ESET Mail Security

Посібник користувача

Натисніть тут щоб відкрити версію цього документа

Digital Security
Progress. Protected.

ESET Mail Security розроблено компанією ESET, spol. s r.o.

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

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

REV. 04.08.2023

Огляд

ESET Mail Security для Microsoft Exchange Server — це інтегроване рішення, яке захищає поштові сервери й поштові скриньки користувачів від різних типів шкідливого вмісту. Зокрема, це вкладення з електронних листів, інфіковані хробаками чи троянами, а також документи, що містять шкідливі сценарії, фішингові схеми, спам, повідомлення з підробленою адресою відправника.

ESET Mail Security забезпечує чотири типи захисту: антивірус, антиспам, захист від фішинг-атак і правила. ESET Mail Security фільтрує шкідливий вміст у базах даних поштових скриньок і на рівні передавання електронних листів, перш ніж він надійде в поштову скриньку одержувача.

ESET Mail Security підтримує Microsoft Exchange Server 2010 і новіших версій, а також Microsoft Exchange Server у кластерному середовищі. Специфічні ролі Exchange Server (поштова скринька, транспортний сервер-концентратор, сервер межового транспорту).

ESET Mail Security не тільки захищає Microsoft Exchange Server, а й надає функції захисту самого сервера (захист файлової системи в режимі реального часу, захист мережі, захист веб-доступу і захист поштового клієнта).

У великих мережах ESET PROTECT дає змогу віддалено керувати ESET Mail Security. Окрім того, ESET Mail Security дає змогу використовувати його зі сторонніми інструментами віддаленого моніторингу й керування (RMM).

Основні функції

У таблиці нижче наведено список функцій, які доступні в ESET Mail Security.

Справжній 64-розрядний продукт	Підвищення продуктивності та стабільності в основних компонентах продукту.
Захист від шкідливого програмного забезпечення	Відзначений нагородами та інноваційний захист від шкідливого програмного забезпечення. Ця провідна технологія захищає від атак і всіх типів загроз, зокрема вірусів, програм-вимагачів, руткітів, хробаків і шпигунського програмного забезпечення. Для сканування використовуються хмарні технології, що дозволяє ще більше поліпшити показники виявлення. Невеликий розмір і невибагливість до ресурсів не впливають на продуктивність роботи. У програмі реалізовано багаторівневу модель захисту. Кожний рівень (етап) має низку ключових технологій. Рівень Pre-execution (Попереднє виконання) має такі технології, як сканер UEFI, захист від мережевих атак, репутація й кеш, вбудована пісочниця, родові виявлення. Рівень Execution (Виконання) має такі технології, як захист від експлойтів, захист від програм-вимагачів, розширений сканер пам'яті та сканер сценаріїв Script Scanner (AMSI). На рівні Post-execution (Після виконання) використовується захист від ботнетів, хмарна система захисту від шкідливого програмного забезпечення й пісочниця. Цей багатофункціональний набір основних технологій забезпечує неперевершений рівень захисту.

Антиспам	Антиспам — це важливий компонент будь-якого поштового сервера. ESET Mail Security використовує найсучасніший механізм антиспаму, який захищає від спаму й фішингових повідомлень із надзвичайно високим показником виявлення. ESET Mail Security кілька разів поспіль лідирує в тестах на фільтрацію спаму, які проводяться Virus Bulletin — провідною компанією тестування продуктів безпеки; окрім того, протягом кількох років нашому модулю антиспаму надається сертифікат VBSpam+. Показник виявлення механізму антиспаму досяг 99,99 % із нульовою кількістю помилкових спрацювань, що свідчить про те, що він є провідною технологією захисту від спаму. Антиспам ESET Mail Security містить низку технологій (RBL, DNSBL, аналіз цифрових відбитків, перевірка репутації, аналіз вмісту, правила, ручне складання білих/чорних списків, захист від несправжніх сповіщень про стан доставки й перевірка повідомлення з використанням SPF і DKIM) для максимального виявлення загроз. Антиспам ESET Mail Security працює в хмарі, а більшість баз даних розташована в центрах обробки даних ESET. Хмарні служби антисмапу дозволяють швидко оновити дані, забезпечуючи швидку реакцію на появу нового спаму.
Захист від фішинг-атак	Функція, яка не дозволяє користувачам отримувати доступ до веб-сторінок, для яких відомо, що вони використовуються для фішинг-атак. Електронні листи можуть містити посилання на веб-сайти, на яких розповсюджуються фішингові програми, а ESET Mail Security використовує покращений аналізатор, який виявляє такі URL-посилання в тілі й темі вхідних електронних листів. Посилання перевіряються за базою даних фішингу.
Правила	Ці правила дають адміністраторам змогу фільтрувати небажані електронні листи та вкладення відповідно до політики компанії. Вкладення, зокрема виконувані файли, мультимедійні файли, захищені паролем архіви тощо. З відфільтрованими повідомленнями електронної пошти та їхніми вкладеннями можна виконувати різні дії, зокрема переміщати в карантин, видаляти, надсилати сповіщення або входити в події.
Експортувати на сервер syslog (Arcsight)	Дає змогу дублювати вміст журналу захисту поштового сервера на сервері syslog у форматі Common Event Format (CEF) для подальшого використання з рішеннями для керування журналами, таким як Micro Focus ArcSight. Події можна передавати в ArcSight через ArcSight або експортувати у файли. Це забезпечує зручний спосіб централізованого моніторингу подій безпеки та керування ними. Ця функція може стати в пригоді, особливо в тих випадках, коли у вас є складна інфраструктура з великою кількістю серверів Microsoft Exchange Server із рішенням ESET Mail Security.
Сканування поштових скриньок Office 365	Для організацій, які використовують гібридне середовище Exchange, додає можливість сканувати поштові скриньки в хмарі.
ESET LiveGuard Advanced	Хмарна служба ESET. Якщо ESET Mail Security оцінює електронний лист як підозрілий, він тимчасово переміщується в карантин ESET LiveGuard Advanced. Підозрілі електронні листи автоматично надсилаються на сервер ESET LiveGuard Advanced для аналізу за допомогою обробників виявлення шкідливого програмного забезпечення. Після цього ESET Mail Security отримує результат аналізу. Підозрілий електронний лист обробляється залежно від отриманого результату.

Диспетчер поштового карантину з веб-інтерфейсом	Адміністратор може перевіряти об'єкти в карантині та видаляти або розблоковувати їх. Ця функція забезпечує простий у використанні інструмент керування. Веб-інтерфейс карантину дає змогу керувати вмістом віддалено. Можна вибрати його адміністраторів і (або) делегувати доступ. Окрім того, користувачі з доступом лише до своїх повідомлень можуть переглядати власний спам і керувати ним після входу в веб-інтерфейс поштового карантину.
Надіслати звіти про поштовий карантин	Звіти про карантин — це електронні листи, надіслані вибраним користувачам або адміністраторам, щоб надати інформацію про всі повідомлення електронної пошти в карантині. Вони також дають їм змогу віддалено керувати вмістом на карантині.
Сканування бази даних поштових скриньок за вимогою	Сканування бази даних поштових скриньок за вимогою дає адміністраторам можливість вручну просканувати вибрані поштові скриньки або запланувати запуск сканування в неробочі години. Сканер бази даних поштових скриньок використовує API EWS (Exchange Web Services) для підключення до Microsoft Exchange Server через HTTP/HTTPS. Окрім цього, для підвищення продуктивності сканер використовує паралелізм під час сканування.
Кластер ESET	Кластер ESET дає змогу керувати кількома серверами з одного місця. Як і випадку з ESET File Security для Microsoft Windows Server, підключення вузлів сервера до кластера полегшує керування через можливість розповсюдити одну конфігурацію на всі вузли учасників кластера. Кластер ESET також можна використовувати для синхронізації баз даних сірих списків і вмісту локального поштового карантину.
Виключення процесів	Виключає певні процеси зі сканування на наявність шкідливого програмного забезпечення за доступом. У деяких ситуаціях сканування на наявність шкідливого програмного забезпечення за доступом може спричиняти конфлікти, наприклад під час резервного копіювання або перенесення віртуальних машин. Виключення процесів допомагають мінімізувати ризик потенційних конфліктів і підвищити продуктивність виключених програм, що позитивно впливає на загальну продуктивність і стабільність системи. Виключення процесу або програми – це виключення його/її виконуваного файлу (.exe).
eShell (Оболонка ESET)	eShell 2.0 тепер доступний у ESET Mail Security. eShell — це інтерфейс командного рядка, який надає досвідченим користувачам та адміністраторам більше можливостей для керування серверними продуктами ESET.
ESET PROTECT	Ефективніша інтеграція з ESET PROTECT, зокрема можливість запланувати різні завдання. Більш докладну інформацію див. в онлайн-довідці ESET PROTECT.
Інсталяція на основі компонентів	Під час інсталяції можна вибрати лише потрібні компоненти продукту.
Захист від підміни відправника	Нова функція, яка захищає від поширених практик підробки даних відправника електронного листа називається підміною відправника. Одержувач електронного листа, найімовірніше, не зможе відрізнити дійсного відправника від підробленого, оскільки електронний лист має такий вигляд, ніби його надіслано від надійного джерела. У розділі "Додаткові параметри" можна ввімкнути й налаштувати захист від підмін відправника або створити налаштовувані правила.

Підписання DKIM	ESET Mail Security забезпечує функцію підписання DKIM, яка підвищує безпеку вихідних електронних листів. Виберіть сертифікат клієнта та вкажіть, які заголовки електронного листа будуть підписуватися з використанням DKIM. Якщо потрібно налаштувати підписування DKIM для кількох доменів, для кожного домену його можна налаштувати окремо.

Нові функції та можливості

Нові функції й поліпшення в ESET Mail Security:

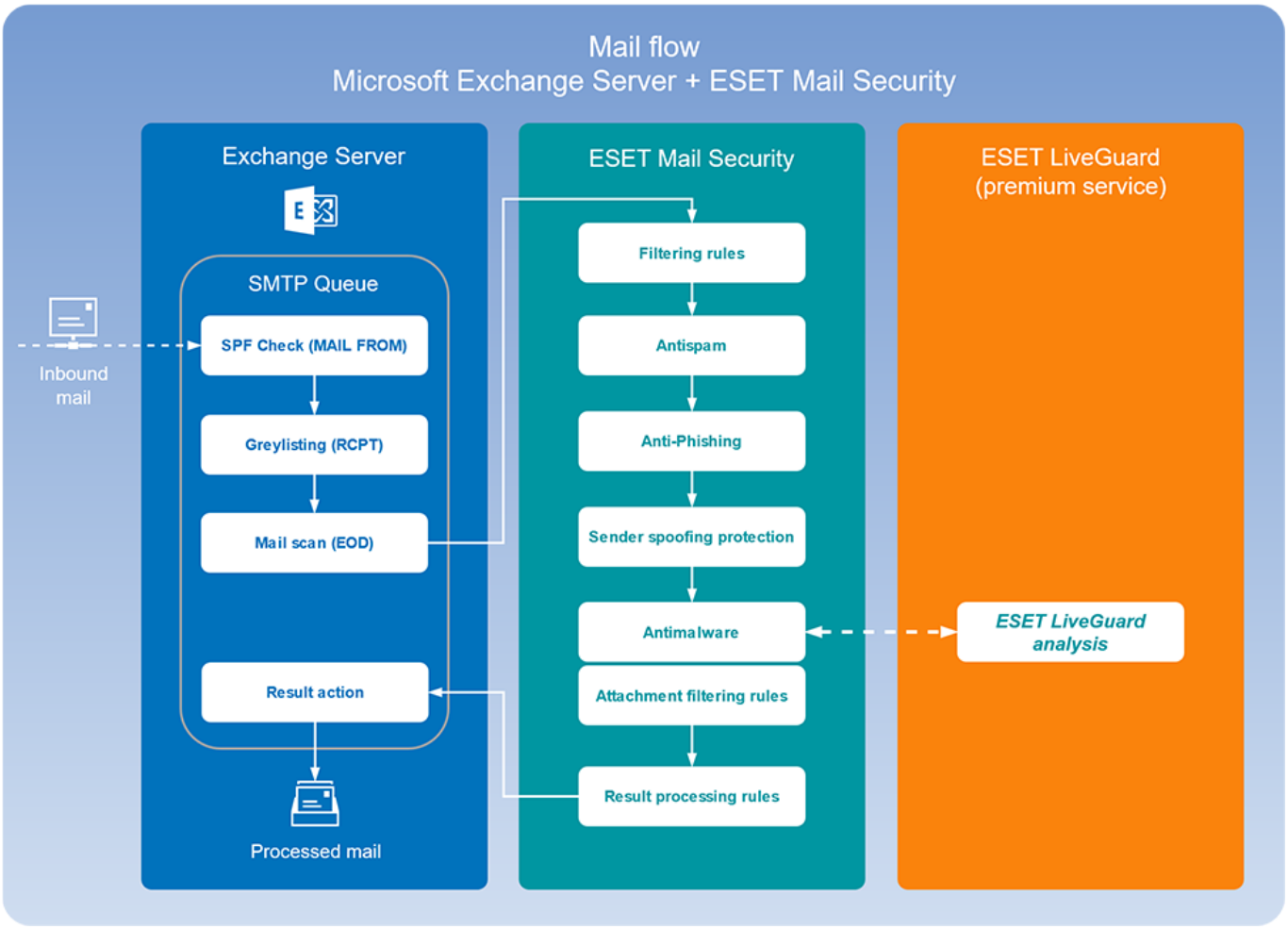
- Справжній 64-розрядний продукт
- Сканування поштових скриньок Office 365
- Захист електронної пошти від фішинг-атак
- Захист від несправжніх сповіщень про стан доставки
- Надіслати адміністраторські звіти про поштовий карантин
- Синхронізація локального поштового карантину в кластері ESET
- Журнал захисту SMTP
- ESET LiveGuard Advanced
- ESET Inspect підтримка
- ESET RMM
- Експортувати на сервер syslog (Arcsight)
- Ізоляція мережі
- Захист на основі машинного навчання
- Журнали аудиту
- Оновлення компонентів мікропрограми
- Захист від підміни відправника
- Підписання DKIM
- Сканування поштових скриньок Microsoft 365

Див. детальні журнали змін для ESET Mail Security.

Передавання пошти

На діаграмі нижче показано передавання пошти в Microsoft Exchange Server і ESET Mail Security. Докладні відомості про використання ESET LiveGuard Advanced з ESET Mail Security див. в онлайн-

довідці ESET LiveGuard Advanced.



Функції ESET Mail Security і ролі Exchange Server

У наведеній нижче таблиці наведено інформацію про функції, доступні для кожної підтримуваної версії Microsoft Exchange Server і відповідних ролей. Майстер інсталяції ESET Mail Security перевіряє ваше середовище під час інсталяції. Після інсталяції в ESET Mail Security відображатимуться тільки ті функції, які відповідають виявленій версії сервера Exchange Server та його ролям.

Версія Exchange Server і роль сервера	**Антиспам**	**Захист від фішинг-атак**	**Правила**	**Захист передачі пошти**	**Сканування бази даних поштових скриньок за вимогою**	**Захист бази даних поштової скриньки**
Microsoft Exchange Server 2010 (кілька ролей)	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2010 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2010 (роль "Транспортний сервер-концентратор")	✔	✔	✔	✔	✔	✔

Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2010 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (кілька ролей)	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2016 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2016 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2019 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2019 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔

Ролі Exchange Server

Ролі "Межовий транспорт" і "Транспортний сервер-концентратор"

Для обох серверних ролей ("Межовий транспорт" і "Транспортний сервер-концентратор") функції антиспаму вимкнуто за замовчуванням. Це бажана конфігурація в організації Exchange із сервером межового транспорту. Рекомендуємо мати сервер межового транспорту з налаштованим модулем "Антиспам" ESET Mail Security, який буде фільтрувати повідомлення перед їхнім пересиланням в організацію Exchange.

Бажано, щоб модуль "Антиспам" виконувався на сервері з роллю "Межовий транспорт", оскільки в такому разі ESET Mail Security може відфільтровувати спам завчасно. Це дасть змогу уникнути зайвого навантаження на рівнях мережі. На основі цієї конфігурації вхідні повідомлення фільтруються ESET Mail Security на сервері межового транспорту, тому їх можна безпечно перенести на транспортний сервер-концентратор без потреби в подальшій фільтрації.

Припустимо, ваша організація не використовує сервер межового транспорту, а має лише транспортний сервер-концентратор. У такому разі рекомендуємо ввімкнути функції модуля "Антиспам" на транспортному сервері-концентраторі, який отримує вхідні повідомлення з Інтернету через протокол SMTP.

Через технічні обмеження Microsoft Exchange Server 2010 і новіших версій ESET Mail Security не підтримує розгортання Microsoft Exchange Server тільки із серверною роллю "Клієнтський доступ" (CAS, автономний сервер клієнтського доступу).

Модулі захисту

До основних функцій ESET Mail Security належать такі модулі захисту:

Антивірус

Антивірусний захист — одна з основних функцій ESET Mail Security. Антивірус забезпечує захист від зловмисних атак на систему завдяки контролю файлів, електронної пошти та обміну даними через інтернет-з'єднання. Якщо виявлено загрозу зі шкідливим кодом, антивірусний модуль може знешкодити її блокуванням, очистити інфікований об'єкт, видалити його, а потім перемістити його в карантин.

Антиспам

Захист від спаму містить низку технологій (RBL, DNSBL, аналіз цифрових відбитків, перевірка репутації, аналіз вмісту, правила, ручне складання білих/чорних списків тощо) для максимального виявлення загроз, пов'язаних із електронною поштою.
Антиспам ESET Mail Security працює в хмарі, а більшість хмарних баз даних розташована в центрах обробки даних ESET. Хмарні служби антиспаму дають змогу швидко оновлювати дані для швидкого застосування відповідних дій на появу нового спаму. Він також дає змогу видаляти неправильні або хибні дані з чорних списків ESET. Обмін даними з хмарними службами модуля "Антиспам" здійснюється за власним протоколом через порт 53535 (якщо це можливо). Якщо неможливо обмінюватися даними за протоколом ESET, замість нього використовуються служби DNS (порт 53). Однак використання DNS не настільки ефективне, оскільки для одного електронного листа потрібно надіслати кілька запитів під час класифікації спаму.

Рекомендується відкрити порт TCP/UDP 53535 для IP-адрес, зазначених у цій статті бази знань. Цей порт використовується ESET Mail Security для надсилання запитів.

Зазвичай під час класифікації спаму електронні листи або їхні частини не надсилаються. Припустимо, ESET LiveGrid® увімкнуто й ви явно дозволили надсилали зразки для аналізу. У цьому разі можуть надсилатися повідомлення, позначені як спам (або ймовірний спам). Це допоможе ретельно проаналізувати й вдосконалити хмарну базу даних.
Щоб повідомити про помилкове спрацювання або про помилковий негативний результат щодо спаму, див. докладну інформацію в нашій статті бази знань.
Окрім того, ESET Mail Security може використовувати метод фільтрації спаму Технологія сірих списків (за замовчуванням вимкнено).

Захист від фішинг-атак

ESET Mail Security містить захист від фішинг-атак, який не дозволяє користувачам отримувати доступ до веб-сторінок, для яких відомо, що вони використовуються для фішинг-атак. Електронні листи можуть містити посилання на веб-сайти, на яких розповсюджуються фішингові програми, а ESET Mail Security використовує покращений аналізатор, який виявляє такі посилання (URL-адреси) в тілі й темі вхідних електронних листів. Посилання перевіряються за базою даних фішингових веб-сайтів. Окрім того, вони оцінюються на відповідність правилам із умовою Тіло повідомлення.

Правила

Доступність правил для параметрів Захист бази даних поштової скриньки, Сканування бази даних поштових скриньок за вимогою і Захист передачі пошти у вашій системі залежить від того, яку версію Microsoft Exchange Server інстальовано на сервері з ESET Mail Security.
За допомогою правил можна вручну визначати умови фільтрації електронних листів і дії, які будуть виконуватися з відфільтрованими електронними листами. Є різні набори умов і дій. Можна створити окремі правила й комбінувати їх. Якщо в одному правилі використовуються кілька умов, вони об'єднуються за допомогою логічного оператора AND. Відповідно, правило виконується тільки тогді, коли виконано всі його умови. Якщо створено кілька правил, буде застосовано логічний оператор OR. Це означає, що програма запустить перше правило, для якого виконано умови.
Перший метод, який використовується в послідовності процедур сканування, — це технологія сірих списків (якщо ввімкнуто відповідний параметр). Наступні процедури завжди виконуватимуть такі методи (у вказаній послідовності): захист на основі правил, визначених користувачем, антивірусне сканування і сканування на наявність спаму.

Багаторівневий захист

ESET Mail Security забезпечує комплексний захист на різних рівнях:

- Захист бази даних поштової скриньки
- Захист передачі пошти
- Сканування бази даних поштових скриньок за вимогою
- Сканування бази даних поштових скриньок Microsoft 365

> Подання з докладними відомостями див. в таблиці зіставлення функцій ESET Mail Security з версіями Microsoft Exchange Server і ролями сервера.

Захист бази даних поштової скриньки

Процес сканування поштових скриньок ініціюється і контролюється Microsoft Exchange Server. Електронні листи в базі даних сховища Microsoft Exchange Server постійно скануються. Залежно від версії Microsoft Exchange Server, версії інтерфейсу VSAPI та визначених користувачем параметрів процес сканування може бути ініційовано в будь-якій із наведених нижче ситуацій:

- Коли користувач отримує доступ до електронної пошти, наприклад, в поштовому клієнті (електроні листи завжди скануються обробником виявлення найновішої версії).
- У фоновому режимі за умови незначного використання Microsoft Exchange Server.
- Проактивно (на основі внутрішнього алгоритму Microsoft Exchange Server).

> Захист бази даних поштових скриньок недоступний для Microsoft Exchange Server 2013, 2016 і 2019.

Захист бази даних поштових скриньок доступний для таких систем:

Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2010 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2010 (кілька ролей)	✔	✔	✔	✔	✔	✔

Сканування цього типу можна виконати в конфігурації з одним сервером, де на одному комп'ютері налаштовано кілька ролей Exchange Server (за наявності ролей "Поштова скринька" або "Внутрішній сервер").

Захист передачі пошти

Фільтрація на рівні сервера SMTP захищена спеціальним плагіном. На сервері Microsoft Exchange Server 2010 і 2010, який має роль "Межовий транспорт" і "Транспортний сервер-концентратор", плагін реєструється як транспортний агент.

Фільтрація на рівні сервера SMTP, яку виконує транспортний агент, забезпечує захист у формі правил антивірусу й антиспаму, а також правил, налаштованих користувачами. На відміну від фільтрації VSAPI, фільтрація на рівні сервера SMTP виконується до прибуття просканованого електронного листа в поштову скриньку Microsoft Exchange Server.

Раніше ця функціональність називалася фільтрацією повідомлень на рівні сервера SMTP. Цей захист надається транспортним агентом і доступний тільки для сервера Microsoft Exchange Server 2010 (або новішої версії), який має роль "Межовий транспорт" і "Транспортний сервер-концентратор". Сканування цього типу можна виконати в конфігурації з одним сервером, де на одному комп'ютері налаштовано кілька ролей Exchange Server (за умови наявності на ньому однієї з наведених вище ролей).

Захист передачі пошти доступний для таких систем:

Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2010 (кілька ролей)	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (кілька ролей)	✔	✔	✔	✔	✔	✔

Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2013 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2016 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2016 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2019 (роль "Межовий транспорт")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2019 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔

Сканування бази даних поштових скриньок за вимогою

Дає змогу виконувати сканування бази даних поштових скриньок Exchange або створити розклад його запуску. Ця функція доступна тільки для Microsoft Exchange Server 2010 (або новіших версій), які виконують роль "Поштовий сервер" або "Транспортний сервер-концентратор". Це також стосується конфігурацій з одним сервером, де на одному комп'ютері налаштовано кілька ролей Exchange Server (за наявності однієї з указаних вище ролей сервера).

Сканування бази даних поштових скриньок за вимогою доступне для таких систем:

Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2010 (кілька ролей)	✔	✔	✔	✔	✔	✔

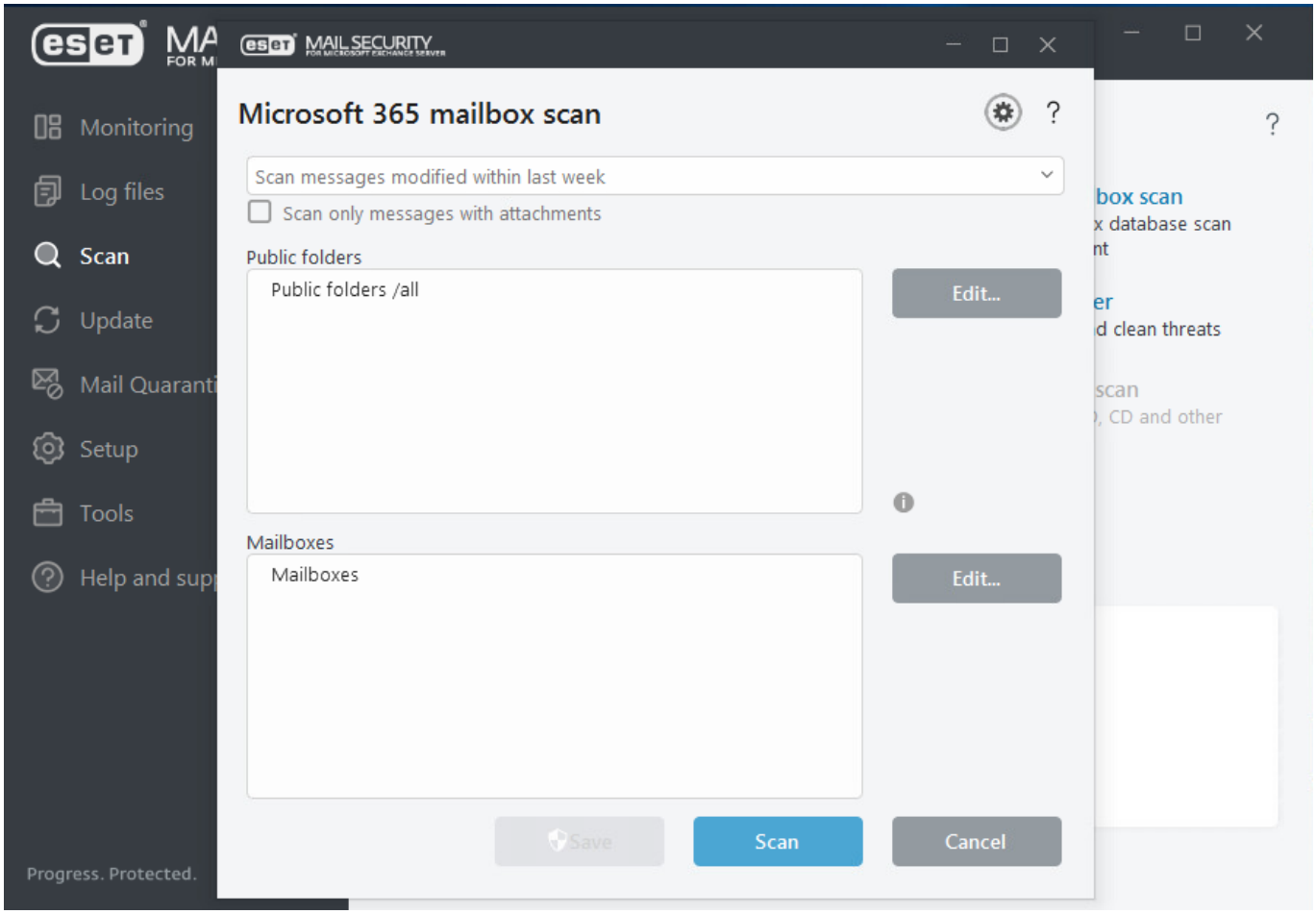
Версія Exchange Server і роль сервера	Антиспам	Захист від фішинг-атак	Правила	Захист передачі пошти	Сканування бази даних поштових скриньок за вимогою	Захист бази даних поштової скриньки
Microsoft Exchange Server 2010 (роль "Транспортний сервер-концентратор")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2010 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (кілька ролей)	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2013 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2016 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔
Microsoft Exchange Server 2019 (роль "Поштова скринька")	✔	✔	✔	✔	✔	✔

Сканування бази даних поштових скриньок Microsoft 365

ESET Mail Security забезпечує функцію сканування гібридних середовищ Microsoft 365. Вона доступна й відображається в ESET Mail Security тільки тоді, коли ви маєте гібридне середовище Exchange (локальний сервер і хмара). Підтримуються обидва сценарії маршрутизації: через **Exchange Online** або через **локальну** організацію. Докладніші відомості див. в розділі Transport routing in Exchange hybrid deployments (Транспортні маршрути в гібридних середовищах Exchange).

Щоб активувати цю функцію, зареєструйте сканер ESET Mail Security.

Сканування віддалених поштових скриньок Microsoft 365 і загальнодоступних папок можна використовувати так само, як і звичайне сканування бази даних поштових скриньок за вимогою.



Запуск повного сканування бази даних електронної пошти у великих середовищах може призвести до небажаних навантажень системи. Щоб уникнути цієї проблеми, запускайте сканування для окремих баз даних або поштових скриньок. Щоб додатково мінімізувати вплив на систему, використовуйте фільтр часу у верхній частині вікна. Наприклад, замість того, щоб використовувати функцію **Сканувати всі повідомлення**, можна вибрати параметр **Сканувати повідомлення, змінені за останній тиждень**.

Рекомендуємо налаштувати Microsoft 365. Натисніть клавішу **F5** і виберіть пункти **Сервер** > **Сканування бази даних поштових скриньок за вимогою**. Див. також розділ Відомості облікового запису сканування бази даних.

Щоб переглянути активність сканування поштових скриньок Office 365, установіть прапорець **Файли журналу** > **Сканування бази даних поштових скриньок**.

Системні вимоги

Непідтримувана операційна система:

- Microsoft Windows Server 2022 (основні серверні компоненти й досвід роботи з комп’ютером)
- Microsoft Windows Server 2019 (Server Core й Desktop Experience)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

- Microsoft Windows Server 2012

Підтримувані версії Microsoft Exchange Server:

- Microsoft Exchange Server 2019 (до CU13)
- Microsoft Exchange Server 2016 (до CU23)
- Microsoft Exchange Server 2013 до CU23 (CU1 і CU4 не підтримуються)
- Microsoft Exchange Server 2010 SP1, SP2, SP3 (до RU32)

Роль автономного клієнтського доступу (CAS) не підтримується. Докладнішу інформацію див. в розділі Ролі сервера Exchange.
Див. функції ESET Mail Security і ролі Exchange Server Roles, щоб визначити, які функції доступні для кожної підтримуваної версії Microsoft Exchange Server і її ролей.

Мінімальні системні вимоги:

Компонент	Вимога
Процесор	Одноядерний Intel або AMD x64
Пам’ять	256 МБ вільної пам’яті
Жорсткий диск	700 МБ вільного місця на диску
Роздільна здатність екрана	800 x 600 пікселів або вище

ESET Mail Security має такі самі рекомендовані вимоги до обладнання, які застосовуються до Microsoft Exchange Server. Більш докладні відомості див. в наведених нижче технічних статтях Microsoft:

Microsoft Exchange Server 2010

Microsoft Exchange Server 2013

Microsoft Exchange Server 2016

Перед інсталяцією продукту з безпеки ESET захисту наполегливо рекомендуємо інсталювати найновіший пакет оновлень для операційної системи Microsoft Server і програми. Рекомендуємо інсталювати останні оновлення і виправлення Windows завжди, коли вони будуть доступні.

Підготовка до інсталяції

Щоб підготуватися до інсталяції продукту, рекомендовано виконати наведені нижче дії.

- Після придбання ESET Mail Security завантажте пакет інсталяції *.msi* з веб-сайту ESET.
- Переконайтеся, що сервер, де ви плануєте інсталювати ESET Mail Security, відповідає системним вимогам.
- Увійдіть на сервер за допомогою облікового запису адміністратора.

• Якщо ви збираєтеся оновлювати поточну версію ESET Mail Security, рекомендуємо створити резервну копію конфігурації за допомогою функції Експорт параметрів.

• За потреби видаліть стороннє антивірусне програмне забезпечення із системи. Рекомендуємо використовувати ESET AV Remover. Список сторонніх антивірусів, які можна видалити за допомогою ESET AV Remover, наведено в цій статті бази знань.

• Якщо ви інсталюєте ESET Mail Security на Windows Server 2016, корпорація Майкрософт рекомендує видалити компоненти Windows Defender і скасувати дію Windows Defender ATP, щоб уникнути проблем, спричинених роботою кількох антивірусних продуктів на комп'ютері.

• Якщо ви інсталюєте ESET Mail Security на Windows Server 2019 або Windows Server 2022, корпорація Майкрософт рекомендує перевести Windows Defender у пасивний режим, щоб уникнути проблем, спричинених роботою кількох антивірусних продуктів на комп'ютері.

Якщо під час інсталяції ESET Mail Security у Windows Server 2016, 2019 або 2022 є **компоненти Windows Defender**, ESET Mail Security вимикає ці компоненти, щоб уникнути конфліктів між кількома антивірусними продуктами в режимі реального часу. Окрім того, компоненти Windows Defender вимикаються ESET Mail Security під час кожного запуску і перезапуску системи.
Проте є виняток: якщо ви інсталюєте компонент без **функції захисту файлової системи в режимі реального часу**, Windows Defender у Windows Server 2016 не вимикається.

• Подання з докладними відомостями див. в таблиці зіставлення функцій ESET Mail Security з версіями Microsoft Exchange Server і ролями сервера.

• Докладні відомості про те, як перевірити кількість поштових скриньок за допомогою інструмента "Кількість поштових скриньок", див. в нашій статті бази знань. Після інсталяції ESET Mail Security у нижній частині вікна "Моніторинг" відображатимуться поточне значення лічильника поштових скриньок.

Інсталятор ESET Mail Security можна запускати у двох режимах.

• Головне вікно програми — Рекомендується виконувати інсталяцію за допомогою майстра інсталяції.

• Автоматична інсталяція — ESET Mail Security також можна інсталювати через командний рядок.

• Оновлення до останньої версії – Якщо ви використовуєте старішу версію ESET Mail Security, можна вибрати відповідний спосіб оновлення.

Після інсталяції або оновлення ESET Mail Security виконайте наведені нижче дії.

Активація продукту

Сценарії активації, доступні у вікні активації, залежать від країни й джерела отримання продукту.

Завдання після інсталяції

Список рекомендованих завдань, які можна виконати після інсталяції програми ESET Mail Security.

Налаштування загальних параметрів

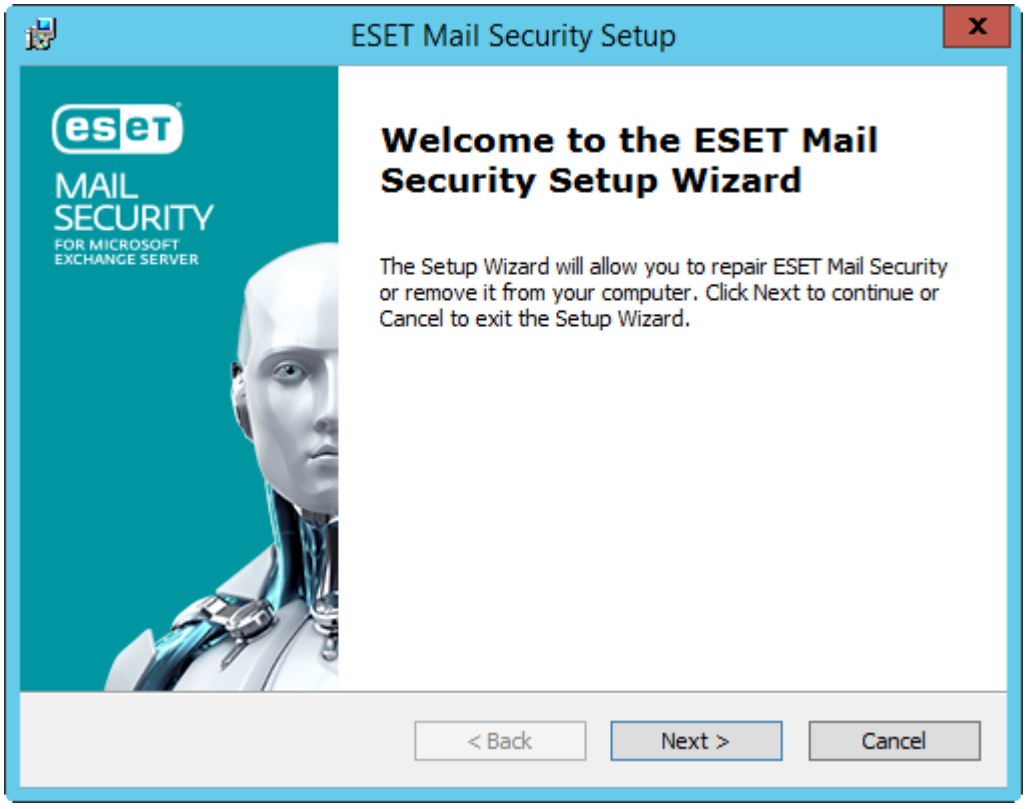
Щоб налаштувати параметри ESET Mail Security, змінюйте додаткові параметри для кожної функції.

Етапи інсталяції ESET Mail Security

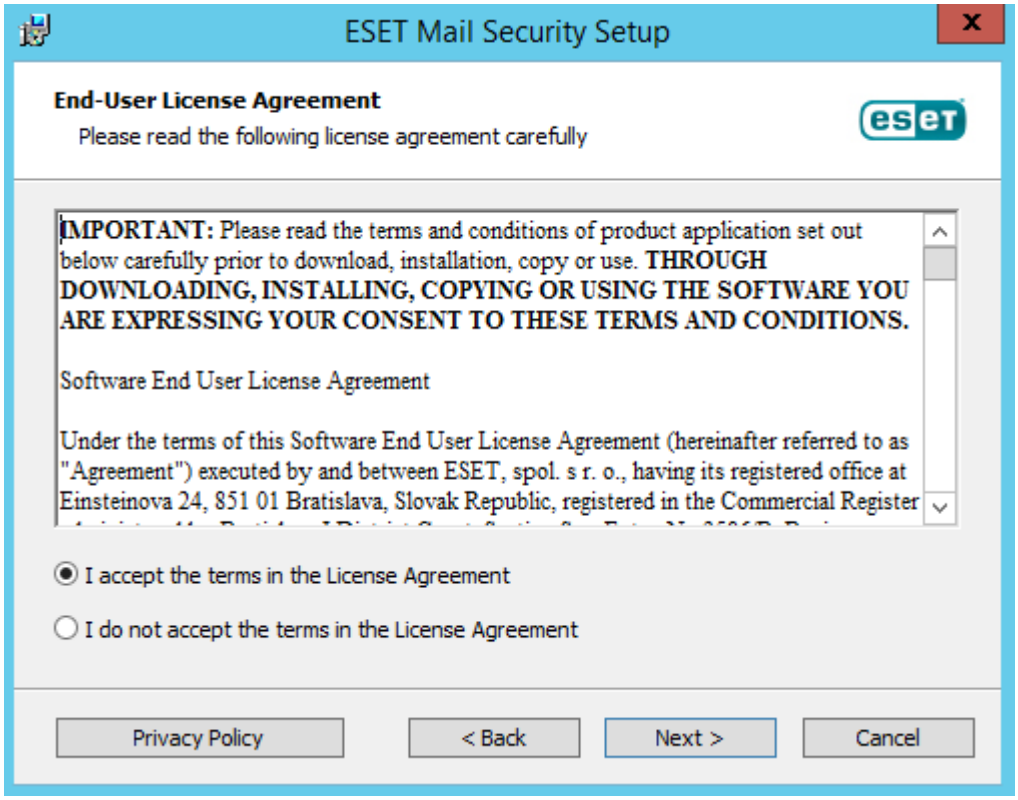
Це типовий майстер інсталяції головного вікна програми. Двічі натисніть пакет .msi і дотримуйтеся наведених нижче вказівок з інсталяції ESET Mail Security.

1. Клацніть **Далі**, щоб продовжити, або **Скасувати**, щоб закрити вікно інсталяції.

2. Майстер інсталяції запускається мовою, указаною в полі **Ваше розташування** в розділі **Регіон** > **Розташування** операційної системи (або полі **Поточне розташування** в розділі **Мова та регіон** > **Розташування** в старіших системах). У розкривному меню виберіть **мову продукту**, якою буде інстальовано ESET Mail Security. Вибрана для ESET Mail Security мова не залежить від мови майстра інсталяції.



3. Натисніть **Далі**. Відобразиться ліцензійна угода з кінцевим користувачем. Коли приймете умови ліцензійної угоди з кінцевим користувачем і політики конфіденційності, натисніть **Далі**.



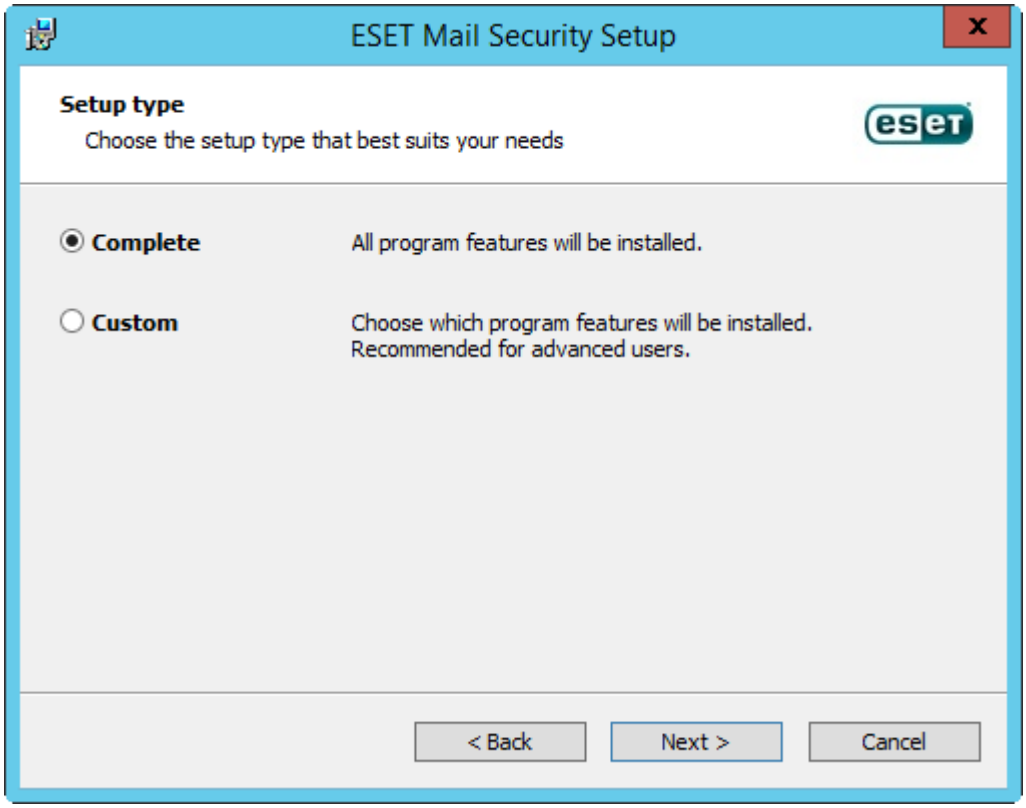
4. Виберіть один із доступних типів інсталяції (вони залежать від операційної системи).

Повна

Інсталяція всіх функцій ESET Mail Security.

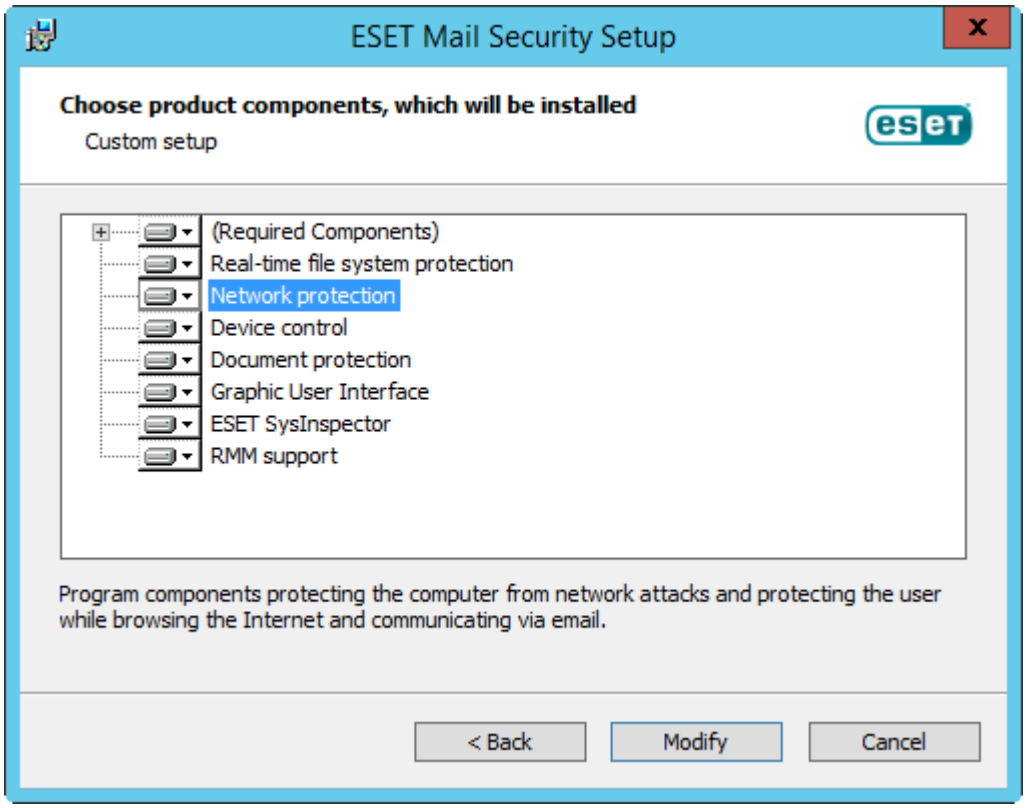
Інсталятор містить тільки важливі модулі. Усі інші модулі завантажуються під час першого оновлення модуля після активації продукту.

Якщо ви плануєте використовувати локальний карантин для електронних листів й не хочете зберігати на диску C: файли повідомлень у карантині, змініть шлях до **папки даних** на потрібний диск і розташування. Однак пам'ятайте, що всі файли даних ESET Mail Security будуть зберігатися в цьому розташуванні.



