зниженого енергоспоживання, щоб можна було швидко відновити роботу.
- **Режим глибокого сну:** всі запущені в оперативній пам'яті процеси зберігаються в окремому файлі на жорсткому диску. Комп'ютер вимикається, проте після запуску він відновлює попередній робочий стан.
- **Нічого не робити:** після завершення сканування жодна дія не виконується.

i Зверніть увагу, що в режимі сну комп'ютер усе одно працює. Базові функції продовжують виконуватися, споживаючи енергію батареї (якщо комп'ютер живиться від неї). Щоб зберегти заряд, наприклад, коли ви залишили місце роботи, рекомендується користуватися режимом глибокого сну.

Виберіть параметр **Дію не може бути скасовано користувачем**, щоб користувачі без відповідних повноважень не могли переривати дії, що виконуються після сканування.

Виберіть параметр **Перевірка може бути зупинена користувачем на (хв)**, щоб надати деяким користувачам можливість призупиняти сканування комп'ютера на визначений період часу.

Також див. розділ [Хід сканування](#).

Контроль пристроїв

ESET Endpoint Antivirus дає змогу автоматично керувати носіями (CD/DVD/USB тощо). За допомогою цього модуля можна блокувати й налаштовувати розширені фільтри чи дозволи, а також

контролювати доступ користувачів до пристрою та роботу з ним. Такі функції можуть бути корисними, якщо адміністратор комп'ютера хоче запобігти використанню пристроїв із недозволеним вмістом.

Підтримувані зовнішні пристрої:

- Дисковий накопичувач (HDD, змінний диск USB)
- CD/DVD
- USB принтер
- Сховище FireWire
- Пристрій Bluetooth
- Пристрій для читання смарт-карток
- Пристрій обробки зображень
- Модем
- LPT/COM порт
- Портативний пристрій (пристрої з батареєю, зокрема медіапрогравачі, смартфони, самонастроювані пристрої тощо).
- Усі типи пристроїв

Параметри контролю пристроїв можна змінити в розділі **Додаткові параметри (F5) > Контроль пристроїв**.

Увімкнення перемикача **Увімкнути контроль пристроїв** активує функцію контролю пристроїв у програмі ESET Endpoint Antivirus. Щоб зміни набули сили, комп'ютер потрібно перезавантажити. Після цього стане доступним параметр **Правила**, за допомогою якої можна відкрити вікно [Редактор правил](#).

Якщо під'єднати пристрій, який блокується поточним правилом, на екрані відобразиться вікно сповіщення, а доступ до пристрою буде заборонено.

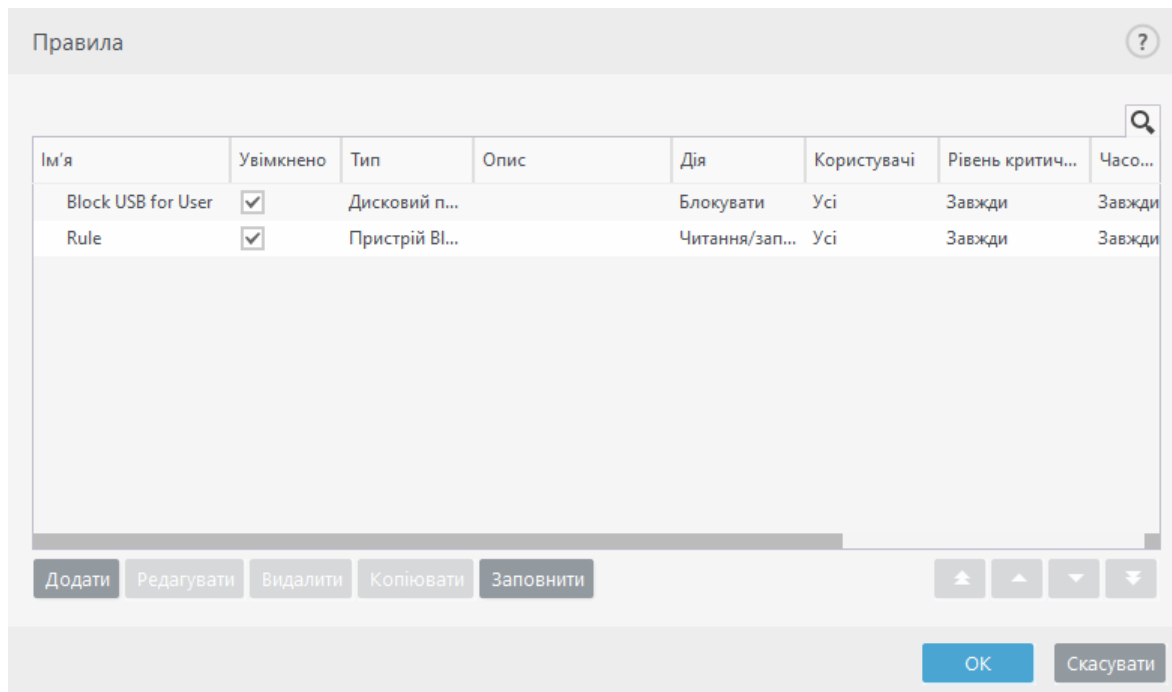
Редактор правил контролю пристроїв

У вікні **Редактор правил контролю пристроїв** можна переглянути наявні правила, а також налаштувати детальні правила контролю зовнішніх пристроїв, які користувачі підключають до комп'ютера. Перегляньте інформацію про те, [як додавати правила контролю пристроїв](#).



Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Додавання й змінення правил контролю пристроїв у продуктах ESET Endpoint](#)



Можна дозволяти та блокувати певні пристрої за даними користувача (індивідуально чи для груп), а також на основі додаткових параметрів, які потрібно вказувати в конфігурації правила. У переліку правил зазначено кілька описів правила, зокрема ім'я, тип зовнішнього пристрою, дію, яку потрібно виконати після підключення наявного зовнішнього пристрою до комп'ютера, а також зареєстрований у журналі рівень суворості.

Натисніть **Додати** або **Змінити**, щоб керувати правилом. Щоб вимкнути правило, зніміть прапорець **Увімкнено** поруч із ним до того часу, коли правило знадобиться знову. Виберіть одне або кілька правил і натисніть **Видалити**, щоб видалити їх остаточно.

Копіювати: дає змогу створити нове правило з попередньо визначеними параметрами, які вже використовуються для іншого вибраного правила.

Натисніть **Заповнити**, щоб автоматично застосувати вибрані параметри для підключених до комп'ютера знімних носіїв.

Правила розташовуються у списку за пріоритетом: правила з вищим пріоритетом розміщуються вгорі. Правила можна переміщувати окремо або групами за допомогою стрілок




Угору/у самий верх/униз/у самий низ.

У журналі контролю пристроїв фіксуються всі випадки застосування відповідної функції. Записи журналу можна переглянути в головному вікні програми ESET Endpoint Antivirus у розділі **Інструменти > Журнали**.

Виявлені пристрої


За допомогою кнопки **Заповнити** можна відобразити огляд усіх наразі підключених пристроїв з інформацією про їх тип, постачальника, модель і серійний номер (якщо доступно).

Виберіть пристрій у списку виявлених пристроїв і клацніть **ОК**, щоб [додати правило контролю пристроїв](#) із попередньо визначеною інформацією (усі параметри можна змінювати).

Пристрої в режимі зниженого енергопостачання (у режимі сну) позначено піктограмою попередження . Щоб активувати кнопку **ОК** і додати правило для цього пристрою, дотримуйтеся таких інструкцій:

- Заново підключіть пристрій.
- Використовуйте пристрій (наприклад, запустіть програму "Камера" у Windows, щоб активувати веб-камеру).

Групи пристроїв

 Пристрій, під'єднаний до комп'ютера, може становити загрозу безпеці.

Вікно "Групи пристроїв" розділено на дві частини. У правій частині вікна міститься список пристроїв, що належать до відповідної групи, а в лівій – створені групи. Виберіть групу, а також пристрої, які потрібно відобразити в області справа.

Якщо відкрити вікно "Групи пристроїв" і вибрати одну з груп, можна додати пристрої до списку чи видалити їх. Інший спосіб додавання пристроїв до групи – імпорт із файлу. Також можна натиснути кнопку **Заповнити**. Після цього список усіх пристроїв, підключених до комп'ютера, відобразиться у вікні **Виявлені пристрої**. Виберіть пристрої в заповненому списку, а потім натисніть **ОК**, щоб додати їх до групи.

Елементи керування

Додати: можна додати групу, ввівши її ім'я, або додати пристрій до наявної групи (додатково можна вказати інші дані, наприклад постачальника, модель і серійний номер), залежно від того, у якій частині вікна було натиснуто кнопку.

Змінити: дає змогу редагувати ім'я вибраної групи або параметри пристрою (постачальника, модель і серійний номер).

Видалити: видаляє вибрану групу або пристрій залежно від того, у якій частині вікна натиснуто кнопку.

Імпорт: імпортує список пристроїв із текстового файлу. Для імпорту пристроїв із текстового файлу потрібне правильне форматування:

- Кожен пристрій починається з нового рядка.
- Для кожного пристрою через кому необхідно вказати **постачальника, модель і серійний номер**.

Нижче наведено приклад вмісту текстового файлу:

✓ Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Експорт: експортує список пристроїв у файл.

За допомогою кнопки **Заповнити** можна відобразити огляд усіх наразі підключених пристроїв з інформацією про їх тип, постачальника, модель і серійний номер (якщо доступно).

Завершивши налаштування, натисніть **ОК**. Натисніть **Скасувати**, щоб закрити вікно **Групи пристроїв** без збереження змін.

i Можна створювати різні групи пристроїв, до яких застосовуватимуться різні правила. Наприклад, можна створити тільки одну групу пристроїв, до яких застосовуватиметься правило з дією **Читання/запис** або **Лише читання**. Таким чином засіб контролю пристроїв блокуватиме нерозпізнані пристрої в разі їх підключення до комп'ютера.

Зверніть увагу: для деяких типів пристроїв доступні не всі дії (дозволи). Для пристроїв збереження даних доступні всі чотири дії. Для пристроїв, не призначених для зберігання даних, доступні лише три дії (наприклад, дія **Лише читання** не доступна для пристроїв Bluetooth, тому до них можна застосувати лише функції надання доступу, блокування чи попередження користувача).

Додавання правил контролю пристроїв

Правило контролю пристроїв визначає дію, що виконується після підключення до комп'ютера пристрою, який відповідає критеріям правила.

The screenshot shows a 'Змінити правило' (Change Rule) dialog box. It contains several fields and controls:

- Ім'я** (Name): A text input field with the placeholder 'Rule'.
- Правило ввімкнено** (Rule enabled): A toggle switch currently set to 'on' (blue).
- Застосовувати протягом** (Apply for): A dropdown menu with 'Завжди' (Always) selected.
- Тип пристрою** (Device type): A dropdown menu with 'Пристрій Bluetooth' (Bluetooth device) selected.
- Дія** (Action): A dropdown menu with 'Читання/записування' (Read/Write) selected.
- Тип критеріїв** (Criteria type): A dropdown menu with 'Пристрій' (Device) selected.
- Постачальник** (Manufacturer): An empty text input field.
- Модель** (Model): An empty text input field.
- Серійний номер** (Serial number): An empty text input field.
- Рівень критичності** (Criticality level): A dropdown menu with 'Завжди' (Always) selected.
- Список користувачів** (User list): A button labeled 'Редагувати' (Edit).
- Сповістити користувача** (Notify user): A toggle switch currently set to 'on' (blue).
- OK**: A blue button at the bottom right.

Уведіть у поле **Ім'я** опис правила, щоб спростити його розпізнавання. Натисніть перемикач **Правило ввімкнено**, щоб увімкнути або вимкнути правило. Це може бути корисно, якщо ви не хочете видаляти правило остаточно.

Застосовувати протягом: дає змогу застосовувати створене правило протягом певного часу. Для цього в розкриттвому меню виберіть створений часовий інтервал. [Докладніше про часові проміжки.](#)

Тип пристрою

Вибір типу зовнішнього пристрою в розкритому меню (дисковий накопичувач/портативний пристрій/Bluetooth/FireWire тощо). Інформація про типи пристроїв надходить від операційної системи. Її можна переглянути в диспетчері пристроїв системи, попередньо під'єднавши пристрій до комп'ютера. До пристроїв збереження даних належать зовнішні диски й традиційні пристрої для читання карток пам'яті, які підключаються через USB або FireWire. Пристрої для читання смарт-карток включають пристрої з підтримкою смарт-карток із вбудованою мікросхемою, зокрема SIM-картки або картки автентифікації. Прикладами пристроїв обробки зображень є сканери або фотокамери. Оскільки такі пристрої надають інформацію лише про свої дії, але не про користувачів, їх можна заблокувати лише повністю.



Модеми не підтримують список користувачів. Правило буде застосовано до всіх користувачів, а поточний список буде видалено.

Дія

Можна дозволити або заборонити доступ до пристроїв, не призначених для зберігання даних. Натомість правила, які стосуються пристроїв для зберігання даних, дають змогу вибрати один із наведених нижче параметрів.

- **Читання/запис:** повний доступ до пристрою.
- **Блокування:** заборона доступу до пристрою.
- **Лише читання:** доступ лише для читання даних, збережених на пристрої.
- **Попереджати:** під час кожного підключення пристрою користувач отримуватиме сповіщення про виконану дію (дозволено/заблоковано), а в журналі фіксуватиметься відповідний запис. Пристрої не запам'ятовуються: сповіщення відображається щоразу, коли підключається навіть один і той самий пристрій.

Зверніть увагу: для деяких типів пристроїв доступні не всі дії (дозволи). Для пристроїв збереження даних доступні всі чотири дії. Для пристроїв, не призначених для зберігання даних, доступні лише три дії (наприклад, дія **Лише читання** не доступна для пристроїв Bluetooth, тому до них можна застосувати лише функції надання доступу, блокування чи попередження користувача).

Тип критеріїв

Виберіть **Група пристроїв** або **Пристрій**.

Відповідно до використовуваних пристроїв можна налаштовувати правила за допомогою наведених нижче додаткових параметрів. Залежать від реєстру:

- **Постачальник:** фільтрація за іменем постачальника чи ідентифікатором.
- **Модель:** поточне ім'я пристрою.
- **Серійний номер:** номер, який має більшість зовнішніх носіїв. Якщо це компакт-/DVD-диск, серійний номер відповідає конкретному носію, а не пристрою для його читання.



Якщо певні параметри не вказано, під час застосування правила система ігноруватиме відповідні поля. В усіх полях параметри фільтрації вводяться урахування реєстру. Символи узагальнення (*, ?) не підтримуються.



Щоб переглянути інформацію про пристрій, створіть для нього спеціальне правило, підключіть пристрій до комп'ютера та відкрийте [журнал контролю пристроїв](#).

Рівень критичності

- **Завжди:** фіксуються всі події.
- **Діагностика:** фіксується інформація, необхідна для оптимізації програми.
- **Інформація:** фіксуються інформаційні повідомлення, включно зі сповіщеннями про успішне оновлення, і всі зазначені вище елементи.
- **Попередження:** запис критичних помилок і попереджувальних повідомлень та їх надсилання на ERA Server.
- **Нічого:** жодні дані не фіксуватимуться.

Можна обмежувати правила для окремих користувачів або для груп, додаючи їх до **Списку користувачів**.

- **Додати:** відкриває діалогове вікно **Типи об'єкта: користувачі або групи**, де можна вибрати потрібних користувачів.
- **Видалити** – видалляє вибраного користувача зі списку фільтрації.



За допомогою правил користувача можна фільтрувати не всі пристрої (наприклад, пристрої обробки зображень не надають інформацію про користувачів, а лише повідомляють про дії).

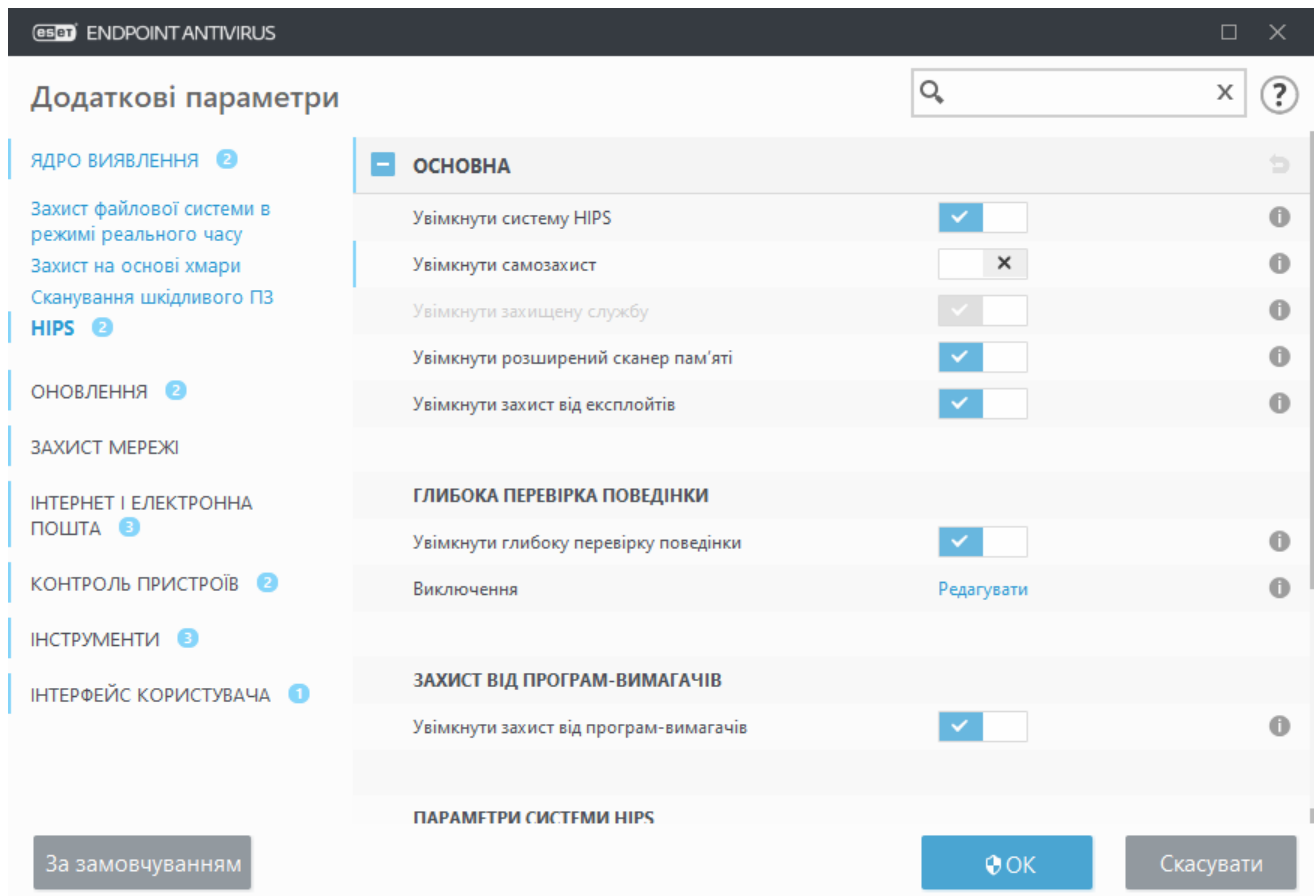
Система виявлення вторгнень (HIPS)



Зміни до параметрів HIPS має вносити лише досвідчений користувач. Оскільки помилка в налаштуваннях може призвести до нестабільності системи.

Система виявлення вторгнень (HIPS) захищає комп'ютер від шкідливих програм і небажаної активності, що негативно впливає на його роботу. Система HIPS використовує розширений поведінковий аналіз і можливості системи виявлення на основі мережного фільтра для стеження за запущеними процесами, файлами та розділами реєстру. Система HIPS працює окремо від захисту файлової системи в режимі реального часу та не є брандмауером: вона лише відстежує процеси, запущені в операційній системі.

Параметри HIPS можна знайти в меню **Додаткові параметри (F5) > Ядро виявлення > HIPS > Базові**. Інформація про стан системи HIPS (увімкнута/вимкнута) відображається в головному вікні програми ESET Endpoint Antivirus (розділ **Параметри > Комп'ютер**).



Основна

Увімкнути HIPS: систему запобігання вторгненням (HIPS) увімкнено за замовчуванням у ESET Endpoint Antivirus. Вимкнення HIPS призведе до деактивації решти функцій HIPS, зокрема функції «Захист від експлойтів».

Увімкнути самозахист: ESET Endpoint Antivirus використовує вбудовану технологію **самозахисту** (складова HIPS), яка не дозволяє шкідливому програмному забезпеченню пошкоджувати або відключати антивірусні та антишпигунські модулі. Система самозахисту захищає критично важливі процеси системи та програми ESET, розділи реєстру та файли від маніпуляцій. Інстальований ESET Management Agent також захищено.

Увімкнути захищену службу: вмикає захист для ESET Service (ekrn.exe). Якщо цей параметр увімкнено, ця служба запускається як захищений процес Windows, забезпечуючи захист від атак із боку шкідливого програмного забезпечення. Цей параметр доступний у Windows 8.1 і Windows 10.

Увімкнути розширений сканер пам'яті: працює разом із засобом захисту від експлойтів. Він посилює захист від зловмисного ПЗ, призначеного для обходу захисних продуктів за допомогою обфускації або шифрування. Удосконалений сканер пам'яті увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).

Увімкнути захист від експлойтів: служить для захисту програм, які зазвичай використовуються для зараження системи, зокрема веб-браузерів, засобів читання PDF, клієнтів електронної пошти й компонентів MS Office. Захист від експлойтів увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).

Глибока перевірка поведінки

Увімкнути глибоку перевірку поведінки: це ще один засіб захисту, який включено до системи HIPS. Це розширення HIPS аналізує поведінку всіх програм, запущених на комп'ютері, та попереджає вас про підозрілу поведінку процесу.

У розділі [Виключення HIPS із глибокої перевірки поведінки](#) можна виключити процеси з перевірки. Щоб система сканувала всі процеси на наявність загроз, рекомендуємо створювати виключення лише за крайньої потреби.

Захист від програм, які вимагають викуп

Увімкнути захист від програм-вимагачів: це ще один засіб захисту, який включено до системи HIPS. Щоб такий тип захисту працював, потрібно мати систему перевірки репутації ESET LiveGrid®. [Докладніше про цей тип захисту можна прочитати тут](#).

Увімкнути режим аудиту: жоден об'єкт, виявлений модулем "Захист від програм-вимагачів", не блокуватиметься автоматично. Натомість, усі ці об'єкти [заносятимуться до журналу з попередженням](#) і надсилатимуться на консоль керування з прапорцем "AUDIT MODE (РЕЖИМ АУДИТУ)". Адміністратор може виключити такий об'єкт, щоб більше не виявляти його, або залишити його активним. В останньому разі після завершення аудиту об'єкт буде заблоковано й видалено. Увімкнення/вимкнення режиму аудиту також записується в журнал ESET Endpoint Antivirus. Цей параметр доступний тільки в редакторі конфігурації ESET PROTECT.

Параметри системи HIPS

Режим фільтрації може виконуватися в одному з таких режимів:

Режим фільтрації	Опис
Автоматичний режим	операції ввімкнено (окрім заблокованих попередньо визначеними правилами, які захищають систему).
Інтелектуальний режим	користувач отримуватиме сповіщення лише про дуже підозрілі події.
Інтерактивний режим	користувач має підтверджувати виконання операцій.
Режим на основі положень політики	блокує всі операції, які не визначені певним правилом, що дозволяє їх.
Режим навчання	Операції ввімкнено, а після кожної операції створюється правило. Правила, створені в цьому режимі, можна переглядати в редакторі Правила HIPS , проте їх пріоритет нижчий за пріоритет правил, створених уручну або в автоматичному режимі. Якщо в розкривному меню Режим фільтрації вибрати Режим навчання , стане доступним налаштування Режим навчання стане неактивним о . Виберіть тривалість використання в режимі навчання (максимум — 14 днів). Після завершення зазначеного періоду відобразиться запит на зміну правил, створених системою HIPS у режимі навчання. Можна також вибрати інший режим фільтрації або відкласти рішення й користуватися режимом навчання далі.

Установлено після виходу з режиму навчання: укажіть режим фільтрації, який

застосовуватиметься після завершення роботи в режимі навчання. Після завершення строку дії зміна режиму фільтрації HIPS за допомогою опції **Запитувати користувача** потребуватиме наявності прав адміністратора.

Система HIPS контролює події в операційній системі та реагує на них відповідно до правил, подібних до тих, які використовує брандмауер. Щоб відкрити редактор **правил HIPS**, натисніть **Змінити** біля елемента **Правила**. У вікні правил HIPS можна вибирати, додавати, змінювати й вилучати правила. Докладніше про створення правил і операції HIPS див. в розділі [Змінення правила HIPS](#).

Інтерактивне вікно HIPS

У вікні сповіщень системи запобігання вторгненням (HIPS) можна створити правило на основі будь-якої нової дії, виявленої системою HIPS, а потім визначити умови, за яких ця дія дозволятиметься або блокуватиметься.

Створені таким чином правила рівноцінні заданим уручну. Тому правило, створене у вікні сповіщень, може бути менш конкретним у порівнянні з тим правилом, що ініціювало появу цього вікна. Це означає, що після створення такого правила в діалоговому вікні одна операція може ініціювати появу того самого вікна. Більш докладну інформацію див. в розділі [Пріоритет для правил HIPS](#).

Якщо за замовчуванням для правила вибрано дію **Запитувати щоразу**, під час кожного його застосування відображатиметься відповідне діалогове вікно. Ви можете **Відхилити** або **Дозволити** певну операцію. Якщо за відведений час ви не вказали жодної дії, її буде вибрано на основі правил.

Параметр **Запам'ятати до закриття програми** ініціює використання дії (**Дозволити/Відхилити**) до наступної зміни правил або режимів фільтрації, оновлення модуля HIPS або перезапуску системи. Після будь-якої з цих трьох дій тимчасові правила буде видалено.

Параметр **Створити правило та запам'ятати безстроково** дозволяє створити нове правило HIPS, яке пізніше можна змінити в розділі [Керування правилами HIPS](#) (для цього потрібні права адміністратора).

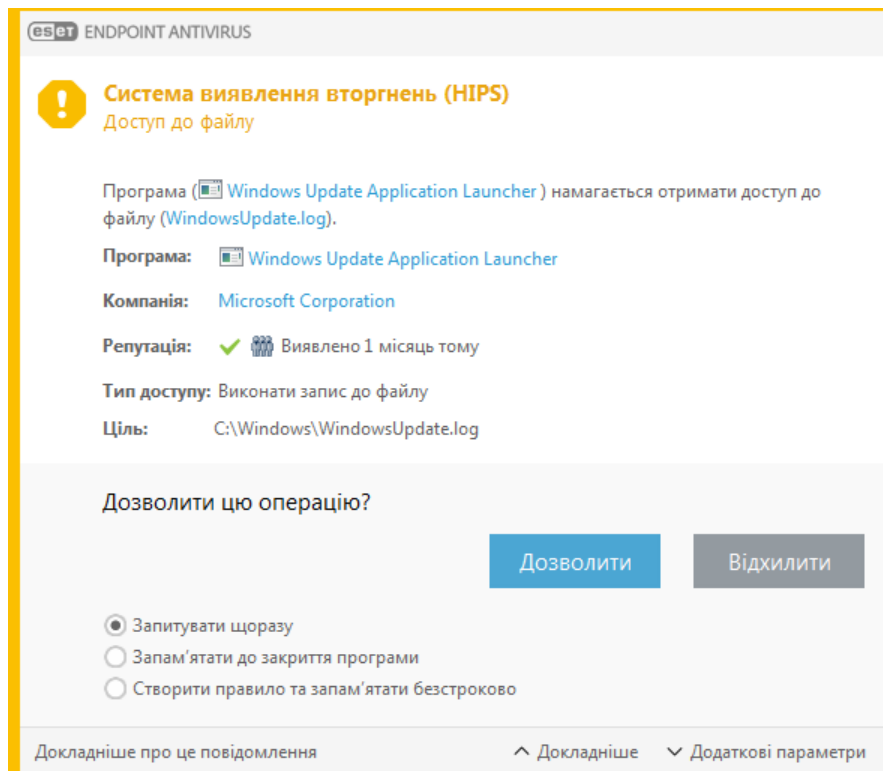
Клацніть **Докладніше** в нижній частині вікна, щоб дізнатися більше про програму, яка ініціює операцію, репутацію файлу або тип операції, яку вам потрібно підтвердити або відхилити.

Щоб відкрити розширені параметри правила, клацніть **Розширені параметри**. Якщо вибрати **Створити правило та запам'ятати безстроково**, будуть доступні вказані нижче параметри:

- **Створити правило, дійсне лише для цієї програми:** якщо зняти цей прапорець, правило буде створено для всіх вихідних програм.
- **Лише для операції:** виберіть операції правила для файлу (програми, реєстру). [Див. описи всіх операцій HIPS](#).
- **Лише для об'єкта:** виберіть об'єкти правила для файлу (програми, реєстру).



Щоб більше не показувати сповіщення, змініть режим фільтрації на **Автоматичний режим** у розділі **Додаткові параметри (F5) > Ядро виявлення > HIPS > Базові**.



Виявлено потенційно зловмисну програму, яка вимагає викуп

Це інтерактивне вікно з'являється, коли виявлено потенційно зловмисну програму. Ви можете **Відхилити** або **Дозволити** певну операцію.

Щоб переглянути окремі параметри виявлення, клацніть **Докладніше**. У діалоговому вікні можна **надіслати файл на аналіз** або **виключити з перевірки**.

Щоб функція [захисту від програм-вимагачів](#) працювала належним чином, потрібно ввімкнути ESET LiveGrid®.

Керування правилами HIPS

Список визначених користувачем і автоматично доданих правил у системі HIPS. Більш докладну інформацію про створення правил та операції HIPS можна переглянути в розділі [Параметри правил HIPS](#). Див. також розділ [Загальні принципи роботи HIPS](#).

Стовпці

Правило: визначене користувачем або автоматично вибране ім'я правила.

Увімкнено: деактивуйте цей параметр, якщо потрібно тільки зберегти правило в списку, а не використовувати його.

Дія: правило визначає дію (**Дозволити**, **Заблокувати** або **Запитувати**), яка виконуватиметься в разі дотримання відповідних умов.

Джерела: правило використовуватиметься лише в тому випадку, коли подію ініціює програма.

Об'єкти: правило використовуватиметься лише в тому випадку, коли операція пов'язана з певним файлом, програмою або записом реєстру.

Рівень критичності – якщо увімкнути цей параметр, інформацію про таке правило буде записано в [журнал HIPS](#).

Сповіщати: у разі ініціювання події в правому нижньому куті відображатиметься невелике спливаюче сповіщення.

Елементи керування

Додати: створити нове правило.

Редагувати: редагувати вибрані елементи.

Видалити: видаляє вибрані записи.

Пріоритет для правил HIPS

Немає параметрів, які б дозволили змінити рівень пріоритету правил HIPS за допомогою кнопок переходу у верхню або нижню частину вікна.

- Усі створювані правила мають однаковий пріоритет
- Що більш конкретне правило, то вищий пріоритет (наприклад, правило для певної програми має вищий пріоритет відносно правил для всіх програм)
- Система запобігання вторгненням (HIPS) має внутрішні правила з більш високим пріоритетом, що недоступні для користувача (наприклад, користувач не може змінити визначені правила самозахисту)
- Якщо створюване правило може вповільнити роботу операційної системи, воно не буде застосовуватися (буде мати найнижчий пріоритет)

Параметри правила HIPS

Спочатку див. розділ [Керування правилами HIPS](#).

Ім'я правила: визначене користувачем або автоматично вибране ім'я правила.

Дія: дає змогу визначити дію (Дозволити, Заблокувати або Запитувати), яка виконуватиметься в разі виконання відповідних умов.

Задіяні операції: потрібно вибрати тип операції, для якої застосовуватиметься правило. Правило використовуватиметься лише для цього типу операцій і для вибраної цілі.

Увімкнено: вимкніть цей перемикач, щоб зберегти правило у списку, але не застосовувати його.

Рівень критичності – якщо ввімкнути цей параметр, інформацію про таке правило буде записано в [журнал NIPS](#).

Сповістити користувача: у разі ініціювання події в правому нижньому куті відображається невелике спливаюче вікно.

Правило складається з частин, що описують умови, які його ініціюють.

Програми-джерела: правило використовуватиметься лише в тому випадку, якщо подію ініціює ця програма. У розкритому меню виберіть **Окремі програми** й натисніть **Додати**, щоб додати нові файли. Також можна вибрати **Усі програми**, щоб додати всі програми.

Цільові файли: правило використовуватиметься лише в тому випадку, якщо операцію пов'язано з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі файли** й натисніть **Додати**, щоб додати нові файли чи папки, або виберіть **Усі файли**, щоб додати всі файли.

Програми: правило використовуватиметься лише в тому випадку, якщо операція пов'язана з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі програми** й натисніть **Додати**, щоб додати нові файли або папки, або виберіть **Усі програми**, щоб додати всі програми.

Записи реєстру: правило використовуватиметься лише в тому випадку, якщо операція пов'язана з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі записи** й натисніть **Додати**, щоб додати нові файли або папки, або виберіть **Усі записи**, щоб додати всі програми.

i Деякі операції за певними правилами, визначені системою NIPS, не можна заблокувати, оскільки їх дозволено за замовчуванням. Крім того, NIPS контролює не всі системні операції. А відстежує лише ті, які можна класифікувати як небезпечні.

i Коли вказуєте шлях, майте на увазі, що C:\example відноситься до дій із самою папкою, а C:\example*. * — до дій із файлами в цій папці.

Операції з програмами

- **Налагодити іншу програму:** приєднання до процесу засобу налагодження. Під час виправлення неполадок у роботі іншої програми певні відомості про її поведінку можна переглядати й коригувати. Також можна отримати доступ до даних цієї програми.
- **Зупиняти події від іншої програми:** програма-джерело намагається перехопити події, пов'язані з певною програмою (наприклад, клавіатурний шпигун робить спробу перехопити події, пов'язані з браузером).
- **Припинити/призупинити роботу іншої програми:** призупинення, відновлення або припинення процесу (доступ можна отримати безпосередньо з диспетчера процесів або на вкладці "Процеси").
- **Запустити нову програму:** запуск нових програм або процесів.
- **Змінити стан іншої програми:** програма-джерело намагається здійснити запис у пам'ять цільової програми або виконати певний код від її імені. Така функція може бути корисною для захисту важливої програми: просто визначте її як цільову у правилі, що блокує використання подібної операції.

i Не можна зупинити виконання процесу на 64-розрядній версії Windows XP.

Операції з реєстром

- **Змінити параметри запуску:** будь-які зміни в параметрах запуску програм під час завантаження Windows. Їх можна знайти, наприклад, здійснивши пошук за назвою розділу Run у реєстрі Windows.
- **Видалити з реєстру:** видалення розділу або його значення.
- **Перейменувати розділ реєстру:** перейменування розділів реєстру.
- **Внести зміни до реєстру:** створення нових значень розділів реєстру, зміна наявних значень, переміщення даних у дереві бази даних або налаштування прав доступу до розділів реєстру для користувачів і груп.

Використання символів узагальнення в правилах

Зірочку в правилах можна використовувати тільки для заміни певного ключа, наприклад "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start/". Використання символів узагальнення будь-яким іншим чином не підтримується.

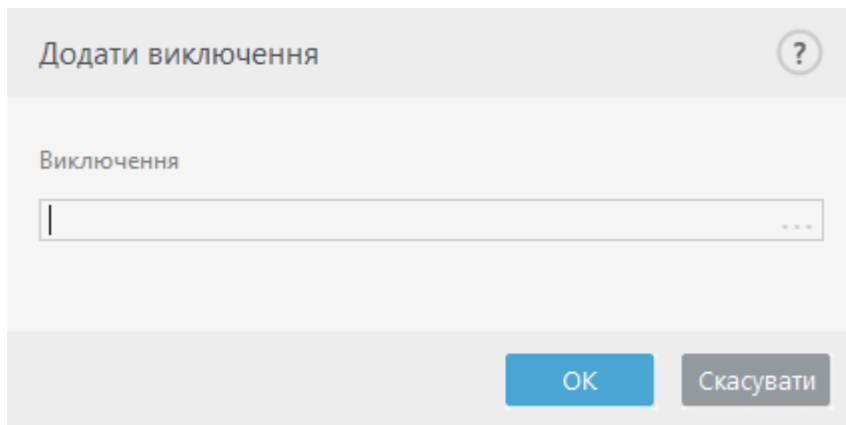
i Створення правил відносно ключа HKEY_CURRENT_USER

Цей ключ являє собою просто посилання на певний підрозділ HKEY_USERS, який є специфічним для користувача, визначеного SID (ідентифікатором безпеки). Щоб створити правило тільки для поточного користувача, замість шляху HKEY_CURRENT_USER використовуйте шлях, який вказує на HKEY_USERS\%SID%. У якості SID можна використовувати зірочку, щоб зробити правило застосовним для всіх користувачів.

! Якщо створити дуже загальне правило, з'явиться відповідне попередження.

На наведеному нижче прикладі ми продемонструємо, як обмежити небажану поведінку окремої програми.

1. Призначте ім'я правилу й виберіть **Заблокувати** (або **Запитати**, якщо ви маєте намір вибрати дію пізніше) в розкритому меню **Дія**.
2. Увімкніть перемикач **Сповістити користувача**, щоб відображати сповіщення щоразу, коли застосовується правило.
3. Виберіть щонайменше одну операцію в списку **Операції для розділу**, до якого застосовуватиметься правило.
4. Натисніть кнопку **Далі**.
5. У розкритому меню вікна **Програми-джерела** виберіть **Окремі програми**, щоб застосувати нове правило до всіх програм, які намагаються виконати будь-яку з вибраних операцій з указаними програмами.
6. Клацніть **Додати**, а потім ..., щоб вибрати шлях до певної програми, і натисніть кнопку **ОК**. За бажанням додайте більше програм.
Приклад: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Виберіть операцію **Записати у файл**.
8. У розкритому меню виберіть пункт **Усі файли**. Після цього будуть блокуватися будь-які спроби програм, вибраних у попередньому кроці, виконати запис у будь-які файли.
9. Натисніть кнопку **Готово**, щоб зберегти нове правило.



Додаткові параметри HIPS

Наведені нижче опції стануть у пригоді під час налагодження програми й аналізу її поведінки.

Драйвери, які дозволено завжди завантажувати: виберіть драйвери, які можна завантажувати в усіх режимах фільтрації, якщо їх не блокує правило користувача.

Запис усіх заблокованих дій: усі заблоковані операції буде записано в журнал HIPS. Використовуйте цю функцію лише для вирішення проблеми або за запитом служби підтримки ESET, оскільки вона може створювати великий файл журналу й сповільнювати роботу комп'ютера.

Повідомляти, коли в автоматично виконувані програми вносяться зміни: на робочому столі відображатимуться сповіщення щоразу, коли програма додається до списку завантажуваних під час запуску системи або видаляється з нього.

Драйвери, які дозволено завантажувати завжди

Драйвери в цьому списку можна завантажувати в усіх режимах фільтрації HIPS, якщо їх не блокує правило користувача.

Додати: додати новий драйвер.

Змінити: редагувати дані вибраного драйвера.

Видалити: видалити драйвер зі списку.

Скинути: перезавантажити набір системних драйверів.

i Натисніть **Скинути**, якщо ви не бажаєте включати драйвери, додані вручну. Це може бути корисно, якщо вам не вдається вручну видалити зі списку додані драйвери.

Режим презентації

Режим презентації – це функція для користувачів, які не хочуть переривати робочий процес, відволікатися на спливаючі вікна й надмірно навантажувати процесор. Режим презентації також може використовуватися під час ілюстрованих доповідей, які небажано переривати антивірусною перевіркою. Коли цей режим увімкнено, показ спливаючих вікон заборонено, а заплановані завдання не виконуються. Функції захисту системи продовжують роботу у фоновому режимі, не вимагаючи втручання користувача.

Виберіть **Параметри > Комп'ютер** і натисніть перемикач **Режим презентації**, щоб уручну активувати відповідний режим. У меню **Додаткові параметри (F5)** виберіть **Інструменти > Режим презентації**, після чого натисніть перемикач **Автоматично вмикати режим презентації під час запуску програм у повноекранному режимі**, щоб програма ESET Endpoint Antivirus автоматично вмикала режим презентації під час запуску застосунків у повноекранному режимі. Увімкнення режиму презентації становить потенційний ризик для безпеки комп'ютера, тому колір піктограми статусу захисту на панелі завдань стане жовтим, а також відобразиться відповідне попередження. Це попередження також відображатиметься в головному вікні, де з'явиться оранжеве сповіщення **Режим презентації ввімкнено**.

Якщо ввімкнути параметр **Автоматично вмикати режим презентації під час запуску програм у повноекранному режимі**, режим презентації активуватиметься під час запуску програми в повноекранному режимі й автоматично вимикатиметься після її закриття. Таким чином, можна активувати режим презентації відразу після запуску гри, відкриття програми в повноекранному режимі або початку презентації.

Також можна встановити прапорець **Автоматично вимкнути режим презентації через**, щоб визначити у хвилину проміжок часу, через який режим презентації буде автоматично вимкнено.

Сканування під час запуску

За замовчуванням автоматична перевірка файлу під час запуску виконується після запуску системи або під час оновлення модулів. Цей процес перевірки залежить від параметрів і завдань, визначених у розділі [Завдання за розкладом](#).

Параметри сканування під час запуску є частиною запланованого завдання **Перевірка файлів під час запуску системи**. Щоб змінити параметри сканування під час запуску, перейдіть до розділу **Інструменти > Планувальник**, натисніть **Автоматична перевірка файлів під час запуску системи**, а потім – **Змінити**. На останньому кроці відобразиться вікно [Автоматична перевірка файлів під час запуску системи](#) (див. наступний розділ для отримання докладніших відомостей).

Детальні інструкції щодо створення запланованого завдання та керування див. у розділі [Створення нових завдань](#).

Автоматична перевірка файлів під час

запуску системи

Створюючи заплановане завдання перевірки файлів під час запуску, можна змінити перелічені нижче параметри.

У розкритому меню **Об'єкт сканування** визначається глибина перевірки файлів, що виконується під час запуску системи, на основі секретного прогресивного алгоритму. Відповідно до вказаних критеріїв файли розташовуються за спаданням:

- **Всі зареєстровані файли** (перевіряється більшість файлів)
- **Файли, які рідко використовуються**
- **Файли, які зазвичай використовуються**
- **Файли, які часто використовуються**
- **Тільки файли, які найчастіше використовуються** (перевірка виконується на мінімальній кількості файлів)

Включено також дві конкретні групи:

- **Файли, запущені перед входом користувача в систему:** файли з розташувань, доступні без обов'язкового входу користувача в систему (практично всі розташування під час запуску, зокрема служби, додаткові компоненти браузера, сповіщення winlogon, записи інструмента "Завдання за розкладом", відомі dll тощо).
- **Файли, що запускаються після входу користувача в систему** – файли з розташувань, які дають змогу запускати їх лише після входу користувача в систему (файли, які запускаються лише для певного користувача, зокрема файли в розташуванні `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Списки файлів, які потрібно перевірити, незмінні для кожної групи.

Пріоритет сканування: рівень пріоритетності, що визначається перед початком сканування:

- **Під час простою:** завдання виконуватиметься лише тоді, коли система неактивна.
- **Найнижчий:** за мінімально можливого рівня завантаження системи.
- **Низький:** за низького завантаження системи.
- **Нормальний:** за середнього завантаження системи.

Захист документів

Модуль захисту документів сканує документи Microsoft Office перед їх відкриттям, а також файли, автоматично завантажені браузером Internet Explorer (такі як елементи Microsoft ActiveX). Функція захисту документів забезпечує ще один рівень безпеки, додатково до захисту файлової системи в режимі реального часу. Для підвищення продуктивності її можна вимкнути в системах, робота яких не пов'язана з опрацюванням великої кількості документів Microsoft Office.

Щоб увімкнути захист документів, відкрийте вікно **Додаткові параметри (F5) > Ядро виявлення > Сканування на шкідливе ПЗ > Захист документів** і натисніть перемикач **Увімкнути захист документів**.

i Цю функцію активують програми, у яких використовується прикладний інтерфейс Microsoft Antivirus API (наприклад, Microsoft Office 2000 та пізніших версій або Microsoft Internet Explorer 5.0 та пізніших версій).

Виключення

У розділі **Виключення** можна виключити [об'єкти](#) з ядра виявлення. Щоб система сканувала всі об'єкти, рекомендується створювати виключення лише за необхідності. Існують ситуації, коли може виникнути потреба виключити об'єкт. Прикладом таких ситуацій, коли потрібно виключити об'єкт зі списку сканування, може бути сканування елементів великих баз даних, що значно сповільнить роботу комп'ютера, або програмного забезпечення, яке конфліктує зі сканером.

У розділі [Виключення в роботі](#) можна виключити файли й папки зі сканування. Виключення в роботі стають у пригоді для виключення зі сканування певних файлів для ігор, або коли сканування певних файлів спричиняє відхилення в роботі або продуктивності системи.

[Виключення об'єктів виявлення](#) дозволяє виключати об'єкти з очищення за їх іменем, шляхом і хешем. Виключення об'єктів виявлення не виключає файли й папки зі сканування, як виключення в роботі. Виключення об'єктів виявлення стосуються тільки виявлених ядром виявлення об'єктів, для яких є застосовуване правило в списку виключень.

[Для виключень у версії 7.1 і попередніх версіях](#) функції виключення в роботі й виключення виявлених об'єктів були об'єднані.

Не слід плутати з іншими типами виключень:

- [Виключення процесу](#): усі операції з файлами, які відносяться до виключених програмних процесів, виключаються зі сканування (це може знадобитися для підвищення швидкості резервного копіювання або рівня доступності сервісу).
- [Виключені розширення файлів](#)
- [Виключення HIPS](#)
- [Фільтр виключень для хмарного захисту](#)

Виключення в роботі

У розділі "Виключення в роботі" можна виключити файли й папки зі сканування.

Щоб система сканувала всі об'єкти на наявність загроз, рекомендуємо створювати виключення в роботі лише за крайньої потреби. Проте існують ситуації, коли може виникнути потреба виключити об'єкт. Це, наприклад, можуть бути елементи великих баз даних, сканування яких значно сповільнить роботу комп'ютера, або програмне забезпечення, що конфліктує зі сканером.

Щоб виключити файли й папки зі сканування, додайте їх у список виключень: **Додаткові параметри (F5) > Ядро виявлення > Виключення > Виключення в роботі > Змінити**.

Щоб [виключити об'єкт](#) (шлях до файлу або папки) зі сканування, клацніть **Додати** й уведіть відповідний шлях або виберіть його в структурі дерева.

Виключення в роботі

?

Виключити шлях

Коментар

C:\Backup*

C:\pagefile.sys

Додати

Редагувати

Видалити

Імпортувати

Експортувати

ОК

Скасувати



Загрозу у файлі не буде виявлено модулем **захисту файлової системи в режимі реального часу** або модулем **перевірки комп'ютера**, якщо файл відповідає критеріям виключення під час сканування.

Елементи керування

- **Додати:** додати новий запис для виключення об'єктів зі сканування.
- **Редагувати:** редагувати вибрані елементи.
- **Видалити:** видаляє вибрані записи (щоб вибрати кілька записів, клацніть їх мишею, утримуючи клавішу CTRL).
- **Імпорт/Експорт:** імпорт і експорт виключень у роботі є корисними функціями, якщо потрібно створити резервну копію поточних виключень для використання в майбутньому. Опція експорту параметрів також стане в пригоді в некерованих середовищах для користувачів, які бажають застосовувати власну конфігурацію на кількох комп'ютерах: вони зможуть легко перенести ці параметри, імпортувавши файл .txt.

 [Показати зразок формату файлу імпорту/експорту](#)

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}
```

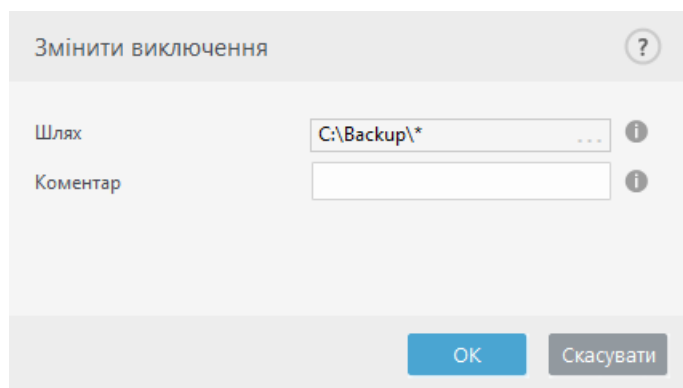
```
C:\Backup\*,custom comment
```

```
C:\pagefile.sys
```

Додавання або зміна виключення в роботі

У цьому діалоговому вікні можна виключити певний шлях (файл або каталог) для цього комп'ютера.

Щоб вибрати певний шлях, клацніть ... у полі **Шлях**.
i Якщо ви вводите файл уручну, ознайомтеся з наведеними нижче прикладами [прикладami формату виключення](#).



Щоб виключити групу файлів, можна використовувати символи узагальнення. Знак запитання (?) позначає окремий символ, а зірочка (*) представляє рядок, який складається з нуля або більшої кількості символів.

- Якщо необхідно виключити всі файли та підпапки в папці, введіть шлях до папки та скористайтесь маскою *
- Щоб виключити лише файли у форматі doc, скористайтесь маскою *.doc
- Якщо ім'я виконуваного файлу має певну кількість символів (і вони різняться), а точно відомий лише перший (наприклад, "D"), використовуйте такий формат: D?????.exe (знаки запитання замінюють відсутні або невідомі символи)

✓ Приклади


- C:\Tools* – для виключення папки та всього вмісту в ній (файлів і підпапок) шлях має закінчуватися зворотною скісною рисою (\) і зірочкою (*).
- C:\Tools*. * – те саме, що й з C:\Tools*
- C:\Tools: папку Tools не буде виключено. Для сканера Tools може бути іменем.
- C:\Tools*.dat: цей шлях дозволяє виключити всі файли .dat в папці Tools.
- C:\Tools\sg.dat: цей шлях дозволяє виключити лише конкретний указаний файл.

Для визначення виключень зі сканування `%PROGRAMFILES%` можна використовувати системні змінні.

- Щоб виключити папку Program Files, використовуючи цю системну змінну, скористайтеся шляхом `%PROGRAMFILES%*` (обов'язково вкажіть зворотну скісну риску й зірочку в кінці шляху).
- Щоб виключити всі файли й папки в підкаталозі `%PROGRAMFILES%`, використовуйте шлях `%PROGRAMFILES%\Excluded_Directory*`

☐ [Розгорнути список підтримуваних системних змінних](#)

У шлях до виключень можна використовувати такі змінні:


- 
- `%ALLUSERSPROFILE%`
 - `%COMMONPROGRAMFILES%`
 - `%COMMONPROGRAMFILES(X86)%`
 - `%COMSPEC%`
 - `%PROGRAMFILES%`
 - `%PROGRAMFILES(X86)%`
 - `%SystemDrive%`
 - `%SystemRoot%`
 - `%WINDIR%`
 - `%PUBLIC%`

Системні змінні, визначені користувачем (наприклад, `%TEMP%` або `%USERPROFILE%`) та змінні оточення (наприклад, `%PATH%`) не підтримуються.

Символи узагальнювання в середині шляху (наприклад, `C:\Tools*\Data\file.dat`) можуть працювати, але офіційно не підтримуються у виключеннях. Щоб дізнатися більше, перегляньте цю [статтю бази знань](#).

Якщо використовується [виключення виявлених об'єктів](#), символи узагальнення можна використовувати в середині шляху без обмежень.

Порядок виключень:

- 
- Немає параметрів, які б дозволили змінити рівень пріоритету виключень за допомогою кнопок переходу у верхню або нижню частину вікна.
 - Коли сканер виявить відповідність до першого застосовного правила, друге застосовне правило не буде оцінюватися.
 - Що менше правил, то вище швидкодія сканування.
 - Не створюйте паралельні правила.

Формат виключення шляху

Щоб виключити групу файлів, можна використовувати символи узагальнення. Знак запитання (?) позначає окремий символ, а зірочка (*) представляє рядок, який складається з нуля або більшої кількості символів.

- Якщо необхідно виключити всі файли та підпапки в папці, введіть шлях до папки та скористайтесь маскою *
- Щоб виключити лише файли у форматі doc, скористайтесь маскою *.doc
- Якщо ім'я виконуваного файлу має певну кількість символів (і вони різняться), а точно відомий лише перший (наприклад, "D"), використовуйте такий формат: D????.exe (знаки запитання замінюють відсутні або невідомі символи)

✓ Приклади

- C:\Tools* - для виключення папки та всього вмісту в ній (файлів і підпапок) шлях має закінчуватися зворотною скісною рисою (\) і зірочкою (*).
- C:\Tools*. - те саме, що й з C:\Tools*
- C:\Tools: папку Tools не буде виключено. Для сканера Tools може бути іменем.
- C:\Tools*.dat: цей шлях дозволяє виключити всі файли .dat в папці Tools.
- C:\Tools\sg.dat: цей шлях дозволяє виключити лише конкретний указаний файл.

Для визначення виключень зі сканування %PROGRAMFILES% можна використовувати системні змінні.

- Щоб виключити папку Program Files, використовуючи цю системну змінну, скористайтесь шляхом %PROGRAMFILES%* (обов'язково вкажіть зворотну скісну риску й зірочку в кінці шляху).
- Щоб виключити всі файли й папки в підкаталозі %PROGRAMFILES%, використовуйте шлях %PROGRAMFILES%\Excluded_Directory*

☐ [Розгорнути список підтримуваних системних змінних](#)

У шлях до виключень можна використовувати такі змінні:



- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Системні змінні, визначені користувачем (наприклад, %TEMP% або %USERPROFILE%) та змінні оточення (наприклад, %PATH%) не підтримуються.

Виключення об'єктів виявлення

У розділі "Виключення об'єктів виявлення" можна виключити об'єкти з [очищення](#) за допомогою фільтрації імен виявлених об'єктів, шляху до них або їх хешу.

Виключення об'єктів виявлення не виключає файли й папки зі сканування, як [виключення в роботі](#). Виключення об'єктів виявлення стосуються тільки виявлених ядром виявлення об'єктів, для яких є застосовуване правило в списку виключень.



У прикладі, який наведено в першому рядку, виявлено об'єкт Win32/Adware.Optmedia у файлі C:\Recovery\file.exe. У другому рядку є правило, згідно з яким кожен файл із відповідним хешем SHA-1 завжди буде виключати незалежно від імені виявленого об'єкта.

Виключення об'єктів виявлення

?

Q

Критерій об'єкта	Виключити виявлення	Коментар
C:\Recovery*.*	Win32/Adware.Optmedia	
2723cb8ca015209528d3fbdcaa801124f4f40ad4	Будь-який об'єкт виявлення	SuperApi.exe

Додати
Редагувати
Видалити
Імпортувати
Експортувати

ОК
Скасувати

Щоб система виявила всі загрози, рекомендується створювати виключення лише за необхідності.

Щоб додати файли й папки в список виключень, виберіть **Додаткові параметри (F5) > Ядро виявлення > Виключення > Виключення об'єктів виявлення > Змінити**.

Щоб [виключити об'єкт \(за його іменем або хешем\)](#) з очищення, клацніть **Додати**.


Нижче наведено способи створення виключення для [потенційно небажаних](#) і [потенційно небезпечних](#) програм за іменем виявленого об'єкта:

- У вікні сповіщень з інформацією про виявлений об'єкт клацніть **Показати додаткові параметри**, а потім виберіть пункт **Виключити виявлення**.
- У контекстному меню "Файли журналу" за допомогою [майстрі створення виключень виявлених об'єктів](#).
- Виберіть пункти **Інструменти > Карантин**, клацніть правою кнопкою миші файл у карантині й в контекстному меню виберіть пункт **Відновити та виключити з перевірки**.

Критерій об'єкта виключення

- **Шлях:** обмежити виключення виявлених об'єктів для певного шляху.
- **Ім'я виявленого об'єкта:** якщо поруч із виключеним файлом указано ім'я [об'єкта виявлення](#), це означає, що файл виключений не цілком, а лише для відповідного об'єкта. Якщо цей файл пізніше буде інфіковано іншою шкідливою програмою, її буде виявлено.
- **Хеш:** дозволяє виключити файл у залежності від указанного хешу SHA-1 незалежно від типу, розташування, імені або розширення файлу.

Елементи керування

- **Додати:** додати новий запис для виключення об'єктів з очищення.
- **Редагувати:** редагувати вибрані елементи.
- **Видалити:** видаляє вибрані записи (щоб вибрати кілька записів, клацніть їх мишею, утримуючи клавішу CTRL).
- **Імпорт/Експорт:** імпорт і експорт виключень виявлених об'єктів є корисними функціями, якщо потрібно створити резервну копію поточних виключень для використання в майбутньому. Опція експорту параметрів також стане в пригоді в некерованих середовищах для користувачів, які бажають застосовувати власну конфігурацію на кількох комп'ютерах: вони зможуть легко перенести ці параметри, імпортувавши файл .txt.
 [Показати зразок формату файлу імпорту/експорту](#)

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}
```

```
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
```

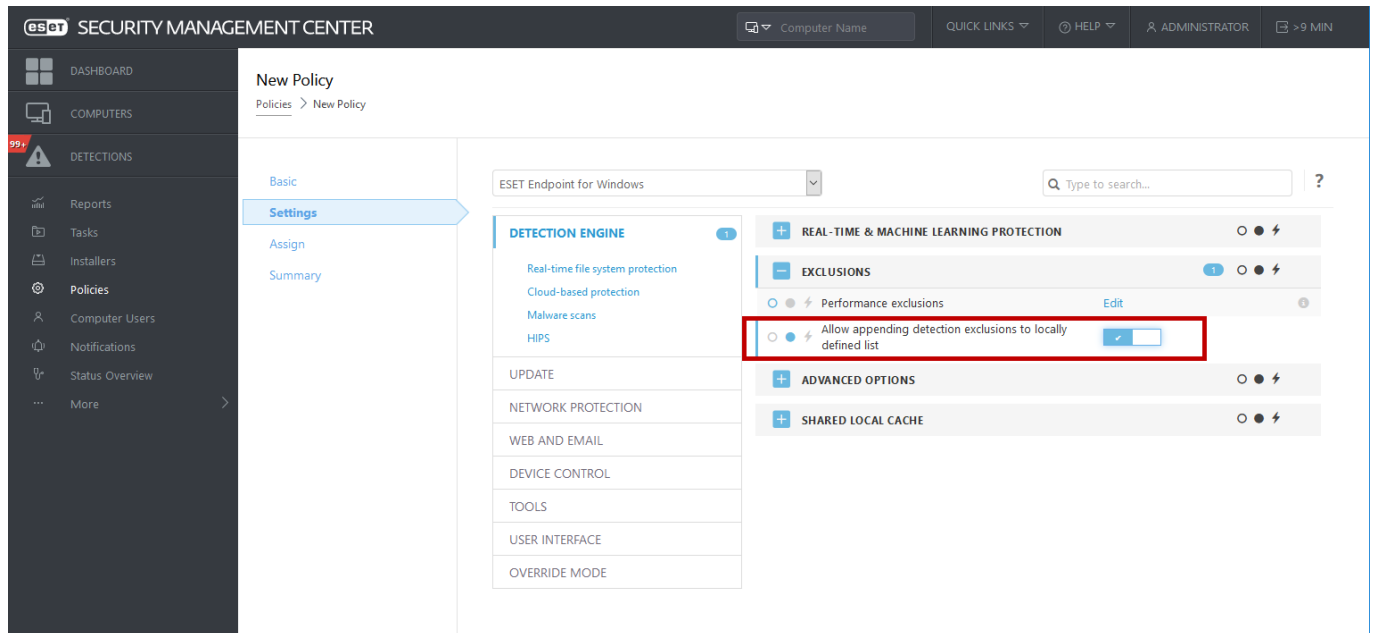
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Налаштування виключень об'єктів виявлення в ESET PROTECT

У програмі ESET PROTECT 8.0 є [новий майстер для керування виключеннями об'єктів виявлення](#). Створіть виключення об'єкта виявлення й застосуйте його до кількох комп'ютерів/груп.

Можливі виключення об'єктів виявлення можна змінити в ESET PROTECT

Якщо є наявний локальний список виключених об'єктів, адміністратор має застосувати політику з **Дозволити доповнювати локально визначений список виключеннями об'єктів виявлення**. Після цього додавання виключення виявлених об'єктів із ESET PROTECT буде працювати належним чином.



Додавання або зміна виключення об'єкта виявлення

Виключити виявлення

Потрібно вказати правильне ім'я виявленого об'єкта ESET. Правильне ім'я виявленого об'єкта див. в розділі [Файли журналу](#): у розкритому меню "Файли журналу" виберіть пункт **Виявлені об'єкти**. Це корисно, коли в ESET Endpoint Antivirus виявляються [помилкові зразки](#). Створювати виключення для реальних проникнень дуже небезпечно. Рекомендуємо виключати тільки певні файли або каталоги (клацніть ... у полі **Маска шляху** та (або) застосовуйте виключення лише на певний період часу. Виключення також застосовуються до [потенційно небажаних програм](#), потенційно небезпечних і підозрілих програм.

Див. також [Формат виключення шляху](#).

Змінити виключення

Шлях

C:\Recovery*.*

...

i

Хеш

i

Ім'я виявленого об'єкта

Win32/Adware.Optmedia

i

Коментар

i

OK

Скасувати

Див. пункт [Приклад виключень виявленого об'єкта](#).

Виключити хеш

Дозволяє виключити файл у залежності від указанного хешу SHA-1 незалежно від типу, розташування, імені або розширення файлу.

Змінити виключення ?

Шлях	<input type="text"/>	i
Хеш	2723cb8ca015209528d3fbdcaa801*	i
Ім'я виявленого об'єкта	<input type="text"/>	i
Коментар	SuperApi.exe	i

OK
Скасувати

Щоб виключити певний об'єкт виключення за його ім'ям, уведіть його дійсне ім'я:

Win32/Adware.Optmedia

Якщо для виявленого об'єкта виключення створюється у вікні сповіщень ESET Endpoint Antivirus, можна також використовувати такий формат:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Елементи керування

- **Додати:** виключити об'єкти з перевірки.
- **Редагувати:** редагувати вибрані елементи.
- **Видалити:** видаляє вибрані записи (щоб вибрати кілька записів, клацніть їх мишею, утримуючи клавішу CTRL).

Майстер створення виключень виявлених об'єктів

Виключення виявлених об'єктів також можна створити в контекстному меню [Файли журналу](#) (ця можливість недоступна для виявлених об'єктів шкідливого програмного забезпечення):

1. У головному вікні програми клацніть **Інструменти > Файли журналу**.
2. Правою кнопкою миші клацніть виявлений об'єкт у **журналі виявлених об'єктів**.
3. Клацніть **Створити виключення**.

Щоб виключити один або кілька виявлених об'єктів, у розділі **Критерій виключення** клацніть **Змінити критерій**:

- **Точно вказані файли:** виключити кожен файл із певним хешем SHA-1.
- **Виявлений об'єкт:** виключити кожен файл за певним іменем виявленого об'єкта.
- **Шлях + виявлений об'єкт:** виключити кожен файл за певним іменем виявленого об'єкта й шляхом, у якому вказано ім'я файлу (наприклад, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Рекомендований параметр попередньо вибраний за типом виявлення.

Перш ніж натиснути **Створити виключення**, можна додати **коментар**.

Виключення (7.1 і попередніх версій)

Для виключень у версії 7.1 і попередніх версіях функції [виключення в роботі](#) й [виключення виявлених об'єктів](#) були об'єднані.