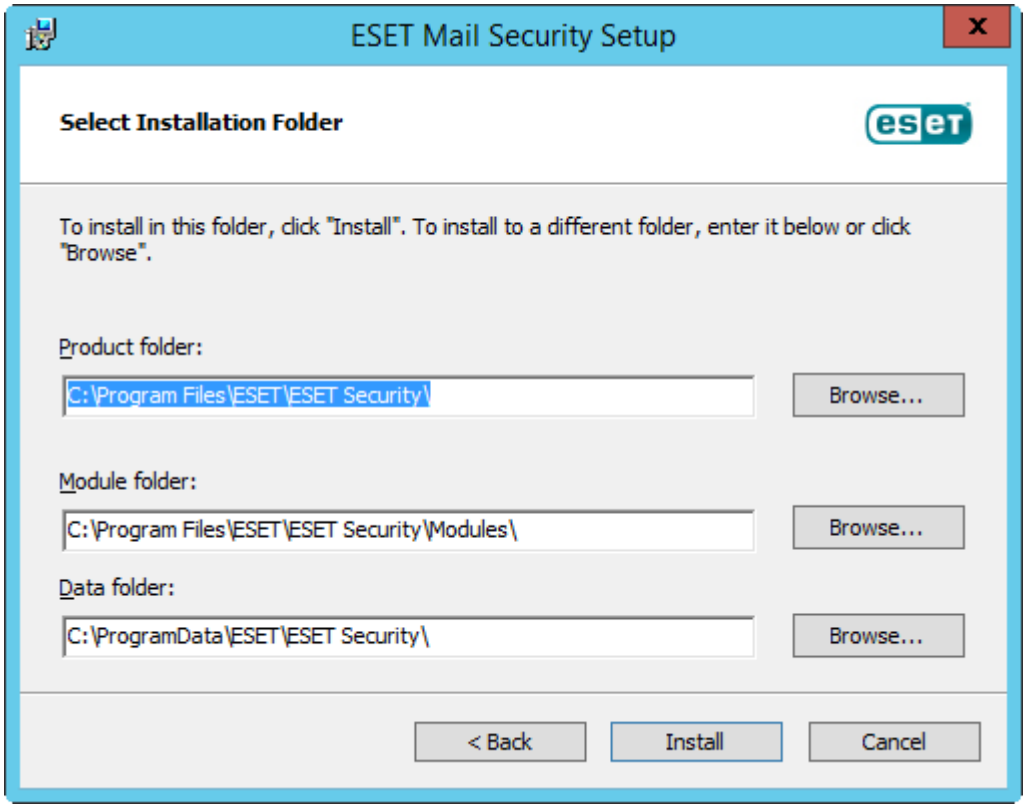
Спеціальна

Дає змогу вибрати функції ESET Mail Security, які буде інстальовано в системі. Перед початком інсталяції відобразиться список модулів і функцій продукту. Це корисно, якщо потрібно встановити лише певні компоненти ESET Mail Security.



5. З’явиться запит на вибір розташування для інсталяції ESET Mail Security. За замовчуванням програма інсталюється в папці *C:\Program Files\ESET\ESET Mail Security*. Щоб змінити

розташування, натисніть **Огляд** (не рекомендовано).

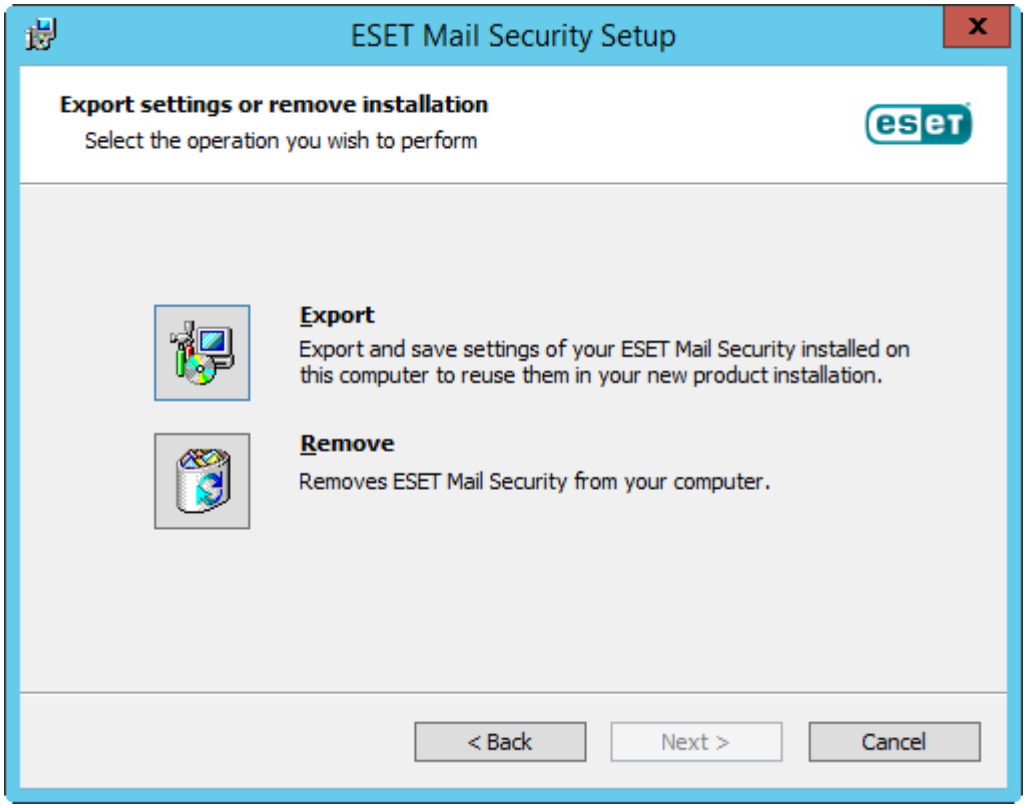


6. Клацніть **"Інсталювати"**, щоб розпочати інсталяцію. Після інсталяції з'явиться запит на активацію ESET Mail Security.

Експортувати настройки або видалити інстальований продукт

Можна експортувати й зберегти параметри або видалити інсталяцію. Для цього запустіть пакет інсталятора *.msi*, який використовувався для початкової інсталяції, або перейдіть до розділу **Програми й засоби** (доступний на панелі керування Windows), клацніть правою кнопкою миші ESET Mail Security і виберіть пункт **Змінити**.

Можна **експортувати** параметри ESET Mail Security або повністю **видалити** ESET Mail Security.



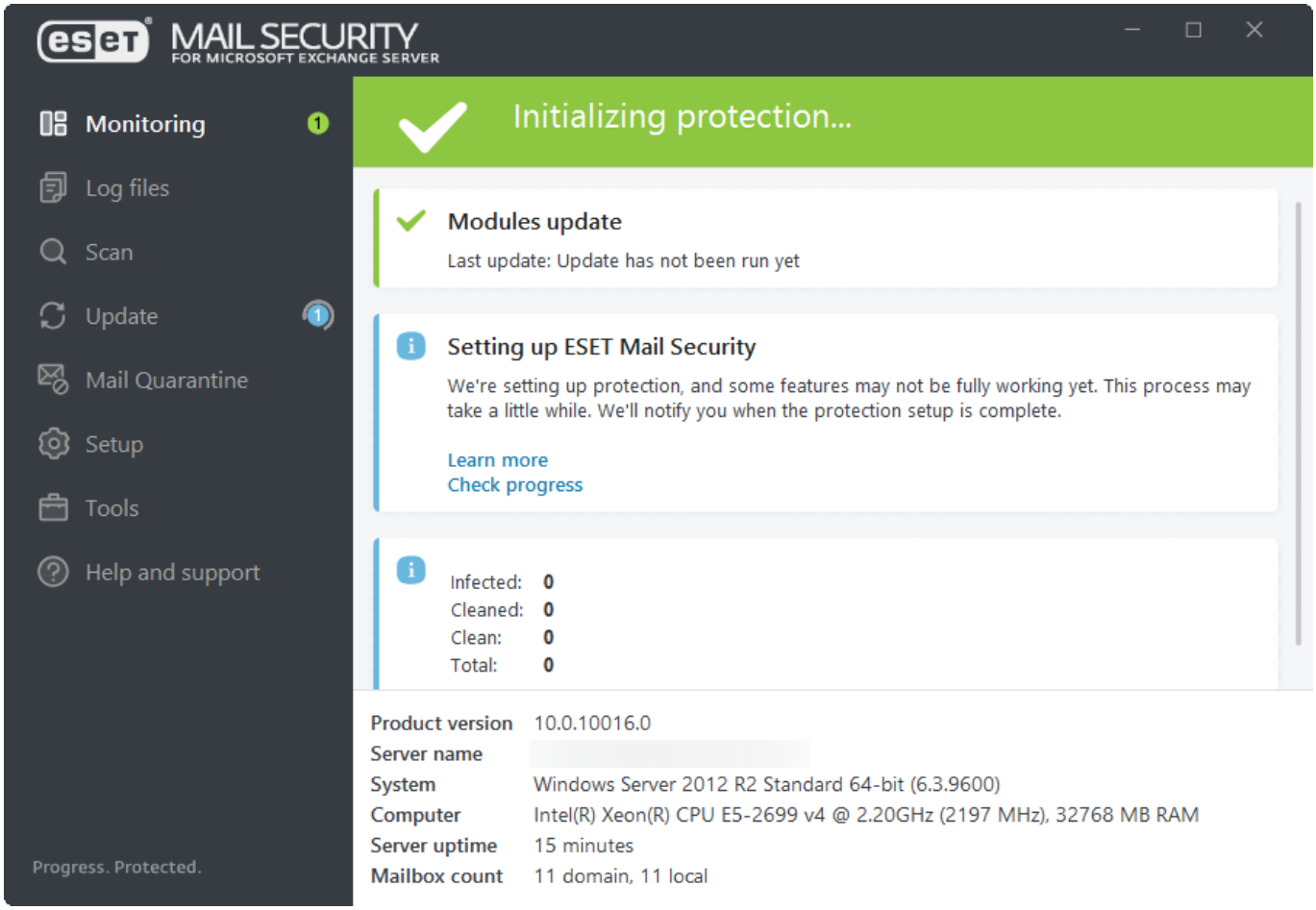
Початкове оновлення модулів

До складу інсталятора входять тільки основні модулі. Це дає змогу зменшити мережевий трафік, пов’язаний із розміром інсталятора, й зекономити ресурси. Усі інші модулі завантажуватимуться під час першого оновлення модуля після активації продукту. Основна перевага — інсталятор значно меншого розміру; ESET Mail Security завантажує тільки найновіші модулі програми під час активації продукту.

Мінімальний інсталятор модулів містить такі модулі:

- Loaders
- Модуль підтримки Anti-Stealth
- Модуль зв’язку Direct Cloud
- Модуль підтримки перетворення
- Конфігурація
- SSL

Після активації продукту з’являється статус **Ініціалізація захисту** з відомостями про ініціалізацію функцій.



У разі виникнення проблем із завантаженням модулів (наприклад, через відсутнє підключення до мережі, параметри брандмауера або проксі-сервера) відобразиться попередження про статус програми **Слід звернути увагу**.
Щоб знову запустити процес оновлення, у головному вікні програми клацніть **Оновлення** > **Перевірка наявності оновлень**.
Після кількох невдалих спроб для програми відображатиметься статус **Не вдалося налаштувати захист** (червоного кольору). Якщо не вдається оновити модулі, завантажте повний інсталятор *.msi* для ESET Mail Security.

Якщо сервер не підключено до Інтернету й потребує оновлень, скористайтеся наведеними нижче способами, щоб завантажити файли модуля оновлення із серверів оновлення ESET:

- Оновлення із дзеркала
- Використання інструмента "Дзеркало"

Автоматична інсталяція

Щоб завершити інсталяцію через командний рядок, виконайте цю команду: `msiexec /i <packagename> /qn /l*xv msi.log`

Скористайтеся засобом перегляду подій Windows для перегляду **журналу програми** (див. записи в розділі Source: MsiInstaller). Інформація, наведена в журналі, дасть змогу переконатися, що інсталяцію виконано успішно, або дізнатися про проблеми з інсталяцією.

Повна інсталяція на 64-розрядній системі:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Після завершення інсталяції запуститься графічний інтерфейс користувача ESET, а в області сповіщень Windows відобразиться піктограма .

Інсталяція продукту **вказаною мовою** (наприклад, німецькою):
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Додаткові відомості й список кодів мови див. в розділі **Параметри мови** теми Інсталяція з командного рядка.

Визначаючи значення для параметра `REINSTALL`, необхідно вказати решту функцій, які не використовуються як значення для параметра `ADDLOCAL` або `REMOVE`. Для коректної інсталяції командного рядка необхідно вказати всі функції як значення для параметрів `REINSTALL, ADDLOCAL` і `REMOVE`. Додавання або видалення може завершитися невдало, якщо не використовувати параметр `REINSTALL`.
Повний список функцій можна переглянути в розділі Інсталяція з командного рядка.

Повне видалення із 64-розрядної системи:
```
msiexec /x emsx_nt64.msi /qn /l*xv msi.log
```

Після успішного видалення сервер перезавантажиться автоматично.

Інсталяція з командного рядка

Наведені нижче параметри потрібно використовувати лише зі **скороченим**, основним або **відсутнім** рівнем інтерфейсу користувача. Щоб дізнатися версію, яка використовувалася `msiexec` для відповідних перемикачів командного рядка, див. документацію.

Підтримувані параметри:

APPDIR=<path>

- Шлях – дійсний шлях до каталогу.
- Каталог для інсталяції програми.
- Приклад: `emsx_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

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

MODULEDIR=<path>

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

ADDLOCAL=<list>

• Інсталяція компонентів – список необов'язкових функцій, які потрібно інсталювати локально.

• Використання з пакетами ESET *.msi*: `emsx_nt64.msi /qn ADDLOCAL=<list>`.

• Щоб дізнатися більше про властивість `ADDLOCAL`, перегляньте сторінку https://docs.microsoft.com/uk-ua/windows/desktop/Msi/addlocal.

• Список `ADDLOCAL` – це розділений комами список усіх функцій, які буде інстальовано.

• Під час вибору функції, яку потрібно інсталювати, додайте в список повний шлях (усі батьківські функції).

REMOVE=<list>

• Інсталяція компонентів – батьківська функція, яку ви не хочете інсталювати локально.

• Використання з пакетами ESET .msi: `emsx_nt64.msi /qn REMOVE=<list>`.

• Щоб дізнатися більше про властивість `REMOVE`, перегляньте сторінку https://docs.microsoft.com/uk-ua/windows/desktop/Msi/remove.

• Список `REMOVE` – це розділений комами список батьківських функцій, які не інсталюватимуться (або видалятимуться, якщо їх уже інстальовано).

• Достатньо вказати лише батьківську функцію. Не потрібно додавати в список всі дочірні функції.

ADDEXCLUDE=<list>

• Список `ADDEXCLUDE` — це розділений комами список імен усіх функцій, які не інсталюватимуться.

• Під час вибору функції, яку не потрібно інсталювати, у список потрібно додати весь шлях (наприклад, усі його підфункції) і пов'язані невидимі функції.

• Приклад: `emsx_nt64.msi /qn ADDEXCLUDE=<list>`

> `ADDEXCLUDE` не можна використовувати з `ADDLOCAL`

Наявність функцій:

• **Обов'язкова**: функція інсталюється завжди.

• **Необов'язкова**. Функцію можна не вибирати для інсталяції.

• **Невидима**. Логічна функція, що обов'язково інсталюється для належної роботи інших функцій.

Список функцій ESET Mail Security:

Імена всіх функцій чутливі до регістру, наприклад `RealtimeProtection` – не те ж саме, що `REALTIMEPROTECTION`.

Ім’я функції	Наявність функцій
SERVER	Обов’язкова
RealtimeProtection	Обов’язкова
MAILSERVER	Обов’язкова
WMIProvider	Обов’язкова
HIPS	Обов’язкова
Updater	Обов’язкова
eShell	Обов’язкова
UpdateMirror	Обов’язкова
DeviceControl	Необов’язково
DocumentProtection	Необов’язково
WebAndEmail	Необов’язково
ProtocolFiltering	Невидима
NetworkProtection	Необов’язково
IdsAndBotnetProtection	Необов’язково
Rmm	Необов’язково
WebAccessProtection	Необов’язково
EmailClientProtection	Необов’язково
MailPlugins	Невидима
Cluster	Необов’язково
_Base	
eula	
ShellExt	Необов’язково
_FeaturesCore	
GraphicUserInterface	Необов’язково
SysInspector	Необов’язково
SysRescue	Необов’язково
EnterpriseInspector	Необов’язково

Якщо потрібно видалити якусь із наведених функцій, видаліть усю групу, указавши всі функції, що входять до неї. В іншому разі функцію не буде видалено. Ось дві групи (кожен рядок позначає одну групу):

```
GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailP
lugins,EmailClientProtection
```

Виключення розділу **NetworkProtection** (разом із дочірніми функціями) з інсталяції за допомогою параметра `REMOVE` та вказанням лише батьківської функції:
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

Можна також використати параметр `ADDEXCLUDE`, але потрібно вказати всі дочірні функції:
```
msiexec /i emsx_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

Щоб рішення ESET Mail Security налаштувалось автоматично після інсталяції, укажіть у команді інсталяції основні параметри конфігурації.

Інсталюйте ESET Mail Security і вимкніть ESET LiveGrid®:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log CFG_LIVEGRID_ENABLED=0
```

Список усіх властивостей конфігурації:

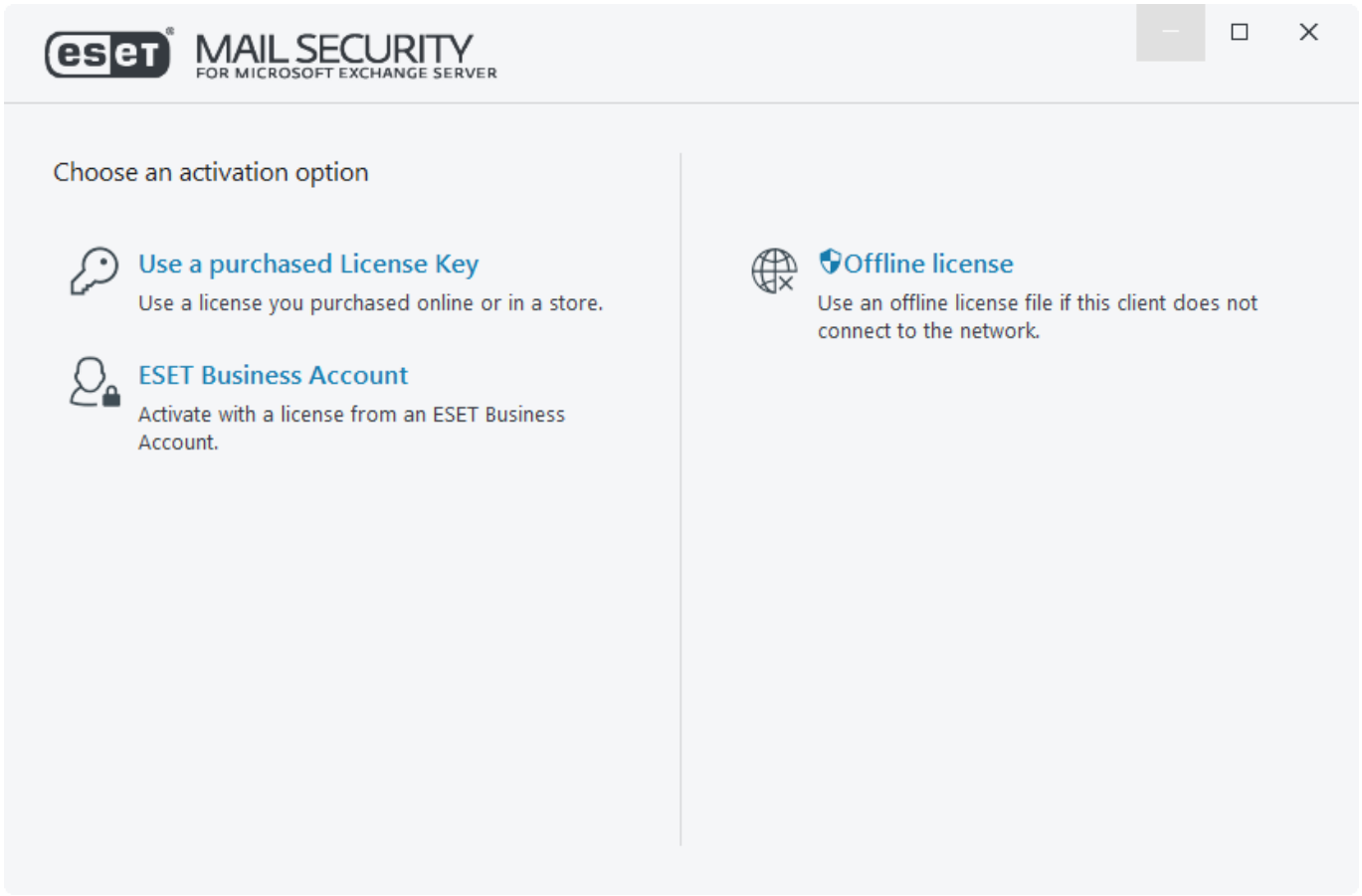
Перемикач	Значення
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0 – вимкнено, 1 – увімкнено
`CFG_LIVEGRID_ENABLED=1/0`	0 – вимкнено, 1 – увімкнено
`FIRSTSCAN_ENABLE=1/0`	0 – вимкнути, 1 – увімкнути
`CFG_PROXY_ENABLED=0/1`	0 – вимкнено, 1 – увімкнено
`CFG_PROXY_ADDRESS=<ip>`	IP-адреса проксі-сервера
`CFG_PROXY_PORT=<port>`	Номер порту проксі-сервера
`CFG_PROXY_USERNAME=<user>`	Ім’я користувача для автентифікації
`CFG_PROXY_PASSWORD=<pass>`	Пароль для автентифікації

Параметри мови: мова продукту (необхідно вказати обидва параметри)

Перемикач	Значення
`PRODUCT_LANG=`	Десятковий код мови, наприклад 1033 для English - United States. Перегляньте список кодів мов.
`PRODUCT_LANG_CODE=`	Рядок коду мови (мова й регіональні параметри) у нижньому регістрі, наприклад en-us для English - United States. Перегляньте список кодів мов.

Активація продукту

Після завершення інсталяції з’явиться запит активувати продукт.



Щоб активувати ESET Mail Security, скористайтеся будь-яким із наведених нижче способів.

За допомогою придбаного ліцензійного ключа

У полі **Ліцензійний ключ** уведіть або скопіюйте/вставте ліцензійний ключ від ESET і клацніть **Продовжити**. Уводьте ліцензійний ключ так, як його вказано, зокрема не пропускайте дефіси. Після копіювання або вставки ліцензії переконайтеся, що ви випадково не залишили додатковий простір навколо тексту.

ESET Business Account

Використовуйте цю опцію, якщо ви зареєстровані та маєте обліковий запис ESET Business Account, у який імпортовано ліцензію ESET Mail Security.

Файл автономної ліцензії

Це автоматично згенерований файл, який передається в продукт ESET. Файл автономної ліцензії створюється на порталі ліцензування та використовується в середовищах, у яких програма не може підключитися до центру ліцензування.

Натисніть **Активувати пізніше** за допомогою ESET PROTECT, якщо комп'ютер входить до керованої мережі, і адміністратор віддалено виконає активацію через ESET PROTECT. Цю опцію також можна використовувати, якщо клієнт потрібно активувати пізніше.

Щоб керувати інформацією про ліцензію, у головному вікні програми виберіть **Довідка та підтримка** > **Змінити ліцензією**. Відобразиться відкритий ідентифікатор ліцензії, який використовується для ідентифікації продукту й ліцензії. Ім'я користувача, під яким зареєстровано комп'ютер, можна знайти в розділі Про програму. Для цього натисніть

піктограму в області сповіщень Windows правою кнопкою миші.

Після успішної активації ESET Mail Security відкриється головне вікно програми, де на сторінці Моніторинг відображатиметься поточний статус. Можливо, на початку потрібно буде приділити продукту трохи часу (наприклад, вам буде запропоновано приєднатися до ESET LiveGrid®).

У головному вікні програми також відображатимуться сповіщення про інші елементи, наприклад системні оновлення (оновлення Windows) або оновлення ядра виявлення. Після обробки всіх сповіщень стан моніторингу буде відображатися зеленим кольором зі статусом **Ваш пристрій захищено**.

Продукт також можна активувати в головному меню, натиснувши **Довідка та підтримка** > **Активувати продукт** або **Стан моніторингу** > **Продукт не активовано**.

ESET PROTECT може автоматично активувати клієнтські комп'ютери з використанням ліцензій, які надав адміністратор.

Активація успішна

ESET Mail Security тепер активовано. Відтепер ESET Mail Security регулярно отримуватиме оновлення про виявлення найновіших загроз і забезпечуватиме захист комп'ютера.

Щоб завершити активацію продукту, натисніть **Готово**.

Помилка активації

Якщо активацію ESET Mail Security не виконано успішно, можливі такі сценарії:

- Ліцензійний ключ уже використовується
- Недійсний ліцензійний ключ: помилка форми активації продукту
- Потрібно вирішити проблему з відсутніми або недійсними даними
- Не вдалося підключитися до бази даних активації: повторіть спробу через 15 хвилин
- Підключення до серверів активації ESET недоступне або вимкнуто

Переконайтеся, що вказано правильний **ліцензійний ключ** або додано правильну **автономну ліцензію**. Після цього повторіть спробу.

Якщо не вдається виконати активацію, скористайтеся майстром виправлення неполадок активації.

Ліцензія

Буде запропоновано вибрати ліцензію для ESET Mail Security, пов'язану з вашим обліковим записом. Щоб продовжити активацію, натисніть **Продовжити**.

Оновлення до останньої версії

Нові версії ESET Mail Security випускаються, щоб внести поліпшення або виправити проблеми, які неможливо усунути за допомогою автоматичних оновлень модулів програми.

Нижче наведено способи оновлення.

• **Видалення та інсталяція**: видалення попередньої версії перед інсталяцією нової. Завантажте останню версію ESET Mail Security. Експортуйте параметри з наявної версії ESET Mail Security, щоб зберегти конфігурацію. Видаліть ESET Mail Security і перезавантажте сервер. Виконайте нову інсталяцію за допомогою завантаженого інсталятора. Імпортуйте параметри, щоб завантажити конфігурацію. Радимо використовувати цю процедуру, якщо ESET Mail Security працює на одному сервері.

• **Доступно**: спосіб оновлення, що не потребує видалення наявної версії. Інсталяція нової версії ESET Mail Security виконується поверх старої.

Обов'язкова умова: на вашому сервері **не має бути відкладених оновлень Windows**, а також **перезавантаження в очікуванні** через оновлення Windows чи з іншої причини. В іншому разі наявну версію ESET Mail Security може бути видалено неналежним чином. Крім цього, якщо ви вирішите видалити стару версію ESET Mail Security вручну, можуть виникнути інші проблеми.

У процесі оновлення ESET Mail Security потрібно буде перезавантажити сервер.

• Віддалене: у процесі оновлення ESET PROTECT потрібно буде перезавантажити сервер. Це, по суті, спосіб прямого оновлення, яке виконується віддалено. Його зручно використовувати, якщо ESET Mail Security працює на кількох серверах.

• Майстер кластерів ESET: можна також використовувати як спосіб оновлення. Рекомендується використовувати цей метод для 2 або кількох серверів із ESET Mail Security. Це, по суті, спосіб оновлення на місці, який виконується через кластер ESET. Після оновлення ви можете продовжити користуватися всіма можливостями кластера ESET.

Оновлення з версії 4.x не зберігає певні параметри, а конкретні правила не можна перенести. Це пов'язано зі змінами в функціях правил, які були впроваджені в новіших версіях продукту. Перед оновленням із версії 4.x рекомендуємо запам'ятати параметри правил. Можна налаштувати правила після завершення оновлення. Нові правила дають вам більше гнучкості й можливостей порівняно з правилами в попередній версії ESET Mail Security.

Наведені нижче параметри залишатимуться такими, як і в попередніх версіях ESET Mail Security:

• Загальна конфігурація ESET Mail Security.

Параметри захисту від спаму:

• усі параметри з попередніх версій; для всіх нових параметрів будуть використовуватися значення за замовчуванням.

• Записи в білому й чорний списку.

Після оновлення ESET Mail Security радимо переглянути всі параметри, щоб переконатися, що програму налаштовано належним чином і відповідно до потреб.

Оновлення за допомогою ESET PROTECT

ESET PROTECT дає змогу оновити кілька серверів, на яких запущено старішу версію ESET Mail Security. Перевагою цього способу є можливість одночасного оновлення великої кількості серверів, під час якого всі екземпляри програми ESET Mail Security мають однакову конфігурацію (за потреби).

Процедура включає наведені нижче етапи.

• **Оновіть перший сервер** вручну, інсталювавши останню версію ESET Mail Security на наявну, щоб зберегти конфігурацію, зокрема правила та білі й чорні списки. Цей етап виконується локально на сервері, на якому працює ESET Mail Security.

• **Надішліть запит на конфігурацію** програми ESET Mail Security, оновленої до версії 7.x, і перетворіть її на політику в ESET PROTECT. Політика буде застосована пізніше до всіх оновлених серверів. Цей і наступні етапи виконуються віддалено за допомогою ESET PROTECT.

• **Запустіть завдання видалення програмного забезпечення** на всіх серверах, на яких використовується стара версія ESET Mail Security.

• **Запустіть завдання з інсталяції програмного забезпечення** на всіх серверах, де потрібно інсталювати останню версію ESET Mail Security.

• **Призначте політику конфігурації** всім серверам, на яких установлено найновішу версію ESET Mail Security.

Щоб оновити систему за допомогою ESET PROTECT, дотримуйтеся наведених нижче інструкцій.

1. Увійдіть на один із серверів, на якому працює програма ESET Mail Security, і оновіть її, завантаживши й інсталювавши найновішу версію поверх наявної. Дотримуйтесь інструкцій зі звичайної інсталяції. Під час інсталяції зберігаються оригінальні конфігурації ESET Mail Security.

2. Відкрийте **веб-консоль** ESET PROTECT, виберіть клієнтський комп'ютер у статичній або динамічній групі та натисніть **Показати інформацію**.

3. Виберіть вкладку Конфігурація та натисніть кнопку **Надіслати запит на отримання конфігурації**, щоб отримати конфігурації керованого продукту. Зверніть увагу, що на цей процес потрібен певний час. Коли в списку з'явиться остання конфігурація, натисніть **Продукт із безпеки** та виберіть **Відкрити конфігурацію**.

4. Створіть політику конфігурації. Для цього клацніть кнопку **Перетворити на політику**. Уведіть **ім'я** нової політики й клацніть **Завершити**.

5. Вибрати**Завдання клієнта** та виберіть завдання Видалення програмного забезпечення.

Під час створення завдання видалення радимо налаштувати перезавантаження сервера після видалення. Для цього поставте прапорець **Автоматично перезавантажити за необхідності**. Після створення завдання додайте всі цільові комп'ютери, які потрібно видалити.

6. Переконайтеся, що програму ESET Mail Security видалено з усіх цільових комп'ютерів.

7. Створіть завдання Інсталяція програмного забезпечення, щоб інсталювати найновішу версію програми ESET Mail Security на всіх потрібних комп'ютерах.

8. **Призначте політику конфігурації** всім серверам, на яких установлено ESET Mail Security (найкраще зробити це для групи серверів).

Оновлення за допомогою кластера ESET

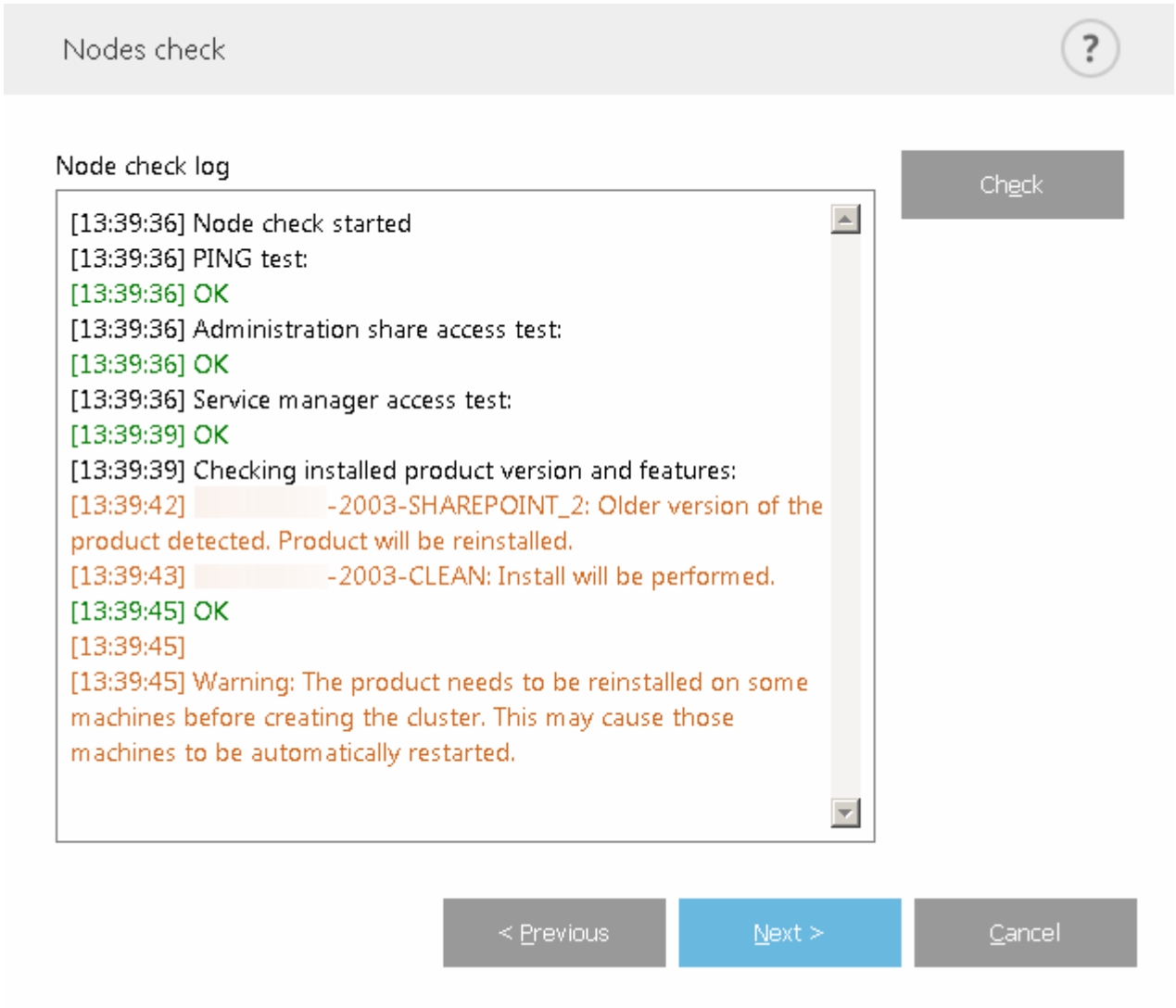
Створення кластера ESET дає змогу оновити кілька серверів, на яких використовуються старіші версії ESET Mail Security. Якщо у вашому середовищі є щонайменше два сервери з ESET Mail Security, радимо використовувати спосіб із застосуванням кластера ESET. Ще однією перевагою цього способу оновлення є можливість подальшого використання кластера ESET для синхронізації конфігурації програми ESET Mail Security на всіх вузлах-учасниках.

Дотримуйтеся наведених нижче вказівок з оновлення за допомогою цього способу.

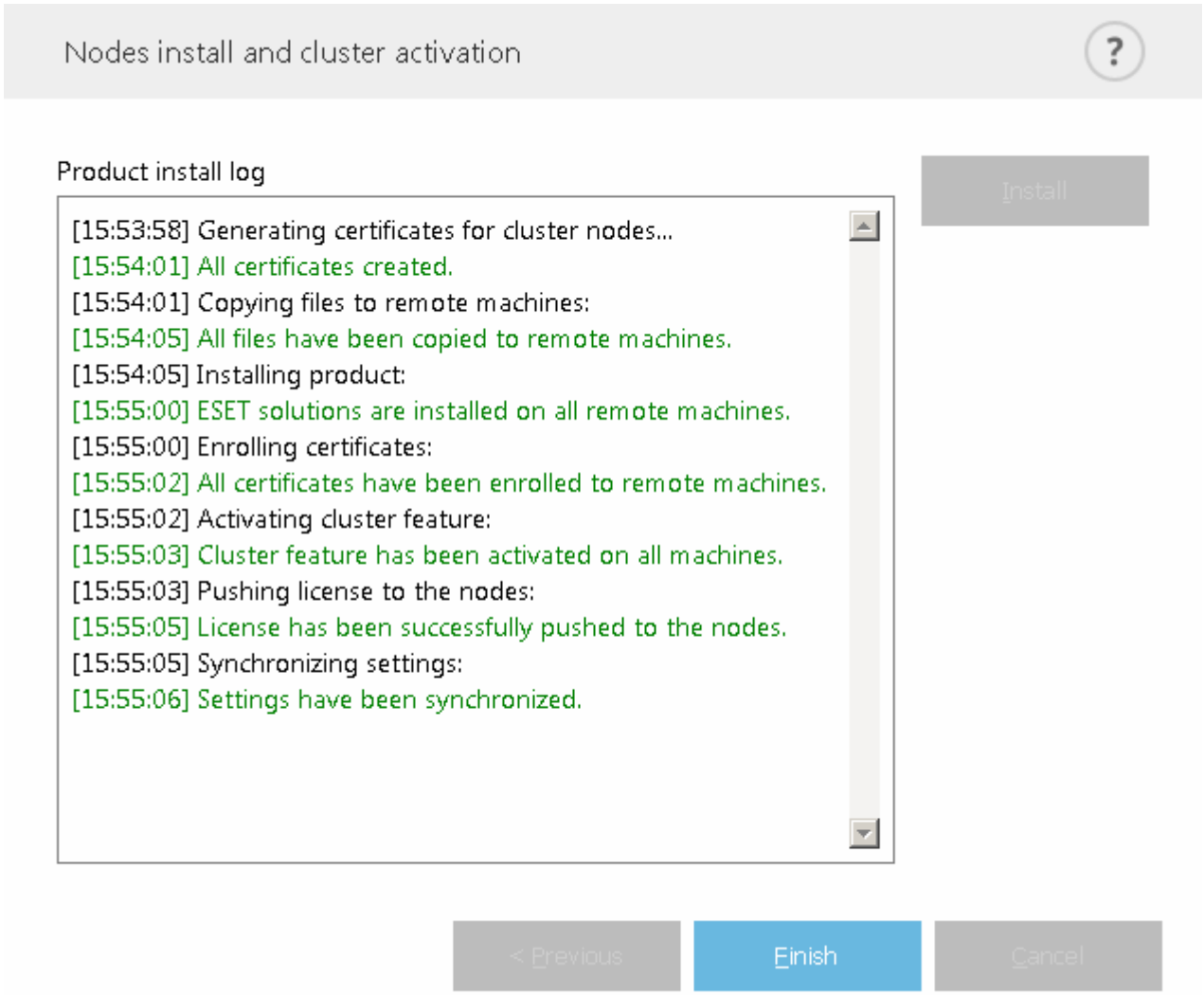
1. Увійдіть на один із серверів, на якому працює програма ESET Mail Security, і оновіть її, завантаживши й інсталювавши найновішу версію поверх наявної. Дотримуйтеся вказівок зі звичайної інсталяції. Усю вихідну конфігурацію старої версії ESET Mail Security буде збережено під час інсталяції.

2. Запустіть майстер кластерів ESET і додайте вузли кластера (сервери, на яких потрібно оновити ESET Mail Security). За потреби можна додати інші сервери, на яких ще не інстальовано ESET Mail Security (на них буде виконано інсталяцію). Радимо не змінювати стандартні параметри, коли вказуватимете ім'я кластера та тип інсталяції (переконайтеся, що поставили прапорець Передати ліцензію на вузли без активованого продукту).

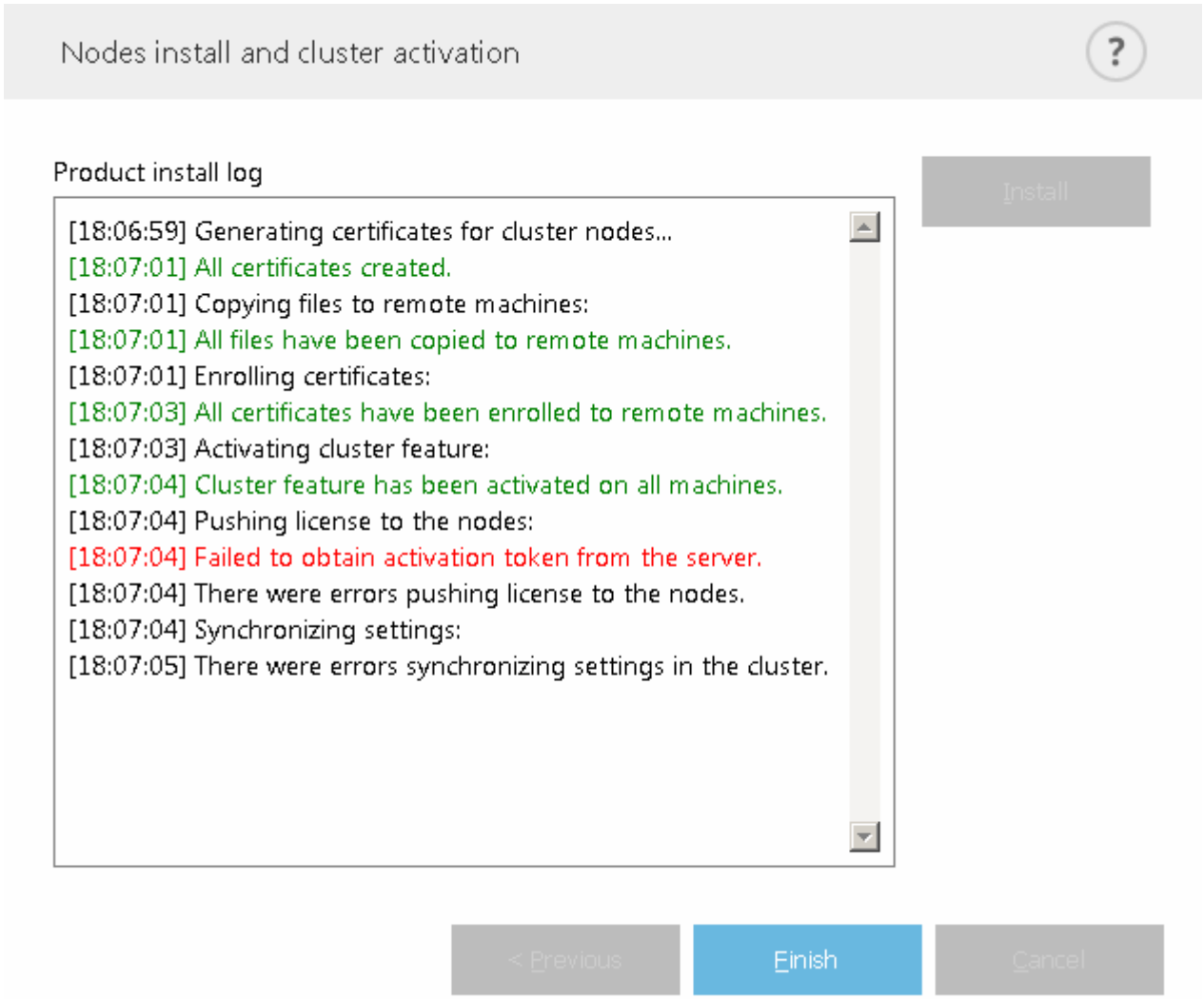
3. Перегляньте екран "Журнал перевірки вузлів". У ньому буде перелічено сервери з більш ранніми версіями продукту, а також сповіщення про повторну інсталяцію продукту. ESET Mail Security також буде інстальовано на всіх доданих серверах, де його ще не інстальовано.



4. На екрані **Інсталяції вузлів і активація кластера** показується перебіг інсталяції. У разі успішної інсталяції має відобразитися такий результат:



Якщо мережу або DNS налаштовано неправильно, може з’явитися повідомлення про помилку **Не вдалось отримати маркер активації із сервера**. Спробуйте запустити майстер кластерів ESET ще раз. Він знищить кластер, а замість нього створить новий (без повторної інсталяції продукту), після чого активація має завершитись успішно. Якщо проблема не зникне, перевірте параметри мережі та DNS.



Інсталяція в кластерному середовищі

ESET Mail Security можна розгорнути в кластерному середовищі (наприклад, у відмовостійкому кластері). Радимо інсталювати ESET Mail Security на активному вузлі, а потім розповсюдити інсталяцію по пасивних вузлах за допомогою функції Кластер ESET програми ESET Mail Security. Окрім інсталяції, кластер ESET слугуватиме реплікацією конфігурації ESET Mail Security, забезпечуючи узгодженість між вузлами кластера, необхідними для правильної роботи.

Сервер терміналів

Якщо ви інсталюєте ESET Mail Security у Windows Server, який працює як сервер терміналів, рекомендуємо вимкнути графічний інтерфейс користувача ESET Mail Security, щоб запобігти його запуску під час кожного входу користувача в систему. Інструкції з вимкнення графічного інтерфейсу користувача див. в статті Disable GUI on Terminal Server (Відключення графічного інтерфейсу користувача в сервері терміналів).

Багатосерверні середовища / середовище DAG

ESET Mail Security підтримує багатосерверні середовища. Якщо інфраструктура складається з кількох серверів, наприклад групи доступності бази даних (DAG), ESET Mail Security можна інсталювати на кожному сервері Exchange Server із роллю поштової скриньки.

Найпростіший спосіб – інсталювати ESET Mail Security на всі сервери за допомогою кластера ESET. Окрім того, рекомендуємо ввімкнути використання кластера ESET для зберігання всіх повідомлень у карантині на одному вузлі в параметрах поштового карантину. Якщо ви плануєте використовувати технологію сірих списків, увімкніть параметр Синхронізувати бази даних сірих списків у кластері ESET.

Початок роботи

Наведені нижче теми допоможуть розпочати роботу з ESET Mail Security.

Моніторинг

Це стислий огляд поточного статусу ESET Mail Security, де можна швидко дізнатися, чи наявні проблеми, що потребують вашої уваги.

Керування за допомогою ESET PROTECT

ESET PROTECT дає змогу віддалено керувати ESET Mail Security. Відомості в наведеному нижче розділі допоможуть розпочати роботу з ESET Mail Security.

Завдання після інсталяції

Довідка з початкової конфігурації.

Завдання після інсталяції

Нижче наведено рекомендовані завдання для початкового налаштування вашого екземпляра ESET Mail Security.

Тема	Опис
Активація продукту	Переконайтеся, що ESET Mail Security активовано. Активацію можна виконати кількома різними способами.
Оновлення	Після активації продукту оновлення модуля запускатиметься автоматично. Перевірте статус оновлення, щоб дізнатися, чи воно виконано успішно.

Тема	Опис
Диспетчер поштового карантину	Ознайомтеся з диспетчером поштового карантину, який доступний у головному вікні програми. Ця функція дає змогу керувати повідомленнями в карантині, такими як спам, інфіковані вкладення, що містять шкідливе програмне забезпечення, фішингові повідомлення та повідомлення, відфільтровані за правилами. Ви можете переглянути докладні відомості про кожне повідомлення й виконати дію (розблокувати або видалити).
Веб-інтерфейс поштового карантину	Веб-інтерфейс поштового карантину — це альтернатива диспетчеру поштового карантину, яка дає змогу віддалено керувати елементами в карантині. Окрім того, веб-інтерфейс поштового карантину дає змогу користувачам (одержувачам електронних листів) керувати повідомленнями в карантині. Користувачі можуть отримувати сповіщення про новий вміст, перенесений у карантин, у звітах про поштовий карантин, які надсилаються електронною поштою. Рекомендуємо налаштувати звіти.
Надіслати звіти про поштовий карантин	Створіть заплановане завдання, щоб надіслати звіти про поштовий карантин пошти собі та вибраним користувачам. Це дасть змогу розблоковувати (доставляти) певні типи повідомлень, поміщених у карантин через помилкове спрацювання, а також керувати їхнім вмістом у карантині через веб-інтерфейс поштового карантину (онлайн-засіб перегляду). Користувачі можуть отримати доступ до веб-інтерфейсу за посиланням, яке наведено в звітах поштового карантину. Для цього потрібно буде ввійти в систему, указавши облікові дані домену.
Антиспам: фільтрація й перевірка	Антиспам — це складна хмарна функція, яка запобігає надходженню користувачам (одержувачам електронних листів) спаму. Рекомендуємо використовувати фільтрацію і перевірку, а також додати локальні IP-адреси в список "Ігноровані IP-адреси". IP-адреси у вашій мережевій інфраструктурі будуть ігноруватись під час класифікації. Для налаштування фільтрації та перевірки можна налаштувати решту списків "Дозволені", "Заблоковані" та "Ігноровані" та керувати ними. Якщо ви вирішите використовувати цю функцію, можна ввімкнути технологію сірих списків.
Правила	Потужна функція, яка дає змогу відфільтрувати електронні листи на основі визначених умов і дій. Використовуйте попередньо налаштовані правила (змініть їх за потреби) або створіть нові налаштовувані правила відповідно до ваших потреб. Правила можна налаштувати для будь-яких рівнів захисту (захист передачі пошти, захист бази даних поштових скриньок або сканування бази даних поштових скриньок за вимогою).
Перевірка антивірусу	Переконайтеся, що антивірус працює належним чином.
Перевірка функції "Антиспам"	Переконайтеся, що антиспам працює належним чином.
Перевірка функції "Захист від фішинг-атак"	Переконайтеся, що захист від фішинг-акцій працює належним чином.