Виключення

Тип	Докладніше
Шлях: Опис:	C:\Backup*.*
Шлях: Опис:	C:\pagefile.sys
Загроза: Шлях: Опис:	@NAME=Win32/Advare.Optmedia C:\Recovery*.*
Хеш: Опис:	678C1422DE867141B947EA700E8A2D6114AFAE97 SuperApi.exe

Додати

Редагувати

Видалити

Зберегти

Скасувати

Виключення процесів

Функція «Виключення процесів» дозволяє виключати процеси програм із компонента «Захист файлової системи в режимі реального часу». Щоб підвищити швидкість резервного копіювання, забезпечити цілісність процесу й доступність служб під час резервного копіювання застосовуються деякі методи, які конфліктують із системою захисту від шкідливого програмного забезпечення на рівні файлів. Деякі проблеми можуть виникати під час спроб динамічної міграції віртуальних машин. Єдиний дієвий спосіб уникнути обох ситуацій — деактивувати програму захисту від шкідливого програмного забезпечення. Якщо певні процеси (наприклад, процеси резервного копіювання) виключено, усі операції з файлами, пов'язані з цими виключеними процесами, ігноруються й розглядаються як безпечні. Це дозволяє мінімізувати перешкоди для процесу резервного копіювання. До створення виключень необхідно підходити обачно, адже виключений із перевірки інструмент резервного копіювання може отримати доступ до інфікованих файлів, а відповідне попередження системи безпеки не буде ініційоване. Саме тому розширені дозволи доступні тільки в модулі захисту в режимі реального часу.

Виключення процесів допомагають мінімізувати ризик потенційних конфліктів і підвищити швидкодію виключених програм, що позитивно впливає на загальну швидкодію й стабільність операційної системи. Виключення процесу (програми) — це виключення відповідного виконуваного файлу (.exe).

Можна додати виконувані файли в список виключених процесів у розділі **Додаткові**

параметри (F5) > Ядро виявлення > Захист файлової системи в режимі реального часу > Виключення процесів.

Ця функція призначена для виключення інструментів резервного копіювання. Виключення процесу інструмента резервного копіювання зі сканування не тільки забезпечує стабільність системи, але й виключає негативний вплив сканування на продуктивність резервного копіювання, оскільки воно не вповільнюється під час сканування.

Щоб відкрити вікно керування **Виключення процесів**, клацніть **Змінити**. У цьому вікні можна [додати](#) виключення й знайти виконуваний файл (наприклад, *Backup-tool.exe*), який буде виключено зі сканування.

✓ Щойно файл .exe буде додано до виключень, активність цього процесу не буде відстежуватись програмою ESET Endpoint Antivirus. Окрім того, сканування не запускатиметься для жодної операції з файлами, виконуваної цим процесом.

⚠ Якщо для вибору виконуваних файлів ви не використовуєте файловий провідник, необхідно вручну ввести повний шлях до виконуваного файлу. Інакше виключення не буде працювати правильно, а [система запобігання вторгненням \(HIPS\)](#) може повертати помилки.

Можна також **Змінити** наявні процеси або **Видалити** їх із виключень.

i Це виключення ігнорується модулем [захисту доступу до інтернету](#), тому якщо виключити виконуваний файл веб-браузера, завантажені файли все одно скануватимуться. Це дозволяє виявляти загрози. Цей сценарій наведено лише для довідки. Ми не рекомендуємо створювати виключення для веб-браузерів.

Додавання або зміна виключень процесів

У цьому діалоговому вікні можна **додавати** процеси, виключені з ядра виявлення. Виключення процесів допомагають мінімізувати ризик потенційних конфліктів і підвищити швидкодію виключених програм, що позитивно впливає на загальну швидкодію й стабільність операційної системи. Виключення процесу (програми) — це виключення відповідного виконуваного файлу (.exe).

Виберіть шлях до файлу потрібної програми. Для цього клацніть ... (наприклад, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводьте назву програми.

✓ Щойно файл .exe буде додано до виключень, активність цього процесу не буде відстежуватись програмою ESET Endpoint Antivirus. Окрім того, сканування не запускатиметься для жодної операції з файлами, виконуваної цим процесом.


⚠ Якщо для вибору виконуваних файлів ви не використовуєте файловий провідник, необхідно вручну ввести повний шлях до виконуваного файлу. Інакше виключення не буде працювати правильно, а [система запобігання вторгненням \(HIPS\)](#) може повертати помилки.

Можна також **Змінити** наявні процеси або **Видалити** їх із виключень.

Виключення HIPS

Виключення дозволяють виключати процеси із системи глибокої перевірки поведінки HIPS.

Щоб виключити об'єкт, клацніть **Додати** й уведіть шлях до об'єкта або виберіть його в структурі дерева. Окрім того, вибрані записи можна **змінити** або **видалити**.

 Див. розділ [Виключення](#).

Параметри ThreatSense

ThreatSense – це технологія, яка складається з багатьох комплексних методів виявлення загроз. Вона проактивна, тобто забезпечує захист навіть у перші години поширення нової загрози. У ній поєднуються різні методи (аналіз коду, емуляція коду, родові сигнатури, сигнатури вірусів), які працюють узгоджено, що суттєво підвищує рівень захисту системи. Підсистема сканування може контролювати одночасно кілька потоків даних, тим самим збільшуючи ефективність системи та швидкість виявлення загроз. Окрім того, технологія ThreatSense успішно знищує руткити.

У налаштуваннях підсистеми ThreatSense можна задати кілька параметрів сканування:

- типи й розширення файлів, які потрібно сканувати;
- комбінація різних методів виявлення;
- рівні очистки тощо.

Щоб відкрити вікно параметрів, натисніть **Параметри ThreatSense** у вікні додаткових параметрів будь-якого модуля, у якому використовується технологія ThreatSense (її описано нижче). Для різних сценаріїв інколи потрібно налаштувати індивідуальні конфігурації. Зважаючи на це, підсистему ThreatSense можна налаштовувати окремо для кожного з таких модулів захисту:

- Захист файлової системи в режимі реального часу
- Сканування в неактивному стані
- Сканування під час запуску
- Захист документів
- Захист поштового клієнта
- Захист доступу до Інтернету
- Сканування комп'ютера

Параметри ThreatSense оптимізовано для кожного модуля, тому їх змінення може суттєво вплинути на роботу системи. Наприклад, якщо ввімкнути обов'язкове сканування упакованих програм або розширену евристику для модуля захисту файлової системи в режимі реального часу, робота системи може значно сповільнитися (зазвичай такі методи використовуються лише для сканування щойно створених файлів). Не рекомендуємо змінювати параметри ThreatSense за замовчуванням для всіх модулів, окрім перевірки комп'ютера.

Перевірити об'єкти

У цьому розділі можна визначати компоненти комп'ютера та файли, які скануватимуться на наявність проникнень.

Оперативна пам'ять: сканування на предмет проникнень, орієнтованих на оперативну пам'ять комп'ютера.

Завантажувальні сектори/UEFI: сканування завантажувальних секторів на наявність шкідливого програмного забезпечення в головному завантажувальному записі. [Докладніше про UEFI див. в глосарії](#).

Файли електронної пошти: програма підтримує такі розширення: DBX (Outlook Express) і EML.

Архіви: програма підтримує розширення ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE та багато інших.

Саморозпакувальні архіви: ці архіви (SFX) можуть розпаковуватися самостійно.

Упаковані програми: після виконання ці програми (на відміну від стандартних типів архіву) розпаковуються в пам'яті. Окрім стандартних статичних пакувальників (UPX, yoda, ASPack, FSG та інших), сканер здатен розпізнати кілька додаткових типів пакувальників завдяки емуляції коду.

Опції сканування

Виберіть методи сканування системи на наявність проникнень. Доступні наведені нижче варіанти:

Евристика: алгоритм, який аналізує зловмисні дії програм. Основна перевага цієї технології – можливість виявляти шкідливе програмне забезпечення, яке не існувало під час формування попередньої версії обробника виявлення або не було в ній зареєстроване. Недолік – (дуже мала) імовірність помилкових сигналів.

Розширені евристики/DNA-підписи – у розширеній евристиці реалізовано унікальний евристичний алгоритм, розроблений компанією ESET, який оптимізовано для виявлення комп'ютерних черв'яків, троянських програм і написано мовами програмування високого рівня. Використання розширеної евристики значно розширює можливості продуктів ESET для виявлення загроз. Сигнатури – надійний засіб виявлення й визначення вірусів. Автоматична система оновлення дає змогу отримувати нові сигнатури протягом кількох годин із моменту виявлення загрози. Недолік використання сигнатур полягає в тому, що визначити можна лише відомі віруси (або їх дещо змінені версії).

Очистка

[Параметри очистки](#) визначають поведінку ESET Endpoint Antivirus під час очистки інфікованих об'єктів.

Виключення

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст файлу. Цей розділ налаштування параметрів підсистеми ThreatSense дає змогу визначити типи файлів, які потрібно сканувати.

Інше

Під час налаштування параметрів підсистеми ThreatSense для сканування комп'ютера за вимогою доступні також наведені нижче опції розділу **Інше**.

Перевіряти альтернативні потоки даних (ADS) – файлова система NTFS використовує альтернативні потоки даних, тобто асоціації файлів і папок, невидимі в разі застосування звичайних методів перевірки. Багато загроз намагаються обійти виявлення, маскуючись як альтернативні потоки даних.

Запускати фонові перевірки з низьким пріоритетом: на кожну процедуру сканування витрачається певний обсяг ресурсів системи. Якщо запущено програму, яка спричиняє значне використання ресурсів системи, можна активувати фонову перевірку з низьким пріоритетом і зберегти ресурси для програм.

Реєструвати всі об'єкти: у [журналі сканування](#) будуть відображені всі файли, проскановані в саморозпакувальних архівах, навіть неінфіковані (можуть генеруватися великі об'єми даних, що збільшуватиме розмір файлу журналу).

Увімкнути Smart-оптимізацію: коли Smart-оптимізацію увімкнено, система використовує оптимальні параметри для забезпечення найефективнішого рівня сканування, одночасно підтримуючи найвищу швидкість цього процесу. Різноманітні модулі захисту виконують інтелектуальне сканування, використовуючи різні методи й застосовуючи їх до відповідних типів файлів. Якщо Smart-оптимізацію вимкнено, під час сканування застосовуються лише визначені користувачем у ядрі ThreatSense параметри для певних модулів.

Зберегти час останнього доступу: установіть цей прапорець, щоб зберігати початковий час доступу до сканованих файлів, а не оновлювати їх (наприклад, якщо цього потребує робота систем резервного копіювання даних).

Обмеження

У розділі "Обмеження" можна вказати максимальний розмір об'єктів і число рівнів вкладених архівів, які необхідно сканувати.

Параметри об'єкта

Максимальний розмір об'єкта: визначає максимальний розмір об'єктів, які потрібно сканувати. Після встановлення цього параметра відповідний антивірусний модуль скануватиме лише об'єкти, розмір яких не перевищуватиме зазначений. Цей параметр рекомендується змінювати тільки досвідченим користувачам, у яких може виникнути потреба виключити з перевірки великі об'єкти. Значення за замовчуванням: необмежено.

Максимальний час перевірки об'єкта (с): визначає максимальний час перевірки файлів у контейнері (наприклад, архіві RAR/ZIP або електронному листі з кількома вкладеннями). Не застосовується для окремих файлів. Якщо в поле введено користувацьке значення, після завершення часу перевірка завершиться за найближчої можливості, навіть якщо в контейнері залишаться неперевірені файли. Якщо в архіві містяться великі файли, перевірка завершиться лише після того, як з архіву буде видобуто файл (наприклад, якщо користувач указав 3 секунди, а на видобування потрібно щонайменше 5 секунд). Інші файли в архіві не будуть перевірятися після завершення вказаного часу. Щоб обмежити час перевірки, зокрема для

великих архівів, скористайтесь параметрами **Максимальний розмір об'єкта** й **Максимальний розмір файлу в архіві** (не рекомендується через ризики для безпеки). Значення за замовчуванням: необмежено.

Параметри перевірки архівів

Глибина архіву: визначає максимальну глибину сканування архіву. За замовчуванням використовується файл: 10.

Максимальний розмір файлу в архіві: за допомогою цього параметра можна вказати максимальний розмір для файлів, що містяться в архівах (у видобутому стані), які потрібно просканувати. Максимальне значення 3 ГБ.

i Змінювати значення за замовчуванням не рекомендується, оскільки за нормальних обставин для цього немає причин.

Рівні очистки

Щоб відкрити параметри рівня очищення для бажаного модуля захисту, розгорніть **параметри ThreatSense** (наприклад, **Захист файлової системи в режимі реального часу**), а потім клацніть **Очистка**.

Захист у режимі реального часу та інші модулі захисту мають указані нижче рівні виправлення (очищення).

Виправлення в ESET Endpoint Antivirus 9

Рівень очистки	Опис
Завжди виправляти виявлені об'єкти	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, для системних файлів) виявлений об'єкт неможливо виправити, тому він залишатиметься у вихідному розташуванні. Завжди виправляти виявлені об'єкти — рекомендований параметр за замовчуванням у керованому середовищі .
Виправити виявлені об'єкти, якщо безпечно. В іншому разі залишити все як є	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, системні файли або архіви з чистими та інфікованими файлами), якщо виявлений об'єкт не можна виправити, він залишається у вихідному розташуванні.
Виправити виявлені об'єкти, якщо безпечно. В іншому разі надіслати запит	Спробувати виправлення виявленого об'єкта під час очищення об'єктів. У деяких випадках, коли жодну операцію виконати неможливо, кінцевий користувач отримує інтерактивне сповіщення, де необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей параметр рекомендовано в більшості випадків.
Завжди запитувати кінцевого користувача	Під час очищення об'єктів для кінцевого користувача відкривається вікно, у якому необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей рівень призначений для більш досвідчених користувачів, які знають, що потрібно зробити у випадку виявлення.



Список розширень файлів, виключених із перевірки

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст файлу. Цей розділ налаштування параметрів підсистеми ThreatSense дає змогу визначити типи файлів, які потрібно сканувати.

i Не слід плутати з іншими типами [Виключень](#).

За замовчуванням скануються всі файли. Будь-яке розширення можна додати до списку файлів, виключених із перевірки.

Іноді доцільно виключити з перевірки певні типи файлів, якщо сканування таких файлів заважає належній роботі відповідних програм. Наприклад, рекомендується виключати файли з розширеннями `.edb`, `.eml` і `.tmp` в разі використання серверів Microsoft Exchange.

Щоб додати до списку нове розширення, натисніть кнопку **Додати**. Уведіть розширення в пусте поле (наприклад, `tmp`) та натисніть кнопку **ОК**. Якщо вибрати параметр **Введіть кілька значень**, можна додати декілька розширень файлів, розділяючи їх рисками, комами або крапкою з комою. Наприклад, у розкритому меню виберіть **Крапка з комою** для розділового знаку та введіть `edb;eml;tmp`. Можна використовувати спеціальний символ `?` (знак питання). Він позначає будь-який символ (наприклад, `?db`).

i Щоб дізнатися точне розширення (якщо є) файлу в ОС Windows, відкрийте сторінку **Панель керування**, виберіть **Параметри папки** та перейдіть на вкладку **Вигляд**. Після цього зніміть прапорець **Приховувати розширення для зареєстрованих типів файлів**.

Додаткові параметри ThreatSense

Додаткові параметри ThreatSense для новостворених і змінених файлів: імовірність виявлення інфекції в новостворених або змінених файлах порівняно вища, ніж у наявних. Тому програма перевіряє ці файли з використанням додаткових параметрів сканування. Крім традиційних методів сканування на основі сигнатур вірусів, також використовується розширена евристика, орієнтована на виявлення нових загроз до випуску оновленого обробника виявлення. Окрім новостворених файлів, сканування поширюється також на саморозпакувальні файли (`.sfx`) та упаковані програми (запаковані виконувані файли). За замовчуванням архіви перевіряються до 10-ого рівня вкладення, причому сканування виконується незалежно від їх фактичного розміру. Щоб змінити параметри сканування архіву, зніміть прапорець **Параметри сканування архівів за замовчуванням**.


Докладніше про упаковані програми, саморозпакувальні архіви й розширену евристику див. у розділі [Налаштування параметрів підсистеми ThreatSense](#).

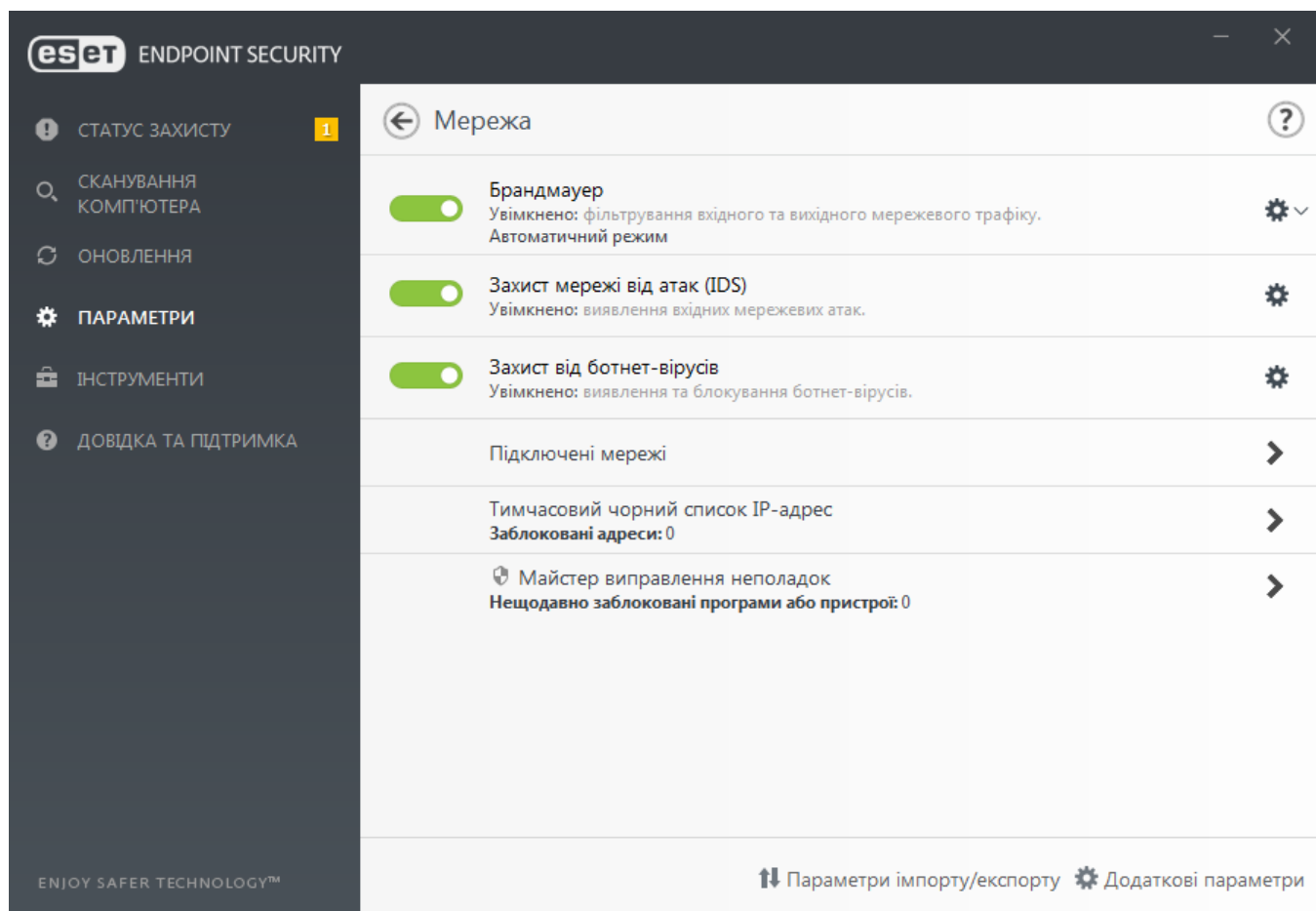
Додаткові параметри ThreatSense для виконуваних файлів: за замовчуванням [розширені евристики](#) використовуються в разі виконання файлів. Коли цей параметр увімкнено,

наполегливо рекомендуємо також активувати [Smart-оптимізацію](#) й ESET LiveGrid®, щоб запобігти зниженню продуктивності системи.

Мережа

Розділ **Мережа** забезпечує швидкий доступ до таких компонентів або налаштувань розділу "Додаткові параметри":

- **Захист мережі від атак (IDS):** аналізує вміст мережевого трафіку й захищає від мережевих атак. Увесь трафік, який уважатиметься шкідливим, буде заблоковано. ESET Endpoint Antivirus сповістить вас про підключення до незахищеної бездротової мережі або мережі зі слабким захистом.
- **Захист від ботнет-вірусів:** швидко й точно визначає зловмисне ПЗ в системі. Щоб тимчасово вимкнути захист від ботнет-вірусів, натисніть  (не рекомендовано).
- **Тимчасовий чорний список IP-адрес:** список IP-адрес, визначених як джерело атак і доданих до чорного списку, що блокує підключення до них протягом певного періоду часу. Щоб отримати додаткову інформацію, клацніть цей параметр і натисніть F1.
- **Майстер виправлення неполадок:** допомагає вирішувати проблеми з підключенням, спричинені брандмауером ESET. Докладніше див. у розділі [Майстер виправлення неполадок](#).



Захист від мережевих атак

Увімкнути захист мережі від атак (IDS): аналізує вміст мережевого трафіку й захищає від мережевих атак. Увесь трафік, який вважатиметься шкідливим, буде заблоковано.

Увімкнути захист від ботнет-вірусів: виявляє та блокує обмін даними зі зловмисними командними серверами на основі типових шаблонів, коли комп'ютер заражено, а бот намагається встановити зв'язок. [Більш докладну про захист від ботнет-вірусів див. в глосарії.](#)

Правила IDS: Ця опція дозволяє налаштовувати додаткові параметри фільтрування, які виявлятимуть різні типи можливих зловмисних атак і проникнень.

Захист від атак повним перебором

Захист від атак повним перебором блокує атаки за допомогою вгадування пароля до сервісів RDP й SMB. Атака повним перебором — це метод добору потрібного пароля через систематичний перебір усіх можливих комбінацій букв, цифр і символів. Щоб налаштувати захист від атак повним перебором, у [головному вікні програми](#) натисніть **Налаштування > Додаткові параметри (F5) > Захист мережі > Захист мережі від атак > Захист від атак повним перебором.**

Захист від атак повним перебором: програма ESET Endpoint Antivirus перевіряє вміст мережевого трафіку й блокує спроби атак за допомогою вгадування пароля.

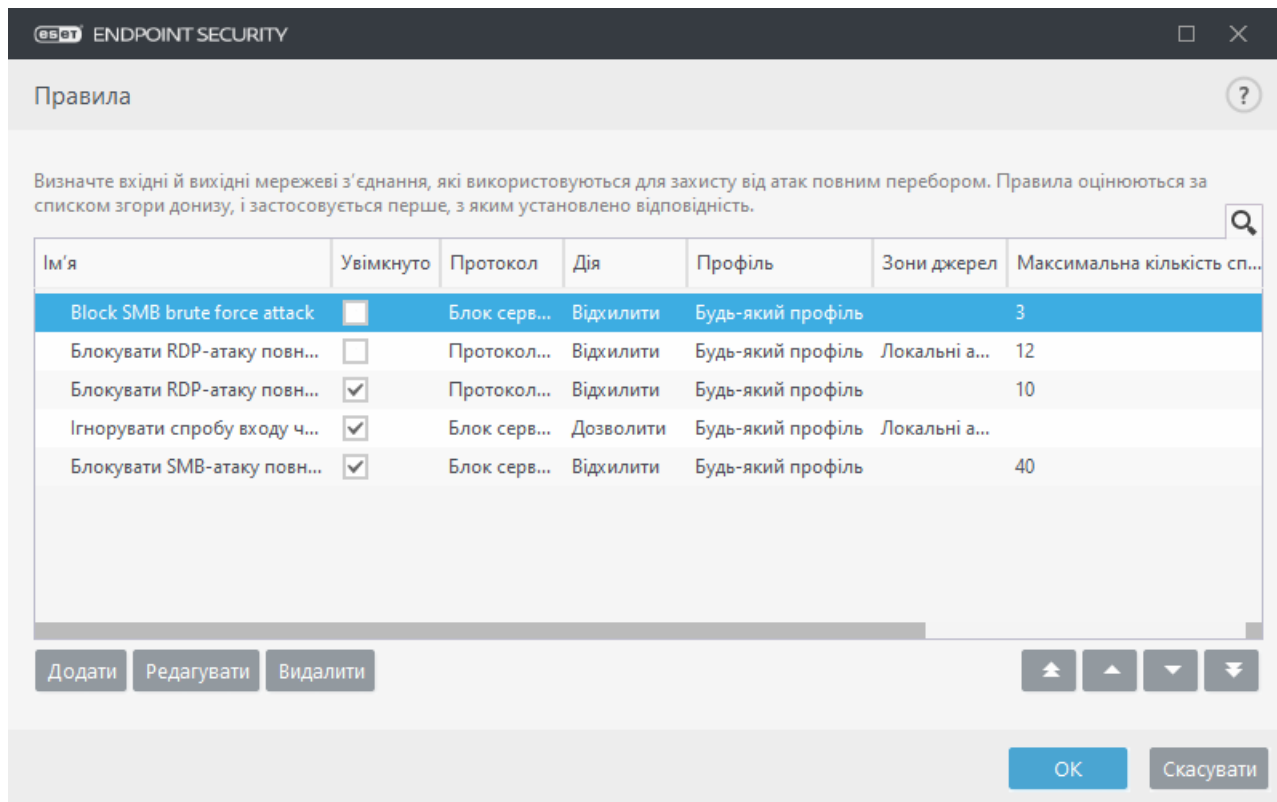
Правила: тут можна створити, редагувати й переглядати правила для вхідних і вихідних мережевих з'єднань. Більш докладну інформацію див. в розділі [Правила](#).





Виключення: список виключених виявлених об'єктів, заданих IP-адресою або шляхом до програми. Ви можете створювати й редагувати виключення на консолі ESET PROTECT. Більш докладну інформацію див. в розділі [Виключення](#).

Правила

Правила захисту від атак повним перебором дають змогу створювати, редагувати й переглядати правила для вхідних і вихідних мережевих з'єднань. Попередньо встановлені правила не можна редагувати чи видаляти.

Керування правилами захисту від атак повним перебором



- **Додати:** клацніть, щоб створити нове правило захисту від атак повним перебором.
- **Редагувати:** клацніть, щоб змінити наявне правило захисту від атак повним перебором.
- **Видалити:** виберіть і клацніть, якщо потрібно видалити наявне виключення зі списку правил IDS.
-     **Вгору / у самий верх / вниз / у самий низ:** дає змогу визначати рівень пріоритетності правил.



Якщо кілька правил блокування відповідають умовам виявлення, то для забезпечити максимально можливого рівня захисту застосовується правило блокування з найнижчим значенням **Максимальна кількість спроб**, навіть якщо це правило розташовано нижче в списку правил.

Редактор правил

ESet ENDPOINT SECURITY [X]

Змінити правило [?]

Ім'я: Block SMB brute force attack

Увімкнено: ☐ X

Дія: Відхилити [v]

Протокол: Блок серверних повідомлень (SMB) [v]

Профіль: Будь-який профіль [v] [i]

Максимальна кількість спроб: 3 [i]

Період зберігання чорного списку (хвилини): 20 [i]

IP-адреса джерела: [] [i]

Зони джерел [i]

[Додати] [Видалити]

[OK]

Ім'я: ім'я правила.

Увімкнено: вимкніть цей параметр за допомогою повзунка, щоб зберегти правило у списку, але не застосовувати його.

Дія: виберіть, чи потрібно **відхиляти** або **дозволяти** підключення за відповідних параметрів правила.

Протокол: протокол зв'язку, який правило перевірятиме.

Профіль: спеціальні правила можна задати й застосувати для певних профілів.

Максимальна кількість спроб — Максимальна кількість дозволених спроб повторення атаки, доки IP-адресу не буде заблоковано й додано в чорний список.

Період зберігання чорного списку (хвилини): задає час, протягом якого адреса буде міститися в чорному списку.

IP-адреса джерела: список IP-адрес, діапазонів або підмереж. Адреси потрібно розділяти комами.

Зони джерел: дає змогу додати попередньо визначену або створену зону з діапазоном IP-адрес. Для цього потрібно клацнути **Додати**.

Виключення

Виключення захисту від атак повним перебором можна використовувати для вимкнення виявлення таких атак у випадках, які відповідають заданим критеріям. Ці виключення створюються ESET PROTECT на основі виявлених атак повним перебором.

Стовпці


- **Виявлений об'єкт:** уведіть виявлений об'єкт.
- **Програма :** виберіть шлях до файлу потрібної програми. Для цього клацніть ... (наприклад, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводьте назву програми.
- **Віддалена IP-адреса:** список віддалених адрес IPv4 або IPv6/діапазонів IP-адрес/підмереж. Адреси потрібно розділяти комами.


Керування виключеннями

Виключення відображатимуться, якщо адміністратор [створить виключення захисту від атак повним перебором на веб-консолі ESET PROTECT](#). Виключення можуть містити тільки правила дозволів і оцінюються перед застосуванням правил IDS.

Розширені параметри фільтрації

У розділі "Захист мережі від атак" можна налаштувати додаткові параметри фільтрації для виявлення деяких типів атак і вразливостей, які можуть бути використані проти вашого комп'ютера.

 У деяких випадках сповіщення про заблоковані зв'язки не відображатимуться. Зверніться до розділу [Ведення журналу й створення правил або виключень на основі журналу](#), щоб дізнатися, як переглянути всі заблоковані зв'язки в журналі брандмауера.

 Доступність певних параметрів у розділі "**Додаткові параметри**" (F5) > **Захист мережі** > **Захист мережі від атак** може різнитися залежно від типу або версії вашого продукту ESET Endpoint і модуля брандмауера, а також від версії операційної системи. Деякі з них можуть бути доступні тільки для ESET Endpoint Security.

Виявлення вторгнення

- **Протокол SMB:** виявляє та блокує різноманітні проблеми, пов'язані з безпекою протоколу SMB, а саме:
- **Виявлення виклику автентифікації неправомірним сервером:** захищає від атак, які під час автентифікації використовують неправомірний виклик із метою отримання облікових даних користувача.
- **Виявлення обходу IDS під час відкриття іменованого каналу:** виявлення відомих методів обходу, які використовуються для відкриття іменованих каналів MSRPC в протоколі SMB.
- **Виявлення CVE** (Common Vulnerabilities and Exposures – поширені слабкі місця й помилки):

упроваджені методи виявлення різноманітних атак, форм, слабких місць у системі безпеки та проникнень через протокол SMB. Відвідайте [веб-сайт CVE за адресою cve.mitre.org](https://cve.mitre.org), який надає можливості пошуку й отримання докладнішої інформації про ідентифікатори CVE.

- **Протокол RPC:** виявлення й блокування різноманітних слабких місць і помилок у системі віддаленого виклику процедур для середовища розподілених розрахунків (Distributed Computing Environment, DCE).
- **Протокол RDP:** виявлення й блокування різноманітних слабких місць у протоколі RDP (див. вище).
- **Блокувати небезпечну адресу після виявлення атаки:** додавання до чорного списку IP-адрес, визначених як джерело атаки, що запобігає з'єднанню з ними протягом певного періоду часу.
- **Відображати сповіщення після виявлення атаки:** вмикає відображення сповіщень у системному треї в нижньому правому куті екрана.
- **Також відображати сповіщення про атаки, спрямовані на слабкі місця в системі безпеки:** сповіщає про виявлені атаки, спрямовані на слабкі місця в системі безпеки, або про спроби проникнення загрози в систему в такий спосіб.

Перевірка пакетів

- **Дозволити вхідні запити спільних адміністративних ресурсів у протоколі SMB** – адміністративними спільними ресурсами називаються мережеві спільні ресурси, які використовують розділи на жорсткому диску в системі (C\$, D\$ тощо) разом із системною папкою (ADMIN\$). Заборонивши підключення до адміністративних спільних ресурсів, можна усунути багато загроз для безпеки. Наприклад, черв'як Conficker для підключення до адміністративних спільних ресурсів здійснює атаки за словником.
- **Відхилити застарілі (непідтримувані) діалекти SMB:** відхилення сеансів SMB, що використовують застарілі діалекти SMB, не підтримувані IDS. Сучасні операційні системи Windows підтримують застарілі діалекти SMB з метою забезпечення сумісності з попередніми версіями (наприклад, Windows 95). Зловмисник може використовувати застарілий діалект під час сеансу SMB, щоб уникнути перевірки трафіку. Активуйте відхилення застарілих діалектів SMB, якщо ваш пристрій не використовується для обміну файлами (або комунікації SMB загалом) із комп'ютером під керуванням старих версій Windows.
- **Відхилити SMB без розширення функції безпеки:** розширена функція безпеки може використовуватися під час сеансу SMB з метою забезпечення надійнішого механізму автентифікації, ніж метод "запит-відповідь" для автентифікації диспетчера локальної мережі. Цей метод вважається слабким, і використовувати його не рекомендується.
- **Дозволити виклики Security Account Manager:** докладніше про цю службу див. у розділі [\[MS-SAMR\]](#).
- **Дозволити виклики Local Security Authority:** докладніше про цю службу див. у розділах [\[MS-LSAD\]](#) і [\[MS-LSAT\]](#).
- **Дозволити виклики Remote Registry:** докладніше про цю службу див. у розділі [\[MS-RRP\]](#).
- **Дозволити виклики Service Control Manager:** докладніше про цю службу див. у розділі [\[MS-SCMR\]](#).

- **Дозволити виклики служби сервера:** докладніше про цю службу див. у розділі [\[MS-SRVS\]](#).
- **Дозволити виклики інших служб.** MSRPC — це реалізація механізму DCE RPC від компанії Microsoft. Окрім того, MSRPC може використовувати іменовані канали, виконувати за протоколом SMB (обмін файлами в мережі), для транспортування даних (ncacn_np transport). Служби MSRPC дають змогу отримувати віддалений доступ до систем Windows і керувати ними. У системі Windows MSRPC було виявлено кілька вразливих місць, які використовувалися "дикими вірусами" (черв'яки Conficker, Sasser тощо). Заборонивши комунікацію з непотрібними службами MSRPC, можна усунути багато ризиків для безпеки (віддалене виконання коду, відмова в обслуговуванні тощо).

Правила IDS

В деяких випадках [служба виявлення вторгнень \(Intrusion Detection Service, IDS\)](#) може класифікувати зв'язок між маршрутизаторами або іншими внутрішніми пристроями в мережі як потенційну атаку. Для обходу IDS можна додати відомий безпечний адрес до списку адрес, виключених із зони IDS.

- i Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:
- [Створення правил IDS на клієнтських робочих станціях у ESET Endpoint Antivirus](#)
 - [Створення правил IDS для клієнтських робочих станцій у ESET PROTECT](#)





Стовпці

- **Виявлений об'єкт:** уведіть виявлений об'єкт.
- **Програма :** виберіть шлях до файлу потрібної програми. Для цього клацніть ... (наприклад, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводьте назву програми.
- **Віддалена IP-адреса:** список віддалених адрес IPv4 або IPv6 / діапазонів IP-адрес / підмереж. Адреси потрібно розділяти комами.
- **Блокувати:** кожен системний процес має власну поведінку за замовчуванням, а також призначену йому дію («блокувати» або «дозволити»). Щоб змінити поведінку за замовчуванням для ESET Endpoint Antivirus, можна вибрати потрібний параметр («блокувати» або «дозволити») в розкритому меню.
- **Сповістити :** виберіть Так, щоб показати [Сповіщення на робочому столі](#) вашого комп'ютера. Виберіть Ні, якщо не потрібно показувати сповіщення на робочому столі. Доступні значення: За замовчуванням/Так/Ні.
- **Журнал:** виберіть **Так**, щоб записувати події у файли журналу [ESET Endpoint Antivirus](#). Виберіть **Ні**, щоб не записувати події у файли журналу. Доступні значення: **За замовчуванням/Так/Ні**.

Вкладка "Виключення" відображатиметься, якщо адміністратор [створить виключення IDS у ESET PROTECT Web Console](#). Виключення IDS можуть містити тільки правила дозволів і оцінюються перед правилами IDS.

Керування правилами IDS

- **Додати:** клацніть, щоб створити нове правило IDS.
- **Редагувати:** клацніть, щоб змінити наявне правило IDS.

- **Видалити:** виберіть і клацніть, якщо потрібно видалити наявне виключення зі списку правил IDS.
-     **Угору/у самий верх/униз/у самий низ:** дає змогу коригувати рівень пріоритетності для правил (виключення оцінюються згори вниз).

Вам потрібно, щоб відображалось сповіщення й кожна подія реєструвалася в журналі.

1. Клацніть **Додати**, щоб додати нове правило IDS.
2. Виберіть певне оповіщення в розкритому меню **Виявлений об'єкт**.
3. Клацніть ... і виберіть шлях до файлу програми, для якої необхідно застосувати сповіщення.
4. Залиште пункт **За замовчуванням** у розкритому меню **Блокувати**. Це призведе до успадкування дії за замовчуванням, застосованої до ESET Endpoint Antivirus.
5. В обох розкритих меню **Сповістити** й **Журнал** установіть пункт **Так**.
6. Щоб зберегти це сповіщення, натисніть кнопку **ОК**.

Якщо потрібно вимкнути сповіщення, які постійно відображаються, інформуючи про хибні загрози:

1. Клацніть **Додати**, щоб додати нове розширення IDS.
2. Виберіть певне оповіщення в розкритому меню **Виявлений об'єкт**, наприклад, **Сеанс SMB без розширень безпеки**.
3. У розкритому меню виберіть пункт **Вхідний**, якщо це вхідне з'єднання.
4. У розкритому меню **Сповістити** виберіть пункт **Ні**.
5. У розкритому меню **Журнал** виберіть пункт **Так**.
6. Залиште поле **Програма** пустим.
7. Якщо запит на зв'язок не знаходить від певної IP-адреси, залиште поле **Віддалені IP-адреси** пустим.
8. Щоб зберегти це сповіщення, натисніть кнопку **ОК**.

Заблоковано можливу загрозу

Подібна ситуація може виникнути тоді, коли програма на комп'ютері намагається передати зловмисний код на інший комп'ютер у мережі, використовуючи вразливе місце системи безпеки, або навіть коли хтось намагається просканувати порти у вашій мережі.

Загроза: ім'я загрози.

Джерело: мережева адреса джерела.

Об'єкт: мережева адреса об'єкта.

Припинити блокування: створити правило IDS для можливої загрози з параметрами, що дозволяють обмін даними.

Продовжувати блокування: блокувати виявлену загрозу. Щоб створити правило IDS із параметрами блокування обміну даними для цієї загрози, установіть прапорець **Більше не сповіщати**.



Інформація, що відображається в цьому вікні сповіщень, може відрізнятися залежно від виявленої загрози.

Більш докладну інформацію про загрози або пов'язані теми див. в розділах [Типи віддалених атак](#) або [Типи виявлених об'єктів](#).

Майстер усунення помилок

Майстер виправлення неполадок допомагає вирішувати проблеми з підключенням, спричинені брандмауером ESET. Із розкривного меню виберіть проміжок часу, протягом якого блокуватиметься зв'язок. У списку нещодавно заблокованих зв'язків наводяться короткі відомості про тип програми чи пристрою, репутацію та загальну кількість програм або пристроїв, заблокованих протягом зазначеного проміжку часу. Щоб дізнатися докладніше про заблокований зв'язок, натисніть **Докладніше**. Наступний крок – це розблокування програми або пристрою, у яких є проблеми з підключенням.

Якщо натиснути **Розблокувати**, раніше заблокований зв'язок буде знову дозволено. Якщо проблеми із програмою не зникнуть або пристрій продовжуватиме працювати неправильно, натисніть **Програма досі не працює**, і всі зв'язки, заблоковані для цього пристрою, буде дозволено. Якщо проблема не зникає, перезавантажте комп'ютер.

Натисніть **Показати зміни**, щоб переглянути правила, створені майстром.

Натисніть **Розблокувати інший**, щоб усунути неполадки з підключенням іншого пристрою або програми.

Відомі мережі

У разі частого підключення комп'ютера до сторонніх мереж або мереж спільного використання, рекомендується перевіряти їхню надійність. Після розпізнавання мережі ESET Endpoint Antivirus може визначати її надійність (домашня/робоча) на основі різноманітних параметрів, указаних у розділі **Ідентифікаційні дані мережі**. Комп'ютери часто підключаються до мереж з IP-адресами, подібними до адреси довіреної мережі. У таких випадках ESET Endpoint Antivirus може сприймати невідому мережу як довірену (домашню/робочу). Рекомендуємо використовувати **Ідентифікаційні дані мережі**, щоб уникнути подібних ситуацій.

Коли мережевий адаптер підключається до мережі або його налаштування змінюються, ESET Endpoint Antivirus здійснюватиме пошук у списку відомих мереж запису, що збігатиметься з параметрами нової мережі. Якщо параметри в розділах **Ідентифікаційні дані мережі** й **Автентифікація мереж** (необов'язково) збігатимуться, у цьому інтерфейсі мережу буде позначено як підключену. Якщо не знайдено жодної відомої мережі, на основі ідентифікаційних даних створюється нова мережа, яка розпізнаватиметься під час наступного підключення до неї. За замовчуванням до нової мережі застосовується тип захисту **Мережа спільного використання**. У діалоговому вікні **Виявлено нове мережеве підключення** можна вибрати тип захисту **Ненадійна мережа**, **Надійна мережа** чи **Використовувати параметр Windows**. Якщо мережевий адаптер підключено до відомої мережі, позначеної як **Надійна мережа**, локальні підмережі адаптера додаються до довіреної зони.

Тип захисту нових мереж: виберіть один із таких варіантів: Використовувати параметр Windows, Запитувати користувача або Позначити як загальнодоступну (за замовчуванням для нових мереж).

i Якщо вибрати **Використовувати параметр Windows**, діалогове вікно не з'являтиметься, а тип захисту підключеної мережі буде автоматично визначено відповідно до параметрів Windows. Тому деякі функції (наприклад, обмін файлами та віддалений робочий стіл) будуть доступні в разі підключення до нових мереж.

Відомі мережі можна налаштувати вручну у вікні [Редактор відомих мереж](#).

Редактор відомих мереж

Відомі мережі можна налаштувати вручну. Для цього виберіть **Додаткові параметри > Захист мережі > Базові > Відомі мережі**. Потім поруч з елементом **Відомі мережі** клацніть **Змінити**.

Стовпці

Ім'я: ім'я відомої мережі.

Тип захисту: показує налаштування захисту мережі (**Надійна мережа**, **Ненадійна мережа** або **Використовувати параметр Windows**).

Профіль брандмауера: виберіть профіль у розкритому меню **Показувати правила, які використовуються у профілі**, щоб відобразити фільтр правил профілю.

Профіль оновлення: дає змогу застосувати створений профіль оновлення після підключення до цієї мережі.

Елементи керування

Додати: створює нову відому мережу.

Змінити: натисніть, щоб змінити наявну відому мережу.

Видалити: виберіть мережу й натисніть **Видалити**, щоб видалити її зі списку відомих мереж.



Угору/у самий верх/униз/у самий низ: дає змогу коригувати рівень пріоритетності для відомих мереж (оцінюється згори вниз).

Налаштування конфігурації мережі розташовано на вказаних нижче вкладках.

Мережа

Тут можна налаштувати параметр **Ім'я мережі** та вибрати **Тип захисту** ("Ненадійна мережа", "Надійна мережа", "Використовувати параметр Windows"). Скористайтеся розкритим меню **Профіль брандмауера**, щоб вибрати профіль для цієї мережі. Якщо використовується **Надійна мережа**, усі безпосередньо підключені до неї підмережі вважаються довіреними. Наприклад, якщо мережевий адаптер підключено до цієї мережі з IP-адресою 192.168.1.5 і маскою підмережі 255.255.255.0, підмережа 192.168.1.0/24 додається до довіреної зони цього адаптера. Якщо адаптер має кілька адрес/підмереж, усі вони вважатимуться довіреними, незалежно від параметра **Ідентифікаційні дані мережі** відомої мережі.

Крім того, адреси, додані в розділі **Додаткові довірені адреси**, завжди додаються до довіреної зони адаптерів, підключених до відповідної мережі (незалежно від її типу захисту).

Попереджати про слабкий захист мережі WiFi: ESET Endpoint Antivirus сповістить вас про підключення до незахищеної бездротової мережі або мережі зі слабким захистом.

Профіль брандмауера: виберіть профіль брандмауера, який буде використовуватись для підключення до цієї мережі.

Профіль оновлення: виберіть профіль оновлення, який буде використовуватись для підключення до цієї мережі.

Щоб мережу було позначено у списку підключених мереж, мають виконуватися наведені нижче вимоги:

- **Ідентифікаційні дані мережі:** усі вказані параметри мають збігатися з параметрами активного підключення.
- **Автентифікація мережі:** якщо вибрано сервер автентифікації, автентифікація сервером ESET має бути успішною.

Ідентифікаційні дані мережі

Ідентифікація мережі виконується на основі параметрів адаптера локальної мережі. Усі вибрані параметри порівнюються з фактичними параметрами активних мережевих підключень. Допускаються адреси IPv4 і IPv6.

The screenshot shows a dialog box titled "Змінити параметри мережі" (Change network parameters) with a help icon. It has three tabs: "Мережа" (Network), "Ідентифікаційні дані мережі" (Network identification), and "Автентифікація мережі" (Network authentication). The "Ідентифікаційні дані мережі" tab is active. It contains several settings, each with a checkbox and a text input field:

- Коли поточний суфікс DNS (наприклад, "company.com") є таким:** ☒
- Коли IP-адреса сервера WINS є такою:** ☐
- Коли IP-адреса DNS-сервера є такою:** ☒
- Коли локальна IP-адреса є такою:** ☒
- Коли IP-адреса сервера DHCP є такою:** ☒

At the bottom right, there are two buttons: "ОК" (OK) and "Скасувати" (Cancel).

Автентифікація мережі

Функція автентифікації мережі здійснює пошук певного сервера в мережі й використовує асиметричне шифрування (RSA) для його автентифікації. Ім'я мережі, що автентифікується, має збігатися з іменем зони, указаним у параметрах сервера автентифікації. Ім'я чутливе до регістру. Укажіть ім'я сервера, порт прослуховування сервера та відкритий ключ, який відповідає приватному ключу сервера (див. розділ [Автентифікація мережі – конфігурація сервера](#)). Ім'я сервера можна вести у форматі IP-адреси, DNS-адреси або імені NetBios разом зі шляхом розташування ключа на сервері (наприклад, ім'я_сервера_каталог1/каталог2/автентифікація). Можна вказати альтернативні сервери для використання, додаючи їх до шляху, розділені крапкою з комою.

[Завантажте сервер автентифікації ESET.](#)

Відкритий ключ, що імпортується, може бути файлом одного з наведених нижче типів.

- Зашифрований відкритий ключ PEM (.pem). Його можна згенерувати за допомогою сервера автентифікації ESET (див. розділ [Автентифікація мережі – конфігурація сервера](#)).
- Зашифрований відкритий ключ
- Сертифікат відкритого ключа (.crt)

Змінити параметри мережі ?

Мережа

Ідентифікаційні дані мережі

Автентифікація мережі

Ім'я або IP-адреса сервера

10.1.1.24

Порт сервера

80

Відкритий ключ (із кодуванням base64)

Додати

Тест

OK

Скасувати

Натисніть **Тест**, щоб перевірити налаштування. Якщо автентифікацію сервера виконано успішно, відобразиться сповіщення Автентифікацію сервера здійснено успішно. Якщо автентифікацію не налаштовано належним чином, відобразиться одне з наведених нижче повідомлень про помилку.

Не вдалося здійснити автентифікацію сервера. Неприпустимий або невідповідний підпис. Підпис сервера не збігається із введеним відкритим ключем.

Не вдалося здійснити автентифікацію сервера. Невідповідність імені мережі. Визначене ім'я мережі не відповідає імені зони сервера автентифікації. Перевірте ідентичність обох імен.

Не вдалося здійснити автентифікацію сервера. Неприпустима відповідь сервера або немає відповіді.

Відповідь не надійде, якщо сервер не запущено або він недоступний. Якщо за вказаною адресою запущено інший HTTP-сервер, може надійти неприпустима відповідь.

Введено недійсний відкритий ключ.

Переконайтеся, що файл відкритого ключа не пошкоджено.

Автентифікація мережі – конфігурація сервера

Автентифікація може виконуватися будь-яким комп'ютером/сервером, підключеним до мережі, автентифікацію якої потрібно виконати. Програму сервера автентифікації ESET потрібно інсталиювати на комп'ютері/сервері, завжди доступному для автентифікації (незалежно від

того, коли клієнт здійснює підключення до мережі). Файл інсталяції програми сервера автентифікації ESET можна завантажити на веб-сайті ESET.

Після інсталяції програми відобразиться діалогове вікно (отримати доступ до програми можна в меню **Пуск > Програми > ESET > Сервер автентифікації ESET**).

Щоб налаштувати сервер автентифікації, введіть ім'я мережі автентифікації, порт прослуховування сервера (за замовчуванням – 80), а також шлях до каталогу, у якому зберігатимуться відкритий і приватний ключі. Потім створіть відкритий і приватний ключі, які використовуватимуться у процесі автентифікації. Приватний ключ залишатиметься на сервері, а відкритий необхідно імпортувати на клієнтський комп'ютер у розділі автентифікації мережі під час її налаштування в брандмауері.

Тимчасовий чорний список IP-адрес

IP-адреси, визначені як джерело атаки, додаються до чорного списку, унаслідок чого підключення до них блокується протягом певного періоду часу. Щоб переглянути їх, відкрийте ESET Endpoint Antivirus і виберіть **Параметри > Мережа > Тимчасовий чорний список IP-адрес**. Тимчасово заблоковані IP-адреси блокуються на 1 годину.

Стовпці

IP-адреса – заблокована IP-адреса.

Причина блокування – тип заблокованої атаки з відповідної адреси (наприклад, атака сканування порту TCP).

Тайм-аут – час і дата, коли адресу буде виключено з чорного списку.

Елементи керування

Видалити – натисніть, щоб видалити адресу з чорного списку, перш ніж це відбудеться автоматично.

Видалити все – натисніть, щоб негайно очистити весь список.

Додати виключення – натисніть, щоб додати виключення для брандмауера в налаштуваннях фільтрування IDS.

Налаштування зон

Зона — це набір мережевих адрес, які утворюють одну логічну групу IP-адрес. Може знадобитися, якщо потрібно використовувати один і той самий набір адрес для різних правил. Для кожної адреси в цій групі призначаються однакові правила, визначені централізовано для всієї групи. Одним із прикладів такої групи є **Довірена зона**. Довірена зона – це група мережевих адрес, які не блокуються брандмауером за жодних умов. Щоб налаштувати зони, відкрийте меню **Додаткові параметри > Захист мережі > Базові > Зони**, а тоді поруч із полем **Зони** натисніть **Змінити**. Щоб додати нову зону, натисніть **Додати**, уведіть **Ім'я** й **Опис** зони, а тоді вкажіть віддалену IP-адресу в полі **Адреса віддаленого комп'ютера (IPv4, IPv6, діапазон, маска)**. Також див. [Зони брандмауера](#).

Зони брандмауера

Докладніше про зони можна прочитати в розділі [Налаштування зон](#).

Стовпці

Ім'я – ім'я групи віддалених комп'ютерів.

IP-адреси – віддалені IP-адреси, що належать до певної зони.

Елементи керування

Коли ви **додаєте** чи **змінюєте** зону, доступні наведені нижче поля.

Ім'я – ім'я групи віддалених комп'ютерів.

Опис – загальний опис групи.

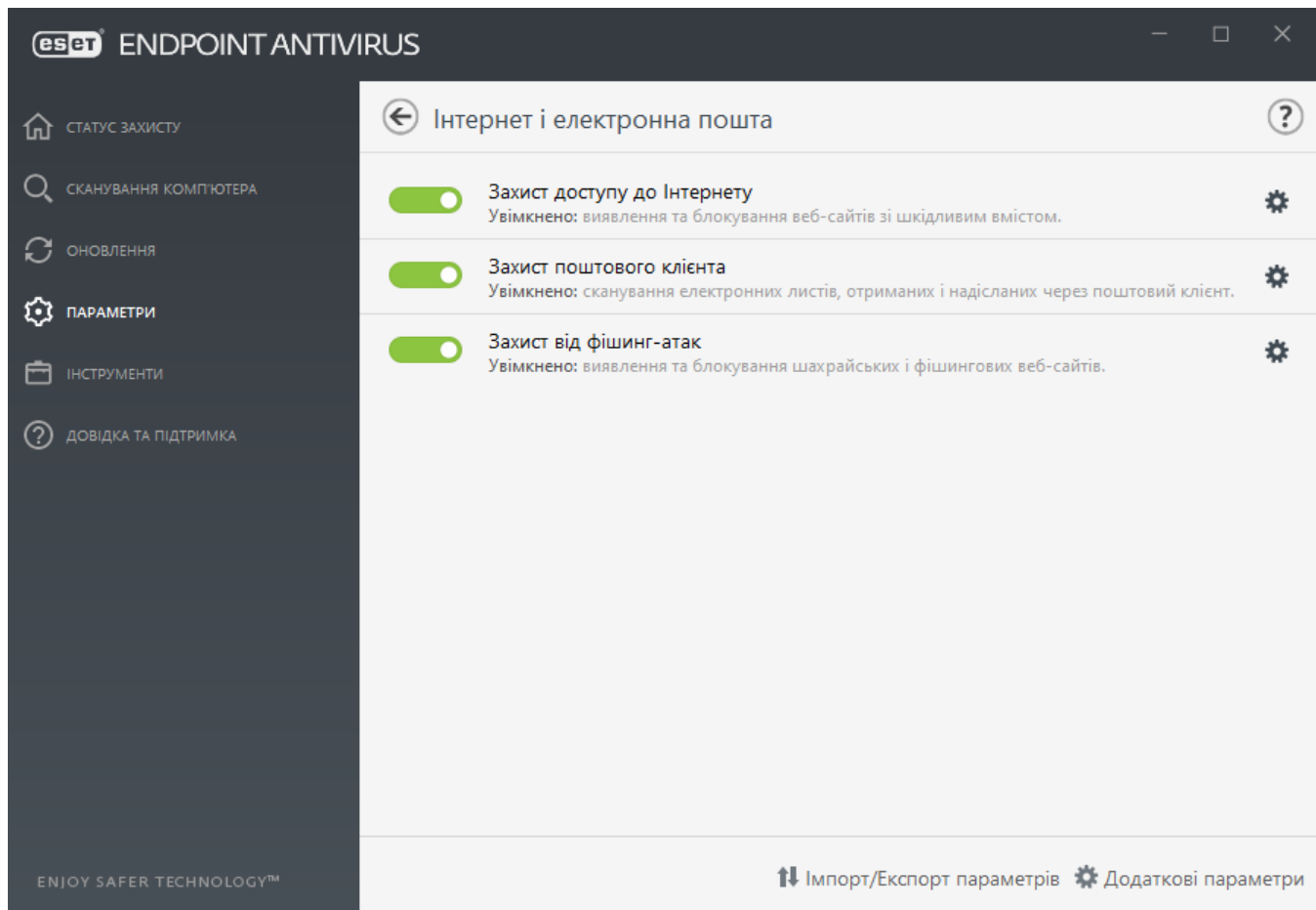
Адреса віддаленого комп'ютера (IPv4, IPv6, діапазон, маска): дає змогу додавати віддалену адресу, діапазон адрес або підмережу.

Видалити – вилучити зону зі списку.

i зверніть увагу, що попередньо визначені зони видалити не можна.

Інтернет і електронна пошта


Параметри захисту доступу до Інтернету й електронної пошти знаходяться в меню **Параметри** > **Інтернет і електронна пошта**. З цього вікна можна отримати доступ до додаткових параметрів програми.



Підключення до Інтернету – це стандартна функція персонального комп’ютера. На жаль, Інтернет став основним засобом для передачі шкідливого коду. Тому [Захист доступу до Інтернету](#) – це одна з функцій, якій слід приділяти особливу увагу.

[Захист поштового клієнта](#) забезпечує керування поштовими комунікаціями через протоколи POP3(S) та IMAP(S). За допомогою модуля plug-in для поштового клієнта ESET Endpoint Antivirus забезпечує керування поштовими комунікаціями.

[Захист від фішинг-атак](#) – інший рівень захисту, орієнтований на зловмисні веб-сайти, що намагаються отримати паролі й іншу конфіденційну інформацію. Налаштування захисту від фішинг-атак можна знайти в області Параметри розділу Інтернет і електронна пошта. Докладніше див. у розділі [Захист від фішинг-атак](#).

Можна тимчасово вимкнути захист доступу до Інтернету/електронної пошти та захист від фішинг-атак, , натиснувши елемент .

Фільтрація протоколів

Антивірусний захист для протоколів програм забезпечується ядром сканування ThreatSense, у яке повністю інтегровано всі вдосконалені методики виявлення шкідливих програм. Фільтрація протоколів здійснюється автоматично, незалежно від використовуваного веб-браузера або клієнта електронної пошти. Щоб змінити параметри зашифрованого підключення (SSL), виберіть **Додаткові параметри (F5) > Інтернет і електронна пошта > [SSL/TLS](#)**.


Увімкнути фільтрацію вмісту протоколів програм: може використовуватися для вимкнення

фільтрації протоколів. Зверніть увагу, що робота багатьох модулів програми ESET Endpoint Antivirus (захист доступу до Інтернету, захист протоколів електронної пошти, захист від фішингу, веб-контроль) неможлива без цього компонента.

Виключені програми: дає змогу виключати певні програми з фільтрації протоколів. Цей параметр доцільно використовувати в разі виникнення проблем із сумісністю, пов'язаних із фільтрацією протоколів.

Виключені IP-адреси: дає змогу виключати певні віддалені адреси з фільтрації протоколів. Цей параметр доцільно використовувати в разі виникнення проблем із сумісністю, пов'язаних із фільтрацією протоколів.

Адреса IPv4 та маска:

- *192.168.0.10* – додайте IP-адресу окремого комп'ютера, до якого має застосовуватися правило.
- *192.168.0.1–192.168.0.99* - введіть першу й останню IP-адреси, щоб визначити діапазон (для кількох комп'ютерів), до якого має застосовуватися правило.
- Підмережа (група комп'ютерів), визначена IP-адресою та маскою. Наприклад,  *255.255.255.0* – це маска мережі для префіксу *192.168.1.0/24*, що позначає діапазон адрес від *192.168.1.1* до *192.168.1.254*.

Адреса IPv6 і маска:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – додайте адресу IPv6 окремого комп'ютера, до якого має застосовуватися правило.
- *2002:c0a8:6301:1::1/64* – адреса IPv6 із префіксом довжиною 64 біти, що означає від *2002:c0a8:6301:0001:0000:0000:0000:0000* до *2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

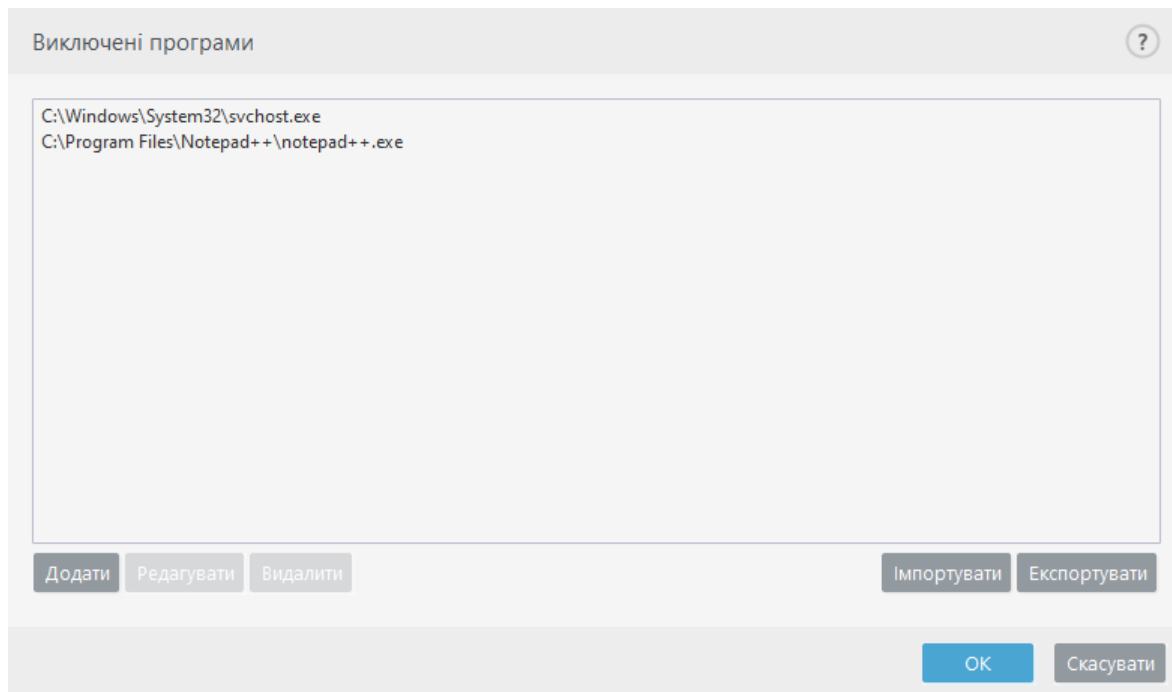
Виключені програми

Щоб виключити певні мережеві програми зі сфери охоплення фільтра протоколу, додайте їх до списку. Підключення HTTP/POP3/IMAP, які встановлюватимуться за участі вибраних програм, не перевірятимуться на наявність загроз. Рекомендується використовувати лише цей метод у випадках, коли програми не працюють належним чином за ввімкненої фільтрації протоколів.

Програми й служби, які вже потрапили до сфери охоплення фільтрації протоколів, автоматично відображатимуться після натискання кнопки **Додати**.

Змінити: редагувати вибрані записи в списку.

Видалити: видалити вибрані записи зі списку.



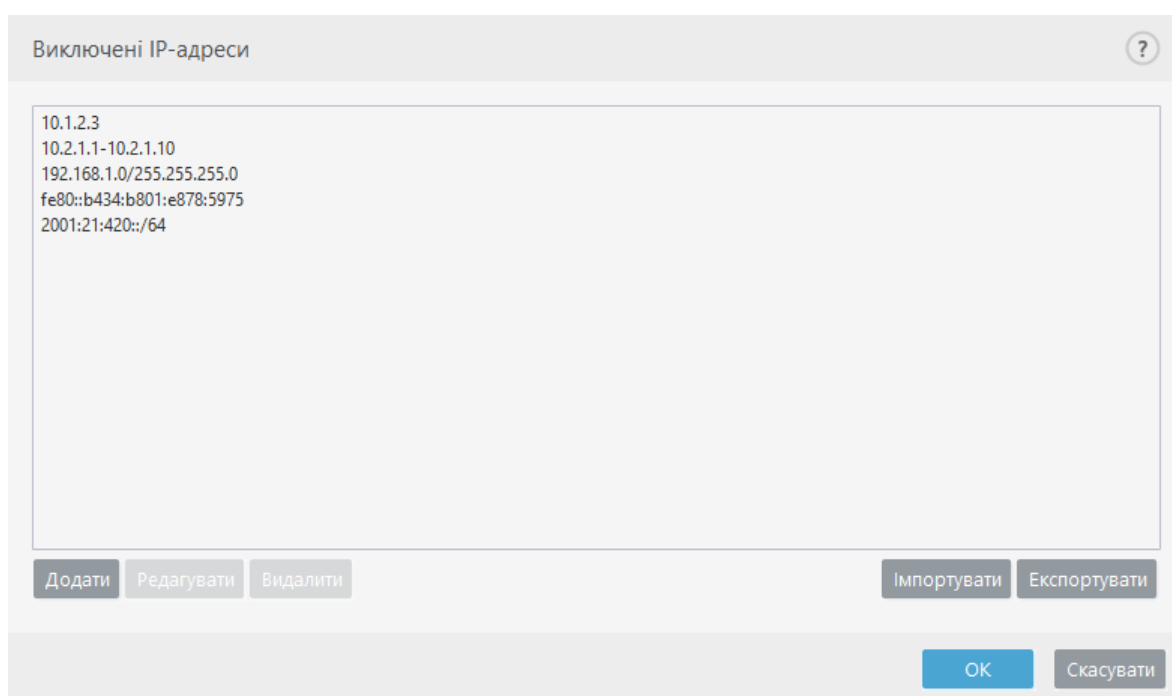
Виключені IP-адреси

IP-адреси з цього списку буде виключено з фільтрації вмісту протоколів. Підключення HTTP/POP3/IMAP, які встановлюватимуться за участю вказаних адрес, не перевірятимуться на наявність загроз. Рекомендується використовувати цей параметр лише для довірених адрес.

Додати: натисніть, щоб додати IP-адреси, діапазон адрес або підмережу віддаленої точки, до якої застосовується правило.

Змінити: редагувати вибрані записи в списку.

Видалити: видалити вибрані записи зі списку.



SSL/TLS

Програма ESET Endpoint Antivirus здатна перевіряти наявність загроз зв'язки, у яких використовується протокол SSL. Можна використовувати різні режими сканування для перевірки захищених SSL-зв'язків, коли застосовуються довірені сертифікати, невідомі сертифікати або сертифікати, виключені з перевірки захищених SSL-зв'язків.

Увімкнути фільтрацію протоколу SSL/TLS: фільтрацію протоколу увімкнено за замовчуванням. Можна вимкнути фільтрацію протоколу SSL/TLS у розділі **Додаткові параметри > Інтернет і електронна пошта > SSL/TLS** або за допомогою політики. Якщо фільтрацію протоколу вимкнено, програма не скануватиме канали обміну даними за протоколом SSL.

Для параметра **Режим фільтрації протоколу SSL/TLS** доступні наведені нижче опції.

Режим фільтрації	Опис
Автоматичний режим	Режим за замовчуванням, у якому скануються лише відповідні програми, зокрема веб-браузери та поштові клієнти. Його можна обійти, вибравши програми, чиї зв'язки потрібно сканувати.
Інтерактивний режим	Якщо ввести адресу веб-сайту із захистом SSL- (з невідомим сертифікатом), з'явиться діалогове вікно вибору дії . У цьому режимі можна створити список сертифікатів SSL або програм, які не перевірятимуться.
Режим політики	Виберіть цей параметр, щоб сканувати всі захищені SSL-зв'язки, окрім тих, які захищено виключеними з перевірки сертифікатами. Якщо встановлюється новий зв'язок із використанням невідомого підписаного сертифіката, вас не буде сповіщено про це й зв'язок буде автоматично відфільтровано. Якщо сервер має недовірений сертифікат, позначений як довірений (доданий до списку довірених), зв'язок із сервером буде дозволено, а вміст каналу зв'язку відфільтровуватиметься.

Список програм, до яких застосовуються фільтри SSL/TLS: дає змогу коригувати поведінку ESET Endpoint Antivirus відносно окремих програм.

Список відомих сертифікатів також дає змогу коригувати поведінку програми ESET Endpoint Antivirus відносно певних сертифікатів SSL.

Виключити зв'язок із довіреними доменами: якщо увімкнено цей параметр, обмін даними між довіреними доменами не буде перевірятись. Довірені домени визначаються вбудованим білим списком.

Блокувати зашифрований зв'язок, що використовує застарілий протокол SSL v2: автоматично блокує зв'язки, для встановлення яких використовується попередня версія протоколу SSL.

i Адреси не будуть фільтруватися, якщо увімкнено параметр **Виключити зв'язок із довіреними доменами** і домен вважається довіреним.

Кореневий сертифікат

Кореневий сертифікат: для належного функціонування зв'язків за протоколом SSL у

браузерах і клієнтах електронної пошти важливо, щоб до списку відомих корневих сертифікатів (видавців) було додано кореневий сертифікат для ESET. Параметр **Додати кореневий сертифікат до відомих браузерів** має бути ввімкнено. Установіть цей прапорець, щоб автоматично додати кореневий сертифікат ESET до відомих браузерів (наприклад, Opera та Firefox). Для браузерів, які використовують системне сховище сертифікатів, він додається автоматично (наприклад, Internet Explorer).

Щоб застосувати сертифікат до непідтримуваних браузерів, виберіть **Переглянути сертифікат > Відомості > Копіювати у файл...**, після чого вручну імпортуйте його до браузера.

Дійсність сертифікатів

Дія, якщо неможливо перевірити надійність сертифіката: у деяких випадках сертифікат веб-сайту не можна перевірити за допомогою сховища довірених корневих центрів сертифікації (Trusted Root Certification Authorities, TRCA) (наприклад, прострочений сертифікат, недовірений сертифікат, сертифікат, недійсний для певного домену, або підпис, який підписує сертифікат неправильно й піддається аналізу). Надійні веб-сайти завжди використовують довірені сертифікати. Якщо вони не надають довірений сертифікат, це може означати, що зломисник дешифрував ваш сеанс обміну даними або на цьому веб-сайті є певні технічні проблеми.

Якщо прапорець **Запитувати про дійсність сертифіката** встановлено (за замовчуванням), користувач отримає запит на вибір дії, яку потрібно виконати в разі встановлення зашифрованого зв'язку. З'явиться діалогове вікно вибору дії, у якому можна позначити сертифікат як довірений або виключений. Якщо сертифіката немає у списку TRCA, вікно відображається червоним. Якщо сертифікат зазначено у списку TRCA, вікно відображається зеленим.

Можна встановити прапорець **Блокувати зв'язок, який використовує сертифікат**, щоб завжди переривати зашифровані підключення до веб-сайту, який використовує недовірений сертифікат.

Дія для пошкоджених сертифікатів: пошкоджений сертифікат означає, що для нього використовується формат, який не розпізнається ESET Endpoint Antivirus, або сертифікат отримано пошкодженням (наприклад, його перезаписано випадковими даними). У такому випадку рекомендуємо не знімати прапорець **Блокувати зв'язок, який використовує сертифікат**. Якщо вибрано параметр **Запитувати про дійсність сертифіката**, користувачу буде запропоновано вибрати дію для виконання в разі утворення зашифрованого з'єднання.

Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Сповіщення про сертифікати в продуктах ESET](#)
- [«Зашифрований мережевий трафік: недовірений сертифікат» відображається під час відвідування веб-сторінок](#)

Сертифікати

Для належного функціонування зв'язків за протоколом SSL у браузерах і клієнтах електронної пошти важливо, щоб до списку відомих корневих сертифікатів (видавців) було додано кореневий сертифікат для ESET. Параметр **Додати кореневий сертифікат до відомих браузерів** має бути ввімкнено. Установіть цей прапорець, щоб автоматично додати кореневий

сертифікат ESET до відомих браузерів (наприклад, Opera і Firefox). Для браузерів, які використовують системне сховище сертифікатів, сертифікат додається автоматично (наприклад, до Internet Explorer). Щоб застосувати сертифікат до непідтримуваних браузерів, виберіть **Переглянути сертифікат > Відомості > Копіювати в файл**, після чого вручну імпортуйте його до браузера.

У деяких випадках сертифікат неможливо перевірити за допомогою сховища довірених кореневих сертифікатів (наприклад, VeriSign). Це означає, що сертифікат самостійно підписаний певною особою (наприклад, адміністратором веб-сервера або невеликої компанії), тому вважати його довіреним не завжди небезпечно. Більшість великих комерційних організацій (наприклад, банки) використовують сертифікати, підписані TRCA. Якщо прапорець **Запитувати про дійсність сертифіката** встановлено (за замовчуванням), користувач побачить запит на вибір дії, яку потрібно виконати в разі встановлення зашифрованого зв'язку. З'явиться діалогове вікно вибору дії, у якому можна позначити сертифікат як довірений або виключений. Якщо сертифіката немає у списку TRCA, вікно відображається червоним. Якщо сертифікат зазначено у списку TRCA, вікно відображається зеленим.

Можна встановити прапорець **Блокувати зв'язок, який використовує сертифікат**, щоб завжди переривати зашифровані підключення до сайту, який використовує неперевірений сертифікат.

Якщо сертифікат недійсний або пошкоджений, це означає, що термін його дії минув або його неправильно підписано. У такому випадку рекомендується блокувати зв'язок, що використовує такий сертифікат.

Зашифрований мережевий трафік

Якщо систему налаштовано на використання сканування трафіку за SSL-протоколом, у двох наведених нижче ситуаціях відображатиметься діалогове вікно з пропозицією вибрати дію.

Перша: якщо веб-сайт використовує недійсний сертифікат або такий, що не можна перевірити, і програму ESET Endpoint Antivirus налаштовано запитувати вказівки користувача (за замовчуванням "Так" — для сертифікатів, які не вдається перевірити, а "Ні" — для недійсних), відображатиметься діалогове вікно із запитом про дію, яку потрібно застосувати до відповідного підключення (**Заблокувати** чи **Дозволити**). Якщо сертифікат не знайдено в Trusted Root Certification Authorities store (TRCA), він вважається недовіреним.

Друга: якщо для параметра **Режим фільтрації протоколу SSL** встановлено значення **Інтерактивний режим**, для кожного веб-сайту відображатиметься діалогове вікно із запитом про дію, яку потрібно застосувати до трафіку (**Сканувати** чи **Ігнорувати**). Деякі програми перевіряють, чи не зазнавав змін або перевірок оброблюваний ними SSL-трафік. У такому разі ESET Endpoint Antivirus має **ігнорувати** трафік, щоб забезпечити роботу цих програм.

Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Сповіщення про сертифікати в продуктах ESET](#)
- [«Зашифрований мережевий трафік: недовірений сертифікат» відображається під час відвідування веб-сторінок](#)

В обох випадках користувач може зафіксувати вибрану ним дію. Збережені дії можна знайти в розділі [Список відомих сертифікатів](#).

Список відомих сертифікатів

Список відомих сертифікатів можна використовувати для коригування поведінки ESET Endpoint Antivirus стосовно певних сертифікатів SSL, а також для запам'ятовування вибраних дій, коли в розділі **Режим фільтрації протоколу SSL/TLS** вибрано параметр **Інтерактивний режим**. Список можна переглянути й відредагувати в меню **Додаткові параметри (F5) > Інтернет і електронна пошта > SSL/TLS > Список відомих сертифікатів**.

Вікно **Список відомих сертифікатів** складається з наведених нижче елементів.

Стовпці

Ім'я: ім'я сертифіката.

Видавець сертифіката: ім'я автора сертифіката.

Предмет сертифіката: тема, пов'язана з відкритим ключем, указаним у відповідному полі.

Доступ: виберіть значення **Дозволити** або **Заблокувати** для параметра **Доступ**, щоб дозволити чи заблокувати зв'язок, захищений відповідним сертифікатом незалежно від його надійності. Виберіть **Автоматично**, щоб програма дозволяла довірені сертифікати й запитувала про недовірені. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Перевірка: виберіть значення **Перевіряти** або **Ігнорувати** для параметра **Перевірка**, щоб перевіряти або ігнорувати зв'язок, захищений відповідним сертифікатом. Виберіть **Автоматично**, щоб в автоматичному режимі система виконувала перевірку, а в інтерактивному – зверталася за вказівками до користувача. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Елементи керування

Додати: сертифікат можна завантажити вручну; це має бути файл із розширенням *.cer*, *.crt* або *.pem*. Натисніть **Файл**, щоб завантажити локальний сертифікат, або **URL**, щоб указати сертифікат на сайті.

Змінити: виберіть сертифікат, який потрібно налаштувати, і натисніть **Змінити**.

Видалити : виберіть потрібний сертифікат і натисніть **Видалити**.

ОК/Скасувати: натисніть **ОК**, щоб зберегти зміни, або **Скасувати**, щоб залишити сторінку без збереження змін.

Список програм, до яких застосовуються фільтри SSL/TLS

Параметр **Список програм, до яких застосовуються фільтри SSL/TLS** можна використовувати, щоб налаштувати роботу ESET Endpoint Antivirus у певних програмах, а також зберегти вибрані дії, якщо в розділі **Режим фільтрації протоколу SSL/TLS** активовано **Інтерактивний режим**. Щоб переглянути й відредагувати список, відкрийте меню **Додаткові параметри (F5) > Інтернет і електронна пошта > SSL/TLS > Список програм, до яких**

застосовуються фільтри SSL/TLS.

Вікно **Список програм, до яких застосовуються фільтри SSL/TLS** складається з наведених нижче елементів.

Стовпці

Програма: виберіть виконуваний файл у дереві каталогів, натисніть кнопку ... або введіть шлях вручну.

Перевірка: виберіть **Перевіряти** чи **Ігнорувати**. Виберіть **Автоматично**, щоб в автоматичному режимі система виконувала перевірку, а в інтерактивному – зверталася за вказівками до користувача. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Елементи керування

Додати: додати відфільтровані програми.

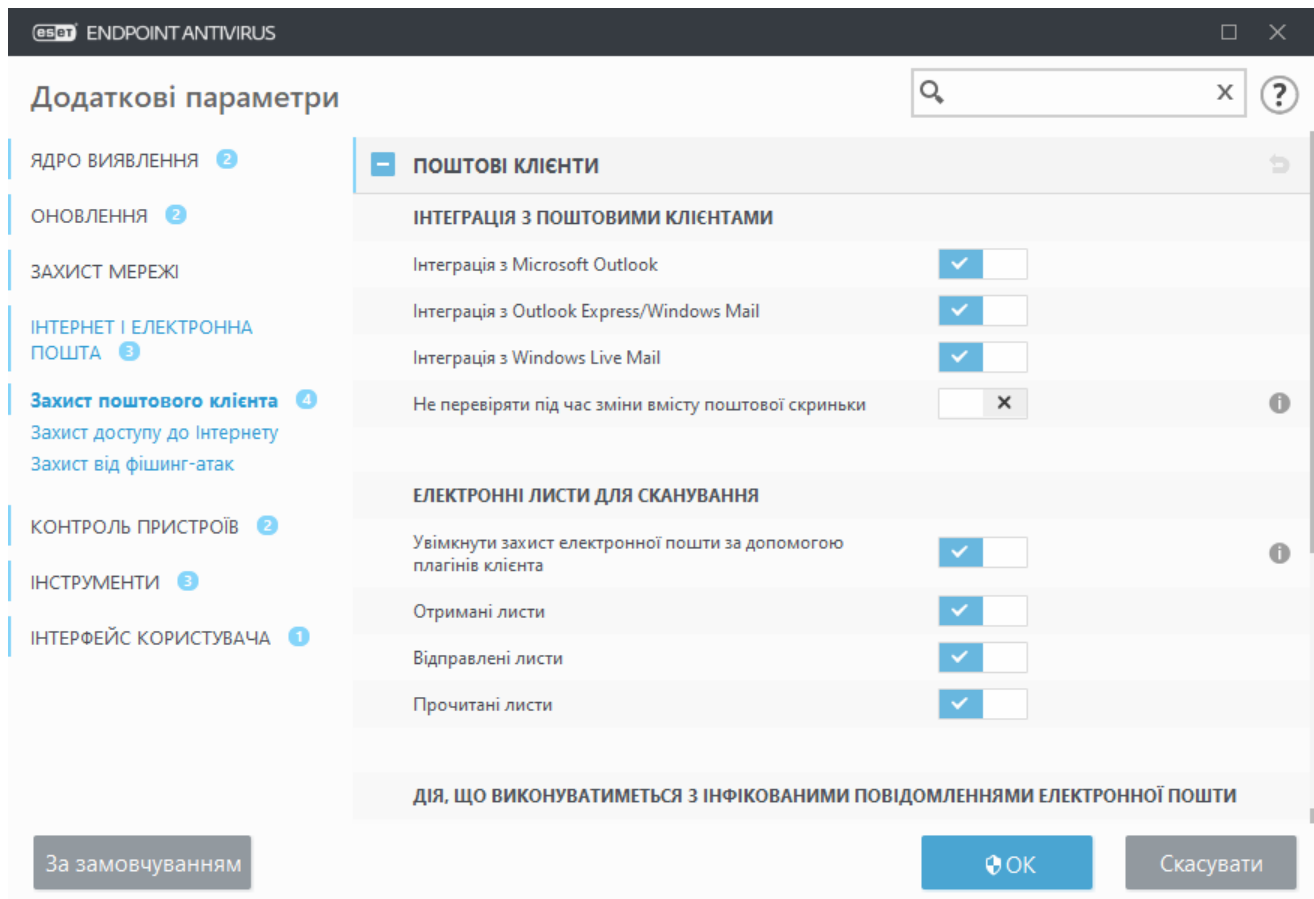
Змінити: виберіть сертифікат, який потрібно налаштувати, і натисніть **Змінити**.

Видалити : виберіть потрібний сертифікат і натисніть **Видалити**.

ОК/Скасувати: натисніть **ОК**, щоб зберегти зміни, або виберіть **Скасувати**, щоб залишити налаштування без змін.

Захист поштового клієнта

Інтеграція ESET Endpoint Antivirus з поштовими клієнтами підвищує рівень активного захисту від шкідливих кодів у повідомленнях електронної пошти. Якщо ваш поштовий клієнт підтримується, інтеграцію можна активувати за допомогою елементів керування ESET Endpoint Antivirus. Якщо інтеграцію ввімкнено, панель інструментів ESET Endpoint Antivirus вставляється безпосередньо в поштовий клієнт, що підвищує ефективність захисту електронної пошти. Параметри інтеграції доступні в меню **Додаткові параметри (F5) > Інтернет і електронна пошта > Захист поштового клієнта > Поштові клієнти**.



Електронні листи для сканування

Увімкнути захист електронної пошти за допомогою плагінів клієнта: якщо цей параметр вимкнено, захист за допомогою плагінів клієнта не працює.

Отримані листи: якщо цей параметр увімкнено, перевіряються отримані повідомлення електронної пошти.

Відправлені листи: якщо цей параметр увімкнено, перевіряються надіслані повідомлення електронної пошти.

Прочитані листи: якщо цей параметр увімкнено, перевіряються прочитані повідомлення електронної пошти.

Рекомендуємо не вимикати параметр **Увімкнути захист електронної пошти за допомогою плагінів клієнта. Навіть якщо інтеграцію вимкнено або вона не працює, поштовий зв'язок усе одно захищено функцією [фільтрації протоколу](#) (IMAP/IMAPS і POP3/POP3S).**

Дія, що виконуватимуться інфікованими повідомленнями електронної пошти

Пропустити – програма виявлятиме інфіковані вкладення, але не застосовуватиме жодних дій до повідомлень електронної пошти.

Видалити лист: програма повідомлятиме користувачу про виявлені загрози й видалятиме повідомлення.

Перемістити лист до папки «Видалені»: інфіковані повідомлення буде автоматично переміщено до папки "Видалені".

Перемістити лист до папки (дія за замовчуванням): інфіковані повідомлення будуть автоматично переміщені до вказаної папки.

Папка: укажіть спеціальну папку, куди потрібно переміщувати інфіковані повідомлення електронної пошти.

Повторити перевірку після оновлення: якщо цей параметр увімкнено, інфіковані повідомлення електронної пошти повторно скануватимуться після оновлення ядра виявлення.

Прийняти результати сканування іншими модулями: дозволяє модулю захисту електронної пошти використовувати результати сканування, отримані від інших модулів захисту, замість повторного сканування.

Протоколи електронної пошти

IMAP і POP3 – це найпоширеніші протоколи, які використовуються для поштового зв'язку в програмах поштових клієнтів. IMAP (Internet Message Access Protocol – протокол доступу до електронної пошти) – інший інтернет-протокол для отримання доступу до електронної пошти. Протокол IMAP має певні переваги над POP3: кілька клієнтів можуть одночасно підключатися до однієї поштової скриньки, не змінюючи стан повідомлення (прочитане/непрочитане, з відповіддю/видалене). Модуль захисту, який забезпечує контроль цього типу, ініціюється автоматично під час запуску операційної системи й залишається активним у пам'яті.

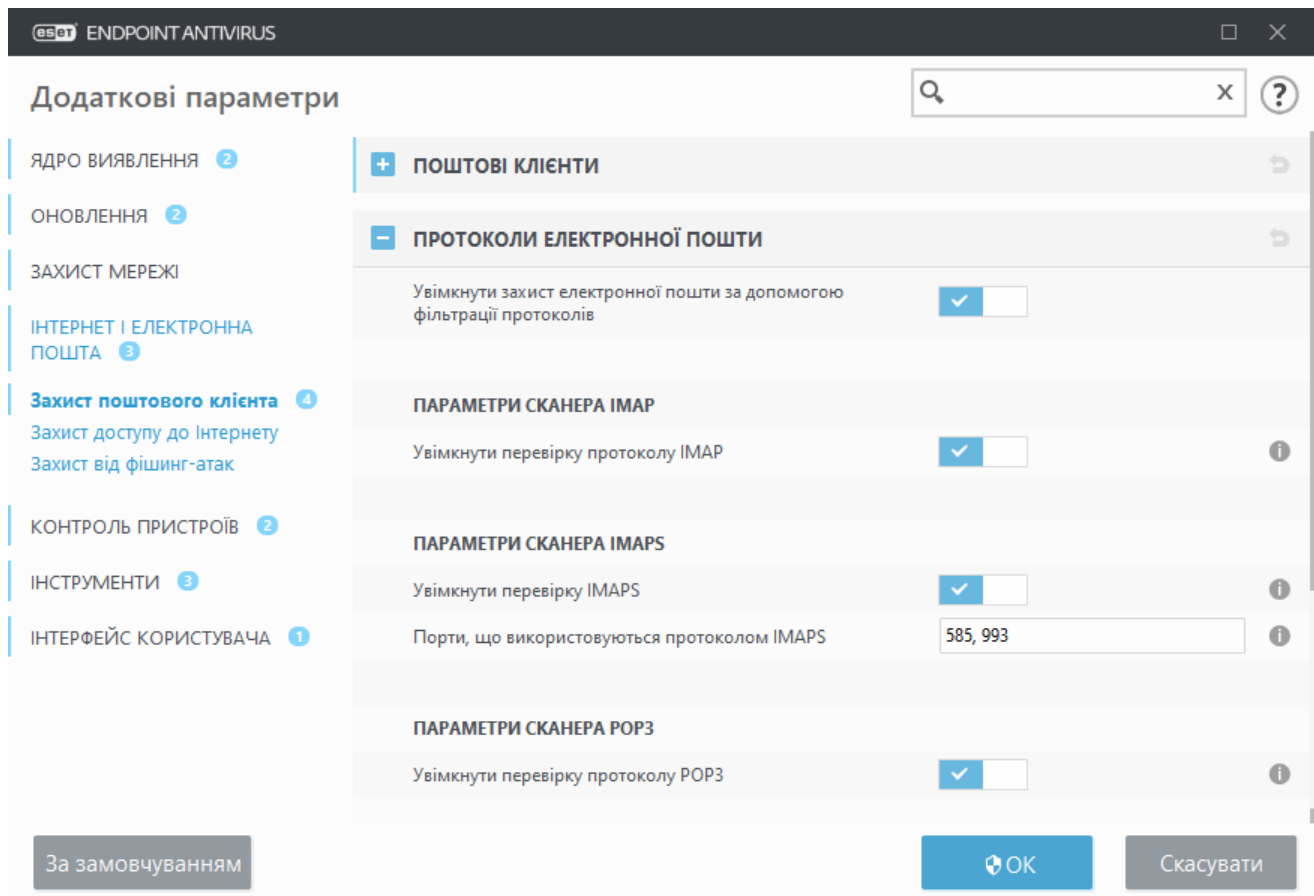
ESET Endpoint Antivirus забезпечує захист користувачів цього протоколу незалежно від їхнього поштового клієнта й без необхідності його повторного налаштування. За замовчуванням перевіряються всі операції обміну даними через протоколи POP3 й IMAP, незалежно від стандартних номерів портів POP3/IMAP.

Протокол IMAP не перевіряється. Проте обмін даними із сервером Microsoft Exchange може перевіряти [модуль інтеграції](#) з поштовими клієнтами, такими як Microsoft Outlook.

Рекомендуємо не вимикати параметр **Увімкнути захист електронної пошти за допомогою фільтрації протоколів**. Щоб налаштувати перевірку протоколів IMAP/IMAPS і POP3/POP3S, перейдіть у меню Додаткові параметри > **Інтернет і електронна пошта** > **Захист поштового клієнта** > **Протоколи електронної пошти**.

ESET Endpoint Antivirus також підтримує сканування протоколів IMAPS (585, 993) і POP3S (995), які використовують зашифрований канал для передачі інформації між сервером і клієнтом. ESET Endpoint Antivirus перевіряє комунікаційні зв'язки, що використовують протоколи SSL (Secure Socket Layer – рівень захищених сокетів) і TLS (Transport Layer Security – захист на транспортному рівні). Програма скануватиме лише трафік, який передається через **Порти, що використовуються протоколом IMAPS/POP3S**, незалежно від версії операційної системи. В разі необхідності можна додати інші комунікаційні порти. Якщо портів кілька, розділяйте їх номери комою.

Зашифровані зв'язки скануються за замовчуванням. Щоб переглянути налаштування сканера, перейдіть до розділу [SSL/TLS](#) у дереві "Додаткові параметри", клацніть **Інтернет і електронна пошта** > **SSL/TLS** та виберіть параметр **Увімкнути фільтрацію протоколу SSL/TLS**



Теги електронної пошти

Параметри цієї функції доступні в меню **Додаткові параметри в розділі Інтернет і електронна пошта > Захист поштового клієнта > Сигнали та сповіщення**.

Після завершення перевірки електронної пошти сповіщення з результатом сканування може бути додано до повідомлення. Можна вибрати параметр **Додавати повідомлення-ознаки до отриманої чи прочитаної пошти** або **Додавати повідомлення-ознаки до надісланої пошти**. Пам'ятайте, що іноді повідомлення-ознаки можуть опускатися в проблемних HTML-повідомленнях або підроблятися шкідливим ПЗ. Повідомлення-ознаки можуть додаватися до прочитаних вхідних повідомлень електронної пошти та до надісланих листів. Можна вибрати один із наведених нижче варіантів.

- **Ніколи:** повідомлення-ознаки взагалі не додаватимуться.
- **Коли виявлено певний об'єкт** – як перевірені позначатимуться лише повідомлення, що містять шкідливе програмне забезпечення (за замовчуванням).
- **До всіх перевірених електронних листів** – програма додаватиме повідомлення до всієї перевіреної електронної пошти.

Оновити тему надісланого повідомлення електронної пошти: зніміть цей прапорець, щоб модуль захисту електронної пошти не додавав попередження про віруси до теми інфікованого повідомлення. Ця функція дає можливість налаштувати звичайну фільтрацію інфікованої електронної пошти за темою повідомлення (якщо підтримується поштовою програмою). Ця функція також підвищує рівень довіри одержувача до повідомлень, а якщо виявлено загрозу — надає корисні дані про рівень небезпеки повідомлення чи відправника.

Текст, що додається до тем виявлених електронних листів – відредагуйте цей шаблон, якщо потрібно змінити формат префіксу теми інфікованої електронної пошти. Ця функція змінюватиме тему повідомлення "Вітаємо!" на такий формат: "виявлений об'єкт [%DETECTIONNAME%] Вітаємо!". Змінна %DETECTIONNAME% вказує на виявлений об'єкт.

Інтеграція з поштовими клієнтами

Наразі підтримуються такі поштові клієнти: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) і Windows Live Mail. Захист електронної пошти працює як компонент plug-in для цих програм. Головна перевага компонента plug-in – незалежність від використовуваного протоколу. Коли клієнт електронної пошти отримує зашифроване повідомлення, воно розшифровується й передається на обробку до антивірусного сканера. Щоб отримати повний список підтримуваних поштових клієнтів і їхніх версій, див. відповідну [статтю бази знань ESET](#).

Спеціальні параметри

Оптимізація обробки вкладень: якщо оптимізацію вимкнено, усі вкладення скануватимуться негайно. Якщо цей параметр вимкнено, це може сповільнити роботу поштового клієнта.

Розширена обробка поштового клієнта: якщо під час роботи з поштовим клієнтом система вповільнюється, вимкніть цей параметр.

Панель інструментів Microsoft Outlook

Захист клієнта Microsoft Outlook забезпечується за допомогою модуля plug-in. Після інсталяції ESET Endpoint Antivirus панель інструментів, яка містить параметри захисту від вірусів/ додається до Microsoft Outlook:

ESET Endpoint Antivirus – натисканням піктограми відкривається головне вікно програми ESET Endpoint Antivirus.

Повторне сканування повідомлень: дає змогу вручну запустити перевірку електронної пошти. Можна вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Докладніше див. у розділі [Захист поштового клієнта](#).

Налаштування сканера: відображає параметри [захисту поштового клієнта](#).

Панель інструментів Outlook Express і Windows Mail

Модуль захисту для Outlook Express і Windows Mail працює як компонент plug-in. Після інсталяції ESET Endpoint Antivirus панель інструментів, яка містить параметри захисту від вірусів/ додається до Outlook Express або Windows Mail:

ESET Endpoint Antivirus – натисканням піктограми відкривається головне вікно програми ESET Endpoint Antivirus.

Повторне сканування повідомлень: дає змогу вручну запустити перевірку електронної

пошти. Можна вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Докладніше див. у розділі [Захист поштового клієнта](#).

Налаштування сканера: відображає параметри [захисту поштового клієнта](#).

Інтерфейс користувача

Настройка вигляду: вигляд панелі інструментів для поштового клієнта можна змінити. Зніміть цей прапорець, щоб налаштувати вигляд незалежно від параметрів поштової програми.

Показувати текст: відображення опису піктограм.

Текст праворуч: переміщення опису параметрів з області під піктограмою в область праворуч від неї.

Великі піктограми: відображення великих піктограм для пунктів меню.

Діалогове вікно підтвердження

Це сповіщення використовується для того, щоб переконатися, що користувач дійсно бажає виконати вибрану дію, і уникнути можливих помилок.

З іншого боку, це вікно також пропонує можливість скасувати підтвердження.

Повторне сканування повідомлень

Панель інструментів ESET Endpoint Antivirus, інтегрована в поштовий клієнт, дає змогу користувачам вибрати кілька опцій сканування електронної пошти. Опція **Повторне сканування повідомлень** пропонує два режими сканування:

Усі повідомлення в поточній папці: сканування всіх повідомлень у поточній папці.

Тільки вибрані повідомлення: сканування лише тих повідомлень, які позначив користувач.

Установивши прапорець **Повторне сканування вже просканованих повідомлень**, користувач може повторно просканувати повідомлення, які вже сканувалися раніше.

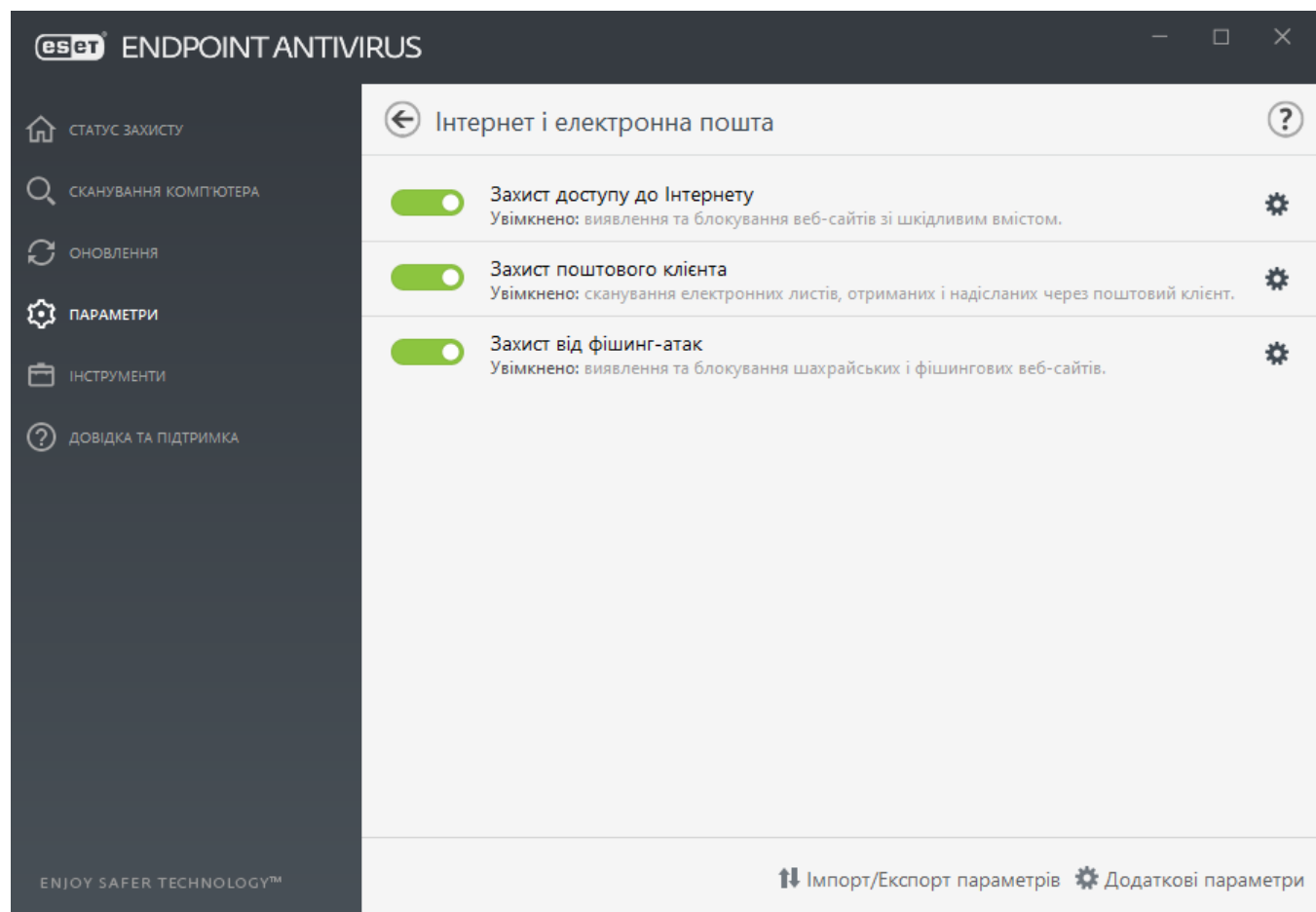
Захист доступу до Інтернету

Підключення до Інтернету – це стандартна функція персонального комп'ютера. На жаль, саме вона стала основним засобом для передачі шкідливого коду. Захист доступу до Інтернету здійснюється за допомогою контролю зв'язків між веб-браузерами й віддаленими серверами відповідно до правил протоколів HTTP (протокол передавання гіпертексту) і HTTPS (зашифрований HTTP).

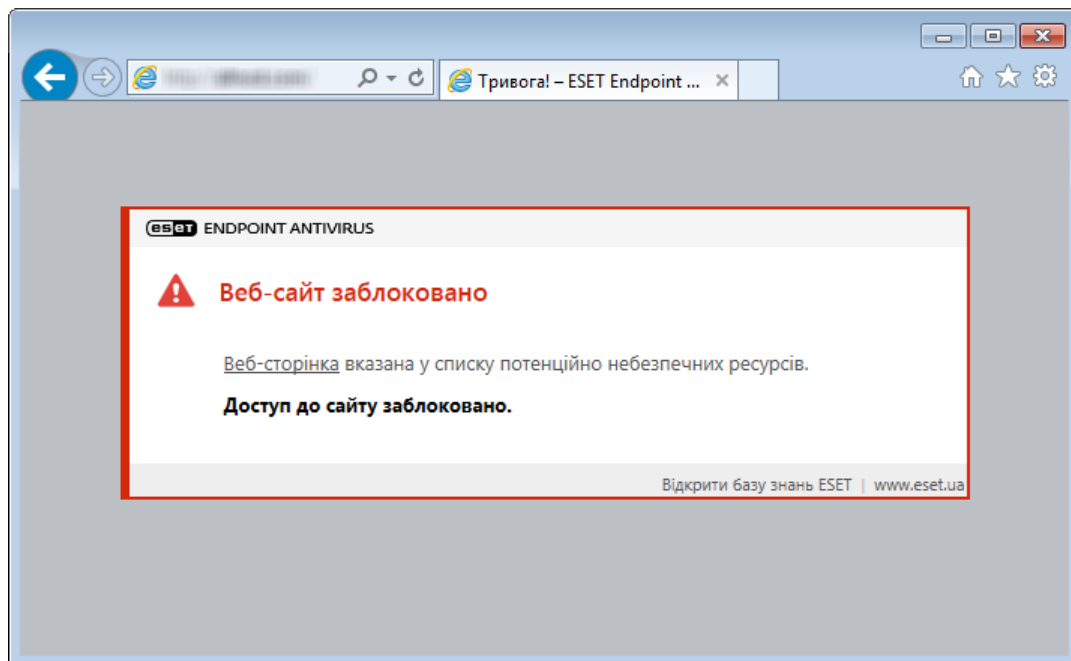
Доступ до відомих веб-сторінок зі шкідливим вмістом блокується до початку його завантаження. Усі інші веб-сторінки перевіряються підсистемою сканування ThreatSense під час

завантаження та блокуються в разі виявлення зловмисного вмісту. Захист доступу до Інтернету має два рівні: блокування за чорним списком і блокування за вмістом.

Наполегливо рекомендується активувати функцію захисту доступу до Інтернету. Щоб отримати доступ до цієї опції, у головному вікні програми ESET Endpoint Antivirus перейдіть на вкладку **Параметри > Захист від загроз з Інтернету > Захист доступу до Інтернету**.



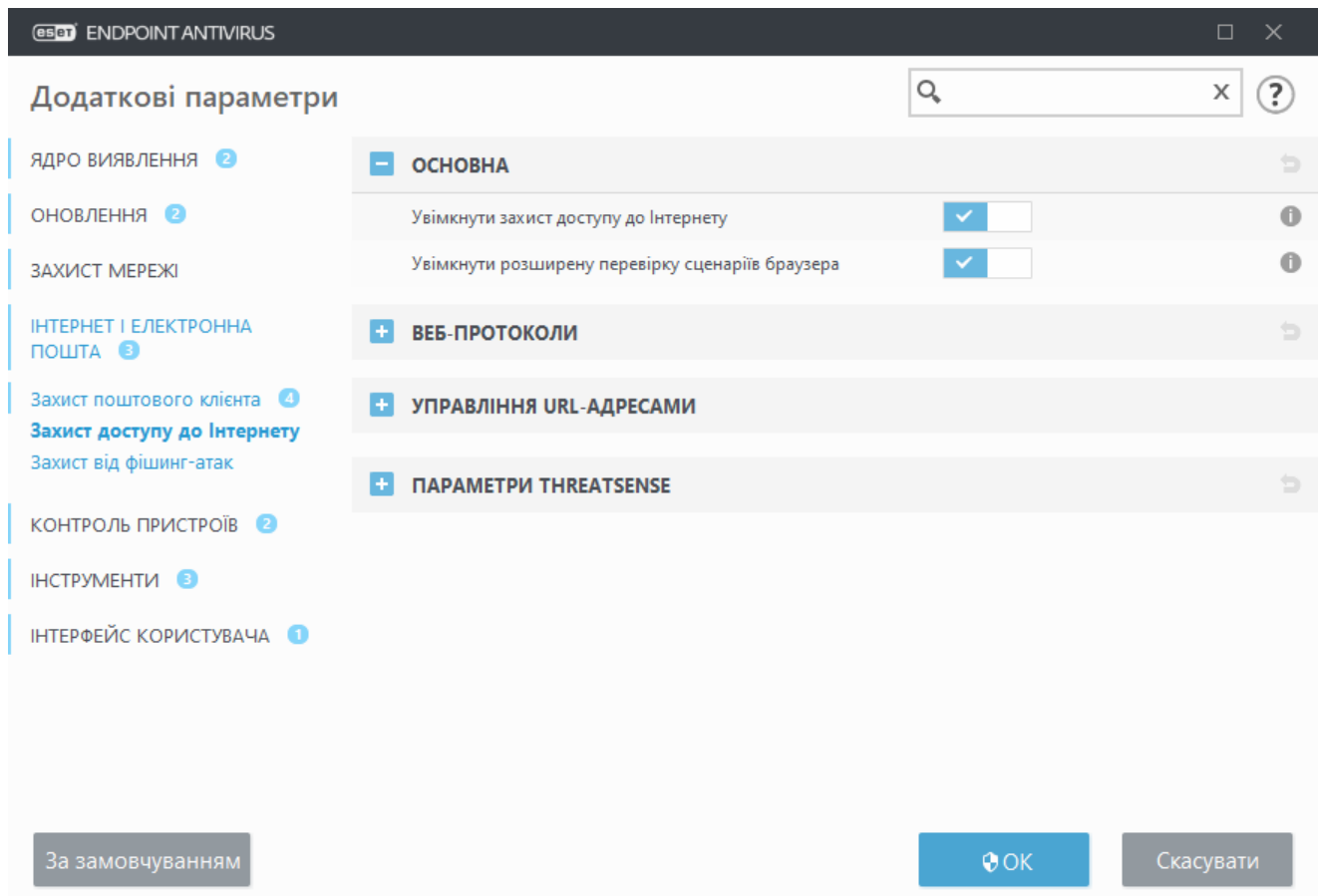
Якщо функція "захист доступу до інтернету" заблокує веб-сайт, у веб-браузері відобразиться таке повідомлення:



- i** Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:
- [Розблокування безпечного веб-сайту на окремій робочій станції в ESET Endpoint Antivirus](#)

У меню **Додаткові параметри** (F5) > **Інтернет і електронна пошта** > **Захист доступу до Інтернету** доступні такі параметри:

- **Базові**: дозволяє ввімкнути або вимкнути цю функцію в розділі "Додаткові параметри".
- **Веб-протоколи**: дає змогу налаштувати моніторинг для стандартних протоколів, що використовуються більшістю веб-браузерів.
- **Керування URL-адресою**: дає змогу вказати списки URL-адрес, які потрібно заблокувати, дозволити або виключити з перевірки.
- **Параметри підсистеми ThreatSense** – додаткові параметри антивірусного сканера, за допомогою яких можна, зокрема, вказати типи об'єктів для перевірки (електронна пошта, архіви тощо), методи виявлення загроз для захисту доступу до Інтернету тощо.



Розширене налаштування функції захисту доступу до Інтернету

У меню **Додаткові параметри** (F5) > **Інтернет і електронна пошта** > **Захист доступу до Інтернету** > **Базові** доступні такі параметри:

Увімкнути захист доступу до Інтернету: коли цей параметр вимкнено, [захист від фішинг-атак](#) і [захист доступу до Інтернету](#) не забезпечуються.

Увімкнути розширену перевірку сценаріїв браузера: коли цей параметр увімкнено, ядро виявлення перевіряє всі програми JavaScript, що виконуються у веб-браузерах.

i Наполегливо рекомендуємо не вимикати функцію захисту доступу до Інтернету.

Веб-протоколи

За замовчуванням ESET Endpoint Antivirus налаштовано на відстеження протоколу HTTP, що використовується більшістю веб-браузерів.

Параметри сканера HTTP

Трафік за протоколом HTTP завжди відстежується на всіх портах для всіх програм.

Параметри сканера HTTPS

ESET Endpoint Antivirus також підтримує перевірку протоколу HTTPS. У разі застосування зв'язку HTTPS для передавання інформації між сервером і клієнтом використовується зашифрований канал. ESET Endpoint Antivirus перевіряє зв'язки, для яких використовується шифрування за протоколами SSL (Secure Socket Layer – рівень захищених сокетів) і TLS (Transport Layer Security – захист на транспортному рівні). Програма скануватиме лише трафік, порти (443, 0-65535), який передається через **Порти, що використовуються протоколом HTTPS**, незалежно від версії операційної системи.

Зашифровані зв'язки скануються за замовчуванням. Щоб переглянути налаштування сканера, перейдіть до розділу [SSL/TLS](#) у дереві "Додаткові параметри", клацніть **Інтернет і електронна пошта > SSL/TLS** та виберіть параметр **Увімкнути фільтрацію протоколу SSL/TLS**

Управління URL-адресами

У розділі керування URL-адресами можна вказати списки HTTP-адрес, які буде заблоковано, дозволено чи виключено з перевірки вмісту.

Виберіть параметр [Увімкнути фільтрацію протоколу SSL/TLS](#), якщо крім веб-сторінок із протоколом HTTP потрібно також фільтрувати адреси HTTPS. Інакше додаватимуться лише домени відвіданих вами сайтів HTTPS, а не повні URL-адреси.

Веб-сайти зі **списку заблокованих адрес** будуть недоступні, якщо їх не перемістити до **списку дозволених адрес**. Веб-сайти зі **списку адрес, виключених зі сканування вмісту**, не скануються на наявність шкідливого програмного коду.

Щоб заблокувати всі HTTP-адреси, окрім включених в активний **список дозволених адрес**, додайте символ * в активний **список заблокованих адрес**.

У списках можна використовувати такі спеціальні символи, як-от * (зірочка) і ? (знак запитання). Зірочка означає будь-яку послідовність символів, а знак запитання – будь-який окремий символ. Необхідно дуже обережно визначати виключені адреси, тому що список має містити лише довірені та безпечні адреси. Окрім того, необхідно переконатися, що символи * та ? використовуються в списку правильно. Перегляньте розділ [Додати HTTP-адресу/маску домену](#), щоб дізнатися, як безпечно визначити весь домен разом із субдоменами. Щоб активувати список, виберіть опцію **Активний список**. Щоб отримувати попередження про введення адреси з поточного списку, виберіть **Сповіщати про застосування**.

i Адреси не будуть фільтруватися, якщо увімкнено параметр **Інтернет і електронна пошта > SSL/TLS > Виключити зв'язок із довіреними доменами** й домен уважається довіреним.

Список адрес?

Назва списку

Типи адрес

Опис списку

Список дозволених адрес	Дозволено	
Список заблокованих адрес	Заблоковано	
Список адрес, виключених зі сканування вмісту	Знайдене шкідливе пр...	

Додати Редагувати Видалити

Імпортувати Експортувати

Додайте до списку заблокованих адрес символ узагальнення (*), щоб заблокувати всі URL, окрім включених у список дозволених.

ОК

Скасувати

Елементи керування

Додати – створити список додатково до попередньо налаштованих. Це може знадобитися, коли потрібно розділити різні групи адрес за певною логікою. Наприклад, один список заблокованих адрес може містити веб-сторінки із зовнішнього загальнодоступного чорного списку, а другий – включати вашу особисту добірку небажаних сайтів. Це полегшить оновлення зовнішнього списку, натомість особистий список залишатиметься без змін.

Змінити – редагувати наявні списки. Використовуйте цю опцію, щоб додавати чи видаляти адреси.

Видалити: дає змогу видаляти наявні списки. Видаляти можна лише списки, створені за допомогою опції **Додати**, на відміну від списків за замовчуванням.

Список URL-адрес

У цьому розділі можна вказати списки адрес HTTP, які буде заблоковано, дозволено або виключено з перевірки.

За замовчуванням доступні такі три типи списків:

- **Список адрес, виключених зі сканування вмісту:** для будь-якої адреси, доданої до цього списку, перевірка на наявність шкідливого програмного коду не виконуватиметься.
- **Список дозволених адрес:** якщо встановлено прапорець "Дозволити доступ лише до URL-адрес, які містяться у списку дозволених", а список заблокованих адрес містить символ * (відповідає будь-якому символу), користувач зможе переходити лише за адресами, зазначеними в цьому списку. Перехід за адресами зі списку буде дозволено, навіть якщо їх включено до списку заблокованих.
- **Список заблокованих адрес:** користувачеві заборонено переходити за адресами з цього списку, доки їх також не буде додано до списку дозволених адрес.

Щоб створити новий список, клацніть **Додати**. Щоб видалити вибрані списки, клацніть

Видалити.

Список адрес ?

Назва списку	Типи адрес	Опис списку
Список дозволивих адрес	Дозволено	
Список заблокованих адрес	Заблоковано	
Список адрес, виключених зі сканування вмісту	Знайдене шкідливе пр...	

Додайте до списку заблокованих адрес символ узагальнення (*), щоб заблокувати всі URL, окрім включених у список дозволивих.

- i** Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:
- [Розблокування безпечного веб-сайту на окремій робочій станції в ESET Endpoint Antivirus](#)

Докладніші відомості наведено в розділі [Керування URL-адресами](#).

Створення списку

У цьому діалоговому вікні можна налаштувати новий [список URL-адрес/масок](#), які будуть заблоковані, дозволені або виключені з перевірки.

Можна налаштувати такі параметри:

Тип списку адрес – доступні три типи списків:

- **Знайдене шкідливе програмне забезпечення ігнорується:** для жодної адреси з цього списку перевірка шкідливого програмного коду виконуватися не буде.
- **Заблоковано:** доступ до адрес, указаних у цьому списку, буде заблоковано.
- **Дозволено:** доступ до адрес, указаних у цьому списку, буде дозволено. Перехід за адресами із цього списку буде дозволено, навіть якщо вони входять до списку заблокованих.

Назва списку: укажіть назву списку. Під час редагування одного з попередньо визначених списків це поле буде недоступним.

Опис списку – введіть короткий опис списку (необов'язково). Недоступно під час редагування одного з попередньо визначених списків.

Щоб активувати список, виберіть поруч із ним параметр **Список активний**. Щоб отримувати сповіщення про використання певного списку під час доступу до веб-сайтів, виберіть **Сповіщати під час застосування**. Наприклад, ви отримуватимете сповіщення, коли доступ до

веб-сайту блокуватиметься або дозволятиметься відповідно до налаштувань списку заблокованих або дозволених адрес. У сповіщенні буде вказано назву списку.

Рівень критичності: виберіть рівень критичності в розкривному меню. ESET PROTECT може збирати записи журналів й інформацію про попередження.



Детальність журналу попереджень та інформації доступна лише для правил, які містять принаймні два компоненти без групових символів у домені. Приклад:

- *.domain.com/*
- *www.domain.com/*

Елементи керування

Додати: додати нову URL-адресу до списку (можна вказати кілька значень, використовуючи роздільник).

Редагувати: дає змогу редагувати адреси в списку. Доступно лише для адрес, створених за допомогою параметра **Додати**.

Видалити – дає змогу видалити наявні адреси зі списку. Доступно лише для адрес, створених за допомогою параметра **Додати**.

Імпортувати: імпортувати файл із URL-адресами (ім'я кожного файлу починається з нового рядка, наприклад, *.txt з використанням кодування UTF-8).



Більш докладну інформацію див. в розділі [Додавання маски URL-адреси](#).

Додавання маски URL-адреси

Перед введенням потрібної адреси/маски домену виконайте інструкції, наведені в цьому діалоговому вікні.

Програма ESET Endpoint Antivirus дає змогу користувачеві заблокувати доступ до визначених веб-сайтів, перешкоджаючи веб-браузеру відображати їх вміст. Окрім того, можна вказати адреси, які мають бути виключені з перевірки. Якщо повне ім'я віддаленого сервера невідоме або користувач бажає вказати цілу групу віддалених серверів, для визначення такої групи можна використовувати так звані маски. Маски містять символи "?" та "*":

- "?" представляє окремий символ;
- "*" представляє текстовий рядок.

Наприклад, маска *.c?m застосовується до всіх адрес, остання частина яких починається літерою "c", закінчується літерою "m" і містить будь-який символ між ними (.com, .cam тощо).

Наприклад, маска *x? позначає будь-яку адресу, яка закінчується одним символом "x". Для повної відповідності домену використовуйте формат *.domain.com/*. У масці обов'язково вказувати префікс протоколу *http://*, *https://*. Якщо його опустити, маска відповідатиме будь-якому протоколу. До послідовності "*" застосовуються особливі правила, якщо вона стоїть на початку імені домену. По-перше, у цьому випадку символ узагальнення "*" не відповідає символу скісної риски (/). Це запобігає можливості обійти маску. Наприклад, маска *.domain.com

не відповідатиме `http://anydomain.com/anypath#.domain.com` (такий суфікс можна додати до будь-якої URL-адреси, і це не вплине на завантаження). По-друге, у цьому особливому випадку послідовність "*" також відповідатиме пустому рядку. Саме тому за допомогою однієї маски можна охопити весь домен разом із субдоменами. Наприклад, маска `*.domain.com` також відповідатиме `http://domain.com`. Використання `*domain.com` буде помилковим, оскільки така маска також відповідатиме `http://anotherdomain.com`.



Детальність журналу попереджень та інформації доступна лише для правил, які містять принаймні два компоненти без групових символів у домені. Приклад:

- `*.domain.com/*`
- `*www.domain.com/*`

Захист від фішинг-атак

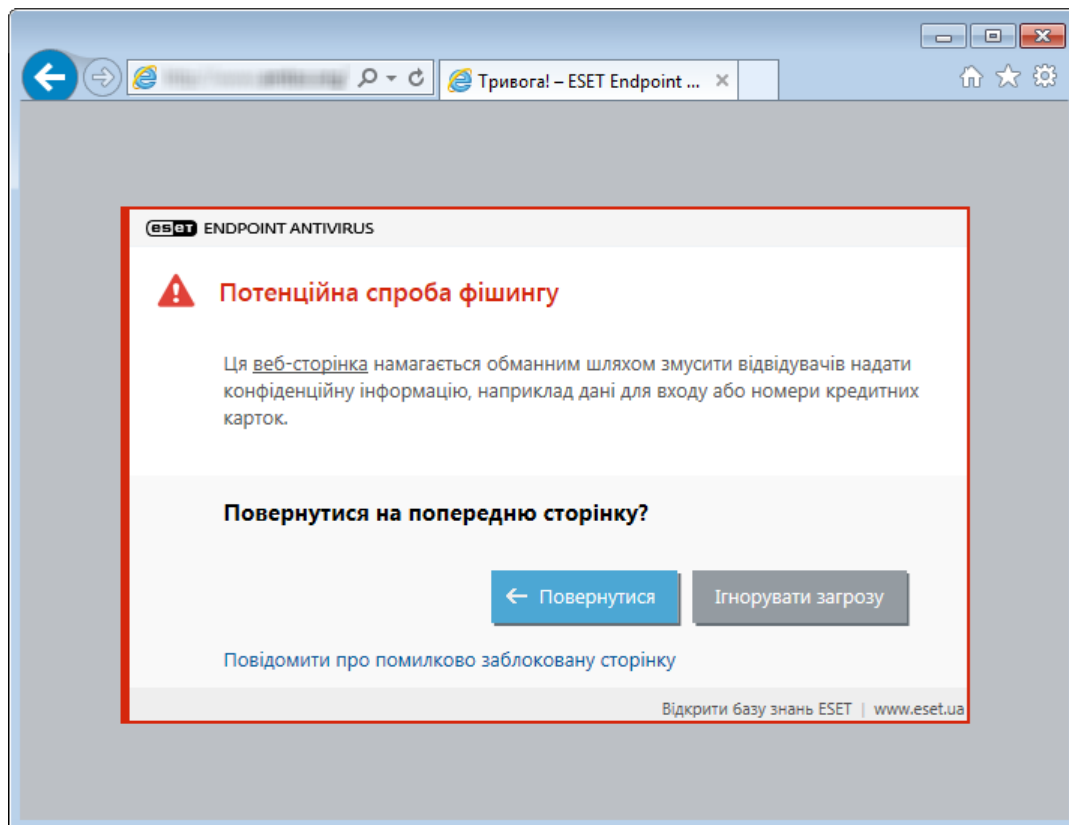
Фішинг — це злочинна активність із використанням соціотехніки (маніпулювання користувачами з метою отримати конфіденційні дані). Шахраї використовують фішинг-атаки для доступу до таких даних, як номери банківських рахунків, PIN-коди тощо. Більш докладну інформацію див. в [глосарії](#). У програмі ESET Endpoint Antivirus є модуль захисту від фішинг-атак, який блокує веб-сторінки, про які відомо, що на них поширюється відповідний вміст.

Захист від фішинг-атак увімкнено за замовчуванням. Цей параметр доступний у головному вікні програми: **Додаткові параметри (F5) > Інтернет і електронна пошта > Захист від фішинг-атак**.

Перегляньте цю [статтю в базі знань](#), щоб дізнатися більше про захист від фішинг-атак у ESET Endpoint Antivirus.

Відвідування шахрайського веб-сайту

Під час доступу до відомого фішинг-сайту у веб-браузері відкриється наведене нижче діалогове вікно. Якщо ви все одно бажаєте відвідати такий веб-сайт, натисніть **Ігнорувати загрозу** (не рекомендується).



За замовчуванням потенційні шахрайські веб-сайти, які було додано до білого списку, через кілька годин видаляються з нього. Щоб остаточно визначити веб-сайт як безпечний, скористайтесь інструментом [Управління URL-адресами](#). У меню **Додаткові параметри** (F5) розгорніть гілку **Інтернет і електронна пошта > Захист доступу до Інтернету > Керування URL-адресою > Список адрес**, натисніть **Змінити** й додайте до списку той веб-сайт, статус якого потрібно змінити.

Повідомлення про шахрайський сайт

Скористайтесь посиланням [Повідомити](#) й передайте дані про шахрайський/шкідливий веб-сайт компанії ESET для його подальшої перевірки.

Перш ніж відправляти дані про веб-сайт до ESET, упевніться, що виконується один або кілька перелічених нижче критеріїв.

- Веб-сайт узагалі не виявляється.
- Веб-сайт неправильно виявляється як загроза. У такому разі можна [Повідомити про помилковий результат фішингу](#).

Дані про веб-сайт також можна відправити електронною поштою. Надішліть повідомлення на адресу samples@eset.com. Обов'язково вкажіть тему повідомлення та надайте якомога більше інформації про веб-сайт (наприклад, веб-сайт, з якого ви на нього перейшли, як про нього дізналися тощо).

Оновлення програми

Регулярне оновлення ESET Endpoint Antivirus — найкращий спосіб забезпечити максимальний захист комп'ютера. Модуль оновлення гарантує, що програма завжди матиме актуальний стан. Це досягається двома шляхами: оновленням обробника виявлення та системних компонентів.

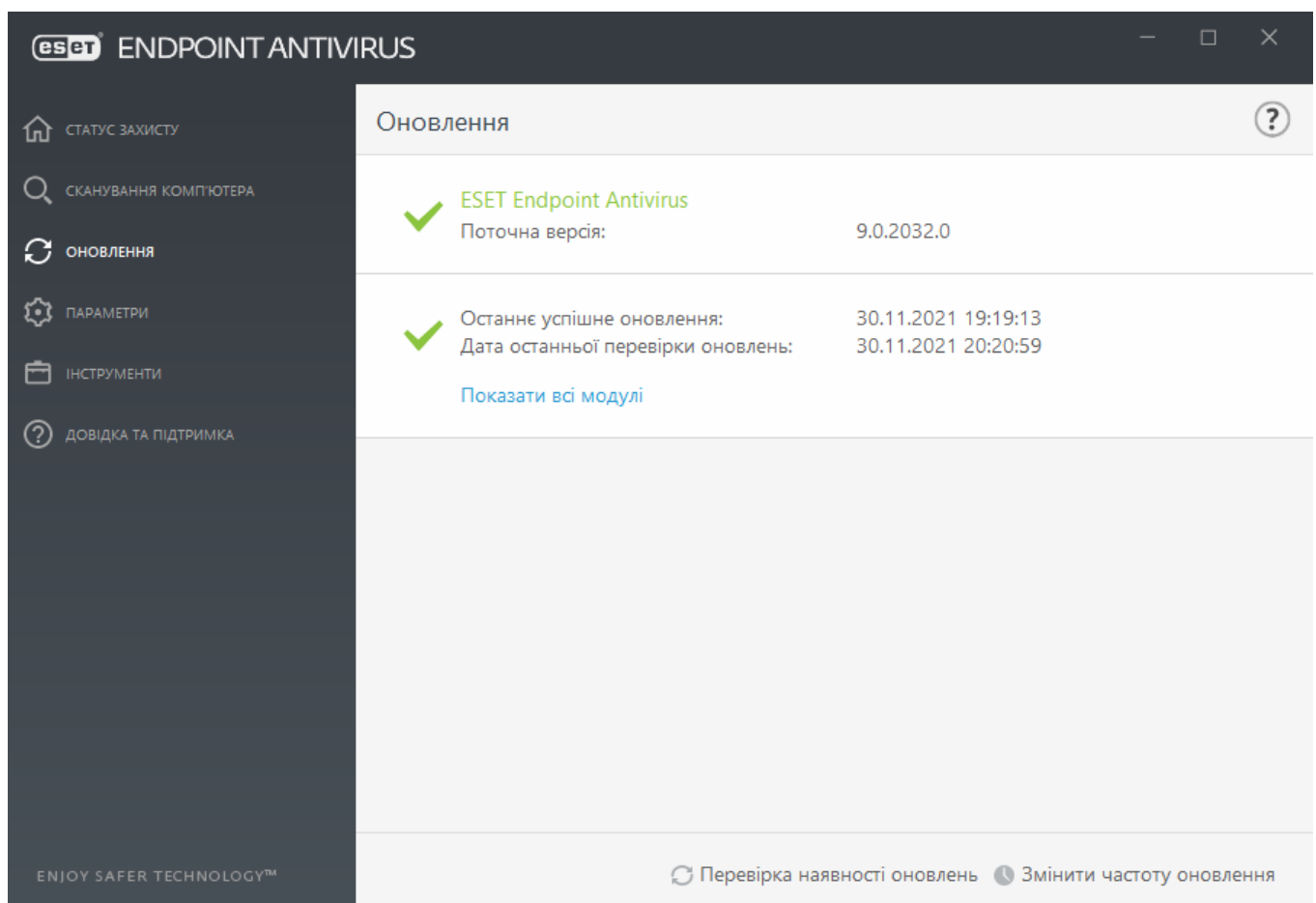
Якщо програму активовано, оновлення виконуються автоматично за замовчуванням.

Натиснувши **Оновлення** в головному вікні програми, можна переглянути поточний стан оновлення, відомості про дату й час останнього успішного оновлення, а також про те, чи потрібно його виконувати зараз. Також можна натиснути **Показати всі модулі**, щоб відкрити список інстальованих модулів і перевірити їх версію та дату останнього оновлення.

Окрім цього, тут доступний параметр, який дає можливість запустити процедуру вручну, – **Перевірити наявність оновлень**. Оновлення обробника виявлення і компонентів програми є важливою складовою частиною підтримки повного захисту від шкідливого коду. Приділіть особливу увагу налаштуванню та роботі цієї функції. Якщо дані ліцензії не було введено під час інсталяції, ліцензійний ключ можна додати, натиснувши **Активувати продукт** під час оновлення, щоб отримати доступ до серверів ESET.

Якщо активувати ESET Endpoint Antivirus за допомогою файлу автономної ліцензії, не вказуючи ім'я користувача та пароль, а потім спробувати оновити продукт, з'явиться повідомлення червоного кольору **Помилка оновлення модулів**. Це означає, що оновлення можна виконати лише із дзеркала.

i Ліцензійний ключ надається компанією ESET після придбання ESET Endpoint Antivirus.



Поточна версія: номер збірки ESET Endpoint Antivirus.

Останнє успішне оновлення: дата й час останнього успішного оновлення. Переконайтеся, що ця дата недавня: це означає, що обробник виявлення має актуальний стан.