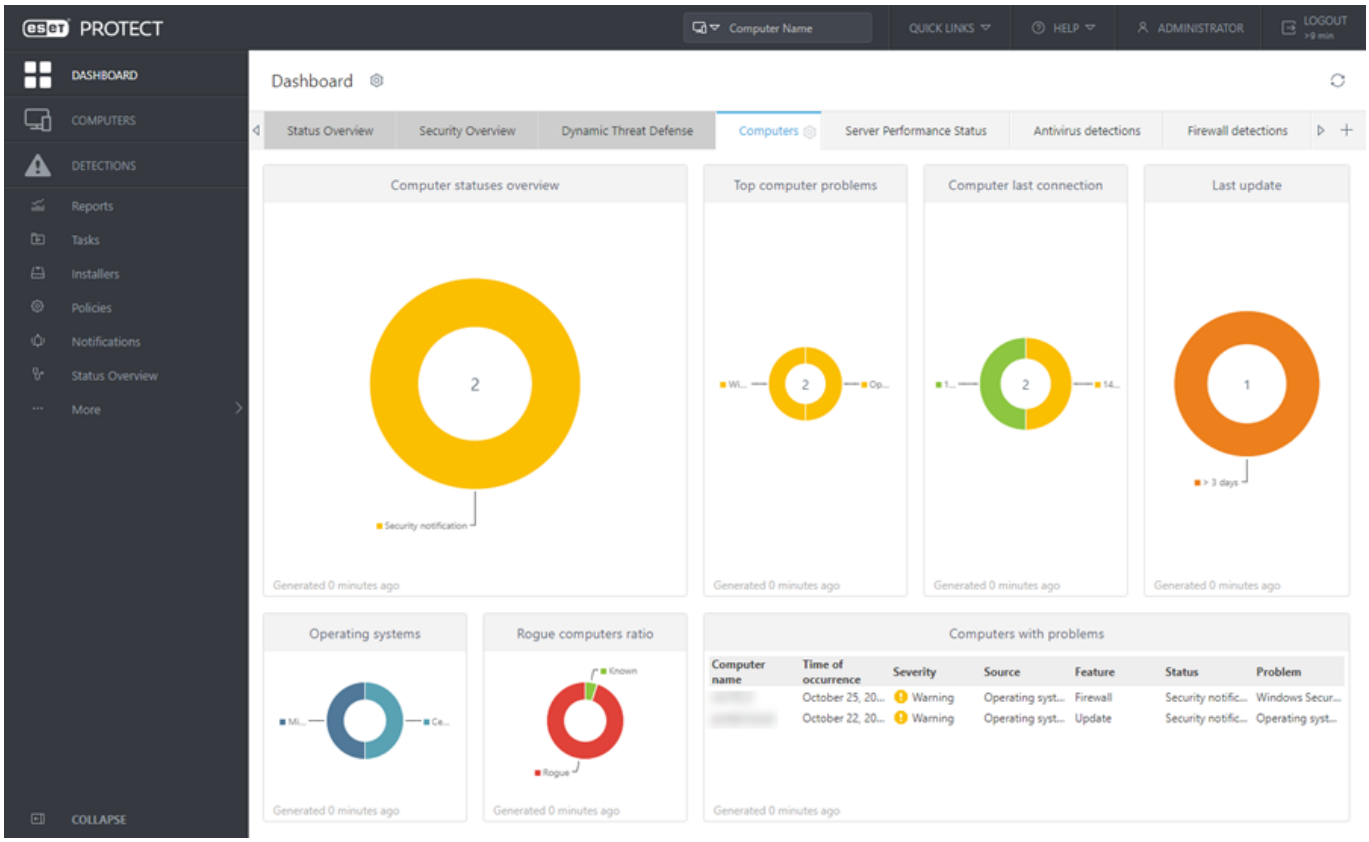
Керування за допомогою ESET PROTECT

ESET PROTECT – це програма, яка дозволяє вам з єдиного центру керувати продуктами ESET у мережевому середовищі. Система керування завданнями ESET PROTECT дозволяє інсталювати рішення для захисту ESET на віддалених комп’ютерах і швидко реагувати на нові проблеми й

загрози.

ESET PROTECT сама по собі не забезпечує захисту від шкідливого коду. Натомість її функційність залежить від наявності рішень для захисту ESET на кожному клієнті.

Рішення для захисту ESET підтримують мережі з кількома типами платформ. Ваша мережа може містити в собі комбінацію операційних систем Microsoft, операційних систем на основі Linux, macOS, а також операційних систем для мобільних пристроїв.



Щоб дізнатися більше, перегляньте ESET PROTECTонлайн-довідку.

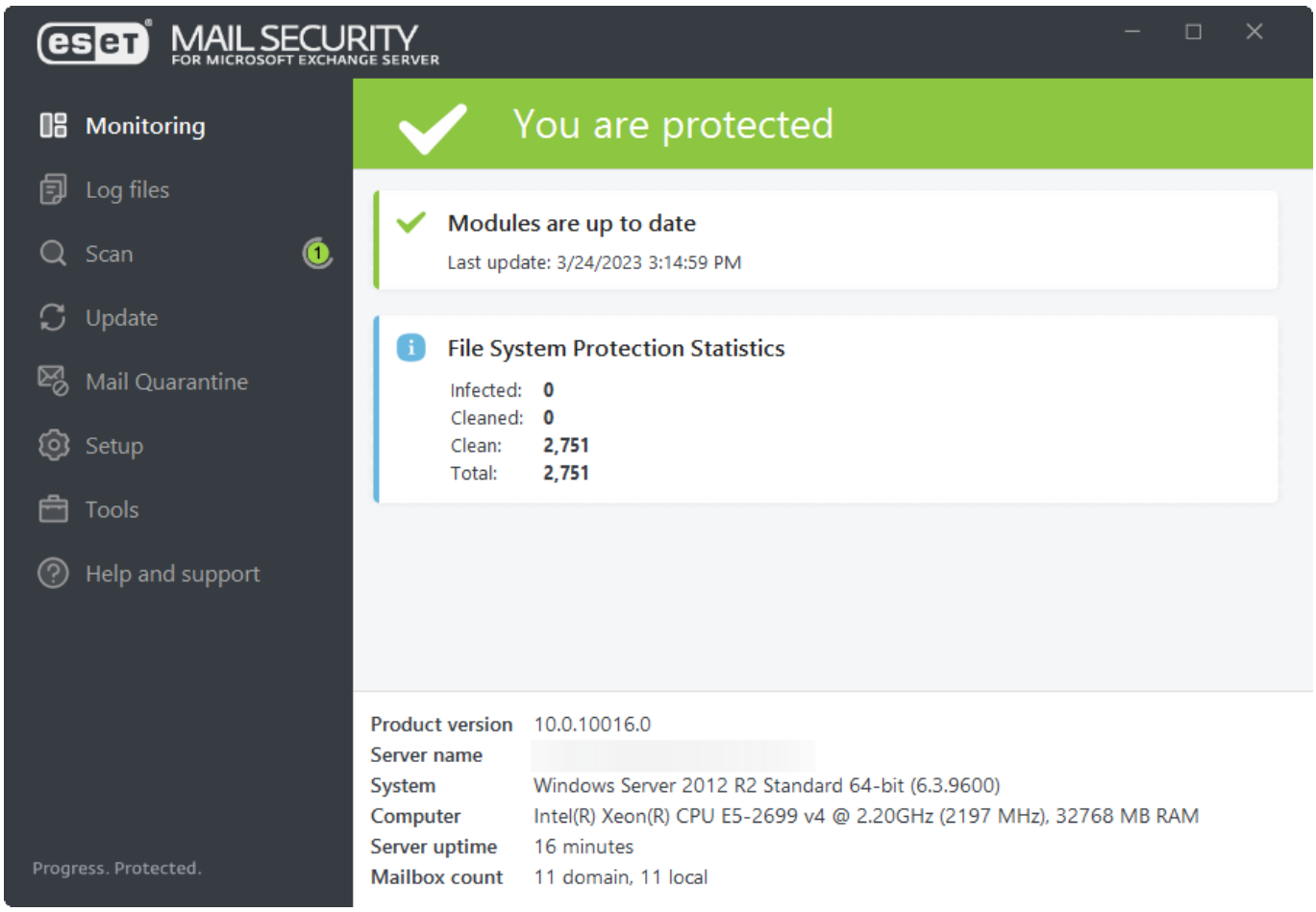
Моніторинг

Статус захисту, що відображається в розділі **Моніторинг**, інформує про поточний рівень захисту комп’ютера. В основному вікні показується зведена інформація про роботу ESET Mail Security.

Зелений статус **Ваш комп’ютер захищено** вказує на максимальний рівень захисту.

Червона піктограма вказує на критичні проблеми, через які максимальний захист системи не гарантується. Детальний опис у повідомленні про помилку має допомогти краще розуміти природу проблеми. Якщо не вдається вирішити проблему, виконайте пошук у базі знань ESET. Якщо вам досі потрібна допомога, надішліть запит до служби технічної підтримки. Спеціалісти служби технічної підтримки ESET швидко дадуть відповідь на запитання й допоможуть знайти вирішення проблеми. Щоб отримати повний список статусів, виберіть **Додаткові параметри** (**F5**) > **Сповіщення** > Статуси програми, а потім — **Змінити**.

Оранжева піктограма вказує на те, що продукт ESET потребує уваги щодо некритичної проблеми.



Модулі, які працюють належним чином, позначаються зеленим прапорцем. Модулі, які працюють неправильно, позначаються червоним знаком оклику або оранжевою піктограмою сповіщення. У верхній частині вікна відображається додаткова інформація про модуль. Також пропонується вирішення проблеми.

Щоб змінити статус окремого модуля, натисніть Параметри в головному меню й виберіть потрібний модуль.

На сторінці "Моніторинг" також міститься інформація про вашу систему, зокрема зазначена нижче.

- Версія продукту: номер версії ESET Mail Security.
- Ім’я сервера: ім’я хоста комп’ютера або FQDN.
- Система: інформація про операційну систему.
- Комп’ютер: інформація про обладнання.
- Час роботи сервера: інформація про те, скільки система працює без зупинки на цей момент (протилежно до простою).

Кількість поштових скриньок

ESET Mail Security виявляє кількість поштових скриньок і відображає кількість на основі виявлення:

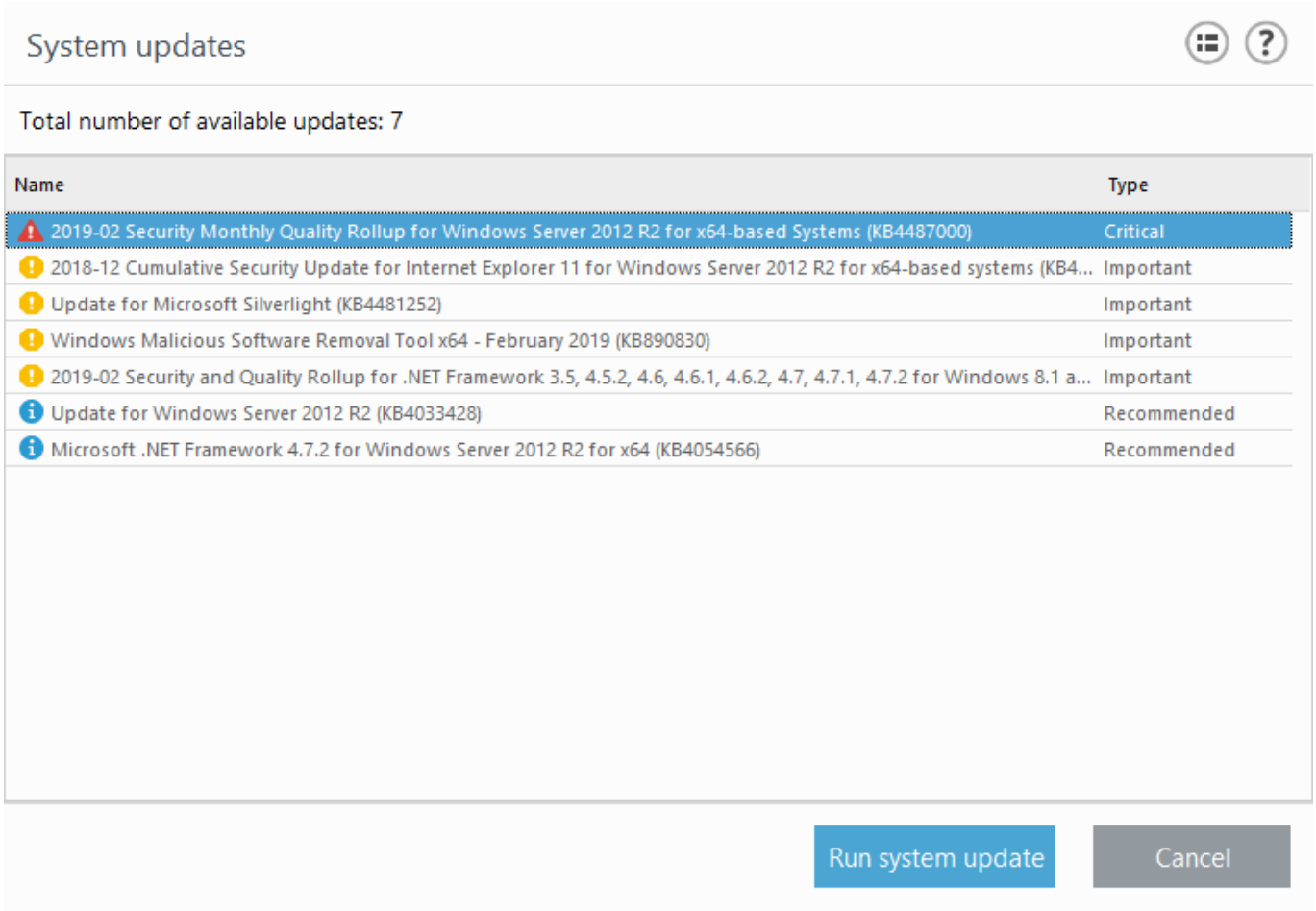
• **Домен**: кількість всіх поштових скриньок у певному домені, до якого належить Exchange Server. Цей підрахунок також застосовується до середовища DAG і загальної кількості його поштових скриньок.

• **Локальний**: відображає кількість поштових скриньок на сервері Exchange Server з інстальованим ESET Mail Security. Якщо сервер входить у DAG, це число відповідає кількості поштових скриньок (із загальної кількості доменів), які зберігаються на локальному сервері Exchange Server.

Якщо не вдається вирішити проблему за допомогою рекомендованих рішень, натисніть **Довідка та підтримка**, щоб отримати доступ до файлів довідки або виконати пошук у базі знань ESET. Якщо вам досі потрібна допомога, надішліть запит до служби технічної підтримки. Спеціалісти служби технічної підтримки ESET швидко дадуть відповідь на запитання й допоможуть знайти вирішення проблеми.

Доступне оновлення ОС Windows

У вікні "Оновлення системи" показано список доступних оновлень, готових для завантаження та інсталяції. Рівень пріоритету оновлення відображається поруч із назвою оновлення. Клацніть правою кнопкою миші будь-який рядок оновлення і виберіть пункт **Додаткова інформація**, щоб відкрити спливаюче вікно з додатковою інформацією:



Натисніть **Запустити оновлення системи**, щоб відкрити вікно **Windows Update** і перейти до системних оновлень.

Ізоляція мережі

ESET Mail Security дає змогу здійснювати ізоляцію мережі, коли ви блокуєте мережеве підключення до сервера. У деяких випадках ізоляція сервера від мережі потрібна як запобіжний захід. Це актуально, наприклад, якщо виявиться, що сервер інфіковано шкідливим програмним забезпеченням або його безпеку порушено іншим чином.

Після активації ізоляції мережі весь мережевий трафік блокується, за винятком:

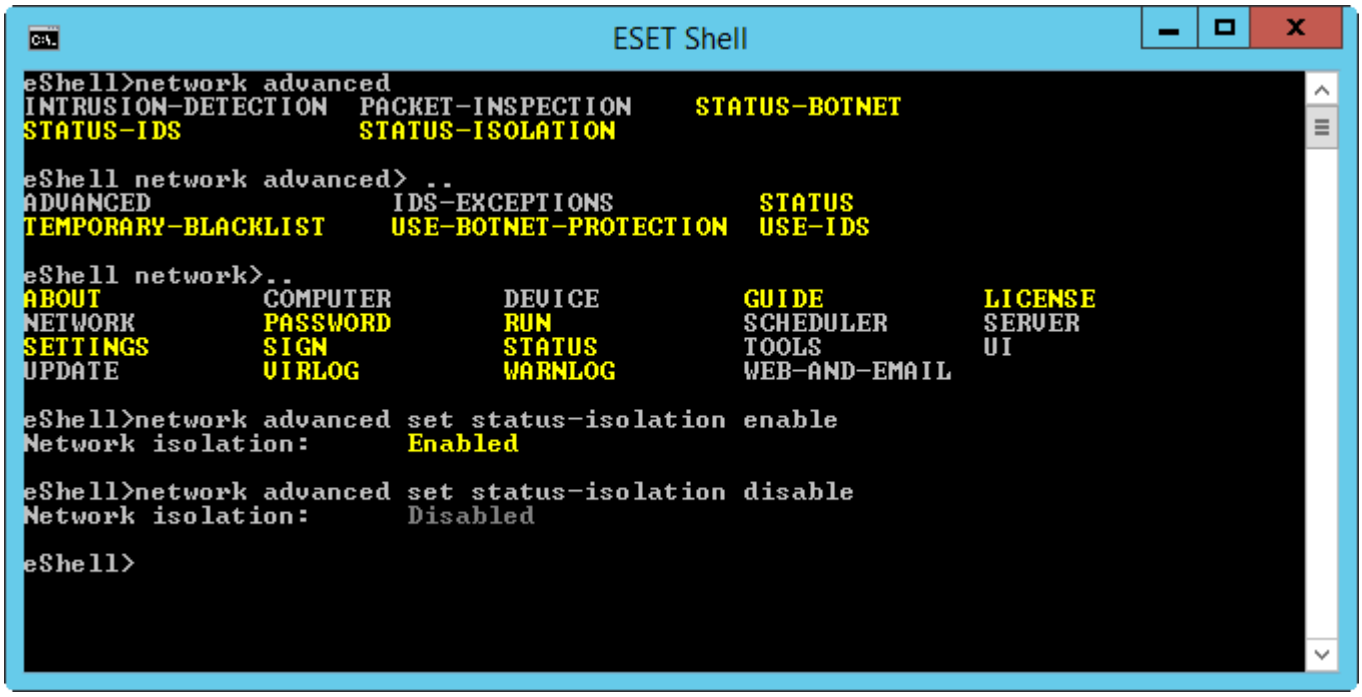
- Підключення до контролера домену
- Передачі даних із ESET Mail Security
- Передачі даних між ESET Management Agent і ESET Inspect Connector через мережу (якщо доступно)

Активувати й деактивувати ізоляцію мережі можна за допомогою команди eShell або завдання клієнта ESET PROTECT.

eShell

В інтерактивному режимі:

- Активувати ізоляцію мережі: `network advanced set status-isolation enable`
- Деактивувати ізоляцію мережі: `network advanced set status-isolation disable`



Крім цього, можна створити й запустити пакетний файл у режимі пакета або сценарію.

ESET PROTECT

- Активація ізоляції мережі за допомогою завдання клієнта.
- Деактивація ізоляції мережі за допомогою завдання клієнта.

Якщо активовано ізоляцію мережі, статус ESET Mail Security змінюється на червоний і відображається повідомлення **Доступ до мережі заблоковано**.

Використання ESET Mail Security

У цій частині міститься докладний опис інтерфейсу програми й пояснюється, як використовувати ESET Mail Security.

Інтерфейс користувача дає змогу швидко отримати доступ до найпоширеніших функцій.

- Моніторинг
- Файли журналу
- Сканування
- Оновлення
- Поштовий карантин
- Налаштування
- Інструменти

Сканування

Сканер на вимогу є важливою складовою ESET Mail Security. Він використовується для сканування файлів і папок на комп'ютері. Щоб забезпечити захист мережі, важливо виконувати сканування комп'ютера регулярно, а не лише коли є підозра на зараження.

Рекомендовано виконувати регулярні (наприклад, раз на місяць) детальні сканування системи, щоб виявляти віруси, які не виявила функція захисту файлової системи в режимі реального часу. Це могло статися, якщо в момент появи загрози було вимкнено захист файлової системи в режимі реального часу, ядро виявлення застаріло або файл не було виявлено під час першого збереження на диску.

Виберіть доступні сканування на вимогу для ESET Mail Security.

Сканування бази даних поштових скриньок

Дозволяє запустити сканування бази даних на вимогу. Для сканування можна вибрати спільні папки, поштові сервери й поштові скриньки. Крім того, ви можете скористатися розкладом, щоб запускати сканування бази даних у певний час або в разі певної події.

У системі Microsoft Exchange Server 2007, 2010, 2013 або 2016 можна вибрати захист бази даних поштових скриньок або сканування бази даних на вимогу. Одночасно можна активувати лише один тип захисту. Якщо ви вирішите використовувати сканування бази даних на вимогу, потрібно буде вимкнути інтеграцію захисту бази даних поштових скриньок у розділі "Додаткові параметри" меню Сервер. В іншому разі сканування бази даних на вимогу буде недоступне.

Сканування поштових скриньок Microsoft 365

Дає змогу сканувати віддалені поштові скриньки в гібридних середовищах Microsoft 365.

Сканування сховища

Сканує всі спільні папки на локальному сервері. Якщо сканування сховища недоступне, на сервері немає спільних папок.

Проскануйте свій комп'ютер

Дає змогу швидко запустити сканування комп'ютера й очистити інфіковані файли без втручання користувача. Перевага функції "Сканувати комп'ютер" полягає в тому, що вона проста у використанні й не потребує детального налаштування сканування. Під час сканування перевіряються всі файли на локальних дисках та автоматично очищаються або видаляються виявлені загрози. Для рівня очистки автоматично вибрано значення за замовчуванням. Щоб дізнатися більше про типи очистки, перегляньте статтю Очищення.

Радимо виконувати сканування комп'ютера принаймні раз на місяць. Сканування можна налаштувати як заплановане завдання.

Вибіркове сканування

Вибіркове сканування – це оптимальне рішення, якщо потрібно вказати параметри сканування (наприклад, об'єкти й методи сканування). Перевагою вибіркового сканування є можливість детально налаштувати параметри сканування. Конфігурації можна зберігати в користувацьких профілях сканування, які зручно використовувати, якщо регулярно виконується сканування з однаковими параметрами.

Сканування змінних носіїв

Аналогічно інтелектуальному скануванню, ця функція швидко запускає сканування змінних носіїв (наприклад, компакт-дисків, DVD-дисків, пристроїв USB), підключених до комп'ютера. Вона може бути корисною, коли ви підключите до комп'ютера пристрій USB та хочете перевірити його вміст на наявність шкідливого програмного забезпечення й інших потенційних загроз. Цей тип сканування також можна запустити, натиснувши пункт "Вибіркове сканування", а потім вибравши в розкривному меню "Об'єкти сканування" опцію "Змінні носії" й натиснувши "Сканувати".

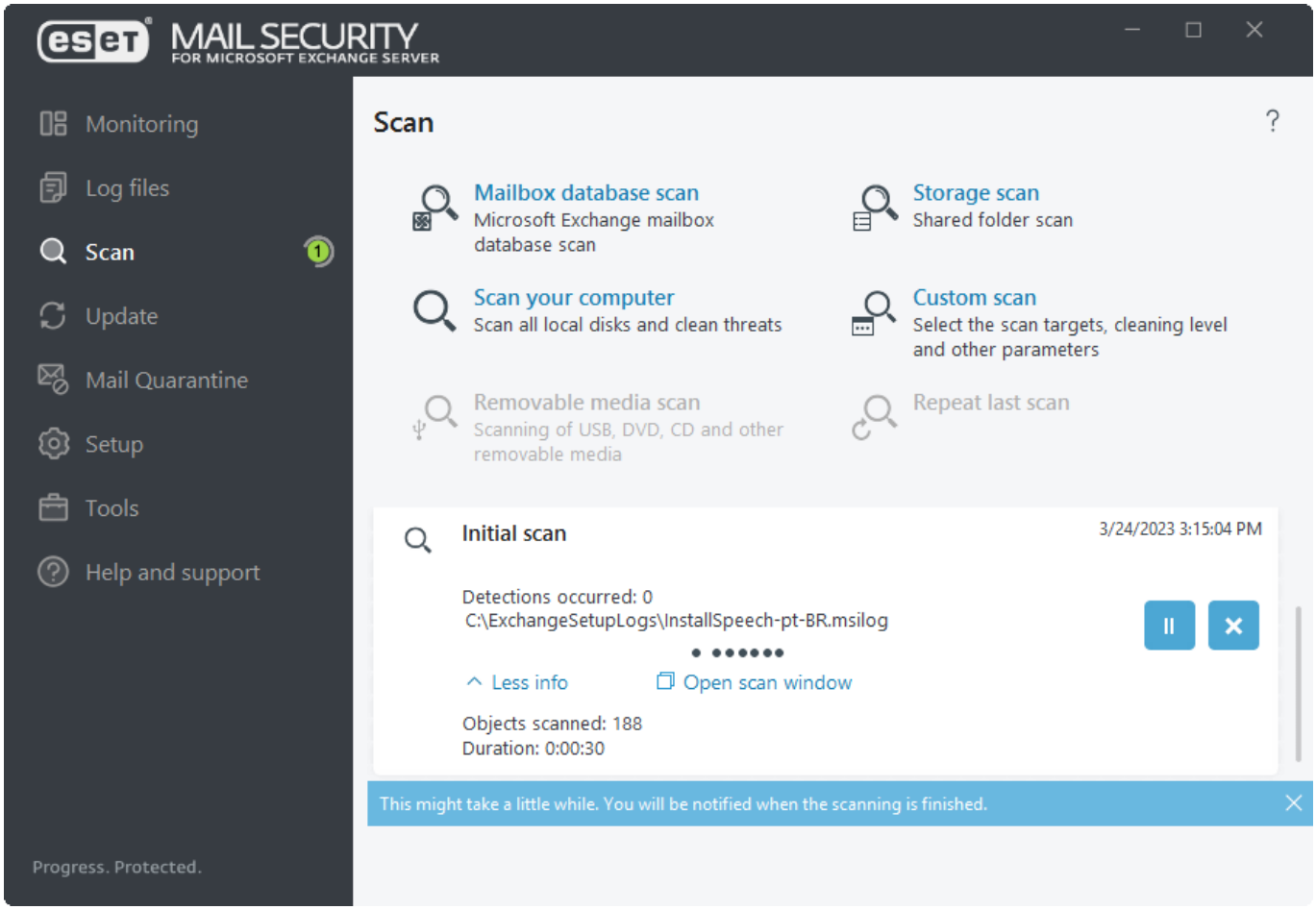
Сканування Hyper-V

Ця опція доступна в меню, лише якщо диспетчер Hyper-V інстальовано на сервері, на якому виконується ESET Mail Security. Сканування Hyper-V дозволяє сканувати диски віртуальної машини на сервері Microsoft Hyper-V без необхідності інсталювати будь-який агент на відповідній віртуальній машині.

Повторити останнє сканування

Повторює останню операцію сканування з такими самими параметрами.

> Якщо використовується сканування бази даних на вимогу, функція "Повторити останнє сканування" недоступна.



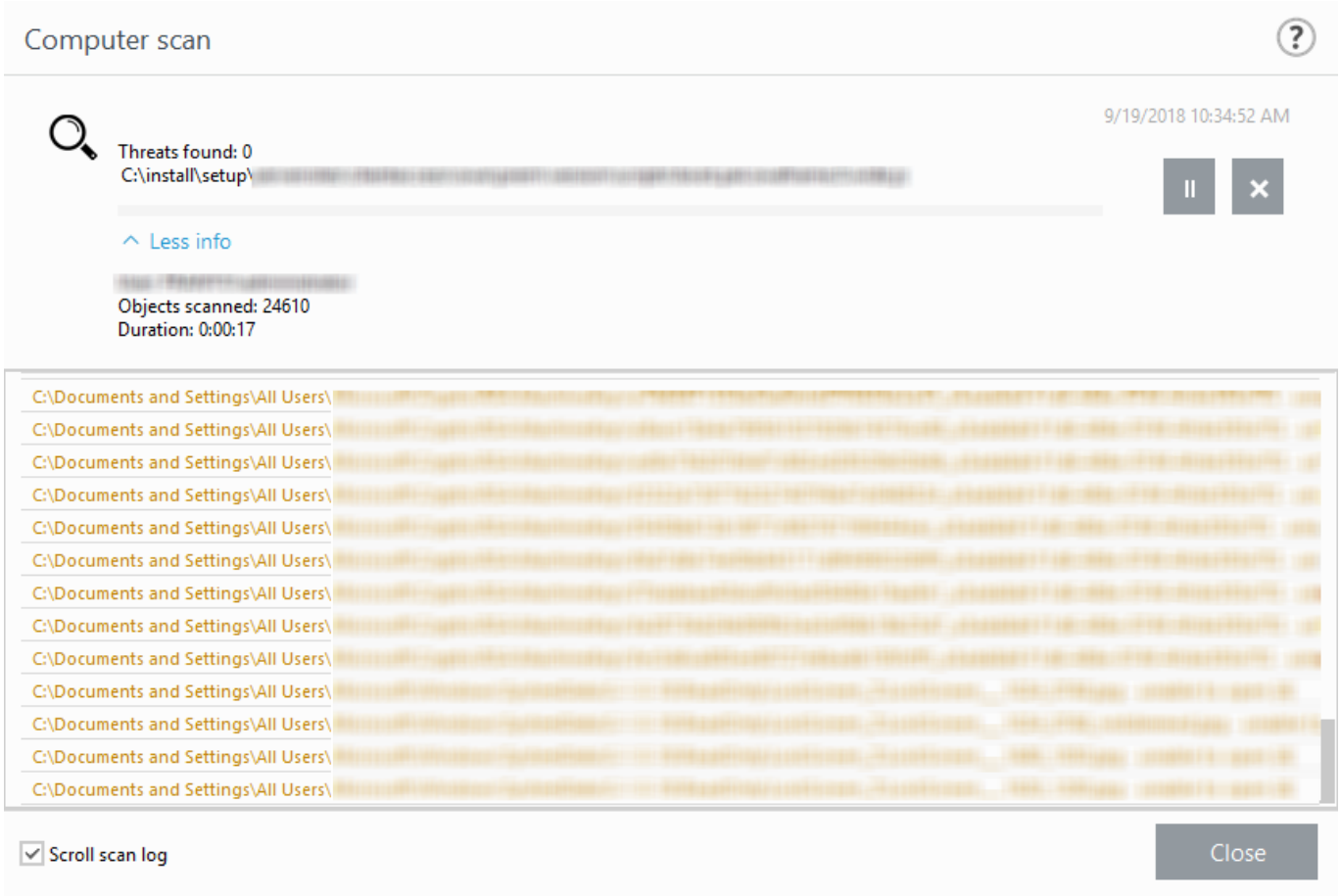
Ви можете використовувати вказані нижче опції й переглянути додаткову інформацію про стан сканування.

Перетягування файлів	**Дає змогу перетягувати файли у вікно сканування ESET Mail Security. Ці файли негайно перевірятимуться на наявність вірусів.**
Закрити/Закрити всі	Закриття цих повідомлень.
Статуси сканування	Показ статусу першого сканування. Це сканування завершено або його перервав користувач.
Показати журнал	Показує докладнішу інформацію.
Докладніше	Під час сканування можна переглянути інформацію про користувача, який виконав сканування, кількість просканованих об’єктів і **тривалість** сканування. Якщо виконується сканування бази даних на вимогу, відображається користувач, який виконав сканування, а не фактичний обліковий запис сканування бази даних, що використовується для підключення до EWS (веб-служби Exchange) під час сканування.
Відкрити вікно сканування	У вікні перебігу сканування відображається поточний статус сканування та інформація про кількість файлів, які містять шкідливий код.

Вікно сканування та журнал сканування

У вікні сканування відображаються просканові об’єкти, зокрема їх розташування, кількість знайдених загроз (якщо є), кількість просканованих об’єктів і тривалість сканування. У нижній частині вікна розташовано журнал сканування, у якому відображаються номер версії ядра виявлення, дата й час початку сканування й вибрані об’єкти.

Під час перебігу сканування натисніть **Призупинити**, щоб тимчасово перервати сканування. Опція **Відновити** доступна, якщо процес сканування призупинено.

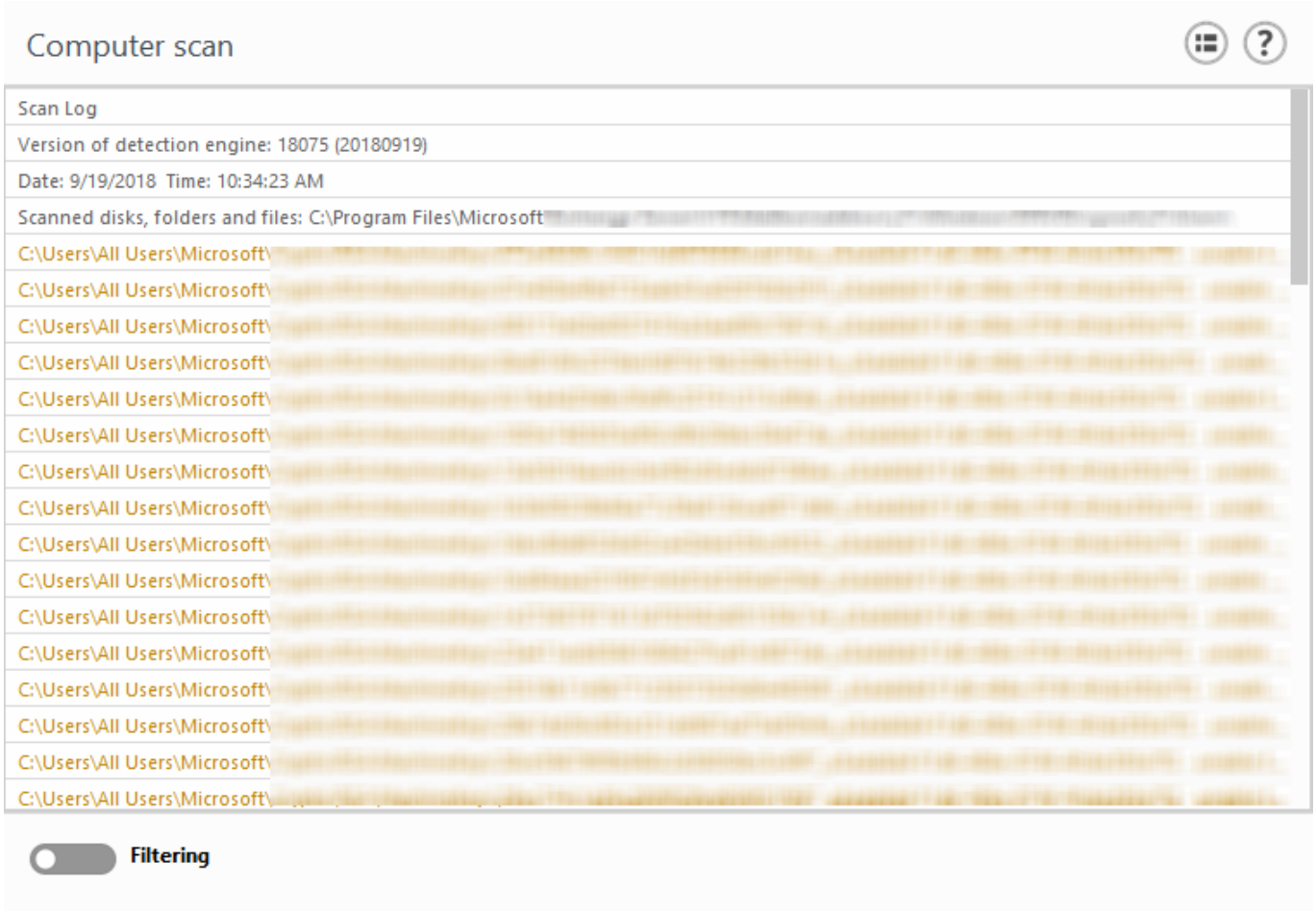


Прокручування журналу сканування

Не вимикайте цю опцію, щоб автоматично прокручувати старі журнали й переглядати активні журнали у вікні "Файли журналу".

> Деякі файли, наприклад захищені паролем або ті, що ексклюзивно використовуються системою (зазвичай *pagefile.sys* і певні файли журналу), не можна сканувати. Це явище не є неполадкою.

Коли сканування завершиться, відобразиться журнал сканування з усією відповідною інформацією, пов’язаною з конкретним скануванням.



Натисніть піктограму перемикача **Фільтрація** , щоб відкрити вікно Фільтрація журналу, де можна визначати критерії фільтрації або пошуку. Щоб переглянути контекстне меню, натисніть певний запис журналу правою кнопкою миші.

Дія	Використання	Ярлик	Переглянути також
Відфільтровувати однакові записи	Активація фільтра журналу, у якому відображаються лише записи вибраного типу.	Ctrl + Shift + F	
Фільтрувати...	Після вибору цієї опції у вікні "Фільтрація журналу" можна визначати критерії фільтрації для певних записів журналу.		Фільтрація журналу
Увімкнути фільтр	Активація параметрів фільтра. Під час першої активації фільтрації потрібно вибрати параметри.		
Вимкнути фільтр	Вимкнення фільтрації (аналогічно до натискання перемикача внизу).		
Копіювати	Копіювання інформації вибраних/виділених записів у буфер обміну.	Ctrl + C	
Копіювати все	Копіювання інформації з усіх записів у вікні.		
Експортувати...	Експорт інформації вибраних/виділених записів у файл XML.		
Експортувати все...	Експорт усієї інформації у вікні у файл XML.		

Файли журналу

Файли журналу містять інформацію про важливі програмні події та зведені дані про результати сканування, виявлені загрози тощо. Журнали – це важливий інструмент аналізу, виявлення загроз і виправлення неполадок у системі. Ведення журналів активно виконується у фоновому режимі без втручання користувача. Інформація реєструється відповідно до поточних параметрів детальності журналу. Ви можете переглядати текстові повідомлення та журнали просто в середовищі ESET Mail Security або експортувати їх для перегляду в іншому розташуванні.

У розкривному меню виберіть відповідний тип журналу. Доступні вказані нижче журнали.

Виявлені об’єкти

Журнал виявлених об’єктів містить докладну інформацію про загрози, виявлені модулями ESET Mail Security. Інформація охоплює час виявлення, ім’я загрози, розташування, виконану дію та ім’я користувача, який увійшов у систему під час виявлення загрози.

Двічі натисніть будь-який запис журналу, щоб відобразити докладну інформацію про нього в окремому вікні. Можна створити виключення виявленого об’єкту (за потреби), натиснувши правою кнопкою миші запис журналу (виявлений об’єкт) і вибравши **Створити виключення**. Відкриється майстер виключень із попередньо визначеними критеріями. Якщо поруч із виключеним файлом указано ім’я виявленого об’єкта, це означає, що файл виключено лише для цього виявленого об’єкта. Якщо цей файл пізніше буде інфіковано іншим шкідливим програмним забезпеченням, його буде виявлено.

Події

Усі важливі дії, що виконуються програмою ESET Mail Security, реєструються в журналі подій. Він містить інформацію про події та помилки, які відбулися в програмі. Він допомагає системним адміністраторам і користувачам вирішувати проблеми. Часто інформація, що міститься в цьому журналі, може допомогти знайти вирішення проблеми, яка виникає в програмі.

Сканування комп'ютера

Усі результати сканування відображаються в цьому вікні. Кожен рядок відповідає одній перевірці комп’ютера. Двічі натисніть будь-який запис, щоб переглянути докладну інформацію про відповідне сканування.

Заблоковані файли

Містить записи заблокованих і недоступних файлів. Протокол показує причину та вихідний модуль, що заблокував файл, а також програму й користувача, який запустив файл.

Надіслані файли

Містить записи файлів хмарного захисту, ESET LiveGuard Advanced і ESET LiveGrid®.

Журнали аудиту

Містить записи про зміни в конфігурації або стані захисту й створює знімки для подальшого використання. Натисніть правою кнопкою миші будь-який запис типу "Зміна параметрів" і виберіть "Показати" в контекстному меню, щоб переглянути докладну інформацію про

виконану зміну. Якщо потрібно використовувати попередні налаштування, виберіть "Відновити". Також можна скористатися параметром "Видалити все", щоб видалити записи журналу. Щоб деактивувати ведення журналу аудиту, перейдіть у меню "Додаткові параметри" > "Інструменти" > "Файли журналу" > Журнал аудиту.

HIPS

Містить записи про певні правила, позначені для реєстрації в журналі. Протокол показує програму, яка викликала операцію, результат (дозволено чи заборонено правило) і назву створеного правила.

Захист мережі

Містить записи про файли, заблоковані захистом від ботнетів і мережевих атак.

Відфільтровані веб-сайти

Список веб-сайтів, заблокованих захистом доступу до Інтернету та захистом електронної пошти від фішинг-атак. У журналах відображається час, URL-адреса, користувач і програма, за допомогою якої встановлено підключення до певного веб-сайту.

Контроль пристроїв

Містить записи про змінні носії або пристрої, підключені до комп'ютера. Пристрої реєструватимуться у файлі журналу лише на основі правила контролю пристроїв. Запис про підключений пристрій, який не відповідає умовам правила, у журналі не створюватиметься. Тут також можна переглянути інформацію, як-от тип пристрою, серійний номер, ім'я постачальника й розмір носія (якщо доступно).

Захист поштового сервера

Тут реєструються всі повідомлення, які ESET Mail Security визначає як загрозу або спам. Ці журнали застосовуються до таких типів захисту: захист від спаму, захист від фішинг-атак, захист від підміни відправника, правила й захист від шкідливого програмного забезпечення.

Якщо двічі натиснути елемент, відкриється вікно з додатковою інформацією про виявлене повідомлення електронної пошти (IP-адреса, домен HELO, ідентифікатор повідомлення й тип сканування), а також рівень захисту, на якому його було виявлено. Окрім того, ви можете переглянути результат сканування на наявність шкідливого програмного забезпечення, фішингу й спаму разом із причинами їхнього виявлення, а також дізнатися, чи було активовано правило.

> **i** Не всі оброблені повідомлення реєструються в журналі захисту поштового сервера. Проте всі повідомлення, які було змінено (видалене вкладення, додавання спеціального рядка в заголовок повідомлення тощо), записуються в журнал.

Сканування бази даних поштових скриньок

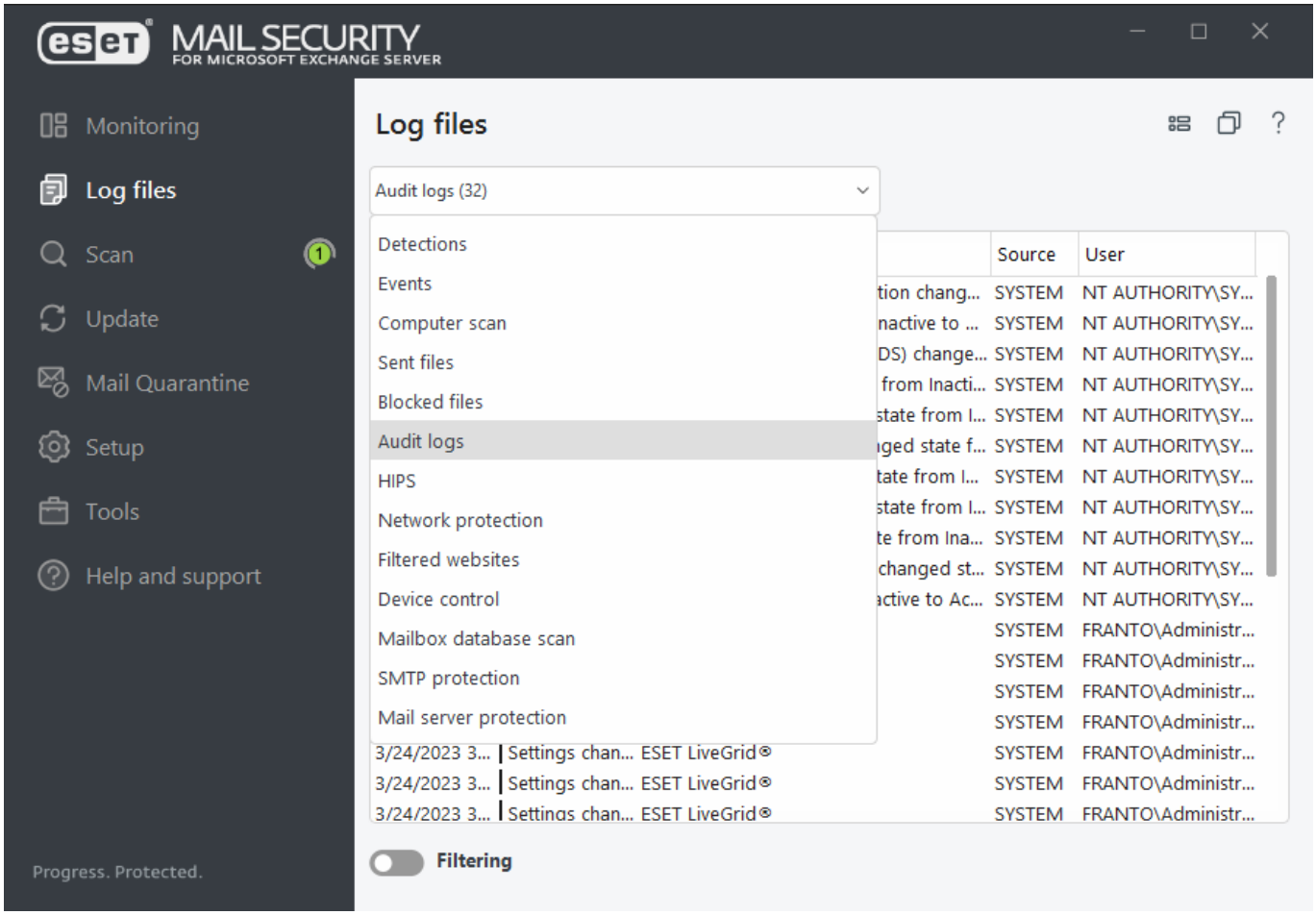
Містить версію ядра виявлення, дату, проскановане розташування, кількість просканованих об'єктів, кількість знайдених загроз, кількість звернень до правил і час виконання.