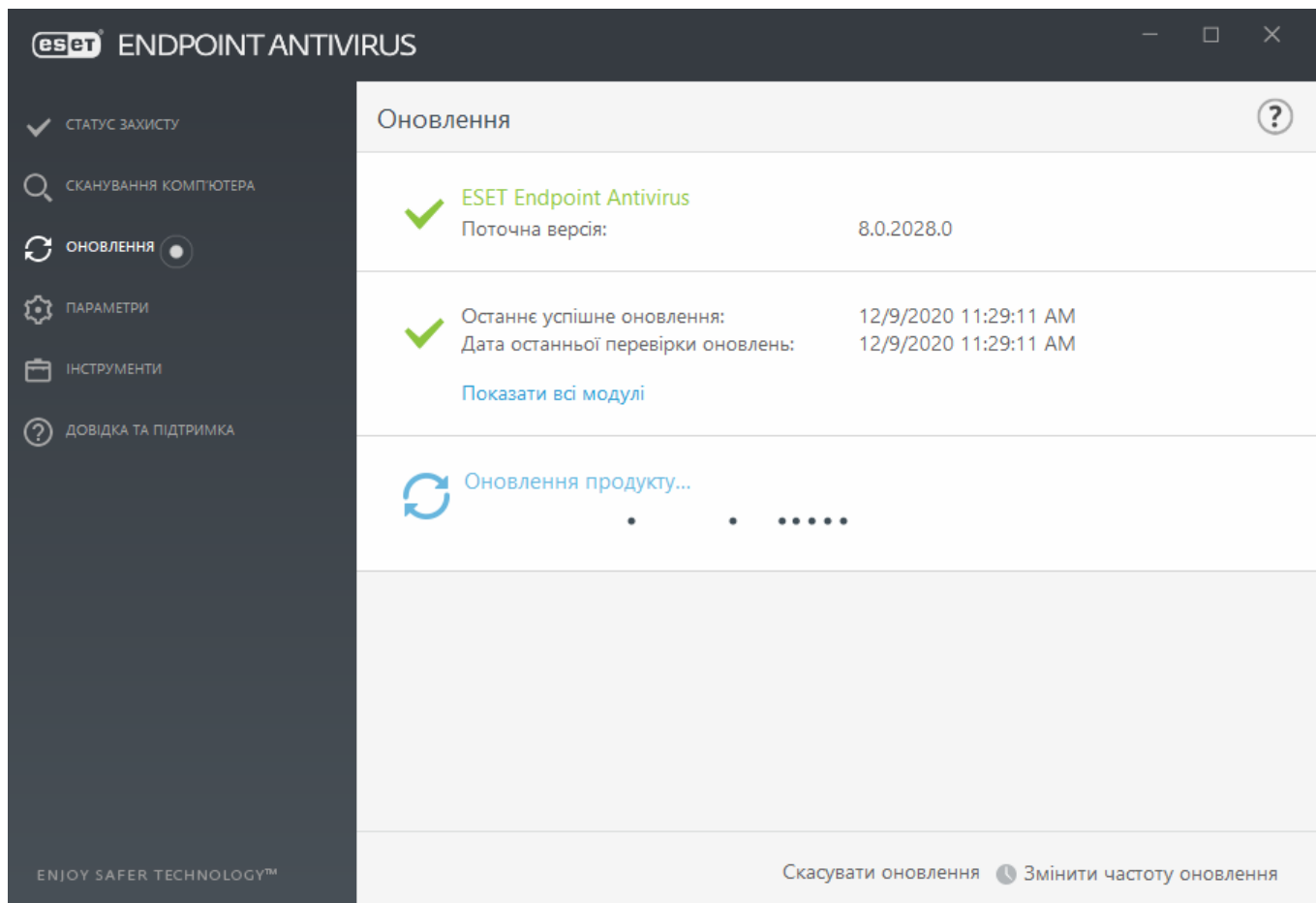
Дата останньої перевірки оновлень: дата й час останньої успішної перевірки наявності

оновлень для модулів.

Показати всі модулі: натисніть, щоб відкрити список інстальованих модулів і перевірити їх версію та дату останнього оновлення.

Процес оновлення

Щойно ви натиснете **Перевірити наявність оновлень**, почнеться завантаження. На екрані відображається індикатор виконання та час до закінчення завантаження. Щоб перервати процес оновлення, натисніть **Скасувати оновлення**.



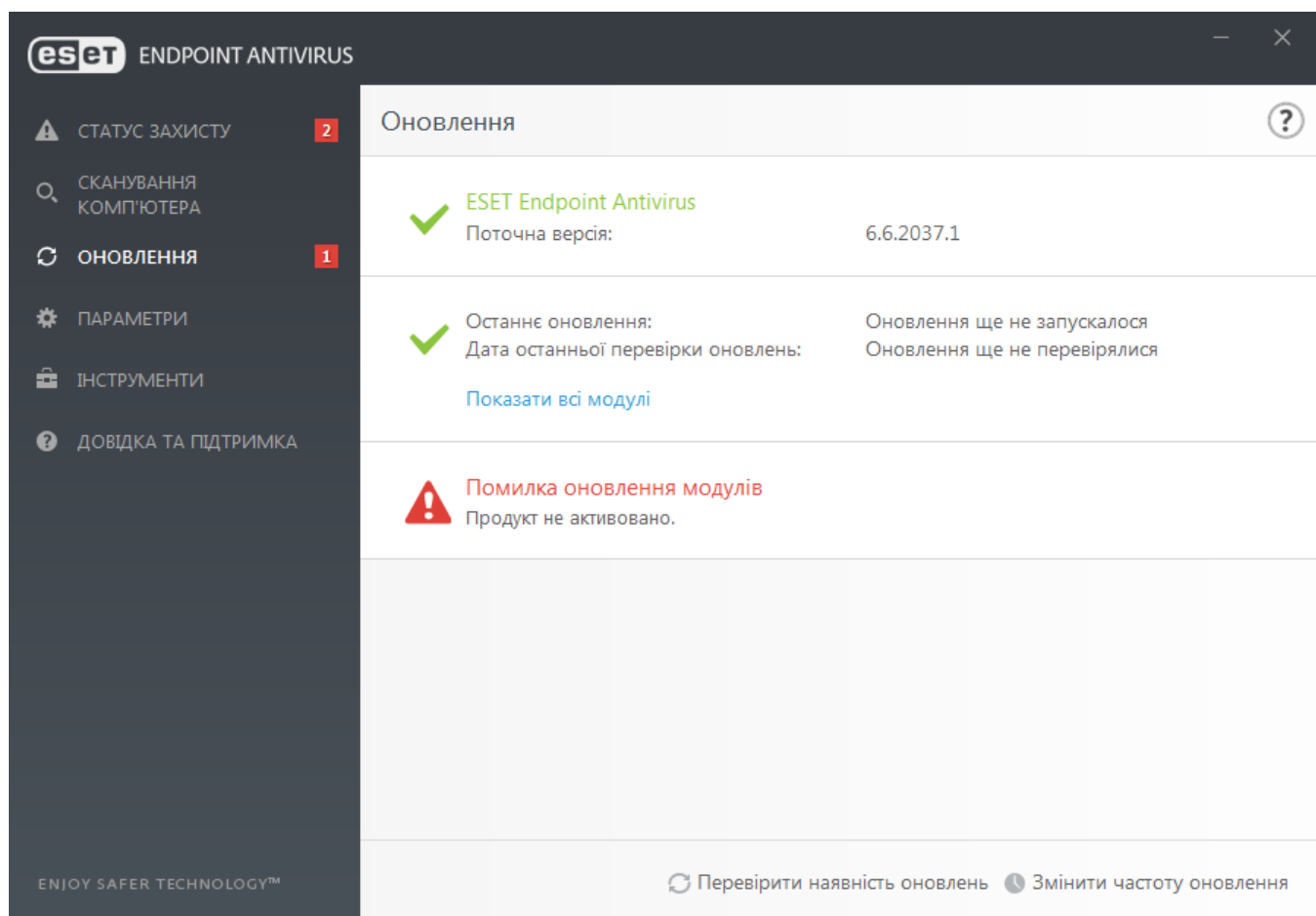
Зазвичай модулі оновлюються кілька разів на день. Якщо повідомлення не відображається, програма застаріла, у зв'язку з чим вона є більш уразливою до зараження. У цьому випадку оновіть модулі якомога швидше.

Обробник виявлення застарілий: ця помилка відображається після кількох невдалих спроб оновити модулі. Рекомендується перевірити параметри оновлення. Найпоширеніша причина помилки – неправильно введені дані автентифікації чи неналежним чином налаштовані [параметри підключення](#).

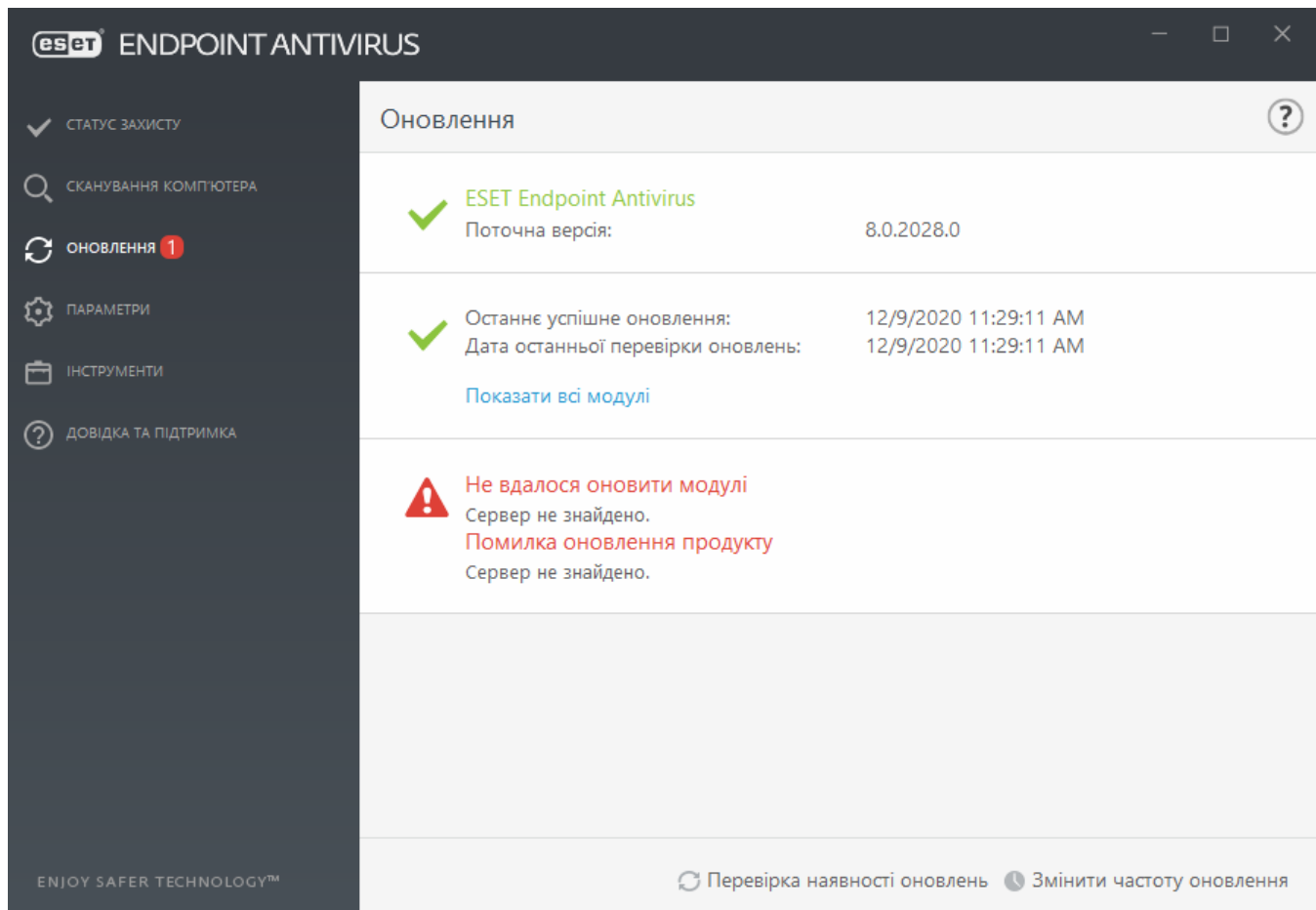
Попереднє сповіщення зумовлене двома наведеними нижче повідомленнями **Не вдалося оновити модулі** про невдале оновлення:

1. **Недійсна ліцензія** – у розділі параметрів оновлення неправильно введено ліцензійний ключ. Рекомендуємо перевірити дані автентифікації. Вікно додаткових параметрів (у головному меню натисніть **Параметри**, після чого виберіть **Додаткові параметри** або натисніть F5 на клавіатурі) містить додаткові опції оновлення. Натисніть **Довідка та**

підтримка > Керування ліцензією у головному меню та введіть новий ліцензійний ключ.



2. **Помилка під час завантаження файлів оновлення:** до появи цього повідомлення можуть призводити неправильні [параметри підключення до Інтернету](#). Рекомендується перевірити підключення до Інтернету (наприклад, відкривши в браузері будь-який веб-сайт). Якщо веб-сайт не відкривається, імовірно, підключення Інтернету не встановлено або комп'ютер має проблеми з підключенням. Зверніться до свого інтернет-провайдера, якщо не вдається встановити активне підключення до Інтернету.



i Докладнішу інформацію можна знайти в цій [статті бази знань ESET](#).

Параметри оновлення

Параметри налаштування оновлення доступні в дереві **Додаткові параметри** (F5) у розділі **Оновлення**. У розділі параметрів оновлення вказується інформація про відповідне джерело (наприклад, сервери оновлення й дані автентифікації для них).



Щоб оновлення були завантажені належним чином, важливо правильно вказати всі параметри. Якщо ви використовуєте брандмауер, переконайтеся, що програмі ESET дозволено взаємодіяти з Інтернетом (тобто дозволено зв'язок за протоколом HTTPS).

Основна

Поточний профіль оновлення відображається в розкритому меню **Вибрати профіль оновлення за замовчуванням**.

Інформацію щодо створення нового профілю, див. в розділі [Профілі](#).

Налаштування сповіщень про оновлення: клацніть Редагувати, щоб вибрати [сповіщення програми](#) для відображення. Можна вибрати спосіб доставки сповіщень: Показати на робочому столі та (або) Надіслати електронною поштою.

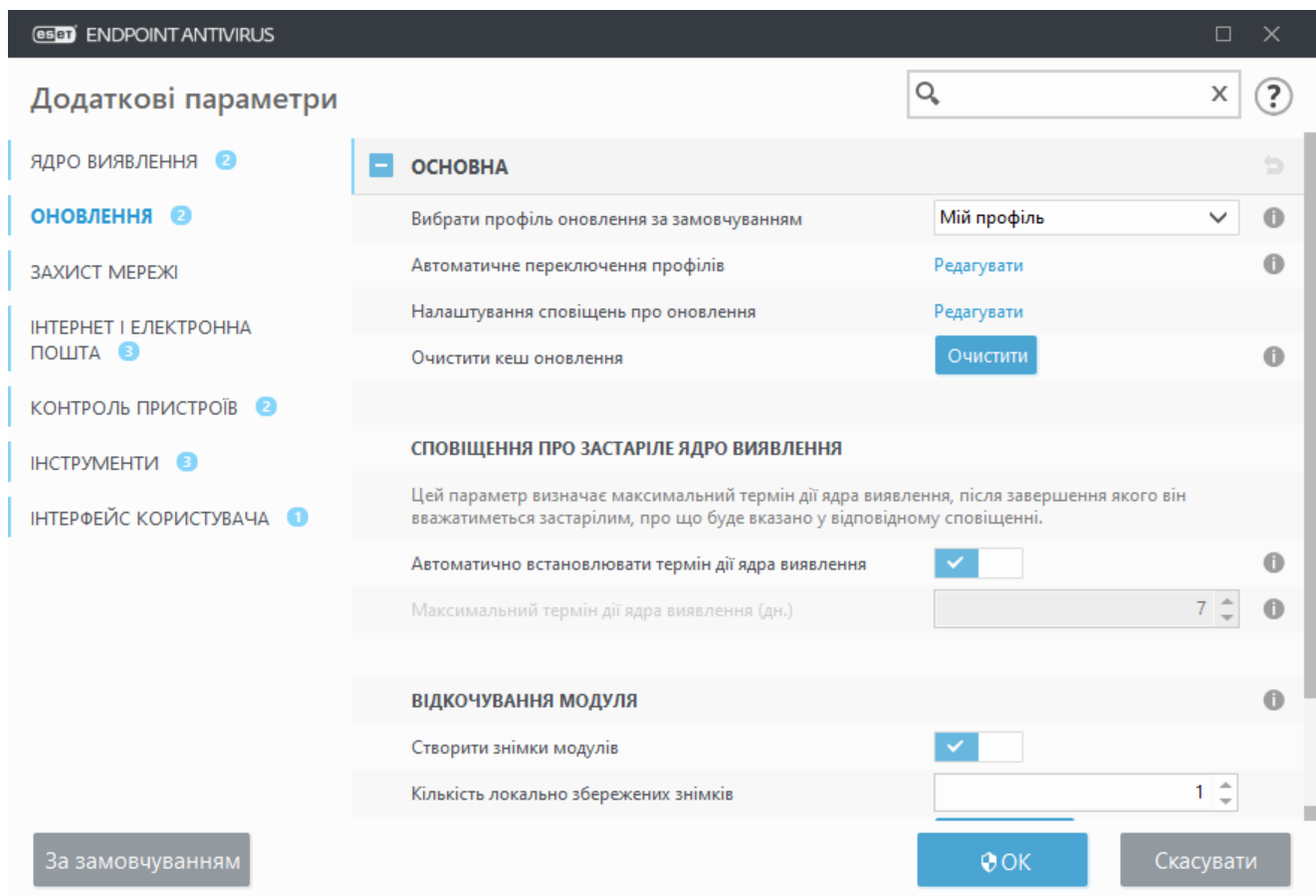
Якщо вам не вдається завантажити оновлення для модулів, клацніть **Очистити** поруч з елементом **Очистити кеш оновлення**, щоб видалити тимчасові файли/кеш оновлення.

Сповіщення про застарілий обробник виявлення

Автоматично встановлювати термін дії ядра виявлення: дає змогу встановити максимальний час (у днях), після завершення якого ядро виявлення позначатиметься як застаріле. Для параметра **Максимальний вік ядра виявлення (дні)** за замовчуванням встановлено значення 7.

Відкочування модуля

Якщо ви підозрюєте, що останнє оновлення обробника виявлення та/або модулів програми нестабільне або пошкоджене, можна [повернутися до попередньої](#) версії та вимкнути всі оновлення для вибраного періоду часу.



Профілі

Профілі оновлення можна створювати для різних конфігурацій і завдань оновлення. Зокрема ця функція стане в пригоді користувачам мобільних пристроїв, яким потрібен альтернативний профіль, оскільки їхні параметри підключення до Інтернету часто змінюються.

Активний профіль указано в розкритому меню **Виберіть профіль, який потрібно відредагувати** (за замовчуванням для цього параметра встановлено значення **Мій профіль**).

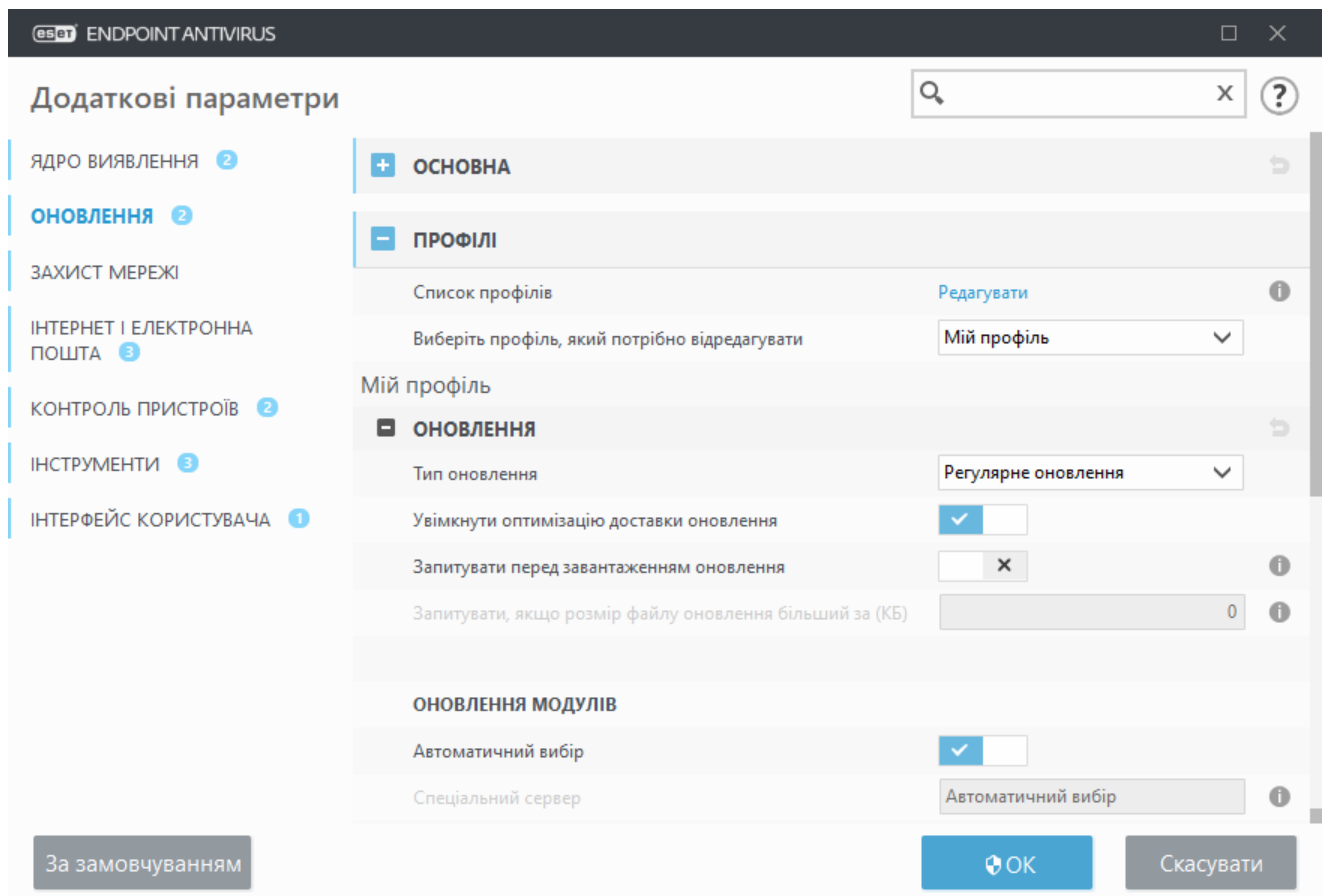
Щоб створити новий профіль, клацніть **Змінити** поруч з елементом **Список профілів**, уведіть **Ім'я профілю** й натисніть **Додати**.

Оновлення

За замовчуванням для параметра Тип оновлення вибрано значення Регулярне оновлення. Так файли оновлень автоматично завантажуватимуться із сервера ESET із мінімальним споживанням мережевого трафіку. Оновлення попередніх версій (параметр Бета-версії оновлень) – це оновлення, які пройшли повну внутрішню перевірку й незабаром будуть доступні для широкого загалу. Перевага бета-версії оновлення – доступ до найновіших методів виявлення й виправлення. Однак бета-версії оновлення можуть бути недостатньо стабільними, тому їх НЕ МОЖНА використовувати на виробничих серверах і робочих станціях, де потрібен високий рівень доступності й стабільності. Параметр Відкладені оновлення дає змогу виконувати оновлення зі спеціальних серверів, після чого нові версії вірусних баз даних буде інстальовано із затримкою щонайменше X год. Це будуть бази даних, протестовані в реальному середовищі, а тому класифіковані як стійкі.

Увімкнути оптимізацію доставки оновлень: якщо цей параметр увімкнено, файли оновлення можна завантажити з CDN (мережа доставки вмісту). Вимкнення цього параметра може призвести до переривань і уповільнення завантаження, коли виділені сервери оновлення ESET перевантажені. Таке вимкнення корисне, коли брандмауер обмежений доступом тільки до [IP-адрес сервера оновлення ESET](#), або підключення до сервісів CDN не працює.

Запитувати перед завантаженням оновлення: у сповіщенні можна буде підтвердити або скасувати завантаження файлу оновлення. Якщо розмір файлу оновлення перевищуватиме значення, указане в полі Запитувати, якщо розмір файлу оновлення більший за (КБ), програма відображатиме діалогове вікно підтвердження. Якщо вибрати розмір файлу 0 КБ, сповіщення відображатиметься завжди.



Оновлення модулів

За замовчуванням параметр **Автоматичний вибір** увімкнено. **Спеціальний сервер** — це місце зберігання оновлень. У разі використання сервера оновлень ESET рекомендується залишити параметр за замовчуванням без змін.

Увімкнути частіші оновлення вірусної бази даних: вірусна база даних буде оновлюватись через коротші проміжки часу. Якщо цей параметр вимкнено, це може негативно позначитися на ефективності виявлення.

Дозволити оновлення модулів зі змінного носія: дає змогу оновлювати зі змінного носія, якщо на ньому створено дзеркало. Якщо вибрано параметр Автоматично, оновлення відбуватиметься у фоновому режимі. Щоб з'являлися діалогові вікна стосовно оновлення, виберіть Завжди запитувати.

У разі використання локального HTTP-сервера (або "дзеркала") параметри сервера оновлення потрібно вказати таким чином:


`http://ім'я_комп'ютера_або_його_IP-адреса:2221`

У разі використання локального HTTP-сервера з протоколом SSL параметри сервера оновлення потрібно вказати таким чином:

`https://ім'я_комп'ютера_або_його_IP-адреса:2221`

У разі використання спільної папки параметри сервера оновлення потрібно вказати таким чином:

`\\ім'я_комп'ютера_або_його_IP-адреса\спільна_папка`

 Номер порту сервера HTTP, указаний у прикладах вище, залежить від того, на якому порту працює сервер HTTP/HTTPS.

Оновлення продукту

Див. розділ [Оновлення продукту](#).

Параметри підключення

Див. розділ [Параметри підключення](#).

Дзеркало оновлень

Див. розділ [Дзеркало оновлень](#).

Відкочування оновлення

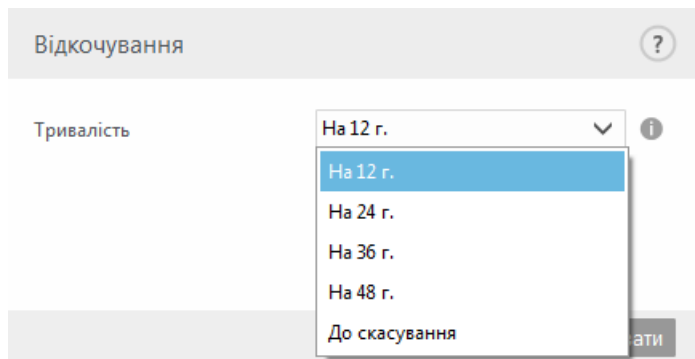
Якщо ви підозрюєте, що нове оновлення ядра виявлення або модулів програми нестабільне або пошкоджене, можна повернутися до попередньої версії й тимчасово вимкнути оновлення. Окрім того, можна активувати попередньо вимкнуті оновлення, якщо їх було призупинено на невизначений час.

ESET Endpoint Antivirus зберігає знімки ядра виявлення й модулів програми, які можна використовувати з функцією відкочування. Щоб створювати знімки вірусної бази даних, залиште перемикач **Створити знімки модулів** увімкненим. Якщо перемикач **Створити знімки модулів** увімкнено, під час першого оновлення створюється перший знімок. Наступний знімок

створюється через 48 годин. У полі **Кількість локально збережених знімків** відображається кількість збережених знімків ядра виявлення.

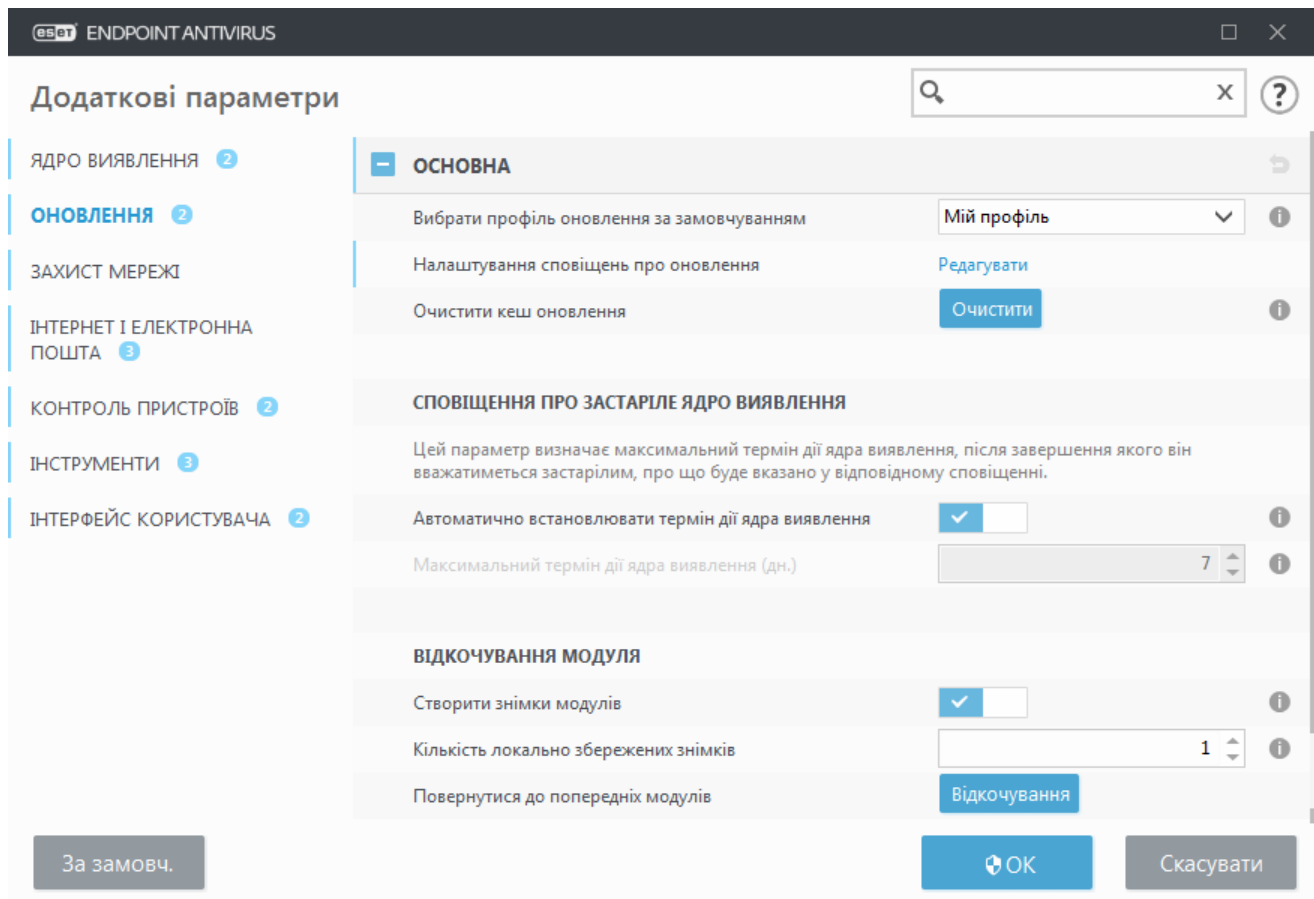
i Коли досягнуто максимальної кількості знімків (наприклад, три), найстаріший знімок замінюється новим знімком кожні 48 годин. ESET Endpoint Antivirus відкочує оновлення ядра виявлення й модуля програми до найстарішої версії знімка.

Якщо ви вибираєте параметр **Відкочування (Додаткові параметри (F5) > Оновити > Базові > Відкочування модуля)**, з'явиться розкривне меню **Тривалість**, де потрібно буде вибрати часовий інтервал.



Для призупинення оновлень на невизначений час (доки отримання оновлень не буде відновлено вручну) виберіть **До скасування**. Оскільки цей параметр спричиняє потенційну загрозу для безпеки, не рекомендується вибирати його.

Якщо відкочування вже виконано, кнопка **Відкочування** замінюється на **Дозволити оновлення**. Протягом періоду, вибраного в розкривному меню **Призупинити оновлення**, оновлення не дозволятимуться. Версію ядра виявлення буде понижено до найстарішої серед доступних, тож вона зберігатиметься як знімок у файловій системі на локальному комп'ютері.



✓ Припустімо, що найновішою версією обробника виявлення є версія 22700, а версії 22698 і 22696 зберігаються як знімки ядра виявлення. Зверніть увагу, що версія 22697 недоступна. У цьому прикладі комп'ютер було вимкнено, коли версія 22697 була актуальною, і ще до завантаження цієї версії вже з'явилася інша найновіша версія. Якщо в полі **Кількість локально збережених знімків** задано значення 2, і ви клацнули **Відкочування**, ядро виявлення (разом із модулями програми) буде відкочено до версії 22696. Цей процес може тривати деякий час. На екрані [Оновити](#) перевірте, чи було понижено версію ядра виявлення.

Оновлення продукту

У розділі **Оновлення продукту** містяться параметри, пов'язані з оновленнями продукту. Програма дає можливість налаштувати її поведінку на випадок появи оновлень продукту.

Оновлення продукту додають нові можливості або змінюють наявні в попередніх версіях. Оновлення може бути застосовано автоматично без участі користувача або з відображенням відповідного сповіщення. Після інсталяції оновлень продукту може знадобитися перезавантажити комп'ютер.


Автоматичні оновлення: призупинення автоматичних оновлень для певних профілів оновлення тимчасово деактивує автоматичні оновлення продуктів під час підключення до Інтернету з інших мереж або під час використання лімітних підключень. Не вимикайте цей параметр, щоб мати постійний доступ до найновіших функцій і забезпечити максимально можливий рівень захисту. Докладніше про автоматичні оновлення див. в темі [Запитання й відповіді щодо автоматичних оновлень](#).

За замовчуванням оновлення продукту завантажуються із серверів репозиторію ESET. У великих

або автономних середовищах можна розподілити трафік, щоб забезпечити внутрішнє кешування файлів продукту.

[Визначення настроюваного сервера для оновлень компонентів програми](#)

1. Визначте шлях до оновлень продукту в полі **Спеціальний сервер**. Можна вказати посилання HTTP(S), шлях до мережевої папки SMB або папки на локальному диску або змінному носії. Для мережевих дисків замість букви на їх позначення використовуйте шлях UNC.
2. Залиште поля **Ім'я користувача** й **Пароль** пустими, якщо вони не потрібні. За потреби вкажіть тут відповідні облікові дані для автентифікації HTTP на настроюваному веб-сервері.
3. Підтвердьте зміни й перевірте наявність оновлень продукту, виконавши стандартне оновлення ESET Endpoint Antivirus.

 Вибір опції залежить від особливостей робочої станції, де застосовуватимуться відповідні параметри. Пам'ятайте про відмінності між робочими станціями й серверами. Наприклад, автоматичне перезавантаження сервера після оновлення продукту може завдати серйозної шкоди компанії.

Параметри підключення

Щоб отримати доступ до параметрів проксі-сервера для певного профілю оновлення, виберіть елемент **Оновлення** в дереві **Додаткові параметри** (F5) і натисніть **Профілі > Оновлення > Параметри оновлення**.

Проксі-сервер

Клацніть розкривне меню **Режим проксі-сервера** й виберіть один із трьох наведених нижче параметрів.

- Не використовувати проксі-сервер
- Підключення через проксі-сервер
- Використовувати глобальні параметри проксі-сервера

Якщо вибрати параметр **Використовувати глобальні параметри проксі-сервера**, програма використовуватиме параметри проксі-сервера, уже вказані в гілці **Інструменти > Проксі-сервер** дерева додаткових параметрів.

Виберіть параметр **Не використовувати проксі-сервер**, щоб указати, що для оновлення ESET Endpoint Antivirus не потрібно використовувати проксі-сервер.

Параметр **Підключення через проксі-сервер** слід вибрати в наведених нижче випадках.

- Якщо для оновлення ESET Endpoint Antivirus використовується проксі-сервер, відмінний від вказаного в меню "Інструменти" > **Проксі-сервер**. У цій конфігурації інформацію для нового проксі-сервера має бути вказано в полі адреси **Проксі-сервер**, у полі зв'язку **Порт** (за промовчанням – 3128), а також у полях **Ім'я користувача** та **Пароль** (якщо потрібно).
- Якщо параметри проксі-сервера для загального використання не було встановлено, але для оновлення програма ESET Endpoint Antivirus підключатиметься до проксі-сервера.
- Якщо комп'ютер підключено до Інтернету через проксі-сервер. Під час інсталяції

програми значення параметрів беруться з конфігурації браузера, але якщо вони змінюються (наприклад, ви звертаєтесь до іншого постачальника послуг Інтернету), переконайтеся, що в цьому вікні вказано правильні параметри проксі-сервера. В іншому разі програма не зможе підключитися до серверів оновлень.

За замовчування для проксі-сервера застосовується параметр **Використовувати глобальні параметри проксі-сервера**.

Використовувати пряме підключення, якщо проксі-сервер недоступний – якщо проксі-сервер недоступний, у процесі оновлення буде виконано його обхід.

Спільні папки Windows

Під час оновлення з локального сервера під керуванням операційної системи Windows NT автентифікація кожного мережевого підключення вимагається за замовчуванням.

Щоб налаштувати такий обліковий запис, виберіть у розкритому меню **Підключатися до локальної мережі як**:

- **Системний обліковий запис (за замовчуванням),**
- **Поточний користувач,**
- **Вказаний користувач.**

Виберіть **Системний обліковий запис (за замовчуванням)**, щоб використовувати системний обліковий запис для автентифікації. Як правило, процес автентифікації не відбувається, якщо в розділі головних параметрів оновлення не вказані дані автентифікації.

Щоб для автентифікації програма використовувала дані облікового запису користувача, який увійшов до системи, виберіть параметр **Поточний користувач**. Недолік цього рішення полягає в тому, що програма не зможе підключитися до сервера оновлень, якщо в потрібний момент жоден користувач не увійшов у систему.

Використовуйте параметр **Зазначений користувач**, коли потрібно, щоб для автентифікації програма використовувала обліковий запис конкретного користувача. Використовуйте цей метод, якщо не вдається виконати підключення за допомогою системного облікового запису. Пам'ятайте, що обліковий запис зазначеного користувача повинен мати доступ до каталогу файлів оновлення на локальному сервері. Інакше програма не зможе встановити підключення та завантажити оновлення.

Параметри **Ім'я користувача** та **Пароль** необов'язкові.

Якщо вибрано параметр **Поточний користувач** або **Зазначений користувач**, у разі зміни ідентифікації програми з використанням даних потрібного користувача може статися помилка. Дані автентифікації для локальної мережі рекомендується вводити в розділі головних параметрів оновлення. У цьому розділі параметрів оновлення дані автентифікації слід вводити таким чином: назва_домену\користувач (для робочої групи – назва_робочої_групи\назва) і пароль. У разі оновлення з HTTP-версії локального сервера автентифікація не вимагається.

Виберіть параметр **Відключатися** від сервера після оновлення, щоб примусово розривати підключення до сервера, яке залишається активним навіть після завантаження оновлень.

Дзеркало оновлень

ESET Endpoint Antivirus дає змогу користувачеві створювати копії файлів оновлень, які можна використовувати для оновлення інших робочих станцій у мережі. Використовувати дзеркало (копію файлів оновлень у середовищі локальної мережі) зручно, оскільки файли оновлень не потрібно щоразу завантажувати із серверів оновлень постачальників на кожну робочу станцію. Оновлення завантажуються на локальний сервер-дзеркало й потім поширюються на всі робочі станції. Це дає можливість уникнути ризику перевантаження мережі надлишковим трафіком. Оновлення клієнтських робочих станцій із дзеркала оптимізує навантаження на мережу й зберігає пропускну здатність каналу підключення до Інтернету.

i Щоб мінімізувати інтернет-трафік у мережах, де ESET PROTECT використовується для керування великою кількістю клієнтів, рекомендуємо використовувати проксі-сервер Apache HTTP, а не налаштовувати клієнт як дзеркало. Проксі-сервер Apache HTTP можна інсталювати з ESET PROTECT за допомогою універсального інсталятора або автономного компонента. Докладні відомості, зокрема інформацію про відмінності між проксі-сервером Apache HTTP, інструментом "Дзеркало" й прямим підключенням, див. на нашій [сторінці онлайн-довідки ESET PROTECT](#).

Налаштування локального сервера-дзеркала доступні в розділі **Оновлення** меню додаткових параметрів. Щоб перейти до нього, натисніть **F5**, виберіть **Оновлення > Профілі** й відкрийте вкладку **Дзеркало оновлень**.

The screenshot shows the 'Додаткові параметри' (Additional Parameters) window with the 'ДЗЕРКАЛО' (Mirror) tab selected. The left sidebar contains a list of categories: АНТИВІРУС, ОНОВЛЕННЯ (selected), ІНТЕРНЕТ І ЕЛЕКТРОННА ПОШТА, КОНТРОЛЬ ПРИСТРОЇВ, ІНСТРУМЕНТИ, and ІНТЕРФЕЙС КОРИСТУВАЧА. The main area is divided into sections: 'ДЗЕРКАЛО' with a toggle for 'Створити дзеркало оновлення' (checked), 'ДОСТУП ДО ФАЙЛІВ ОНОВЛЕННЯ' with a toggle for 'Оновлення файлів через внутрішній HTTP-сервер' (checked), a text field for the folder path (C:\ProgramData\ESET\ESET Smart Security Premium\mirror) with a 'Очистити' button, and fields for 'Ім'я користувача' and 'Пароль'. Below this is a 'ФАЙЛИ' section with a 'Файли' button and a 'Редагувати' link. At the bottom, there are three expandable sections: 'HTTP-СЕРВЕР', 'ПІДКЛЮЧАТИСЯ ДО ЛОКАЛЬНОЇ МЕРЕЖІ ЯК', and 'ОНОВЛЕННЯ КОМПОНЕНТІВ ПРОГРАМИ'. The bottom of the window has three buttons: 'За замовч.' (Default), 'OK', and 'Скасувати' (Cancel).

Щоб створити дзеркало на клієнтській робочій станції, активуйте параметр **Створити дзеркало оновлення**. Адже він відкриває доступ до інших параметрів дзеркала, зокрема тих, які визначають спосіб доступу до файлів оновлення та шлях до файлів дзеркала.

Доступ до файлів оновлення

Увімкнути HTTP-сервер: якщо увімкнено, доступ до файлів оновлень можна [отримати через протокол HTTP](#) (облікові дані вводити не потрібно).

Способи отримання доступу до сервера-дзеркала детально описано в розділі [Оновлення із дзеркала](#). Існує два основних способи отримання клієнтами доступу до дзеркала: папка з файлами оновлень може бути представлена як спільна папка в мережі або як HTTP-сервер.

Папку, у яку зберігатимуться файли оновлень для дзеркала, можна вказати в розділі **Папка для дзеркальних дублікатів файлів**. Якщо потрібно вказати іншу папку, натисніть **Очистити**, щоб видалити попередньо вибрану папку `C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror`, а потім – **Змінити**, щоб знайти папку на локальному комп'ютері або спільну папку в мережі. Якщо для вибраної папки потрібна авторизація, слід ввести дані автентифікації в полях **Ім'я користувача** та **Пароль**. Якщо вибрана цільова папка розташована на мережевому диску з операційною системою Windows NT/2000/XP, зазначені ім'я користувача та пароль мають надавати права запису для вибраної папки. Формат імені користувача й пароля має бути таким: Домен/користувач або Робоча група/користувач. Не забудьте вказати відповідні паролі.

HTTP-сервер і SSL для дзеркала

У розділі **HTTP-сервер** на вкладці **Дзеркало** можна вказати **порт сервера**, на якому працюватиме HTTP-сервер, а також тип **автентифікації**, яка буде використовуватися HTTP-сервером. За замовчуванням для сервера використовується порт **2221**.

Автентифікація: визначає спосіб автентифікації для доступу до файлів оновлень. Доступні наведені нижче варіанти: **Немає**, **Базова** й **NTLM**. Виберіть **Базова**, щоб використовувати кодування base64 з базовою автентифікацією за допомогою імені користувача та пароля. Варіант **NTLM** передбачає кодування з використанням безпечного методу. Для автентифікації використовується обліковий запис користувача робочої станції зі спільним доступом до файлів оновлень. За замовчуванням використовується значення **Немає**, що надає доступ до файлів оновлень, не вимагаючи автентифікації.

i Дані автентифікації (**ім'я користувача й пароль**) використовуватимуться тільки для доступу до дзеркала HTTP-сервера. Заповнюйте ці поля тільки тоді, коли для доступу потрібно використовувати ім'я користувача й пароль.

Додайте **Файл ланцюжка сертифікатів** або створіть самостійно підписаний сертифікат, щоб забезпечити підтримку HTTP-сервера через протокол HTTPS (SSL). Доступні такі **типи сертифікатів**: ASN, PEM і PFX. Для забезпечення додаткового захисту завантажувати файли оновлень можна через протокол HTTPS. У разі використання цього протоколу практично неможливо відстежити передачу даних і облікові дані для входу. За замовчуванням для параметра **Тип приватного ключа** встановлено значення **Інтегрований** (тому параметр **Файл приватного ключа** за замовчуванням вимкнено). Це означає, що приватний ключ є частиною вибраного файлу ланцюжка сертифікатів.

Самопідписані сертифікати для дзеркала HTTPS



Якщо використовується дзеркало HTTPS-сервера, імпортуйте його сертифікат у надійне кореневе сховище на всіх клієнтських комп'ютерах. Див. розділ [Installing the trusted root certificate](#) (Інсталяція довіреного кореневого сертифіката) в документації Windows.

Оновлення із дзеркала

Існує два основних способи налаштування дзеркала – сховища, з якого клієнти завантажують файли оновлення. Папка з файлами оновлень може бути представлена як спільна папка в мережі або як HTTP-сервер.

Доступ до дзеркала за допомогою внутрішнього HTTP-сервера

Ця конфігурація використовується за замовчуванням, і її заздалегідь указано в налаштуваннях програми. Щоб дозволити доступ до дзеркала за допомогою HTTP-сервера, перейдіть до меню **Додаткові параметри > Оновлення > Профілі > Дзеркало оновлення** та виберіть **Створити дзеркало оновлення**.

У розділі **HTTP-сервер** на вкладці **Дзеркало** можна вказати **порт сервера**, на якому працюватиме HTTP-сервер, а також тип **автентифікації**, яка буде використовуватися HTTP-сервером. За замовчуванням для сервера використовується порт **2221**.

Аутентифікація: визначає спосіб автентифікації для доступу до файлів оновлень. Доступні наведені нижче варіанти: **Немає**, **Базова** й **NTLM**. Виберіть **Базова**, щоб використовувати кодування base64 з базовою автентифікацією за допомогою імені користувача та пароля. Варіант **NTLM** передбачає кодування з використанням безпечного методу. Для автентифікації використовується обліковий запис користувача робочої станції зі спільним доступом до файлів оновлень. За замовчуванням використовується значення **Немає**, що надає доступ до файлів оновлень, не вимагаючи автентифікації.



Якщо потрібно надати доступ до файлів оновлень через HTTP-сервер, папка дзеркала має бути розташована на тому ж комп'ютері, на якому інстальовано програму ESET Endpoint Antivirus, що використовуувалася для її створення.



Якщо кілька разів поспіль не вдалося виконати оновлення із дзеркала, на панелі оновлень головного меню відобразиться помилка **Недійсне ім'я користувача і/або пароль**. Рекомендуємо перейти до розділу **Додаткові параметри > Оновити > Профілі > Дзеркало оновлень** і перевірити ім'я користувача й пароль. Найчастіше причиною цієї помилки є неправильно введені дані автентифікації.

Після завершення налаштування сервера-дзеркала потрібно додати новий сервер оновлення на клієнтські робочі станції. Для цього виконайте наведені нижче дії.

- Відкрийте розділ **Додаткові параметри** (F5) і клацніть **Оновити > Профілі > Оновлення > Оновлення модуля**.
- Зніміть прапорець **Автоматичний вибір** і додайте новий сервер у полі **Сервер оновлення** в одному з таких форматів:
`http://IP_адреса_вашого_сервера:2221`

https://IP_адреса_вашого_сервера:2221 (якщо використовується SSL)

Доступ до дзеркала через спільні папки системи

Спочатку потрібно створити спільну папку на локальному або мережевому пристрої. Під час створення папки дзеркала потрібно надати доступ для запису користувачеві, який зберігатиме файли оновлень, і доступ для читання всім користувачам, які оновлюватимуть ESET Endpoint Antivirus з цієї папки.

Потім налаштуйте доступ до дзеркала в меню **Додаткові параметри > Оновлення > Профілі > вкладка Дзеркало оновлення**, вимкнувши параметр **Увімкнути HTTP-сервер**. Цей параметр вмикається за замовчуванням під час інсталяції програми.

Якщо спільна папка розташована на іншому комп'ютері в мережі, необхідно ввести дані автентифікації для доступу до нього. Щоб указати дані автентифікації, відкрийте розділ ESET Endpoint Antivirus **Додаткові параметри (F5)** і клацніть **Оновити > Профілі > Оновлення > Параметри підключення > Спільні папки Windows > Підключитися до локальної мережі як**. Це той самий параметр оновлення, який описано в розділі [Підключатися до локальної мережі як](#).

Для доступу до папки дзеркала необхідно увійти в систему з тим же самим обліковим записом, що використовувався для входу на комп'ютер, на якому створено дзеркало. Якщо комп'ютер знаходиться в домені, необхідно використовувати ім'я користувача в форматі "домен\користувач". Якщо комп'ютер не знаходиться в домені необхідно використовувати ім'я користувача в форматі "IP_адреса_вашого_сервера\користувач" або "ім'я хоста\користувач".

Після завершення налаштування дзеркала перейдіть до клієнтської робочої станції та вкажіть `\\UNC\ШЛЯХ` як сервер оновлення відповідно до наведених нижче інструкцій.

1. Відкрийте меню **Додаткові параметри** ESET Endpoint Antivirus та натисніть **Оновлення > Профілі > Оновлення**.
2. Зніміть прапорець **Автоматичний вибір** поруч з елементом **Оновлення модуля** й додайте новий сервер у полі **Сервер оновлення** у форматі `\\UNC\PATH`.

i Для належного функціонування оновлень шлях до папки дзеркала потрібно вказати у форматі UNC. Оновлення з підключених мережевих дисків можуть не працювати.

Створення дзеркала за допомогою інструмента "Дзеркало"

Інструмент "Дзеркало" створює структуру папок, яка відрізняється від аналогічної структури дзеркала Endpoint. Кожна папка містить файли оновлення для групи продуктів. Необхідно вказати повний шлях до правильної папки в параметрах оновлення продукту, який використовує дзеркало.

Наприклад, щоб оновити ESET PROTECT із дзеркала, для параметра [Сервер оновлень](#) встановіть указане нижче значення (відповідно до основного розташування сервера HTTP): `http://your_server_address/mirror/eset_upd/era6`

Останній розділ контролює компоненти програми. За замовчуванням компоненти завантаженої програми підготовлені до копіювання до локального дзеркала. Якщо активовано параметр **Оновлення продукту**, не потрібно натискати **Оновити**, оскільки файли копіюються до локального дзеркала автоматично, щойно стають доступними. Докладніше про оновлення компонентів програми див. в розділі [Режим оновлення](#).

Виправлення неполадок під час оновлення із дзеркала

У більшості випадків проблеми в процесі оновлення із сервера-дзеркала викликані однією або кількома причинами: неправильними параметрами папки дзеркала, некоректними даними автентифікації для папки дзеркала, помилковими параметрами локальних робочих станцій, які намагаються завантажити файли оновлення із дзеркала, або поєднанням усіх цих чинників. Нижче розглядаються найпоширеніші проблеми, які можуть виникати в процесі оновлення із дзеркала.

ESET Endpoint Antivirus повідомляє про помилку підключення до сервера-дзеркала:

імовірно, неправильно вказано сервер оновлення (мережевий шлях до папки дзеркала), з якого локальні робочі станції завантажують оновлення. Щоб перевірити папку, натисніть меню **Пуск** в ОС Windows, виберіть **Виконати**, введіть ім'я папки й натисніть **ОК**. Після цього має відобразитися вміст папки.

ESET Endpoint Antivirus вимагає введення імені користувача й пароля: імовірно, введено неправильні дані автентифікації (ім'я користувача й пароль) у розділі оновлення. Ім'я користувача та пароль використовуються для надання доступу до сервера оновлень, з якого програма буде оновлюватися. Переконайтеся, що дані автентифікації правильні та введені в належному форматі. Наприклад, Домен/ім'я_користувача або Робоча_група/ім'я_користувача й відповідні паролі. Якщо сервер-дзеркало доступний "Для всіх", це зовсім не означає, що доступ надається будь-якому користувачеві. "Для всіх" не означає "для будь-якого неавторизованого користувача". Це значить, що відповідна папка доступна для всіх користувачів домену. Отже, навіть якщо папка доступна "Для всіх", усе одно в розділі параметрів оновлення потрібно ввести ім'я користувача домену та пароль.

ESET Endpoint Antivirus повідомляє про помилку підключення до сервера-дзеркала: зв'язок через порт, визначений для доступу до HTTP-версії дзеркала, блокується.

ESET Endpoint Antivirus повідомляє про помилку під час завантаження файлів: імовірно, неправильно вказано сервер оновлення (мережевий шлях до папки дзеркала), з якого локальні робочі станції завантажують оновлення.

Створення завдань оновлення

Процес оновлення можна ініціювати вручну, натиснувши **Перевірити наявність оновлень** в основному вікні, яке відобразиться після вибору елемента **Оновлення** в головному меню.

Оновлення також можна виконувати як заплановані завдання. Щоб налаштувати заплановане завдання, натисніть **Інструменти > Завдання за розкладом**. За замовчуванням у програмі ESET Endpoint Antivirus активовано наведені нижче завдання.

- **Регулярне автоматичне оновлення**
- **Автоматичне оновлення після встановлення модемного підключення**
- **Автоматичне оновлення після входу користувача в систему**

Кожне завдання оновлення за бажанням можна змінювати. Окрім стандартних завдань оновлення, користувач може створювати нові завдання із власною користувацькою

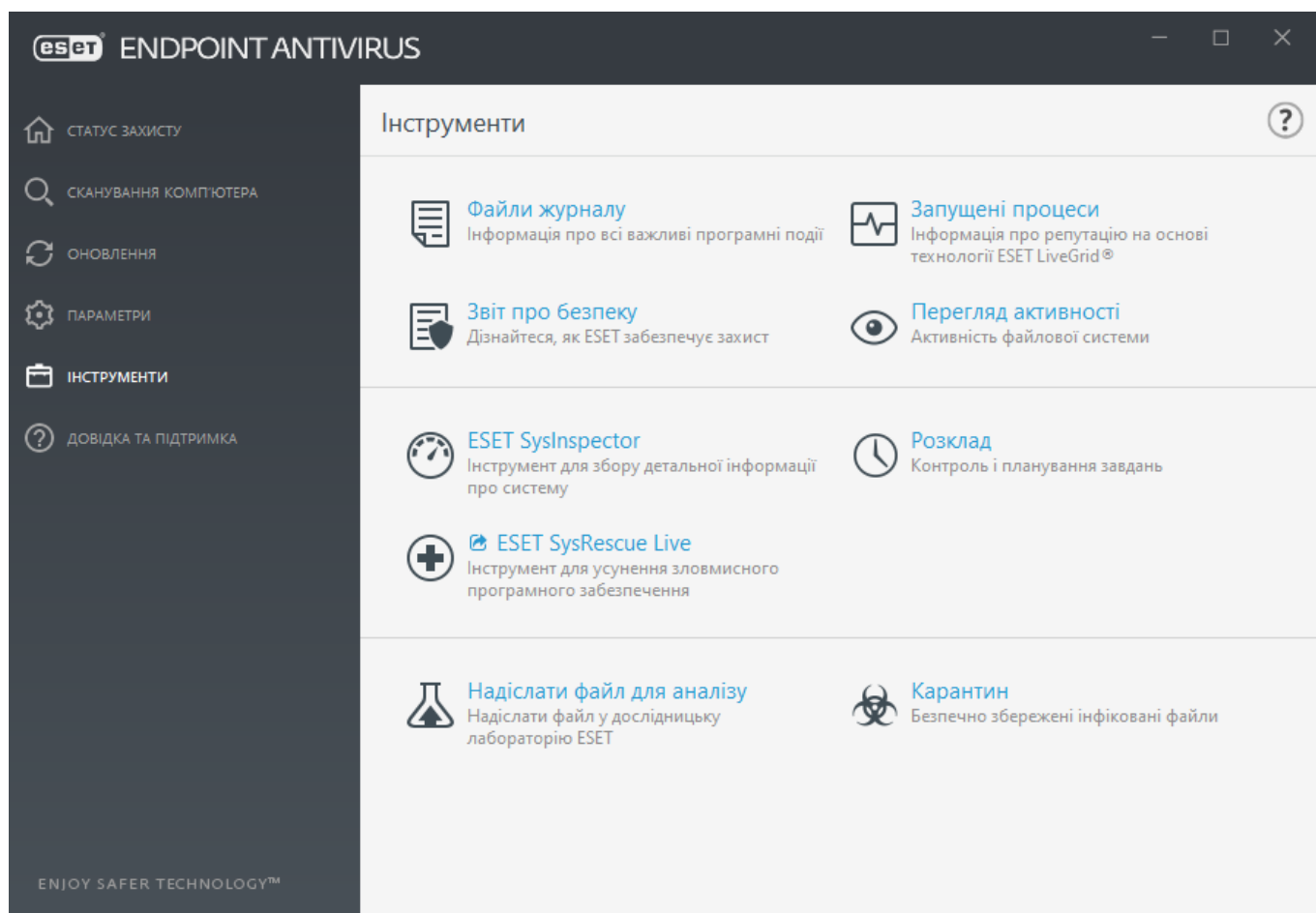
конфігурацією. Докладніше про створення й налаштування завдань оновлення див. у розділі [Планувальник](#).

Інструменти

У меню **Інструменти** представлено ряд модулів, які допомагають спростити адміністрування програми та надають додаткові можливості для досвідчених користувачів.

Цей розділ містить такі елементи:

- [Журнали](#)
- [Запущені процеси](#) (якщо ESET LiveGrid® увімкнено в програмі ESET Endpoint Antivirus)
- [Звіт про безпеку](#) (для некерованих робочих станцій)
- [ESET SysInspector](#)
- [Планувальник](#)
- [ESET SysRescue Live](#): виконує переспрямування на веб-сайт ESET SysRescue Live, де можна завантажити образ .iso для запису ESET SysRescue Live на диск CD/DVD.
- [Надіслати файл для аналізу](#) – дає змогу надсилати підозрілі файли на аналіз до дослідницької лабораторії ESET (доступність функції залежить від конфігурації ESET LiveGrid®).
- [Карантин](#)



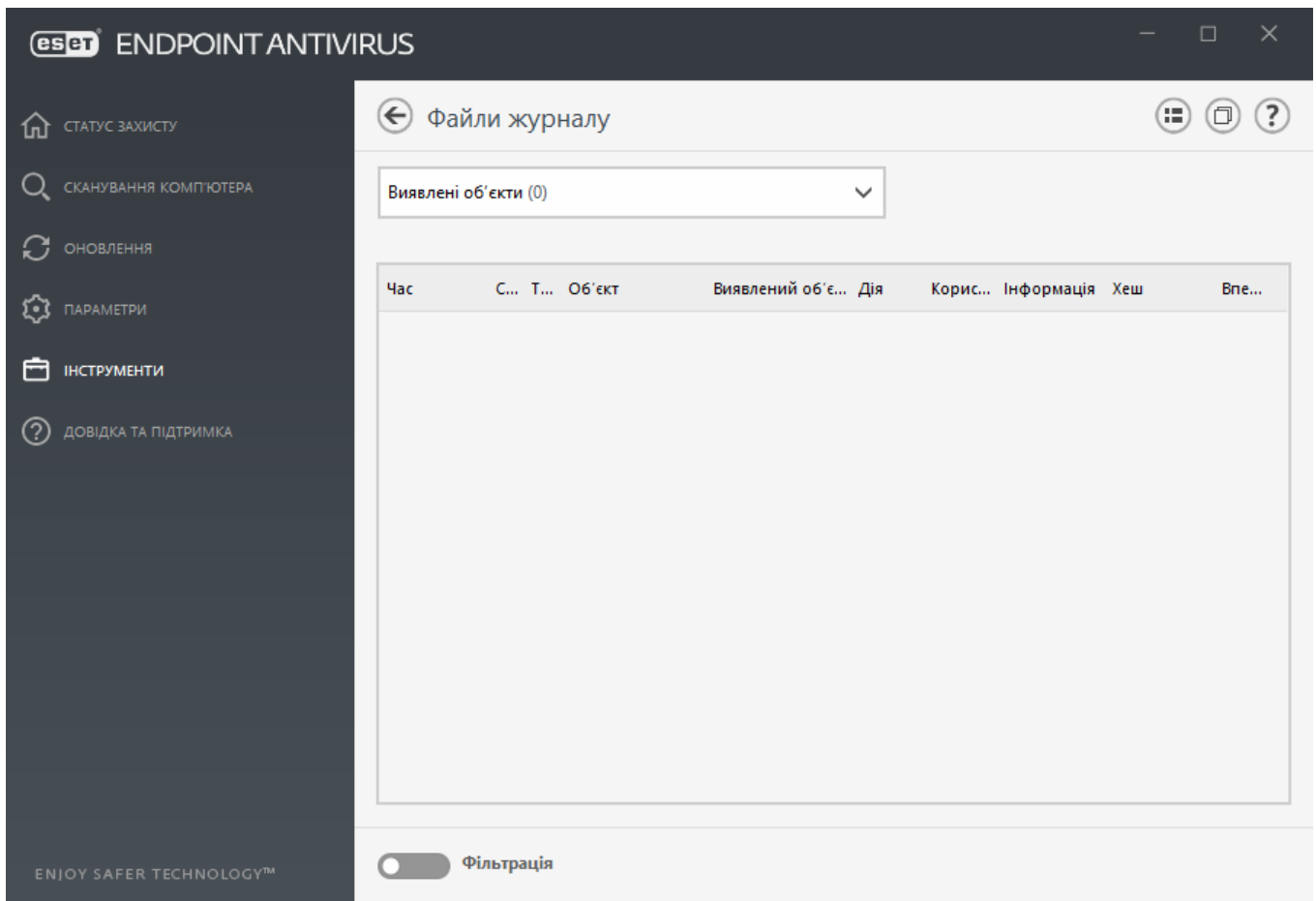
Журнали

Журнали містять інформацію про важливі програмні події та надають огляд виявлених загроз. Ведення журналу є важливим засобом системного аналізу, виявлення загроз і виправлення неполадок. Запис у журнал відбувається у фоновому режимі без втручання користувача. Інформація, яка може записуватися в журнал, залежить від поточних параметрів деталізації журналу. Текстові повідомлення й журнали можна переглядати безпосередньо в середовищі ESET Endpoint Antivirus. Також можна архівувати файли журналів.


Доступ до журналів можна отримати з головного вікна програми, натиснувши **Інструменти > Журнали**. Виберіть потрібний тип журналу в розкритому меню **Журнал**. Доступні такі журнали:

- **Виявлені об'єкти:** цей журнал містить детальну інформацію про інфіковані об'єкти й загрози, виявлені модулями ESET Endpoint Antivirus. У журналі міститься інформація про час виявлення, назву загрози, її розташування, виконану дію й ім'я користувача, який перебував у системі в момент виявлення загрози. Двічі натисніть будь-який запис журналу, щоб відобразити детальні відомості в окремому вікні. Загрози, які не вдалося очистити, завжди позначаються червоним текстом на яскраво-червоному фоні. Очищені загрози позначаються жовтим текстом на білому фоні. Потенційно небезпечні або небажані програми, які не очищено, позначаються жовтим текстом на білому фоні.
- **Події:** усі важливі дії, виконані ESET Endpoint Antivirus, записуються в журналі подій. Журнал містить інформацію про події та помилки, які сталися в програмі. Він призначений для системних адміністраторів і користувачів, яким потрібна допомога з вирішенням проблем. Часто інформація в ньому допомагає знайти вирішення проблеми, яка виникла під час роботи програми.
- **Перевірка комп'ютера:** усі результати сканування відображаються в цьому вікні. Кожний рядок відповідає одному скануванню комп'ютера. Двічі клацніть будь-який рядок, щоб переглянути докладну інформацію про відповідний сеанс сканування.
- **Заблоковані файли:** містять записи заблокованих файлів, які були недоступні для використання під час підключення до ESET Enterprise Inspector. Протокол указує причину блокування та модуль, який заблокував файл, а також програму й користувача, який запустив цей файл. Більш докладну інформацію див. в [онлайн посібнику користувача ESET Enterprise Inspector](#).
- **Надіслані файли:** містить записи файлів, надісланих у ESET LiveGrid® або [ESET LiveGuard](#) для аналізу.
- **Журнали аудиту:** кожний журнал містить інформацію про дату й час зміни, її тип, опис, джерело, а також про користувача, який уніс цю зміну. Більш докладні відомості див. в розділі [Журнали аудиту](#).
- **HIPS:** містить записи певних правил, позначених для запису. Протокол показує програму, яка викликала операцію, результат (правило було дозволено чи заборонено), а також ім'я створеного правила.
- **Захист мережі** – У журналі брандмауера відображаються всі віддалені атаки, виявлені модулем [Захист мережі від атак](#). У цьому журналі можна переглянути інформацію про всі атаки на комп'ютері. У стовпці Подія наводиться список виявлених атак. У стовпці Джерело надається детальніша інформація про зловмисника. У стовпці Протокол зазначається, який комунікаційний протокол використовувався для проведення атаки. Аналіз журналу брандмауера може допомогти вчасно виявити спроби проникнення в систему, а також попередити несанкціонований доступ. Щоб отримати додаткові відомості про певні мережні атаки, див. [IDS і додаткові параметри](#).

- **Відфільтровані веб-сайти:** список веб-сайтів, заблокованих модулем [захисту доступу до Інтернету](#). У журналах містяться дані про час, URL-адресу, користувача та програму, пов'язані з переходом на окремий сайт.
- **Контроль пристроїв:** містить записи про змінні носії та пристрої, підключені до комп'ютера. У файлі журналу реєструються ті пристрої, для яких створено правило контролю. Якщо правило не відповідає підключеному пристрою, запис у журналі для підключеного пристрою не створюватиметься. У цьому ж журналі можна переглянути відомості про тип пристрою, серійний номер, ім'я постачальника та розмір носія (якщо доступно).



Виберіть вміст будь-якого журналу й натисніть комбінацію клавіш **Ctrl + C**, щоб скопіювати його в буфер обміну. Натисніть та утримуйте **Ctrl + Shift**, щоб вибрати кілька записів.


Натисніть елемент  **Фільтрація**, щоб відкрити вікно [Фільтрація журналу](#), де можна визначати критерії фільтрації.

Клацніть певний запис правою кнопкою миші, щоб відкрити контекстне меню. У контекстному меню ви зможете отримати доступ до наведених нижче параметрів.

- **Показати:** показ додаткової інформації про вибраний журнал у новому вікні.
- **Відфільтровувати однакові записи:** після активації цього фільтра відображатимуться лише записи певного типу (діагностичні, попереджувальні тощо).
- **Фільтрувати:** після натискання цієї опції у вікні [Фільтрація журналу](#) можна визначати критерії фільтрації для певних записів журналу.
- **Увімкнути фільтр:** активація параметрів фільтра.
- **Вимкнути фільтр:** очищення всіх параметрів фільтра (як описано вище).

- **Копіювати/Копіювати все:** копіювання інформації про всі записи у вікні.
- **Видалити/Видалити все:** видалення вибраних або всіх відображуваних записів (для виконання цієї дії необхідні права адміністратора).
- **Експорт...:** експорт інформації про записи у форматі XML.
- **Експортувати все:** експорт інформації про всі записи у форматі XML.
- **Знайти/Знайти наступні/Знайти попередні:** після натискання цієї опції у вікні Фільтрація журналу можна визначати критерії фільтрації для пошуку певних записів.
- **Створити виключення:** дозволяє створити нове [виключення виявленого об'єкта з використанням майстра](#) (недоступно для виявленого шкідливого програмного забезпечення).

Фільтрація журналу

Натисніть  **Фільтрація** в розділі **Інструменти > Файли журналу**, щоб визначити критерії фільтрації.

Функція фільтрації журналів допоможе знайти потрібну інформацію. Особливо вона стане в нагоді, коли записів багато. Фільтрація дозволяє зменшити кількість відображуваних записів журналу, наприклад, для пошуку певних подій, станів або проміжків часу. Щоб відфільтрувати записи журналу, укажіть певні параметри пошуку. Після цього у вікні «Файли журналу» відображатимуться тільки записи, які відповідають параметрам пошуку.

Уведіть ключове слово для пошуку в поле **Знайти текст**. Щоб виокремити результати пошуку, скористайтеся розкритим меню **Знайти в стовпцях**. У розкритому меню **Типи журналів запису** виберіть один запис або кілька записів. Укажіть **проміжок часу**, за який потрібно відобразити результати. Можна також указати додаткові параметри пошуку, наприклад **Тільки слово повністю** або **З урахуванням реєстру**.

Знайти текст

Уведіть рядок (слово або частину слова). Відображатимуться тільки ті записи, які містять цей рядок. Інші записи будуть пропущені.

Знайти в стовпцях

Виберіть стовпці, які прийматимуться до уваги під час пошуку. Можна вибрати один стовпчик або кілька стовпчиків, які будуть використовуватися для пошуку.

Типи запису

У розкритому меню виберіть один або кілька типів записів журналу:

- **Діагностика:** запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи:** запис інформаційних повідомлень, включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження:** запис усіх критичних помилок і попереджувальних повідомлень.
- **Помилки:** запис таких помилок, як "Помилка під час завантаження файлу", і критичних помилок.
- **Критичні помилки:** запис лише критичних помилок (помилка запуску антивірусного захисту,

Проміжок часу

укажіть проміжок часу, за який потрібно відобразити результати.

- **Не вказано** (за замовчуванням): пошук буде здійснюватися по всьому журналу, а не тільки в межах певного проміжку часу.
- **Останній день**
- **Останній тиждень**
- **Останній місяць**
- **Проміжок часу**: можна вказати точний проміжок часу («Від»: і «До:») для фільтрації записів тільки в межах цього проміжку.

Тільки слово повністю

Це дозволяє отримати точніші результати пошуку за конкретними словами, уведеними повністю.

З урахуванням регістру

Увімкніть цей параметр, щоб під час фільтрації враховувалися верхній і нижній регістри літер. Після налаштування параметрів фільтрації/пошуку, натисніть кнопку **ОК**, щоб показати відфільтровані записи журналу, або кнопку **Знайти**, щоб розпочати пошук. Пошук у файлах журналу виконується згори вниз, починаючи з поточного місця (виділеного запису). Пошук зупиняється, коли буде знайдено перший відповідний запис. Для пошуку наступного запису натисніть клавішу **F3**. Щоб уточнити параметри пошуку, клацніть правою кнопкою миші й виберіть пункт **Знайти**.

Налаштування ведення журналу

Налаштувати параметри ведення журналу можна в головному вікні ESET Endpoint Antivirus. Натисніть **Параметри > Додаткові параметри > Інструменти > Журнали**. Розділ журналів використовується для налаштування параметрів керування журналами. Для економії місця на жорсткому диску програма автоматично видаляє найстаріші журнали. Для журналів можна налаштувати такі параметри:

Мінімальна детальність журналу: визначає, наскільки докладно описуватимуться події в журналі.

- **Діагностика** – запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи**: запис інформаційних повідомлень, включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження**: запис усіх критичних помилок і попереджувальних повідомлень.
- **Помилки**: запис таких помилок, як "Помилка під час завантаження файлу", і критичних помилок.
- **Критичні помилки**: запис лише критичних помилок (помилка запуску антивірусного захисту, тощо).



Якщо вибрати рівень детальності **діагностики**, система реєструватиме всі заблоковані підключення.

У полі **Автоматично видаляти записи, старіші за (дн.)** можна вказати термін зберігання записів журналу, після завершення якого вони видалятимуться автоматично.

Автоматично оптимізувати файли журналу: якщо цей параметр увімкнено, журнали автоматично дефрагментуються, коли відсоток фрагментації перевищує значення, вказане в полі **Якщо кількість записів, що не використовуються, перевищує (%)**.

Натисніть **Оптимізувати**, щоб запустити дефрагментацію файлів журналів. Усі пусті записи журналів видаляються, щоб підвищити продуктивність і швидкість обробки даних. Переваги такого вдосконалення особливо помітні, коли журнали містять велику кількість записів.

Параметр **Увімкнути текстовий протокол** дає змогу зберігати журнали у файлах іншого формату окремо від розділу [Журнали](#):

- **Цільовий каталог:** виберіть каталог, у якому зберігатимуться файли журналів (застосовується тільки до файлів TXT/CSV). Можна скопіювати шлях або вибрати інший каталог, натиснувши **Очистити**. Кожен розділ журналів містить окремий файл із попередньо визначеним іменем (наприклад, *virlog.txt* для розділу **Виявлені загрози**, якщо для збереження журналів використовується звичайний текстовий формат).
- **Тип:** якщо вибрати формат **Текст**, журнали зберігатимуться в текстовому файлі, а дані розділятимуться знаками табуляції. Те саме стосується формату **CSV** (файл із роздільниками-комами). Якщо вибрати параметр **Подія**, дані зберігатимуться в журналі подій Windows (їх можна переглянути за допомогою засобу перегляду подій на панелі керування), а не у файлі.
- **Видалити всі файли журналу:** видаляє всі збережені журнали, вибрані в розкритому меню **Тип** у цей момент. Відобразиться сповіщення про успішне видалення журналів.

Увімкнути відстеження змін конфігурації в журналі аудиту: містить інформацію про кожну зміну конфігурації. Більш докладну інформацію див. в розділі за посиланням [Журнали аудиту](#).

i Щоби прискорити вирішення деяких проблем, ESET може попросити вас надати копії журналів, збережених на комп'ютері. Інструмент ESET Log Collector полегшує збір потрібної інформації. Докладніше про ESET Log Collector можна прочитати у відповідній статті [бази знань ESET](#).

Журнали аудиту

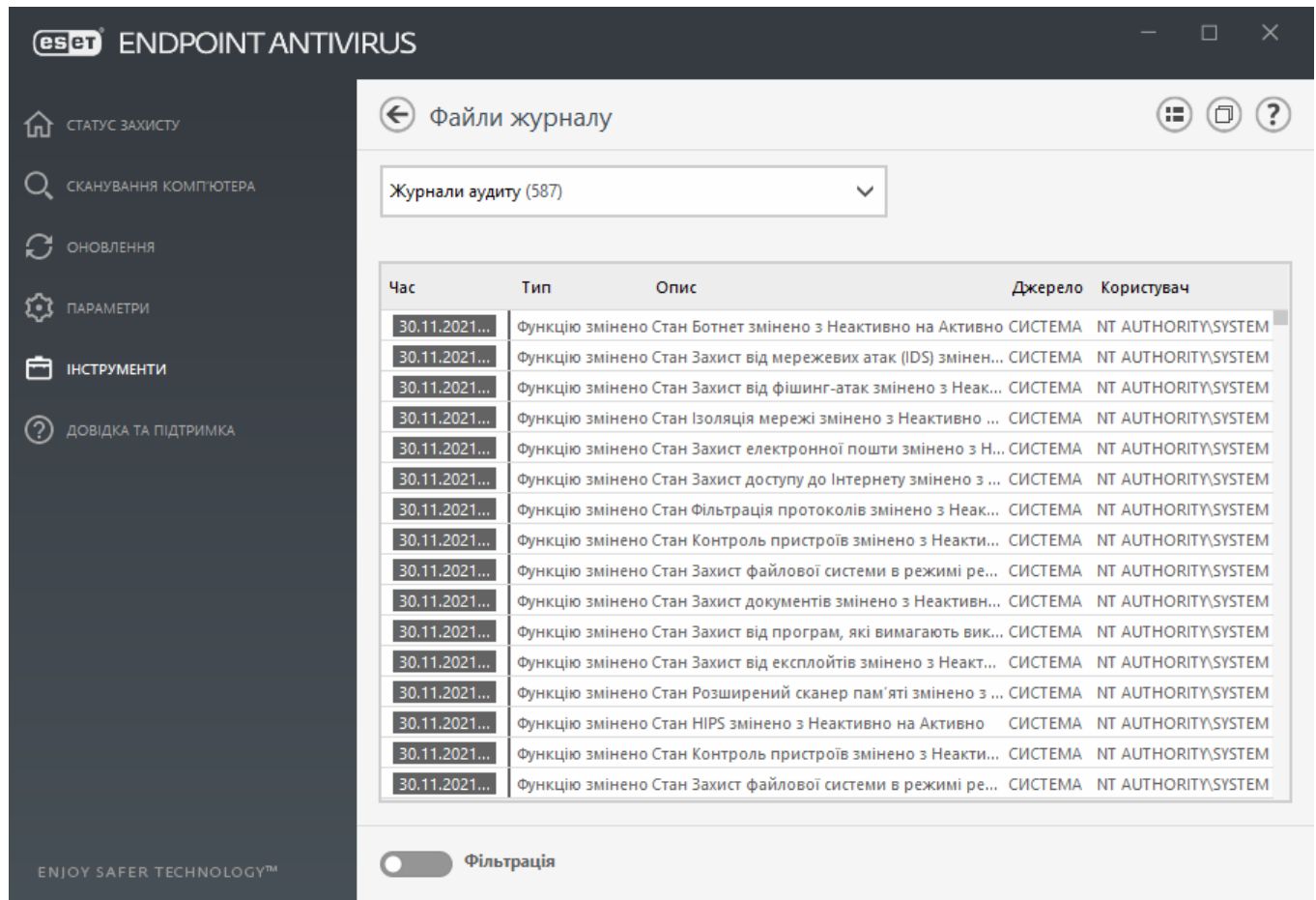
У корпоративному середовищі зазвичай певна кількість користувачів має права доступу до налаштування кінцевих точок. Оскільки внесення змін у конфігурацію продукту може істотно вплинути на його роботу, адміністраторам украй важливо мати змогу відстежувати зміни, які вносять користувачі, аби швидко ідентифікувати й усувати проблеми, а також запобігати виникненню таких або схожих проблем у майбутньому.

Журнал аудиту — це новий тип реєстрації подій у журналі, упроваджений у ESET Endpoint Antivirus версії 7.1, а також рішення для виявлення джерела проблем. Журнал аудиту дозволяє відстежувати зміни в конфігурації або стані захисту й записувати знімки для подальшого використання.

Щоб переглянути **Журнал аудиту**, у головному меню клацніть **Інструменти**, потім клацніть **Файли журналу** й у розкритому меню виберіть **Журнали аудиту**.

Журнал аудиту містить таку інформацію:

- Час: час унесення зміни.
- Тип: тип зміненого налаштування або функції.
- Опис: конкретний об'єкт, що зазнав змін, а також частина налаштувань, які було змінено. Окрім того, указано кількість змінених налаштувань.
- Джерело: вказує на джерело зміни.
- Користувач: користувач, який уніс зміну.



Щоб вивести докладні відомості про внесену зміну, у вікні "Файли журналу" виберіть потрібний тип журналу аудиту **Параметри змінено** й виберіть пункт **Показати зміни**. Окрім того, зміну налаштування можна скасувати. Для цього в контекстному меню виберіть пункт **Відновити** (недоступно для продукту під керуванням ESET PROTECT). Якщо в контекстному меню вибрати пункт **Видалити все**, буде створено журнал з інформацією про цю дію.

Якщо у вікні **Додаткові параметри > Інструменти > Файли журналу** ввімкнено параметр **Автоматично оптимізувати файли журналу**, журнали аудиту автоматично дефрагментуватимуться, як інші журнали.

Якщо у вікні **Додаткові параметри > Інструменти > Файли журналу** ввімкнено параметр **Автоматично видаляти записи, старіші за (дн.)**, автоматично видалятимуться записи журналу, старіші за період, вказаний у цьому полі.

Планувальник

інструмент "Розклад" керує запланованими завданнями та запускає їх із попередньо визначеною конфігурацією та заданими властивостями.

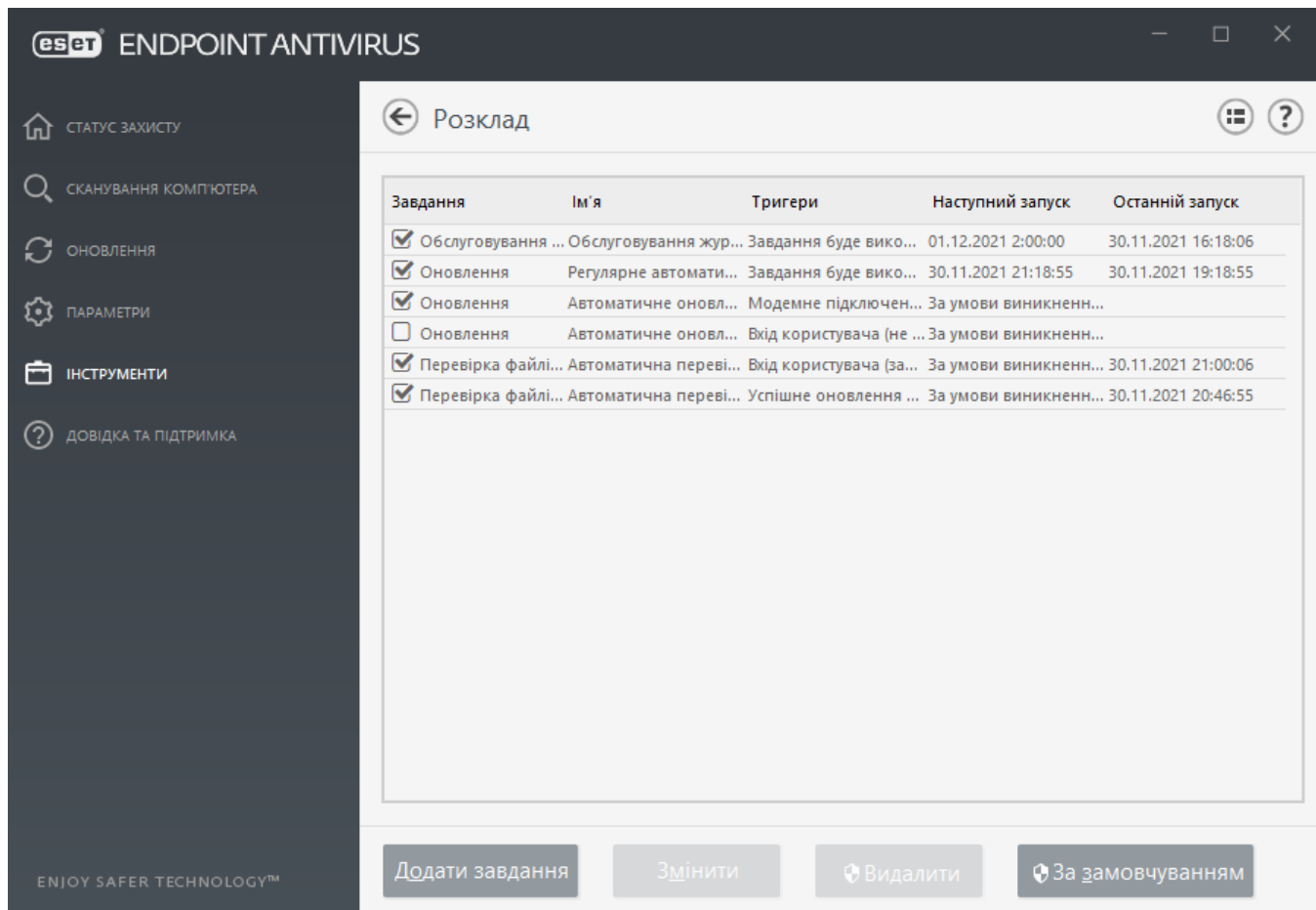
Щоб відкрити планувальник, у головному вікні програми ESET Endpoint Antivirus клацніть **Інструменти > Розклад**. У розділі **Розклад** міститься список усіх завдань і властивостей конфігурацій, зокрема такі параметри, як дата, час і профіль сканування.

Модуль завдань за розкладом використовується для планування таких завдань: оновлення обробника виявлення, сканування за розкладом, сканування файлів під час запуску системи й обслуговування журналів. Завдання можна додавати або видаляти безпосередньо з головного вікна планувальника (натисніть у нижній частині **Додати завдання** або **Видалити**). Клацніть правою кнопкою миші в будь-якій частині вікна, щоб виконати такі дії: відобразити детальну інформацію, виконати завдання негайно, додати нове завдання або видалити наявне. Використовуйте прапорці на початку кожного запису, щоб активувати або вимкнути завдання.

За замовчуванням у вікні **Розклад** відображаються такі завдання:

- **Обслуговування журналу**
- **Регулярне автоматичне оновлення**
- **Автоматичне оновлення після встановлення модемного підключення**
- **Автоматичне оновлення після входу користувача в систему**
- **Автоматична перевірка файлів під час запуску системи** (після входу користувача в систему)
- **Автоматична перевірка файлів під час запуску системи** (після успішного оновлення модулів)

Щоб змінити конфігурацію наявного запланованого завдання (як стандартного, так і користувацького), натисніть завдання правою кнопкою миші й виберіть команду **Змінити** або вкажіть потрібне завдання й натисніть кнопку **Змінити**.



Додавання нового завдання

- Натисніть **Додати завдання** в нижній частині вікна.
- Укажіть ім'я завдання.
- Виберіть потрібне завдання в розкритому меню:
 - **Запуск зовнішньої програми:** планування запуску зовнішньої програми.
 - **Обслуговування журналу** – окрім усього іншого, у журналах також містяться залишки видалених записів. Це завдання регулярно оптимізує записи в журналах для підвищення ефективності роботи.
 - **Перевірка файлів під час запуску системи:** перевірка файлів, що запускаються автоматично під час завантаження системи або входу до облікового запису.
 - **Створити знімок стану системи:** створення знімка системи засобом ESET SysInspector, який збирає докладну інформацію про системні компоненти (наприклад, драйвери, програми) й оцінює рівень ризику для кожного з них.
 - **Сканування комп'ютера за вимогою:** сканування файлів і папок на комп'ютері.
 - **Оновлення:** планування завдання оновлення, у рамках якого оновлюються обробник виявлення та модулі програми.
- Увімкніть перемикач **Увімкнено**, щоб активувати завдання (це можна зробити пізніше, установивши/знявши прапорець у списку запланованих завдань), натисніть **Далі** й виберіть один із часових параметрів:
 - **Один раз:** завдання буде виконано у визначений день і час.
 - **Багаторазово:** завдання буде виконуватися багаторазово через зазначений інтервал часу.
 - **Щодня:** завдання буде виконуватися багаторазово кожен день у визначений час.

- **Щотижня:** завдання буде виконуватись у вибраний день і час.
- **За умови виникнення події:** завдання буде виконано, якщо відбудеться зазначена подія.

5. **Виберіть Не запускати завдання, якщо комп'ютер працює від батареї**, щоб зменшити використання системних ресурсів, коли портативний комп'ютер працює від батареї. Завдання буде виконуватись у вибраний день і час відповідно до параметрів розділу **Запуск завдання**. Якщо завдання не вдалося запустити в заданий час, можна зазначити, коли його необхідно виконати наступного разу:

- **Під час наступного запланованого виконання**
- **Якомога швидше**
- **Негайно, якщо час з останнього запуску перевищує зазначений інтервал** (інтервал можна вибрати за допомогою поля прокрутки **Минуло часу з останнього запуску**)

Щоб переглянути інформацію про заплановане завдання, натисніть його правою кнопкою миші й виберіть **Показати деталі задачі**.

Огляд запланованого завдання
?

Назва завдання
Автоматичне оновлення після входу користувача в систему.
Тип завдання
Оновлення
Запуск завдання
Вхід користувача в систему (не частіше одного разу за година)
Дія в разі, якщо завдання не запущено в зазначений час
Під час наступного запланованого виконання

ОК

ESET SysInspector

[ESET SysInspector](#) — це програма, яка ретельно перевіряє комп'ютер і збирає докладну інформацію про такі системні компоненти, як драйвери та програми, мережеві підключення й важливі розділи реєстру. Крім того, вона оцінює рівень ризику для кожного компонента. Ця інформація може допомогти виявити причину підозрілого поведіння системи, яке може бути спричинено несумісністю програмного забезпечення або обладнання чи проникненням шкідливої вірусної програми. [Див. також онлайн-посібник користувача для ESET SysInspector.](#)

Вікно SysInspector містить таку інформацію про створені журнали:

- **Час:** час створення журналу.
- **Коментар:** короткий коментар.
- **Користувач:** ім'я користувача, який створив журнал.
- **Статус:** статус створення журналу.

Можливі такі дії:

- **Показати** – відкривання створеного журналу. Також відповідний файл журналу можна натиснути правою кнопкою миші й вибрати **Показати** в контекстному меню.
- **Створити**: створити новий журнал. Перш ніж відкривати журнал, дочекайтеся, поки ESET SysInspector завершить роботу (статус журналу зміниться на "**Створено**").
- **Видалити**: видалити вибрані журнали зі списку.

Для одного або кількох вибраних файлів журналу в контекстному меню доступні такі елементи:

- **Показати**: відкрити вибраний журнал в ESET SysInspector (аналогічно подвійному натисканню журналу).
- **Створити**: створити новий журнал. Перш ніж відкривати журнал, дочекайтеся, поки ESET SysInspector завершить роботу (статус журналу зміниться на "**Створено**").
- **Видалити**: видаляє вибраний журнал.
- **Видалити все**: видалити всі журнали.
- **Експорт**: експортувати файл у журнал .xml або стиснутий .xml.

Захист із використанням хмари

Технологію ESET LiveGrid® створено на основі системи завчасного попередження ThreatSense.Net. Вона збирає дані від користувачів ESET з усього світу й передає до дослідницької лабораторії ESET. Отримуючи підозрілі зразки та метадані від ESET LiveGrid®, ми можемо миттєво реагувати на потреби користувачів і своєчасно оновлювати системи ESET.

Доступні три варіанти (див. нижче).

Варіант 1. Увімкнути систему репутації ESET LiveGrid®

Система репутації ESET LiveGrid® дає змогу використовувати білі й чорні списки на основі хмарних технологій.

Перевіряйте репутацію [запущених процесів](#) і файлів безпосередньо з інтерфейсу програми чи контекстного меню. Додаткова інформація доступна завдяки технології ESET LiveGrid®.

Варіант 2. Увімкніть систему зворотного зв'язку ESET LiveGrid®

Доповнюючи систему репутації ESET LiveGrid®, система ESET LiveGrid® збиратиме пов'язану з нововиявленими загрозами інформацію про комп'ютер. Ця інформація може містити зразок або копію файлу, у якому виявлено загрозу, шлях до нього, його ім'я, інформацію про дату й час, відомості про процес, який викликав появу загрози на комп'ютері, а також дані про операційну систему комп'ютера.

За замовчуванням ESET Endpoint Antivirus налаштовано на передачу підозрілих файлів для детального аналізу до антивірусної лабораторії ESET. Файли з такими розширеннями, як .doc або .xls, завжди виключаються. До списку виключень можна додати й інші розширення файлів, які ви чи ваша організація не бажаєте відправляти.

Варіант 3. Не вмикати ESET LiveGrid®

Функціональні можливості програми обмежено не буде, але в деяких випадках продукт ESET Endpoint Antivirus швидше реагує на нові загрози, які ще не включено до обробника виявлення, коли технологію ESET LiveGrid® увімкнено.

i Більш докладну інформацію про ESET LiveGrid® див. в [глосарії](#).
У наших [ілюстрованих інструкціях](#), які доступні англійською та іншими мовами, наочно показано, як умикати або вимикати ESET LiveGrid® у ESET Endpoint Antivirus.

Конфігурація захисту з використанням хмари в додаткових параметрах

Щоб отримати доступ до налаштувань ESET LiveGrid®, натисніть **F5**. У меню "Додаткові параметри", що відкриється, розгорніть розділ **Ядро виявлення > Захист на основі хмари**.

Увімкнути систему репутації ESET LiveGrid® (рекомендується): система репутації ESET LiveGrid® підвищує ефективність рішень ESET для захисту від шкідливого ПЗ, порівнюючи проскановані файли з хмарною базою даних об'єктів, доданих до білих і чорних списків.

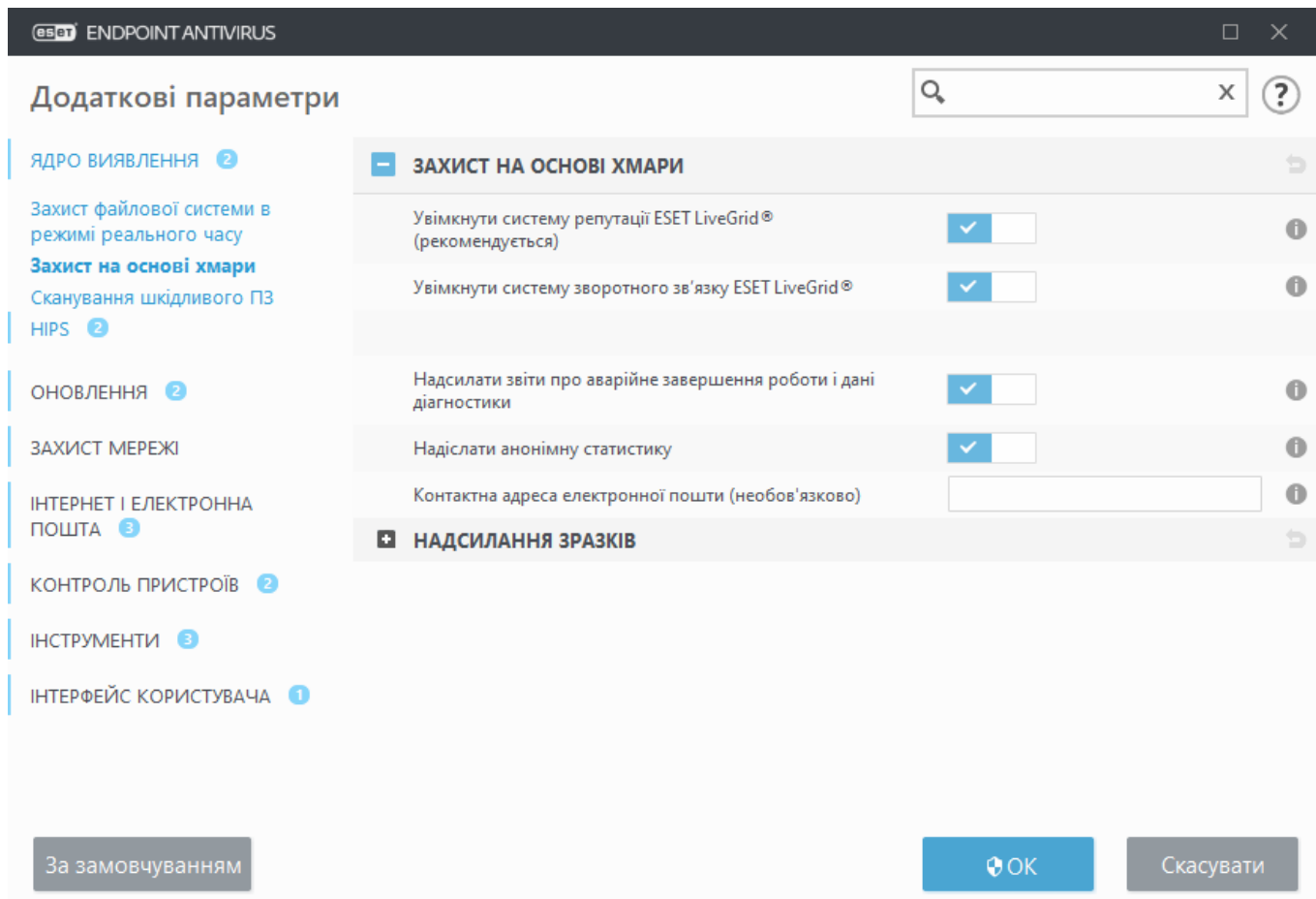
Увімкнути систему зворотного зв'язку ESET LiveGrid®: надсилає відповідні дані (описані в розділі **Надсилання зразків** нижче), а також звіти про аварійне завершення роботи й статистичні дані в дослідницьку лабораторію ESET для подальшого аналізу.

Увімкніть ESET LiveGuard (не відображається в ESET Endpoint Antivirus): ESET LiveGuard — це платна служба від ESET. Її призначення — додати рівень захисту, спеціально призначений для запобігання новим загрозам. Підозрілі файли автоматично передаються в хмару ESET. У хмарі вони аналізуються [вдосконаленими ядрами виявлення шкідливого програмного забезпечення](#). Користувач, який надав зразок, отримує звіт про поведінку зі зведеною інформацією про поведінку дослідженого зразка.

Надсилати звіти про аварійне завершення роботи й дані діагностики: надсилатимуться пов'язані з ESET LiveGrid® діагностичні дані, зокрема звіти про аварійне завершення й дампи пам'яті модулів. Рекомендуємо не вимикати цю функцію, щоб допомагати ESET покращувати продукти й захист кінцевих користувачів.

Надіслати анонімну статистику – дає змогу компанії ESET збирати інформацію про нові виявлені загрози, зокрема їхні імена, дати й час виявлення, методи виявлення та пов'язані метадані, версії та конфігурації продуктів із відомостями про систему.

Контактна адреса електронної пошти (необов'язково): ваша контактна адреса електронної пошти може відправлятися з будь-якими підозрілими файлами й використовуватися для зв'язку з вами, якщо для проведення аналізу знадобляться додаткові відомості. Зверніть увагу, що ви не отримаєте відповіді від ESET, якщо додаткова інформація не буде потрібна.



Надсилення зразків

Ручне надсилення зразків: дає змогу вручну надіслати зразки в ESET із контекстного меню, [карантину](#) або команди [Інструменти > Надіслати зразок для аналізу](#).

Автоматичне надсилення виявлених зразків

Виберіть типи зразків, які надсилатимуться до ESET для аналізу та покращення ефективності сканування в майбутньому. Доступні наведені нижче варіанти:

- **Усі виявлені зразки:** усі [об'єкти](#), виявлені [ядром виявлення](#) (включно з потенційно небажаними програмами, якщо увімкнено в налаштуваннях сканера).
- **Усі зразки, за винятком документів:** усі виявлені об'єкти, окрім **документів** (див. нижче).
- **Не відправляти:** виявлені об'єкти не надсилатимуться до ESET.

Автоматичне надсилення підозрілих зразків

Ці зразки також надсилатимуться в ESET, якщо ядро виявлення не розпізнає їх. Наприклад, зразки, яким майже вдалось уникнути виявлення або які видалися [модулям захисту](#) ESET Endpoint Antivirus підозрілими, зокрема, через свою незрозумілу поведінку.

- **Виконувані файли:** файли з розширенням .exe, .dll, .sys.
- **Архіви:** файли з розширенням .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Сценарії:** файли з розширенням .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Інше:** файли з розширенням .jar, .reg, .msi, .sfw, .lnk.
- **Повідомлення електронної пошти з підозрою на спам:** дає змогу надіслати

вірогідний або вкрай вірогідний спам для подальшого аналізу спеціалістами ESET. Увімкнення цього параметра дає змогу вдосконалити глобальне виявлення спаму зараз і в майбутньому.

- **Документи:** документи Microsoft Office або PDF з активним вмістом чи без нього.

☐ [Розгорніть список усіх охоплюваних типів документів](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Виключення

Фільтр виключень дає можливість запобігати відправленню для аналізу певних типів файлів або папок. Наприклад, доцільно виключити файли, які можуть містити конфіденційну інформацію (документи, електронні таблиці тощо). Указані файли ніколи не надсилатимуться на аналіз до лабораторії ESET, навіть якщо вони містять підозрілий код. Найпоширеніші типи файлів виключено за замовчуванням (.doc тощо). За потреби можна доповнити список виключених файлів.

✓ Щоб виключити файли, завантажені з download.domain.com, перейдіть у меню **Додаткові параметри > Захист на основі хмари > Надсилання зразків > Виключення** та додайте виключення *download.domain.com*.

ESET LiveGuard

Інструкції з увімкнення служби ESET LiveGuard на клієнтській машині з ESET PROTECT Web Console див. у темі за посиланням [Налаштування ESET LiveGuard для ESET Endpoint Antivirus](#).

Якщо ви раніше використовували систему ESET LiveGrid®, а потім вимкнули її, на комп'ютері ще можуть залишатися пакети даних, підготовлені до надсилання. Навіть після вимкнення системи завчасного попередження ці пакети будуть надіслані до ESET. Після відправлення всієї поточної інформації пакети не створюватимуться.

Фільтр виключень для хмарного захисту

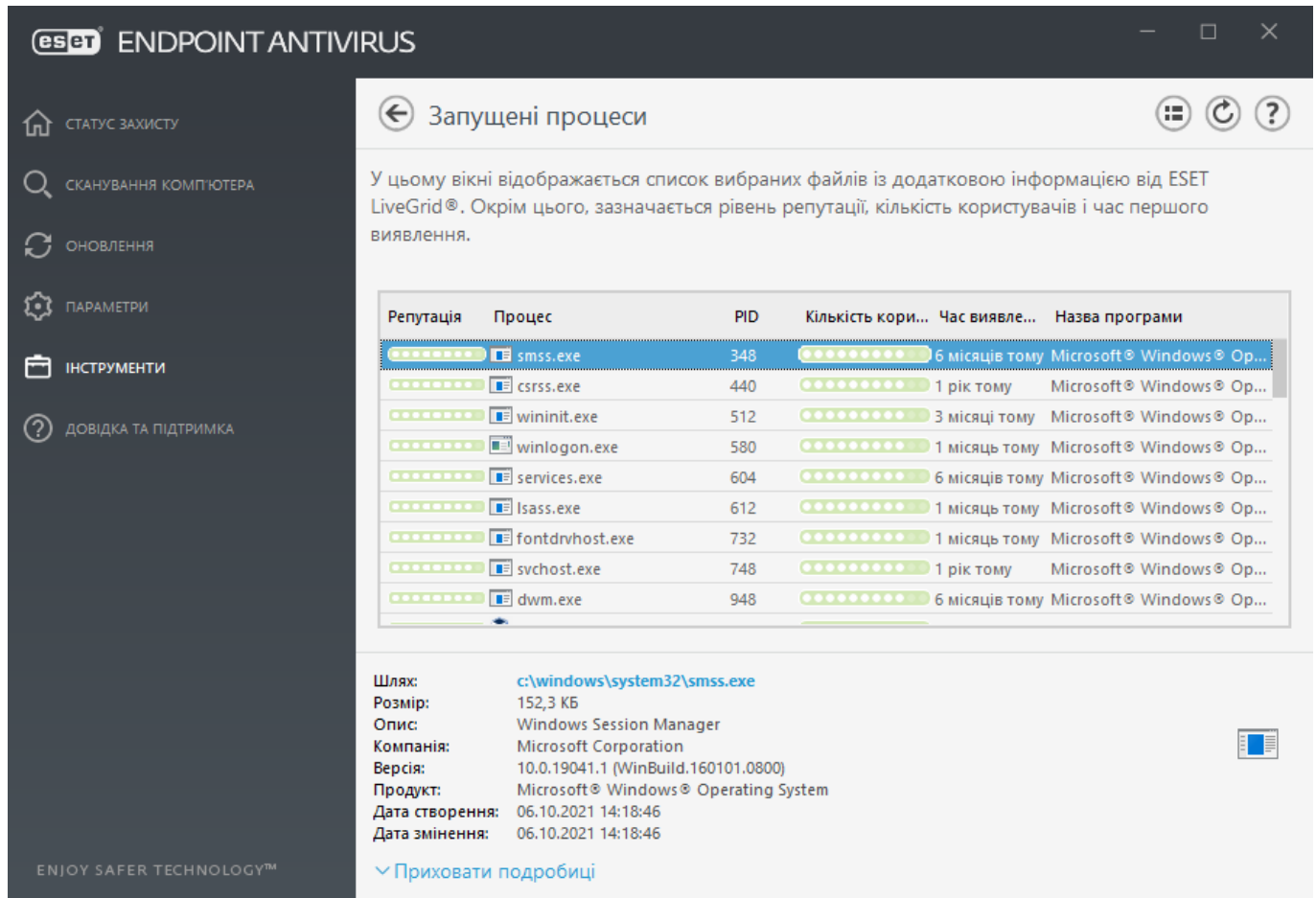
Фільтр виключень дає можливість не відправляти для аналізу певні файли або папки. Указані файли ніколи не надсилатимуться на аналіз до лабораторії ESET, навіть якщо вони містять підозрілий код. Найпоширеніші типи файлів виключено за замовчуванням (.doc тощо).

i Доцільно виключити файли, які можуть містити конфіденційну інформацію (документи, електронні таблиці тощо).

✓ Щоб виключити файли, завантажені з download.domain.com, перейдіть у меню **Додаткові параметри > Захист на основі хмари > Надсилання зразків > Виключення** та додайте виключення *download.domain.com*.

Запущені процеси

Модуль стеження за запущеними процесами відображає інформацію про програми або процеси на комп'ютері та є засобом негайного й постійного інформування ESET про нові загрози. ESET Endpoint Antivirus надає детальну інформацію про запущені процеси, захищаючи користувачів за допомогою активної технології [ESET LiveGrid®](#).



Запущені процеси

У цьому вікні відображається список вибраних файлів із додатковою інформацією від ESET LiveGrid®. Окрім цього, зазначається рівень репутації, кількість користувачів і час першого виявлення.

Репутація	Процес	PID	Кількість кори...	Час виявле...	Назва програми
●●●●●●	smss.exe	348	●●●●●●	6 місяців тому	Microsoft® Windows® Оп...
●●●●●●	csrss.exe	440	●●●●●●	1 рік тому	Microsoft® Windows® Оп...
●●●●●●	wininit.exe	512	●●●●●●	3 місяці тому	Microsoft® Windows® Оп...
●●●●●●	winlogon.exe	580	●●●●●●	1 місяць тому	Microsoft® Windows® Оп...
●●●●●●	services.exe	604	●●●●●●	6 місяців тому	Microsoft® Windows® Оп...
●●●●●●	lsass.exe	612	●●●●●●	1 місяць тому	Microsoft® Windows® Оп...
●●●●●●	fontdrvhost.exe	732	●●●●●●	1 місяць тому	Microsoft® Windows® Оп...
●●●●●●	svchost.exe	748	●●●●●●	1 рік тому	Microsoft® Windows® Оп...
●●●●●●	dwm.exe	948	●●●●●●	6 місяців тому	Microsoft® Windows® Оп...

Шлях: c:\windows\system32\smss.exe
Розмір: 152,3 КБ
Опис: Windows Session Manager
Компанія: Microsoft Corporation
Версія: 10.0.19041.1 (WinBuild.160101.0800)
Продукт: Microsoft® Windows® Operating System
Дата створення: 06.10.2021 14:18:46
Дата змінення: 06.10.2021 14:18:46

✓ Приховати подробиці

Репутація: у більшості випадків ESET Endpoint Antivirus і технологія ESET LiveGrid® призначають рівні ризику об'єктам (файлам, процесам, розділам реєстру тощо), використовуючи ряд евристичних правил, за якими досліджуються характеристики кожного об'єкта й потім визначається потенціал шкідливої активності. На основі цієї евристики об'єктам призначається певний рівень репутації: від 9 — найкраща репутація (зелений) до 0 — найгірша репутація (червоний).

Процес – ім'я процесу або програми, запущеної на комп'ютері. Усі запущені процеси доступні для перегляду також у диспетчері завдань Windows. Диспетчер завдань можна відкрити, клацнувши правою кнопкою миші пусту область на панелі завдань і вибравши пункт "Диспетчер завдань" або натиснувши сполучення клавіш **Ctrl+Shift+Esc** на клавіатурі.

PID: ідентифікатор процесу, запущеного в середовищі операційної системи Windows.

i Програми з позначкою зелений без сумніву безпечні (зазначені в білому списку) і не скануватимуться. Це допоможе пришвидшити процес перевірки комп'ютера за вимогою або роботу модуля захисту файлової системи в режимі реального часу.

Кількість користувачів: кількість користувачів, які працюють із певною програмою. Збір цієї інформації виконує технологія ESET LiveGrid®.

Час виявлення: час, коли програму було виявлено технологією ESET LiveGrid®.

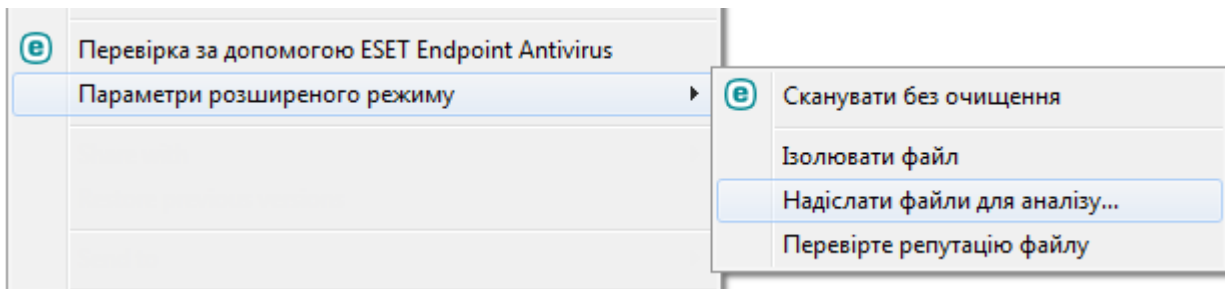
i Якщо програму позначено рівнем Невідомі (оранжевий), вона необов'язково шкідлива. Зазвичай таку позначку отримують нові програми. Якщо ви не впевнені, чи шкідливий певний файл, можна [відправити його на аналіз](#) до антивірусної лабораторії ESET. Якщо буде визначено, що цей файл – шкідлива програма, засоби для його виявлення буде додано до одного з наступних оновлень обробника виявлення.

Назва програми: ім'я, присвоєне програмі або процесу.

Якщо вибрати одну із програм у нижній частині екрана, внизу вікна відобразиться наведена нижче інформація.

- **Шлях:** розміщення програми на комп'ютері.
- **Розмір:** розмір файлу в кілобайтах (КБ) або мегабайтах (МБ).
- **Опис:** характеристики файлу на основі його опису операційною системою.
- **Компанія:** ім'я постачальника або прикладного процесу.
- **Версія:** інформація від видавця програми.
- **Продукт:** ім'я програми та/або фірмове найменування.
- **Дата створення:** дата й час створення програми.
- **Дата змінення:** дата й час останньої зміни програми.

i Перевірку репутації також можна виконати для файлів, які не належать до категорії запущених програм/процесів. Для цього позначте файли, які потрібно перевірити, натисніть їх правою кнопкою миші й у [контекстному меню](#) виберіть **Додаткові параметри > Перевірити репутацію файлу за допомогою ESET LiveGrid®**.



Звіт про безпеку

Ця функція забезпечує короткий огляд статистичних даних для наведених нижче категорій.

Заблоковані веб-сторінки: відображає кількість заблокованих веб-сторінок (URL-адресу вказано в чорному списку потенційно небажаних програм, фішингових веб-сайтів, зламаних маршрутизаторів, небезпечних IP-адрес або ненадійних сертифікатів).

Інфіковані об'єкти, виявлені в електронній пошті: відображає кількість таких [об'єктів](#).

Виявлені потенційно небажані програми: відображає кількість [потенційно небажаних програм](#).

Перевірені документи: відображає кількість таких документів.


Перевірені програми: відображає кількість просканиваних виконуваних об'єктів.

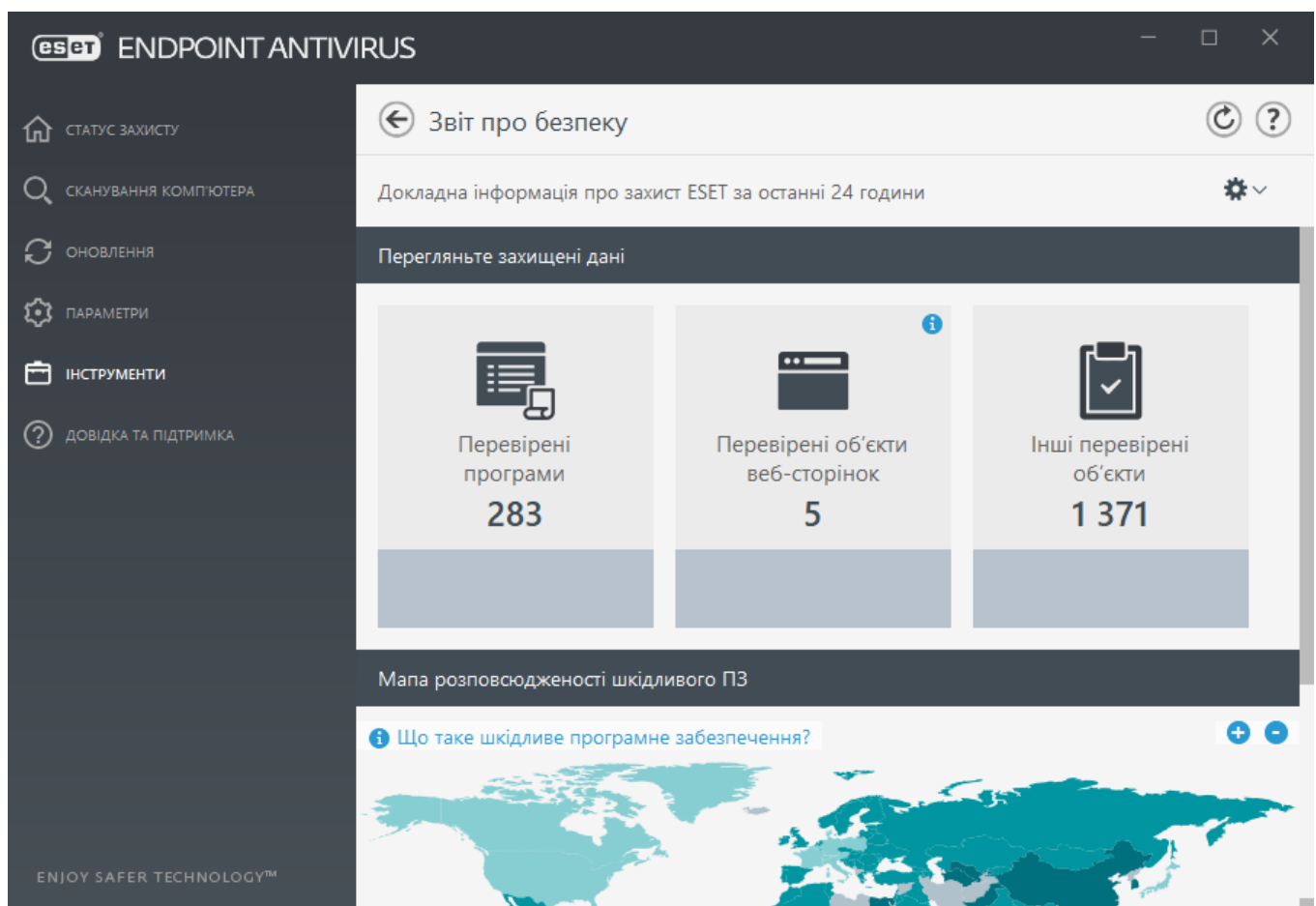
Інші перевірені об'єкти: відображає кількість таких об'єктів.

Перевірені об'єкти веб-сторінок: відображає кількість перевірених об'єктів веб-сторінок.

Перевірені об'єкти електронних листів: відображає кількість таких об'єктів.

Порядок відображення цих категорій визначається їх числовим значенням (від найвищого до найнижчого). Категорії з нульовими значеннями не відображаються. Натисніть "**Розгорнути**", щоб відобразити приховані категорії.

Натисніть значок шестірні  у верхньому правому куті, щоб **увімкнути чи вимкнути сповіщення звіту про безпеку** або вибрати період, за який збиратимуться дані (за останні 30 днів або з моменту активації продукту). Якщо ESET Endpoint Antivirus інстальовано менше ніж 30 днів тому, можна вибрати лише ту кількість днів, яка минула з моменту інсталяції. За замовчуванням вибрано 30 днів.



Скинути дані: очищає всю статистику й видаляє наявні дані звіту про безпеку. Цю дію необхідно підтверджувати, якщо не знято прапорець **Запитувати перед скиданням даних статистики** в меню **Додаткові параметри > Сповіщення > Інтерактивні сповіщення > Повідомлення про підтвердження**.

ESET SysRescue Live

ESET SysRescue Live — це безкоштовна утиліта, яка дозволяє створити завантажувальний компакт-диск (DVD-диск) або USB-носіїв. Ви можете завантажити інфікований комп'ютер із компакт-диска, щоб просканувати його на наявність шкідливого програмного забезпечення й очистити інфіковані файли.

Головна перевага утиліти ESET SysRescue Live полягає в тому, що вона запускається незалежно від базової операційної системи, проте має прямий доступ до диска й усієї файлової системи. Це дає змогу видаляти загрози, які неможливо видалити за звичайних умов (наприклад, коли операційну систему запущено тощо).

- [Інтерактивна довідка ESET SysRescue Live](#)

Відправлення зразків на аналіз

Якщо ви виявили підозрілий файл на комп'ютері або підозрілий веб-сайт в Інтернеті, їх можна надіслати на аналіз у дослідницьку лабораторію компанії ESET (доступність функції залежить від конфігурації ESET LiveGrid®).

Не надсилайте зразок, якщо він не відповідає хоча б одному з наведених нижче критеріїв:

- Зразок взагалі не виявляється вашим продуктом ESET.
- Зразок неправильно визначається як загроза.
- Ми не приймаємо особисті файли, що надсилаються нам як зразки для сканування на наявність шкідливого програмного забезпечення (дослідницька лабораторія ESET не виконує сканування на вимогу для користувачів)
- Укажіть інформативну тему повідомлення, а також надайте якомога більше інформації про файл (наприклад, надайте знімок або вкажіть веб-сайт, з якого його завантажено)

Ви можете відправляти зразки файлів та сайтів у компанію ESET для аналізу, використовуючи один із наведених нижче методів.

1. Скористайтесь формою надсилання зразків: **Інструменти > Надіслати файл для аналізу**.
2. Файл також можна відправити електронною поштою. Якщо цей варіант зручніший для вас, додайте відповідні файли до архіву WinRAR/ZIP, установивши для нього пароль "infected", і надішліть на адресу samples@eset.com.
3. Повідомлення про спам або повідомлення, помилково розпізнані як спам, дотримуйтесь інструкцій, наведених у [цій статті бази знань ESET](#).

Коли ви відкрите вікно **Вибір зразка для аналізу**, у розкритому меню **Причини відправлення зразка** виберіть опис, який найкраще відповідає отриманому повідомленню:

- [Підозрілий файл](#)
- [Підозрілий сайт](#) (веб-сайт, інфікований будь-яким шкідливим ПЗ)
- [Помилковий результат файлу](#) (файли, неправильно розпізнані як інфіковані)
- [Сайт, заблокований помилково](#)
- [Інше](#)

Файл/сайт – шлях до файлу або веб-сайту, який потрібно відправити.

Контактна адреса електронної пошти – контактна адреса електронної пошти, яка відправляється до ESET разом із підозрілими файлами, і може використовуватися для зв'язку з вами, якщо для аналізу будуть потрібні додаткові відомості про надіслані файли. Додавати контактну адресу електронної пошти необов'язково. Щоб не вказувати її, виберіть **Надіслати анонімно**.

i Ви не отримаєте відповіді від ESET (окрім тих випадків, коли для аналізу будуть потрібні додаткові відомості від вас). Щодня на наші сервери надходять десятки тисяч файлів, тому ми не маємо можливості відповідати на всі повідомлення. Якщо буде визначено, що файл або веб-сайт шкідливий, ми додамо засоби для його виявлення до одного з наступних оновлень продукту ESET.

Вибір зразка для аналізу: підозрілий файл

Виявлені ознаки та симптоми зараження шкідливою програмою: введіть опис поведінки підозрілого файлу, виявленого на комп'ютері.

Походження файлу (URL-адреса чи постачальник): укажіть походження файлу (джерело) і те, яким чином його було знайдено.

Примітки й додаткова інформація: тут можна ввести додаткову інформацію чи опис, які допоможуть під час обробки або виявлення підозрілого файлу.

i Лише перший параметр (**Виявлені ознаки та симптоми зараження шкідливою програмою**) потрібно вказати обов'язково, але додаткова інформація значно допоможе співробітникам наших лабораторій у процесі ідентифікації зразків.

Вибір зразка для аналізу: підозрілий сайт

Виберіть один із наведених нижче елементів розкривного меню **Проблема із сайтом**.

- **Інфікований:** веб-сайт, що містить віруси або інше шкідливе ПЗ, поширюване різними способами.
- **Фішинговий:** часто використовується для отримання доступу до конфіденційних даних (PIN-кодів, номерів банківських рахунків тощо). Докладніше про цей тип атаки див. у [глосарії](#).
- **Шахрайський:** оманливий або зловмисний веб-сайт, часто створюваний із метою отримання швидкого прибутку.
- Виберіть **Інше**, якщо жоден із наведених вище варіантів не відповідає вашому випадку.

Примітки й додаткова інформація: тут можна ввести додаткову інформацію чи опис, які можуть бути корисними під час аналізу підозрілого веб-сайту.

Вибір зразка для аналізу: помилково

розпізнаний файл

Якщо файл помилково визначено як інфікований, надішліть його нам. Це допоможе покращити роботу модулів захисту від вірусів і шпигунських програм, а також посилити безпеку інших користувачів. Помилкові результати можуть виникати, коли шаблон файлу збігається із шаблоном, збереженим в обробнику виявлення.

Назва й версія програми: назва програми та її версія (наприклад, номер або альтернативна чи кодова назва).

Походження файлу (URL-адреса чи постачальник): укажіть походження файлу (джерело) і те, яким чином його було знайдено.

Призначення програми: загальний опис програми, її тип (наприклад, веб-браузер, медіапрогравач тощо) і функції.

Примітки й додаткова інформація: тут можна вказати додаткову інформацію або опис, які допоможуть під час обробки підозрілого файлу.

i Перші три параметри необхідні для того, щоб виявити легальні програми й відрізнити їх від шкідливого коду. Надання додаткової інформації значно допоможе працівникам наших лабораторій під час ідентифікації й обробки зразків.

Вибір зразка для аналізу: помилково розпізнаний сайт

Якщо сайт помилково визначено як інфікований, шахрайський або фішинговий, повідомте про це нам. Помилкові результати можуть виникати, коли шаблон файлу збігається із шаблоном, збереженим в обробнику виявлення. Повідомляйте нам про такі випадки, щоб ми могли покращити роботу модулів захисту від вірусів і фішинг-атак, а також посилити захист інших користувачів.

Примітки й додаткова інформація: тут можна вказати додаткову інформацію або опис, які допоможуть під час обробки підозрілого веб-сайту.

Вибір зразка для аналізу: інше

Використовуйте цю форму, якщо файл не можна віднести до категорії **Підозрілий файл** або **Помилковий результат**.

Причина відправлення файлу: введіть детальний опис файлу й причину його відправлення.

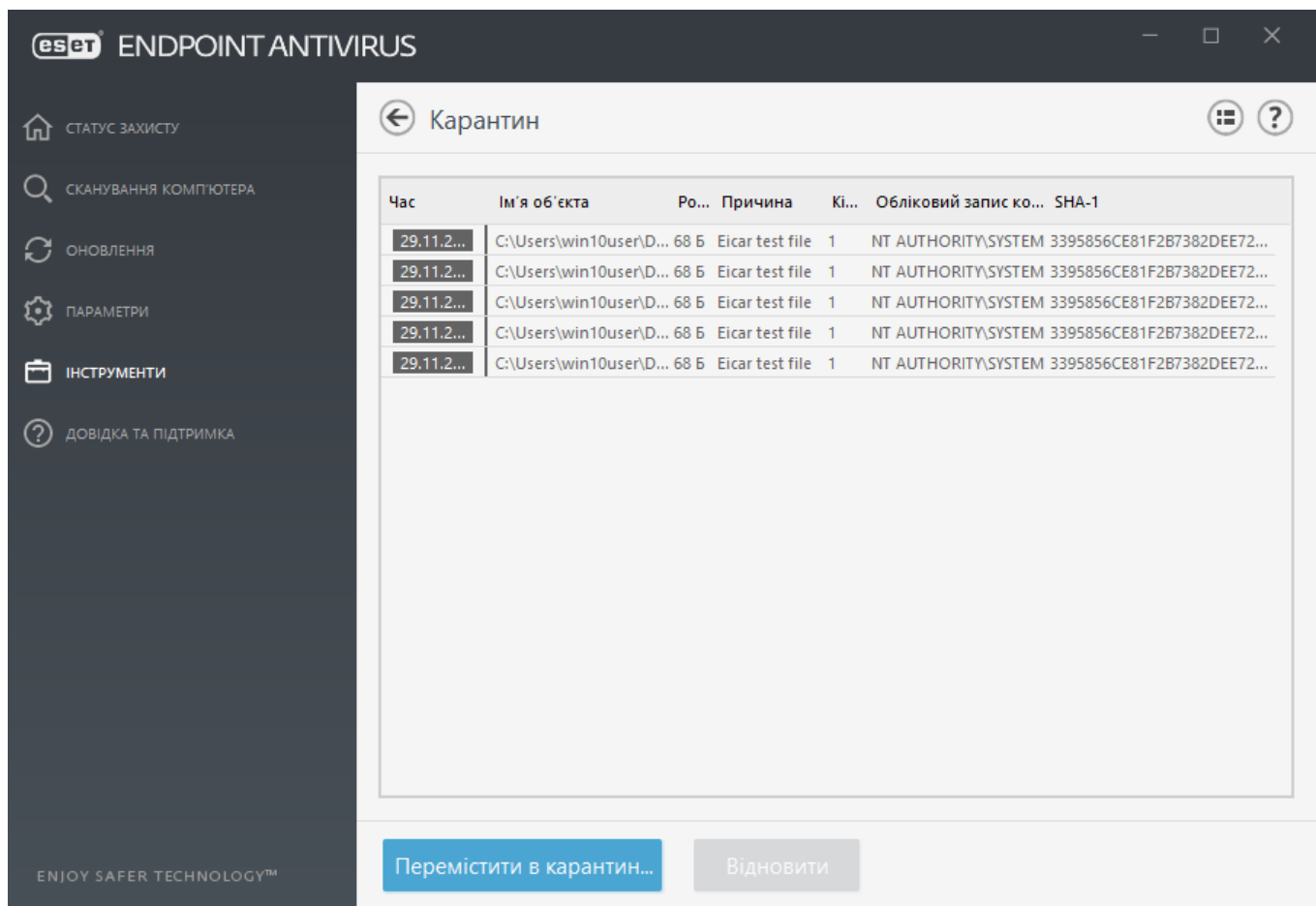
Карантин

Основна функція карантину — безпечно ізолювати виявлені об'єкти (наприклад, шкідливе програмне забезпечення, інфіковані файли або потенційно небажані програми).

Щоб відкрити карантин, у головному вікні програми ESET Endpoint Antivirus натисніть **Інструменти > Карантин**.

Файли, які зберігаються в папці карантину, можна переглядати в таблиці, де вказано:

- дату й час переміщення в карантин;
 - шлях до вихідного місця розташування інфікованого файлу;
 - розмір у байтах;
 - причину (наприклад, об'єкт додано користувачем);
 - кількість виявлених об'єктів (наприклад, багаторазове виявлення одного файлу, або якщо це архів із кількома загрозами).
- [Я віддалено керую карантинном на клієнтських робочих станціях](#)



Карантинування файлів

ESET Endpoint Antivirus автоматично переміщує в карантин видалені файли (якщо ви не скасували цю опцію у [вікні тривоги](#)).

Додаткові файли можна перемістити в карантин, якщо:

- їх не вдається очистити;
- вони небезпечні або їх рекомендується видалити;
- їх випадково виявлено програмою ESET Endpoint Antivirus;
- файл поводить себе підозріло, але його не виявляє [сканер](#).

Перемістити файл у карантин можна кількома способами.

- a. за допомогою перетягування – для цього вручну натисніть файл і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку, щоб програма перемістилася на передній план. Щоб просканувати файл або папку вручну, натисніть відповідний елемент і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку. після цього програма переміститься на передній план.
- b. У головному вікні програми натисніть **Перемістити в карантин**.
- c. Це також можна зробити за допомогою контекстного меню: натисніть правою кнопкою миші у вікні **Карантин** і виберіть **Карантин**.