Захист SMTP

Усі повідомлення, оцінювані за допомогою технології сірих списків. Тут також відображаються правила SPF і Backscatter. Кожен запис містить домен HELO, IP-адреси відправника й одержувача, стан дій (відхилені, відхилені [не підтверджені] та перевірені вхідні повідомлення). Є нова дія для додавання субдомену до білого списку, пов’язаного з технологією сірих списків. Перегляньте таблицю нижче.

Сканування Hyper-V

Містить список результатів сканування Hyper-V. Двічі натисніть будь-який запис, щоб переглянути докладну інформацію про відповідне сканування.



У контекстному меню (натискання правою кнопкою миші) можна вибрати дію з вибраним записом журналу.

Дія	Використання	Ярлик	Переглянути все
Показати	Показує докладнішу інформацію про вибраний журнал у новому вікні (таку саму, що й подвійне натискання).		
Відфільтровувати однакові записи	Активація фільтра журналу, у якому відображаються лише записи вибраного типу.	Ctrl + Shift + F	
Фільтрувати...	Після вибору цієї опції у вікні "Фільтрація журналу" можна визначати критерії фільтрації для певних записів журналу.		Фільтрація журналу

Дія	Використання	Ярлик	Переглянути все
Увімкнути фільтр	Активація параметрів фільтра. Під час першої активації фільтрації потрібно вибрати параметри.		
Вимкнути фільтр	Вимкнення фільтрації (аналогічно до натискання перемикача внизу).		
Копіювати	Копіювання інформації вибраних/виділених записів у буфер обміну.	Ctrl + C	
Копіювати все	Копіювання інформації з усіх записів у вікні.		
Видалити	Видалення вибраних/виділених записів. Щоб виконати цю дію, потрібні права адміністратора.	Del	
Видалити все	Видалення всіх записів у вікні. Щоб виконати цю дію, потрібні права адміністратора.		
Експортувати...	Експорт інформації вибраних/виділених записів у файл XML.		
Експортувати все...	Експорт всієї інформації у вікні у файл XML.		
Знайти...	Цей параметр відкриває вікно "Пошук у журналі" та дає змогу визначати критерії пошуку. За допомогою функції пошуку можна знайти певний запис, навіть якщо ввімкнено фільтрацію.	Ctrl + F	Пошук у журналі
Знайти наступні	Пошук наступного збігу, який відповідає визначеним критеріям пошуку.	F3	
Знайти попередні	Пошук попереднього збігу.	Shift + F3	
Створити виключення	Щоб виключити об’єкти з очищення за допомогою імені виявленого об’єкта, шляху або його хешу.		Створити виключення

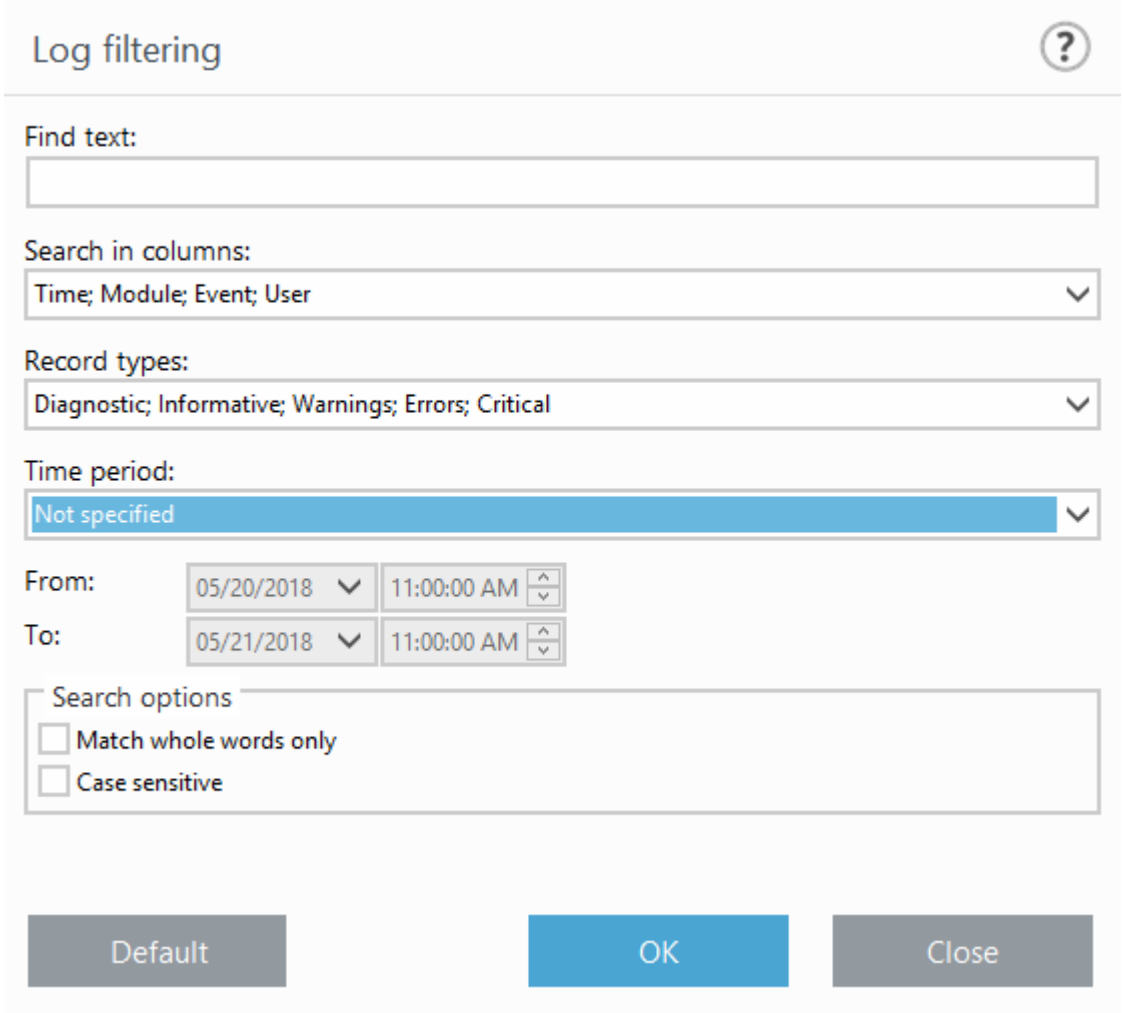
Додати IP-адресу в білий список, пов’язаний із технологією сірих списків	Додавання IP-адреси відправника в білий список IP-адрес. Білий список IP-адрес можна знайти в розділі "Технологія сірих списків і SPF" статті Фільтрація й перевірка. Це стосується елементів, зареєстрованих за допомогою технології сірих списків або SPF.
Додати домен у сірий список і білий список SPF	Додавання домену відправника в білий список доменів та IP-адрес. Додається лише домен, піддомени ігноруються. Наприклад, якщо адреса відправника – sub.domain.com, лише domain.com додається в білий список. Білий список доменів та IP-адрес можна знайти в розділі "Технологія сірих списків і SPF" статті Фільтрація й перевірка. Це стосується елементів, зареєстрованих за допомогою технології сірих списків.
Додати піддомен у сірий список і білий список SPF	Додавання піддомену відправника в білий список доменів та IP-адрес. Додається весь домен разом із піддоменом (наприклад, sub.domain.com). За необхідності це дає більше гнучкості для фільтрації. Білий список доменів та IP-адрес можна знайти в розділі "Технологія сірих списків і SPF" статті Фільтрація й перевірка. Це стосується елементів, зареєстрованих за допомогою технології сірих списків.

Фільтрація журналу

Функція фільтрації журналу допоможе знайти потрібну інформацію, зокрема коли записів багато. Це дає змогу звузити коло записів журналу, наприклад, якщо ви шукаєте певний тип події, статус або період часу.

Можна відфільтрувати записи журналу, указавивши певні параметри пошуку. У вікні "Файли журналу" відображатимуться лише ті записи, які відповідають параметрам пошуку.

Укажіть ключове слово, яке ви шукаєте, у полі **пошуку тексту**. Щоб увімкнути пошук, скористайтеся розкривним меню **Пошук у стовпцях**. Виберіть один або кілька записів у розкривному меню **Типи записів журналу**. Укажіть **проміжок часу** для відображення результатів. Окрім того, можна використовувати подальші параметри пошуку, наприклад **Тільки слово повністю** або **З регістром**.



Знайти текст

Введіть рядок (слово або частину слова). Будуть показані лише записи, що містять цей рядок. Інші записи буде пропущено.

Знайти в стовпцях

Виберіть стовпці, які будуть враховуватися під час пошуку. Можна вибрати один або кілька стовпців для пошуку.

Типи запису

У розкривному меню виберіть один або кілька типів записів журналу:

• **Діагностика** – запис інформації, необхідної для налаштування програми й усіх зазначених вище записів.

• **Інформація** – запис інформаційних повідомлень, зокрема повідомлень про успішні оновлення, а також усіх зазначених вище записів.

• **Попередження** – запис критичних помилок і попереджувальних повідомлень.

• **Помилки** – запис критичних та інших помилок (як-от "Помилка завантаження файлу").

• **Критичні помилки** – запис лише критичних помилок.

Проміжок часу

Укажіть проміжок часу для відображення результатів.

• Не вказано (за замовчуванням): пошук виконується не в межах проміжку часу, а в усьому журналі.

• Останній день

• Останній тиждень

• Останній місяць

• Проміжок часу: можна вказати точний проміжок часу («Від»: і «До:»), щоб фільтрувати лише записи за вказаний період.

Тільки слово повністю

Використовуйте цей прапорець, щоб отримати точніші результати пошуку за словами повністю.

З урахуванням регістру

Увімкніть цей параметр, якщо для фільтрації важливі літери верхнього й нижнього регістру. Під час налаштування параметрів фільтрації/пошуку натисніть **ОК**, щоб показати відфільтровані записи журналу, **Пошук**, щоб почати пошук.

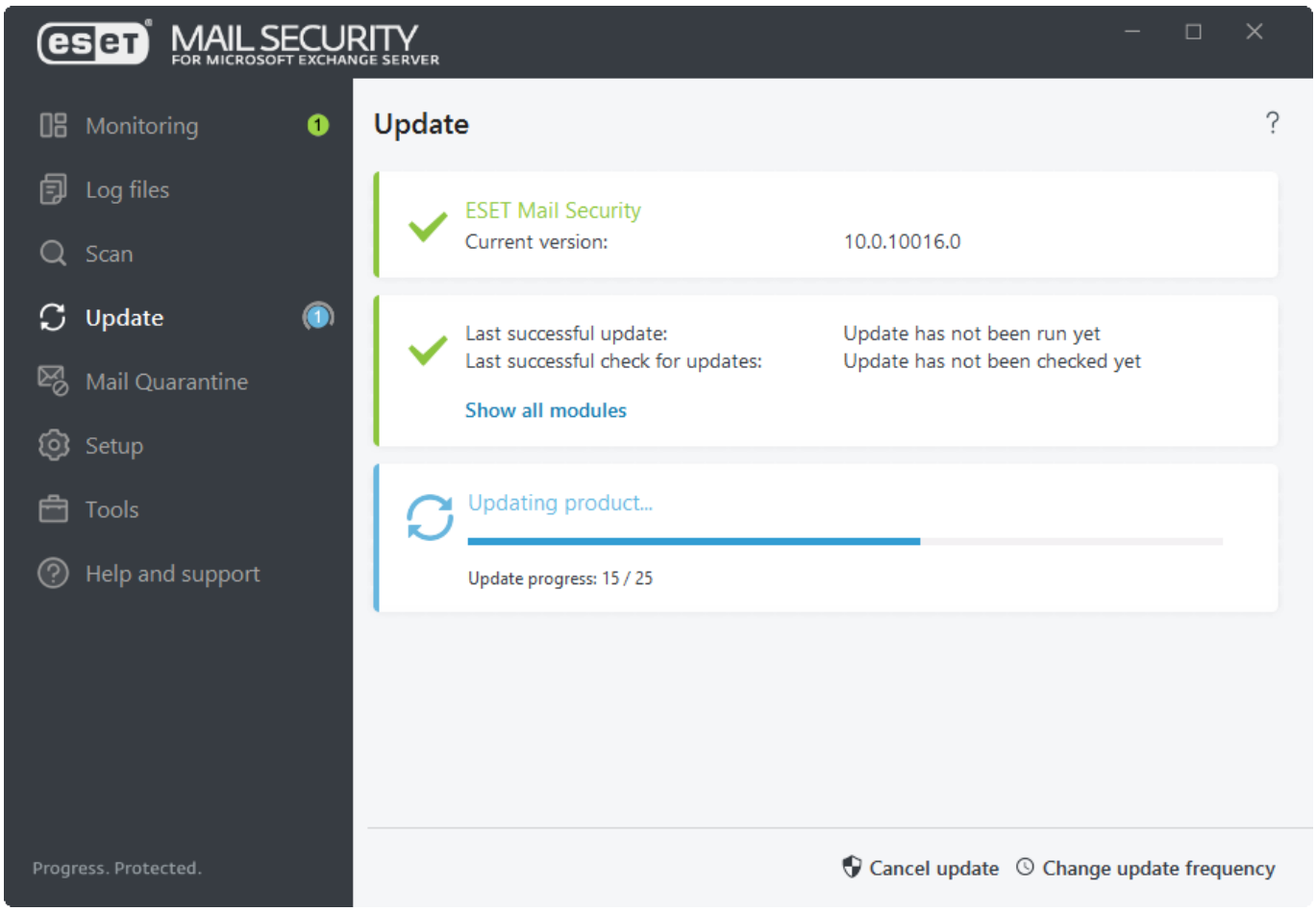
Пошук файлів журналу здійснюється згори донизу, починаючи з поточного місця розташування (виділеного запису). Пошук зупиняється, коли знайдеться перший відповідний запис. Натисніть **F3**, щоб знайти наступний запис, або клацніть правою кнопкою миші й виберіть **Пошук**, щоб увімкнути параметри пошуку.

Оновлення

У розділі "Оновлення" відображається інформація про поточний стан оновлення ESET Mail Security, зокрема дата й час останнього оновлення. Регулярне оновлення ESET Mail Security – найкращий спосіб забезпечити максимальний захист на сервері.

Модуль оновлення гарантує, що програма завжди матиме актуальний стан. Це досягається двома шляхами: оновленням ядра виявлення та системних компонентів. Оновлення ядра виявлення та компонентів програми є важливою частиною забезпечення повного захисту комп'ютера від зловмисного коду.

Якщо ви ще не вводили ліцензійний ключ, то не зможете отримувати оновлення й вам буде запропоновано активувати продукт. Для цього перейдіть у розділ **Довідка та підтримка** > **Активувати продукт**.



Поточна версія

Версія збірки ESET Mail Security.

Останнє успішне оновлення

Дата останнього оновлення. Переконайтеся, що в цьому полі вказано нещодавню дату. Це означатиме, що модулі актуальні.

Дата останньої перевірки оновлень

Дата останньої спроби оновити модулі.

Показати всі модулі

Щоб відкрити список інстальованих модулів.

Перевірити наявність оновлень

Оновлення модулів є важливою складовою забезпечення комплексного захисту від зловмисного коду.

Змінити частоту оновлення

Можна змінити часові параметри для запланованого завдання Регулярне автоматичне оновлення.

Якщо не перевірити наявність оновлень якнайшвидше, з'явиться одне з указаних нижче повідомлень.

Повідомлення про помилку	Описи
Версія оновлення модулів застаріла	Ця помилка з'являється після кількох невдалих спроб оновити модуль. Радимо перевірити параметри оновлення. Найпоширеніша причина помилки – неправильно введені дані для автентифікації або неправильно налаштовані параметри підключення.
Не вдалось оновити модулі: продукт не активовано	Ліцензійний ключ введено неправильно в параметрах оновлення. Радимо перевірити дані для автентифікації. **Додаткові параметри** (**F5**) містять розширені параметри оновлення. Щоб ввести новий ліцензійний ключ, у головному меню натисніть **Довідка та підтримка** > Керувати ліцензією.
Помилка під час завантаження файлів оновлення	Можлива причина цієї помилки – параметри підключення до Інтернету. Радимо перевірити підключення до Інтернету. Для цього відкрийте будь-який веб-сайт у веб-браузері. Якщо веб-сайт не відкривається, можливо, не встановлено підключення до Інтернету або на комп'ютері виникли проблеми з підключенням до мережі. У разі відсутності активного інтернет-з'єднання зверніться до постачальника послуг Інтернету.
Не вдалось оновити модулі. Помилка 0073	Натисніть **Оновити** > **Перевірити наявність оновлень**. Щоб дізнатися більше, перегляньте цю статтю бази знань.

Параметри проксі-сервера для різних профілів оновлення можуть відрізнятися. У такому разі налаштуйте різні профілі оновлення в розділі **Додаткові параметри** (**F5**), натиснувши **Оновити** > Профіль.

Поштовий карантин

Повідомлення електронної пошти та їхні компоненти, як-от вкладення, переміщуються в поштовий карантин замість традиційного файлового карантину. Поштовий карантин забезпечує зручніше керування спамом, інфікованими вкладеннями зі шкідливим програмним забезпеченням або повідомленнями з фішингом. Повідомлення електронної пошти потрапляють у поштовий карантин із різних причин, залежно від того, який модуль захисту ESET Mail Security обробляє повідомлення (захист від шкідливого програмного забезпечення,

антиспам, захист від фішинг-атак, захист від підміни відправника або правила).

Фільтрація за піктограмами

Піктограми можна використовувати для фільтрації повідомлень, щоб бачити лише вкладення, повідомлення електронної пошти або повідомлення з вкладеннями.

Часовий проміжок

Виберіть період часу, за який хочете переглянути переміщені в карантин повідомлення електронної пошти. Якщо вибрати параметр **Спеціальний**, можна вказати діапазон ("Дата від" і "Дата до").

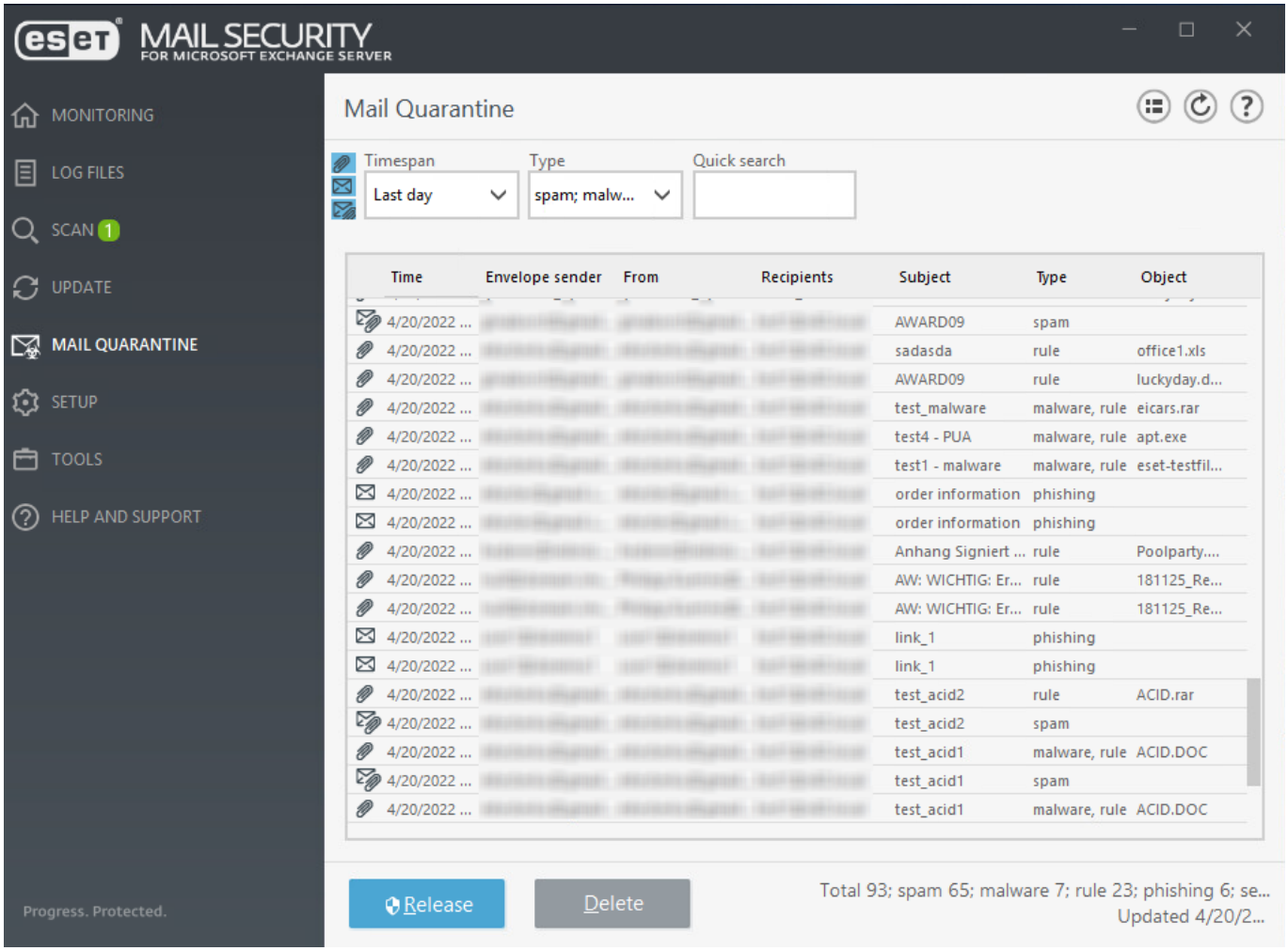
Швидкий пошук

Введіть у текстове поле рядок, щоб відфільтрувати відображувані повідомлення електронної пошти (пошук виконується в усіх стовпцях).

Причина

Використовуйте прапорці, щоб додатково фільтрувати повідомлення за типом причини переміщення в карантин (спам, шкідливе програмне забезпечення, правило, фішинг або підміна відправника).

Дані диспетчера поштового карантину пошти не оновлюються автоматично. Радимо регулярно натискати кнопку **Оновити**  , щоб бачити найновіші елементи в поштовому карантині.



Реліз

Розблоковує надсилання повідомлень електронної пошти їх початковим одержувачам за допомогою каталогу відповіді та видаляє їх із карантину. Натисніть "Так", щоб підтвердити дію. Якщо переміщений у карантин елемент є вкладенням із загальнодоступної папки, для якої вимкнено підтримку пошти, кнопка "Розблокувати" буде недоступна.

Якщо розблокувати повідомлення електронної пошти з карантину, ESET Mail Security ігнорує заголовок MIME `To:`, оскільки його легко підробити. Натомість використовується вихідна інформація про одержувача з команди `RCPT TO:`, яка отримується під час SMTP-з'єднання. Це гарантує, що розблоковане з карантину повідомлення надійде потрібному одержувачу.

Якщо ви розблокуєте повідомлення з карантину в кластерному середовищі, воно більше не буде переміщено в карантин іншими вузлами ESET Mail Security. Це досягається синхронізацією правил між вузлами кластера.

Видалити

Видаляє елементи із карантину. Натисніть **Так**, щоб підтвердити дію. Елементи, видалені в головному вікні програми, видаляються з подання карантину, але залишаються в сховищі. Вони автоматично видаляються пізніше (через три дні за замовчуванням).

Відновити в

Ця опція дає змогу відновити вкладення в указаному розташуванні. Вона доступна лише для

вкладень (для повідомлень ця опція буде неактивна). Якщо потрібно обробити все повідомлення, використовуйте функцію "Розблокувати".

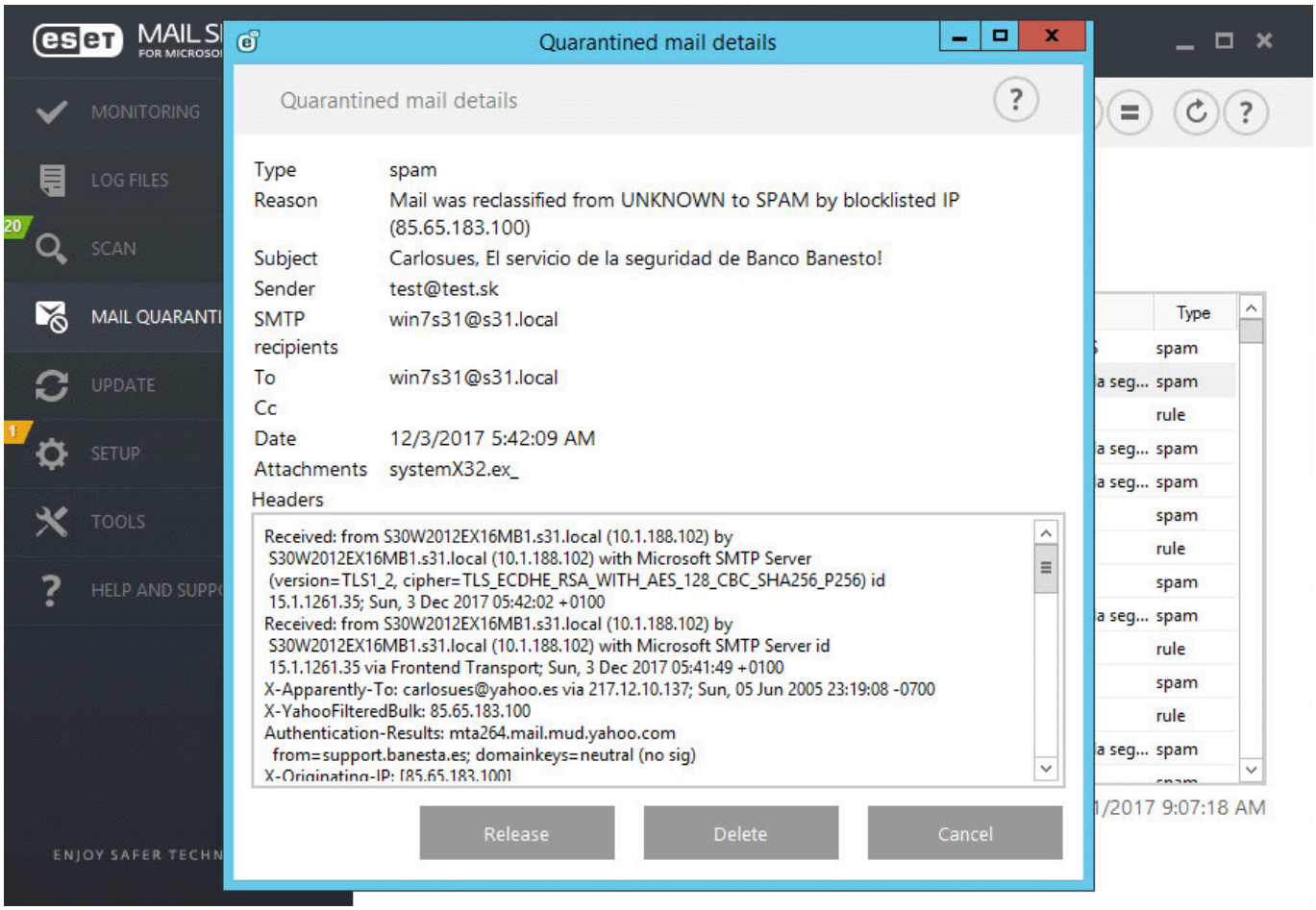
Інформація про переміщену в карантин пошту

Двічі клацніть повідомлення в карантині або клацніть його правою кнопкою миші й виберіть пункт **Показати подробиці**. Відкриється нове вікно з відомостями про електронний лист у карантині. Ви також можете перевірити оригінальні заголовки електронних листів RFC для отримання додаткової інформації.

Відомості про вкладення в карантині

Якщо двічі натиснути вкладення, діалогове вікно з інформацією відрізнятиметься від діалогового вікна з інформацією про повідомлення електронної пошти. Заголовки RFC недоступні, відображається область із текстом конверта вкладення. Можна ввести спеціальний текст конверта вкладення під час розблокування його з поштового карантину.

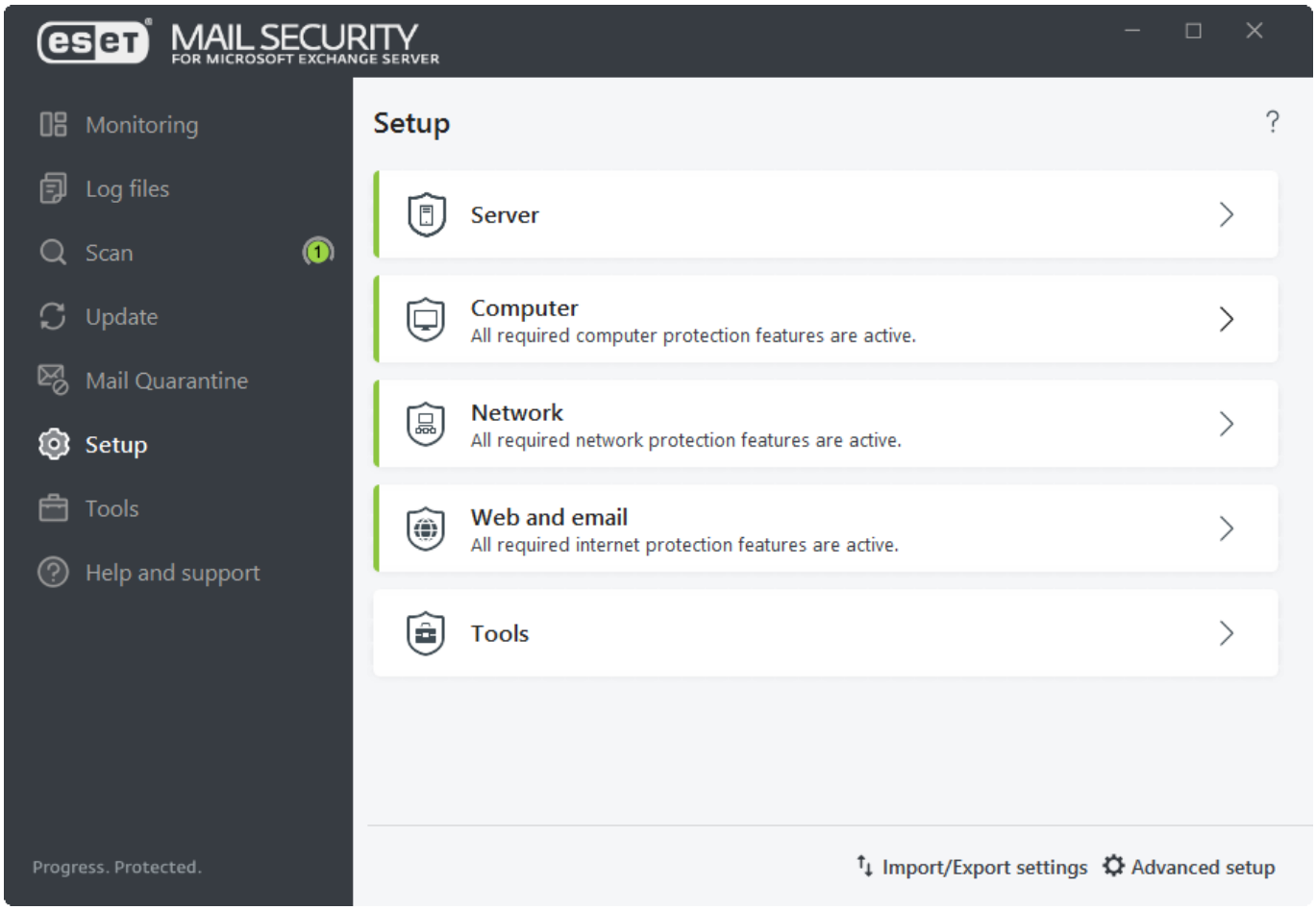
Дії також доступні в контекстному меню. За потреби натисніть **Розблокувати**, **Видалити** або **Видалити назавжди**, щоб вжити дію до переміщеного в карантин повідомлення електронної пошти. Натисніть **Так**, щоб підтвердити дію. Якщо вибрати опцію **Видалити назавжди**, повідомлення також буде видалено з файлової системи. Натомість опція **Видалити** вилучить елемент із подання диспетчера поштового карантину.



Налаштування

Вікно "Параметри" містить наведені далі розділи.

- Сервер
- Комп'ютер
- Мережа
- Інтернет і електронна пошта
- Інструменти – Ведення журналу діагностики



Щоб тимчасово вимкнути певний модуль, натисніть біля нього зелений повзунок . Це може зменшити рівень захисту сервера.

Щоб повторно активувати вимкнений компонент системи безпеки, поруч із відповідним модулем натисніть червоний повзунок . Компонент повернеться до ввімкненого стану.

Щоб відкрити розширені параметри певного компонента системи безпеки, натисніть піктограму шестерні .

Імпорт/Експорт параметрів

Завантажте параметри налаштування за допомогою файлу конфігурації *.xml* або збережіть

поточні параметри у файл.

Додаткові параметри

Налаштуйте додаткові параметри й опції відповідно до своїх потреб. Щоб відкрити **додаткові параметри** з будь-якого екрана програми, натисніть **F5**.

Сервер

Ви побачите список компонентів, які можна ввімкнути або вимкнути за допомогою повзунка  . Щоб налаштувати параметри певного елемента, натисніть піктограму шестерні ⚙.

Захист від вірусів

Забезпечує захист від зловмисних атак на систему завдяки контролю файлів, електронної пошти й обміну даними через інтернет-з'єднання.

Антиспам

Містить низку технологій (RBL, DNSBL, аналіз цифрових відбитків, перевірка репутації, аналіз вмісту, правила, ручне складання білих/чорних списків тощо) для максимального виявлення загроз, пов'язаних з електронною поштою.

Захист від фішинг-атак

Аналізує тіло повідомлення вхідних електронних листів на фішингові посилання (URL-адреси).

Сканування бази даних поштових скриньок Microsoft 365

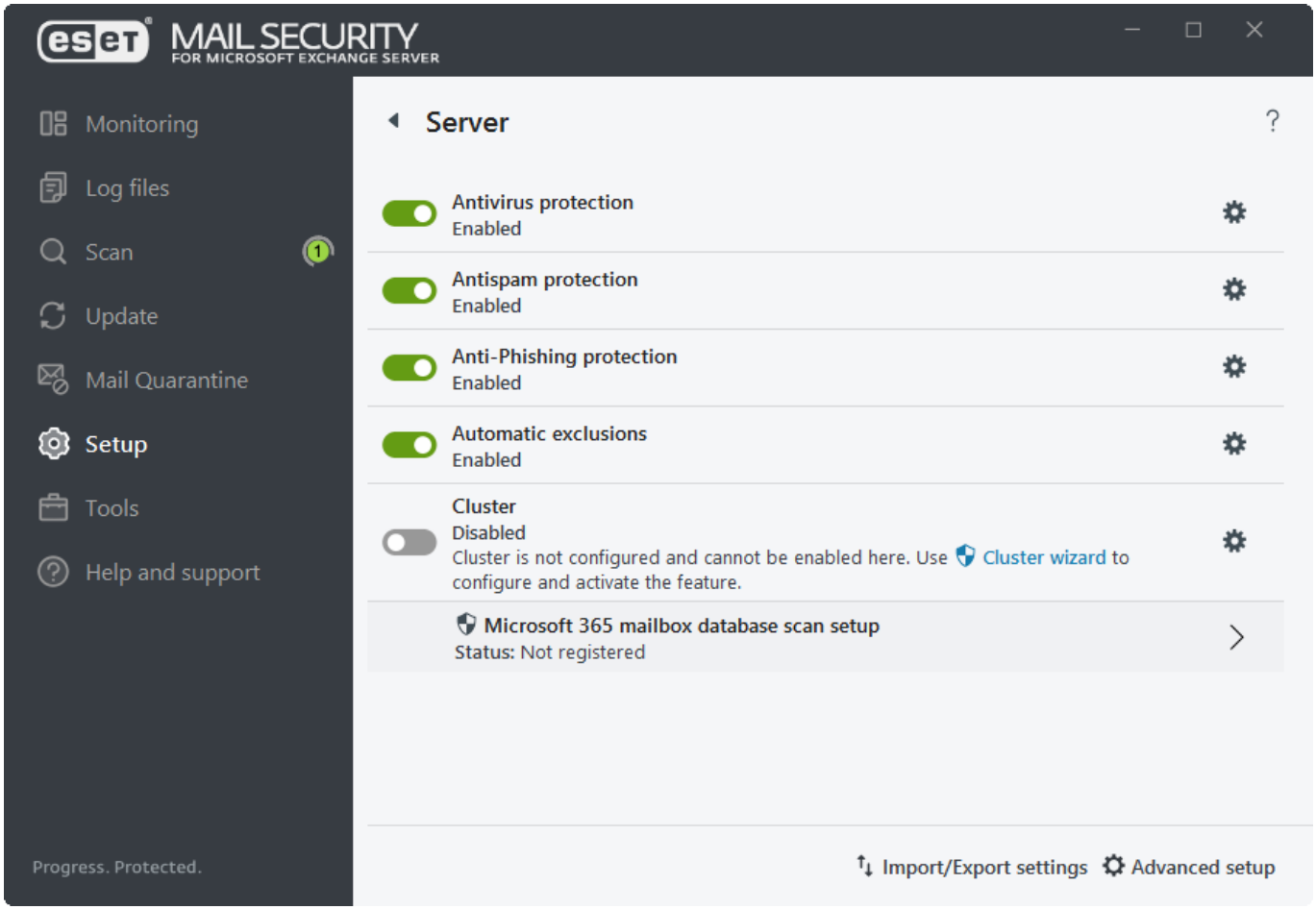
Щоб активувати цю функцію, зареєструйте сканер ESET Mail Security.

Автоматичні виключення

Визначає критичні серверні програми й файли операційної системи сервера й автоматично додає їх до списку виключень. Цей функціонал дає змогу мінімізувати ризик виникнення потенційних конфліктів і підвищити загальну продуктивність сервера під час запуску програмного забезпечення для виявлення загроз.

Кластер

Налаштування та активація кластера ESET.



Комп'ютер

ESET Mail Security має всі необхідні компоненти, щоб забезпечити надійний захист сервера як комп’ютера. За допомогою цього модуля можна вмикати, вимикати й налаштовувати вказані нижче компоненти.

Захист файлової системи в режимі реального часу

Усі файли скануються на наявність шкідливого коду під час відкриття, створення або запуску на комп’ютері. Для захисту файлової системи в режимі реального часу також передбачено параметр **Налаштувати** або **Редагувати виключення**. Якщо його вибрати, відкриється вікно налаштування виключень, у якому можна виключити файли й папки зі сканування.

Контроль пристроїв

За допомогою цього модуля можна сканувати, блокувати та налаштовувати розширені фільтри й дозволи, а також указати, чи може користувач отримувати доступ до пристрою та працювати з ним.

Система запобігання вторгненням (HIPS)

Система відстежує події, які відбуваються в операційній системі, і реагує на них відповідно до спеціального набору правил.

- Розширений сканер пам’яті

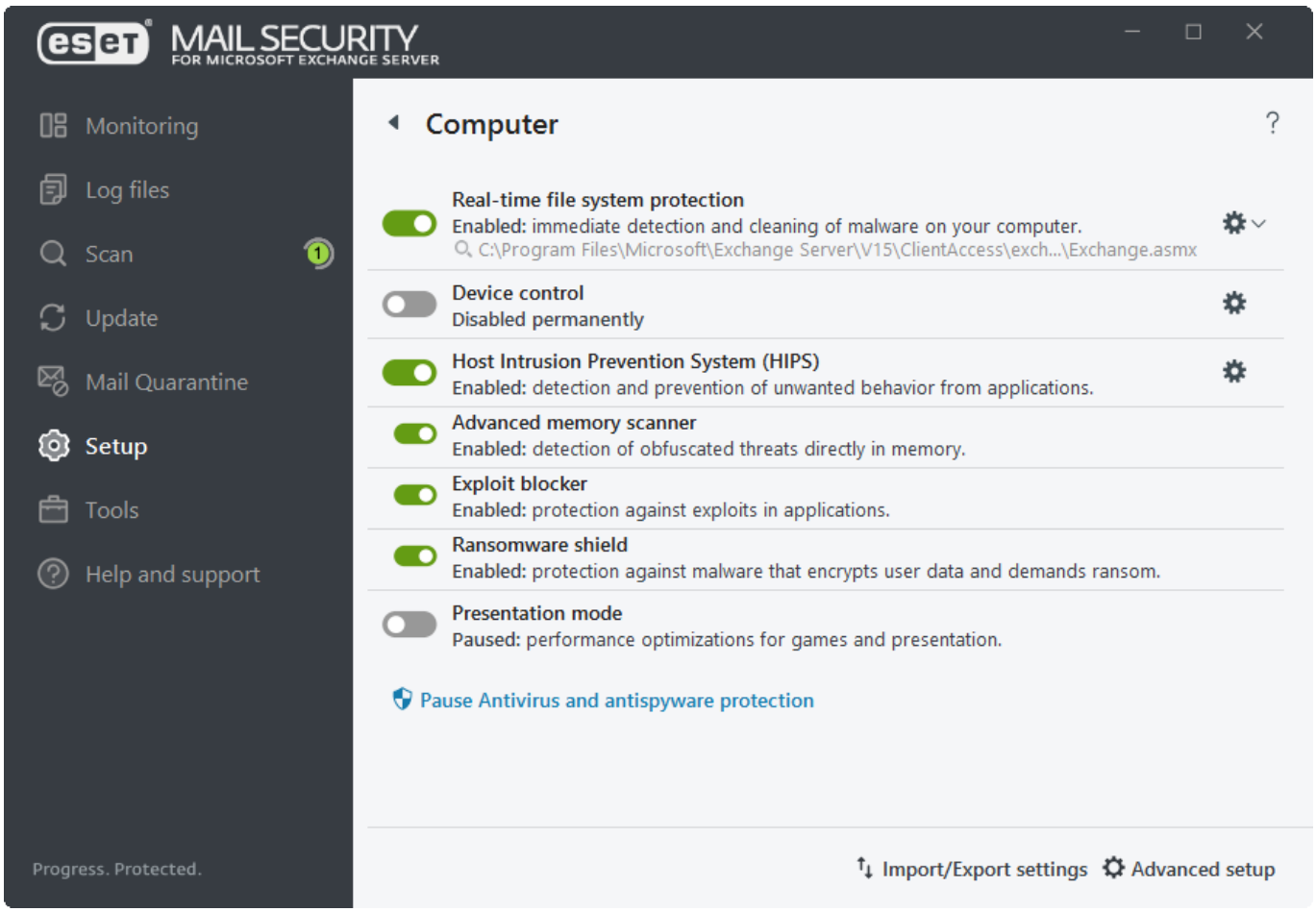
- Захист від експлойтів
- Захист від програм-вимагачів

Режим презентації

Функція для користувачів, яким потрібна відсутність будь-яких перерв під час використання програмного забезпечення та відволікальних спливних вікон, а також коли потрібно звести до мінімуму споживання ресурсів процесора. Ви отримаєте повідомлення з попередженням (потенційна загроза безпеці), а після ввімкнення режиму презентації головне вікно програми стане оранжевим.

Призупинити роботу антивіруса та антишпигуна на певний період часу

Щоразу під час тимчасового вимкнення захисту від вірусів і шпигунських програм у розкривному меню можна вибрати період часу, протягом якого має бути вимкнено вибраний компонент, і натиснути **Застосувати**, щоб вимкнути компонент системи безпеки. Щоб знову ввімкнути захист, натисніть **Увімкнути захист від вірусів і шпигунських програм** або зробіть це за допомогою повзунка.



Мережа

Для цього окремі мережеві з’єднання дозволяються або забороняються на основі заданих правил фільтрації. Це захищає від атак із віддалених комп’ютерів і блокує деякі потенційно небезпечні служби.

Мережа модуль дає змогу вмикати, вимикати й налаштовувати вказані нижче компоненти.

Захист від мережевих атак (IDS)

Аналізує вміст мережевого трафіку й захищає мережу від атак. Трафік, який вважатиметься шкідливим, блокуватиметься.

Захист від ботнетів

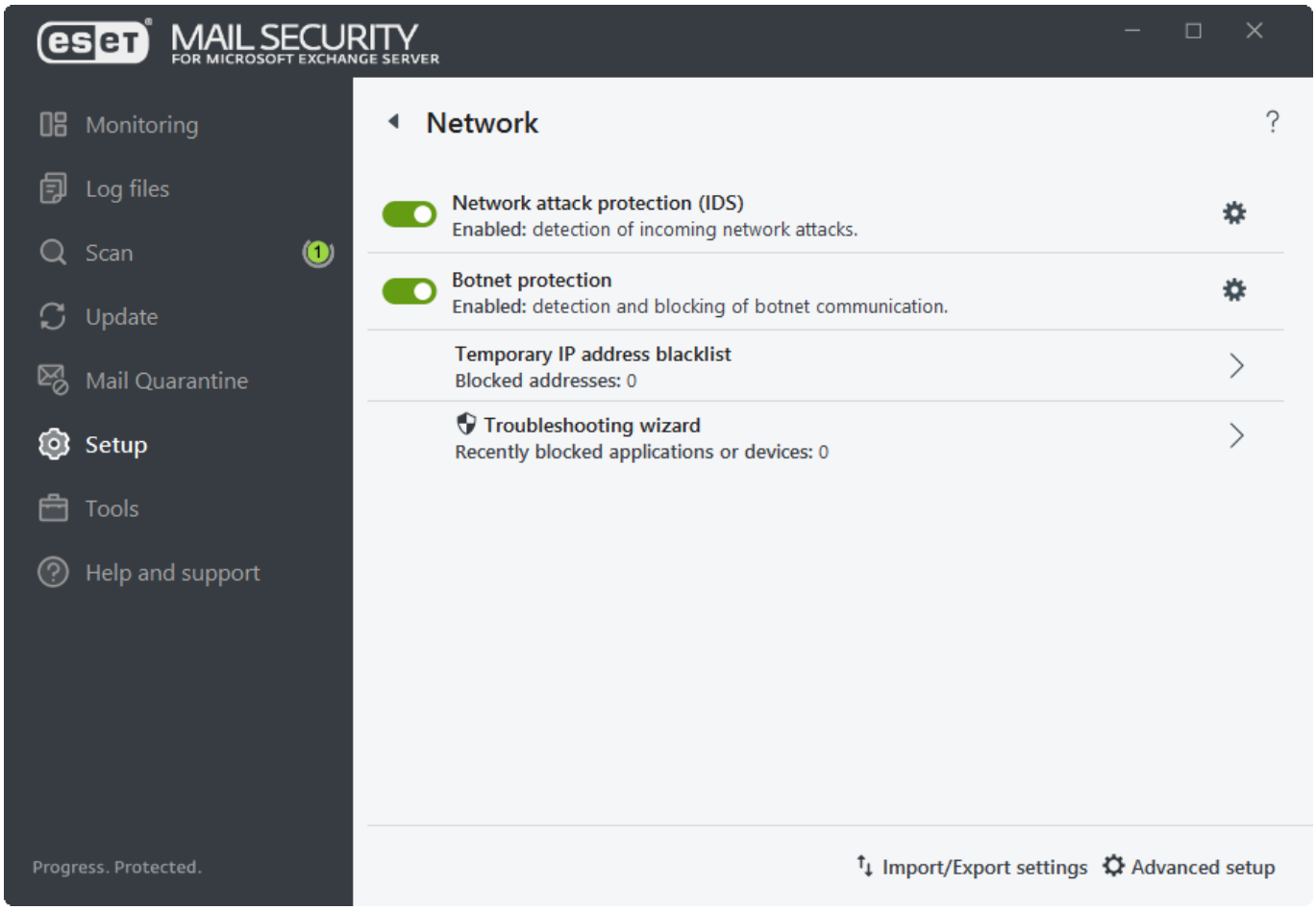
Виявлення і блокування ботнет-з'єднань. Швидко й точно визначає зловмисне ПЗ в системі.