Відновлення з карантину

Файли з карантину також можна відновити й повернути до початкових місць розташування.

- Для цього натисніть правою кнопкою файл у карантині та виберіть опцію **Відновити** в контекстному меню.
- Якщо файл позначено як [потенційно небажану програму](#), доступна опція **Відновити та виключити з перевірки**. Також див. [Виключення](#).
- У контекстному меню також доступна опція **Відновити в**, за допомогою якої користувач може відновити файли в інше місце, а не туди, звідки їх було видалено.
- У деяких випадках функція відновлення недоступна, наприклад, якщо файли знаходилися на мережевому диску, доступному лише для читання.

Видалення з карантину

Натисніть правою кнопкою миші відповідний елемент і виберіть **Видалити з карантину** або виберіть потрібний елемент і натисніть клавішу **Delete** на клавіатурі. Окрім того, можна виділяти й видаляти кілька елементів одночасно. Видалені елементи остаточно видаляються з вашого пристрою й карантину.

Відправка на аналіз файлів із карантину

Якщо ви помістили в карантин підозрілий файл, який програма не виявила, або файл помилково розпізнано як інфікований (наприклад, під час евристичного аналізу коду) і переміщено в карантин, [надішліть файл до дослідницької лабораторії ESET](#). Щоб відправити файл, клацніть його правою кнопкою миші та виберіть **Відправити на аналіз** у контекстному меню.

i Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Керувати карантинном у ESET PROTECT](#)
- [Продукт ESET повідомив про підозрілий об'єкт. Що робити?](#)

Параметри проксі-сервера

У великих локальних мережах проксі-сервер може керувати підключенням комп'ютерів до Інтернету. У такому випадку потрібно визначити наведені нижче параметри. Інакше програма не зможе автоматично оновлюватися. У програмі ESET Endpoint Antivirus параметри проксі-сервера доступні у двох розділах дерева додаткових параметрів.

По-перше, параметри проксі-сервера можна вказати в розділі **Додаткові параметри** меню

Інструменти > Проксі-сервер. Указані на цьому рівні параметри визначають загальні налаштування проксі-сервера для всіх функцій ESET Endpoint Antivirus. Визначені тут параметри використовуватимуться всіма модулями, які вимагають підключення до Інтернету.

Щоб визначити параметри проксі-сервера на цьому рівні, установіть прапорець **Використовувати проксі-сервер**, після чого введіть його адресу в полі **Проксі-сервер** і номер порту в полі **Порт**.

Якщо підключення за допомогою проксі-сервера вимагає автентифікації, установіть прапорець **Проксі-сервер потребує автентифікації** та введіть дійсні дані в полях **Ім'я користувача** й **Пароль**. Клацніть **Виявити проксі-сервер**, щоб налаштування проксі-сервера виявлялись і застосовувались автоматично. Будуть скопійовані параметри, указані для вашої операційної системи. Щоб знайти налаштування проксі-сервера в операційній системі, натисніть сполучення клавіш **Windows + I** і виберіть пункти **Мережі та Інтернет > Проксі-сервер**.

i Ім'я користувача й пароль потрібно вручну вказати в налаштуваннях **проксі-сервера**.

Використовувати пряме підключення, якщо проксі-сервер недоступний: якщо ESET Endpoint Antivirus настроєний на використання проксі-сервера, але той недоступний, то продукт ESET Endpoint Antivirus виконає обхід проксі-сервера й установить зв'язок безпосередньо із серверами ESET.

Параметри проксі-сервера також можна визначити в розділі додаткових параметрів оновлення (у розділі **Додаткові параметри > Оновлення > Профілі > Оновлення > Параметри підключення** виберіть елемент **Підключення через проксі-сервер** із розкритого меню **Режим проксі-сервера**). Ці налаштування застосовуються до відповідного профілю оновлення. Їх рекомендується вказувати на портативних комп'ютерах, які часто отримують оновлення ядра виявлення з віддалених місць розташування. Докладніше про ці налаштування можна прочитати в розділі [Додаткові параметри оновлення](#).

Додаткові параметри

x

?

АНТИВІРУС 1
Оновлення 4
Інтернет і електронна пошта 4
Контроль пристроїв 2
Інструменти 2
Журнали
Проксі-сервер 1
Сповіщення електронною поштою 3
Режим презентації
Діагностичні дані
Інтерфейс користувача

ПРОКСІ-СЕРВЕР

Використовувати проксі-сервер

✓

i

Проксі-сервер

i

Порт

3128

Проксі-сервер потребує автентифікації

✕

i

Ім'я користувача

i

Пароль

i

Виявити проксі-сервер

Виявити

Використовувати пряме підключення, якщо проксі-сервер недоступний

✓

За замовч.

OK

Скасувати

Часові проміжки

Можна створити часові проміжки, а потім призначити їх правилам **контролю пристроїв**. Параметр **Часові проміжки** можна знайти, вибравши пункти **Додаткові параметри** > **Інструменти**. Це дозволить визначити широко використовувані проміжки часу (наприклад, робочий час, вихідні тощо) і використовувати їх заново, не перевизначаючи час для кожного правила. Проміжок часу застосовується для будь-якого підходящого типу правила, для якого підтримується керування за часовими параметрами.

Часові проміжки ?

Ім'я

Опис

Work time	Weekdays 8:00-17:00
Off-work	Evenings & weekends

Додати

Редагувати

Видалити

ОК

Скасувати

Щоб створити часовий проміжок, виконайте такі кроки:

1. Послідовно виберіть пункти **Змінити** > **Додати**.
2. Введіть ім'я та **опис** часового проміжку й клацніть **Додати**.
3. Вкажіть день і час початку/закінчення для проміжку часу або виберіть **Весь день**.
4. Натисніть кнопку **ОК** для підтвердження.

Одиничний проміжок часу можна визначити одним або кількома діапазонами часу на основі днів та часу. Коли проміжок буде створено, він з'явиться в розкритому меню **Застосовувати протягом** вікна [Редактор правил контролю пристроїв](#).

Оновлення Microsoft Windows

Служба Windows Update – важливий компонент захисту користувачів від шкідливого програмного забезпечення. Тому критично необхідно інсталиувати оновлення Microsoft Windows одразу ж, як вони стають доступними. ESET Endpoint Antivirus повідомляє про відсутні оновлення відповідно до рівня, встановленого користувачем. Для вибору доступні наведені нижче рівні.

- **Жодних оновлень:** жодні оновлення системи не пропонуватимуться для завантаження.
- **Необов'язкове оновлення:** для завантаження пропонуватимуться оновлення, позначені як низькопріоритетні, і важливіші.
- **Рекомендовані оновлення:** для завантаження пропонуватимуться оновлення, позначені як найпоширеніші, і такі, що мають пізнішу дату випуску.
- **Важливі оновлення:** для завантаження пропонуватимуться оновлення, позначені як важливіші, і такі, що мають пізнішу дату випуску.
- **Критичні оновлення:** для завантаження пропонуватимуться лише критичні оновлення.

Натисніть кнопку **ОК**, щоб зберегти зміни. Вікно "Оновлення системи" відкриється після перевірки стану на сервері оновлень. Відповідно, інформація про оновлення системи може бути доступна не відразу після збереження змін.

Перевірка періоду ліцензування

Для програми ESET Endpoint Antivirus необхідне автоматичне підключення до серверів ESET. Щоб змінити відповідне налаштування, відкрийте **Додаткові параметри (F5) > Інструменти > Ліцензія**. За замовчуванням для параметра **Перевірка інтервалу** вибрано значення **Автоматично**; сервер ліцензій ESET перевіряє продукт кілька разів на час. Щоб зменшити перевантаження під час підвищеної інтенсивності мережевого трафіку, змініть значення цього параметра на **Обмежено**. Якщо використовується значення **Обмежено**, ESET Endpoint Antivirus перевіряє ліцензійний сервер лише раз на день або під час перезапуску комп'ютера.



Якщо для параметра **Перевірка інтервалу** встановлено значення **Обмежено**, усі пов'язані з ліцензією зміни, унесені в ESET Business Account /ESET MSP Administrator, можуть застосовуватися до параметрів ESET Endpoint Antivirus через певний час (до одного дня).

Інтерфейс користувача

У розділі **Інтерфейс користувача** можна налаштувати графічний інтерфейс програми.

Використовуючи засіб [Елементи інтерфейсу користувача](#), можна змінити вигляд програми й використовувані візуальні ефекти.

Щоб гарантувати максимальну надійність системи безпеки, можна запобігти внесенню будь-яких несанкціонованих змін у її параметри за допомогою інструмента [Параметри доступу](#).

Параметри [Повідомлення про загрози та сповіщення](#) й [Сповіщення](#) дозволяють змінити повідомлення про виявлені загрози й системні сповіщення. Ці параметри можна налаштувати залежно від потреб.

Якщо відображення певних сповіщень скасовано, їх можна переглянути в розділі **Елементи інтерфейсу користувача > Статуси програм**. Тут можна переглянути їх статус або ж скасувати показ таких сповіщень.

Вікно [Інтеграція з контекстним меню](#) відображається, якщо натиснути вибраний об'єкт правою кнопкою миші. Використовуйте цей інструмент, щоб інтегрувати елементи керування ESET Endpoint Antivirus в контекстне меню.

[Режим презентації](#) рекомендовано для користувачів, які не бажають під час роботи з програмою бачити спливаючі вікна та сповіщення про заплановані завдання й не хочуть, щоб певні компоненти перезавантажували процесор або оперативну пам'ять.

Див. також [Згортання інтерфейсу користувача ESET Endpoint Antivirus](#) (стане в пригоді для керованих середовищ).

Елементи інтерфейсу користувача

Параметри конфігурації інтерфейсу користувача в програмі ESET Endpoint Antivirus дають можливість коригувати робоче середовище відповідно до своїх потреб. Доступ до цих параметрів конфігурації можна отримати в гілці **Інтерфейс користувача > Елементи інтерфейсу користувача** дерева додаткових параметрів ESET Endpoint Antivirus.

У розділі **Елементи інтерфейсу користувача** можна відкоригувати робоче середовище. Скористайтеся розкривним меню **Режим запуску**, щоб вибрати один із наведених нижче режимів запуску графічного інтерфейсу користувача.

Повний: графічний інтерфейс користувача відображатиметься повністю.

Мінімальний: графічний інтерфейс користувача виконується, але на екран виводяться лише сповіщення.

Уручну: графічний інтерфейс користувача не запускається автоматично під час входу в систему. Будь-який користувач може запустити його вручну.

Німий: сповіщення й повідомлення про загрози не відображатимуться. Графічний інтерфейс користувача може запустити тільки адміністратор. Цей режим корисно використовувати в керованих середовищах або у випадках, коли потрібно економно використовувати системні ресурси.

i Якщо вибрано мінімальний режим, після перезавантаження комп'ютера сповіщення відображатимуться, а графічний інтерфейс користувача – ні. Щоб відновити повнофункціональний режим графічного інтерфейсу, запустіть інтерфейс від імені адміністратора з меню "Пуск", натиснувши **Усі програми > ESET > ESET Endpoint Antivirus**. Також можна застосувати [політику](#) ESET PROTECT.

Щоб вимкнути стартовий екран ESET Endpoint Antivirus, зніміть прапорець **Відображати стартовий екран під час запуску**.

Щоб під час сканування програма ESET Endpoint Antivirus відтворювала звукове попередження про важливі події (наприклад, виявлення загрози або завершення процесу), установіть прапорець **Використовувати звуковий сигнал**.

Додати до контекстного меню: додати елементи керування ESET Endpoint Antivirus до контекстного меню.

Статуси

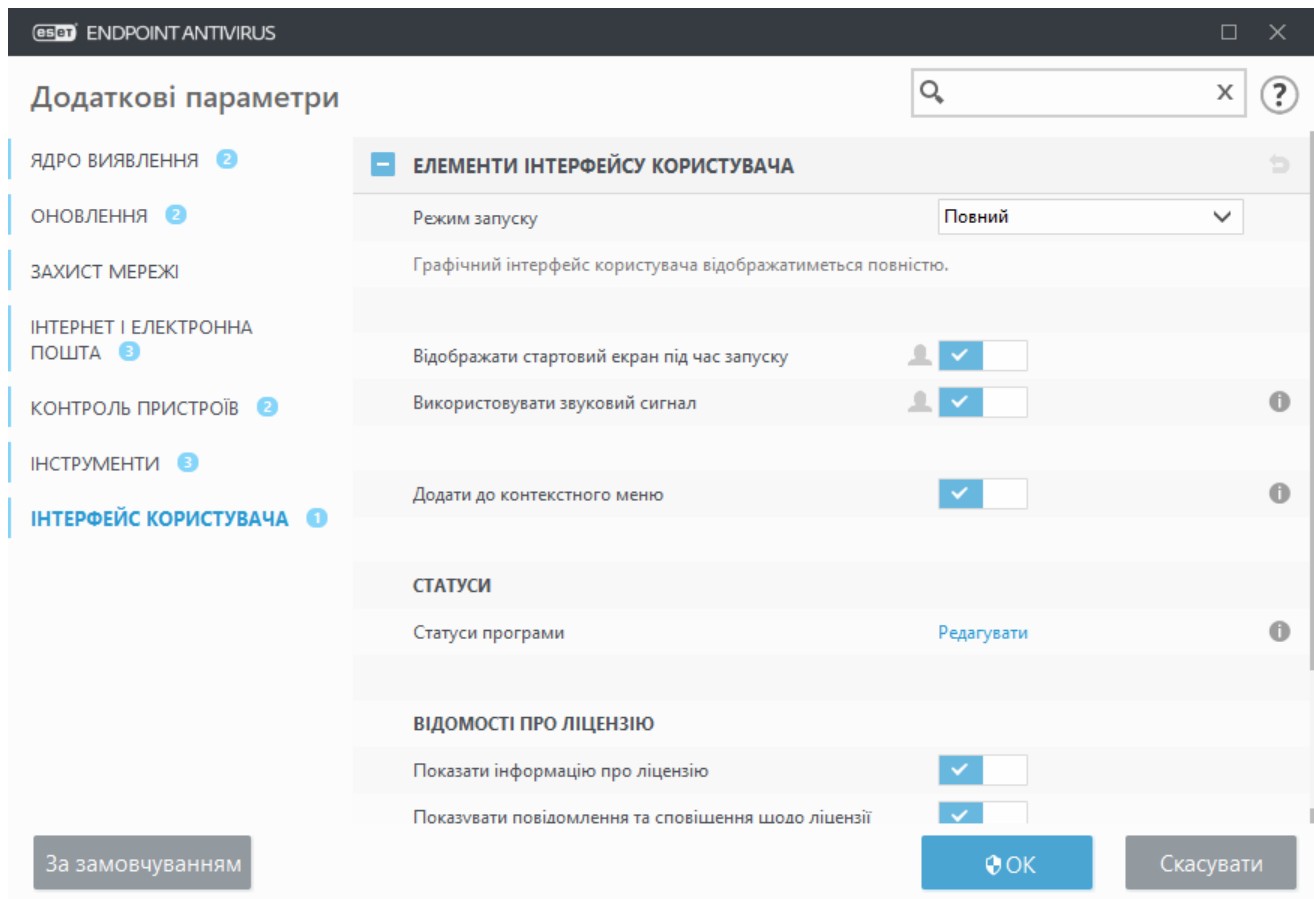
Статуси програм: натисніть кнопку **Редагувати**, щоб вимкнути статуси, які відображаються на панелі **Статус захисту** в головному меню.

Відомості про ліцензію

Показувати інформацію про ліцензію: якщо цей параметр вимкнено, дата завершення строку дії ліцензії на сторінках **Статус захисту** й **Довідка та підтримка** не відображатиметься.

Показувати повідомлення та сповіщення щодо ліцензії: якщо цей параметр вимкнено, сповіщення та повідомлення відображатимуться лише після завершення терміну дії ліцензії.

i Ви можете застосувати параметри інформації про ліцензію. Однак зверніть увагу: для продукту ESET Endpoint Antivirus, активованого за допомогою ліцензії MSP, вони недоступні.



Параметри доступу

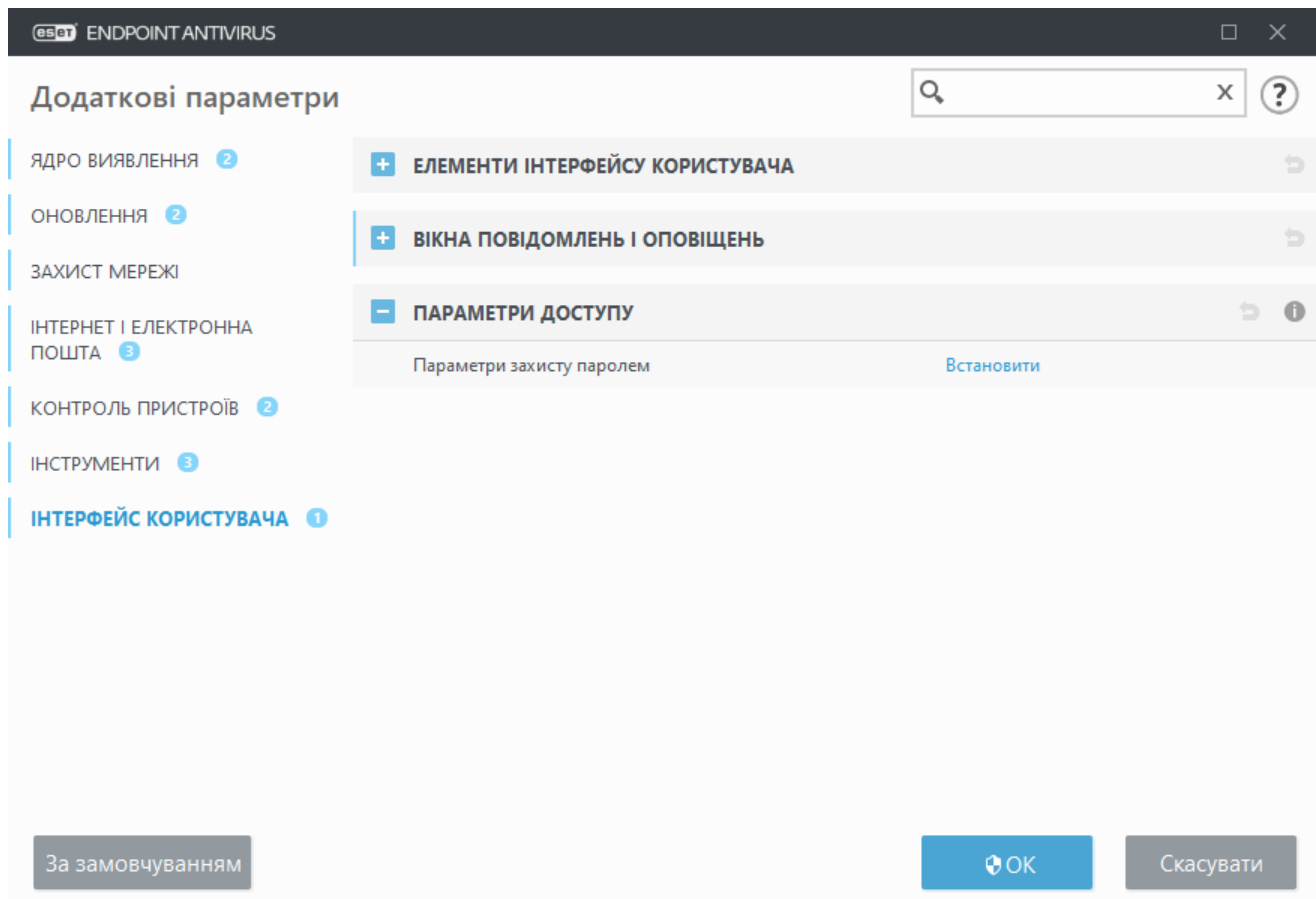
Для максимальної безпеки системи першочергове значення має правильне налаштування програми ESET Endpoint Antivirus. Будь-яка неправильна зміна може призвести до втрати важливих даних. Щоб уникнути несанкціонованих змін, параметри ESET Endpoint Antivirus можна захистити паролем.

Керовані середовища

Адміністратор може створити політику для захисту паролем налаштувань для ESET Endpoint Antivirus на підключених клієнтських комп'ютерах. Інструкції зі створення нової політики див. в розділі [Параметри, захищені паролем](#).

Некерована процедура

Налаштування захисту паролем можна знайти в меню **Додаткові параметри (F5)** у розділі **Інтерфейс користувача > Параметри доступу**.



Параметри захисту паролем: укажіть налаштування пароля. Натисніть, щоб відкрити вікно "Параметри пароля".

Щоб призначити або змінити пароль для захисту параметрів програми, натисніть **Установити**.

Пароль для розділу "Додаткові параметри"

Щоб захистити параметри конфігурації ESET Endpoint Antivirus від несанкціонованих змін, потрібно вказати новий пароль.

Керовані середовища

Адміністратор може створити політику для захисту паролем налаштувань для ESET Endpoint Antivirus на підключених клієнтських комп'ютерах. Інструкції зі створення нової політики див. в розділі [Параметри, захищені паролем](#).

Некерована процедура

Порядок зміни поточного пароля

1. Уведіть поточний пароль у поле **Старий пароль**.
2. Уведіть новий пароль у поля **Новий пароль** і **Підтвердьте пароль**.
3. Клацніть **ОК**.


Цей пароль потрібно буде вводити під час кожної спроби внести зміни до параметрів ESET Endpoint Antivirus.

Якщо ви забули пароль, доступ до додаткових параметрів можна відновити.

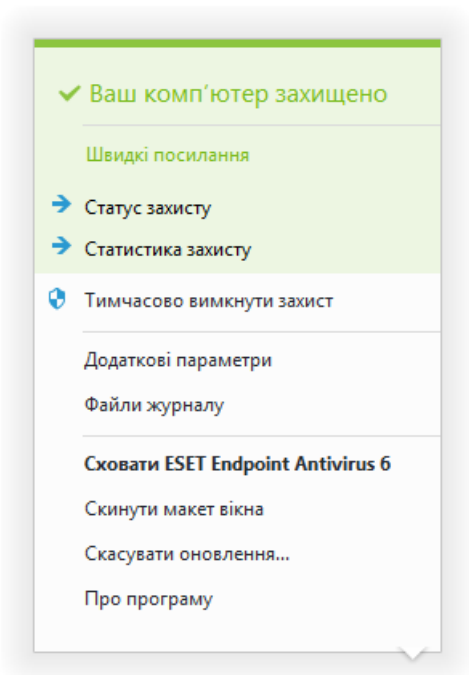
- [Відновлення з використанням методу "Відновити пароль" \(для версії 7.1 і новіших\)](#)
- [Відновлення з використанням інструмента ESET Unlock Tool \(для версії 7.0 і новіших\)](#)

За цим посиланням див. додаткову інформацію, якщо ви забули ліцензійний ключ від ESET, дату завершення терміну дії ліцензії або іншу інформацію про ліцензію для ESET Endpoint Antivirus.

Піктограма в системному треї

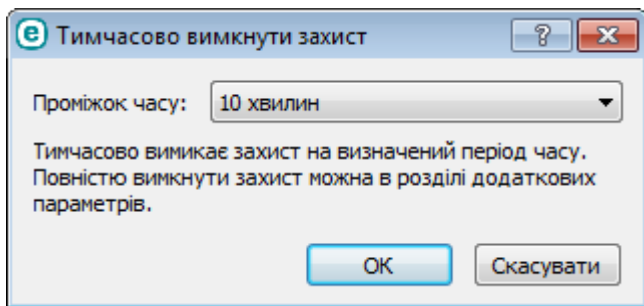
Доступ до деяких найбільш важливих параметрів і функцій можна отримати, клацнувши правою кнопкою миші піктограму в системному треї .

i Щоб відкрити меню піктограм у системному треї, переконайтеся, що для режиму запуску [елементів інтерфейсу користувача](#) вибрано значення "Повний".



Тимчасово вимкнути захист: відображається діалогове вікно з підтвердженням, у якому можна вимкнути [ядро виявлення](#), тобто модуль, який захищає систему від атак, контролюючи передачу даних у файлах, через Інтернет та електронну пошту.

Розкривне меню **Проміжок часу** служить для вибору періоду, протягом якого захист залишатиметься вимкненими.



Додаткові параметри: скористайтеся цією опцією, щоб відкрити дерево **Додаткові параметри**. Меню додаткових параметрів також можна відкрити, натиснувши клавішу F5 або перейшовши до розділу **Параметри > Додаткові параметри**.

Файли журналу: [вони](#) містять інформацію про важливі програмні події й огляд виявлених загроз.

Відкрити ESET Endpoint Antivirus: відкриває головне вікно програми ESET Endpoint Antivirus за допомогою піктограми в системному треї.

Скинути макет вікна: відновлення стандартного розміру та позиції вікна ESET Endpoint Antivirus на екрані.

Перевірка наявності оновлень: запуск оновлення обробника виявлення для забезпечення повного захисту від шкідливого коду.

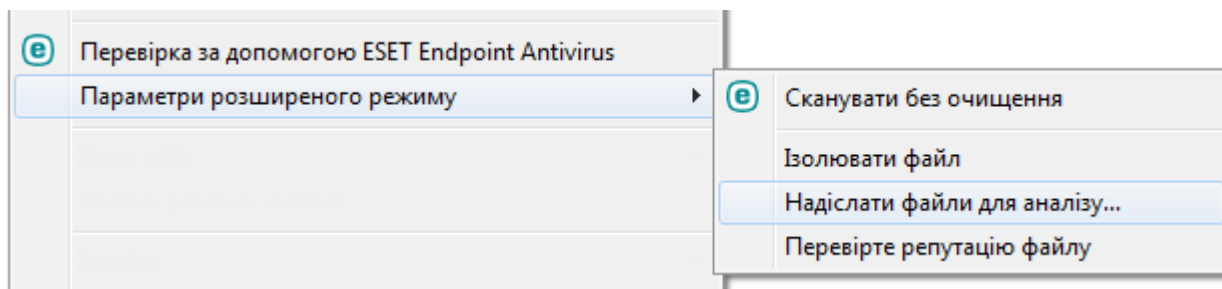
Про програму: вікно, що містить інформацію про систему, версію ESET Endpoint Antivirus й інсталювані модулі програми, а також термін дії ліцензії. Інформацію про операційну систему й системні ресурси можна знайти внизу сторінки.

Контекстне меню

Контекстне меню відкривається, якщо натиснути об'єкт (файл) правою кнопкою миші. У меню перелічені всі дії, які можна виконати з об'єктом.

Можна інтегрувати елементи керування ESET Endpoint Antivirus у контекстне меню. Параметри для налаштування цієї функції доступні в дереві додаткових параметрів у розділі **Інтерфейс користувача > Елементи інтерфейсу користувача**.

Додати до контекстного меню: додати елементи керування ESET Endpoint Antivirus до контекстного меню.



Довідка та підтримка

ESET Endpoint Antivirus містить засоби для виправлення неполадок і технічну інформацію, яка допоможе у вирішенні можливих проблем.



Інстальований продукт

- **Про ESET Endpoint Antivirus** – відомості про вашу копію [ESET Endpoint Antivirus](#).
- **Виправлення неполадок із продуктом**: натисніть це посилання, щоб знайти рішення найпоширеніших проблем.
- **Виправлення неполадок із ліцензією**: натисніть це посилання, щоб знайти рішення проблем з активацією або зміною ліцензії.
- **Змінити ліцензію** – натисніть, щоб відкрити вікно активації й активувати продукт.



Сторінка довідки: натисніть це посилання, щоб відкрити довідку ESET Endpoint Antivirus.



Служба технічної підтримки

- **Надіслати запит до служби технічної підтримки**: якщо вам не вдається знайти відповідь на своє запитання, скористайтесь формою на веб-сайті ESET, щоб швидко зв'язатися зі співробітниками служби технічної підтримки. Залежно від налаштувань перед заповненням веб-форми вам може знадобитися [надіслати дані конфігурації системи](#).
- **Інформація для технічної підтримки**: ви можете скопіювати й надіслати інформацію (наприклад, назву продукту, версію, операційну систему та тип процесора) в службу технічної підтримки ESET, коли відобразиться відповідний запит.
- **ESET Log Collector** – переспрямовує на статтю [бази знань ESET Knowledgebase](#), де можна завантажити програму ESET Log Collector, яка автоматично збирає інформацію й журнали на комп'ютері для швидкого вирішення проблем. Більш докладну інформацію див. в [онлайн-посібнику користувача ESET Log Collector](#).
- Натисніть [Розширене журналювання](#), щоб створити розширені журнали для всіх доступних функцій. Це дасть змогу розробникам діагностувати й усувати проблеми. За замовчуванням задано мінімальний рівень ведення журналу — Діагностика. Розширене журналювання автоматично вимикається через дві години, якщо не зупинити його раніше, натиснувши Припинити розширене журналювання. Коли всі журнали створено, відображається вікно зі сповіщеннями, які надають прямий доступ до папки "Diagnostic" зі створеними журналами.

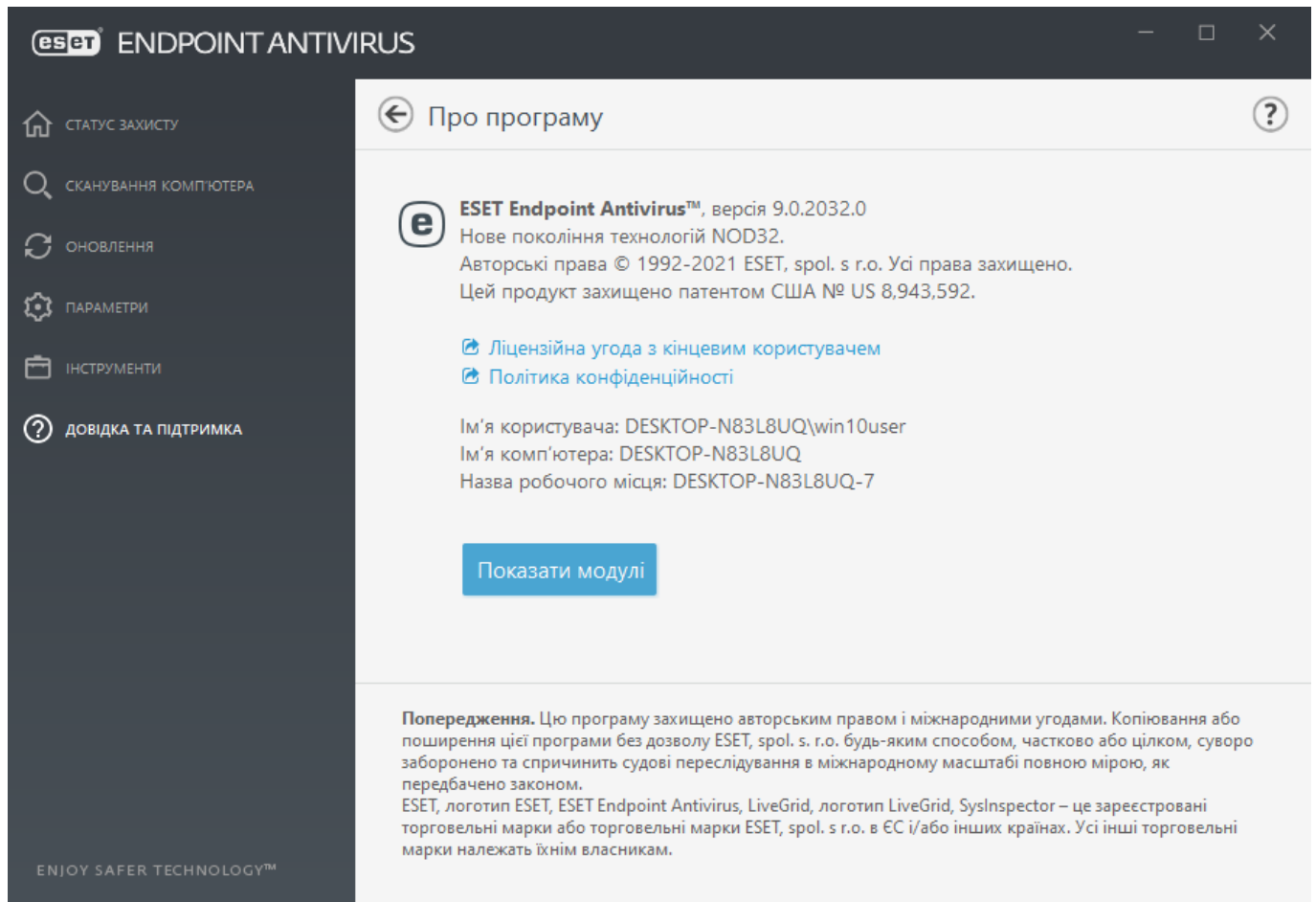


База знань – [база знань ESET](#) містить відповіді на найпоширеніші запитання, а також рекомендовані способи вирішення різноманітних проблем. Регулярне оновлення, яке виконують технічні спеціалісти ESET, робить базу знань найефективнішим інструментом для вирішення різноманітних проблем.

Про продукт ESET Endpoint Antivirus

У цьому вікні вказуються докладні відомості про інстальовану версію ESET Endpoint Antivirus, операційну систему та її ресурси.

Щоб переглянути список інстальованих програмних модулів та їхніх версій, клацніть **Показати модулі**. Інформацію про модулі можна скопіювати в буфер обміну, натиснувши **Копіювати**. Ця функція може бути корисною під час виправлення неполадок і звернення до служби технічної підтримки.



Надсилання даних про конфігурацію системи

Щоб надавати допомогу якомога швидше та якісніше, компанії ESET потрібна інформація про конфігурацію ESET Endpoint Antivirus, систему й запущені процеси ([файл журналу ESET SysInspector](#)), а також дані реєстру. Компанія ESET використовуватиме ці відомості виключно для надання технічної підтримки користувачеві.

Коли ви надсилаєте веб-форму, дані про конфігурацію системи передаються компанії ESET. Установіть прапорець **Завжди надсилати ці дані**, щоб запам'ятати відповідну дію для цього процесу. Щоб надіслати форму без додаткових даних, натисніть **Не надсилати дані**. До служби технічної підтримки ESET можна звернутися за допомогою онлайн-форми.

Цей параметр також можна налаштувати в меню **Додаткові параметри > Інструменти > Діагностика > Служба технічної підтримки**.

i Якщо ви вирішили надіслати дані про систему, заповніть і надішліть веб-форму, інакше ваше звернення не буде зареєстровано, а дані про систему буде втрачено.

Технічна підтримка

Зверніться до служби технічної підтримки

Надіслати запит до служби технічної підтримки: якщо вам не вдається знайти відповідь на своє запитання, скористайтесь формою на веб-сайті ESET, щоб швидко зв'язатися зі співробітниками служби технічної підтримки ESET. Залежно від налаштувань перед заповненням веб-форми вам може знадобитися [надіслати дані конфігурації системи](#).

Отримайте відомості для служби технічної підтримки

Інформація для технічної підтримки: ви можете скопіювати й надіслати інформацію (наприклад, дані ліцензії, назву продукту, версію, операційну систему та відомості про комп'ютер) в службу технічної підтримки ESET, коли відобразиться відповідний запит.

ESET Log Collector – переспрямовує на статтю [бази знань ESET Knowledgebase](#), де можна завантажити програму ESET Log Collector, яка автоматично збирає інформацію й журнали на комп'ютері для швидкого вирішення проблем. Більш докладну інформацію див. в [онлайн-посібнику користувача ESET Log Collector](#).

Натисніть **Розширене журналювання**, щоб створити розширені журнали для всіх доступних функцій. Це дасть змогу розробникам діагностувати й усувати проблеми. За замовчуванням задано мінімальний рівень ведення журналу — **Діагностика**. Розширене журналювання автоматично вимикається через дві години, якщо не зупинити його раніше, натиснувши **Припинити розширене журналювання**. Коли всі журнали створено, відображається вікно зі сповіщеннями, які надають прямий доступ до папки "Diagnostic" зі створеними журналами.

Сповіщення

Щоб керувати сповіщеннями ESET Endpoint Antivirus, відкрийте **Додаткові параметри (F5) > Сповіщення**. Ви можете налаштувати вказані нижче типи сповіщень.

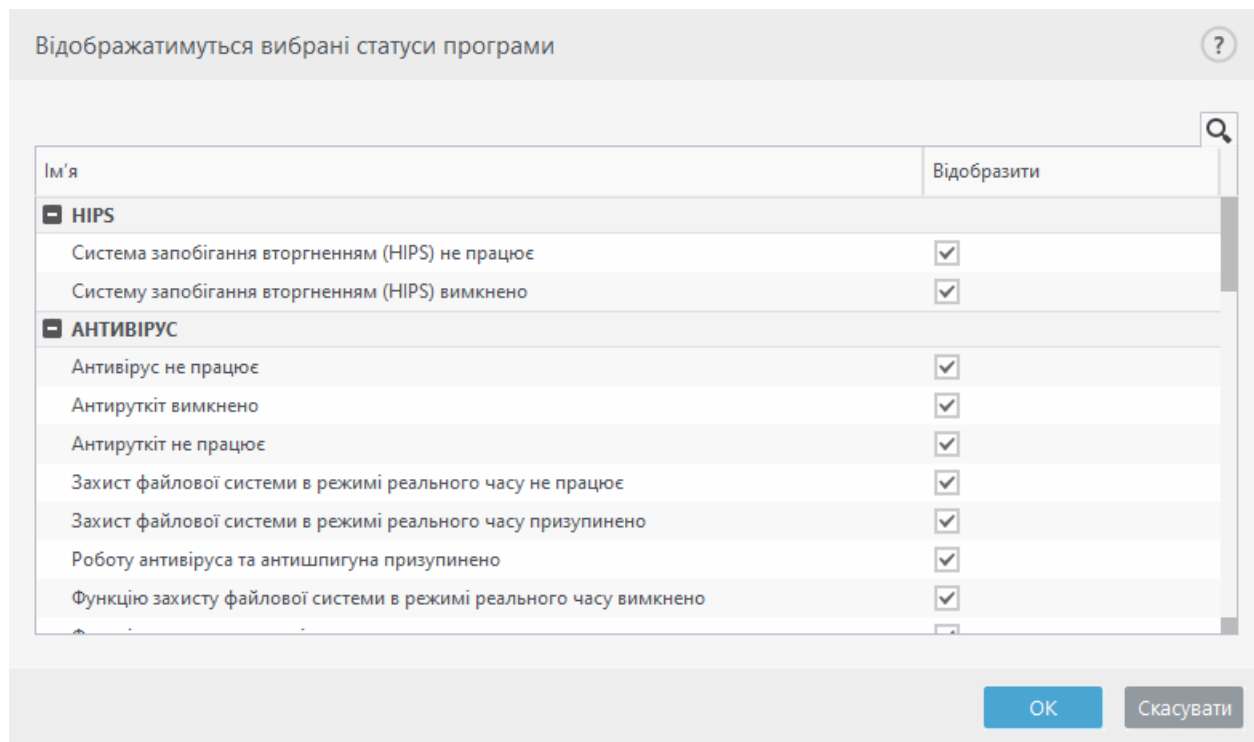
- **Статуси програм:** натисніть **Редагувати**, щоб вибрати статуси програми, що відображаються в основному розділі [головного вікна програми](#).
- **Сповіщення на робочому столі:** невелике спливаюче вікно поруч із панеллю завдань системи.
- **Налаштування сповіщень:** додайте настроюване повідомлення, наприклад, у сповіщення на робочому столі.
- **Інтерактивні сповіщення:** вікна сповіщень і вікна повідомлень, що потребують втручання користувача.
- **Пересилання** (Сповіщення електронною поштою): сповіщення електронною поштою надсилаються на вказану адресу електронної пошти.

Статуси програми

Щоб налаштувати статуси програми для відображення (наприклад, після призупинення захисту від вірусів і шпигунських програм або ввімкнення ігрового режиму), відкрийте **Додаткові параметри (F5) > Сповіщення** і клацніть **Редагувати**, щоб вибрати статуси

програми, які будуть відображатися в основному розділі [головного вікна програми](#).

Статус програми також відображатиметься, якщо продукт не активовано або термін дії ліцензії минув. Цей параметр можна змінити за допомогою [політик ESET PROTECT](#).



Сповіщення на робочому столі

Сповіщення на робочому столі відображається в маленькому спливаючому вікні поруч із панеллю завдань системи. За замовчуванням воно відображається протягом 10 секунд, а потім поступово зникає. Це основний спосіб, яким ESET Endpoint Antivirus сповіщає користувача про успішні оновлення продукту, нові підключені пристрої, завершення сканування на наявність вірусів або знайдені нові загрози.

Показувати сповіщення на робочому столі. Рекомендуємо не вимикати цю опцію, щоб продукт інформував про нові події.

Сповіщення на робочому столі. Натисніть **Редагувати**, щоб увімкнути або вимкнути конкретні [сповіщення на робочому столі](#).

Не показувати сповіщення під час роботи програм у повноекранному режимі: скасовує відображення всіх неінтерактивних сповіщень, коли програми працюють у повноекранному режимі.

Час очікування в секундах: укажіть інтервал часу, протягом якого відображатиметься сповіщення. Значення має бути в діапазоні від 3 до 30 секунд.

Прозорість: укажіть ступінь прозорості сповіщень (у відсотках). Підтримується діапазон значень від 0 (зовсім непрозорі сповіщення) до 80 (сповіщення з дуже високим ступенем прозорості).

Мінімальна детальність подій для відображення: укажіть початковий рівень важливості

сповіщень, які потрібно відображати на екрані. У розкритому меню виберіть один із таких параметрів:

- **Діагностика** – запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи**: запис інформаційних повідомлень (наприклад, про нестандартні події в мережі), включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження**: фіксуються всі критичні помилки й попереджувальні повідомлення (антируткіт не працює належним чином або не вдалося здійснити оновлення).
- **Помилки**: запис помилок (захист документів не запущено) і критичних помилок.
- **Критичні помилки**: запис лише критичних помилок (помилка запуску антивірусного захисту або інфікування системи).

У системі з багатьма користувачами відображати сповіщення на екрані цього користувача: для вибраних облікових записів сповіщення відображатимуться на робочому столі. Наприклад, якщо ви не використовуєте обліковий запис адміністратора, уведіть повне ім'я облікового запису. Після цього ви будете отримувати сповіщення на робочому столі. Сповіщення на робочому столі може отримувати лише один обліковий запис користувача.

Дозволити показ сповіщень на екрані: сповіщення відображатимуться на екрані; для їх перегляду потрібно буде натиснути комбінацію клавіш Alt+Tab.

Діалогове вікно: сповіщення на робочому столі

Щоб налаштувати видимість сповіщень на робочому столі (які відображаються в нижньому правому куті екрана), у меню **Додаткові параметри** (F5) перейдіть у розділ **Сповіщення > Сповіщення на робочому столі**. Натисніть **Редагувати** поруч із пунктом **Сповіщення на робочому столі** й установіть прапорець **Показати на робочому столі**.

і Якщо потрібно налаштувати сповіщення **Файл перевірено** й **Файл не перевірено** перед використанням ESET LiveGuard, для параметра [Проактивний захист](#) необхідно задати **Блокувати виконання до отримання результату аналізу**.

Налаштування сповіщень

У цьому вікні можна налаштувати текст сповіщень.

Тест сповіщення за замовчуванням: текст за замовчуванням у підписі сповіщень.


Виявлені об'єкти

Щоб сповіщення про шкідливе ПЗ не закривалось автоматично, а лише вручну, увімкніть параметр **Не закривати автоматично сповіщення про шкідливе ПЗ**.

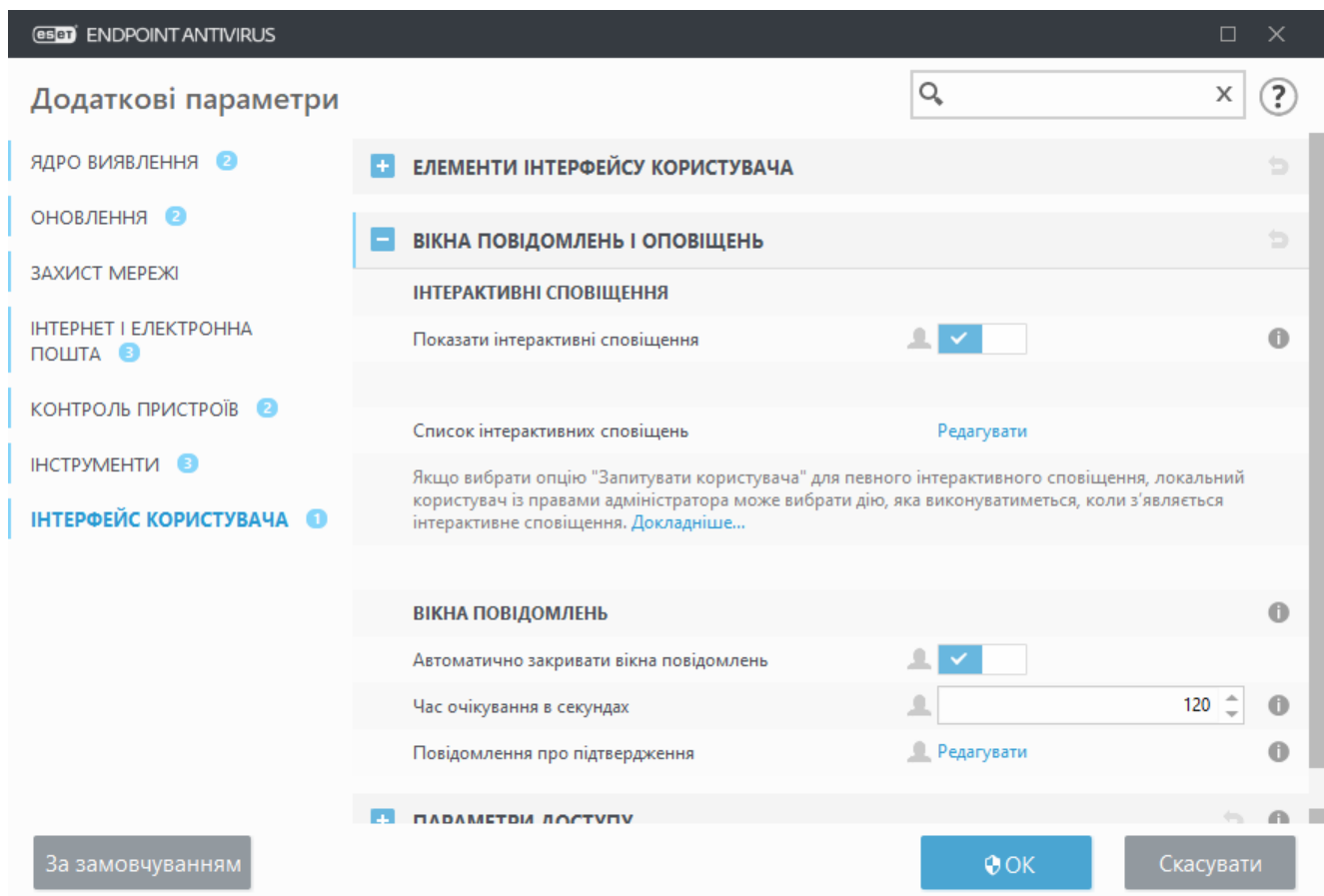
Щоб змінити текст сповіщень, вимкніть параметр **Використовувати повідомлення за замовчуванням** і введіть власний текст у полі **Повідомлення в сповіщенні про виявлений**

Інтерактивні сповіщення

Шукаєте інформацію про стандартні сигнали та сповіщення?

- [Знайдено загрозу](#)
- [Адресу заблоковано](#)
- [Продукт не активовано](#)
- [Доступне оновлення](#)
-  Невідповідність інформації про оновлення
- [Виправлення неполадок, пов'язаних із появою повідомлення "Помилка оновлення модулів"](#)
- ["Файл пошкоджено" або "Не вдалося перейменувати файл"](#)
- [Сертифікат веб-сайту відкликано](#)
- [Мережеву загрозу заблоковано](#)
- [Файл заблоковано, оскільки виконується аналіз](#)

У розділі **Сповіщення** в області **Інтерактивні сповіщення** можна визначати, яким чином ESET Endpoint Antivirus буде оброблювати виявлені об'єкти, щодо яких має прийняти рішення користувач (наприклад, потенційні фішингові веб-сайти тощо).



Інтерактивні сповіщення

Якщо знайдено загрози або потрібно втручання користувача, відображаються вікна інтерактивних сповіщень.

Показати інтерактивні сповіщення

- Для некерованих користувачів, рекомендуємо не змінювати значення цього параметра за замовчуванням.
- Для керованих користувачів не вимикайте цей параметр і виберіть для них попередньо визначену дію в пункті [Список інтерактивних сповіщень](#).

Якщо вимкнути параметр **Показати інтерактивні сповіщення**, усі вікна сповіщень і діалогові вікна браузера будуть вимкнені. Буде автоматично вибрано попередньо визначену дію за замовчуванням (наприклад, "потенційний фішинговий веб-сайт" буде заблоковано).

Вікна повідомлень

Щоб спливаючі вікна закривалися автоматично через певний проміжок часу, установіть параметр **Автоматично закривати вікна повідомлень**. Якщо вікна сигналів тривоги не закрити вручну, їх буде закрито автоматично після завершення вказаного періоду часу.

Повідомлення про підтвердження: показує [список повідомлень про підтвердження](#), де можна вибрати ті, що потрібно відображати.

Список інтерактивних сповіщень

У цьому розділі наведено опис деяких вікон інтерактивних сповіщень, які відображаються в ESET Endpoint Antivirus перед виконанням будь-якої операції.

Щоб змінити поведінку налаштовуваних інтерактивних сповіщень, у дереві ESET Endpoint Antivirus "Додаткові параметри" виберіть пункти **Сповіщення > Інтерактивні сповіщення** й клацніть **Змінити**.

i Може стати в пригоді для керованих середовищ, де адміністратор може скасувати вибір **Звернутися до користувача** для всього середовища й вибрати попередньо визначену операцію, яка буде застосовуватися під час відображення вікон інтерактивних сповіщень. Див. також розділ щодо [статусів внутрішніх програм](#).

Виберіть інтерактивне сповіщення для відображення ?

Q

Ім'я	Запитувати користувача	Дія застосовується без відображення
■ ЗАХИСТ МЕРЕЖІ		
Доступ до мережі заблоковано	<input checked="" type="checkbox"/>	Немає
Мережеве з'єднання заблоковано	<input checked="" type="checkbox"/>	Заблокувати
Мережеву загрозу заблоковано	<input checked="" type="checkbox"/>	Заблокувати
■ ЗМІННІ НОСІЇ		
Виявлено новий пристрій	<input checked="" type="checkbox"/>	Показати параметри сканування
■ КОМП'ЮТЕР		
Перезавантажити комп'ютер (необхідно)	<input checked="" type="checkbox"/>	Немає
Перезавантажити комп'ютер (рекомендується)	<input checked="" type="checkbox"/>	Немає

ОК
Скасувати

Щоб дізнати більше про певне вікно сповіщень, перевірте відповідні розділи довідки:

Знімні носії

- [Виявлено новий пристрій](#)

Захист мережі

- [Доступ до мережі заблоковано](#): відображається в разі активації клієнтського завдання **Ізолювати комп'ютер від мережі** цієї робочої станції з ESET PROTECT.
- [Мережевий зв'язок заблоковано](#)
- [Мережеву загрозу заблоковано](#)

Сповіщення веб-браузера

- [Виявлено потенційно небажаний вміст](#)
- [Веб-сайт заблоковано через фішинг](#)

Комп'ютер

Наявність цих сповіщень змінить колір інтерфейсу користувача на помаранчевий:

- [Перезавантажити комп'ютер \(необхідно\)](#)
- [Перезавантажити комп'ютер \(рекомендується\)](#)

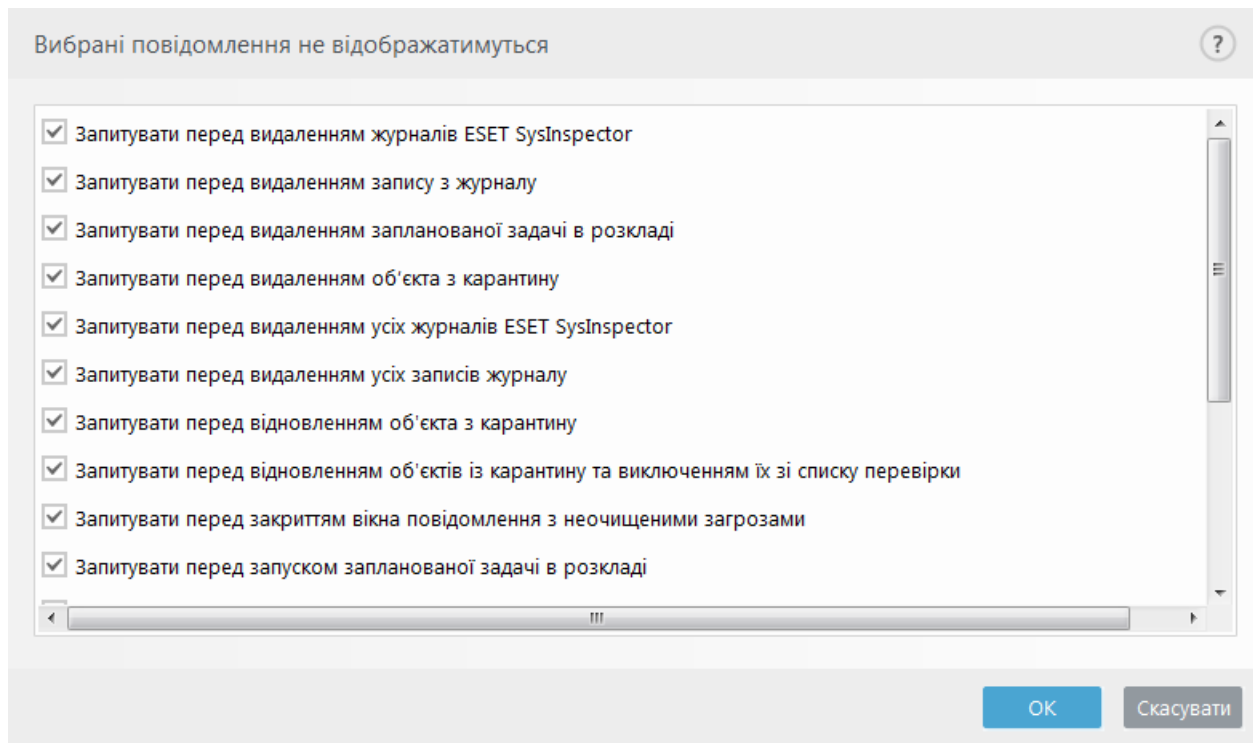


Інтерактивні сповіщення не містять інтерактивних вікон ядра виявлення, системи запобігання вторгненням (HIPS) або брандмауера, оскільки їх поведінку можна налаштувати окремо в спеціальній функції.

Повідомлення про підтвердження

Щоб налаштувати повідомлення про підтвердження, виберіть **Інтерфейс користувача > Вікна повідомлень і оповіщень > Повідомлення про підтвердження** в дереві ESET Endpoint Antivirus

"Додаткові параметри" й клацніть **Змінити**.



У цьому діалоговому вікні відображатимуться повідомлення про підтвердження від програми ESET Endpoint Antivirus перед виконанням будь-якої дії. Установіть або зніміть прапорець біля кожного повідомлення про підтвердження, щоб увімкнути або вимкнути його.

Дізнайтеся більше про функцію, пов'язану з повідомленнями з підтвердженням:

- [Запитувати перед видаленням журналів ESET SysInspector](#)
- [Запитувати перед видаленням усіх журналів ESET SysInspector](#)
- [Запитувати перед видаленням об'єкта з карантину](#)
- Запитувати перед скасуванням змін у розділі додаткових параметрів
- [Запитувати перед закриттям вікна повідомлення з неочищеними загрозами](#)
- [Запитувати перед видаленням запису з журналу](#)
- [Запитувати перед видаленням запланованої задачі в розкладі](#)
- [Запитувати перед видаленням усіх записів журналу](#)
- [Запитувати перед скиданням даних статистики](#)
- [Запитувати перед відновленням об'єкта з карантину](#)
- [Запитувати перед відновленням об'єктів із карантину та виключенням їх зі списку перевірки](#)
- [Запитувати перед запуском запланованої задачі в розкладі](#)
- [Показувати діалоги для підтвердження в продукті операцій для поштових клієнтів Outlook Express і Windows Mail](#)
- [Показувати діалоги для підтвердження в продукті операцій для Windows Live Mail](#)
- [Показувати діалоги для підтвердження в продукті операцій для поштового клієнта Outlook](#)

Помилка через конфлікт додаткових

параметрів

Ця помилка може виникати, якщо певний компонент (наприклад, HIPS) і користувач одночасно створюють правила в інтерактивному або навчальному режимі.

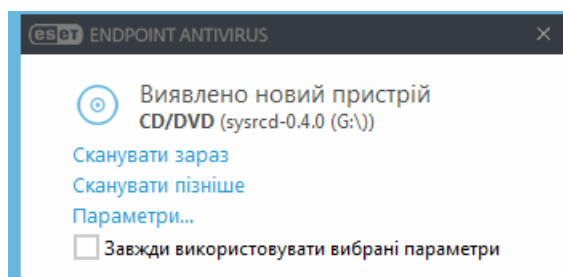


Щоб створити власні правила, рекомендуємо застосувати режим фільтрації за замовчуванням (**Автоматичний режим**). Докладніше про [HIPS і режими фільтрації HIPS](#).

Знімні носії

ESET Endpoint Antivirus забезпечує автоматичне сканування змінних носіїв (компакт-/DVD-диск/USB тощо) після вставлення в комп'ютер. Це може бути корисним, якщо адміністратору комп'ютера потрібно заборонити користувачам застосовувати знімні носії з недозволеним вмістом.

Якщо в ESET Endpoint Antivirus вибрано параметр **Показати параметри сканування**, після вставлення змінного носія відобразиться таке діалогове вікно:



Нижче наведено параметри, доступні в цьому діалоговому вікні.

- **Сканувати зараз**: ініціювати сканування змінного носія.
- **Не сканувати**: жодна дія не виконуватиметься.

Окрім того, ESET Endpoint Antivirus має функцію контролю пристроїв, що дає змогу визначати правила для зовнішніх пристроїв на певному комп'ютері. Докладнішу інформацію про контроль пристроїв можна знайти в розділі [Контроль пристроїв](#).

Щоб відкрити параметри сканування змінних носіїв, відкрийте **Додаткові параметри (F5) > Інтерфейс користувача > Вікна повідомлень і оповіщень > Інтерактивні сповіщення > Список інтерактивних сповіщень > Редагувати > Виявлено новий пристрій**.

Якщо вибрано параметр **Запитувати користувача**, виберіть дію, яка виконуватиметься під час вставлення змінного носія в комп'ютер:

- **Не сканувати**: не виконуватиметься жодна дія, а вікно **Виявлено новий пристрій** не відобразиться.
- **Автоматичне сканування пристроїв**: виконуватиметься сканування використовуваного змінного носія.
- **Примусове сканування пристрою**: на комп'ютері буде виконано сканування використовуваного змінного носія. Це сканування неможливо скасувати.
- **Показати параметри сканування**: відкриває екран налаштування **Інтерактивні сповіщення**.

Необхідно перезавантажити комп'ютер

Якщо на машинах кінцевої точки з'являються красні сповіщення "Необхідно перезавантажити комп'ютер", можна вимкнути відображення сповіщень.

Щоб вимкнути сповіщення "Необхідно перезавантажити комп'ютер" або "Рекомендовано перезавантажити комп'ютер", дотримуйтеся наведених нижче інструкцій:

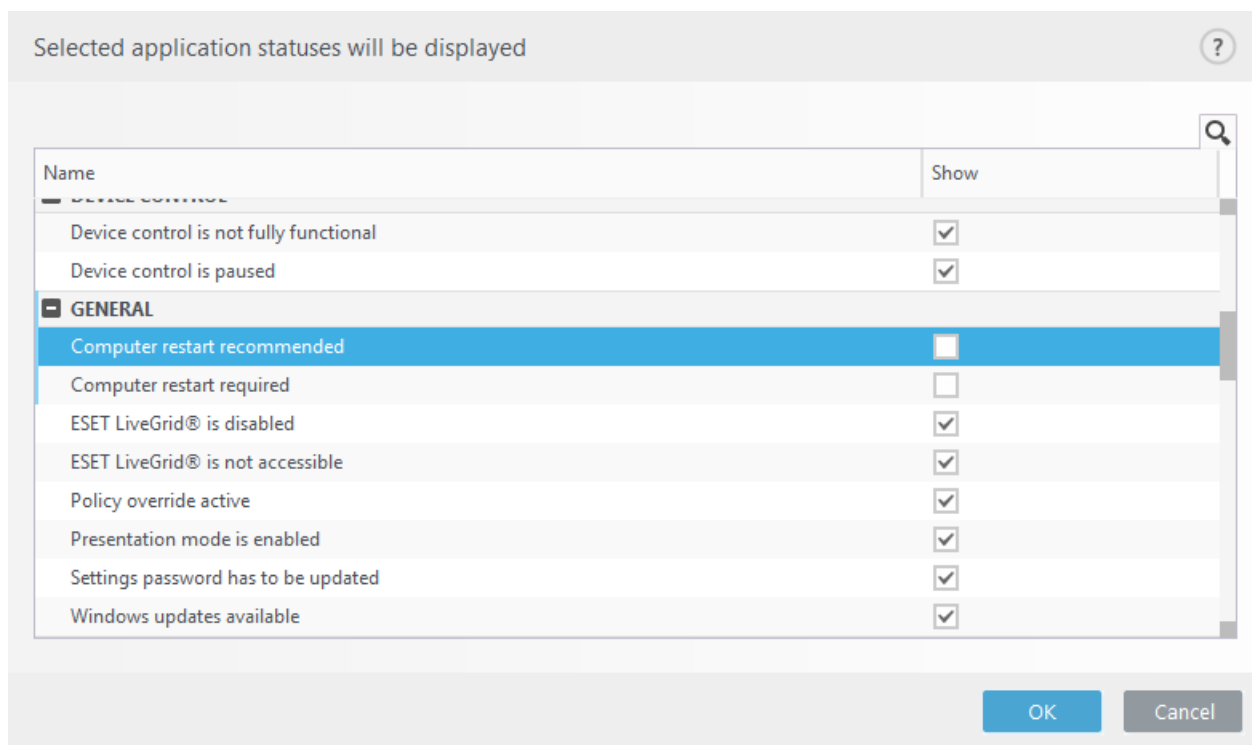
1. Натисніть клавішу **F5**, щоб відкрити вікно "Додаткові параметри" й розгорніть розділ **Вікна повідомлень і оповіщень**.
2. Клацніть **Редагувати** поруч із пунктом **Список інтерактивних сповіщень**. У розділі **Комп'ютер** зніміть прапорці **Перезавантажити комп'ютер (обов'язково)** і **Перезавантажити комп'ютер (рекомендовано)**.

Select which interactive alert will be displayed ?

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

3. Клацніть **OK**, щоб зберегти зміни в обох відкритих вікнах.
4. Сповіщення більше не будуть з'являтися на кінцевій точці.
5. (Необов'язково) Щоб вимкнути статус програми в головному вікні ESET Endpoint Antivirus, у вікні [Статуси програм](#) зніміть прапорці поруч із пунктами **Необхідно перезавантажити комп'ютер** і **Рекомендовано перезавантажити комп'ютер**.



Рекомендовано перезавантажити комп'ютер

Якщо на машинах кінцевої точки з'являються жовті сповіщення "Рекомендовано перезавантажити комп'ютер", можна вимкнути відображення сповіщень.

Щоб вимкнути сповіщення "Необхідно перезавантажити комп'ютер" або "Рекомендовано перезавантажити комп'ютер", дотримуйтеся наведених нижче інструкцій:

1. Натисніть клавішу **F5**, щоб відкрити вікно "Додаткові параметри" й розгорніть розділ **Вікна повідомлень і оповіщень**.
2. Клацніть **Редагувати** поруч із пунктом **Список інтерактивних сповіщень**. У розділі **Комп'ютер** зніміть прапорці **Перезавантажити комп'ютер (обов'язково)** і **Перезавантажити комп'ютер (рекомендовано)**.