Тимчасовий чорний список IP-адрес (заблоковані адреси)

Переглянути список IP-адрес, визначених як джерело атак і доданих до чорного списку, що блокує підключення до них протягом певного періоду часу.

Майстер виправлення неполадок (нещодавно заблоковані програми або пристрої)

Допомагає вирішувати проблеми з підключенням, спричинені захистом від мережевих атак.



Майстер виправлення неполадок мережі

Майстер виправлення неполадок відстежує всі заблоковані підключення й допомагає виконати процес усунення проблем захисту від мережевих атак для певних програм чи пристроїв. Після цього майстер запропонує новий набір правил, які застосовуватимуться, якщо ви схвалите їх.

У розкривному меню виберіть проміжок часу, протягом якого було заблоковано зв’язок. У списку нещодавно заблокованих зв’язків наводяться загальні відомості про тип програми або пристрій, репутацію, а також загальна кількість програм і пристроїв, заблокованих протягом цього проміжку часу. Щоб дізнатися більше про заблоковані зв’язки, клацніть **Докладно**.

На наступному кроці потрібно розблокувати програму або пристрій, де виникли проблеми з підключенням.

Якщо клацнути Розблокувати, раніше заблокований зв’язок буде дозволено. Якщо не вдається усунути проблеми з програмою або пристрій не працює належним чином, клацніть **Програма все одно не працює**. Усі зв’язки, раніше заблоковані для цього пристрою, тепер будуть дозволені. Якщо не вдається усунути проблему, перезавантажте комп’ютер.

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

Клацніть **Розблокувати інший елемент**, щоб усунути проблеми зв’язку з іншим пристроєм або програмою.

Інтернет і електронна пошта

Інтернет і електронна пошта дозволяють вмикати, вимикати й налаштовувати вказані нижче компоненти.

Захист доступу до Інтернету

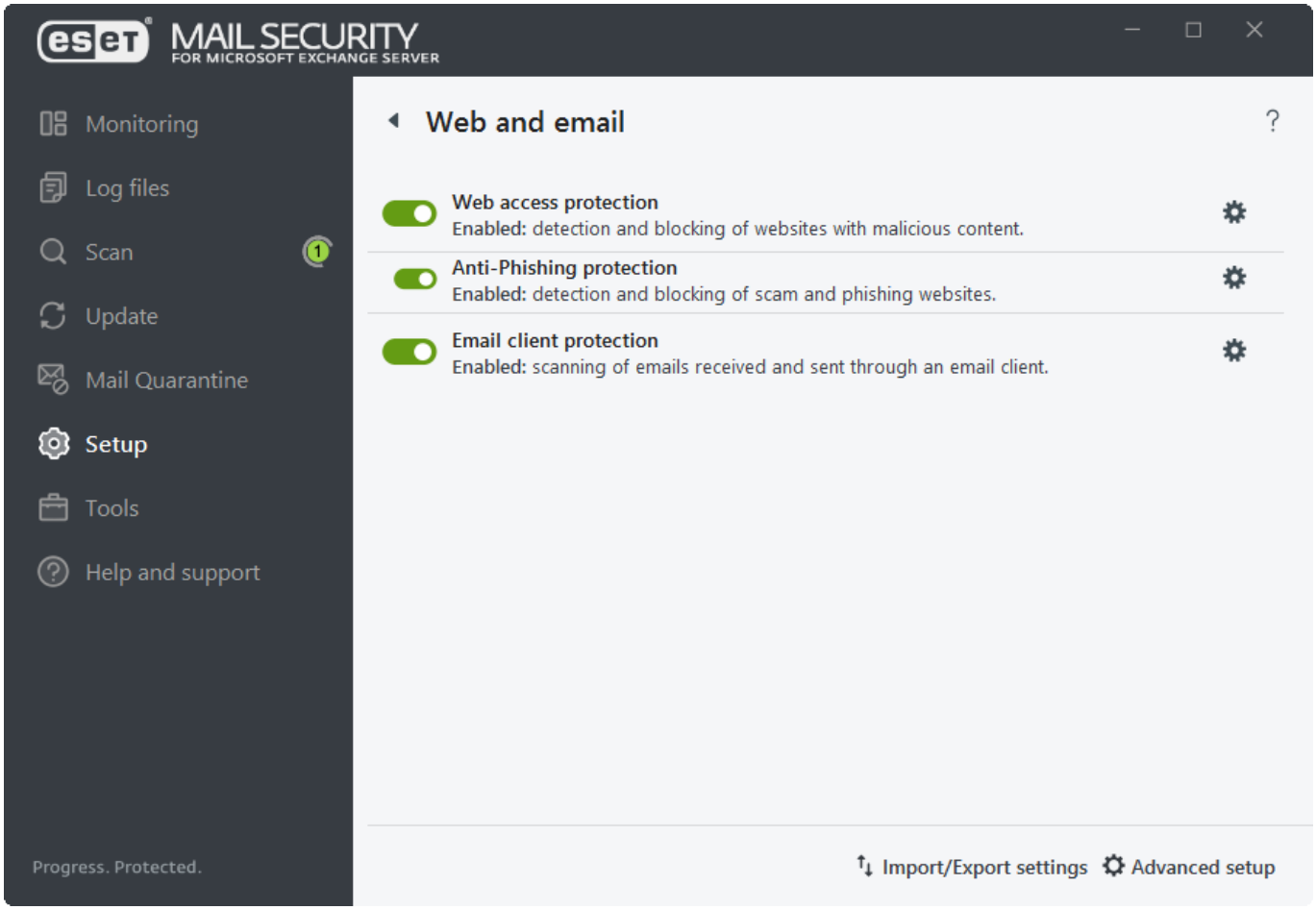
Якщо цей параметр увімкнено, увесь трафік за протоколами HTTP та HTTPS сканується на наявність шкідливого програмного забезпечення.

Захист від фішинг-атак

Захист від спроб незаконних сайтів отримати паролі, банківські дані й іншу конфіденційну інформацію.

Захист поштового клієнта

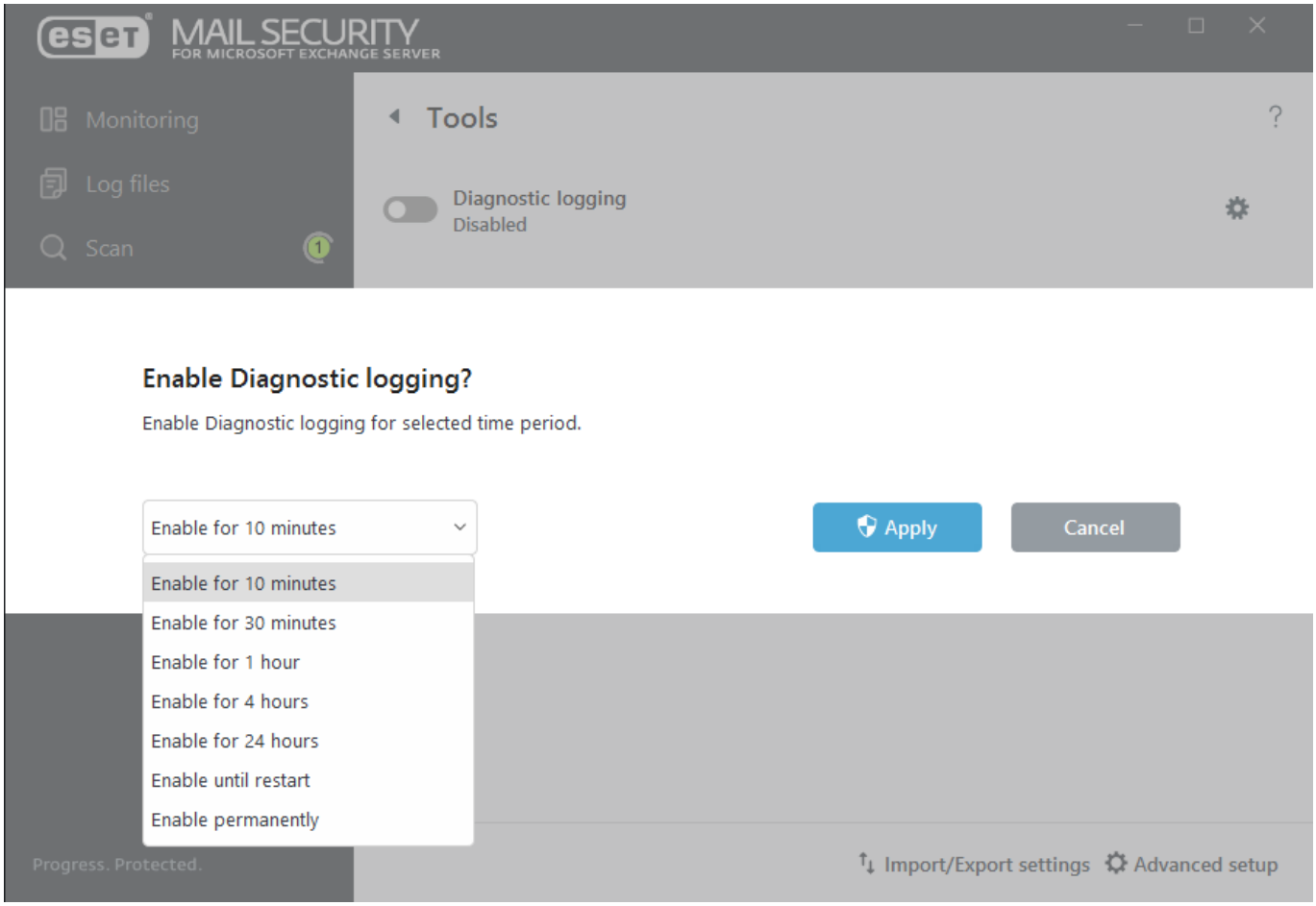
Контролює обмін даними через протоколи POP3 та IMAP.



Інструменти – Ведення журналу діагностики

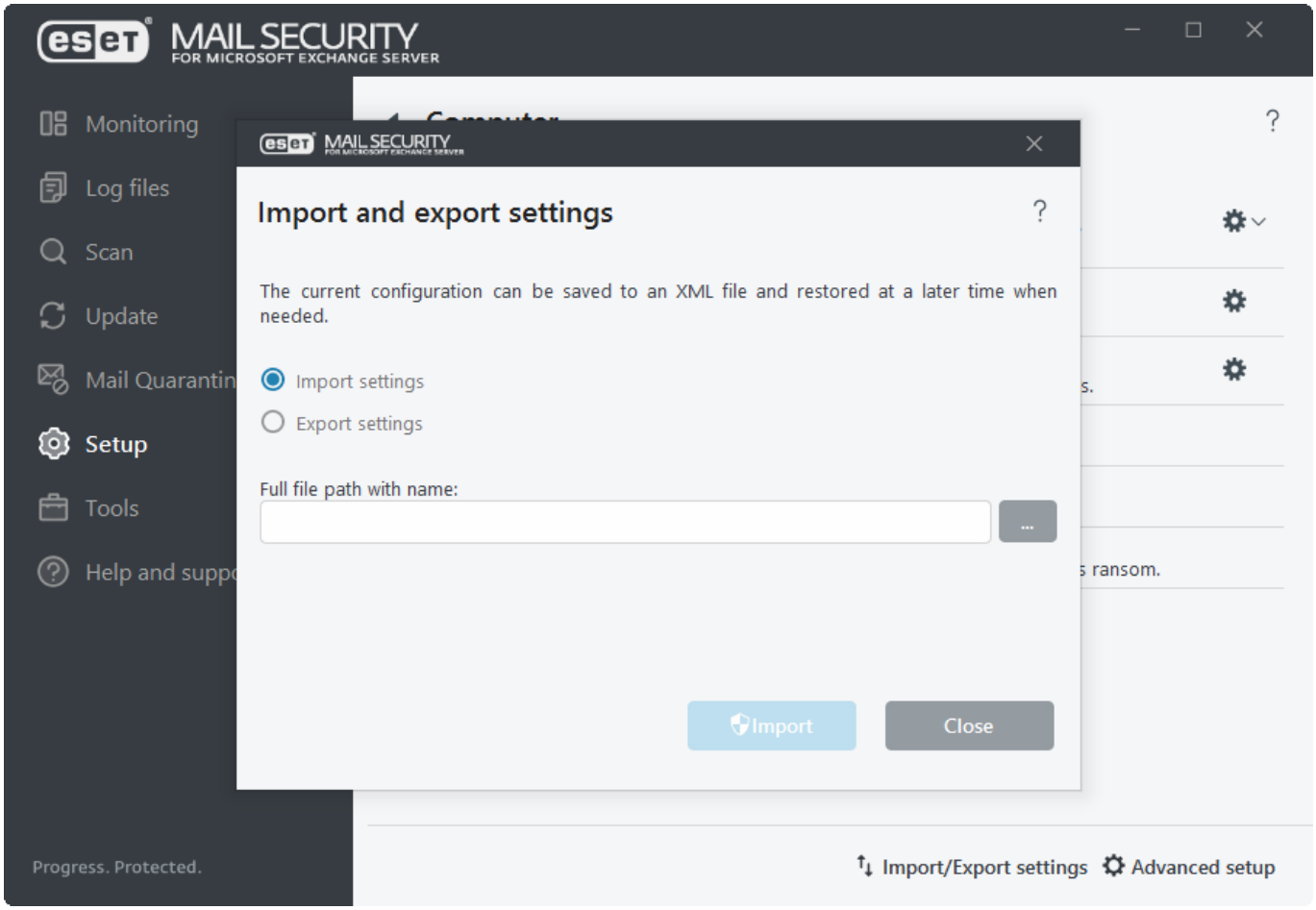
Ведення журналу діагностики можна ввімкнути, якщо потрібна докладна інформація про поведінку певної функції ESET Mail Security, наприклад під час виправлення неполадок. Якщо натиснути піктограму шестерні , можна налаштувати, для яких функцій потрібно збирати журнали діагностики.

Виберіть, протягом якого періоду цю функцію має бути ввімкнено (10 хвилин, 30 хвилин, 1 година, 4 години, 24 години, до наступного перезавантаження сервера або завжди). Щойно ви ввімкнете ведення журналу діагностики, ESET Mail Security збиратиме докладні журнали відповідно до ввімкнених функцій.



Імпорт/Експорт параметрів

Функція імпорту/експорту параметрів стане в пригоді, якщо потрібно створити резервне копіювання поточної конфігурації ESET Mail Security. Також можна використовувати функцію імпорту, щоб застосовувати однакові параметри на інших серверах із ESET Mail Security. Параметри експортуються у файл *.xml*.

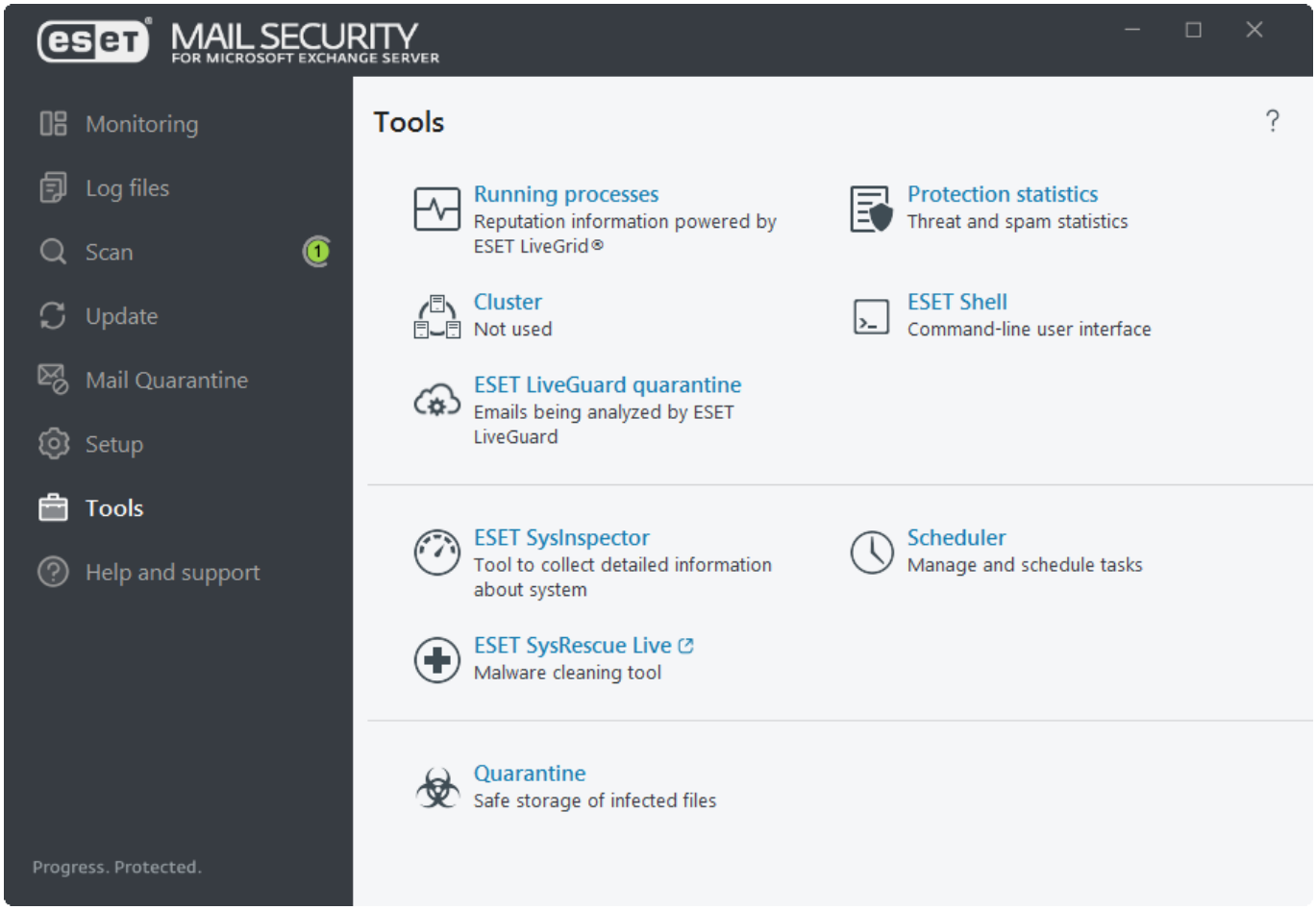


Якщо у вас немає прав на запис експортованого файлу у вказаний каталог, під час експортування параметрів може виникнути помилка.

Інструменти

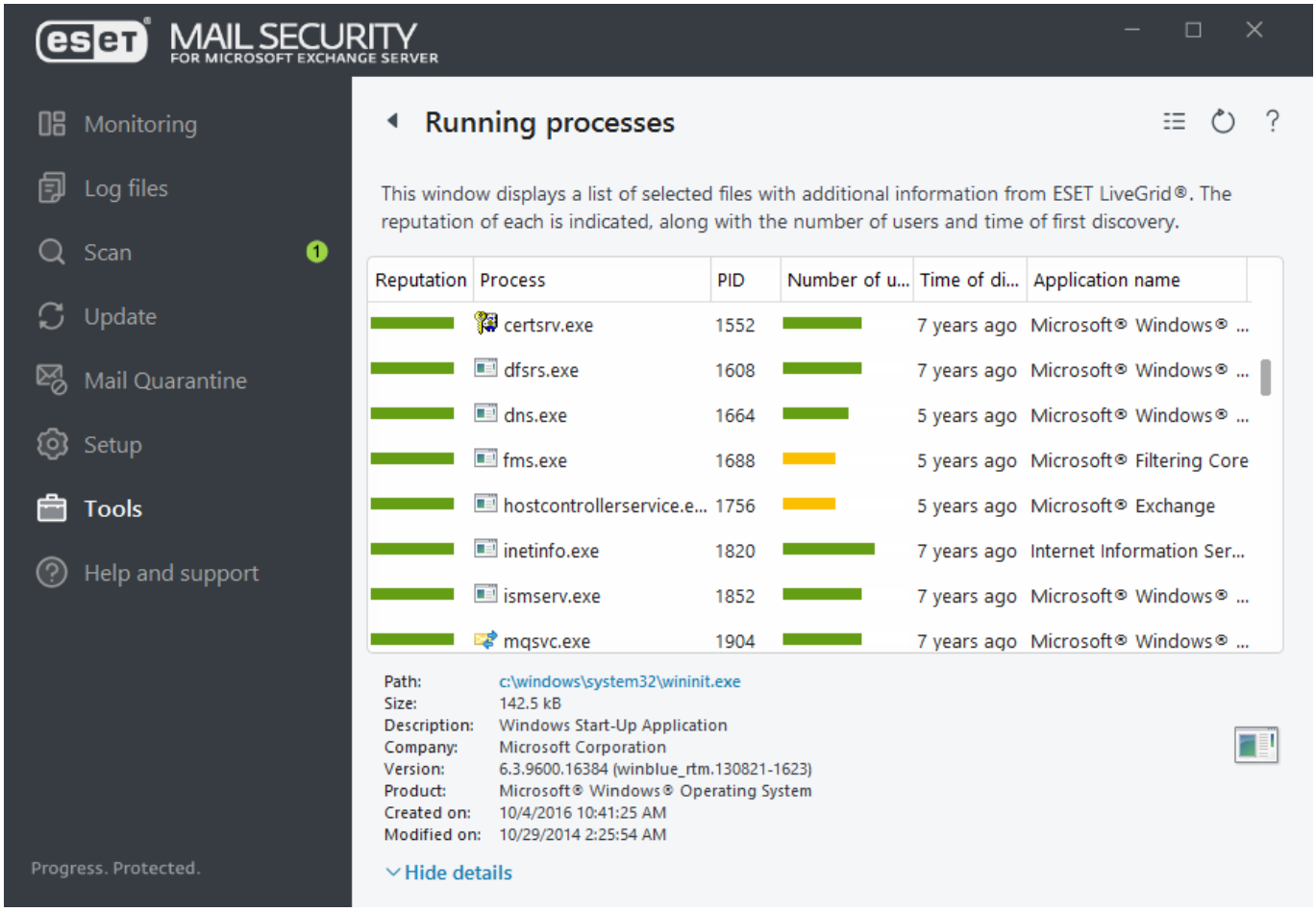
Для адміністрування ESET Mail Security доступні вказані нижче функції.

- Запущені процеси
- Статистика захисту
- Кластер
- Оболонка ESET
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live
- Розклад
- Надіслати файл для аналізу
- Карантин



Запущені процеси

Вкладка запущених процесів відображає на комп’ютері запущені програми або процеси. ESET негайно й постійно сповіщає про нові зараження. ESET Mail Security надає докладну інформацію про запущені процеси, щоб захистити користувачів за допомогою технологій ESET LiveGrid®.



Програми з позначкою "Найкраща репутація" (зелений) є чистими (у білому списку) і не скануватимуться. Це допоможе пришвидшити сканування комп'ютера за вимогою або захист файлової системи в режимі реального часу.

Репутація	**У більшості випадків технології ESET Mail Security та ESET LiveGrid® визначають репутацію об'єкта з використанням низки евристичних правил, які визначають характеристики кожного об'єкта (файли, процеси, розділи реєстру тощо), а потім зважують свій потенціал для зловмисної активності. На основі цих евристичних даних об'єктам призначається рівень репутації від 9 – найкраща репутація (зелений) до 0 – найгірша репутація (червоний).**
Процесор	Назва зображення програми або процесу, що наразі запущено на вашому комп'ютері. Диспетчер завдань Windows також можна використовувати для перегляду всіх запущених на комп'ютері процесів. Щоб відкрити диспетчер завдань, натисніть правою кнопкою миші порожню область на панелі завдань і виберіть диспетчер завдань або натисніть CTRL + SHIFT + ESC на клавіатурі.
PID	Це ідентифікатор процесів, запущених в операційних системах Windows.
Кількість користувачів	Кількість користувачів, які використовують певну програму. Збір цієї інформації технологіями ESET LiveGrid®.
Час виявлення	Період часу, коли програму було виявлено технологією ESET LiveGrid®.
Ім'я програми	Назва програми, до якої належить цей процес.

Якщо програму позначено як невідому (помаранчевий колір), вона не обов’язково є шкідливим програмним забезпеченням. Зазвичай це лише нова програма. Якщо ви не впевнені в цьому файлі, скористайтеся функцією Надіслати файл для аналізу, щоб надати файл в антивірусну лабораторію ESET. Якщо виявиться, що файл шкідливий, виявлений об’єкт буде додано до одного з майбутніх оновлень ядра виявлення.

Показати подробиці

У нижній частині вікна відобразиться така інформація:

- **Шлях**: місцезнаходження програми на комп’ютері.
- **Розмір**: розмір файлу в КБ (кілобайтах) або МБ (мегабайтах).
- **Опис**: характеристики файлу на основі опису операційної системи.
- **Компанія**: назва постачальника або процесу програми.
- **Версія**: інформація від видавця програми.
- **Продукт**: назва програми та/або компанії.
- **Дата створення**: дата й час створення програми.
- **Дата змінення**: дата й час останньої зміни програми.

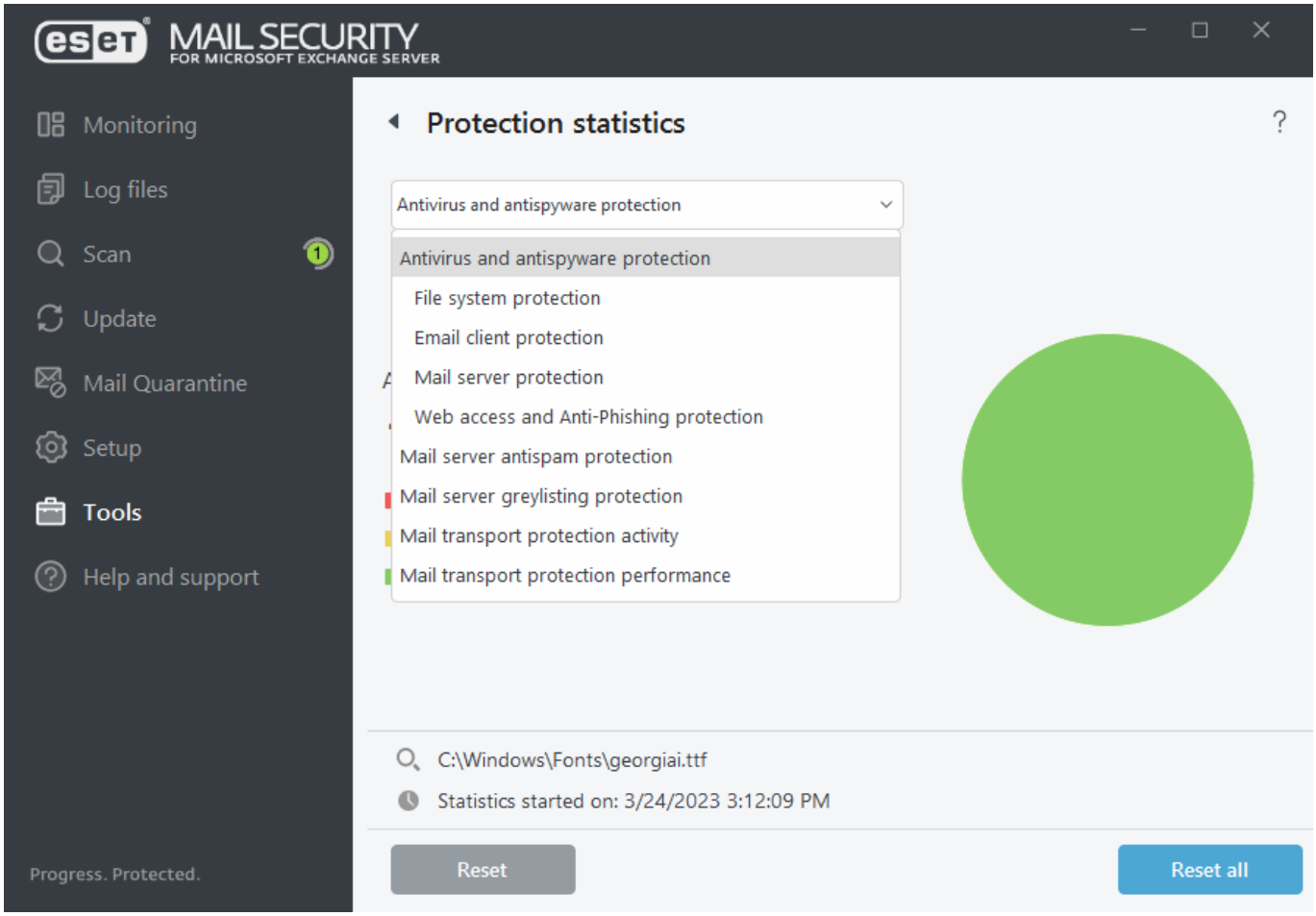
Додати до виключених процесів

Натисніть процес правою кнопкою миші у вікні запущених процесів, щоб виключити його з перевірки. Його шлях буде додано до списку виключень процесів.

Статистика захисту

Щоб переглянути статистичні дані, пов’язані з модулями захисту ESET Mail Security, виберіть потрібний модуль захисту в розкривному меню. Статистика містить інформацію, як-от кількість просканованих, інфікованих, очищених і чистих об’єктів.

Якщо навести курсор миші на об’єкт поруч із діаграмою, відобразяться дані лише конкретного об’єкта. Щоб очистити статистичну інформацію для поточного модуля захисту, натисніть **Скинути**. Щоб очистити дані для всіх модулів, натисніть **Скинути все**.



В ESET Mail Security доступні вказані нижче статистичні діаграми.

Антивірус та антишпигун

Відображення загальної кількості інфікованих та очищених об’єктів.

Захист файлової системи

Відображення лише об’єктів, які зчитуються з файлової системи або записуються в неї.

Захист Hyper-V

Відображення загальної кількості інфікованих, очищених і чистих об’єктів (лише в системах із Hyper-V).

Захист поштового клієнта

Відображення лише об’єктів, надісланих або отриманих поштовими клієнтами.

Захист доступу до Інтернету та захист від фішинг-атак

Відображення лише об’єктів, завантажених веб-браузерами.

Захист поштового сервера

Відображення статистики захисту поштового сервера від шкідливого програмного

забезпечення.

Антиспам для поштового сервера

Відображення журналу статистики антиспаму. Параметр "Кількість не просканованих" позначає об’єкти, виключені зі сканування (відповідно до правил, внутрішніх повідомлень, автентифікованих підключень тощо).

Захист поштового сервера з використанням технології сірих списків

Містить статистику антиспаму, згенеровану за допомогою технології сірих списків.

Активність захисту передачі пошти

Відображення об’єктів, перевірених, заблокованих або видалених поштовим сервером.

Продуктивність захисту передачі пошти

Відображення даних, оброблених за допомогою VSAPI або транспортного агента, у б/с.

Активність захисту бази даних поштових скриньок

Відображення об’єктів, оброблених за допомогою VSAPI (кількість перевірених, переміщених у карантин і видалених об’єктів).

Продуктивність захисту бази даних поштових скриньок

Відображення даних, оброблених за допомогою VSAPI (кількість різних середніх значень на сьогодні, протягом останніх 7 днів і середнє значення з моменту останнього скидання).

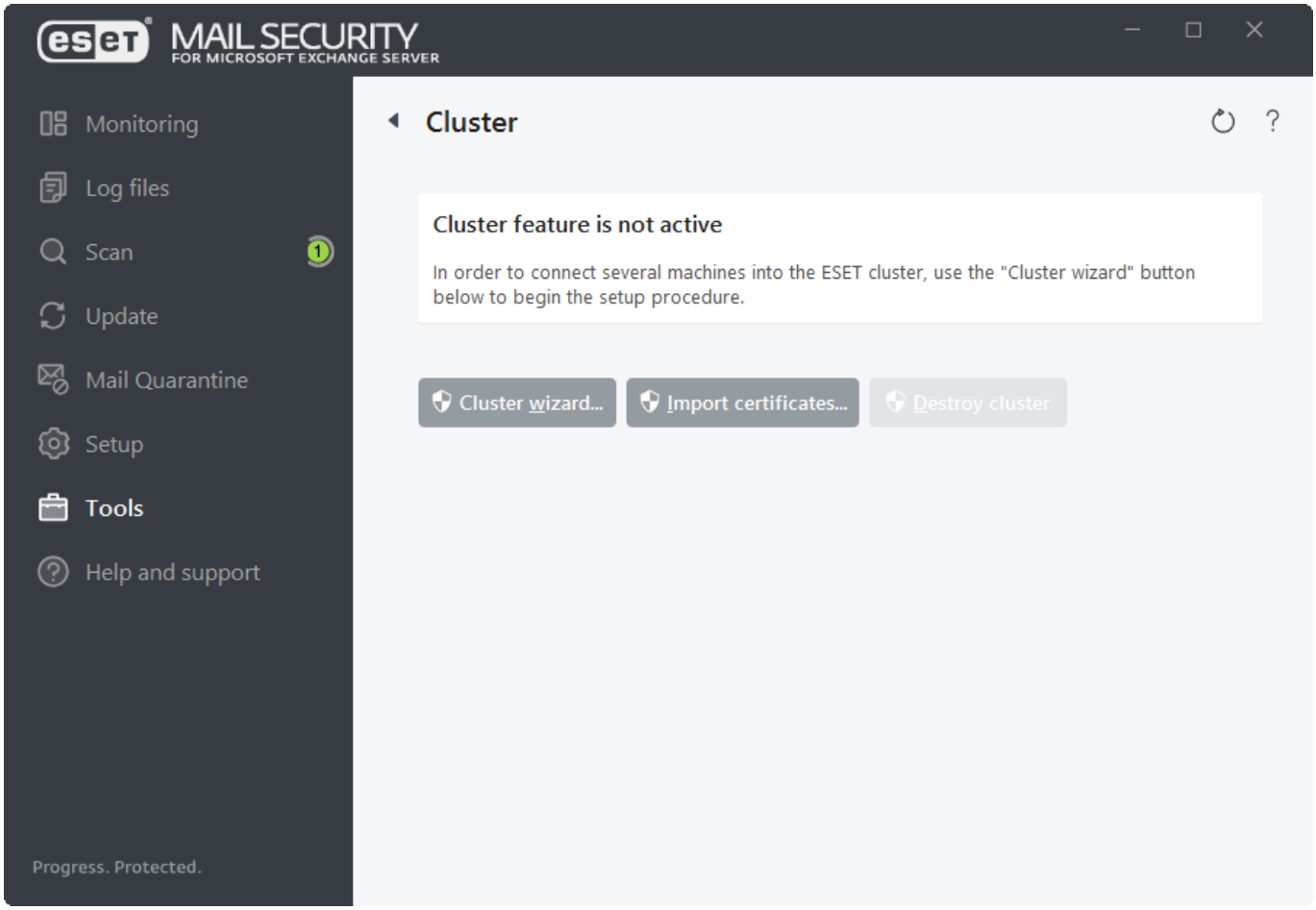
Кластер

Кластер ESET – це однорангова (P2P) комунікаційна інфраструктура лінійки продуктів ESET для Microsoft Windows Server. Кластер ESET ідеально підходить для інфраструктури Exchange із кількома серверами, наприклад DAG.

Ця інфраструктура дає змогу серверним продуктам ESET взаємодіяти один з одним та обмінюватися даними, наприклад відомостями про конфігурацію та сповіщеннями, синхронізувати бази даних "сірих списків", а також синхронізувати дані, необхідні для правильної роботи групи екземплярів продуктів. Прикладом такої групи є група вузлів у відмовостійкому кластері Windows або кластері балансування мережевого навантаження (NLB) з продуктами ESET, інстальованими там, де необхідна однакова конфігурація продукту у всьому кластері. Кластер ESET забезпечує однакову конфігурацію в кількох екземплярах.

Параметри інтерфейсу користувача та запланованих завдань різних вузлів кластера ESET не синхронізуються. Це зроблено навмисно. Наприклад, щоб не запускати заплановане сканування бази даних на вимогу одночасно на всіх вузлах кластера й уникнути непотрібних проблем із продуктивністю.

Журнали захисту поштового сервера залишаються окремими для кожного вузла кластера. Таким чином, журнали не синхронізуються. На кожному вузлі можна скористатися функцією Експортувати на сервер syslog, щоб скопіювати журнали на сервер Syslog у форматі CEF, або скористатися інструментом SIEM. Крім того, ви можете скористатися функцією "Експорт до журналів програм і служб Windows", якщо потрібно отримувати дані журналів звідти.



Створення кластера ESET між ESET Mail Security та ESET File Security для Linux не підтримується.

Під час налаштування кластера ESET вузли можна додавати двома способами.

• **Автовиявлення** – якщо у вас є відмовостійкий кластер Windows / кластер NLB, функція автовиявлення автоматично додасть вузли учасника до кластера ESET.

• **Огляд** – вузли можна додавати вручну. Для цього потрібно ввести імена серверів (учасників однієї робочої групи або одного домену).

Якщо розблокувати повідомлення електронної пошти з карантину, ESET Mail Security ігнорує заголовок MIME `To:`, оскільки його легко підробити. Натомість використовується вихідна інформація про одержувача з команди `RCPT TO:`, яка отримується під час SMTP-з'єднання. Це гарантує, що розблоковане з карантину повідомлення надійде потрібному одержувачу.

Після додавання вузлів до кластера ESET наступний крок – інсталяція ESET Mail Security на кожному вузлі. Це виконується автоматично під час налаштування кластера ESET. Нижче наведено облікові дані, необхідні для віддаленої інсталяції ESET Mail Security на інших вузлах кластера.

- **Сценарій домену –** облікові дані адміністратора домену.
- **Сценарій робочої групи**. Необхідно переконатися, що всі вузли використовують однакові облікові дані локального адміністратора.

Крім того, у кластері ESET можна використовувати комбінацію автоматично доданих вузлів, що є учасниками наявного відмовостійкого кластера Windows / кластера NLB, а також вузлів, доданих у ручному режимі (якщо вони входять в один домен).

Використовувати вузли домену разом із вузлами робочої групи не можна.

Ще однією вимогою для кластера ESET є ввімкнення параметра **Спільний доступ до файлів і принтерів** у брандмауері Windows перед поширенням ESET Mail Security на вузли кластера ESET.

За допомогою Майстра кластера до кластера ESET можна будь-коли додати нові вузли.

Імпортувати сертифікати

Сертифікати використовуються для забезпечення надійної автентифікації від комп'ютера до комп'ютера під час використання протоколу HTTPS. Для кожного кластера ESET існує незалежна ієрархія сертифікатів. Ієрархія має один кореневий сертифікат і набір сертифікатів вузлів, підписаних кореневим сертифікатом. Після створення всіх вузлів сертифікатів закритий ключ кореневого сертифіката знищується. Під час додавання нового вузла до кластера створюється нова ієрархія сертифікатів. Перейдіть до папки, що містить сертифікати (які створив майстер кластера). Виберіть файл сертифіката й натисніть **Відкрити**.

Знищити кластер?

Кластери ESET можна демонтувати. До журналу подій кожного вузла буде додано запис про знищення кластера ESET. Після цього всі правила брандмауера ESET буде видалено з брандмауера Windows. Колишні вузли буде повернуто до попереднього стану, і, якщо необхідно, їх можна буде знову використовувати в іншому кластері ESET.

Майстер кластера – вибір вузлів

Перший крок під час налаштування кластера ESET – додавання вузлів. Для додавання вузлів можна скористатись опцією **Виявляти автоматично** або **Огляд**. Також можна ввести ім'я сервера в текстове поле й натиснути **Додати**.

Виявляти автоматично

Автоматичне додавання вузлів з наявного Windows Failover Cluster / Network Load Balancing (NLB) Cluster. Для автоматичного додавання вузлів сервер, який використовується для створення кластера ESET, повинен бути учасником цього Windows Failover Cluster / NLB Cluster. Щоб кластер ESET міг правильно визначати вузли, у властивості кластера NLB має бути включено функцію **Дозволити віддалений контроль**. Отримавши список доданих вузлів, можна видалити

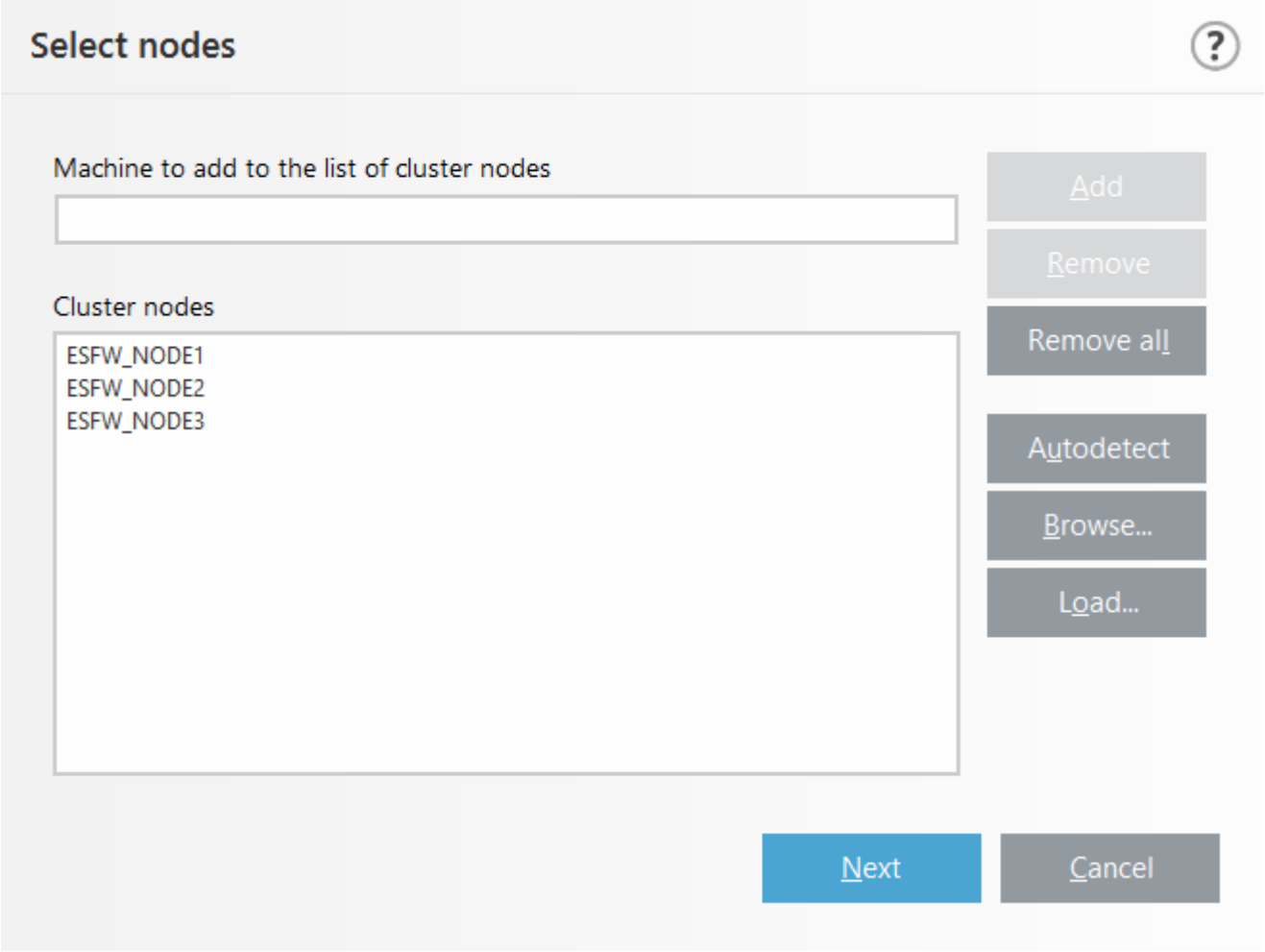
непотрібні вузли.

Огляд

Пошук і вибір комп'ютерів у межах Domain або Workgroup. Цей спосіб дає змогу додавати вузли до кластера ESET у ручному режимі. Крім того, щоб додати вузли, можна ввести ім'я відповідного хоста сервера й натиснути **Додати**.

Завантажити

Імпорт списку вузлів із файлу.



Щоб внести зміни до списку **вузлів кластера**, виберіть вузол, який потрібно видалити, і натисніть **Видалити**. Щоб повністю очистити список, натисніть **Видалити всі**.

Якщо кластер ESET уже використовується, нові вузли можна додати в будь-який момент. Для цього потрібно виконати дії, описані вище.

Усі вузли, що залишаються в списку, мають бути ввімкненими й доступними. За замовчуванням до списку вузлів кластера додано вузол Localhost.

Майстер кластера – налаштування кластера

Укажіть ім’я кластера й особливості мережі (за потреби).

Ім’я кластера

Введіть ім’я кластера й натисніть "Далі".

Порт прослуховування (порт за замовчуванням – 9777)

Якщо ви вже використовуєте порт 9777 у мережевому середовищі, укажіть інший номер порту, який не використовується.

Відкрити порт у брандмауері Windows

Якщо вибрано, у брандмауері Windows створюється правило.

Майстер кластера – налаштування параметрів кластера

Виберіть режим розповсюдження сертифікатів і вкажіть, чи потрібно інсталювати продукт на інші вузли.

Розповсюдження сертифікатів

- **Автоматичне віддалене** – сертифікат інсталюється автоматично.

- **Вручну** – натисніть **Створити** і виберіть відповідну папку для зберігання сертифікатів. Створюється кореневий сертифікат, а також сертифікат кожного вузла, зокрема той, з якого налаштовується кластер ESET (локальний комп’ютер). Щоб зареєструвати сертифікат на локальному комп’ютері, натисніть **Так**.

Інсталяція продукту на інші вузли

- **Автоматичне віддалене** – інсталяція ESET Mail Security на кожен вузол виконується автоматично (якщо операційна система вузла має однакову архітектуру).

- **Вручну** – інсталяція ESET Mail Security у ручному режимі (наприклад, якщо на деяких вузлах використовуються ОС з різною архітектурою).