Select which interactive alert will be displayed

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

3. Клацніть **OK**, щоб зберегти зміни в обох відкритих вікнах.
4. Сповіщення більше не будуть з'являтися на кінцевій точці.
5. (Необов'язково) Щоб вимкнути статус програми в головному вікні ESET Endpoint Antivirus, у вікні [Статуси програм](#) зніміть прапорці поруч із пунктами **Необхідно перезавантажити комп'ютер** і **Рекомендовано перезавантажити комп'ютер**.

Selected application statuses will be displayed

Name	Show
- DEVICE CONTROL	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
- GENERAL	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

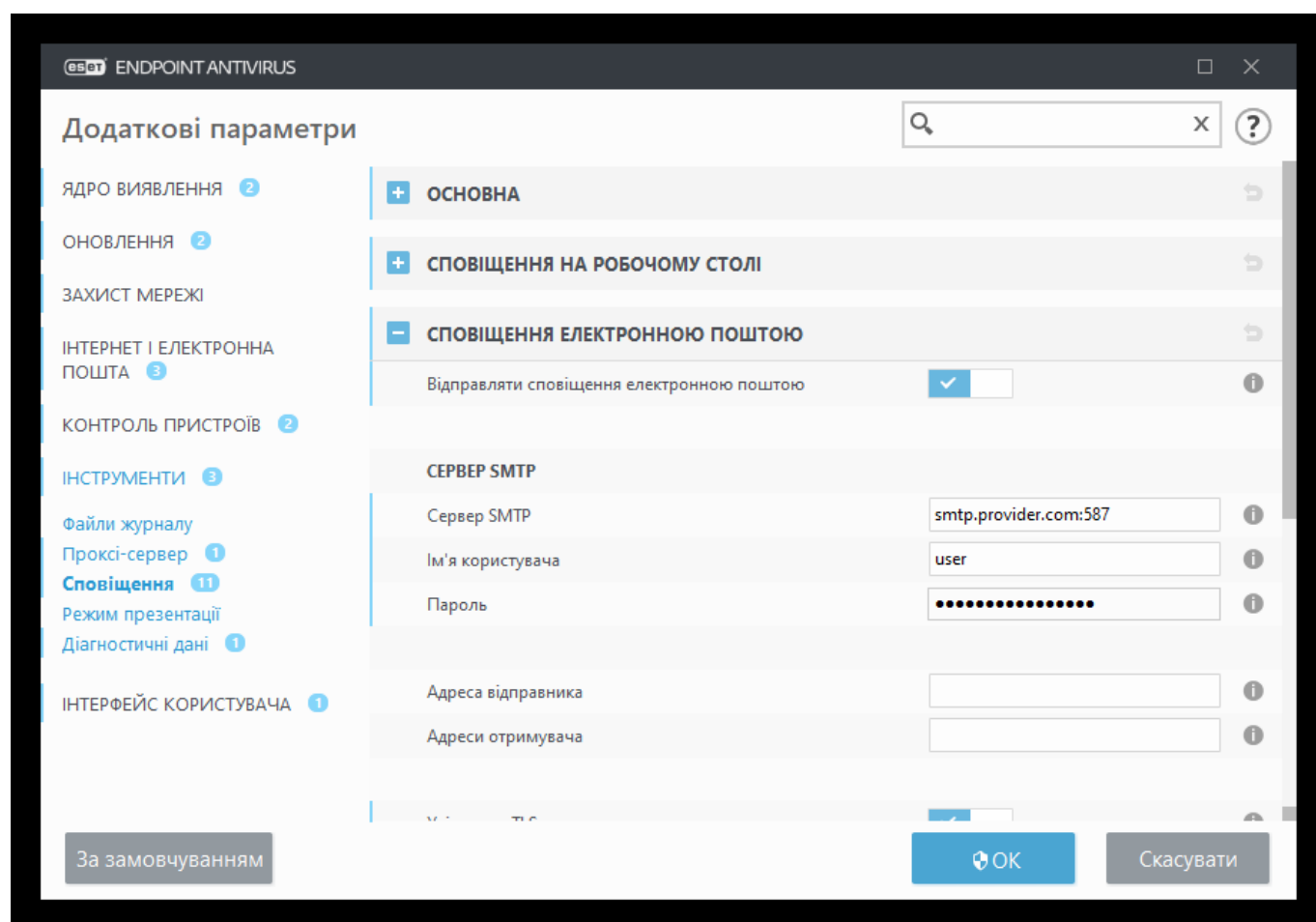
OK Cancel

Пересилання

ESET Endpoint Antivirus може автоматично надсилати сповіщення електронною поштою, якщо відбуватимуться події з вибраним рівнем розголошення. Щоб активувати сповіщення електронною поштою, виберіть пункти **Додаткові параметри** > **Сповіщення** > **Пересилання** >

Пересилати на електронну пошту й увімкніть параметр **Пересилати сповіщення на електронну пошту**.

Переадресовані сповіщення: виберіть сповіщення на робочому столі, які пересилатимуться на електронну пошту.



Сервер SMTP

SMTP-сервер: сервер SMTP для надсилання сповіщень (наприклад, *smtp.provider.com:587*, попередньо визначений порт – 25).

i Сервери SMTP з шифруванням за протоколом TLS підтримуються ESET Endpoint Antivirus.

Ім'я користувача й пароль: якщо SMTP-сервер вимагає автентифікації, у ці поля слід ввести дійсні ім'я користувача та пароль, які надають доступ до SMTP-сервера.

Адреса відправника: у цьому полі слід указати адресу відправника, що відображатиметься в заголовку надісланих електронною поштою сповіщень.

Адреса отримувача: у цьому полі слід указати адресу отримувача, що відображатиметься в заголовку сповіщень електронною поштою. Якщо адрес кілька, вони розділяються крапкою з комою.

Увімкнути TLS: активувати надсилання повідомлень про загрози та сповіщень із підтримкою шифрування TLS.

Параметри електронної пошти

У розкривному меню **Мінімальна детальність повідомлень** можна вибрати початковий рівень важливості сповіщень, які потрібно надсилати.

- **Діагностика** – запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи**: запис інформаційних повідомлень (наприклад, про нестандартні події в мережі), включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження**: фіксуються всі критичні помилки й попереджувальні повідомлення (антируткіт не працює належним чином або не вдалося здійснити оновлення).
- **Помилки**: запис помилок (захист документів не запущено) і критичних помилок.
- **Критичні помилки**: запис лише критичних помилок (помилка запуску антивірусного захисту або інфікування системи).

Надсилати кожне сповіщення окремим електронним листом: якщо ввімкнено, кожне сповіщення надсилатиметься окремо. Їх може надійти чимало за короткий проміжок часу.

Інтервал, через який будуть надсилатися нові сповіщення електронною поштою (хв): інтервал у хвилинах, через який електронною поштою надсилатимуться нові сповіщення. Якщо вибрати 0, сповіщення надходитимуть миттєво.

Формат повідомлень

Зв'язок між програмою та віддаленим користувачем або системним адміністратором установлюється через поштові повідомлення чи повідомлення в локальній мережі (за допомогою служби обміну повідомленнями Windows). Установлений за замовчуванням формат сигнальних повідомлень і сповіщень оптимальний для більшості ситуацій. За деяких обставин вам, можливо, знадобиться змінити формат повідомлень про події.

Формат повідомлень про події: формат повідомлень про події, що відображаються на віддалених комп'ютерах.

Формат попереджень про загрози – визначений за замовчуванням формат повідомлень про загрози та сповіщень. Ми не рекомендуємо змінювати цей формат. Проте за деяких обставин (наприклад, якщо використовується автоматична система обробки електронної пошти) може виникнути необхідність змінити формат повідомлень.

Набір символів: перетворює текст повідомлення електронної пошти на кодування символів ANSI залежно від регіональних параметрів Windows (наприклад, windows-1250, Unicode (UTF-8), ACSII 7-bit або кодування для Японії (ISO-2022-JP)). У результаті "á" буде замінено на "a", а невідомі символи — на "?".

Використовувати кодування даних у формат Quoted-printable – джерело повідомлення електронної пошти буде закодовано у формат Quoted-printable (QP), який використовує символи ASCII та може правильно передати спеціальні символи національного алфавіту електронною поштою у 8-бітному форматі (áéíóú).

Ключові слова (рядки, відокремлені символами %) замінюються в повідомленні фактичною інформацією, визначеною для цього сигналу. Можливі ключові слова:

- **%TimeStamp%** – дата й час реєстрації події.
- **%Scanner%** – задіяний модуль.

- **%ComputerName%** – ім'я комп'ютера, на якому зареєстровано сигнал тривоги.
- **%ProgramName%** – програма, яка спричинила тривогу.
- **%InfectedObject%** – ім'я інфікованого файлу, повідомлення тощо.
- **%VirusName%** – ідентифікатор інфекції.
- **%Action%**: дія, виконана у відповідь на виявлення загрози.
- **%ErrorDescription%** – опис події, не пов'язаної з вірусом.

Ключові слова **%InfectedObject%** і **%VirusName%** використовуються лише в попередженнях про загрозу, а **%ErrorDescription%** – лише в повідомленнях про події.

Менеджер профілів

Менеджер профілів використовується у двох розділах ESET Endpoint Antivirus: **Сканування комп'ютера за вимогою** й **Оновлення**.

Сканування комп'ютера за вимогою

Потрібні параметри сканування можна зберегти для майбутнього використання. Рекомендується створити окремі профілі (з різними об'єктами сканування, способами сканування та іншими параметрами) для кожного типу сканування, які регулярно застосовуються.

Щоб створити новий профіль, відкрийте вікно додаткових параметрів (F5) і натисніть **Антивірус > Сканування комп'ютера за вимогою**, а потім – **Змінити** поруч з елементом **Список профілів**. Розкритиме меню **Профіль оновлення** містить перелік усіх наявних профілів сканування. Щоб створити профіль, який точно відповідатиме вашим вимогам, ознайомтесь із вмістом розділу [Налаштування параметрів підсистеми ThreatSense](#), у якому окремо описуються функції кожного параметра сканування.

Припустімо, що вам потрібно створити власний профіль сканування, для якого частково підходить конфігурація функції **Сканування комп'ютера**, але ви не бажаєте сканувати [упаковані](#) або [потенційно небезпечні програми](#) й додатково хочете застосувати параметр **Ретельна очистка**. Введіть ім'я нового профілю у вікні **Менеджер профілів** і натисніть **Додати**. Виберіть новий профіль у розкритому меню **Вибраний профіль** і відкоригуйте решту параметрів відповідно до своїх потреб. Потім натисніть **ОК**, щоб зберегти свій новий профіль.

Оновлення

Редактор профілів у розділі параметрів оновлення дає змогу користувачам створювати нові профілі оновлення. Створювати й використовувати власні спеціальні профілі (відмінні від стандартного **Мій профіль**) слід лише тоді, коли на комп'ютері застосовується кілька способів підключення до серверів оновлення.

Наприклад, портативний комп'ютер, як правило, підключається до локального сервера (дзеркала) в локальній мережі, а в разі відключення від неї (під час відрядження) завантажує оновлення безпосередньо із серверів оновлення ESET. При цьому можуть використовуватися два профілі: перший – для з'єднання з локальним сервером, другий – для підключення до серверів ESET. Налаштувавши ці профілі, перейдіть до меню **Інструменти > Завдання за розкладом** і змініть параметри завдання оновлення. Призначте один профіль первинним, а інший

вторинним.

Профіль оновлення: профіль оновлення, який зараз використовується. Щоб змінити його, виберіть інший профіль із розкритого меню.

Список профілів: дає змогу створювати й видаляти профілі оновлення.

Сполучення клавіш

Між елементами інтерфейсу ESET Endpoint Antivirus можна легко переходити, використовуючи наведені нижче сполучення клавіш.

Сполучення клавіш	Виконана дія
F1	відкрити сторінку довідки
F5	відкрити додаткові параметри
Up/Down	навігація елементами продукту
TAB	перемістити курсор у вікно
Esc	закрити активне діалогове вікно
Ctrl+U	показує інформацію про ліцензію ESET і ваш комп'ютер (докладна інформація для служби технічної підтримки)
Ctrl+R	відновити стандартний розмір вікна та його розміщення на екрані

Діагностичні дані

Модуль діагностики створює дампи робочих процесів ESET у разі збою програми (наприклад, ekrn). Якщо програма аварійно завершує роботу, створюється дамп. Це може допомогти розробникам вирішити різноманітні проблеми з програмою ESET Endpoint Antivirus і налагодити її роботу.

Клацніть розкритве меню **Тип дампу** й виберіть один із трьох доступних параметрів:

- Виберіть **Вимкнути**, щоб вимкнути цю функцію.
- **Мінімальний** (за замовчуванням) – фіксує мінімальний набір корисної інформації, яка може допомогти визначити причину неочікуваного завершення роботи програми. Дамп такого типу може знадобитися, якщо обсяг вільного місця обмежений. Проте аналіз цього файлу може не виявити помилок, які не було безпосередньо спричинено виконуваним потоком, оскільки зібрана інформація є неповною.
- **Повний** – записує весь вміст системної пам'яті в разі аварійного завершення роботи програми. Повний дамп пам'яті може містити дані про процеси, які виконувалися під час створення дампу пам'яті.

Цільовий каталог: каталог збереження файлу дампу в разі збою програми.

Відкрити папку діагностичних даних – натисніть **Відкрити**, щоб відкрити цей каталог у новому вікні Провідника *Windows*.

Створити дамп із даними діагностики – натисніть **Створити**, щоб додати відповідні файли в **Цільовий каталог**.

Розширене ведення журналів

Розширене ведення журналів Scanner: записувати всі події, які виникають під час сканування файлів і папок компонентом сканування комп'ютера або захисту файлової системи в режимі реального часу.

Увімкнути розширене журналювання для контролю пристроїв: записувати всі події контролю пристроїв. Це може допомогти розробникам діагностувати й усувати проблеми, пов'язані з контролем пристроїв.

Увімкнути розширене ведення журналів Direct Cloud — Записувати всі випадки обміну даними між продуктом і серверами Direct Cloud.

Увімкнути розширене ведення журналів для модуля "Захист документів": записувати всі події модуля "Захист документів" для діагностування й вирішення проблем.

Увімкнути розширене ведення журналів ядра: записувати всі події в ядрі ESET (ekrn) для діагностування та вирішення проблем (доступний у версії 7.2 й новіших).

Увімкнути розширене журналювання для процедур ліцензування: записувати всю інформацію, пов'язану з обміном даними з серверами активації та серверами ESET Business Account.

Увімкнути відстеження пам'яті: Записувати всі події, які допоможуть розробникам діагностувати втрати пам'яті.

Увімкнути розширене журналювання для мережі: записувати всі мережеві дані, що проходять через брандмауер у форматі PCAP, щоб розробники могли діагностувати й усувати проблеми, пов'язані з брандмауером.

Увімкнути розширене ведення журналів для операційної системи: збиратиметься додаткова інформація про операційну систему, зокрема про виконувані процеси, активність ЦП, операції з диском тощо. Це допоможе розробникам діагностувати й усувати проблеми з продуктом ESET у вашій операційній системі.

Увімкнути розширене журналювання для фільтрації протоколів: записувати всі дані, що проходять через підсистему фільтрації протоколів у форматі PCAP, щоб розробники могли діагностувати й усувати проблеми, пов'язані з фільтрацією протоколів.

Увімкнути розширене ведення журналів для push-повідомлень — Записувати всі події, які відбуваються під час надсилання push-повідомлень, щоб дозволити діагностику й вирішення проблем.

Увімкнути розширене ведення журналів для модуля "Захист файлової системи в режимі реального часу": записувати всі події модуля "Захист файлової системи в режимі реального часу" для діагностування й вирішення проблем.

Увімкнути розширене журналювання для підсистеми оновлення: записувати всі події, що трапляються під час оновлення. Це дає розробникам змогу діагностувати й усувати проблеми, пов'язані з підсистемою оновлення.

Розташування файлів журналу

C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics

Сканер командного рядку

Антивірусний модуль ESET Endpoint Antivirus можна запустити з командного рядка: вручну (командою `ecds`) або за допомогою пакетного файлу (`bat`).

Використання сканера командного рядка ESET

```
ecds [OPTIONS..] FILES..
```

У разі запуску антивірусного сканера з командного рядка можна використовувати наведені нижче параметри та перемикачі.

Параметри

<code>/base-dir=ПАПКА</code>	завантажити модулі з ПАПКИ
<code>/quar-dir=ПАПКА</code>	ПАПКА карантину
<code>/exclude=МАСКА</code>	виключити файли, що відповідають МАСЦІ, під час сканування
<code>/subdir</code>	сканувати підпапки (за замовчуванням)
<code>/no-subdir</code>	не сканувати підпапки
<code>/max-subdir-level=РІВЕНЬ</code>	максимальний підрівень папок, вкладених у папки для сканування
<code>/symlink</code>	переходити за символічними посиланнями (за замовчуванням)
<code>/no-symlink</code>	пропускати символічні посилання
<code>/ads</code>	сканувати ADS (за замовчуванням)
<code>/no-ads</code>	не сканувати ADS
<code>/log-file=ФАЙЛ</code>	виводити дані з журналу у ФАЙЛ
<code>/log-rewrite</code>	перезаписувати вихідний файл (за замовчуванням – дозаписувати)
<code>/log-console</code>	виводити дані журналу на консоль (за замовчуванням)
<code>/no-log-console</code>	не виводити дані журналу на консоль
<code>/log-all</code>	також реєструвати чисті файли
<code>/no-log-all</code>	не реєструвати чисті файли (за замовчуванням)
<code>/aind</code>	показувати індикатор активності
<code>/auto</code>	сканувати всі локальні диски та автоматично очищувати інфекції

Параметри сканера

<code>/files</code>	сканувати файли (за замовчуванням)
<code>/no-files</code>	не сканувати файли
<code>/memory</code>	сканувати пам'ять
<code>/boots</code>	сканувати завантажувальні сектори

/no-boots	не сканувати завантажувальні сектори (за замовчуванням)
/arch	сканувати архіви (за замовчуванням)
/no-arch	не сканувати архіви
/max-obj-size=РОЗМІР	сканувати лише файли, розмір яких не перевищує значення РОЗМІР у мегабайтах (за замовчуванням 0 = необмежено)
/max-arch-level=РІВЕНЬ	максимальний підрівень архівів в архівах (вкладених архівів) для сканування
/scan-timeout=ЛІМІТ	сканувати архіви не довше, ніж визначено значенням ЛІМІТ у секундах
/max-arch-size=РОЗМІР	сканувати лише файли в архівах, розмір яких не перевищує значення РОЗМІР (за замовчуванням 0 = необмежено)
/max-sfx-size=РОЗМІР	сканувати лише файли в саморозпакувальних архівах, якщо їх розмір не перевищує значення РОЗМІР у мегабайтах (за замовчуванням 0 = необмежено)
/mail	сканувати файли електронної пошти (за замовчуванням)
/no-mail	не сканувати файли електронної пошти
/mailbox	сканувати поштові скриньки (за замовчуванням)
/no-mailbox	не сканувати поштові скриньки
/sfx	сканувати саморозпакувальні архіви (за замовчуванням)
/no-sfx	не сканувати саморозпакувальні архіви
/rtp	сканувати упаковані файли (за замовчуванням)
/no-rtp	не сканувати програми для стиснення виконуваних файлів
/unsafe	сканувати на наявність потенційно небезпечних програм
/no-unsafe	не сканувати на наявність потенційно небезпечних програм (за замовчуванням)
/unwanted	сканувати на наявність потенційно небажаних програм
/no-unwanted	не сканувати на наявність потенційно небажаних програм (за замовчуванням)
/suspicious	перевіряти на наявність підозрілих програм (за замовчуванням)
/no-suspicious	не перевіряти на наявність підозрілих програм
/pattern	використовувати вірусні сигнатури (за замовчуванням)
/no-pattern	не використовувати вірусні сигнатури
/heur	увімкнути евристику (за замовчуванням)
/no-heur	вимкнути евристику
/adv-heur	увімкнути розширену евристику (за замовчуванням)
/no-adv-heur	вимкнути розширену евристику
/ext-exclude=РОЗШИРЕННЯ	не сканувати файли, які мають указані РОЗШИРЕННЯ, розділені двокрапкою

/clean-mode=РЕЖИМ	використовувати РЕЖИМ очищення інфікованих об'єктів Доступні наведені нижче варіанти: <ul style="list-style-type: none"> • none (за замовчуванням) – автоматичне очищення не виконується. • standard – програма ecls.exe спробує автоматично очистити або видалити інфіковані файли. • ретельно – програма ecls.exe спробує автоматично очистити або видалити інфіковані файли без втручання користувача (перед видаленням не відображатиметься запит на підтвердження дії). • суворо – програма ecls.exe видалятиме файли без спроби очищення незалежно від їх типу. • видалення – програма ecls.exe без спроби очищення видалятиме файли, оминаючи важливі (наприклад, системні файли Windows).
/quarantine	копіювати інфіковані файли (у разі очищення) до карантину (як доповнення до операції, що виконується під час чищення)
/no-quarantine	не копіювати інфіковані файли до карантину

Загальні параметри

/help	відкрити довідку та вийти
/version	показати інформацію про версію та вийти
/preserve-time	зберегти час останнього доступу

Коди завершення

0	загроз не знайдено
1	загрози знайдено й очищено
10	деякі файли не вдалося просканувати (можуть становити загрозу)
50	знайдено загрозу
100	помилка

i Коди завершення зі значенням більше 100 означають, що файл не був просканий і, відповідно, може бути інфікований.

ESET CMD

Ця функція активує додаткові команди escmd. Що дає змогу експортувати й імпортувати параметри за допомогою командного рядка (escmd.exe). До цього часу експорт та імпорт параметрів був можливий лише за допомогою [графічного інтерфейсу користувача](#). Конфігурацію ESET Endpoint Antivirus можна експортувати у файл формату *.xml*.

Якщо ESET CMD ввімкнено, доступні два методи авторизації.

- **Немає:** без авторизації. Ми не рекомендуємо цей метод, оскільки тоді можна буде імпортувати будь-яку непідписану конфігурацію, що становить потенційний ризик.
- **Пароль для додаткових параметрів:** для імпорту конфігурації з файлу *.xml* буде потрібен пароль. Цей файл має бути підписаним (див. файл конфігурації *.xml* нижче). Для імпорту нової конфігурації спочатку необхідно вказати пароль у підменю [Параметри](#)

[доступу](#). Якщо параметри доступу не активовано, то пароль не збігатиметься або файл конфігурації у форматі *.xml* не підписуватиметься, тож конфігурація не імпортуватиметься.

Якщо ESET CMD ввімкнено, то для імпорту або експорту конфігурацій ESET Endpoint Antivirus можна використовувати командний рядок. Це можна зробити вручну або створити сценарій для автоматизації.

Щоб використовувати додаткові команди `escmd`, потрібно запустити їх із правами адміністратора або відкрити командний рядок Windows (`cmd`), вибравши пункт **У режимі адміністратора**. Якщо цього не зробити, з'явиться повідомлення **Error executing command**. Окрім того, щоб експортувати конфігурацію, потрібна цільова папка. Команда експорту працює, навіть якщо вимкнено параметр ESET CMD.

Додаткові команди `escmd` можна виконати тільки локально. Призупинити команди `escmd` можна тільки за допомогою клієнтського завдання **Виконати команду** за допомогою ESET PROTECT.

Команда параметрів експорту:
`escmd /getcfg c:\config\settings.xml`

Команда параметрів імпорту:
`escmd /setcfg c:\config\settings.xml`

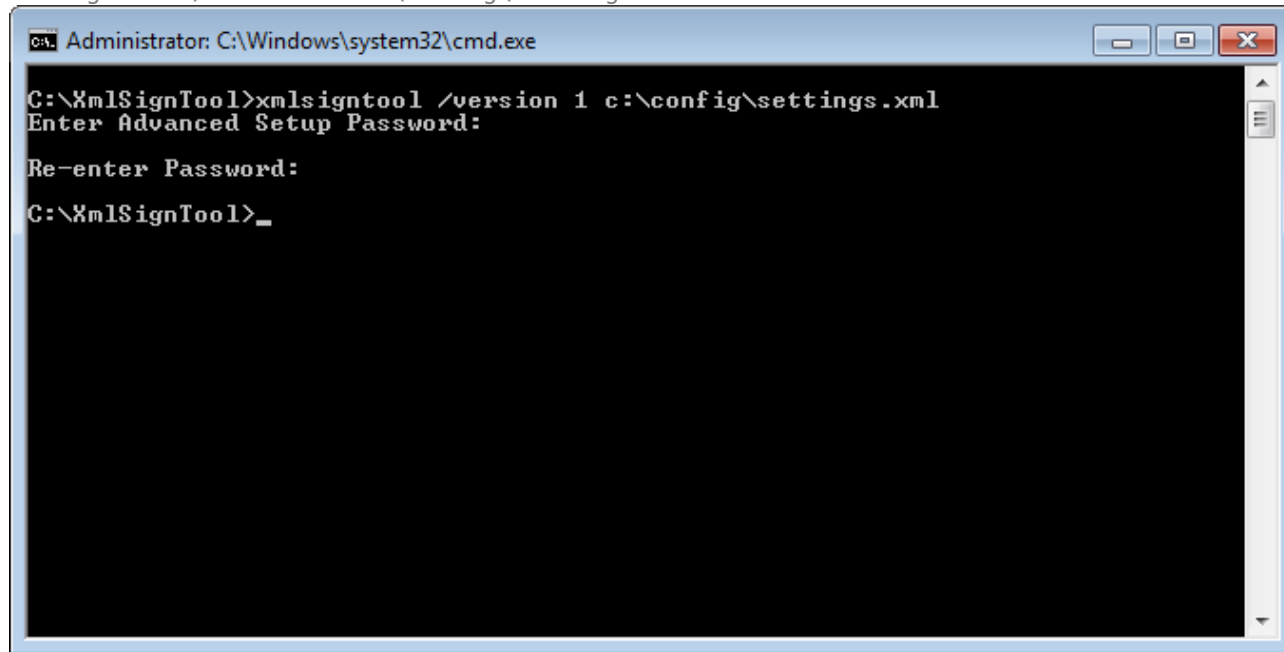
Підписання файлу конфігурації у форматі *.xml*

1. Завантажте виконуваний файл [XmlSignTool](#).
2. Відкрийте командний рядок Windows (`cmd`), вибравши параметр **У режимі адміністратора**.
3. Перейдіть до розташування, в якому збережено файл `xmlsigntool.exe`
4. Щоб підписати файл конфігурації у форматі *.xml*, виконайте таку команду: `xmlsigntool /version 1|2 <xml_file_path>`

Значення параметра `/version` залежить від версії ESET Endpoint Antivirus. Використовуйте параметр `/version 2` для версії 7 і новіших.

5. Коли з'явиться відповідний запит XmlSignTool, введіть пароль для [додаткових параметрів](#), а потім введіть його повторно. Тепер ваш файл конфігурації у форматі *.xml* підписано, тож його можна використовувати для імпорту іншого екземпляра ESET Endpoint Antivirus за допомогою ESET CMD із використанням пароля для авторизації.

Команда для підпису експортованого файлу конфігурації
xmlsigntool /version 2 c:\config\settings.xml



Якщо пароль у підменю [Параметри доступу](#) змінено, і необхідно імпортувати файл конфігурації, раніше підписаний старим паролем, потрібно знову підписати файл конфігурації .xml, використовуючи поточний пароль. Це дозволяє використовувати старий файл конфігурації, не експортуючи його на інший комп'ютер із ESET Endpoint Antivirus перед імпортом.



Ми не рекомендуємо вмикати ESET CMD без авторизації, оскільки тоді можна буде імпортувати будь-яку непідписану конфігурацію. Установіть пароль у меню **Додаткові параметри > Інтерфейс користувача > Параметри доступу**, щоб заборонити несанкціоновану зміну користувачами.

Список команд escmd

Окремі функції безпеки можна ввімкнути й тимчасово вимкнути за допомогою команди запуску завдання клієнта ESET PROTECT. Ці команди не змінюють параметри політики. Після виконання команди або перезапуску пристрою стан усіх параметрів, для яких призупинено дію, буде повернуто до вихідного. Щоб скористатися цією функцією, укажіть команду запуску командного рядка в однойменному полі.

Перегляньте список команд для кожної функції безпеки нижче:

Функція безпеки	Команда тимчасового призупинення	Команда ввімкнення
Захист файлової системи в режимі реального часу	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Захист документів	ecmd /setfeature document pause	ecmd /setfeature document enable
Контроль пристроїв	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable

Функція безпеки	Команда тимчасового призупинення	Команда ввімкнення
Режим презентації	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Технологія «Антируткіт»	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Персональний брандмауер	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Захист мережі від атак (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Захист від ботнетів	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Веб-контроль	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Захист доступу до Інтернету	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Захист поштового клієнта	ecmd /setfeature email pause	ecmd /setfeature email enable
Антиспам	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Захист від фішинг-атак	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Виявлення неактивного стану

Параметри виявлення неактивного стану можна вказати в розділі **Додаткові параметри**. Для цього виберіть **Ядро виявлення > Сканування шкідливого ПЗ > Сканування в неактивному стані > Виявлення неактивного стану**. Ці параметри визначають умови ініціювання [Сканування в неактивному стані](#), коли:

- з'являється заставка;
- комп'ютер заблоковано;
- користувач вийшов із системи.

Щоб активувати чи вимкнути певні умови ініціювання виявлення неактивного стану, скористайтеся відповідними перемикачами.

Параметри імпорту та експорту

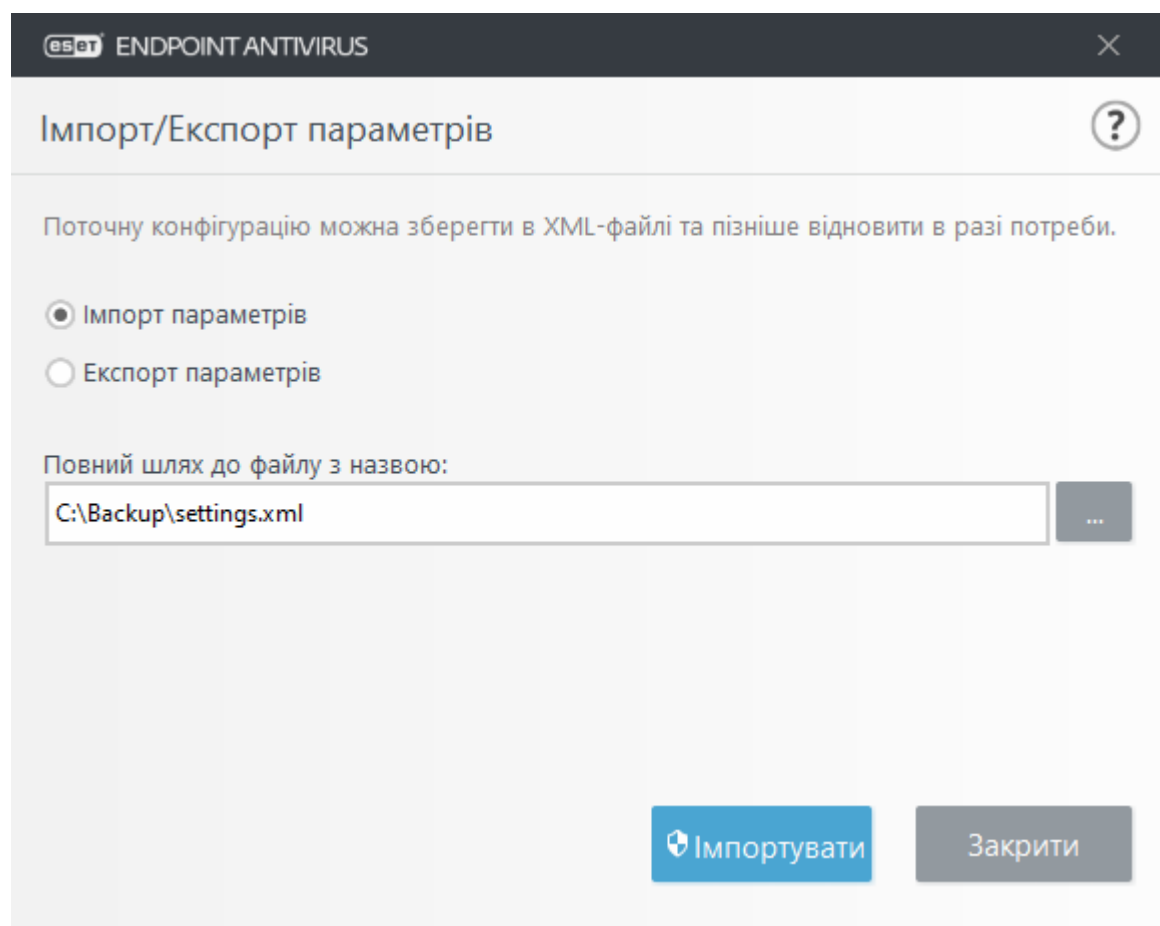
Можна імпортувати або експортувати спеціально визначений файл конфігурації ESET Endpoint Antivirus .xml із меню **Параметри**.

Імпортування й експортування файлів конфігурації є корисними функціями, якщо потрібно створити резервну копію поточної конфігурації ESET Endpoint Antivirus для використання в майбутньому. Опція експорту параметрів також стане в пригоді для користувачів, які бажають застосовувати власну конфігурацію на кількох комп'ютерах: вони зможуть легко перенести ці параметри, імпортувавши файл .xml.

Імпорт конфігурації – це проста процедура. У головному вікні програми натисніть **Параметри > Параметри імпорту/експорту**, після чого виберіть **Параметри імпорту**. Введіть шлях до файлу конфігурації або натисніть кнопку ... і перейдіть до каталогу, де зберігається цей файл.

Аналогічним чином виконується й експорт конфігурації. У головному вікні програми натисніть **Параметри > Параметри імпорту/експорту**. Виберіть **Експорт параметрів**, після чого введіть ім'я файлу конфігурації (наприклад, *export.xml*). Після цього виберіть каталог на комп'ютері, у якому потрібно зберегти файл конфігурації.

i Під час експортування параметрів може виникнути помилка, якщо ви не маєте достатньо прав для запису експортованого файлу в указаний каталог.




Відновлення всіх параметрів за замовчуванням

У розділі "**Додаткові параметри** (F5)" клацніть **За замовчуванням**, щоб повернути всі налаштування програми для всіх модулів до стану, який вони мали б одразу після інсталяції. **За замовчуванням**, щоб повернути всі налаштування програми для всіх модулів до стану, який вони мали б одразу після інсталяції.

Див. також розділ [Імпорт і експорт параметрів](#).

Відновлення всіх параметрів у поточному

розділі

Клацніть круглу стрілку , щоб відновити встановлене ESET значення за замовчуванням для всіх параметрів у поточному розділі.

Зверніть увагу, що після вибору параметра **Відновити параметри за замовчуванням** усі зміни буде втрачено.

Відновити вміст таблиць: після ввімкнення цього параметра правила, завдання або профілі, додані вручну чи автоматично, буде втрачено.

Див. також розділ [Імпорт і експорт параметрів](#).

Помилка під час збереження конфігурації

Це повідомлення про помилку вказує на те, що через помилку параметри не було правильно збережено.

Зазвичай це означає, що користувач, який намагався змінити параметри програми:

- Не має достатніх прав доступу або прав у системі, необхідних для зміни файлів конфігурації й системного реєстру.
 - > Щоб вносити зміни, адміністратор системи має увійти в систему.
- Нещодавно ввімкнув режим навчання в системі запобігання вторгненням (HIPS) чи брандмауері або намагався внести зміни в розділ "Додаткові параметри".
 - > Щоб зберегти конфігурацію й уникнути конфлікту конфігурації, закрийте розділ "Додаткові параметри" без збереження змін і спробуйте внести бажані зміни знову.

Інша типова причина — програма не працює належним чином, пошкоджена, а тому потребує повторного встановлення.

Віддалений моніторинг і керування

Віддалений моніторинг і керування (RMM) — це процес нагляду за програмними системами і контролю їх роботи за допомогою локально інстальованих агентів, доступ до яких може отримати постачальник послуг керування.

ERMM — плагін ESET для RMM

- В інсталяції ESET Endpoint Antivirus за замовчуванням міститься файл `ermm.exe`, розташований у програмі Endpoint у такому каталозі:
`C:\Program Files\ESET\ESET Security\ermm.exe`
- `ermm.exe` — це утиліта командного рядка, яка спрощує керування продуктами Endpoint і обмін даними з будь-яким плагіном RMM.
- Програма `ermm.exe` здійснює обмін даними з плагіном RMM, який у свою чергу обмінюється даними з агентом RMM, підключеним до сервера RMM. За замовчуванням модуль ESET RMM вимкнено.

Додаткові ресурси

- [Командний рядок ERMM](#)
- [Список команд ERMM JSON](#)
- [Активация віддаленого моніторингу та керування ESET Endpoint Antivirus](#)

Плагіни ESET Direct Endpoint Management для сторонніх рішень RMM

Сервер RMM виконується як служба на сторонньому сервері. Більш докладні відомості див. в наведених нижче онлайн-посібниках користувача ESET Direct Endpoint Management:

- [Плагін ESET Direct Endpoint Management для ConnectWise Automate](#)
- [Плагін ESET Direct Endpoint Management для DattoRMM](#)
- [ESET Direct Endpoint Management для Solarwinds N-Central](#)
- [ESET Direct Endpoint Management для NinjaRMM](#)

Командний рядок ERMM

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus 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.

```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:

get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
  scan-info: get information about scan
    -I [--id] arg id of scan to retrieve
  configuration: get product configuration
    -F [--file] arg path where configuration file will be saved
    -O [--format] arg=json format of configuration: json, xml
  update-status: get information about update
  activation-status: get information about last activation

start: start task
  scan: Start on demand scan
    -P [--profile] arg scanning profile
    -T [--target] arg scan target
  activation: Start activation
    -K [--key] arg activation key
    -O [--offline] arg path to offline file
    -T [--token] arg activation token
  deactivation: start deactivation of product
  update: start update of product

set: set configuration to product
  configuration: set product configuration
    -V [--value] arg configuration data (encoded in base64)
    -F [--file] arg path to configuration xml file
    -P [--password] arg password for configuration

Application parameters:
  -H [--help] help
  -L [--log] log application
--debug display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>_

```

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.

Context	Command	Description
get	Get information about products	
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start	Start task	
	scan	Start on demand scan

Context	Command	Description
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		Set options for product
	configuration	Set configuration to product

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.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

Список команд ERMM JSON

- [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](#)

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

```
{
  "command": "get_protection_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "statuses": [{
      "id": "EkrrnNotActivated",
      "status": 2,
      "priority": 768,
      "description": "Product not activated"
    }],
    "status": 2,
    "description": "Security alert"
  },
  "error": null
}
```

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":"0734",
      "date":"2017-03-20"
    },{
      "id":"LOADER32",
      "description":"Update module",
      "version":"1009",
      "date":"2016-12-05"
    },{
      "id":"PERSEUS32",
      "description":"Antivirus and antispysware 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",
      "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
}

```

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",
    "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
}
```

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

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

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"
  }
}
```

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
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, running, failure }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
  "command": "get_activation_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "status": "success"
  },
  "error": null
}
```

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":{
      "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
}
```

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

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdmVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
  "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
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

```
call
{
  "command": "start_scan",
  "id": 1,
  "version": "1",
  "params": {
    "profile": "Smart scan",
    "target": "c:\\\"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "task_id": 458752
  },
  "error": null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value
------	-------

key	Activation key
offline	Path to offline file

Example

call
<pre>{ "command": "start_activation" "id": 1, "version": "1", "params": { "key": "XXXX-XXXX-XXXX-XXXX-XXXX" } }</pre>

result
<pre>{ "id": 1, "result": { }, "error": null }</pre>

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call
<pre>{ "command": "start_deactivation", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { }, "error": null }</pre>

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
<pre>{ "command": "start_update", "id": 1, "version": "1" }</pre>
result
<pre>{ "id": 1, "result": { }, "error": { "id": 4, "text": "Task already running." } }</pre>