Передати ліцензію на вузли без активованого продукту

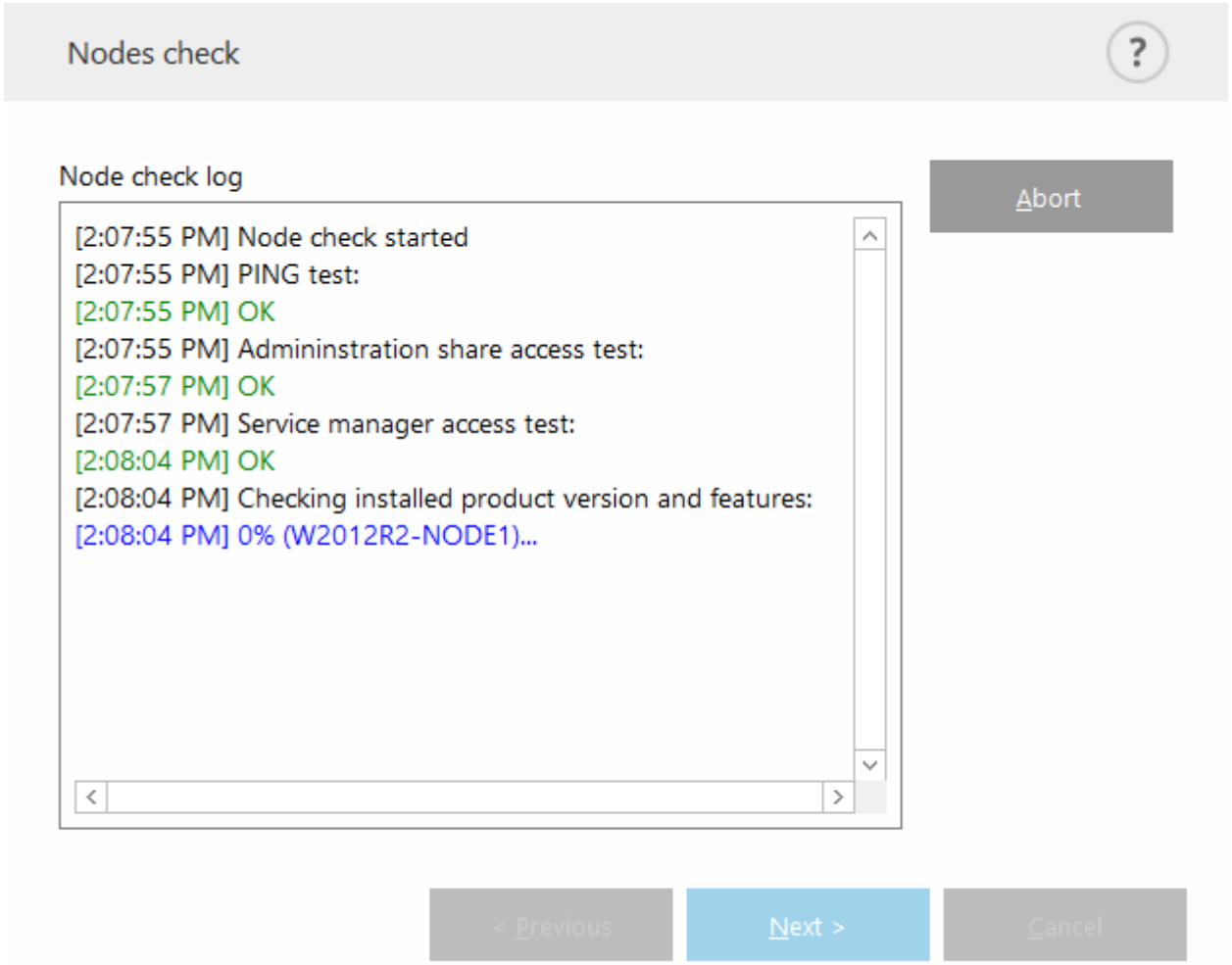
ESET Security автоматично активує рішення ESET, інстальовані на вузлах без ліцензій.

> Щоб створити кластер ESET у середовищах зі змішаними архітектурами операційних систем (32- і 64-розрядних), інсталюйте ESET Mail Security вручну. Операційні системи, що використовуються, визначаються на наступних етапах, і ця інформація відображається у вікні журналу.

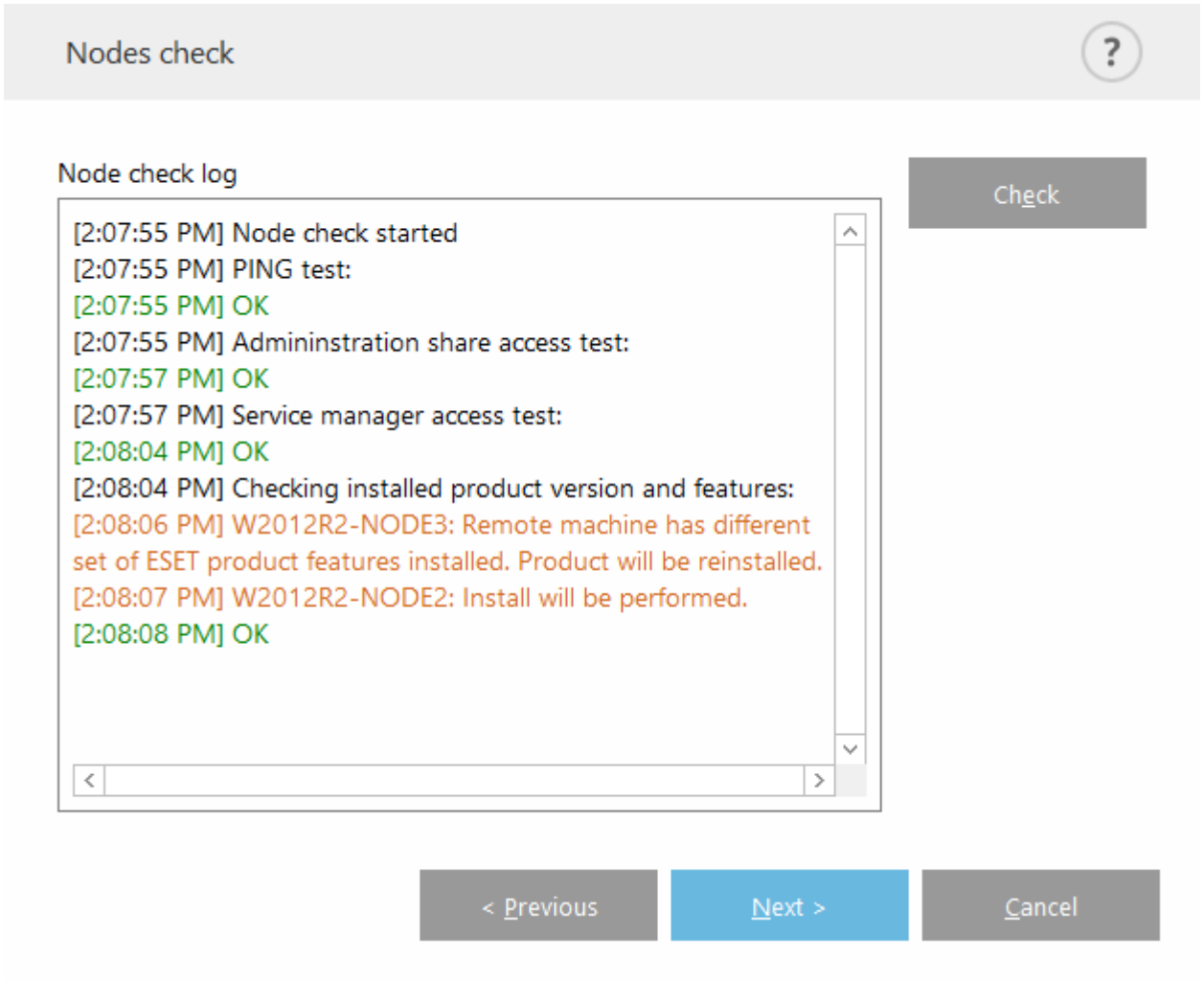
Майстер кластера – перевірка вузлів

Після визначення особливостей інсталяції виконується перевірка вузла. У **журналі перевірки вузлів** відображатиметься така інформація:

- перевірка роботи наявних вузлів;
- перевірка доступності нових вузлів;
- перевірка роботи вузла;
- перевірка доступності спільних ресурсів адміністратора;
- перевірка можливості віддаленого виконання;
- підтвердження правильності версії продукту (або того, що продукт не інстальовано);
- перевірка наявності нових сертифікатів.

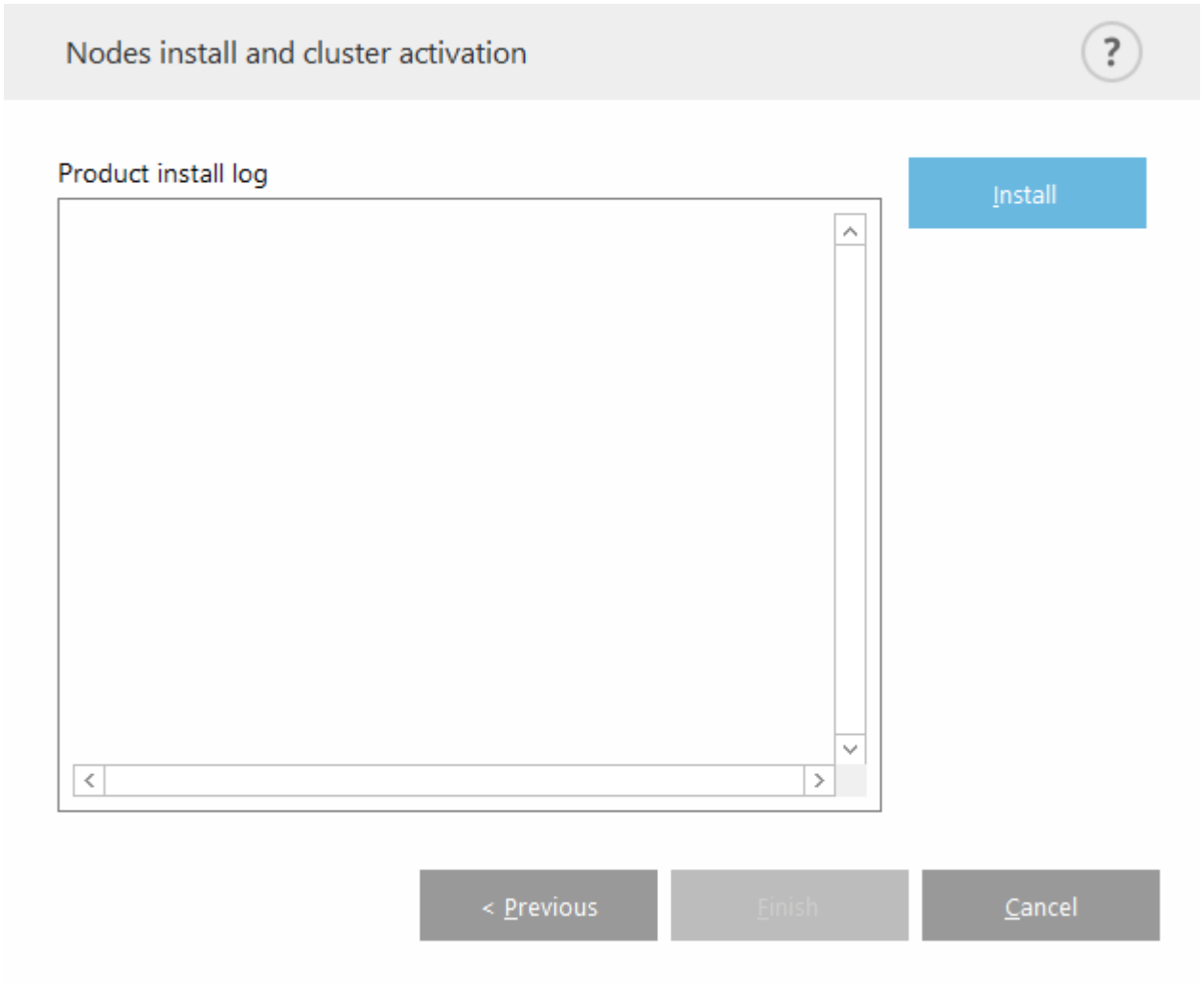


Після завершення перевірки вузла з’явиться звіт.

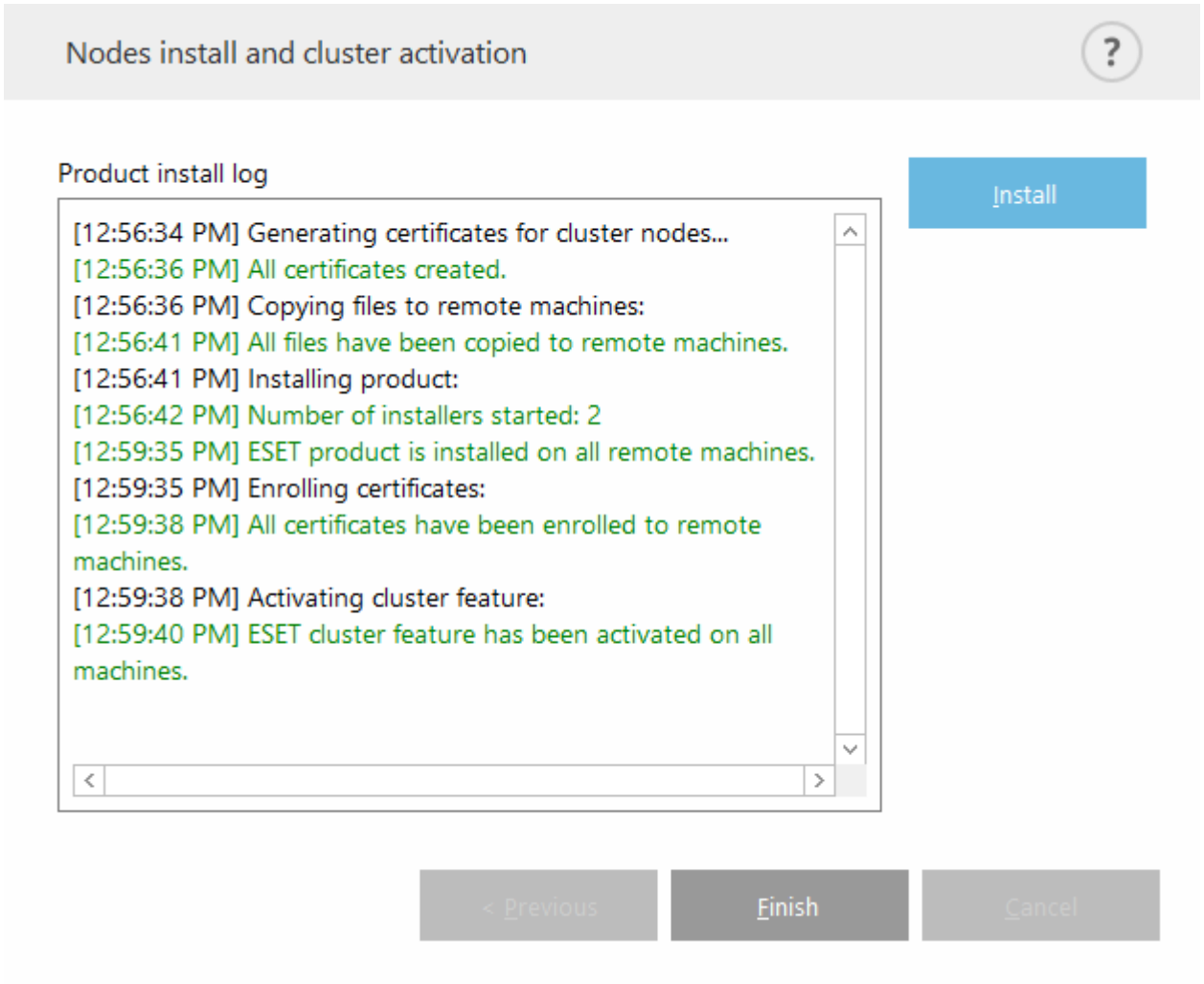


Майстер кластера – інсталяція вузлів

Якщо інсталяція виконується на віддаленому комп'ютері, під час ініціалізації кластера ESET майстер спробує знайти інсталяційний файл у каталозі *%ProgramData%\ESET\ESET Security\Installer*. Якщо файл інсталяції не знайдено в цьому каталозі, відображається запит на пошук його вручну.



Якщо виконується автоматична віддалена інсталяція на вузол з іншою архітектурою (конфлікт між 32- та 64-розрядною платформами), це буде виявлено, і для такого вузла буде запропоновано виконати інсталяцію вручну.



Після правильного налаштування кластера ESET він з'явиться на сторінці **Параметри** > **Сервер** як ввімкнений.

Якщо на деяких вузлах уже інстальовано стару версію ESET Mail Security, з'явиться повідомлення про те, що на ці комп'ютери необхідно інсталювати найновішу версію. Оновлення ESET Mail Security може призвести до автоматичного перезавантаження.

Крім того, поточний стан можна перевірити на сторінці статусу кластера (**Інструменти** > **Кластер**).

Оболонка ESET

eShell (скорочено від ESET Shell) – це інтерфейс командного рядка для ESET Mail Security. Він є альтернативою графічному інтерфейсу користувача. eShell містить усі функції й опції, які зазвичай забезпечує графічний інтерфейс користувача. eShell дає змогу налаштувати й адмініструвати всю програму без графічного інтерфейсу.

Окрім функцій, які доступні в графічному інтерфейсі користувача, продукт також дає можливість автоматизувати роботу за допомогою сценаріїв, які здійснюють налаштування, змінюють конфігурацію або виконують дії. Крім того, eShell може знадобитися тим, хто надає перевагу командному рядку, а не графічному інтерфейсу.

Для повноцінної роботи рекомендуємо запускати eShell у режимі адміністратора. Те ж саме стосується виконання однієї команди командного рядка Windows (cmd). Відкривати рядок слід у режимі **адміністратора**. В іншому разі ви не зможете запускати команди через брак потрібних дозволів.

eShell можна запускати у двох режимах.

1. **Інтерактивний режим** – цей режим корисний, коли в eShell потрібно виконувати різні завдання, наприклад змінювати конфігурацію та переглядати журнали, а не просто одну команду. Інтерактивний режим можна використовувати, якщо ви ще не знаєте всіх команд. В інтерактивному режимі легше орієнтуватися в інтерфейсі eShell. Ви також бачитимете доступні команди, які можна використовувати в певному контексті.

2. **Окрема команда / пакетний режим** – у цьому режимі можна виконати команду, не входячи в інтерактивний режим eShell. Це можна зробити з командного рядка Windows, ввівши відповідні параметри `eshell`.

```
eshell get status or eshell computer set real-time status disabled 1h
```

Щоб виконувати певні команди (зокрема, як у другому прикладі вище) у режимі пакетів/сценаріїв, спершу потрібно налаштувати кілька параметрів. В іншому разі з'явиться повідомлення **Доступ заборонено**. Це зроблено з міркувань безпеки.

Щоб користуватися командами eShell у командному рядку Windows, потрібно внести зміни в налаштування. Додаткові відомості про запуск пакетних файлів див. за цим посиланням.

Увійти в інтерактивний режим eShell можна двома способами:

1. Через **меню "Пуск" у Windows**: Пуск > Усі програми > ESET > ESET Mail Security > Оболонка ESET

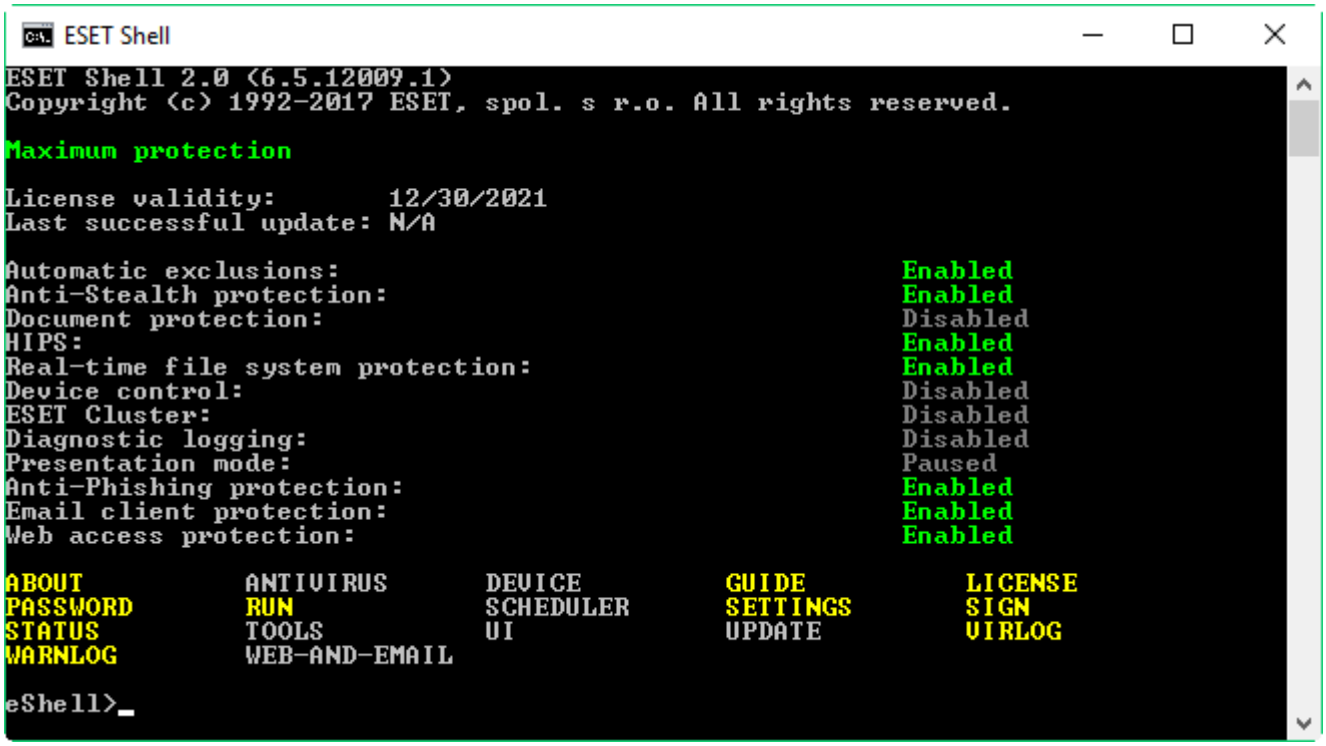
2. У **командному рядку Windows** введіть `eshell` і натисніть клавішу Enter.

Якщо з’являється помилка `'eshell' not recognized as an internal or external command`, це означає, що нові перемінні середовища не завантажуються системою після інсталяції ESET Mail Security.
Відкрийте новий командний рядок і запустіть eShell ще раз. Якщо ви все одно отримуєте помилку або ESET Mail Security інстальовано в базовій версії, почніть використовувати абсолютний шлях eShell, наприклад `"%PROGRAMFILES%\ESET\ESET Mail Security\eShell.exe"` (щоб команда працювала, необхідно додати `""`).

Під час першого запуску eShell в інтерактивному режимі користувач зможе ознайомитися з його особливостями за допомогою екранних підказок.

Щоб згодом ще раз переглянути підказки, введіть команду `guide`. Тут показано кілька основних прикладів використання eShell із синтаксисом, префіксом, шляхом команди, скороченими формами, псевдонімами тощо.

Під час наступного запуску eShell з’являться такий екран:



Команди не чутливі до регістру. Вони виконуватимуться, якщо ви використовуватимете літери як верхнього, так і нижнього регістрів.

Налаштування eShell

Ви можете налаштувати eShell в контексті `ui eshell`. Ви можете налаштувати псевдоніми, кольори, мову, політику виконання для сценаріїв, параметри для прихованих команд тощо.

Використання

Синтаксис

Щоб команди працювали належним чином, потрібно дотримуватися правильного синтаксису під час їх форматування. Структура команди може містити префікс, контекст, аргументи, параметри тощо. Нижче наведено загальний синтаксис, що використовується в інтерфейсі eShell.

[<prefix>] [<command path>] <command> [<arguments>]

Приклад (команда активує захист документів)
`SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

`SET` – префікс

`COMPUTER SCANS DOCUMENT` – шлях до певної команди, контекст, до якого належить ця команда

`REGISTER` – сама команда

`ENABLED` – аргумент для команди

Якщо використовувати `?` як аргумент для команди, відображатиметься синтаксис цієї

конкретної команди. Наприклад, `STATUS ?` показує синтаксис команди `STATUS`:

СИНТАКСИС:

```
[get] status
```

ОПЕРАЦІЇ:

`get` — Показати статус всіх модулів захисту

Як видно вище, конструкцію `[get]` взято у квадратні дужки. Це вказує на те, що префікс `get` використовується за замовчуванням для команди `status`. Це означає, що під час виконання команди `status` без зазначення префіксу використовуватиметься префікс за замовчуванням (у цьому разі – `get status`). Використання команд без префіксу дозволяє заощадити час на введення даних. Зазвичай `get` є префіксом за замовчуванням для більшості команд, але потрібно точно знати префікс за замовчуванням для певної команди й мати впевненість, що він відповідає завданню, яке необхідно виконати.

> **i** Команди не чутливі до регістру. Вони виконуватимуться, якщо ви використовуватимете літери як верхнього, так і нижнього регістрів.

Префікс/операція

Префікс – це операція. Префікс `GET` надає інформацію про те, як налаштовано певну функцію ESET Mail Security, або показує статус (наприклад, `GET COMPUTER REAL-TIME STATUS` покаже поточний статус захисту модуля в режимі реального часу). Префікс `SET` налаштовує функційність або змінює статус (`SET COMPUTER REAL-TIME STATUS ENABLED` активує захист у режимі реального часу).

Це префікси, які дає змогу використовувати eShell. Команда може підтримувати або не підтримувати будь-які із цих префіксів.

GET	повертає поточний параметр/статус
SET	задає значення/статус
SELECT	вибирає елемент
ADD	додає елемент
REMOVE	видаляє елемент
CLEAR	видаляє всі елементи/файли
START	запускає дію
STOP	зупиняє дію
PAUSE	призупиняє дію
RESUME	відновлює дію
RESTORE	відновлює стандартні параметри/об’єкт/файл
SEND	надсилає об’єкт/файл
IMPORT	імпортує з файлу
EXPORT	експортує у файл

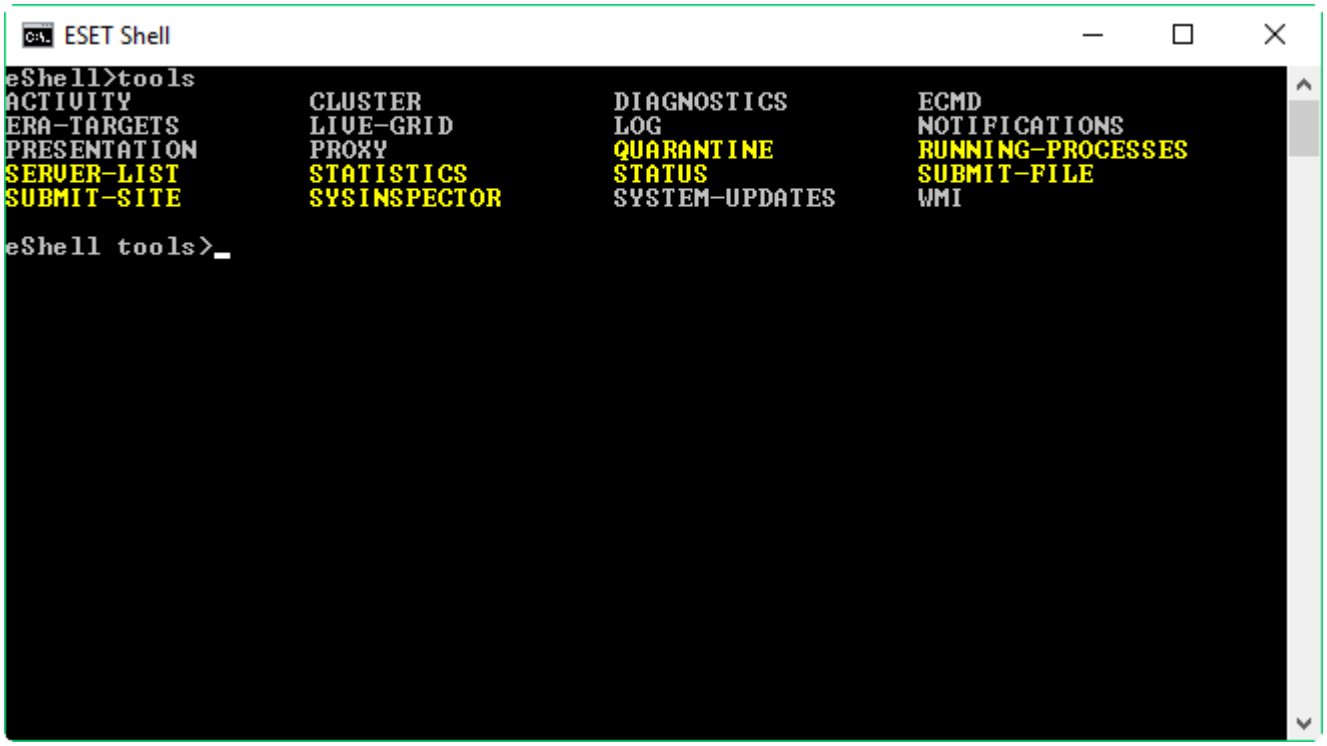
> **i** Префікси, як-от `GET` і `SET`, використовуються з багатьма командами, але в деяких командах (наприклад, `EXIT`) префікс не використовується.

Шлях команди й контекст

Команди розміщуються в контекстах, які утворюють деревовидну структуру. Верхній рівень деревовидної структури є кореневим. Під час запуску eShell відкривається саме кореневий рівень.

```
eShell>
```

Команди можна виконувати безпосередньо тут або вводити ім’я контексту, щоб переміщатися по деревовидній структурі. Наприклад, якщо ввести контекст `TOOLS`, з’явиться список усіх команд і доступні підпорядковані контексти.



Жовтим кольором позначено команди, які можна виконати, а сірим – підпорядковані контексти, у які можна ввійти. Підпорядкований контекст містить подальші команди.

Якщо потрібно повернутися на вищий рівень, використовуйте команду `..` (дві крапки).

> Скажімо, ви перебуваєте тут:
> `eShell computer real-time>`
> Введіть `..`, щоб перейти вгору на один рівень, а саме на цей:
> `eShell computer>`

Якщо потрібно повернутися на кореневий рівень із рівня `eShell computer real-time>` (який розташований на два рівні нижче за кореневий, просто введіть `.. ..` (дві крапки, пробіл і ще дві крапки). Таким чином ви перейдете на два рівні вгору, тобто до кореневого в цій ситуації. Щоб повернутися зразу на кореневий рівень із будь-якого рівня (незалежно від того, на якій глибині деревоподібної структури контекстів ви перебуваєте), використовуйте зворотну косу риску `\`. Якщо потрібно перейти до конкретного контексту на верхніх рівнях, використайте відповідну кількість команд `..` для переходу на потрібний рівень, а як роздільник використовуйте пробіл. Наприклад, якщо потрібно піднятися на три рівні вгору, введіть `.. .. ..`

Шлях указується відносно поточного контексту. Якщо команда міститься в поточному

контексті, шлях вводити не потрібно. Наприклад, щоб виконати команду `GET COMPUTER REAL-TIME STATUS`, введіть:

`GET COMPUTER STATUS` – якщо ви перебуваєте в кореневому контексті (командний рядок показує `eShell>`)

`GET STATUS` – якщо ви перебуваєте в контексті `COMPUTER` (командний рядок показує `eShell computer>`)

`.. GET STATUS` – якщо ви перебуваєте в контексті `COMPUTER REAL-TIME` (командний рядок показує `eShell computer real-time>`)

Можна використовувати одну `.` (крапку) замість двох `..`, оскільки одна крапка є скороченням для двох.

✔ `. GET STATUS` – якщо ви перебуваєте в контексті `COMPUTER REAL-TIME` (командний рядок показує `eShell computer real-time>`)

Аргумент

Аргумент — це дія, яка виконується для певної команди. Наприклад, команду `CLEAN-LEVEL` (розташовується в `COMPUTER REAL-TIME ENGINE`) можна використовувати з наведеними нижче аргументами.

`rigorous` — Завжди виправляти виявлені об’єкти

`safe` — Виправляти виявлений об’єкт, якщо він безпечний, а в іншому разі – залишати

`normal` — Виправляти виявлений об’єкт, якщо він безпечний, а в іншому разі – запитувати

`none` – завжди запитувати кінцевого користувача

Інший приклад: аргументи `ENABLED` або `DISABLED`, які дають змогу ввімкнути або вимкнуто певну функцію.

Скорочена форма й короткі команди

eShell дає змогу скоротити контексти, команди й аргументи (якщо аргумент є перемикачем або альтернативним варіантом). Не можна скоротити префікс або аргумент із конкретними значеннями, як-от цифра, ім’я або шлях. Замість аргументів увімкнення та вимкнення можна натомість використовувати цифри `1` і `0`.

✔
```
computer set real-time status enabled        =>        com set real stat 1
computer set real-time status disabled        =>        com set real stat 0
```

Приклади короткої форми

✔
```
computer set real-time status enabled        =>        com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext        =>        com excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1        =>        com excl rem det 1
```

Якщо дві команди або контексти починаються з однакових літер (наприклад, `ADVANCED` і `AUTO-EXCLUSIONS`, і ви вводите `A` як скорочений контекст), eShell не зможе визначити, який із двох контекстів потрібно ввести. З’явиться повідомлення про помилку та список команд, що

починаються з літери "A", з якого можна вибрати потрібний варіант:

```
eShell>a
```

Наведена нижче команда не є унікальною: `a`

У контексті `COMPUTER` доступні такі підпорядковані контексти:

```
ADVANCED
```

```
AUTO-EXCLUSIONS
```

Якщо додати одну або кілька літер (наприклад, `AD` замість лише `A`), eShell введе підпорядкований контекст `ADVANCED`, оскільки тепер він є унікальним. Те саме стосується скорочених команд.

> **i** Щоб команда виконувалася належним чином, радимо не скорочувати команди, аргументи тощо, а використовувати їх повну форму. У такому разі eShell виконуватиме саме те, що потрібно, і вдасться запобігти небажаним помилкам. Особливо це стосується пакетних файлів і сценаріїв.

Автозаповнення

Ця нова функція представлена в eShell 2.0 і дуже схожа на функцію автозаповнення в командному рядку Windows. У командному рядку Windows заповнюються шляхи до файлів, а в eShell – команди, контекст та імена операцій. Заповнення аргументів не підтримується.

Щоб під час введення команди виконати автозаповнення або переглянути доступні варіанти, натисніть клавішу Tab.

Щоб перегорнути варіанти назад, натисніть SHIFT + Tab. Одночасне використання скороченої форми й автозаповнення не підтримується. Використовуйте одне з двох.

Наприклад, якщо ввести `computer real-time additional` і натиснути Tab, нічого не відбудеться. Натомість введіть `com` і натисніть Tab, щоб заповнити `computer`. Після цього введіть `real` + Tab, `add` + Tab і натисніть клавішу Enter. Введіть `on` + Tab і продовжуйте натискати Tab, щоб переглядати доступні варіанти: `on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default` тощо.

Псевдоніми

Псевдонім – це альтернативна назва, яку можна використовувати для виконання команди (якщо команді призначено псевдонім). Є кілька псевдонімів за замовчуванням:

`(global) close` — Вийти

`(global) quit` — Вийти

`(global) bye` — Вийти

`warnlog` – події журналу інструментів

`virlog` – виявлення журналу інструментів

(global) означає, що команду можна використовувати будь-де незалежно від поточного контексту. Одній команді може бути призначено кілька псевдонімів. Наприклад, команда EXIT має псевдоніми CLOSE, QUIT і BYE. Щоб вийти з eShell, можна скористатися самою командою EXIT або будь-яким із її псевдонімів.

Псевдонім VIRLOG є псевдонімом для команди DETECTIONS, розташованої в контексті TOOLS LOG. Таким чином, команда DETECTIONS доступна в контексті ROOT, що спрощує доступ до неї (не потрібно вводити TOOLS, а потім підпорядкований контекст LOG і виконувати її безпосередньо в ROOT).

eShell дають змогу визначати свої псевдоніми. Команду ALIAS можна знайти в контексті UI ESHELL.

Захищені паролем параметри

Параметри ESET Mail Security можна захистити паролем. Можна встановити пароль за допомогою графічного інтерфейсу або оболонки eShell, використовуючи команду set ui access lock-password.

Для певних команд (наприклад тих, що змінюють параметри або дані) цей пароль потрібно буде вводити в інтерактивному режимі. Якщо ви плануєте працювати в eShell протягом тривалого періоду й не хочете постійно вводити пароль, eShell може запам'ятати його. Для цього скористайтеся командою set password (виконується з root). Після цього пароль вводитиметься автоматично під час кожного виконання команди, для якої він потрібен. Програма eShell пам'ятає пароль, доки ви не вийдете з неї. Тобто після запуску нового сеансу потрібно буде знову скористатися командою set password (якщо потрібно, щоб програма eShell запам'ятала пароль).

Посібник і довідка

Під час виконання команди GUIDE або HELP на екрані з'являється вікно першого запуску, у якому пояснюється, як користуватись eShell. Ця команда доступна лише в контексті ROOT (eShell>).

Історія команд

eShell зберігає журнал виконаних раніше команд. Це поширюється лише на поточний інтерактивний сеанс eShell. Після виходу з eShell журнал команд видаляється. Використовуйте клавіші зі стрілками вгору та вниз на клавіатурі, щоб переміщатися історією. Знайшовши потрібну команду, можна виконати її ще раз або внести в неї зміни (для цього не потрібно вводити наново всю команду повністю).

CLS/очищення екрана

Команду CLS можна використовувати, щоб очистити екран. Вона працює так само, як і в командному рядку Windows або інших схожих інтерфейсах командного рядка.

EXIT/CLOSE/QUIT/BYE

Щоб закрити eShell або вийти з цього інтерфейсу, можна скористатися будь-якою із цих команд: EXIT, CLOSE, BYE або QUIT.

Команди

У цьому розділі наведено кілька основних команд оболонки eShell з описами.

> **i** Команди не чутливі до регістру. Вони виконуватимуться, якщо ви використовуватимете літери як верхнього, так і нижнього регістрів.

Приклади команд (містяться в контексті `ROOT`):

ПРО ПРОГРАМУ

Показує інформацію про програму. Відображається така інформація:

- Назва інстальованого продукту з безпеки ESET і номер його версії.
- Операційна система й основні відомості про обладнання.
- Ім’я користувача (включно з доменом), повне ім’я комп’ютера (FQDN, якщо ваш сервер входить у домен), а також ім’я робочого місця.
- Інстальовані компоненти продукту з безпеки ESET разом із номерами версій кожного компонента.

ШЛЯХ ДО КОНТЕКСТУ:

```
root
```

ПАРОЛЬ

З міркувань безпеки, щоб виконати команди, захищені паролем, потрібно ввести пароль. Це стосується команд, які вимикають захист і можуть впливати на конфігурацію ESET Mail Security. Щоразу, коли ви виконуватимете таку команду, відображатиметься запит на введення пароля. Цей пароль можна задати, щоб не вводити щоразу. eShell його запам’ятає й автоматично вводитиме, коли виконуватиметься команда, захищена паролем.

> **i** Пароль працює лише для поточного інтерактивного сеансу eShell. Заданий пароль буде видалено після виходу з eShell. Під час повторного запуску eShell пароль потрібно задати знову.

Заданий пароль також можна використовувати під час запуску непідписаних пакетних файлів або сценаріїв. Під час запуску непідписаних пакетних файлів переконайтеся, що для політики виконання оболонки ESET установлено повний доступ. Нижче наведено приклад такого пакетного файлу:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Наведена вище об’єднана команда задає пароль і вимикає захист.

> Рекомендуємо використовувати підписані пакетні файли завжди, коли це можливо. Таким чином, ви уникнете звичайних текстових паролів у пакетному файлі (якщо використовується описаний вище метод). Щоб дізнатися більше, перегляньте статтю Пакетні файли / сценарії (розділ "Підписані пакетні файли").

ШЛЯХ ДО КОНТЕКСТУ:

`root`

СИНТАКСИС:

`[get] | restore password`

`set password [plain <password>]`

ОПЕРАЦІЇ:

`get` — Показати пароль

`set` — Задає або скидає пароль

`restore` — Очищує пароль

АРГУМЕНТИ:

`plain` – Вмикає режим введення пароля як параметра

`password` — Пароль

> ✔ `set password plain <yourpassword>` – Установлює пароль для команд, захищених паролем.
> `restore password` — Очищує пароль

> ✔ `get password` – Показує, чи налаштовано пароль (показуються лише зірочки `"*"`, а не сам пароль). Якщо зірочки не відображаються, це означає, що пароль не задано.
> `set password plain <yourpassword>` – Установлює заданий пароль.
> `restore password` – Очищує заданий пароль.

СТАТУС

Показує інформацію про поточний стан захисту ESET Mail Security в режимі реального часу, а також дає змогу призупиняти або відновлювати захист (як у головному вікні програми).

ШЛЯХ ДО КОНТЕКСТУ:

`computer real-time`

СИНТАКСИС:

`[get] status`

`set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]`

`restore status`

ОПЕРАЦІЇ:

`get` — Повертає поточний параметр/статус

`set` — Задає значення/статус

`restore` — Відновлює стандартні параметри/об’єкт/файл

АРГУМЕНТИ:

`enabled` — Увімкнути захист/функцію

`disabled` — Вимкнути захист/функцію

`10m` — Вимкнути на 10 хвилин

`30m` — Вимкнути на 30 хвилин

`1h` — Вимкнути на 1 годину

`4h` — Вимкнути на 4 години

`temporary` – Вимкнути до перезавантаження

> Не можна вимкнути всі функції захисту однією командою. За допомогою команди `status` функціями захисту й модулями можна керувати по черзі. Кожна функція захисту або модуль має власну команду `status`.

Список функцій із командою `status`:

Функція	Контекст і команда
Автоматичні виключення	`COMPUTER AUTO-EXCLUSIONS STATUS`
Система запобігання вторгненням (HIPS)	`COMPUTER HIPS STATUS`
Захист файлової системи в режимі реального часу	`COMPUTER REAL-TIME STATUS`
Контроль пристроїв	`DEVICE STATUS`
Захист від ботнетів	`NETWORK ADVANCED STATUS-BOTNET`
Захист від мережевих атак (IDS)	`NETWORK ADVANCED STATUS-IDS`
Ізоляція мережі	`NETWORK ADVANCED STATUS-ISOLATION`
Кластер ESET	`TOOLS CLUSTER STATUS`
Журналювання даних діагностики	`TOOLS DIAGNOSTICS STATUS`
Режим презентації	`TOOLS PRESENTATION STATUS`
Захист від фішинг-атак	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Захист поштового клієнта	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Захист доступу до Інтернету	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Це псевдонім команди `DETECTIONS`. Він знадобиться, коли потрібно переглянути інформацію про виявлені загрози.

WARNLOG

Це псевдонім команди `EVENTS`. Він знадобиться, коли потрібно переглянути інформацію про різні події.

Сполучення клавіш

eShell підтримує сполучення клавіш (подібно до командного рядка Microsoft Windows *cmd.exe*). Використовуйте певні клавіші (комбінації клавіш) на клавіатурі для виконання дій у eShell. Наприклад, показати історію команд, повторити частину команд з історії, перемістити слово або стерти рядок.

Доступні такі сполучення клавіш:

F1: друк символів команди фактичної історії по одному.

F2, X: заново виконати частину команд з історії до символу X.

F3: записати фактичний вивід історії команд.

F4, X: видалити історію команд від поточного положення курсора до символу X.

F5: ідентично СТРІЛЦІ ВГОРУ.

F7: показати історію команд.

ALT + F7: очистити історію команд.

F8: переміщення назад історією команд; відображатимуться лише команди, які відповідають поточному тексту в командному рядку.

F9: запуск певної команди з історії команд.

СТРІЛКА ВПРАВО: те ж саме, що і F1.

CTRL + HOME: стирання рядка вліво.

CTRL + END: стирання рядка вправо.

CTRL + СТРІЛКА ВЛІВО: переміщення на одне слово вліво.

CTRL + СТРІЛКА ВПРАВО: переміщення на одне слово вправо.

Пакетні файли / сценарії

Ви можете використовувати eShell як потужний інструмент створення сценаріїв для автоматизації. Щоб використовувати пакетний файл з eShell, створіть його за допомогою команди в eShell.

Також підтримуються послідовності команд. Наприклад, якщо ви хочете ввести певне заплановане завдання, введіть такі команди:

```
eshell select scheduler task 4 "&" get scheduler action
```

Вибір елемента (у цьому разі завдання 4) зазвичай застосовується лише до поточного екземпляра eShell. Якщо виконати ці дві команди одна за одною, друга завершиться помилкою ""No task selected or selected task no longer exists"".

З міркувань безпеки за замовчуванням для політики виконання вибрано параметр **Обмежене використання сценаріїв**. Він дозволяє використовувати eShell як інструмент моніторингу, але не дає вносити зміни в конфігурацію ESET Mail Security за допомогою сценаріїв. Якщо спробувати виконати сценарій із командами, які можуть вплинути на безпеку, наприклад вимкнути захист, з'явиться повідомлення **Доступ заборонено**. Рекомендуємо використовувати підписані пакетні файли для виконання команд, які вносять зміни в конфігурацію.

Щоб змінити конфігурацію за допомогою однієї команди, що вводиться вручну в командному рядку Windows, необхідно надати повний доступ для eShell (не рекомендовано). Щоб надати повний доступ, застосуйте `ui eshell shell-execution-policy` в інтерактивному режимі eShell або головному вікні програми в розділі **Додаткові параметри** (**F5**) > **Інтерфейс користувача** > ESET Shell.

Підписані пакетні файли

eShell дає змогу захистити загальні пакетні файли (**.bat*) за допомогою підпису. Сценарії підписуються тим самим паролем, який використовується для захисту налаштувань. Щоб підписати сценарій, спершу потрібно ввімкнути захист налаштувань. Це можна зробити в головному вікні програми або в eShell за допомогою команди `set ui access lock-password`. Після налаштування пароля захисту можна почати підписувати пакетні файли.

> **i** Якщо змінено пароль захисту налаштувань, потрібно заново підписати всі сценарії. В іншому випадку сценарії завершаться помилкою під час виконання наступної зміни пароля. Пароль, введений під час підписання сценарію, має збігатися з паролем захисту параметрів у цільовій системі.

Щоб підписати пакетний файл, запустіть `sign <script.bat>` у кореневому контексті eShell, де *script.bat* – шлях до сценарію, який потрібно підписати. Введіть і підтвердьте пароль, який використовуватиметься для підписання. Цей пароль має збігатися з паролем для захисту параметрів. Підпис розміщується в кінці пакетного файлу як коментар. Якщо цей сценарій уже підписано, підпис буде замінено на новий.

> **i** Якщо ви змінюєте раніше підписаний пакетний файл, його потрібно підписати ще раз.

Щоб виконати підписаний пакетний файл із командного рядка Windows або як заплановане завдання, виконайте таку команду:

```
eshell run <script.bat>
```

Де *script.bat* – це шлях до пакетного файлу.

```
eshell run d:\myeshellscript.bat
```

ESET LiveGuard Advanced

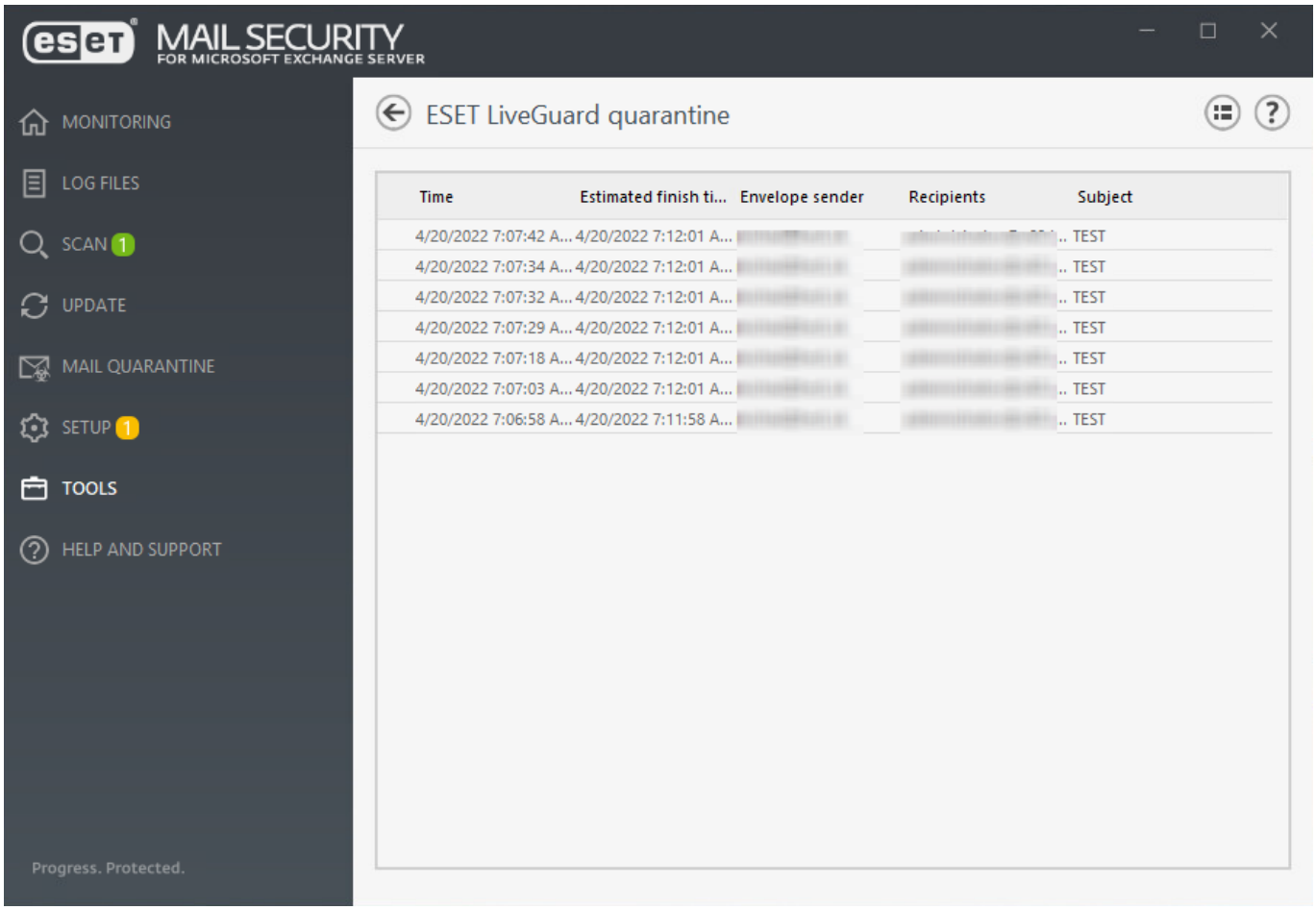
ESET LiveGuard Advanced забезпечує додатковий рівень безпеки завдяки використанню розширеної хмарної технології ESET для виявлення нових загроз, які не були відомі раніше. ESET

LiveGuard Advanced – платна служба, подібна до ESET LiveGrid®, але з перевагами захисту від можливих наслідків, спричинених новими загрозами. Якщо ESET LiveGuard Advanced виявить підозрілий код або поведінку, підозрілі об'єкти тимчасово перенесуться до карантину ESET LiveGuard Advanced, тож загрозу буде відразу ізольовано.

Підозрілий зразок (файл або електронний лист) автоматично надсилається в хмару ESET, де сервер ESET LiveGuard Advanced аналізує зразок із використанням найсучасніших ядер виявлення шкідливого програмного забезпечення. Поки файли або електронні листи заблоковані в карантині ESET LiveGuard Advanced, ESET Mail Security очікує на результати від сервера ESET LiveGuard Advanced.

Після завершення аналізу ESET Mail Security отримає звіт зі зведеною інформацією про поведінку зразка. Якщо зразок виявиться нешкідливим, його буде розблоковано з карантину ESET LiveGuard Advanced. В іншому разі він залишиться в карантині. Якщо блокування було помилковим і ви впевнені, що файл або електронний лист не становить загрозу, його можна вручну розблокувати з карантину ESET LiveGuard Advanced, перш ніж ESET Mail Security отримає результати сервера ESET LiveGuard Advanced.

Результати аналізу зразків від ESET LiveGuard Advanced зазвичай надсилаються протягом кількох хвилин (для електронних листів). Проте тривалість інтервалу очікування за замовчуванням становить 5 хвилин. У поодиноких випадках, коли результати від ESET LiveGuard Advanced не надходять протягом цього інтервалу, з'являється відповідне повідомлення. Можна змінити інтервал на власний розсуд (задати значення від 5 до 60 хвилин із кроком в 1 хвилину).



Функція ESET LiveGuard Advanced видима в ESET Mail Security незалежно від статусу активації. Якщо у вас немає ліцензії, функція ESET LiveGuard Advanced буде неактивною. Ліцензією ESET LiveGuard

Advanced керує ESET PROTECT, а саму активацію слід виконати з ESET PROTECT за допомогою політики.

Після активації ESET LiveGuard Advanced на сервері ESET LiveGuard Advanced буде створено ваш власний профіль ESET LiveGuard Advanced. Цей профіль зберігатиме всі результати аналізу зразків ESET LiveGuard Advanced, надісланих вашим ESET Mail Security.

Щоб функція ESET LiveGuard Advanced працювала, мають виконуватися такі умови:

ESET Mail Security керується за допомогою ESET PROTECT

ESET Mail Security активовано за допомогою ліцензії ESET LiveGuard Advanced

Функцію ESET LiveGuard Advanced увімкнено в ESET Mail Security за допомогою політики ESET PROTECT

Після цього ви зможете скористатися всіма перевагами ESET LiveGuard Advanced, а також вручну надсилати файл зразка на аналіз ESET LiveGuard Advanced.

ESET SysInspector

ESET SysInspector – це програма, яка ретельно перевіряє комп'ютер і збирає докладну інформацію про системні компоненти, зокрема інстальовані драйвери й програми, мережеві підключення або важливі розділи реєстру, а також оцінює рівень ризику для кожного компонента.

Ця інформація корисна, коли потрібно визначити причину підозрілої поведінки системи, яка може бути спричинена несумісністю програмного забезпечення або обладнання чи зараженням шкідливим програмним забезпеченням.

Натисніть **Створити** та введіть короткий **коментар**, що описує журнал, який створюється. Дочекайтеся, доки створиться журнал ESET SysInspector (буде показано статус "Створено"). Створення журналу може тривати певний час, залежно від конфігурації обладнання та системних даних.

У вікні ESET SysInspector відображається вказана нижче інформація про створені журнали.

- **Час**. Час створення журналу.
- **Коментар**. Короткий коментар.
- **Користувач**. Ім'я користувача, який створив журнал.
- **Статус**. Статус створення журналу.

Можливі вказані нижче дії.

- **Показати**. Відкриття створеного журналу. Також можна натиснути журнал правою кнопкою миші й вибрати **"Показати"** в контекстному меню.
- **Створити**. Створення нового журналу. Введіть короткий коментар з описом журналу, який потрібно створити, і натисніть **Створити**. Дочекайтеся, доки завершиться створення журналу ESET SysInspector (буде показано **статус** "Створено").

• **Видалити**. Видалення вибраних журналів зі списку.

Якщо натиснути один або кілька вибраних журналів правою кнопкою миші, у контекстному меню будуть доступні наведені нижче опції.

• **Показати**. Відкриття вибраного журналу ESET SysInspector (аналогічно подвійному натисканню журналу).

• **Створити**. Створення нового журналу. Введіть короткий коментар з описом журналу, який потрібно створити, і натисніть **Створити**. Дочекайтеся, доки завершиться створення журналу ESET SysInspector (буде показано **статус** "Створено").

• **Видалити**. Видалення вибраних журналів зі списку.

• **Видалити все**. Видалення всіх журналів.

• **Експорт**: експортувати журнал у файл *.esil*. Можна вибрати файл *.xml* або ZIP-архів файлу *.xml*.

ESET SysRescue Live

ESET SysRescue Live – це безоплатна утиліта, яка дає можливість створити завантажувальний CD/DVD або USB-диск. Користувач може завантажити систему інфікованого комп'ютера за допомогою такого носія, просканувати його на наявність шкідливого програмного забезпечення й очистити заражені файли.

Головна перевага ESET SysRescue Live полягає в тому, що рішення ESET Security виконується незалежно від операційної системи хоста, але має прямий доступ до диска й файлової системи. Це дозволяє впоратися із загрозами, які у звичайних умовах усунути неможливо (наприклад, у разі запущеної операційної системи тощо).

Розклад

Розклад керує запланованими завданнями й запускає їх відповідно до визначених параметрів. Список усіх запланованих завдань можна переглянути як таблицю, у якій указано їхні параметри, наприклад тип і назва завдання, час запуску й час останнього виконання. Ви також можете створювати нові заплановані завдання, натиснувши Додати завдання. Щоб редагувати конфігурацію наявного запланованого завдання, натисніть кнопку **Редагувати**. Щоб відновити налаштування за замовчуванням для списку запланованих завдань, натисніть **За замовчуванням** і виберіть **Відновити параметри за замовчуванням**. Усі внесені зміни буде втрачено. Цю дію не можна скасувати.

Є набір попередньо заданих за замовчуванням завдань.

• Обслуговування журналу

• Регулярне автоматичне оновлення (використовуйте це завдання для оновлення частоти)

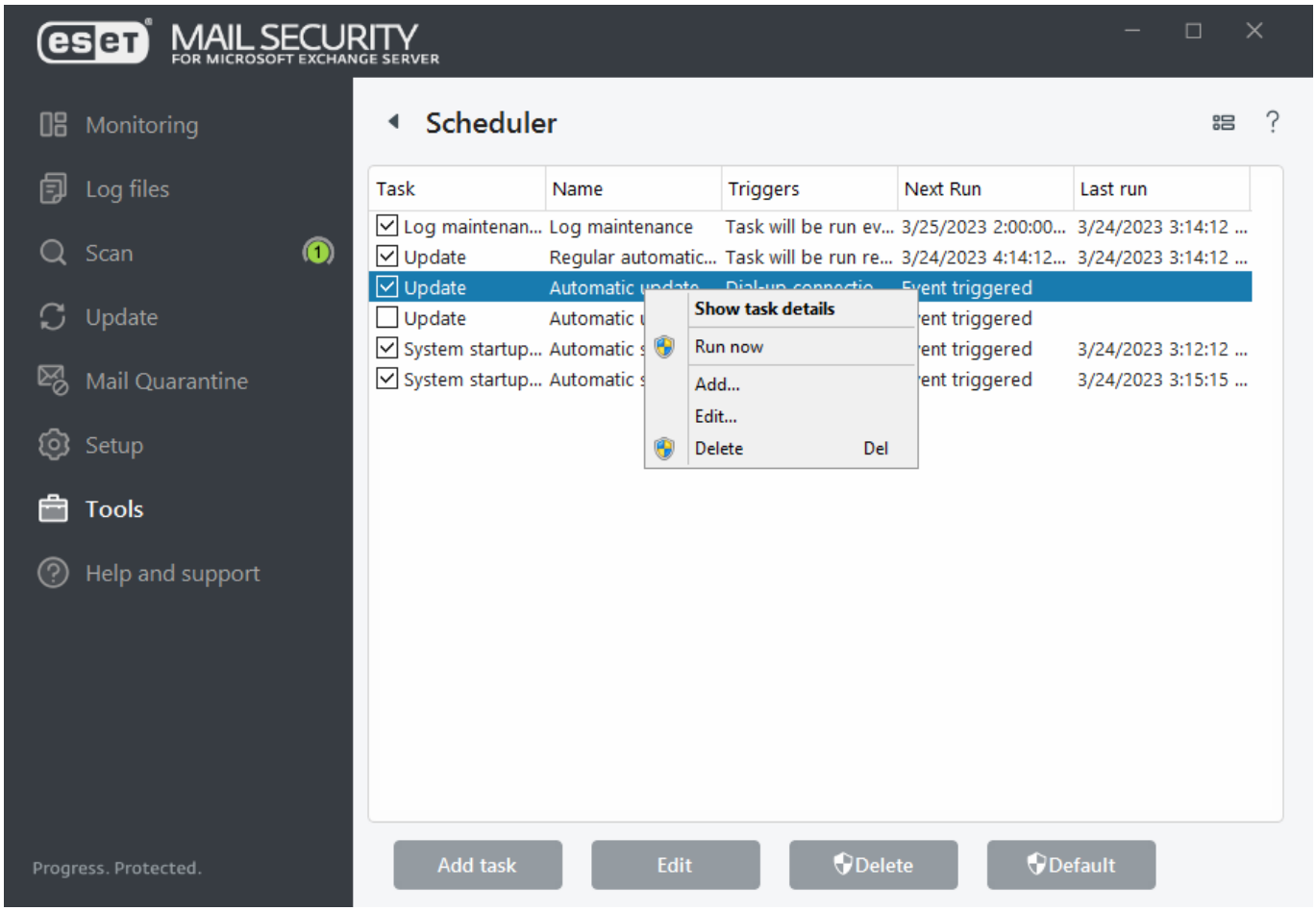
• Автоматичне оновлення після установки модемного підключення

• 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 оновлення модулів)

Установіть відповідні прапорці, щоб активувати або деактивувати завдання.



Щоб виконати наведені нижче дії, натисніть завдання правою кнопкою миші.

Показати деталі задачі	Відображає докладну інформацію про заплановане завдання, якщо його двічі клацнути або натиснути правою кнопкою миші.
Запустити	Запуск вибраного запланованого завдання і його негайне виконання.
Додати...	Запуск майстра, який допоможе створити нове завдання розкладу.
Редагувати...	Редагування конфігурації наявного запланованого завдання (як за замовчуванням, так і користувацького).
Видалити	Видалення наявного завдання.

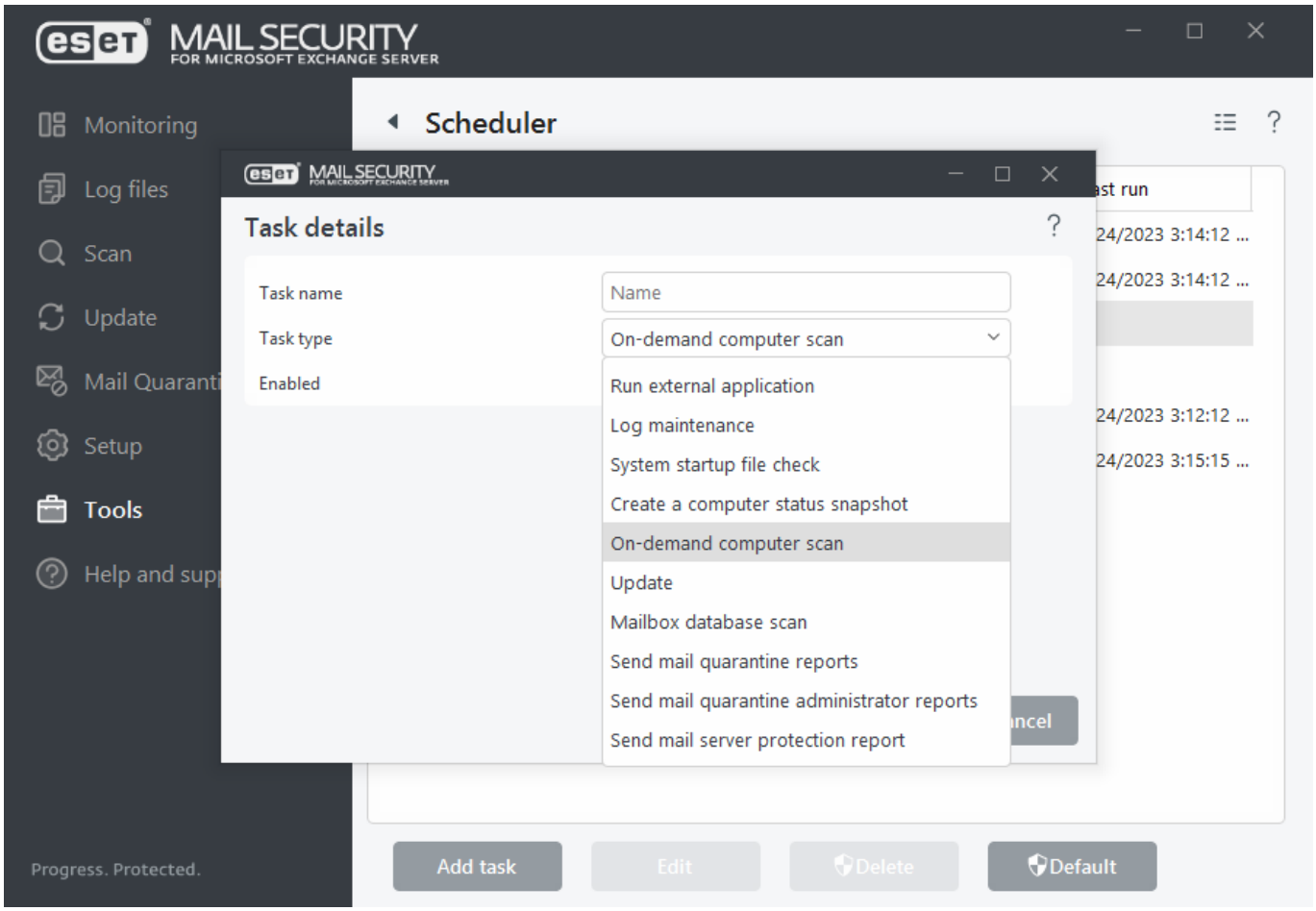
Розклад – Додати завдання

Щоб створити нове заплановане завдання, виконайте дії нижче.

1. Натисніть **Додати завдання**.

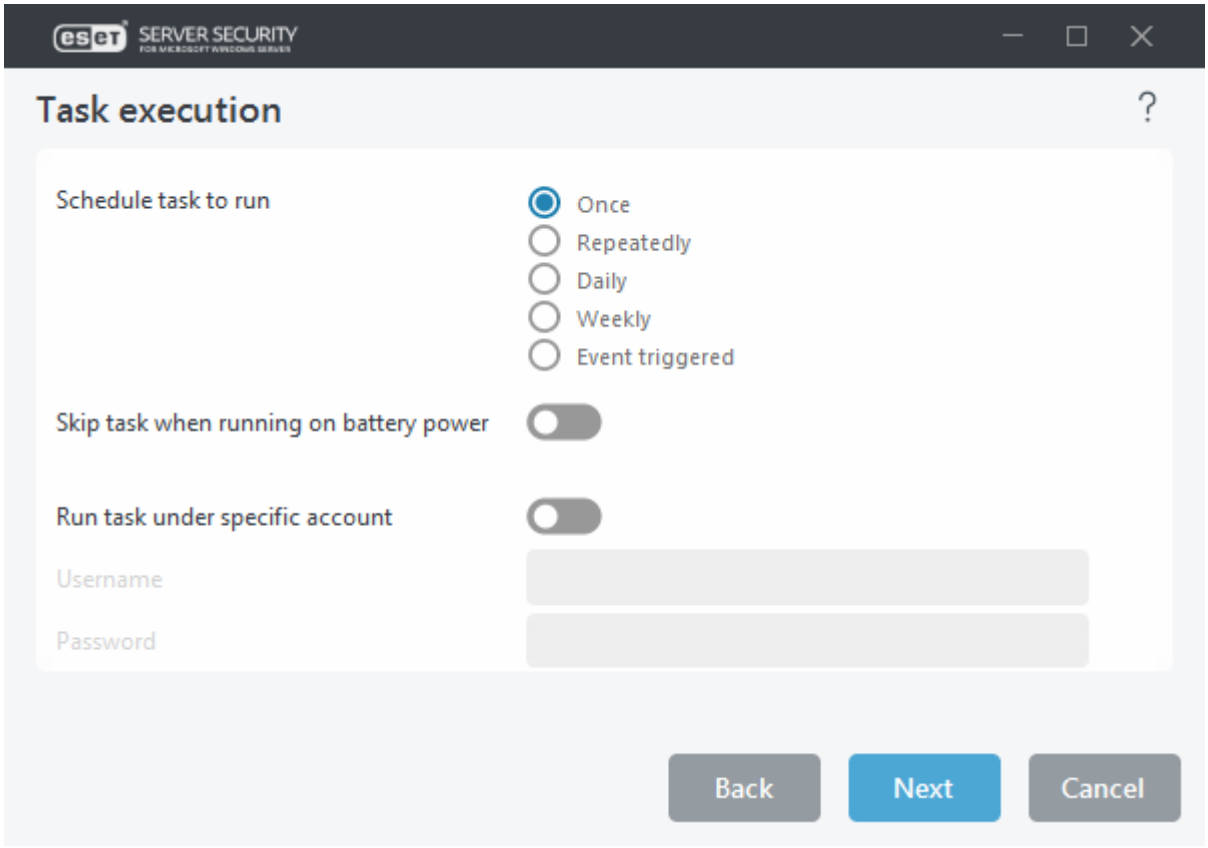
2. Введіть **назву завдання** та налаштуйте заплановане завдання.

3. Тип завдання. Виберіть відповідний **тип завдання** в розкривному меню.

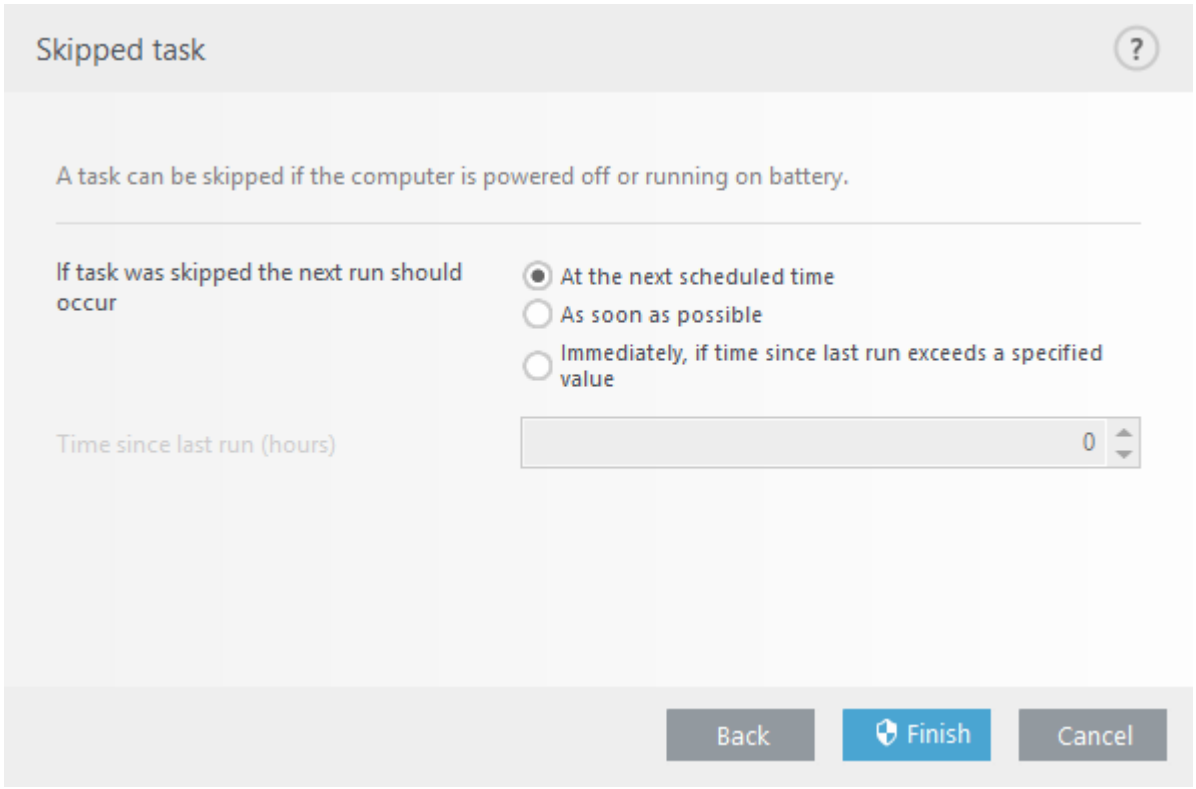


Щоб деактивувати завдання, натисніть повзунок поруч із пунктом **Увімкнено**. Щоб активувати завдання пізніше, установіть прапорець у поданні розкладу.

4. Запуск завдання. Щоб визначити, коли потрібно запустити завдання, виберіть один із варіантів. Залежно від зробленого вибору вам буде запропоновано вибрати певний час, день, інтервал або подію.



5. Пропущене завдання. Якщо завдання не вдалося запустити в попередньо визначений час, можна вказати, коли потрібно здійснити наступну спробу виконання.



6. Запустити програму. Якщо в завданні заплановано запускати зовнішню програму, виберіть виконуваний файл у дереві каталогів.

7. Якщо потрібно внести зміни, натисніть **Назад**, щоб повернутися до попередніх кроків і змінити параметри.

8. Щоб створити завдання або застосувати зміни, натисніть **Готово**.

Нове заплановане завдання з'явиться в поданні розкладу.

Тип завдання

Майстер конфігурації відрізняється для кожного типу запланованого завдання. Введіть **назву завдання** та виберіть потрібний **тип завдання** в розкривному меню.

• **Запуск зовнішньої програми**. Планування виконання зовнішньої програми. Ви можете використовувати певний обліковий запис для запуску запланованого завдання (параметр Запуск завдання під певним обліковим записом).

• **Обслуговування журналів**. Файли журналу також містять залишки видалених записів. Це завдання регулярно оптимізує записи у файлах журналу для ефективної роботи.

• **Перевірка файлів під час запуску системи**. Перевірка файлів, виконання яких дозволено під час запуску системи або входу в систему.

• **Створити знімок стану комп'ютера**. Створення знімка стану комп'ютера в ESET SysInspector, для якого збирається докладна інформація про компоненти системи (наприклад, драйвери, програми) та оцінюється рівень ризику для кожного з них.

• **Сканування комп'ютера за вимогою**: сканування файлів і папок, що зберігаються локально або на спільному мережевому ресурсі (спільному сховищі, наприклад NAS). Використовуйте певний обліковий запис для запуску запланованого завдання (параметр Запуск завдання під певним обліковим записом).

• **Оновлення**. Планування завдання оновлення, під час якого оновлюється ядро виявлення та модулі програм.

• **Сканування бази даних поштових скриньок**. Дає змогу запланувати сканування бази даних і вибрати елементи, які потрібно просканувати. Це є різновидом сканування бази даних на вимогу.

Якщо ввімкнено захист бази даних поштових скриньок, ви все ще можете запланувати це завдання, однак у розділі Сканування в головному вікні програми відображатиметься повідомлення про помилку "Сканування бази даних поштових скриньок перервано через помилку". Щоб запобігти цьому, вимкніть захист бази даних поштових скриньок на час запланованого виконання завдання.

• **Надсилати звіти про поштовий карантин**. Планування надсилання електронною поштою звіту про поштовий карантин.

• **Надсилати адміністраторські звіти про поштовий карантин**. Планування надсилання електронною поштою звіту про поштовий карантин.

• **Сканування у фоновому режимі**. Дає Exchange Server можливість запускати сканування бази даних у фоновому режимі (за потреби).

• **Сканування Hyper-V**. Планування сканування віртуальних дисків у Hyper-V.

- **Сканування Office 365**. Планування сканування для гібридних середовищ Office 365.

Щоб деактивувати завдання після його створення, натисніть перемикач поруч із пунктом **Увімкнено**. Щоб активувати завдання пізніше, установіть прапорець у поданні розкладу. Щоб перейти до наступного кроку, натисніть **Далі**.

Запуск завдання

Виберіть один із варіантів нижче.

- **Один раз**. Завдання виконається один раз у зазначений день і час. Щоб виконати завдання лише один раз у зазначений час, укажіть дату й час початку одноразового виконання в меню **Виконання завдання**.

- **Багаторазово**. Завдання виконуватиметься із зазначеним проміжком часу (у хвилинах). Укажіть час щоденного виконання в меню **Виконання завдання**.

- **Щодня**. Завдання виконуватиметься щодня в указаний час.

- **Щотижня**. Завдання виконуватиметься один або кілька разів на тиждень у вибрані дні й час. Повторне виконання завдання можливе лише у визначені дні тижня, починаючи із зазначеного дня та часу. Укажіть час початку в полі "Час виконання завдання". Виберіть принаймні один день тижня, коли виконуватиметься завдання.

- За певних умов. Завдання виконуватиметься, коли відбудеться певна подія.

Пропускати завдання, якщо пристрій працює від акумулятора: якщо ввімкнуто цей параметр, завдання не запуститься, якщо на момент запланованого запуску система працює від акамулятора (наприклад, якщо комп’ютер працює від джерела безперебійного живлення).

Запуск завдання під певним обліковим записом: задайте ім’я користувача й пароль певного облікового запису для запуску запланованого завдання **Запуск зовнішньої програми** або **Сканування комп’ютера за вимогою**. Використовуйте його для запуску **сканування комп’ютера за вимогою**, якщо потрібно просканувати мережеві папки, наприклад, NAS або інше спільне сховище.

> Переконайтеся, що для облікового запису користувача, який ви використовуєте для **запуску завдання під певним обліковим записом**, дозволено **виконувати вхід як пакетне завдання** (SeBatchLogonRight). Параметри політики можна перевірити за допомогою інструмента керування груповими політиками ("Налаштування безпеки" > "Локальні політики" > "Призначення прав користувача" > "Виконати вхід як пакетне завдання").

За умови виникнення події

Під час планування завдання, що ініціюється подією, можна вказати мінімальний інтервал між виконанням двох завдань.

Завдання може запускати будь-яка з указаних нижче подій.

- Під час кожного запуску комп’ютера

• Кожного дня під час першого запуску комп’ютера

• Модемне підключення до Інтернету/VPN

• Успішне оновлення модуля

• Успішне оновлення продукту

• Вхід користувача в систему. Завдання розгорнеться після входу користувача в систему. Якщо користувач входить у комп’ютер кілька разів на день, укажіть 24 години, щоб завдання виконувалося лише під час першого входу в систему за добу, а потім аж наступного дня.

• Виявлення загрози

Запустити програму

Це завдання призначає виконання зовнішньої заявки.

• **Виконуваний файл**: виберіть виконуваний файл із дерева каталогів, натисніть кнопку огляду або введіть шлях уручну.

• **Робоча папка**: укажіть робочий каталог зовнішньої програми. У цьому каталозі буде створено всі тимчасові файли вибраного виконуваного файлу.

• **Параметри**: параметри командного рядка для програми (необов’язково).

Невиконане завдання

Якщо завдання не вдалося запустити в попередньо визначений час, можна вказати, коли потрібно здійснити наступну спробу виконання.

• **У наступний запланований час**: завдання буде виконано в зазначений час (наприклад, через 24 години).

• **Якнайшвидше**: завдання запуститься за першої змоги, коли дії, що перешкоджають його виконанню, не будуть дійсними.

• **Негайно, якщо з моменту останнього запуску пройшло більше часу, ніж указано**: час із моменту останнього запуску (у годинах). Якщо вибрати цю опцію, завдання завжди повторюватиметься через зазначений проміжок часу (у годинах).

Огляд запланованого завдання

Це діалогове вікно містить докладну інформацію про заплановане завдання. Для цього двічі натисніть завдання в **поданні розкладу** або натисніть його правою кнопкою миші й виберіть **Показати інформацію про завдання**.

Надіслати файл для аналізу

У діалоговому вікні надсилання зразків можна надіслати файл або сайт для аналізу в ESET. Якщо ви виявили файл із підозрілою поведінкою на комп'ютері або підозрілий веб-сайт в Інтернеті, їх можна надіслати для аналізу в лабораторію ESET Virus Lab. Якщо виявиться, що файл є шкідливою програмою або веб-сайтом, виявлений об'єкт буде додано до майбутнього оновлення.

Щоб надіслати файли електронною поштою, заархівуйте їх за допомогою програми WinRAR або WinZip, захистіть архів паролем `infected` і надішліть на адресу samples@eset.com. Додайте інформативну тему листа й надайте якомога більше інформації про файл (наприклад, укажіть веб-сайт, з якого ви його завантажили).

Перед відправленням зразка до ESET перевірте, чи відповідає він одному або обом переліченим нижче критеріям.
• Файл або веб-сайт не визначається взагалі.
• Файл або веб-сайт помилково визначається як такий, що містить загрозу.
• Ми не приймаємо особисті файли як зразки, щоб сканувати їх засобами ESET на наявність шкідливого програмного забезпечення. Дослідницька лабораторія ESET Research Lab не виконує сканування на вимогу для користувачів.
• Додайте інформативну тему листа й надайте якомога більше інформації про файл (наприклад, укажіть веб-сайт, з якого ви його завантажили).

Якщо принаймні один із наведених вище критеріїв не виконується, ви не отримаєте відповіді, доки не надасте додаткову інформацію.

У розкривному меню **Причини надсилання зразка** виберіть опис, який найкраще відповідає вашому повідомленню.

- Підозрілий файл
- Підозрілий сайт (веб-сайт, інфікований шкідливим програмним забезпеченням)
- Помилкове спрацювання (файл помилково розпізнаний як інфікований)
- Сайт, заблокований помилково
- Інше

Файл/сайт

Шлях до файлу або веб-сайту, який потрібно надіслати.

Контактна електронна адреса

Контактна адреса електронної пошти відправляється з будь-якими підозрілими файлами до ESET і може використовуватися для зв'язку з вами, якщо для проведення аналізу знадобляться додаткові відомості. Указувати адресу електронної пошти необов'язково. ESET дасть вам відповідь тільки в тому разі, якщо буде потрібна додаткова інформація. Оскільки щодня на наші сервери надходять десятки тисяч файлів, неможливо надіслати відповідь на кожен запит.

Надіслати анонімно

Установіть прапорець **Надіслати анонімно** для надсилання підозрілого файлу або веб-сайту без введення адреси електронної пошти.

Підозрілий файл

Виявлені ознаки й симптоми зараження шкідливою програмою

Введіть опис поведінки підозрілого файлу, яка спостерігається на комп’ютері.

Походження файлу (URL-адреса чи постачальник)

Укажіть походження файлу (джерело) і спосіб його отримання.

Примітки й додаткова інформація

Тут можна ввести додаткову інформацію або опис, які допоможуть ідентифікувати підозрілий файл.

> Обов’язковим є лише перший параметр: **Виявлені ознаки й симптоми зараження шкідливим програмним забезпеченням**. Проте надання додаткової інформації значно допоможе співробітникам наших лабораторій у процесі ідентифікації зразків.

Підозрілий веб-сайт

У розкривному меню "Що не так із сайтом" виберіть один із наведених нижче варіантів.

Інфіковано

Веб-сайт містить віруси або інше шкідливе програмне забезпечення, поширюване різними способами.

Фішинг

Зазвичай мета фішингу – отримати доступ до конфіденційних даних, як-от номери банківських рахунків, PIN-коди тощо. Дізнайтеся більше про цей тип атаки в глосарії.

Шахрайство

Сумнівний або шахрайський веб-сайт.

Інше

Використовуйте цю опцію, якщо жоден із наведених вище варіантів не відповідає сайту, про який ви хочете повідомити.

Примітки й додаткова інформація

Тут можна ввести додаткову інформацію чи опис, які можуть бути корисними під час аналізу підозрілого веб-сайту.

Помилкове спрацювання: файл

Просимо надсилати нам файли, які помилково визначаються як заражені, щоб ми могли поліпшити роботу ядра виявлення й забезпечити захист іншим користувачам. Помилкове спрацьовування можливе, коли сигнатура файлу збігається із сигнатурою, що міститься в ядрі виявлення.

> Перші три параметри обов'язково потрібно вказати, щоб ідентифікувати нормальні програми й відрізнити їх від шкідливого коду. Надання додаткової інформації значною мірою допомагає лабораторії в процесі ідентифікації та опрацювання зразків.

Назва й версія програми

Назва програми і її версія (наприклад, номер, псевдонім або кодова назва).

Походження файлу (URL-адреса чи постачальник)

Укажіть походження файлу (джерело) і спосіб його отримання.

Призначення програми

Загальний опис програми, її тип (наприклад, браузер, медіапрогравач тощо) і функції.

Примітки й додаткова інформація

Тут можна вказати додаткову інформацію або опис, які допоможуть під час опрацювання підозрілого файлу.

Сайт, заблокований помилково

Рекомендуємо надсилати інформацію про сайти, які помилково визначено як інфіковані, шахрайські або фішинговані. Помилкове спрацьовування можливе, коли сигнатура коду сайту збігається із сигнатурою, що міститься в ядрі виявлення. Надсилайте інформацію про такі веб-сайти, щоб поліпшити наше ядро виявлення й забезпечити захист інших користувачів.

Примітки й додаткова інформація

Можна вказати додаткову інформацію або опис, які допоможуть під час опрацювання підозрілого файлу.

Інше

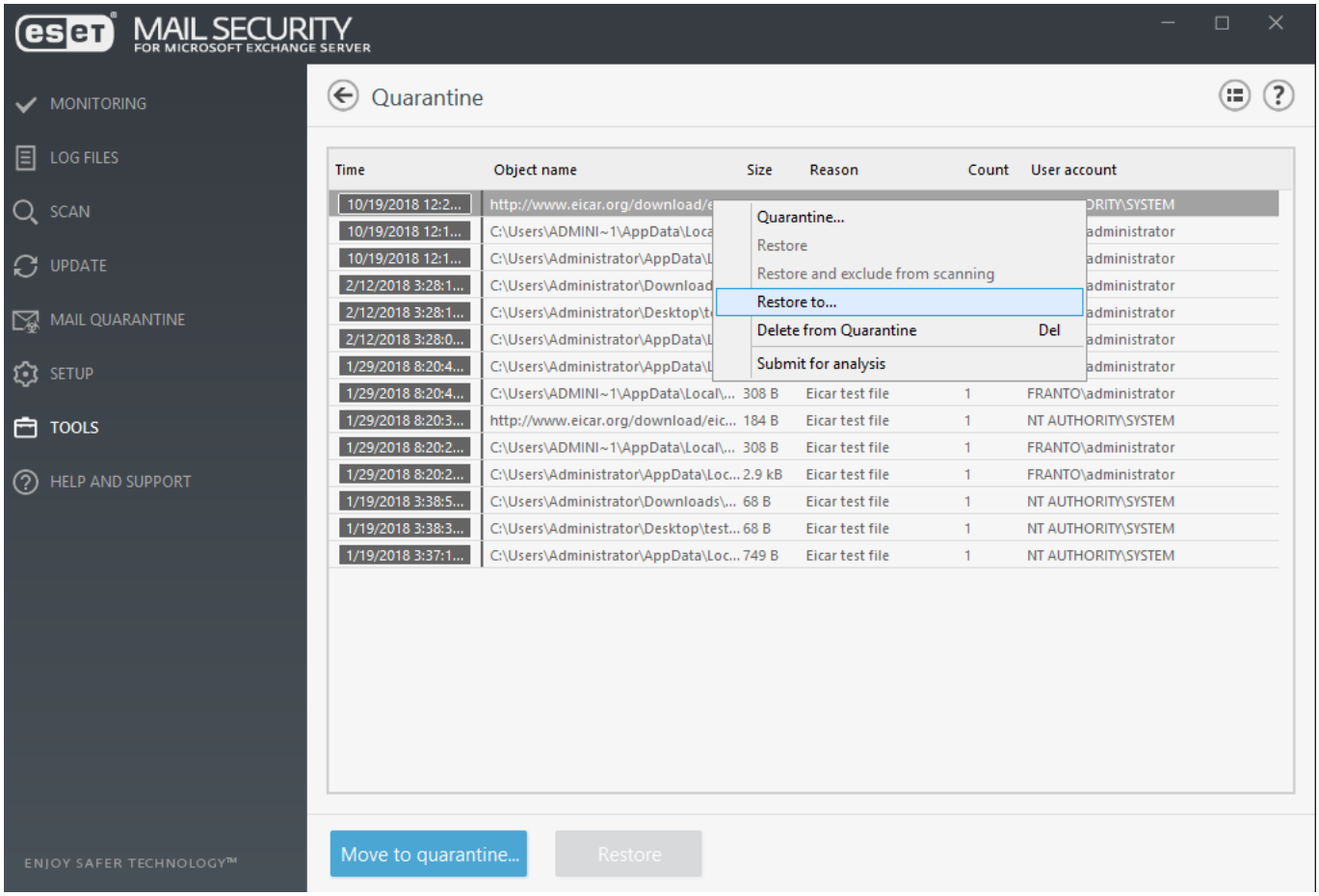
Скористайтеся цією формою, якщо файл не можна віднести до категорії "Підозрілий файл" або "Помилкове спрацювання".

Причина надсилання файлу

Введіть докладний опис і причину надсилання файлу.

Карантин

Основна функція карантину — безпечно ізолювати інфіковані файли. Файли потрібно переміщати в карантин, якщо їх неможливо очистити або безпечно видалити чи якщо видаляти їх не рекомендовано або програма ESET Mail Security хибно визначила їх зараженими. У карантин можна перемістити будь-який файл. Ця дія рекомендована, якщо файл поводиться підозріло, але не виявляється сканером шкідливого програмного забезпечення. Переміщені в карантин файли можна надсилати на аналіз до антивірусної лабораторії ESET.



Файли, що зберігаються в папці карантину, можна переглянути як таблицю, де вказано таку інформацію: дату й час переміщення в карантин, шлях до вихідного розташування зараженого файлу, його розмір у байтах, причину переміщення в карантин (наприклад, об’єкт, доданий користувачем) і кількість загроз (наприклад, якщо це архів, що містить кілька загроз).

Якщо у файловий карантин переміщаються об’єкти повідомлень електронної пошти, відображається шлях до поштової скриньки / папки / імені файлу.

Переміщення файлів у карантин

ESET Mail Security автоматично переміщає в карантин видалені файли (якщо ви не вимкнули цю опцію у вікні оповіщень). Щоб вручну перемістити в карантин підозрілий файл, натисніть **Карантин**. Переміщені в карантин файли буде видалено з вихідного розташування. Це також можна зробити за допомогою контекстного меню. Натисніть правою кнопкою миші у вікні **Карантин** і виберіть **Карантин**.

Відновлення із карантину

Переміщені в карантин файли можна відновити у вихідному розташуванні. Скористайтеся функцією **Відновити** в контекстному меню, натиснувши правою кнопкою миші потрібний файл у вікні карантину. Якщо файл позначено як потенційно небажану програму,, буде доступна опція **Відновити та виключити зі сканування**. У контекстному меню також є опція **Відновити в**, яка дає змогу відновити файл в іншому розташуванні (не вихідному).

> Якщо програма помилково перемістила в карантин нешкідливий файл, після відновлення виключіть цей файл зі сканування та надішліть його до служби технічної підтримки ESET.

Надсилання файлу з карантину

Якщо ви перемістили в карантин підозрілий файл, який не було виявлено програмою, або якщо файл неправильно визначено як заражений (наприклад, шляхом евристичного аналізу коду) і згодом переміщено в карантин, надішліть його до антивірусної лабораторії ESET. Щоб надіслати файл із карантину, натисніть файл правою кнопкою миші та в контекстному меню виберіть Надіслати на аналіз.

Видалити з карантину

Натисніть потрібний елемент правою кнопкою миші й виберіть **Видалити з карантину**. Або виберіть відповідні елементи й натисніть клавішу **Delete** на клавіатурі.

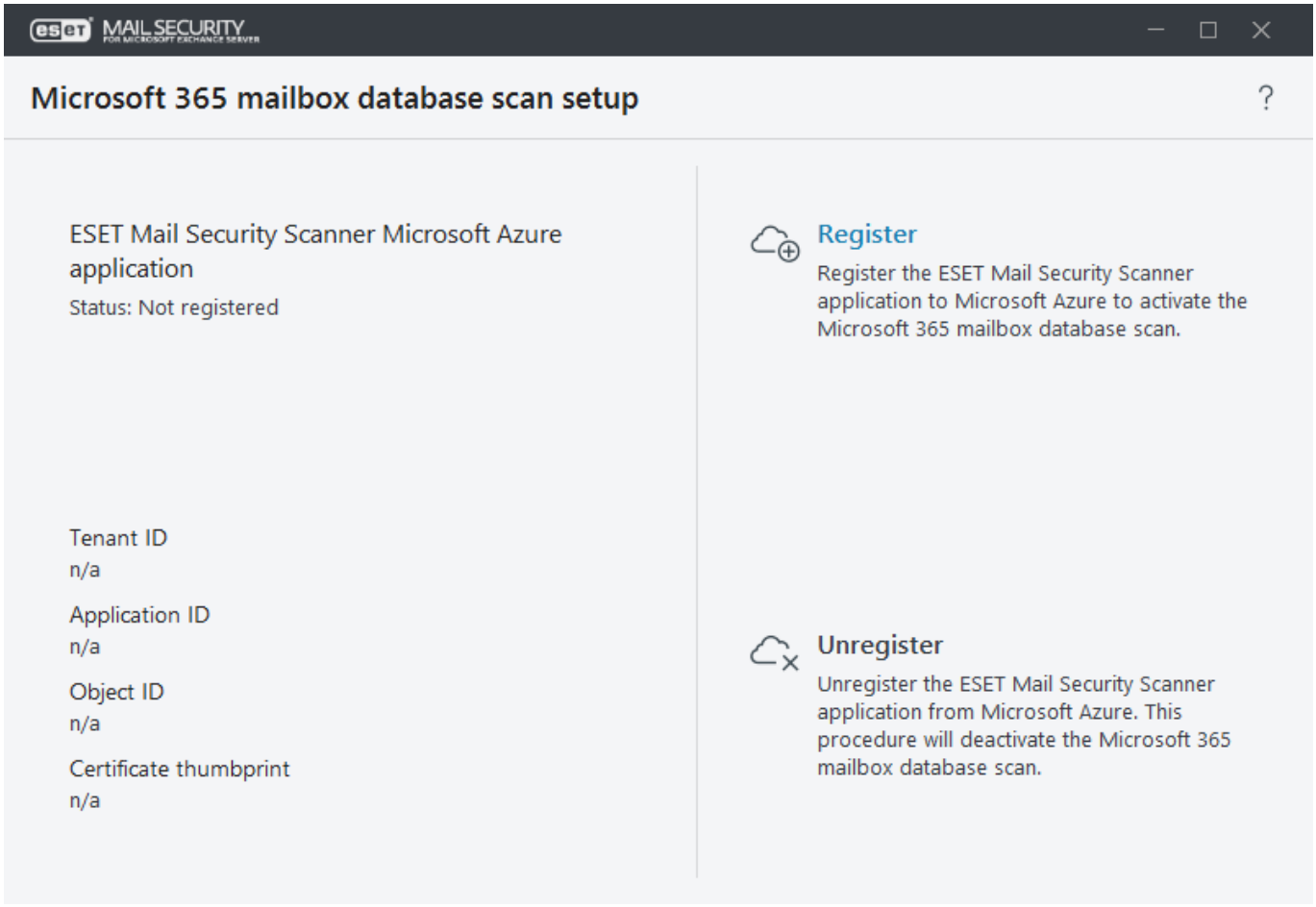
Майстер сканування поштових скриньок Microsoft 365

ESET Mail Security підтримує сканування віддалених поштових скриньок Microsoft 365 і загальнодоступних папок, наприклад стандартне сканування бази даних поштових скриньок на вимогу. Щоб активувати цю функцію, зареєструйте сканер ESET Mail Security.

Швидкі посилання:

- Реєстрація сканера ESET Mail Security
- Скасування реєстрації сканера ESET Mail Security

Щоб почати використовувати сканування бази даних поштової скриньки Microsoft 365 у ESET Mail Security,зареєструйте програму сканера ESET Mail Security у Microsoft Azure. На сторінці параметрів сканування поштових скриньок Microsoft 365 відображається статус реєстрації (якщо його вже зареєстровано), а також дані реєстрації (ідентифікатор клієнта, ідентифікатор програми, ідентифікатор об’єкта й відбиток сертифіката). Можна зареєструвати сканер ESET Mail Security або скасувати його реєстрацію:



Після успішної реєстрації сканера функція сканування бази даних поштових скриньок Microsoft 365 стане доступною в меню Сканування зі списком поштових скриньок (і загальнодоступних папок), які можна вибрати для сканування.