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

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

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
}
```

Поширені запитання

У цьому розділі розглядаються питання та проблеми, які виникають у користувачів найчастіше. Натисніть назву теми, щоб дізнатися, як вирішити проблему:

- [Оновлення ESET Endpoint Antivirus](#)
- [Активація ESET Endpoint Antivirus](#)
- [Використання поточних облікових даних для активації нового продукту](#)
- [Видалення вірусу з ПК](#)
- [Створення нового запланованого завдання](#)
- [Додавання до розкладу завдання щотижневого сканування комп'ютера](#)
- [Керування сповіщеннями та інтерактивними попередженнями](#)
- [Підключення мого продукту до ESET PROTECT](#)
 - [Режим заміщення](#)
 - [Застосування рекомендованої політики для ESET Endpoint Antivirus](#)
- [Налаштування дзеркала](#)
- [Оновлення до ОС Windows 10 за допомогою ESET Endpoint Antivirus](#)
- [Активація віддаленого моніторингу та керування](#)
- [Блокування завантаження певних типів файлів з Інтернету](#)
- [Згорання інтерфейсу користувача ESET Endpoint Antivirus](#)

Якщо ви не знайшли потрібного рішення на наведених вище сторінках довідки, спробуйте пошукати по всій довідці ESET Endpoint Antivirus за ключовим словом або фразою, що описує проблему.

Якщо ви все одно не знайшли способу вирішення проблеми, відвідайте [базу знань ESET](#), яка

містить відповіді на більшість поширених запитань.

- [Рекомендації щодо захисту від шифрувальників файлів \(програм-вимагачів\)](#)
- [Поширені питання щодо ESET Endpoint Security та ESET Endpoint Antivirus](#)
- [Які адреси й порти у своєму брандмауері від стороннього постачальника потрібно відкрити, щоб забезпечити повноцінну функціональність продукту ESET?](#)

У разі необхідності можна зв'язатися з інтерактивним центром технічної підтримки та повідомити про свою проблему або поставити запитання. Посилання на нашу контактну онлайн-форму знаходиться на вкладці **Довідка та підтримка** головного вікна програми.

Запитання й відповіді щодо автоматичних оновлень



Додаткову інформацію про оновлення продукту в ESET Endpoint Antivirus див. в статті бази знань ESET за таким посиланням:

- [Чим оновлення продукту ESET відрізняється від типів випуску?](#)

Чи оновлюватимуться комп'ютери автоматично? Коли завантажуються оновлення — до чи після перезавантаження?

Оновлення завантажуються до перезавантаження. На цьому етапі також підготовлюються оновлені файли. Після перезавантаження оновлені файли залишатимуться лише підготовленими для використання, а поточна інсталювана версія забезпечуватиме безперервний захист. Відповідні зміни застосовуються після наступного запуску продукту ESET Endpoint.

У мене приблизно 3000 комп'ютерів. Чи всі комп'ютери одночасно завантажуватимуть оновлення? Чи можна використовувати проксі-сервер для автоматичного оновлення на багатьох комп'ютерах?

Для великих мереж ESET пропонує інструмент "Дзеркало" і проксі-сервери, які дадуть змогу завантажувати оновлення з Інтернету лише один раз, а потім розповсюджувати їх локально. Оновлення мають менший розмір (зазвичай 5–10 МБ); ESET обмежуватиме потоки оновлень протягом перших кількох тижнів із моменту їхнього випуску. Тому завантаження не розпочнеться одночасно на всіх клієнтах після безпосереднього підключення до серверів ESET.

Чи можна вибрати, скільки комп'ютерів оновлюватимуться автоматично або вказати певні комп'ютери для оновлення? Я хочу, щоб завантаження виконувалося не більше ніж на десяти комп'ютерах на годину або оновити десять комп'ютерів зараз, а інші комп'ютери — через кілька днів.

Керовані середовища мають політику автоматичного оновлення. У цій політиці можна вказати найновішу бажану версію. Окрім того, підтримуються символи узагальнення (наприклад, 9.0.2032.*). Більш докладно див. в розділі "Автоматичні оновлення" в онлайн-довідці для [ESET PROTECT](#) або [ESET PROTECT Cloud](#). На жаль, наразі немає інших параметрів для обмеження

автоматичних оновлень. Для кількох груп можна призначити кілька політик.

Чи налаштовуються автоматичні оновлення лише за допомогою політики? Чи можна вимкнути політику, якщо не потрібно оновлювати продукт ESET?

Якщо для продукту ESET Endpoint доступне поточне виправлення безпеки й стабільності, продукт буде оновлено, навіть якщо автоматичні оновлення вимкнено (згідно з умовами, визначеними у відповідній ліцензійній угоді з кінцевим користувачем). ESET використовує [поточні виправлення безпеки й стабільності](#) для усунення критичних проблем і забезпечення максимальної безпеки й стабільності для вашого продукту ESET.

Можна призначити політику автоматичного оновлення будь-якій групі робочих станцій незалежно від їхньої поточної конфігурації автоматичного оновлення. У некерованих середовищах користувач може локально налаштувати автоматичні оновлення на екрані "Додаткові параметри" в продукті ESET Endpoint.

Що робити, якщо я налаштовую політику для використання найстарішої доступної версії? Чи оновлюватиме після цього продукт ESET мої продукти?

Поточні й критичні виправлення (оновлення безпеки й стабільності) дещо відрізняються за категоріями оновлення. Після прийняття параметрів користувача регулярні виправлення призначаються для автоматичних оновлень зі стандартним пріоритетом. Критичні виправлення застосовуються з найвищим пріоритетом незалежно від параметрів користувача.

Як оновлення працювали в автономному режимі? Коли користувачі використовують офлайн-репозиторій?

Автономний репозиторій також містить файли .dup і .fup. Розділ репозиторію має бути завантажений інструментом «Дзеркало», а не через оновлення модуля. Додаткову інформацію див. в [цій статті бази знань ESET](#).

Яким чином стає відомо, що потрібно оновити продукти ESET? Відповідна інформація надходить із репозиторію? Певні дані надсилаються на сервери? Якщо ESET планує випустити оновлення через місяць після випуску версії, чи воно буде доступним у всьому світі? Чи готові для цього сервери ESET?

Продукти ESET завантажують автоматичні оновлення з репозиторію. Сервери готові до цього, оскільки розмір критичних оновлень складає лише кілька КБ. ESET не застосовує обмеження до критичних оновлень на серверах репозиторію. Проте є можливість обмежувати оновлення сервера, якщо автоматичні оновлення мають більший розмір. У таблиці нижче наведено розміри поточних виправлень для різницевого автоматичного оновлення:

Попередня версія	Нова версія	Розмір
9.0.2032.2	9.0.2032.6	420 КБ

Попередня версія	Нова версія	Розмір
8.1.2037.2	9.0.2032.2	6.5 МБ
8.0.2028.0	9.0.2032.2	11.5 МБ

Якщо не вдається виконати різницеве автоматичне оновлення, продукт ESET ініціює повне оновлення. Це все ще автоматичне оновлення з гарантією функціональності, проте замість файлу .dip буде завантажено файл .fur більшого розміру. Для версії 9.0.2032.2 його розмір складає 27 МБ. Проте такі сценарії є поодинокими.

Чи буде застосовуватися обмеження для випуску оновлення ESET Endpoint Security/ESET Endpoint Antivirus? Якщо так, протягом якого часу оновлення може обмежуватися після випуску?

ESET обмежує оновлення протягом перших кількох тижнів після випуску нової версії, щоб зменшити навантаження на наші сервери й рівномірно розповсюджувати нову версію.

Автоматичні оновлення стануть одним з основних методів оновлення. Яким чином працює?

ESET прагне, щоб функцією автоматичних оновлень користувалося якомога більше клієнтів. За наявності великої кількості старих версій важко забезпечувати підтримку. Автоматичні оновлення працюють за простим принципом: файли .dip завантажуються під час першої перевірки оновлення модуля. Під час оновлення продукт є повнофункціональним і безперервно захищає комп'ютер. Нова версія активується після перезавантаження комп'ютера. У ESET PROTECT (на боці сервера) за допомогою політики можна вказати найновішу версію для оновлення. Окрім того, можна використовувати групові символи. Докладнішу інформацію див. в розділі "Автоматичні оновлення" в онлайн-довідці для [ESET PROTECT](#) або [ESET PROTECT Cloud](#).

Чи правильно працює автоматичне оновлення 1/10? Наразі я використовую ESET Endpoint Security 8.0.2028.1. Якщо запусяться автоматичні оновлення, до якої версії буде оновлено продукт?

Оновлення продуктів із використанням автоматичних оновлень може затримуватися через виконання завдання на серверах репозиторію. Якщо у випущеному оновленні продукту є можливість регулювання, автоматичні перевірки оновлення можуть отримати її трохи згодом. Якщо оновлення вважається безпечним і стабільним, обмеження можна зменшити або повністю видалити, щоб усі інші клієнти отримали оновлення.

Для кожного оновлення обмеження може мати різну тривалість. Вона залежить від того, скільки клієнтів надсилають запит на оновлення, від завантаження наших серверів та інших факторів. Ця процедура постійно змінюється. Окрім того, оскільки функція автоматичних оновлень є новою, напевно, ми будемо вдосконалювати відповідну процедуру, щоб покращити роботу клієнта.

Якщо запустити комп'ютер о 8:45 і вимкнути його о 17:00, коли запуститься автоматичне оновлення?

Під час наступного запланованого оновлення модуля, але не частіше, ніж раз на кожні 24 години.

Якщо під час виконання автоматичних оновлень комп'ютер вимкнеться, коли відновиться оновлення?

Оновлення запуститься під час наступного запланованого вікна оновлення. Є ефективний відмовостійкий механізм для автоматичного оновлення (раніше — uRSU). Після завантаження оновлення й перезавантаження комп'ютера оновлені файли залишатимуться готовими для використання, а поточна інстальована версія забезпечуватиме безперервний захист. Відповідні зміни застосовуються після наступного запуску продукту ESET Endpoint.

Як миттєво запускати автоматичні оновлення без очікування регулярного підключення кожні 24 години? Чи є інші способи, окрім як скористатися параметром "Перевірити наявність оновлень"?

Процедуру автоматичного оновлення можна запустити вручну лише в такий спосіб: відкрийте головне вікно програми й клацніть **Оновлення > Перевірити наявність оновлень**. Усі інші способи запустити оновлення модулів базуються на політиці планувальника автоматичного оновлення з інтервалом 24 години. Наразі неможливо віддалено запустити завантаження автоматичного оновлення. Ми додамо цю функцію в майбутньому.

Оновлення ESET Endpoint Antivirus

Оновлення ESET Endpoint Antivirus можна виконати вручну або автоматично. Щоб запустити оновлення, натисніть кнопку **Оновити** у головному вікні програми, потім — кнопку **Перевірка наявності оновлень**.

Під час інсталяції програми за замовчуванням створюється завдання автоматичного оновлення, яке виконується щогодини. Для зміни інтервалу оновлення перейдіть до розділу **Інструменти > Планувальник** (більш докладну інформацію про планувальник див. [за цим посиланням](#))

Активація ESET Endpoint Antivirus

Після завершення інсталяції з'явиться запит на активацію продукту.

Існує кілька способів активації продукту. Доступність певного сценарію активації у вікні активації може різнитися залежно від країни вашого перебування, а також засобів поширення (веб-сторінка ESET, файл інсталяції .msi або .exe тощо).

Щоб активувати свою копію ESET Endpoint Antivirus безпосередньо в інтерфейсі програми, відкрийте головне вікно ESET Endpoint Antivirus і в головному меню перейдіть до розділу **Довідка та підтримка > Активувати продукт** або **Статус захисту > Активувати продукт**.


Щоб активувати ESET Endpoint Antivirus, можна скористатися одним із наведених нижче методів.


- **Скористайтеся придбаним ліцензійним ключем** – це унікальний рядок символів у форматі XXXX-XXXX-XXXX-XXXX-XXXX, який використовується для ідентифікації власника ліцензії та її активації.
- **ESET Business Account:** обліковий запис, створений на порталі [ESET Business Account](#) з використанням облікових даних (адреса електронної пошти + пароль). У такий спосіб можна керувати кількома ліцензіями з єдиного центру.
- **Автономна ліцензія** – автоматично згенерований файл, який буде передано в продукт ESET для надання інформації про ліцензію. Якщо існує можливість завантаження файлу автономної ліцензії (.If), його можна використовувати для активації без підключення до Інтернету. Кількість автономних ліцензій відніматиметься від загального числа доступних. Докладнішу інформацію про створення файлу автономної ліцензії наведено в [посібнику користувача ESET Business Account](#).

Натисніть **Активувати пізніше**, якщо ваш комп'ютер входить до керованої мережі, адміністратор якої віддалено активує ліцензію за допомогою ESET PROTECT. Цей параметр також можна використовувати, якщо потрібно активувати клієнт пізніше.

Якщо у вас є ім'я користувача й пароль, які використовувалися для активації продуктів ESET більш ранніх версій, і ви не знаєте, як активувати ESET Endpoint Antivirus, [перетворіть застарілі облікові дані в ліцензійний ключ](#).

[Не вдалося активувати продукт?](#)

Ви завжди можете змінити інформацію про ліцензію на продукт. Для цього в головному меню натисніть **Довідка та підтримка > Змінити ліцензію**. Відобразиться ідентифікатор відкритої ліцензії, який потрібно вказати у відповідь на запит служби підтримки ESET. Ім'я користувача, під яким зареєстровано ваш комп'ютер, можна знайти в розділі **Про програму**. Щоб відкрити його, натисніть правою кнопкою миші піктограму в системному треї .

 ESET PROTECT 7.2 або ESET PROTECT 9 може без попередження активувати клієнтські комп'ютери, використовуючи надані адміністратором ліцензії. Відповідні інструкції наведено в [онлайн-довідці з ESET PROTECT](#).

Введення ліцензійного ключа під час активації

Автоматичні оновлення допомагають убезпечити користувачів. ESET Endpoint Antivirus оновлюватиметься лише після активації за допомогою параметра **Ліцензійний ключ**.

Якщо після інсталяції не ввести ліцензійний ключ, продукт не активується. Дані про ліцензію можна змінити в головному вікні програми. Для цього натисніть **Довідка та підтримка > Активувати ліцензію**. У вікні активації введіть дані, отримані з комплектом постачання продукту ESET.

Коли вводите **Ліцензійний ключ**, важливо стежити за відсутністю помилок.

- Ліцензійний ключ – це унікальний рядок символів у форматі XXXX-XXXX-XXXX-XXXX-XXXX, який використовується для ідентифікації власника ліцензії та її активації.

Ми рекомендуємо скопіювати ліцензійний ключ із повідомлення про реєстрацію, щоб не помилитися.

Вхід до ESET Business Account

Обліковий запис адміністратора безпеки створюється на порталі ESET Business Account із використанням вашої **адреси електронної пошти** й **пароля** та дає змогу контролювати авторизацію всіх ролей. Обліковий запис адміністратора безпеки дозволяє керувати кількома ліцензіями. Якщо у вас немає його, натисніть **Створити обліковий запис**, після чого вас буде переспрямовано на портал ESET Business Account, у систему якого можна увійти за допомогою своїх облікових даних.

Якщо ви забули пароль, натисніть посилання **Забули пароль?**, і вас буде переспрямовано на портал ESET Business Account. Уведіть свою адресу електронної пошти й натисніть **Увійти** для підтвердження. Після цього ви отримаєте інструкції зі скидання пароля.

Використання попередніх облікових даних ліцензії для активації новішого продукту ESET Endpoint

Якщо ви вже маєте ім'я користувача й пароль і бажаєте отримати ліцензійний ключ, перейдіть на [ESET Business Account портал](#), де можна пов'язати поточні облікові дані з новим ліцензійним ключем.

Видалення вірусу з ПК

Якщо комп'ютер виявляє ознаки зараження шкідливою програмою, наприклад, працює повільніше, часто "зависає" тощо, рекомендується виконати наведені нижче дії.

1. У головному вікні програми натисніть **Перевірка комп'ютера**.
2. Натисніть **Smart-сканування**, щоб розпочати сканування системи.
3. Після завершення сканування перегляньте журнал, де вказана кількість просканиваних, заражених і очищених файлів.
4. Щоб просканувати лише певну частину диска, натисніть **Вибіркова перевірка** та виберіть об'єкти для перевірки на наявність вірусів.

Додаткові відомості див. у [цьому посібнику бази знань ESET](#), вміст якого регулярно оновлюється.

Створення нового запланованого завдання

Щоб створити нове завдання, у меню **Інструменти > Планувальник** виберіть **Додати завдання** або натисніть праву кнопку миші для виклику контекстного меню й виберіть пункт **Додати**. Запланувати можна завдання п'ятих різних типів:

- **Запуск зовнішньої програми:** планування запуску зовнішньої програми.
- **Обслуговування журналу** – окрім усього іншого, у журналах також містяться залишки видалених записів. Це завдання регулярно оптимізує записи в журналах для підвищення ефективності роботи.
- **Перевірка файлів під час запуску системи:** перевірка файлів, що запускаються автоматично під час завантаження системи або входу до облікового запису.
- **Створити знімок стану системи:** створення знімка системи засобом ESET SysInspector, який збирає докладну інформацію про системні компоненти (наприклад, драйвери, програми) й оцінює рівень ризику для кожного з них.
- **Сканування комп'ютера за вимогою:** сканування файлів і папок на комп'ютері.
- **Оновлення:** планування завдання оновлення, у рамках якого оновлюються модулі програми.

Оскільки найчастіше використовуються завдання **Оновлення**, нижче описано, як його додати.

У розкритому меню **Заплановане завдання** виберіть пункт **Оновлення**. Заповніть поле **Ім'я завдання** й натисніть **Далі**. Виберіть періодичність виконання завдання. Доступні наведені нижче варіанти: **Одноразово**, **Багаторазово**, **Щодня**, **Щотижня** та **За умови виникнення події**. Виберіть **Не запускати завдання, якщо комп'ютер працює від батареї**, щоб зменшити використання системних ресурсів, коли портативний комп'ютер працює від батареї. Завдання буде виконуватись у вибраний день і час відповідно до параметрів розділу **Запуск завдання**. Далі слід визначити, яку дію виконувати, якщо завдання не може бути виконане або завершене в запланований час. Можна вибрати один із наведених нижче варіантів.

- **Під час наступного запланованого виконання**
- **Якомога швидше**
- **Негайно, якщо час після останнього запуску перевищує зазначений інтервал** (інтервал можна вибрати за допомогою повзунка **Минуло часу після останнього запуску**)

У наступному кроці буде показано загальні відомості про поточне заплановане завдання. Натисніть **Готово**, завершивши вносити зміни.

Відкриється діалогове вікно, де користувач може вибрати профілі, які застосовуватимуться для запланованого завдання. Тут можна визначити основний й альтернативний профілі. Альтернативний профіль застосовується, якщо завдання неможливо виконати з використанням основного профілю. Підтвердьте зміни, натиснувши **Готово**. Нове завдання буде додано до списку поточних запланованих завдань.

Додавання до розкладу завдання щотижневого сканування комп'ютера

Щоб запланувати завдання, яке має регулярно виконуватися, відкрийте головне вікно програми й клацніть **Інструменти > Розклад**. Нижче наведено короткі інструкції щодо того, як запланувати завдання зі сканування локальних дисків комп'ютера раз на тиждень. Докладніші інструкції наведено в [цій статті бази знань](#).

Щоб додати до розкладу завдання сканування, виконайте наведені нижче дії.

1. Натисніть **Додати** на головному екрані розділу "Завдання за розкладом".

2. У розкривному меню виберіть елемент **Сканування комп'ютера за вимогою**.
3. Введіть назву завдання та виберіть параметр **Щотижня для періодичності виконання завдання**.
4. Установіть день і час виконання завдання.
5. Виберіть **Запустити завдання за першої нагоди**, щоб виконати завдання пізніше, якщо це не вдалося зробити вчасно з якихось причин (наприклад, комп'ютер було вимкнено).
6. Перегляньте загальні відомості про заплановане завдання й клацніть **Готово**.
7. У розкривному меню **Об'єкти** виберіть опцію **Локальні диски**.
8. Натисніть **Готово**, щоб застосувати завдання.

Підключення ESET Endpoint Antivirus до ESET PROTECT

Якщо ESET Endpoint Antivirus інстальовано на комп'ютері, щоб налаштувати підключення через ESET PROTECT, на клієнтській робочій станції також потрібно інстальовати агент ESET Management. Він є невід'ємною складовою будь-якого клієнтського рішення, що здійснює комунікацію з сервером ESET PROTECT.

- [Інсталюйте або розгорніть агент ESET Management на клієнтських робочих станціях](#)

Див. також:

- [Документація для робочих станцій, якими керують віддалено](#)
- [Режим заміщення](#)
- [Застосування рекомендованої політики для ESET Endpoint Antivirus](#)


Режим заміщення

Користувачі продуктів ESET Endpoint (версії 6.5 або новішої) для Windows, інстальованих на комп'ютері, можуть застосовувати функцію заміщення. Режим заміщення дає змогу на рівні клієнтського комп'ютера змінювати параметри в інстальованому продукті ESET, навіть якщо до них застосовано політику. Цей режим можна ввімкнути для певних користувачів AD або захистити його паролем. Функцію не можна ввімкнути відразу більше ніж на 4 години.

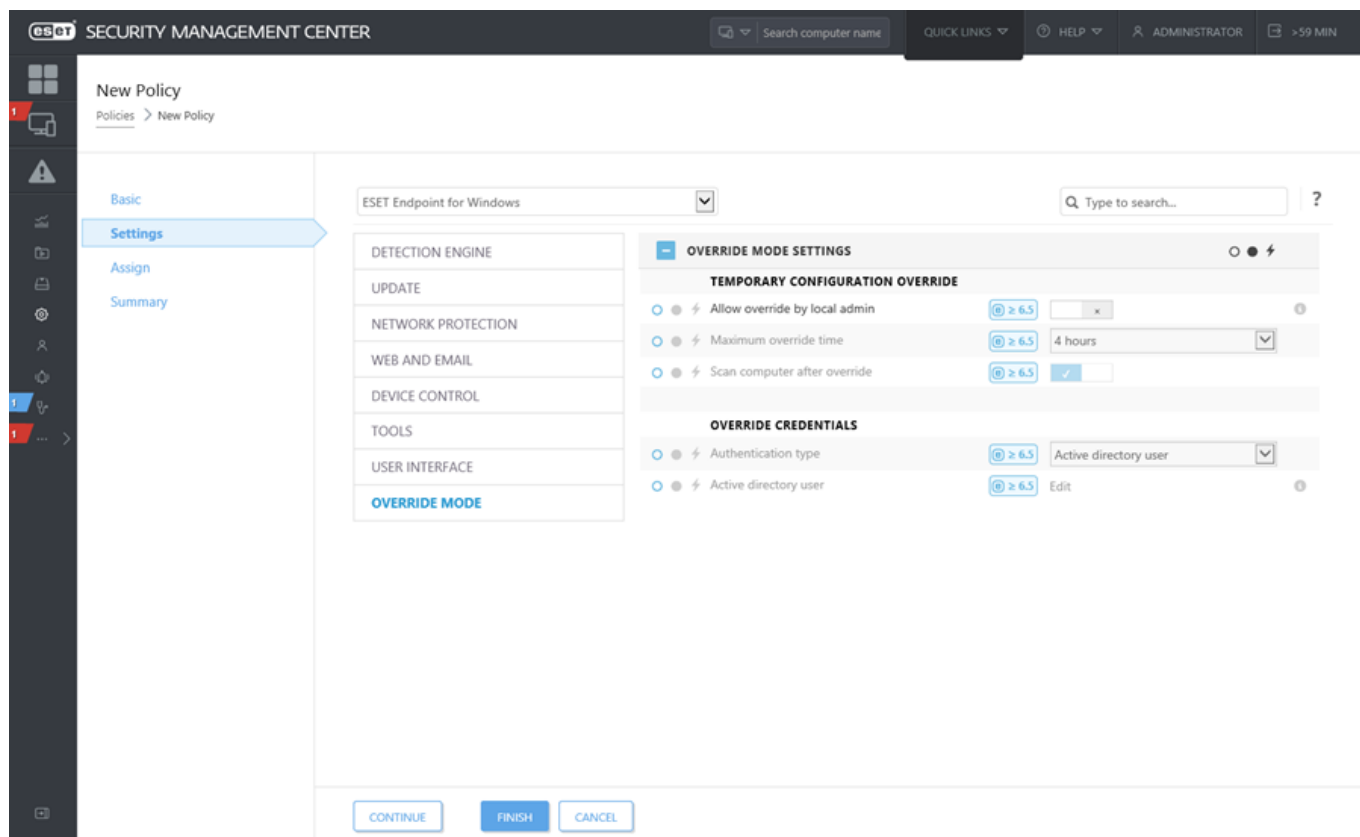


- Після ввімкнення режиму заміщення, його неможливо зупинити на веб-консолі ESET PROTECT. Режим заміщення вимикається автоматично після завершення проміжку часу заміщення. Його також можна вимкнути на клієнтській машині.
- Користувачу, який використовує режим заміщення, необхідно також мати права адміністратора у Windows. В іншому разі користувач не може зберегти зміни в налаштуваннях ESET Endpoint Antivirus.
- Група автентифікації Active Directory підтримується для версії ESET Endpoint Antivirus 7.0.2100.4 й новіших.

Щоб установити **режим заміщення**, виконайте вказані нижче дії.

1. Виберіть пункти  **Політики** > **Створити політику**.
2. У розділі **Базовий** введіть **назву** й **опис** для цієї політики.
3. У розділі **Параметри** виберіть **ESET Endpoint для Windows**.

4. Натисніть **Режим заміщення** та налаштуйте для нього правила.
5. У розділі **Призначити** виберіть комп'ютер або групу комп'ютерів, для яких потрібно застосувати цю політику.
6. Перегляньте параметри в розділі **Зведення** та натисніть **Готово**, щоб застосувати політику.



Якщо в Івана проблеми з кінцевими параметрами, оскільки вони блокують деякі важливі функції або веб-доступ на комп'ютері, адміністратор може дозволити Івану замістити кінцеву політику та вручну налаштувати ці параметри в себе на комп'ютері. Після цього ESET PROTECT може надіслати запит на нові параметри, щоб адміністратор міг створити на основі них нову політику.

Виконайте наведені нижче дії.

1. Виберіть пункти **Політики > Створити політику**.
2. Заповніть поля **Назва** й **Опис**. У розділі **Параметри** виберіть **ESET Endpoint для Windows**.
3. Натисніть **Режим заміщення**, увімкніть режим заміщення на одну годину й виберіть Івана як користувача AD.
4. Застосуйте політику до комп'ютера Івана та натисніть **Готово**, щоб зберегти політику.
5. Іван має ввімкнути **Режим заміщення** у своєму кінцевому продукті ESET і вручну змінити параметри на комп'ютері.
6. На веб-консолі ESET PROTECT виберіть **Комп'ютери**, комп'ютер Івана, а потім – **Показати подробиці**.
7. У розділі **Конфігурація** натисніть **Надіслати запит на конфігурацію**, щоб запланувати клієнтське завдання та якнайшвидше отримати конфігурацію від клієнта.
8. Через деякий час з'явиться нова конфігурація. Натисніть продукт, параметри якого слід зберегти, а потім – **Відкрити конфігурацію**.
9. Перегляньте параметри, а потім натисніть **Конвертувати в політику**.
10. Заповніть поля **Назва** й **Опис**.
11. Якщо потрібно, змініть параметри в розділі **Параметри**.
12. У розділі **Призначити** можна застосувати цю політику до комп'ютера Івана чи іншого користувача.
13. Натисніть **Готово**, щоб зберегти параметри.
14. Щойно заміщена політика стане непотрібною, видаліть її.

Застосування рекомендованої політики для ESET Endpoint Antivirus

Після підключення ESET Endpoint Antivirus до ESET PROTECT рекомендується застосувати рекомендовану або настроювану [політику](#).

Для ESET Endpoint Antivirus є кілька вбудованих політик:


Політика	Опис
Антивірус — збалансована	Конфігурація захисту, рекомендована для більшості налаштувань.
Антивірус — максимальний захист	Переваги машинного навчання, глибокої перевірки поведінки й фільтрації SSL. Це покращує ефективність виявлення потенційно небезпечних, небажаних і підозрілих програм.
Хмарна система репутації й зворотного зв'язку	Активує хмарну систему репутації ESET LiveGrid® , а також систему зворотного зв'язку, що покращує виявлення найновіших загроз і допомагає ділитися відомостями про шкідливі чи потенційні загрози для подальшого аналізу.
Контроль пристроїв — максимальний захист	Усі пристрої заблоковано. Підключення кожного конкретного пристрою має бути дозволено адміністратором.
Контроль пристроїв — лише читання	Усі пристрої можна тільки прочитати. Запис недозволений.

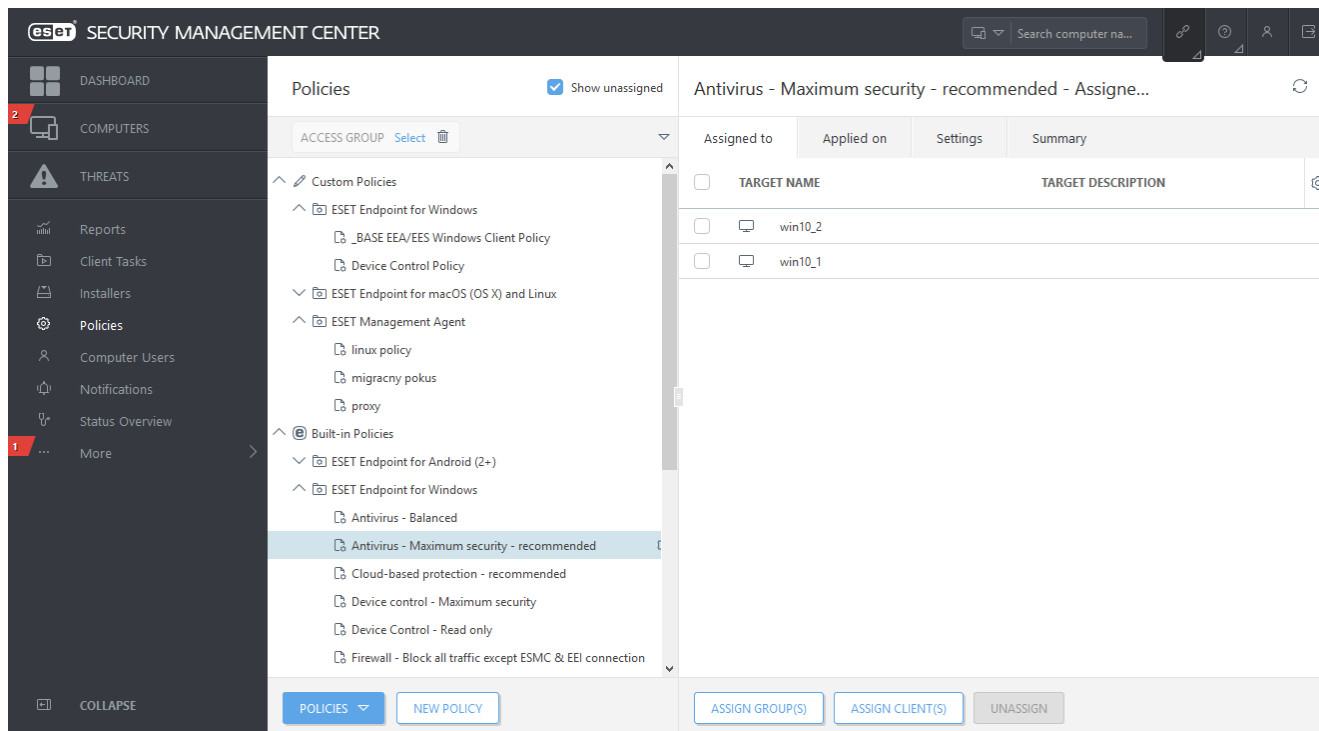
Політика	Опис
Брандмауер: блокування всього трафіку, окрім ESET PROTECT і підключення ESET Inspect	Заблоковано весь трафік, за винятком підключень до ESET PROTECT і ESET Inspect Server (тільки в ESET Endpoint Security).
Ведення журналу — запис всіх подій до журналу	Цей шаблон забезпечує доступність усіх журналів для адміністратора, коли б вони йому не знадобились. У журнал записуватиметься вся активність, навіть із мінімальною детальністю повідомлень, зокрема активність системи запобігання вторгненням (HIPS), параметри ThreatSense і операції брандмауера. Журнали автоматично видаляються кожні 90 днів.
Ведення журналу — запис тільки важливих подій	Політика забезпечує запис до журналу попереджень, помилок і критичних подій. Журнали автоматично видаляються кожні 90 днів.
Видимість — збалансована	Параметри видимості за замовчуванням. Статуси й сповіщення ввімкнено.
Видимість — невидимий режим	Вимкнено сповіщення, оповіщення тривоги, графічний інтерфейс користувача , інтеграцію до контекстного меню. Програма egui.exe не виконується. Підходить для керування виключно з ESET PROTECT Cloud .
Видимість — скорочена взаємодія з користувачем	Вимкнено статуси, вимкнено сповіщення, графічний інтерфейс користувача відображається.

Щоб установити політику **Антивірус — максимальний захист**, яка застосовує більше 50 рекомендованих параметрів для ESET Endpoint Antivirus на ваших робочих станціях, дотримуйтеся наведених нижче інструкцій:

i Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

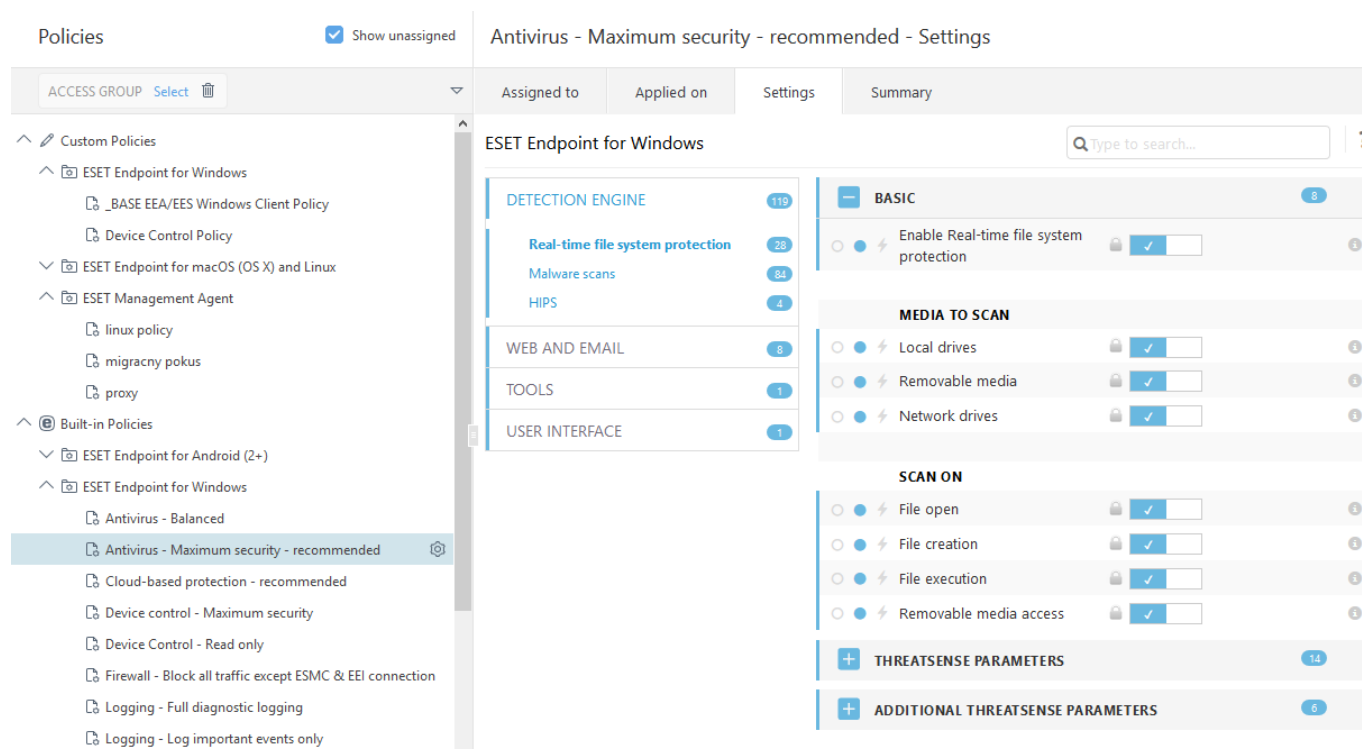
- [Застосування рекомендованої або попередньо визначеної політики для ESET Endpoint Antivirus з використанням ESET PROTECT](#)

1. Відкрийте веб-консоль ESET PROTECT.
2. Відкрийте розділ  **Політики** й розгорніть список **Built-in Policies (Вбудовані політики)** > **ESET Endpoint for Windows**.
3. Клацніть **Антивірус — максимальний захист — рекомендована**.
4. На вкладці **Assigned to (Кому призначено)** клацніть **Assign client(s) (Призначити клієнтів)** або **Assign groups(s) (Призначити групи)** й виберіть комп'ютери, для яких необхідно призначити цю політику.



Щоб дізнатися, які параметри застосовані до цієї політики, відкрийте вкладку **Параметри** й розгорніть дерево "Додаткові параметри".

- Блакитна крапка свідчить про те, що параметри для цієї політики були змінені
- У блакитній рамці відображається кількість параметрів, змінених для цієї політики
- [Докладніше про політики ESET PROTECT](#)



Налаштування дзеркала

ESET Endpoint Antivirus можна налаштувати на зберігання копій файлів оновлень обробника виявлення для їх подальшого розповсюдження на робочих станціях, на яких запущено ESET Endpoint Security або ESET Endpoint Antivirus.

Налаштування ESET Endpoint Antivirus на виконання функцій дзеркала для поширення оновлень через внутрішній HTTP-сервер

1. Натисніть клавішу **F5**, щоб відкрити вікно «Додаткові параметри» й розгорніть елементи **Оновлення > Профілі > Дзеркало оновлення**.
2. Розгорніть елемент **Оновлення** й переконайтеся, що в розділі **Оновлення модулів** вибрано параметр **Автоматичний вибір**.
3. Розгорніть **Дзеркало оновлень** і увімкніть параметри **Створити дзеркало оновлення** й **Увімкнути HTTP-сервер**.

Додаткову інформацію див. за посиланням:



- [Дзеркало оновлень](#)
- [Оновлення із дзеркала](#)

Налаштування сервера дзеркала для поширення оновлень через спільну мережеву папку

1. Створіть спільну папку на локальному або мережевому пристрої. Ця папка має бути доступною для читання всім користувачам рішень ESET і для запису від імені локального СИСТЕМОГО облікового запису.
2. Активуйте параметр **Створити дзеркало оновлення** в розділі **Додаткові параметри > Оновлення > Профілі > Дзеркало оновлення**.
3. Виберіть відповідну **папку для зберігання**. Для цього натисніть **Очистити**, а потім — **Змінити**. Знайдіть і виберіть створену спільну папку.



Якщо ви не бажаєте виконувати оновлення через внутрішній HTTP-сервер, зніміть прапорець **Створити дзеркало оновлення**.

Оновлення до ОС Windows 10 за допомогою ESET Endpoint Antivirus



Перш ніж переходити на ОС Windows 10, наполегливо рекомендуємо оновити продукт ESET до останньої версії та завантажити останні оновлення для модулів. Це допоможе забезпечити максимальний захист і зберегти параметри програми й інформацію про ліцензію під час оновлення до ОС Windows 10.

Версія 7.x:

Натисніть відповідне посилання нижче, щоб завантажити й інсталювати останню версію для підготовки до переходу на Microsoft Windows 10.

[Завантажити 32-розрядну версію ESET Endpoint Security 7](#) [Завантажити 32-розрядну версію ESET Endpoint Antivirus 7](#)

[Завантажити 64-розрядну версію ESET Endpoint Security 7](#) [Завантажити 64-розрядну версію ESET Endpoint Antivirus 7](#)

Версія 5.x:



Продукти ESET Endpoint версії 5 [більше не підтримуються](#). Це означає, що збірки більше недоступні для завантаження. Наполегливо рекомендуємо виконати оновлення до [останньої версії продуктів ESET Endpoint](#).

Інші мовні версії

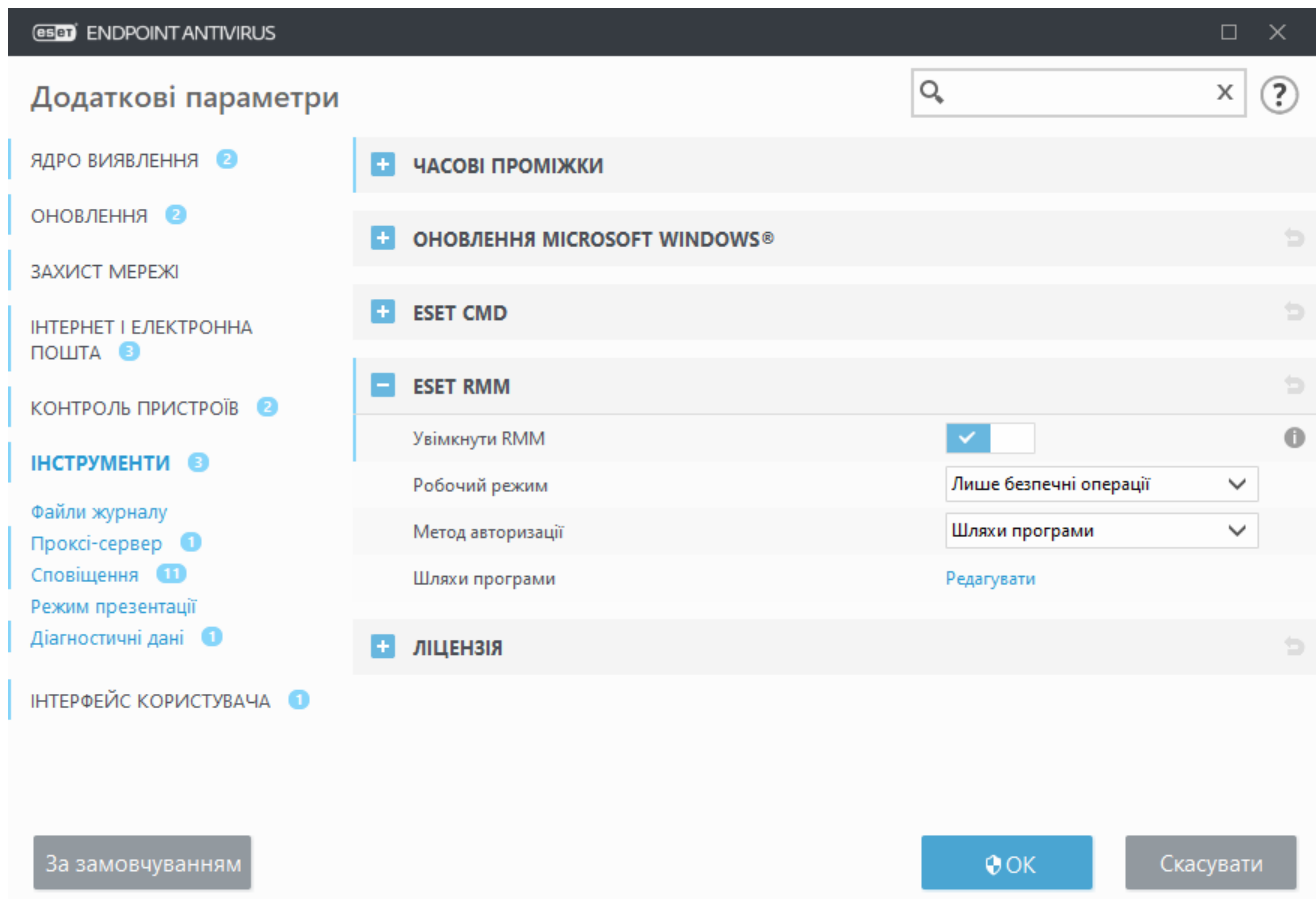
Щоб знайти іншу мовну версію кінцевого продукту ESET, [перейдіть на сторінку завантаження](#).



[Докладніше про сумісність продуктів ESET для бізнесу з ОС Windows 10.](#)

Активація віддаленого моніторингу та керування

Віддалений моніторинг і керування (RMM) — це процес нагляду за програмними системами (наприклад, на настільних ПК, серверах і мобільних пристроях) і контролю їх роботи за допомогою локально інсталюваних агентів, доступ до яких може отримати постачальник послуг керування. Для керування ESET Endpoint Antivirus можна використовувати RMM версії 6.6.2028.0 і новіших.



За замовчуванням модуль ESET RMM вимкнено. Щоб увімкнути модуль ESET RMM, перейдіть у розділ "Додаткові параметри" (F5) і натисніть **Інструменти**. Розгорніть вузол **ESET RMM** і встановіть перемикач **Увімкнути RMM**.

Робочий режим: щоб увімкнути інтерфейс RMM тільки для безпечних операцій і операцій із доступом тільки для читання, виберіть **Лише безпечні операції**. Щоб увімкнути інтерфейс RMM для всіх операцій, виберіть **Усі операції**.

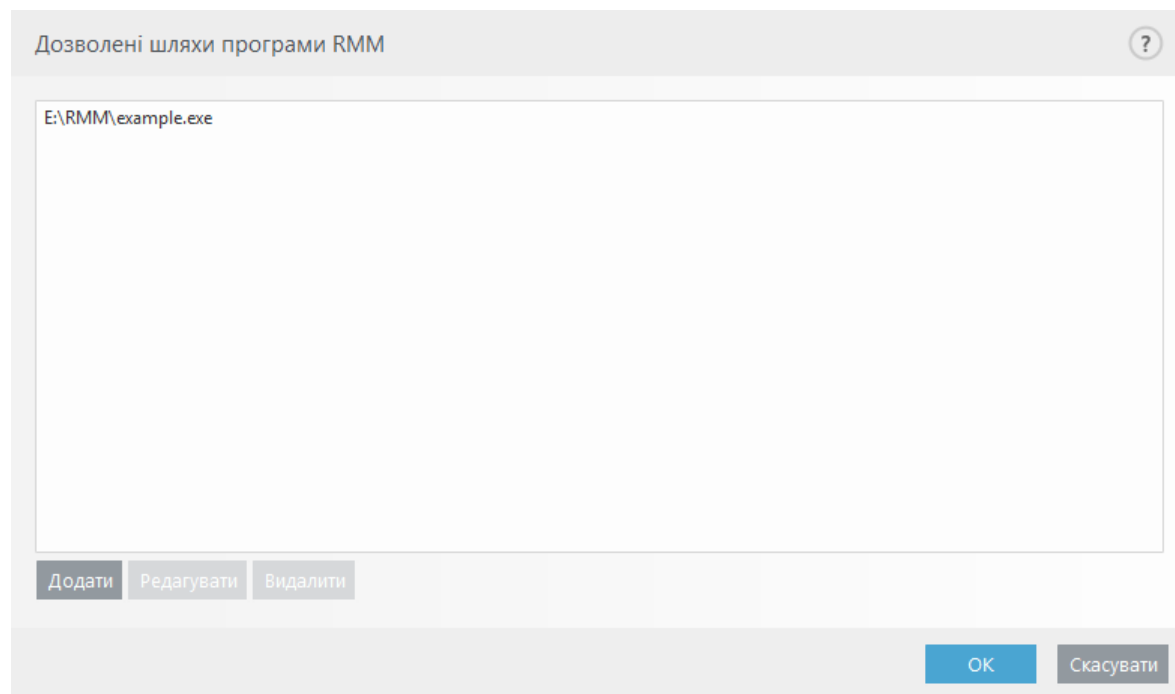
Операція	Режим "Лише безпечні операції"	Режим "Усі операції"
Отримати інформацію про програму	✓	✓
Отримати конфігурацію	✓	✓
Отримати відомості про ліцензію	✓	✓
Отримати журнали	✓	✓
Отримати статус захисту	✓	✓
Отримати статус оновлення	✓	✓
Застосувати конфігурацію		✓
Запустити активацію		✓
Запустити сканування	✓	✓
Запустити оновлення	✓	✓

Метод авторизації: виберіть метод авторизації для модуля RMM. Щоб увімкнути авторизацію, виберіть **Шлях програми** в розкритому меню. Інакше виберіть **Немає**.



RMM має завжди використовувати авторизацію, щоб забороняти зловмисному ПЗ вимикати або обходити захист ESET Endpoint.

Шляхи програми: конкретні програми, яким дозволено запускати RMM. Якщо для методу авторизації вибрано **Шлях програми**, натисніть **Редагувати**, щоб відкрити вікно конфігурації **Дозволені шляхи програми RMM**.



Додати: створити новий дозволений шлях програми RMM. Введіть шлях або натисніть кнопку ..., щоб вибрати виконуваний файл.

Редагувати: змінити наявний дозволений шлях. Використовуйте параметр **Редагувати**, якщо виконуваний файл перенесено до іншої папки.

Видалити: видалити наявний дозволений шлях.

За замовчуванням каталог програми ESET Endpoint Antivirus в кінцевій точці містить файл ermm.exe (як правило, його можна знайти тут: *C:\Program Files\ESET\ESET Security*). Програма ermm.exe здійснює обмін даними з плагіном RMM, який у свою чергу обмінюється даними з агентом RMM, підключеним до сервера RMM.

- ermm.exe – програма командного рядка, розроблена компанією ESET, що дає змогу керувати кінцевими продуктами й забезпечує обмін даними з будь-яким плагіном RMM.
- Плагін RMM – програма стороннього виробника, запущена локально в кінцевій системі Windows. Плагін розроблено для забезпечення обміну даними з певним агентом RMM (наприклад, лише Kaseya), а також програмою ermm.exe.
- Агент RMM – програма стороннього виробника (наприклад, Kaseya), запущена локально в кінцевій системі Windows. Агент обмінюється даними з плагіном і сервером RMM.

Блокування завантаження певних типів файлів з Інтернету

Якщо ви не хочете дозволяти завантажувати файли певних типів (наприклад, exe, pdf або zip) з Інтернету, скористуйтеся функцією [Керування URL-адресами](#) з конфігурацією символів узагальнення. Натисніть клавішу F5, щоб відкрити **розширені налаштування**. Послідовно виберіть пункти **"Інтернет і електронна пошта" > "Захист доступу до Інтернету"** і розкрийте **"Керування URL-адресами"**. Клацніть **"Змінити"** поруч із **списком адрес**.

У вікні списку **"Адреса"** виберіть **"Список заблокованих адрес"** і натисніть кнопку **"Змінити"** або натисніть кнопку **"Додати"**, щоб додати новий список. Якщо ви створюєте новий список. У розкритому меню **"Тип списку"** адрес виберіть пункт **"Заблоковані"** та вкажіть назву списку. Щоб отримувати сповіщення про доступ до файлу певного типу з поточного списку, увімкніть повзунок **"Сповіщати про застосування"**. У розкритому меню виберіть пункт **"Рівень критичності"**. Віддалений адміністратор може збирати записи про **попередження**.



Клацніть **"Додати"**, щоб вказати маску, яка визначатиме типи файлів, для яких необхідно блокувати завантаження. Вкажіть повну URL-адресу, якщо необхідно блокувати завантаження певного файлу з веб-сайту, наприклад, <http://example.com/file.exe>. Щоб охопити групу файлів, можна використовувати символи узагальнення. Знак запитання (?) позначає окремий змінний символ, а зірочка (*) представляє змінний рядок, який складається з нуля або більшої кількості символів. Наприклад, маска [*/*.zip](#) блокує завантаження всіх стиснутих ZIP-файлів.

Зверніть увагу, що цей метод дозволяє блокувати завантаження певних типів файлів тільки в тому разі, коли розширення файлу є частиною URL-адреси цього файлу. Якщо на веб-сторінці є URL-адреси для завантаження файлу, наприклад, www.example.com/download.php?fileid=42, будь-який файл, розташований за цим посиланням, завантажуватиметься, навіть якщо його розширення заблоковане.

Згортання інтерфейсу користувача ESET Endpoint Antivirus

Якщо керування здійснюється віддалено, можна застосувати [попередньо визначену політику "Видимість"](#).

В іншому разі виконайте такі операції:

1. Натисніть клавішу **F5** для доступу до розділу **"Додаткові параметри"** й розгорніть пункти **Інтерфейс користувача > Елементи інтерфейсу користувача**.
2. Задайте бажане значення для параметра **Режим запуску**. [За цим посиланням міститься більш докладні відомості про режим запуску](#).
3. Вимкніть **Відображати стартовий екран під час запуску** й **Використовувати звуковий сигнал**.
4. Налаштуйте [Сповіщення](#).
5. Налаштуйте [Статуси програми](#).

6. Налаштуйте [Повідомлення про підтвердження](#).

7. Налаштуйте [Вікна повідомлень і оповіщень](#).

Ліцензійна угода з кінцевим користувачем

Набуває чинності 19 жовтня 2021 року.

УВАГА! Перш ніж завантажувати, інсталювати, копіювати або використовувати продукт, уважно ознайомтеся з наведеними нижче положеннями й умовами його застосування.

ЗАВАНТАЖИВШИ, ІНСТАЛЮВАВШИ, СКОПІЮВАВШИ АБО ЗАСТОСУВАВШИ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИ ПРИЙМАЄТЕ ЦІ ПОЛОЖЕННЯ Й УМОВИ, А ТАКОЖ ПОГОДЖУЄТЕСЯ З [ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ](#).

Ліцензійна угода з кінцевим користувачем

Ця ліцензійна угода з кінцевим користувачем ("Угода"), укладена між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 85101 Bratislava, Slovak Republic, унесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532 ("ESET" або "Постачальник") і Вами, фізичною або юридичною особою ("Ви" або "Користувач"), надає Вам право використовувати Програмне забезпечення, визначене в статті 1 цієї Угоди. Указане Програмне забезпечення можна отримати на носії даних або електронною поштою, завантажити з Інтернету, серверів Постачальника або отримати з інших джерел відповідно до зазначених нижче умов і положень.

ЦЕ УГОДА ПРО ПРАВА КОРИСТУВАЧА, А НЕ ДОГОВІР КУПІВЛІ. Постачальник залишає за собою право власності на копію Програмного забезпечення та фізичного носія, на якому Програмне забезпечення постачається в товарній упаковці, а також усі інші копії, які Користувач має право створювати відповідно до умов цієї Угоди.

Вибравши під час завантаження, інсталяції, копіювання або використання Програмного забезпечення варіант «Прийняти», Ви засвідчуєте свою згоду дотримуватись умов і положень цієї Угоди та підтверджуєте ознайомлення з Політикою конфіденційності. Якщо Ви не погоджуєтесь з будь-якими положеннями або умовами Угоди та/або Політики конфіденційності, виберіть варіант «Закрити», скасуйте інсталяцію чи завантаження, знищте Програмне забезпечення, інсталяційний носій, супровідну документацію та товарний чек або поверніть їх Постачальнику чи в торгову точку, де Ви отримали Програмне забезпечення.

ВИ ПОГОДЖУЄТЕСЯ, ЩО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАСВІДЧУЄ ФАКТ ПРОЧИТАННЯ ВАМИ ЦЬОЇ УГОДИ, РОЗУМІННЯ ЇЇ УМОВ І ПОЛОЖЕНЬ ТА ВАШУ ЗГОДУ НА ЇЇ ДОТРИМАННЯ.

1. Програмне забезпечення. Термін "Програмне забезпечення" в цій Угоді означає: (i) комп'ютерну програму, що супроводжується цією Угодою, включно з усіма її компонентами; (ii) увесь вміст дисків, компакт- і DVD-дисків, повідомлень електронної пошти та будь-яких вкладень або інших носіїв, з якими надається ця Угода, разом із формою об'єктного коду Програмного забезпечення, що постачається на носії даних, надається електронною поштою чи завантажується через Інтернет; (iii) усі письмові пояснення та будь-яку іншу документацію, пов'язану з Програмним забезпеченням, насамперед опис Програмного забезпечення, його характеристик, властивостей і способу використання, опис операційного середовища, у якому використовується Програмне забезпечення, інструкції із застосування або інсталяції Програмного забезпечення чи будь-який опис правил його використання ("Документація"); (iv)

копії Програмного забезпечення, виправлення можливих помилок Програмного забезпечення, доповнення до нього, його розширення, змінені версії Програмного забезпечення й усі оновлення його компонентів (якщо є), право на використання яких Вам надає Постачальник згідно з розділом 3 цієї Угоди. Програмне забезпечення постачається виключно як виконуваний об'єктний код.

2. Інсталяція, комп'ютер і ліцензійний ключ. Програмне забезпечення, яке надається на носії даних або електронною поштою, завантажується з Інтернету, серверів Постачальника або отримується з інших джерел, необхідно інстальювати. Ви маєте інстальювати Програмне забезпечення на правильно налаштованому комп'ютері відповідно до мінімальних потреб, наведених у відповідній Документації. Метод інсталяції описано в Документації. На Комп'ютері, де Ви інстальюєте Програмне забезпечення, не повинно бути жодних програм або компонентів обладнання, які можуть негативно вплинути на роботу Програмного забезпечення. Під Комп'ютером розуміється обладнання, яке включає в себе, серед іншого, персональні комп'ютери, ноутбуки, робочі станції, надолонні комп'ютери, смартфони, ручні електронні пристрої або інші електронні пристрої, для яких розроблено Програмне забезпечення, на яких воно буде інстальюватися та (або) використовуватися. Ліцензійний ключ — унікальна послідовність символів, літер, цифр або спеціальних символів, що надається Кінцевому користувачу для легального використання Програмного забезпечення, його особливих версій або продовження терміну дії Ліцензії у відповідності до умов цієї Угоди.

3. Ліцензія. Якщо Ви погоджуєтесь з положеннями цієї Угоди й дотримуєтесь усіх наведених тут умов і положень, Постачальник надає Вам указані права ("Ліцензію").

а) Інсталяція та використання. Вам надається невиняткове та непередаване право інстальювати Програмне забезпечення на жорсткому диску комп'ютера або іншому носії для постійного зберігання даних, інсталяції та збереження Програмного забезпечення в пам'яті комп'ютерної системи, а також застосовувати, зберігати й відображати Програмне забезпечення.

б) Застереження щодо кількості ліцензій. Право використання Програмного забезпечення обумовлюється кількістю Користувачів. Наведена нижче інформація стосується одного Користувача: (i) інсталяція Програмного забезпечення на одній комп'ютерній системі або (ii) за умови, що обсяг ліцензії визначається кількістю поштових скриньок, один Користувач означає користувача комп'ютера, який отримує електронну пошту через користувацький поштовий агент («КПА»). Якщо КПА приймає електронну пошту, після чого автоматично розподіляє її між кількома користувачами, кількість Користувачів визначається відповідно до їх фактичного числа, серед якого розподіляється електронна пошта. Якщо поштовий сервер виконує функцію поштового шлюзу, кількість Користувачів дорівнює числу користувачів поштових серверів, яких обслуговує такий шлюз. Якщо адреси електронної пошти (наприклад, псевдоніми), точна кількість яких не визначена, належать одному користувачеві й один користувач приймає всі відповідні повідомлення, а пошта не розподіляється автоматично клієнтом між більшою кількістю користувачів, Ліцензія необхідна лише для одного комп'ютера. Забороняється одночасно використовувати одну й ту саму Ліцензію на кількох комп'ютерах. Кінцевий користувач має право вводити Ліцензійний ключ у Програмному забезпеченні виключно в межах наявних у цього користувача прав на використання Програмного забезпечення та у відповідності до обмеження кількості Ліцензій, наданих Постачальником. Ліцензійний ключ є конфіденційною інформацією. Ви не маєте права ділитися Ліцензійним ключем із третіми особами або дозволяти їм використовувати Ліцензійний ключ, якщо це не дозволено цією Угодою або Постачальником. У випадку порушення конфіденційності Ліцензійного ключа негайно повідомте про це Постачальника.

с) **Home/Business Edition.** Версія Програмного забезпечення Home Edition має використовуватися виключно в приватному та (або) некомерційному середовищі лише для сімейних і домашніх потреб. Для використання в комерційному середовищі та на поштових серверах, засобах пересилання пошти, поштових або інтернет-шлюзах потрібно придбати версію Програмного забезпечення Business Edition.

г) **Термін дії ліцензії.** Право використання Програмного забезпечення обмежено в часі.

е) **ОЕМ-версія Програмного забезпечення.** OEM-версії Програмного забезпечення мають використовуватися лише на Комп'ютері, з яким постачаються. Його заборонено передавати для використання на іншому комп'ютері.

ф) **НДП та ПРОБНА ВЕРСІЯ Програмного забезпечення.** Програмне забезпечення, що визначається як «не для продажу» (НДП), або його ПРОБНА ВЕРСІЯ не підлягає оплаті та має використовуватися лише в демонстраційних цілях чи для тестування функцій Програмного забезпечення.

г) **Припинення дії ліцензії.** Дія ліцензії припиняється автоматично після закінчення періоду, на який вона надається. Якщо Ви не дотримуєтеся положень цієї Угоди, Постачальник має право скасувати Угоду без шкоди для своїх прав або судового захисту, що надається Постачальнику в таких випадках. У разі скасування Ліцензії Ви повинні негайно видалити, знищити чи повернути за власний кошт Програмне забезпечення та всі резервні копії в компанію ESET або торгову точку, де Ви отримали Програмне забезпечення. Якщо дію Ліцензії припинено, Постачальник також має право скасувати право Користувача використовувати функції Програмного забезпечення, для чого потрібно підключення до серверів Постачальника або серверів третіх осіб.

4. Функції, для яких потрібні дозволи на збір даних та доступ до Інтернету. Для правильної роботи Програмному забезпеченню потрібно збирати дані (у відповідності до Політики конфіденційності), підключатися до Інтернету і через рівні проміжки часу з'єднуватися з серверами Постачальника або третіх осіб. Нижче вказано функції Програмного забезпечення, для яких потрібно підключення до Інтернету до дозволи на збір даних:

а) **Оновлення Програмного забезпечення.** Постачальник може час від часу випускати оновлення Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення інстальюються автоматично, якщо Користувач не вимкнув відповідну функцію. Для надання оновлень нам необхідно перевірити автентичність Ліцензії, включаючи інформацію про комп'ютер та (або) платформу, на якій інстальовано Програмне забезпечення у відповідності до Політики конфіденційності.

На надання Оновлень може поширюватися Політика закінчення терміну служби ("Політика EOL"), доступна за адресою https://go.eset.com/eol_business. Оновлення Програмного забезпечення не надаватимуться після завершення терміну служби будь-яких його функцій, визначених у Політиці EOL.

б) **Надсилання Постачальнику Інформації про загрози.** Програмне забезпечення має функції, які збирають зразки вірусів та інших шкідливих комп'ютерних програм, а також підозрілих, проблемних, потенційно небажаних або небезпечних об'єктів: файлів, URL-адрес, IP-пакетів і Ethernet-фреймів ("Загрози"). Ці відомості ("Дані"), зокрема інформація про процес інсталяції, комп'ютер і (або) платформу, на яких інстальовано Програмне забезпечення, операції й роботу Програмного забезпечення, надсилаються Постачальнику. Інформація про

Загрози та Дані можуть містити відомості про Кінцевого користувача й інших користувачів комп'ютера, на якому інстальовано Програмне забезпечення (зокрема випадково отримані особисті дані), і файли, пошкоджені внаслідок Загроз, з відповідними метаданими.

Дані та Інформацію про загрози збирають такі функції ПЗ:

i. LiveGrid Reputation System передбачає збір і надсилання Постачальнику односторонніх хешів, пов'язаних із загрозами. Ця функція активується в стандартних налаштуваннях ПЗ.

ii. LiveGrid Feedback System передбачає збір і надсилання Постачальнику Даних про загрози з відповідними метаданими та Інформації. Цю функцію активує Кінцевий користувач під час інсталяції Програмного забезпечення.

Постачальник використовує Дані й Інформацію про загрози лише для аналізу та дослідження несанкціонованого доступу, удосконалення Програмного забезпечення та перевірки автентичності Ліцензії. Потім Постачальник уживає належних заходів, щоб забезпечити конфіденційність отриманих даних. Активуючи описану вище функцію Програмного забезпечення, Ви надаєте Постачальнику право збирати і обробляти Дані й Інформацію про загрози відповідно до чинних правових норм. Ви завжди можете відключити ці функції.

З метою виконання положень цієї Угоди Постачальнику необхідно збирати, обробляти та зберігати дані, які дають змогу ідентифікувати Вас, у відповідності до Політики конфіденційності. Ви дозволяєте Постачальнику власними засобами перевіряти, чи використовуєте Ви програмне забезпечення у відповідності до положень цієї Угоди. Ви погоджуєтесь, що з метою виконання положень цієї Угоди для забезпечення функціональності Програмного забезпечення і надання авторизації на його використання, а також для захисту прав Постачальника будуть передаватися дані між Програмним забезпеченням і комп'ютерними системами Постачальника та його бізнес-партнерів, що входять до його мережі підтримки та розповсюдження.

Після укладання цієї Угоди Постачальник або його бізнес-партнери (які входять до мережі підтримки і розповсюдження Постачальника) матимуть право передавати, обробляти й зберігати важливі дані, що ідентифікують Вас, для виставлення рахунків, виконання цієї Угоди та передавання сповіщень на Ваш комп'ютер.

Докладні відомості про конфіденційність, захист персональних даних і Ваші права як суб'єкта даних можна знайти в документі "Політика конфіденційності" на веб-сайті Постачальника. Окрім того, ця інформація доступна безпосередньо в процесі інсталяції. Також можна ознайомитися з цим документом у довідці Програмного забезпечення.

5. Реалізація прав Користувача. Ви зобов'язуєтесь реалізувати права Користувача особисто або через своїх співробітників. Ви маєте право використовувати Програмне забезпечення лише для захисту безпеки своєї роботи та тих комп'ютерів і комп'ютерних систем, для яких надано Ліцензію.

6. Обмеження прав. Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Програмного забезпечення. Використовуючи Програмне забезпечення, Ви зобов'язуєтесь дотримуватися наведених нижче обмежень.

а) Ви можете створити одну копію Програмного забезпечення на носії для постійного збереження даних за умови, що така архівна резервна копія не буде інсталюватися та

використовуватися на будь-якому іншому комп'ютері. Створення будь-яких інших копій Програмного забезпечення вважається підставою для скасування цієї Угоди.

b) Ви не маєте права використовувати, змінювати, перебудовувати Програмне забезпечення, робити його копії або передавати право на використання Програмного забезпечення чи його копій будь-яким способом, окрім чітко передбаченого положеннями цієї Угоди.

c) Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, передавати право на його користування чи використовувати його з комерційною метою.

d) Ви не маєте права виконувати зворотне проектування, декомпілювати або дезасемблювати Програмне забезпечення чи застосувати будь-які інші засоби виявлення його вихідного коду, крім випадків, коли таке обмеження прямо заборонене законодавством.

e) Ви погоджуєтесь використовувати Програмне забезпечення лише таким способом, що відповідає всім застосовним юридичним нормам законодавства, яке регулює його застосування, включно з відповідними обмеженнями згідно із законом про авторське право й інші права на інтелектуальну власність, але не обмежуючись цим.

f) Ви даєте свою згоду використовувати Програмне забезпечення та його функції лише таким способом, що не обмежує можливостей доступу до них інших кінцевих користувачів. Постачальник зберігає за собою право обмежити перелік доступних послуг, що надаються окремим кінцевим користувачам, з метою надання своїх послуг максимальній кількості кінцевих користувачів. Обмеження переліку доступних послуг також передбачає повну заборону на використання будь-яких функцій Програмного забезпечення й видалення Даних та інформації із серверів Постачальника або серверів третьої сторони, пов'язаних із конкретною функцією Програмного забезпечення.

g) Ви погоджуєтесь не вчиняти будь-які дії щодо використання Ліцензійного ключа, які суперечать положенням цієї Угоди або можуть призвести до передачі Ліцензійного ключа будь-якій особі, яка не має права використовувати Програмне забезпечення. Зокрема, Ви погоджуєтесь не передавати використовуваний або невикористовуваний Ліцензійний ключ у будь-якій формі, а також утриматися від несанкціонованого відтворення або розповсюдження дублікатів Ліцензійних ключів або створених Ліцензійних ключів або від використання Програмного забезпечення з Ліцензійним ключем, отриманим із будь-якого іншого джерела, окрім Постачальника.

7. Авторське право. Програмне забезпечення та всі права, включно із правами власності та відповідними правами на інтелектуальну власність без обмежень, належать компанії ESET та/або її ліцензіарам. Ці права захищено положеннями міжнародного договірної права та всіма іншими застосовними законами країни, у якій використовується Програмне забезпечення. Структура, організація та код Програмного забезпечення є комерційною таємницею та конфіденційною інформацією компанії ESET і/або її ліцензіарів. Ви не маєте права копіювати Програмне забезпечення, за винятком визначених у розділі 6 (а) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосовуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то погоджуєтесь, що будь-яка отримана таким чином інформація буде автоматично й безповоротно вважатися належною для передавання Постачальнику та цілком належатиме йому з моменту її отримання, незалежно від права Постачальника на розірвання цієї Угоди.

8. Захист прав. Постачальник залишає за собою всі права на Програмне забезпечення, за винятком тих, що чітко надані Вам як Користувачу Програмного забезпечення відповідно до умов цієї Угоди.

9. Багатомовні версії, програмне забезпечення, що постачається на носіях двох типів, кілька копій. Якщо Програмне забезпечення підтримує кілька платформ чи мов, або Ви одержали кілька копій Програмного забезпечення, Ви не маєте права інсталювати Програмне забезпечення на більшій кількості комп'ютерних систем або інші версії ніж ті, на які розповсюджується Ліцензія. Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, укладати договір лізингу, надавати право на користування чи передавати версії або копії Програмного забезпечення, які Ви не використовуєте.

10. Набуття Угодою чинності та припинення дії Угоди. Ця Угода набуває чинності з дати погодження з її умовами. Ви можете припинити дію цієї Угоди, остаточно видаливши, знищивши або повернувши за власний кошт Програмне забезпечення, усі резервні копії та всі пов'язані матеріали, отримані від Постачальника або його ділових партнерів. На право використання Програмного забезпечення та його функцій може поширюватися Політика EOL. Після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL, ваше право на використання Програмного забезпечення буде скасовано. Незалежно від способу припинення дії цієї Угоди, умови розділів 7, 8, 11, 13, 19 і 21 є чинними без обмежень у часі.

11. ЗАЯВА КОРИСТУВАЧА. ЯК КОРИСТУВАЧ, ВИ ВИЗНАЄТЕ, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАДАЄТЬСЯ «ЯК Є» БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОПУСКАЄТЬСЯ ЧИННИМ ЗАКОНОДАВСТВОМ. НІ ПОСТАЧАЛЬНИК РАЗОМ ІЗ ЙОГО ЛІЦЕНЗІАРАМИ Й ДОЧІРНІМИ КОМПАНІЯМИ, НІ ВЛАСНИКИ АВТОРСЬКОГО ПРАВА НЕ НАДАЮТЬ БУДЬ-ЯКИХ ТВЕРДЖЕНЬ АБО СПЕЦІАЛЬНИХ ЧИ НЕПРЯМИХ ГАРАНТІЙ, ЗОКРЕМА ГАРАНТІЙ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ ЧИ КОНКРЕТНОГО ЗАСТОСУВАННЯ АБО ГАРАНТІЙ ТОГО, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НЕ ПОРУШУЄ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЄ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ АБО ВОНО ФУНКЦІОНУВАТИМЕ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ'ЯЗАНІ З ВИБОРОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ, А ТАКОЖ ЗА ІНСТАЛЯЦІЮ, ВИКОРИСТАННЯ ТА НАСЛІДКИ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

12. Відсутність інших зобов'язань. Ця Угода не створює жодних зобов'язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

13. ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ. У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ЛІЦЕНЗІАРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ВТРАЧЕНІ ПРИБУТКИ, ДОХОДИ, ЗНИЖЕННЯ ОБСЯГІВ ПРОДАЖІВ АБО ВТРАТУ ДАНИХ, А ТАКОЖ ДОДАТКОВІ ВИТРАТИ, ПОВ'ЯЗАНІ З ПРИДБАННЯМ ЗАПАСНИХ ТОВАРІВ АБО ПОСЛУГ, ЗАПОДІЯНУ МАЙНУ ШКОДУ, ОСОБИСТУ ШКОДУ, ПРИПИНЕННЯ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, ВТРАТУ ДІЛОВОЇ ІНФОРМАЦІЇ ЧИ БУДЬ-ЯКІ СПЕЦІАЛЬНІ, ПРЯМІ, НЕПРЯМІ, ВИПАДКОВІ, КОМЕРЦІЙНІ, ШТРАФНІ ЧИ ОПОСЕРЕДКОВАНІ ЗБИТКИ, БУДЬ-ЯКИМ ЧИНОМ ОБУМОВЛЕНІ ДІЄЮ УГОДИ, ЦИВІЛЬНЕ ПРАВОПОРУШЕННЯ, НЕДБАЛИСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ІНСТАЛЯЦІЇ, ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНИМ КОМПАНІЯМ ВІДОМО ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ. В ОКРЕМИХ КРАЇНАХ І ЮРИСДИКЦІЯХ НЕ ПЕРЕДБАЧЕНО ВИНЯТКИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ, АЛЕ ЇЇ МОЖЕ БУТИ ОБМЕЖЕНО. ТОБТО

ВІДПОВІДАЛЬНІСТЬ ПОСТАЧАЛЬНИКА, ЙОГО СПІВРОБІТНИКІВ, ЛІЦЕНЗІАРІВ АБО ДОЧІРНИХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ЛІЦЕНЗІЮ.

14. Жодна умова цієї Угоди не має порушувати законні права будь-якої сторони, що виступає як клієнт, у тих випадках, коли вони їм суперечать.

15. **Технічна підтримка.** Компанія ESET або вповноважені нею треті сторони надають технічну підтримку на власний розсуд без жодних гарантій або заяв. Технічна підтримка не надаватиметься після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL. Перед наданням технічної підтримки Користувач повинен створити резервні копії всіх поточних даних, програмного забезпечення та програмних засобів. Компанія ESET або вповноважені нею треті сторони не несуть відповідальності за пошкодження або втрату даних, майна, програмного чи апаратного забезпечення, а також комерційні збитки, що виникають унаслідок надання технічної підтримки. Компанія ESET і/або вповноважені нею треті сторони залишають за собою право приймати рішення щодо того, чи належить проблема до обсягу послуг, які надаються в рамках технічної підтримки. Компанія ESET залишає за собою право на власний розсуд приймати рішення щодо відмови в наданні технічної підтримки, її призупинення чи скасування. Для забезпечення технічного обслуговування може знадобитися інформація про Ліцензію та інші дані у відповідності до Політики конфіденційності.

16. **Передача Ліцензії.** Програмне забезпечення може передаватися з однієї комп'ютерної системи на іншу, якщо такі дії не суперечать умовам Угоди. За умови дотримання положень Угоди Користувач має право остаточної передачі Ліцензії та всіх прав, що виникають унаслідок укладання цієї Угоди, іншому Користувачеві за згоди Постачальника, якщо (i) вихідний Користувач не зберігає жодних копій Програмного забезпечення; (ii) виконується пряма передача прав, наприклад, від вихідного Користувача до нового; (iii) новий Користувач приймає від вихідного всі права, що надаються відповідно до умов цієї Угоди; (iv) вихідний Користувач надає новому документацію, що дозволяє підтвердити автентичність Програмного забезпечення відповідно до розділу 17.

17. **Підтвердження автентичності Програмного забезпечення.** Кінцевий користувач може підтвердити своє право застосовувати Програмне забезпечення одним із таких способів: (i) за допомогою ліцензійного сертифіката, наданого Постачальником або вповноваженою ним третьою особою; (ii) за допомогою ліцензійної угоди в письмовій формі (якщо така укладалася); (iii) надавши надісланий Постачальником електронний лист із ліцензійними даними (ім'я користувача та пароль). Для підтвердження автентичності Програмного забезпечення може знадобитися інформація про Ліцензію та ідентифікаційні дані Кінцевого споживача у відповідності до Політики конфіденційності.

18. **Надання ліцензії органам державної влади й уряду США.** Програмне забезпечення надається органам державної влади, включно з урядом США, з урахуванням ліцензійних прав і обмежень, наведених у цій Угоді.

19. **Дотримання процедур із контролю за торгівлею.**

а) Забороняється в прямий чи непрямий спосіб експортувати, реекспортувати, передавати або іншим чином надавати програмне забезпечення будь-яким іншим особам. Ви зобов'язуєтеся утриматися від будь-яких способів використання цього програмного забезпечення й (або) не брати участь у жодних діях, які можуть призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET, її холдингових і дочірніх компаній або дочірніх компаній будь-яких холдингових компаній ESET, відповідно до законів із контролю за торгівлею,

зокрема тих, що наведені нижче:

i. Усі закони, які регулюють, обмежують або накладають ліцензійні вимоги для експорту, реекспорту або передачі товарів, програмного забезпечення, технологій або послуг, що видані або прийняті будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії

ii. Усі економічні, фінансові, торгові або інші санкції, обмеження, ембарго, заборони експорту або імпорту, заборони передачі коштів або активів чи надання послуг або рівнозначні заходи, які запроваджуються будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії.

(законні акти, зазначені в пунктах i та ii вище, разом згадуються як "Закони з контролю за торгівлею").

b) ESET має право призупинити виконання зобов'язань за цими Умовами або припинити їх дію з негайним набуттям чинності за таких умов:

i. ESET має обґрунтовані підстави вважати, що Користувачем уже порушено, або, імовірно, буде порушено умови Статті 19 а) Угоди; або

ii. Користувач i (або) Програмне забезпечення стали предметом законів із контролю за торгівлею, і через це ESET має обґрунтовані підстави вважати, що подальше виконання зобов'язань за цією Угодою може призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET або афілійованих із нею компаній відповідно до законів із контролю за торгівлею.

c) Жодна умова Угоди в жодному разі не має тлумачитися як така, що має на меті спонукати будь-яку зі сторін або вимагати від неї вчинити дії або утриматися від вчинення дій (чи погодитися на це) у будь-який спосіб, який буде суперечити законам із контролю за торгівлею або заборонений цими законами.

20. Примітки. Усі зауваження та запити на повернення Програмного забезпечення та Документації слід надсилати на адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic без шкоди для права ESET повідомляти Вам про зміни цієї Угоди, Політики конфіденційності, Політики EOL та Документації відповідно до ст. 22 Угоди. ESET може надсилати Вам електронні листи, сповіщення в програмі через Програмне забезпечення або розміщувати повідомлення на Вашому веб-сайті. Ви погоджуєтесь отримувати сповіщення правового характеру від ESET в електронній формі, зокрема всі сповіщення про внесення змін в Умови, Спеціальні Умови або Політики конфіденційності, будь-які пропозиції укласти (прийняти) договір або запрошення до початку ділових відносин, сповіщення з правовою інформацією або будь-які інші повідомлення правового характеру. Отримання таких повідомлень в електронній формі прирівнюється до їх отримання в письмовій формі, якщо інше явно не вимагається застосовними законами.

21. Чинне законодавство. Ця Угода регулюється та тлумачиться відповідно до законодавства Словацької Республіки. Користувач і Постачальник погоджуються, що суперечливі положення регулюючого законодавства та Конвенції Організації Об'єднаних Націй щодо контрактів для

міжнародної торгівлі товарами не мають застосовуватися. Ви повністю погоджуєтесь, що розгляд будь-яких заяв до Постачальника чи суперечок із ним, які викликано цією Угодою, або заяв чи суперечок, будь-яким чином пов'язаних із використанням Програмного забезпечення, і прийняття відповідних рішень здійснюється окружним судом м. Братислава I, а також підтверджуєте виконання юрисдикції вказаним судом.

22. Загальні положення. Якщо будь-яке з положень цієї Угоди юридично не дійсне або не має позовної сили, це не повинно впливати на законність інших положень Угоди. Вони повинні залишатися чинними й такими, що мають законну силу, відповідно до передбачених тут умов. Цю Угоду укладено англійською. У разі розбіжностей між англійською й перекладеною версією Угоди (наданою для зручності або з будь-якою іншою метою) перевага надається документу англійською мовою.

Компанія ESET зберігає за собою право в будь-який час змінювати Програмне забезпечення, а також змінювати текст цієї Угоди, Додатків і Доповнень до неї, Політики конфіденційності, Політики закінчення терміну служби та документації або будь-яких їхніх складових шляхом оновлення застосовного документа (i) відповідно до змін, внесених в Програмне забезпечення або в спосіб ведення бізнесу ESET, (ii) із юридичних, регуляторних причин та з міркувань безпеки або (iii) для запобігання несанкціонованому використанню або нанесенню шкоди. Ми сповістимо Вас про будь-яке внесення змін в Угоду в електронному листі, сповіщеннях в програмі або через інші електронні способи зв'язку. Якщо Ви не згодні із запропонованими змінами в Угоді, то можете припинити її дію відповідно до ст. 10 протягом 30 днів після отримання сповіщення про зміну. Якщо Ви не припините дію Угоди протягом цього терміну, запропоновані зміни вважатимуться прийнятими й наберуть чинності з дати отримання Вами сповіщення про зміну.

Цей документ становить повну Угоду між Вами й Постачальником щодо Програмного забезпечення та цілком заміняє будь-які попередні подання, обговорення, зобов'язання, повідомлення й рекламні матеріали, пов'язані з Програмним забезпеченням.

EULAID: EULA-PRODUCT-LG; 3537.0

Політика конфіденційності

Компанія ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic), внесена до комерційного реєстру окружного суду м. Братислави I, Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532) як Контролер Даних (далі "ESET" або "Ми") прагне прозорості в справах, що стосуються обробки персональних даних і збереження конфіденційності наших клієнтів. З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів ("Кінцевий користувач" або "Ви") про такі теми:

- Обробка персональних даних
- Конфіденційність даних
- Права суб'єкта захисту даних

Обробка персональних даних

Служби, які надаються ESET, реалізовані в нашому продукті й надаються згідно з Ліцензійною угодою з кінцевим користувачем (далі "Ліцензійна угода"). Однак деякі аспекти потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов'язаний із

наданням наших послуг. Ми надаємо різні служби, наведені в Ліцензійній угоді й документації для відповідного продукту. Ідеться, зокрема, про службу оновлення/модернізації, ESET LiveGrid®, захист від несанкціонованого використання даних, служби підтримки тощо. Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

- Інформація про оновлення й інша статистична інформація, пов'язана з процесом інсталяції й вашим комп'ютером, зокрема платформою, на якій інстальовано продукт, а також інформація про операції й функціональність наших продуктів, зокрема інформація про операційну систему й обладнання, ідентифікатори інсталяції, ідентифікатори ліцензії, IP-адреси, MAC-адреси, параметри конфігурації продукту.
- Односторонні хеші, пов'язані з загрозами, як результат аналізу системи репутації ESET LiveGrid®, яка підвищує ефективність рішень для захисту від шкідливого ПЗ, порівнюючи перевірені файли з хмарною базою даних об'єктів, доданих до білих і чорних списків.
- Отримуючи підозрілі зразки та метадані від системи зворотного зв'язку ESET LiveGrid®, ми можемо миттєво реагувати на потреби користувачів і підтримувати системи ESET в актуальному стані. Якість роботи наших продуктів залежить від такої інформації, яку ми отримуємо від Вас:

озагрози, зокрема потенційні зразки вірусів і інших шкідливих та підозрілих програм; проблемні, потенційно небажані або потенційно небезпечні об'єкти, зокрема виконувані файли, повідомлення електронної пошти, позначені Вами або нашим продуктом як спам;

оінформація про пристрої в локальній мережі, зокрема їх тип, виробник, модель і (або) імена;

оінформація щодо використання Інтернету, зокрема IP-адреса й географічні дані, IP-пакети, URL-адреси й кадри Ethernet;

офайли аварійного дампа з пов'язаною інформацією.

Ми не маємо наміру збирати Ваші дані, які не входять до зазначеного переліку, однак іноді цьому неможливо запобігти. Випадково зібрані дані можуть збиратися шкідливим програмним забезпеченням і надходити безпосередньо з нього (без вашого відома або згоди) або надходити в іменах файлів чи URL-адресах. Ми не маємо наміру використовувати такі дані в наших системах або оброблювати їх відповідно до умов, визначених цією Політикою конфіденційності.

- Інформація про ліцензію, зокрема ідентифікатор ліцензії й персональні дані (ім'я, прізвище, адреса, адреса електронної пошти), потрібна для виставлення рахунків, перевірки автентичності ліцензії й надання наших служб.
- Контактна інформація і дані, які містяться в запитах до служби підтримки, можуть знадобитися для надання послуг підтримки. В залежності від обраного каналу зв'язку ми можемо збирати такі дані: адреса електронної пошти, номер телефону, дані ліцензії, дані продукту і опис Вашого звернення до служби підтримки. До Вас може надійти запит щодо надання іншої інформації для прискорення обслуговування службою підтримки.

Конфіденційність даних

ESET — це компанія, яка працює в усьому світі через афілійовані компанії або партнерів, які входять до нашої мережі розповсюдження, обслуговування та підтримки. Інформація, яка оброблюється ESET, може передаватися афілійованим компаніям або партнерам або

отримуватися від них. Це необхідно для виконання вимог Ліцензійної угоди, таких як надання послуг або підтримки або виставлення рахунків. В залежності від розташування і використовуваних Вами служб ми можемо бути змушені передавати Ваші дані державним установам без належного рішення Європейської Комісії. Навіть у такому випадку кожна передача інформації є предметом регулювання з боку законодавства про захист даних і відбувається тільки в тих випадках, коли це необхідно. Стандартні договірні умови й обов'язкові правила організації або інші належні заходи щодо захисту інформації мають застосовуватися без будь-яких обмежень.

Ми робимо все, що від нас залежить, щоб не зберігати довше, ніж це потрібно, дані, зібрані нами в зв'язку з наданням послуг відповідно до Ліцензійної угоди. Дані можуть зберігатися й після закінчення строку дії Вашої ліцензії, що дозволить Вам швидко й зручно поновити дію ліцензії. Статистична інформація в стиснутій і анонімній формі, а також інші дані від ESET LiveGrid® можуть оброблятися для статистичних цілей.

ESET впроваджує відповідні технічні та організаційні заходи, щоб забезпечити безпеку на тому рівні, якій відповідає потенційним ризикам. Ми докладемо всіх зусиль, щоб постійно забезпечувати конфіденційність, цілісність, доступність і стійкість систем обробки й сервісів. Однак у випадку витоку конфіденційної інформації, що загрожує Вашим правам та свободам, ми готові сповістити про це відповідний наглядовий орган, а також суб'єктів захисту персональних даних. Як суб'єкт захисту персональних даних Ви маєте право подавати скарги до вищестоящих органів влади.

Права суб'єкта захисту персональних даних

ESET є суб'єктом регулювання відповідно до законів Словацької Республіки. Для Вас є чинними всі умови, визначені застосовними законами щодо захисту даних. Як суб'єкт захисту персональних даних Ви маєте такі права:

- право запитувати доступ до персональних даних від ESET;
- право на уточнення персональних даних у разі їх неточності (також у Вас є право доповнити неповні персональні дані);
- право надіслати запит на видалення персональних даних;
- право надіслати запит на обмеження обробки персональних даних;
- право не погоджуватися з обробкою даних;
- право подати скаргу, а також
- право забезпечити можливість переносу даних.

Ми вважаємо, що вся інформація, яку ми обробляємо, є значущою й необхідною для реалізації законних інтересів, тобто надання послуг і продуктів нашим клієнтам.

Якщо Ви бажаєте скористатися Вашими правами як суб'єкта захисту даних або маєте питання чи застереження, надішліть нам повідомлення за такою адресою:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic

dpo@eset.sk