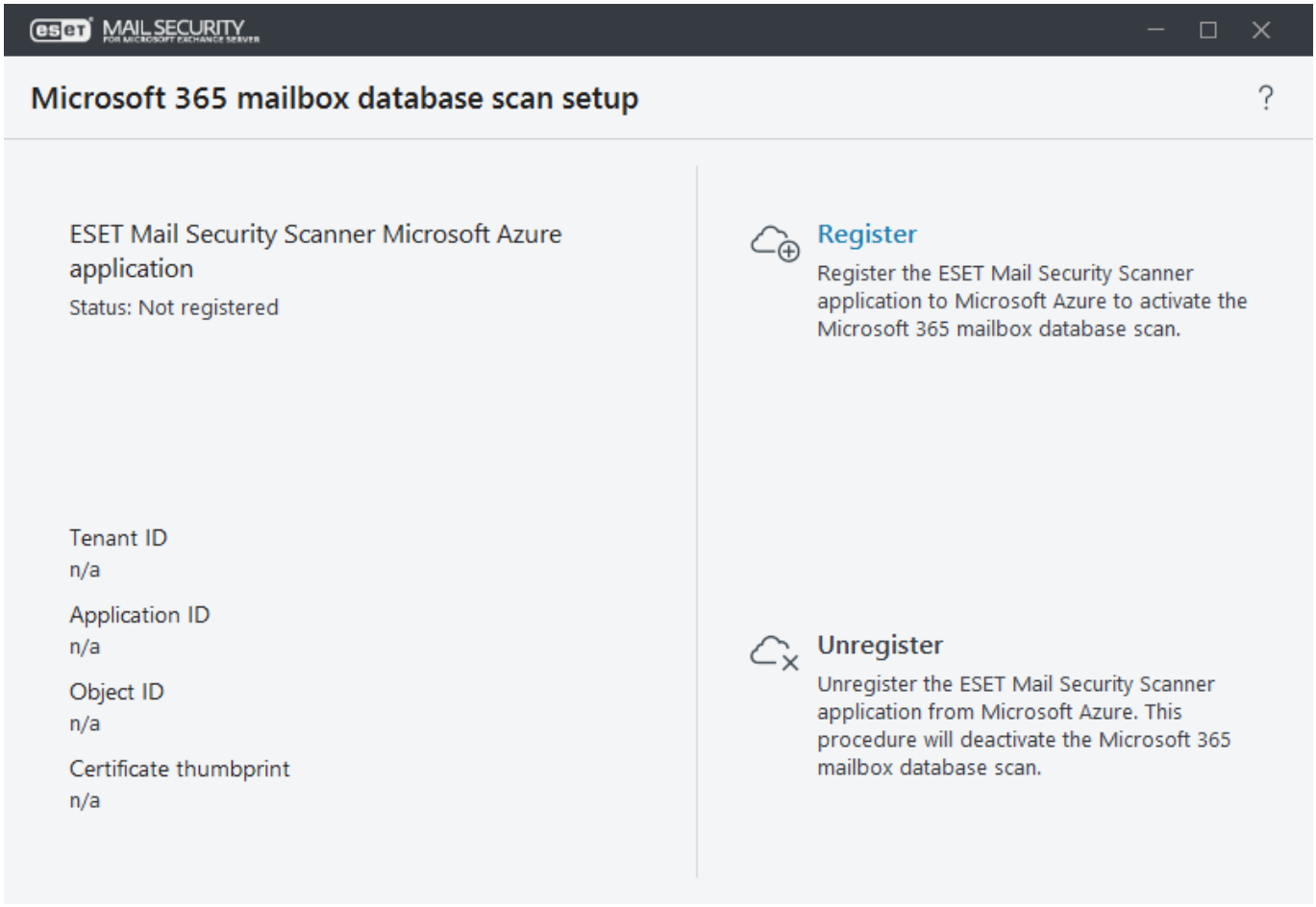
Повторна реєстрація з використанням іншого облікового запису: Щоб зареєструвати сканер ESET Mail Security у новому обліковому записі Microsoft 365, потрібно скасувати реєстрацію сканера ESET Mail Security у попередньому обліковому записі, а потім знову зареєструвати його в новому обліковому записі адміністратора Microsoft 365.

Сканер ESET Mail Security реєструється як програма в Microsoft Azure. Перейдіть до розділу **реєстрацій програм** в **Azure Active Directory** й клацніть **Переглянути всі програми**. У списку відображатимуться програми сканування ESET Mail Security. Натисніть програму, щоб переглянути відомості про неї.

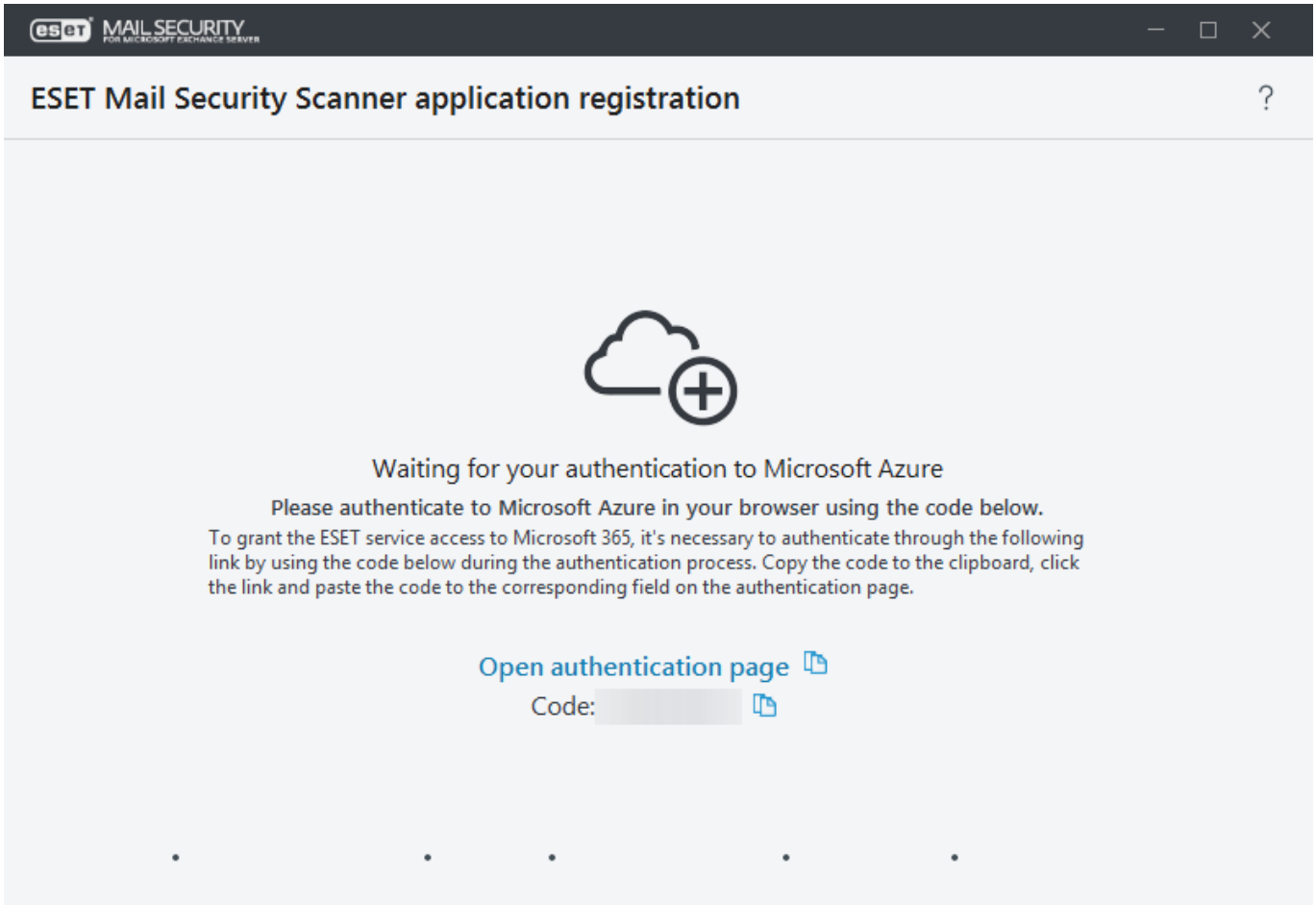
Реєстрація сканера ESET Mail Security

Щоб зареєструвати програму сканера ESET Mail Security у Microsoft Azure для активації сканування бази даних поштових скриньок Microsoft 365, дотримуйтеся наведених нижче інструкцій:

1. Клацніть **Зареєструвати**, щоб розпочати реєстрацію сканера ESET Mail Security. Відкриється майстер реєстрації.

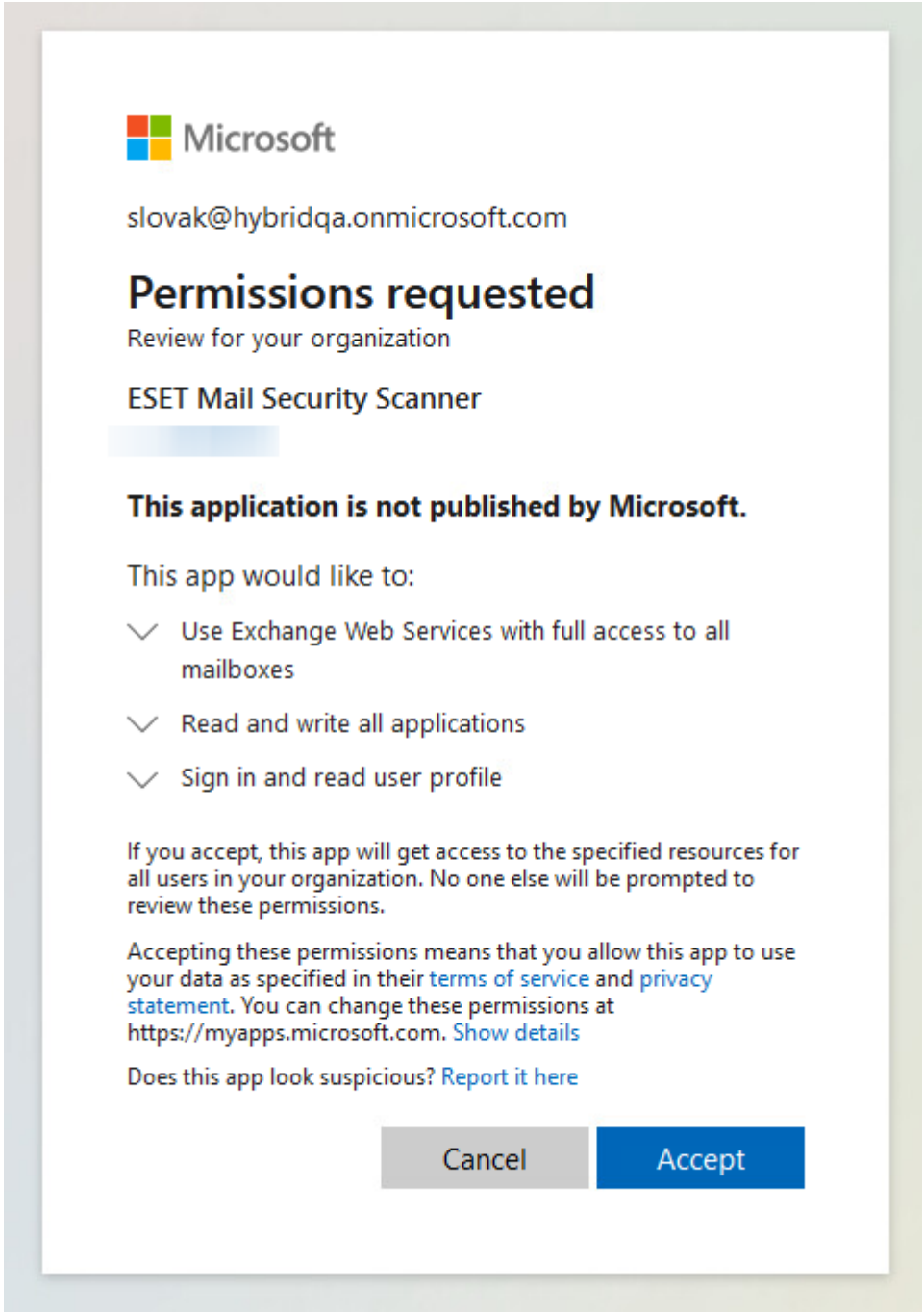


2. Скопіюйте наданий код, клацніть **Відкрити сторінку аутентифікації** та введіть код.

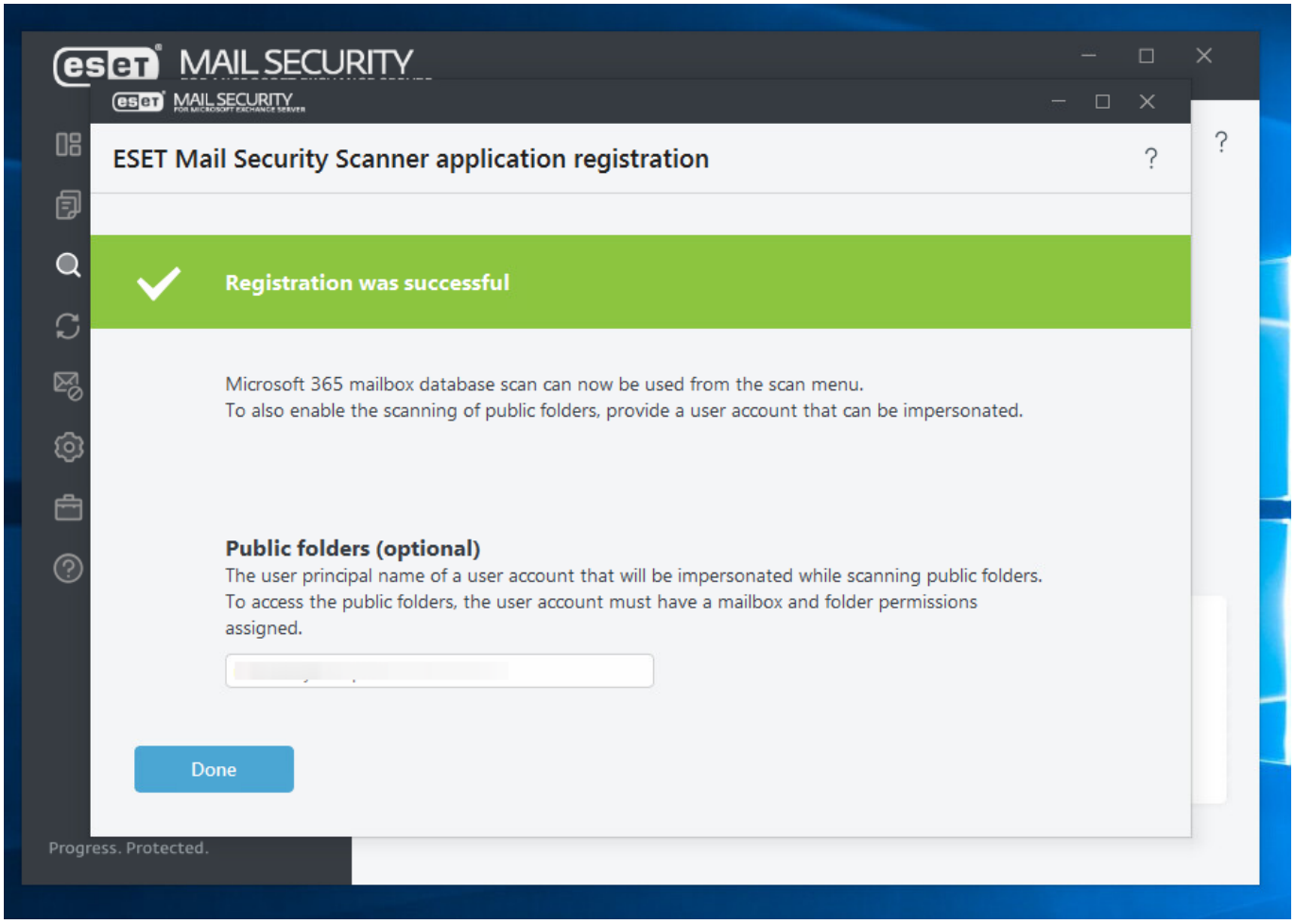


3. Відкривається веб-браузер зі сторінкою **вибору облікового запису** Microsoft. Виберіть обліковий запис, що використовується (якщо доступно), або введіть облікові дані адміністратора Microsoft 365 і натисніть **Увійти**.

4. Для сканера ESET Mail Security потрібні три типи дозволів, зазначених у повідомленні про прийняття. Клацніть **Прийняти**, щоб дозволити для ESET Mail Security доступ до даних Microsoft 365.



5. Закрийте веб-браузер і зачекайте, поки завершиться реєстрація сканера ESET Mail Security. З'явиться повідомлення **"Реєстрацію виконано"**.



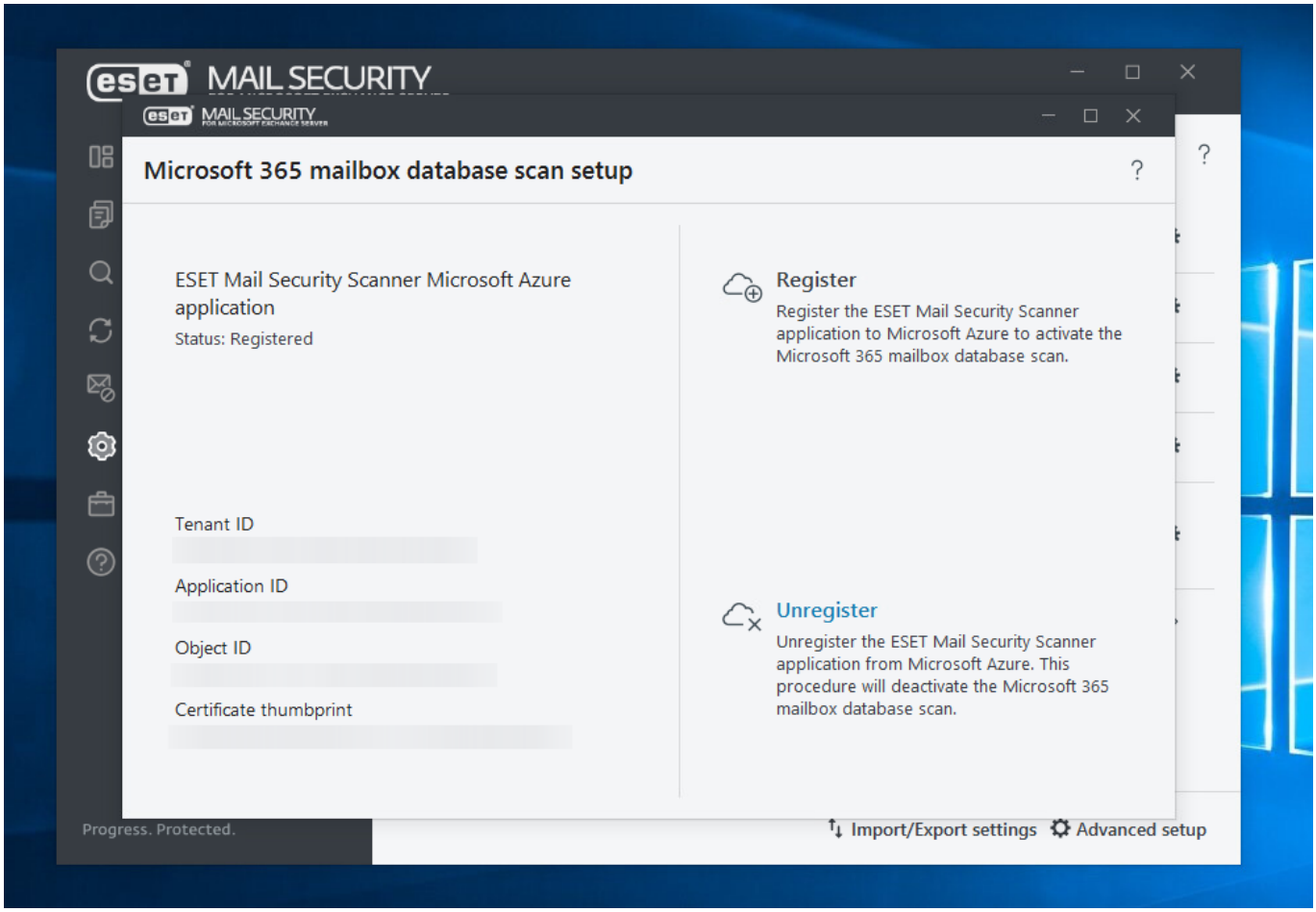
6. **Спільні папки (необов’язково)**

Щоб сканувати спільні папки, укажіть ім’я облікового запису головного користувача (пароль можна не вказувати) для імітації користувача. Переконайтеся, що цей обліковий запис користувача має доступ до всіх спільних папок. Клацніть **Готово**.

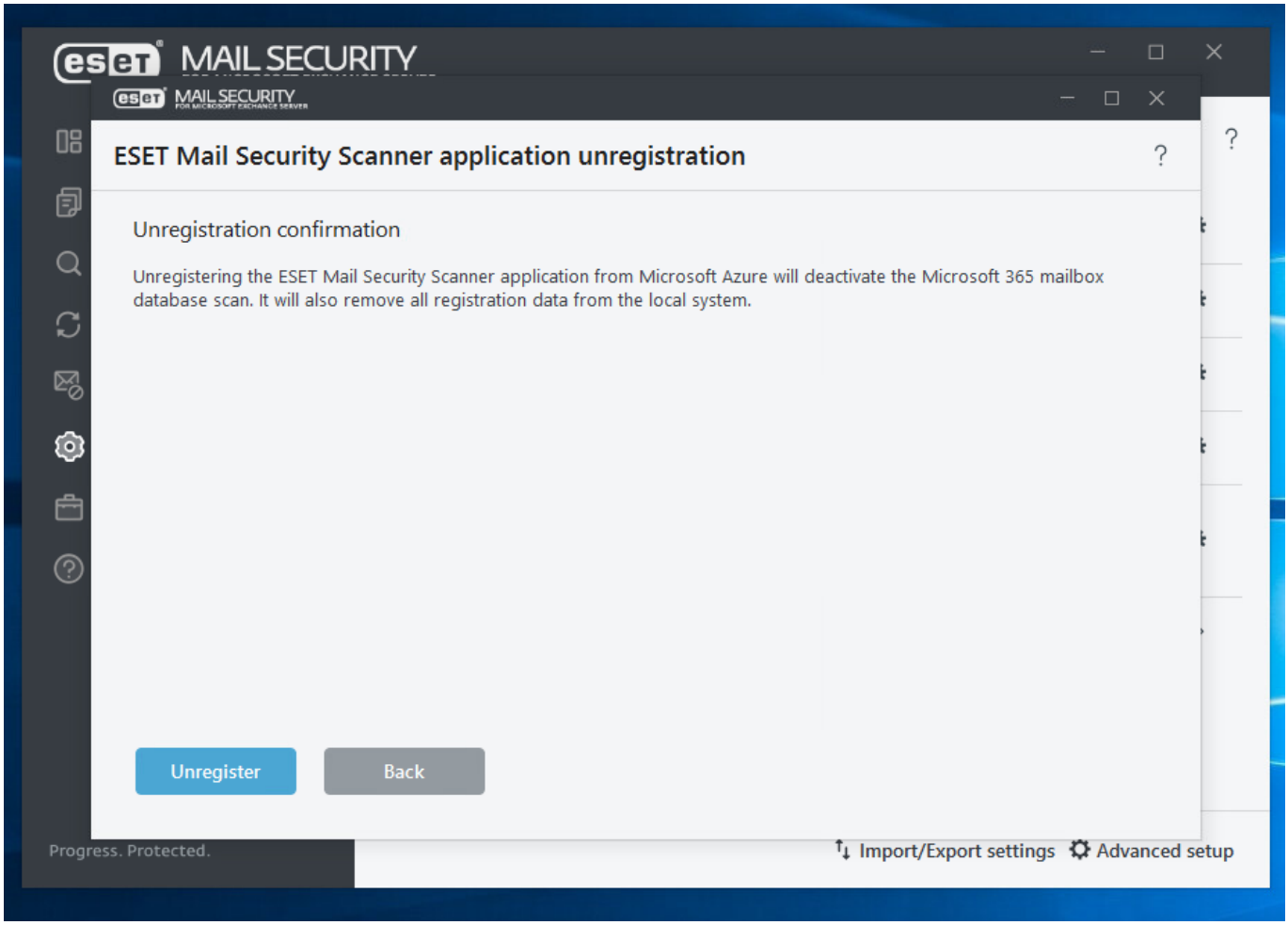
Скасування реєстрації сканера ESET Mail Security

Процес скасування реєстрації дає змогу видалити сертифікат і сканер ESET Mail Security з Microsoft Azure. Цей процес також видаляє локальні залежності й знову активує параметр реєстрації.

1. Клацніть **Параметри** > **Сервер** > **Сканування поштових скриньок Microsoft 365**, а потім клацніть **Скасувати реєстрацію**, щоб розпочати процес видалення сканера ESET Mail Security. Відкриється майстер скасування реєстрації.



2. Клацніть **Скасувати реєстрацію**, щоб підтвердити видалення сканера ESET Mail Security. Зачекайте, поки завершиться скасування реєстрації у Microsoft Azure.



3. Якщо процес скасування реєстрації завершиться без помилок, у майстрі скасування реєстрації з'явиться повідомлення **Скасування реєстрації виконано**.

Параметри захисту сервера

Параметри захисту сервера є основним варіантом інтеграції. Клацніть перемикач, щоб увімкнути або вимкнути інтеграцію захисту бази даних поштових скриньок, захисту передачі пошти або входу з використанням DKIM із сервером Exchange. Для кожного типу захисту можна налаштувати детальні параметри у відповідному розділі. Окрім того, можна змінити пріоритет агента (переконайтеся, що позиція ESET DKIM у списку пріоритетності є останньою).

У системі Microsoft Exchange Server 2010 або 2010 можна вибрати захист бази даних поштових скриньок або сканування бази даних поштових скриньок за вимогою. Одночасно можна активувати лише один тип захисту. Якщо ви вирішите використовувати сканування бази даних поштових скриньок на вимогу, необхідно буде вимкнути захист бази даних поштових скриньок. В іншому разі сканування бази даних поштових скриньок за вимогою буде недоступне.

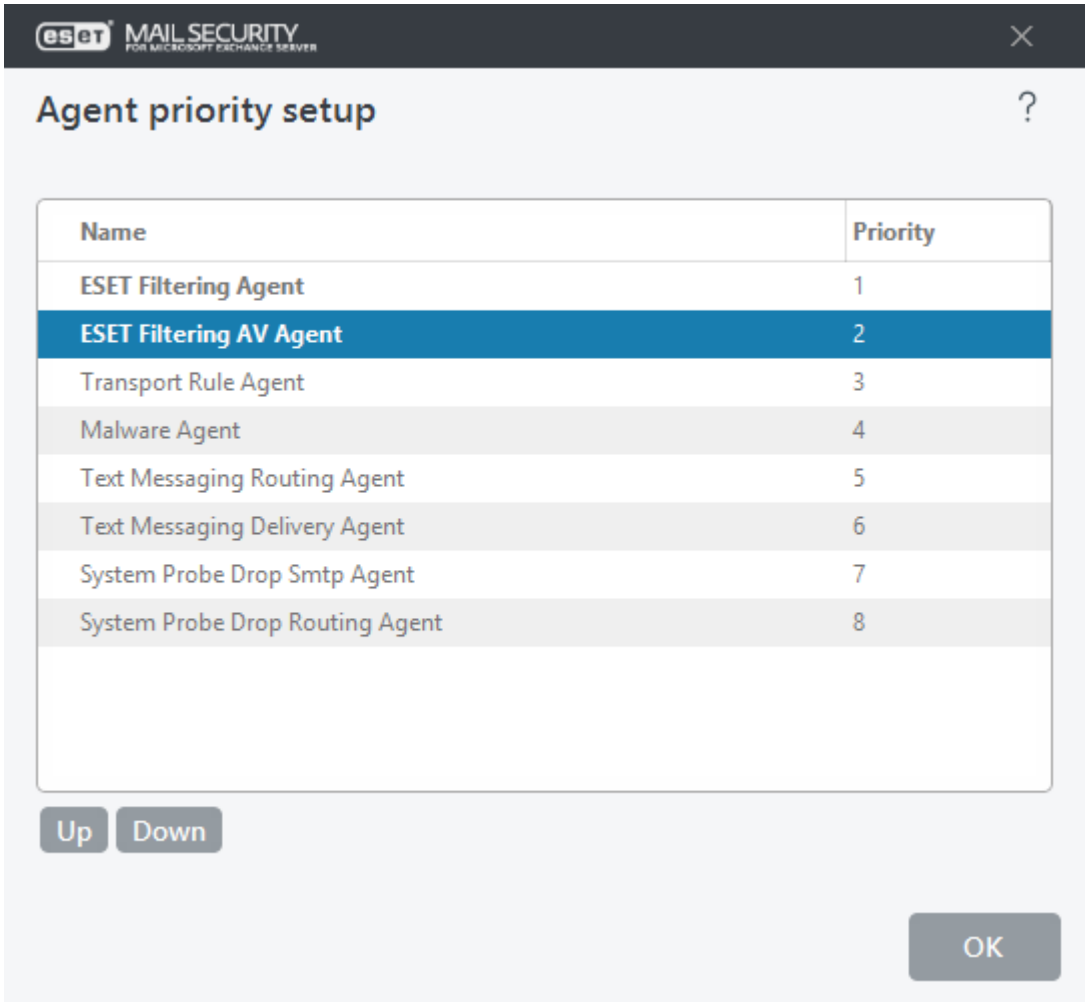
ESET Mail Security забезпечує високий рівень захисту для Microsoft Exchange Server, використовуючи наведені нижче функції:

- Антивірус та антишпигун
- Антиспам

- Захист від фішинг-атак
- Правила
- Захист передачі пошти (Exchange Server 2010, 2013, 2016, 2019)
- Захист бази даних поштових скриньок (Exchange Server 2010)
- Сканування бази даних поштових скриньок за вимогою (Exchange Server 2010, 2013, 2016, 2019, 2019)
- Поштовий карантин (параметри типу поштового карантину)
- Підписання DKIM

Параметри пріоритету агента

За потреби можна вказати порядок, у якому агенти ESET Mail Security ставатимуть активними після запуску Microsoft Exchange Server. Числове значення визначає пріоритет. Що менше номери, то вище пріоритет. Це стосується Microsoft Exchange Server 2010 і новіших версій.



Вгору/Вниз

Щоб підвищити або зменшити пріоритет вибраного агента, переміщайте його в списку вгору або вниз відповідно. Пріоритет можна змінити для відповідних агентів (виділені жирним).

Рекомендуємо не змінювати пріоритет агента ESET DKIM, залишивши його останнім у списку. Таким чином ви будете впевнені, що підписування заголовків виконуватиметься наостанок після того, як попередні агенти внесуть у них усі потрібні зміни.

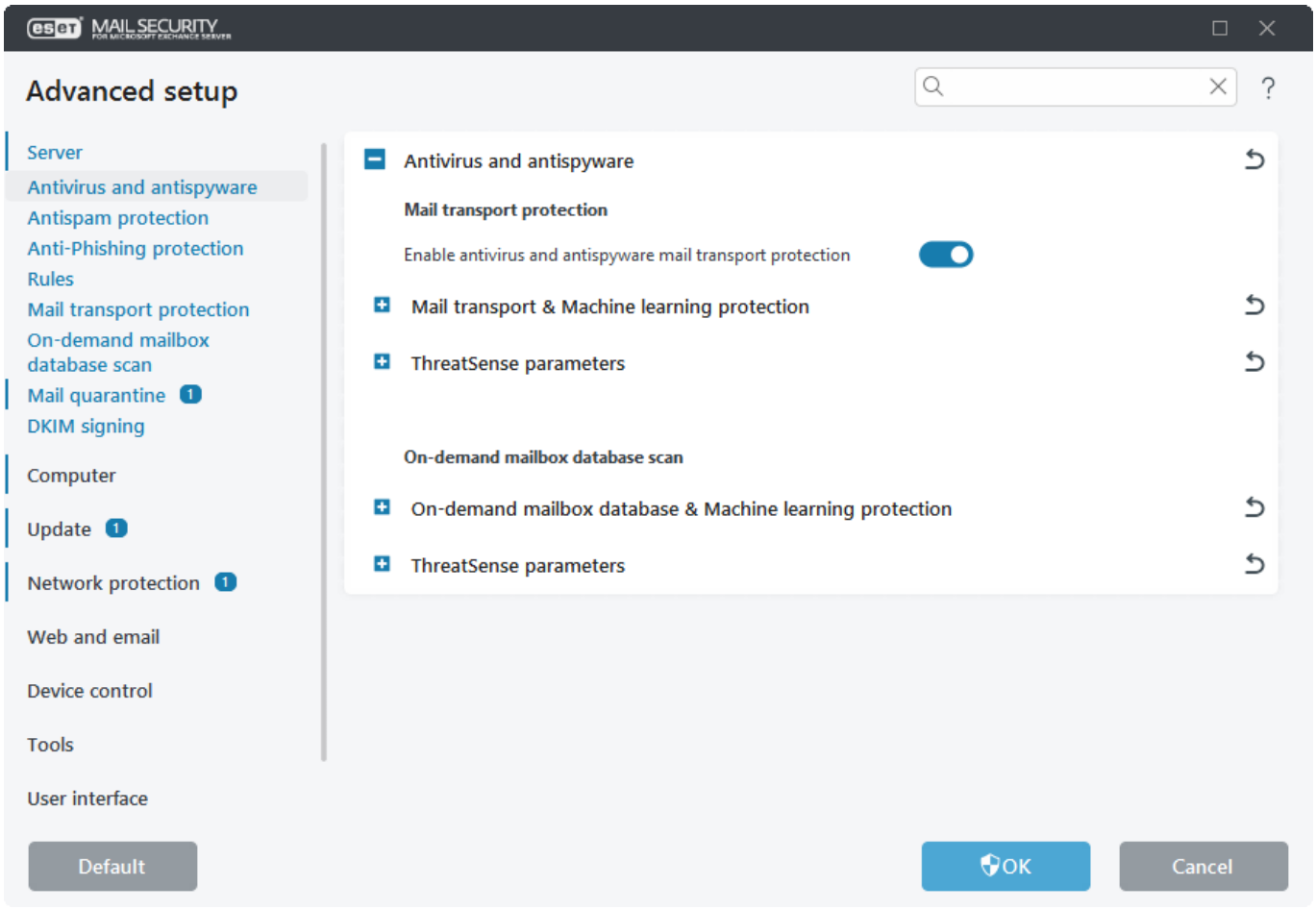
Антивірус та антишпигун

У цьому розділі можна налаштувати параметри антивірусу й захисту від шпигунських програм для поштового сервера.

Транспортний агент забезпечує захист передачі пошти. Він доступний тільки для Microsoft Exchange Server 2010 і новіших версій, проте на сервері Microsoft Exchange Server має бути роль "Межовий транспорт" і "Транспортний сервер-концентратор". Це також стосується конфігурацій з одним сервером, де на одному комп'ютері налаштовано кілька ролей Exchange Server (якщо він має роль "Межовий транспорт" або "Транспортний сервер-концентратор").

Захист передачі пошти

Якщо вимкнути параметр **Увімкнути захист від вірусів і шпигунських програм під час передавання електронних листів**, плагін ESET Mail Security для Exchange Server не буде вивантажено з процесу сервера Microsoft Exchange. Він тільки перевірить повідомлення без перевірки на віруси на транспортному рівні. Повідомлення все одно перевірятимуться на наявність вірусів і спаму на рівні бази даних. Наявні правила будуть застосовані.



Захист бази даних поштової скриньки

Якщо вимкнути параметр **Увімкнути захист бази даних поштових скриньок від вірусів і шпигунських програм**, плагін ESET Mail Security для Exchange Server не буде вивантажено з процесу сервера Microsoft Exchange. Він тільки перевірить повідомлення без перевірки на віруси на рівні бази даних. Повідомлення все одно перевірятимуться на наявність вірусів і спаму на рівні транспорту. Застосовуватимуться наявні правила.

Сканування бази даних поштових скриньок за вимогою

Сканування бази даних поштових скриньок на вимогу стає доступним після вимкнення **захисту бази даних поштових скриньок** у розділі Сервер.

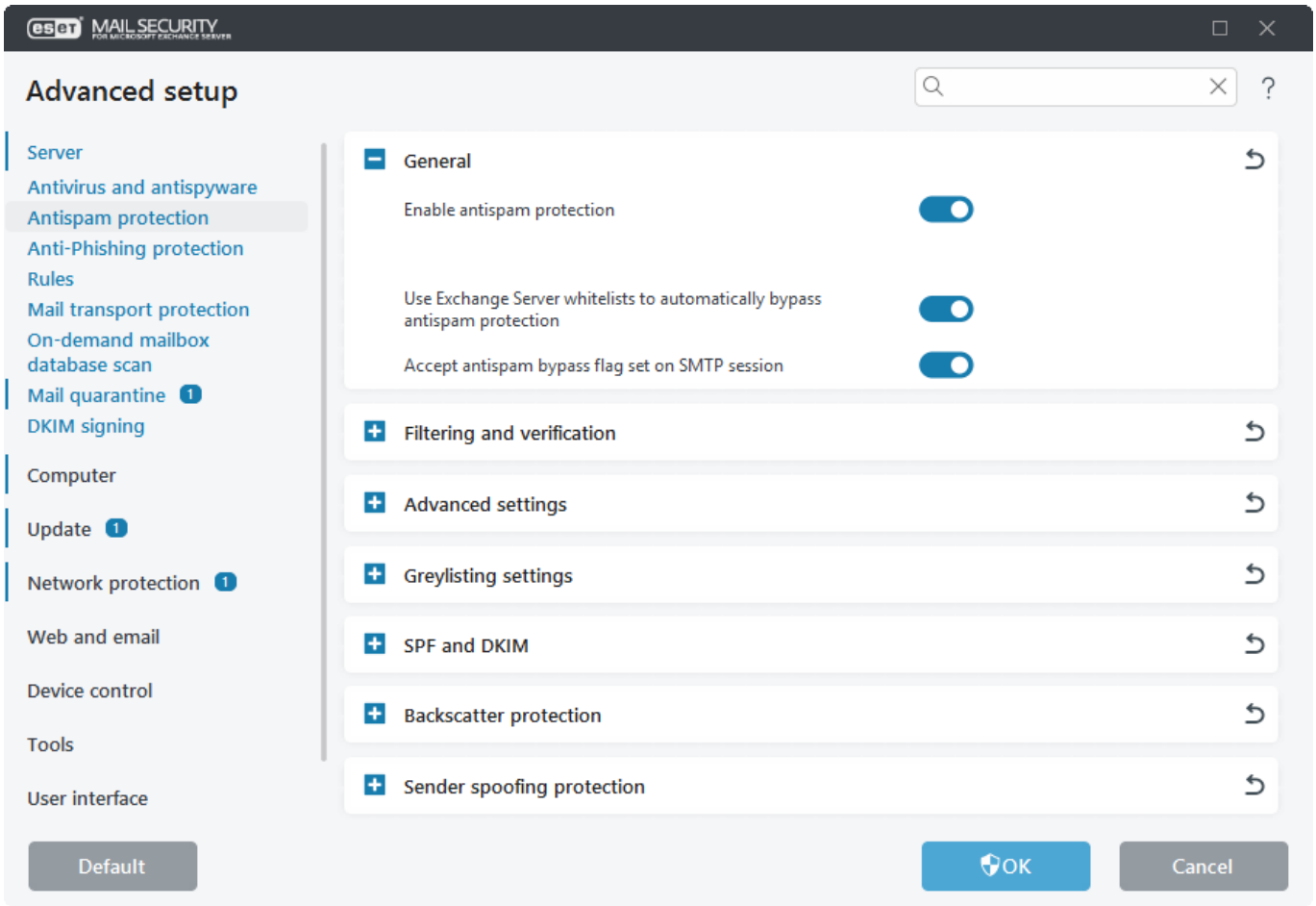
ThreatSense параметри

Змініть параметри сканування для захисту передачі пошти, захисту бази даних поштових скриньок і сканування бази даних поштових скриньок за вимогою.

Захист від спаму

На вашому поштовому сервері за замовчуванням увімкнуто антиспам. Щоб вимкнути його, натисніть перемикач **Увімкнути антиспам**.

> Вимкнення захисту від спаму не змінить статус захисту. Навіть якщо модуль антиспаму вимкнуто, у головному вікні програми в розділі **Моніторинг** усе одно відображатиметься статус **Ваш пристрій захищено** (зелений колір). Вимкнений модуль "Антиспам" не вважається зниженням рівня захисту.



Використовувати білі списки Exchange Server для автоматичного обходу антиспаму

Дає ESET Mail Security змогу використовувати специфічні "білі списки" Exchange. Якщо цей параметр увімкнено, враховуються такі фактори:

- IP-адреса сервера є в списку дозволених IP-адрес Exchange Server
- Для поштової скриньки одержувача повідомлення встановлено позначку обходу антиспаму
- Адреса відправника є в списку безпечних відправників одержувача повідомлення (переконайтеся, що в середовищі Exchange Server налаштовано синхронізацію списку безпечних відправників, зокрема його агрегацію)

Якщо для вхідного повідомлення виконується будь-яке з наведених вище умов, для нього буде застосовано обхід перевірки модулем "Антиспам". Повідомлення не буде оцінюватися як СПАМ і буде доставлено в поштову скриньку одержувача.

Приймати позначку обходу антиспаму, задану в сеансі SMTP

Цей параметр буде корисним, якщо ви маєте автентифіковані сеанси SMTP між серверами Exchange Server, на яких налаштовано параметр обходу антиспаму. Наприклад, якщо у вас є сервер межового транспорту й транспортний сервер-концентратор, немає необхідності сканувати трафік між двома серверами. Параметр **Приймати позначку обходу антиспаму, задану в сеансі SMTP** ввімкнуто за замовчуванням, проте він застосовується тільки коли позначку обходу антиспаму задано для сеансу SMTP вашого Exchange Server. Якщо вимкнути параметр **Приймати позначку обходу антиспаму, задану в сеансі SMTP**, ESET Mail Security просканує сеанс SMTP на наявність спаму незалежно від параметра обходу антиспаму на вашому Exchange Server.

> Потрібно регулярно оновлювати базу даних антиспаму, щоб модуль антиспаму забезпечував найкращий захист. Щоб база даних антиспаму могла оновлюватися регулярно, переконайтеся, що ESET Mail Security має доступ до правильних IP-адрес на необхідних портах. Більш докладні відомості про те, які IP-адреси й порти потрібно ввімкнути на сторонньому брандмауері, див. в нашій статті бази знань.

Параметри функцій доступні в їхніх розділах:

- Фільтрація й перевірка
- Додаткові параметри
- Технологія сірих списків
- SPF і DKIM
- Захист від несправжніх сповіщень про стан доставки
- Захист від підміни відправника

Фільтрація й перевірка

У списках дозволених, заблокованих і ігнорованих IP-адрес можна вказати певні критерії, наприклад діапазон IP-адрес, ім’я домену тощо. Щоб додати, змінити або видалити критерій, клацніть **Змінити** для списку, в який потрібно внести зміни.

> IP-адреси або домени, указані в списку **Ігноровано**, не перевірятимуться антиспамом. Для них застосовуватимуться інші методи захисту від спаму.
> У списках ігнорованих адрес мають міститися всі IP-адреси / імена домену внутрішньої інфраструктури. Ви також можете додати в цей список IP-адреси / імена доменів вашого постачальника послуг Інтернету або зовнішніх поштових серверів, які наразі внесено до чорного списку однією зі служб RBL або DNSBL (чорний список хмари: список заборонних адрес ESET або сторонній список заборонних адрес).
> Це дає змогу отримувати електронні листи з джерел, які входять до списку ігнорованих адрес, навіть якщо їхні IP-адреси є в чорному списку хмари. Такі вхідні листи будуть отримуватися. Їхній вміст перевірятиметься за допомогою інших методів захисту від спаму.

Список дозволених IP-адрес	Автоматично додає до білого списку електронні листи, надіслані із заданих IP-адрес. Вміст електронного листа не перевірятиметься.
Список заблокованих IP-адрес	Автоматично блокує електронні листи, надіслані із заданих IP-адрес.
Список ігнорованих IP-адрес	змушує ігнорувати IP-адреси з цього списку під час класифікації. Вміст електронного листа перевірятиметься. Щоб помістити в білий список локальні IP-адреси вашої мережі, скористайтеся повзунком "Є частиною внутрішньої інфраструктури". Див. приклад нижче.
Список заборонених доменів у тілі електронного листа	Блокує електронні листи, які містять указаний домен у тексті повідомлення. Приймаються лише домени з реальним TLD (top-level domain, домен верхнього рівня).
Список ігнорованих доменів у тілі електронного листа	Під час класифікації змушує ігнорувати домени з цього списку, присутні в тілі повідомлення. Приймаються лише домени з реальним TLD (top-level domain, домен верхнього рівня).
Список заблокованих IP-адрес у тілі електронного листа	Блокує електронні листи, які містять указану IP-адресу в тексті повідомлення.
Список ігнорованих IP-адрес у тілі електронного листа	Під час класифікації змушує ігнорувати IP-адреси з цього списку, присутні в тілі повідомлення.
Список дозволених відправників	Додає в білий список електронні листи від певного відправника. Тільки одна адреса відправника або цілий домен використовується для верифікації на основі такого пріоритету: 1.SMTP 'MAIL FROM' адреса 2.поле заголовка електронного листа "Return-Path:"; 3.поле заголовка електронного листа "X-Env-Sender:"; 4.поле заголовка електронного листа "From:"; 5.поле заголовка електронного листа "Sender:"; 6.поле заголовка електронного листа "X-Apparently-From:";

Список заблокованих відправників	Додає в список блокування електронні листи від певного відправника. Усі ідентифіковані адреси відправника або цілі домени використовуються для верифікації таких атрибутів: SMTP 'MAIL FROM' адреса поле заголовка електронного листа "Return-Path:"; поле заголовка електронного листа "X-Env-Sender:"; поле заголовка електронного листа "From:"; поле заголовка електронного листа "Sender:"; поле заголовка електронного листа "X-Apparently-From:";
Список дозволених доменів та IP-адрес	Поміщає до білого списку електронні листи з IP-адрес, пов'язаних із доменами в цьому списку. Записи SPF (Sender Policy Framework, структура політики фільтрації відправників) розпізнаються під час розпізнавання перетворення IP-адрес.
Список заблокованих доменів та IP-адрес	Блокує електронні листи з IP-адрес, пов'язаних із доменами в цьому списку. Записи SPF розпізнаються під час розпізнавання перетворення IP-адрес.
Список ігнорованих доменів та IP-адрес	Під час класифікації змушує не перевіряти IP-адреси, пов'язані з доменами в цьому списку. Записи SPF розпізнаються під час розпізнавання перетворення IP-адрес.
Список заблокованих країн	Блокує електронні листи з певних країн. Блокування на основі GeoIP. Якщо спам-повідомлення надсилається з поштового сервера з IP-адресою, зазначеною в базі даних геолокації для країни, яку вибрано в списку заблокованих країн, воно автоматично позначатиметься як спам. До цього повідомлення буде застосовано дію по відношенню до спаму. Цю дію визначено в розділі Захист передачі пошти.

> У списки доменів у тілі електронного листа можна внести тільки реальні домени верхнього рівня (TLD) відповідно до офіційної бази даних кореневої зони доменів верхнього рівня.

Щоб додати інші записи, у вікні **Додати** клацніть **Введіть кілька значень** і виберіть роздільник для використання. Це може бути новий рядок, кома або крапка з комою.

> Мета: виключити локальні IP-адреси інфраструктури з антиспаму, додавши їх у список ігнорованих IP-адрес
> Виберіть **Додаткові параметри (F5)** > **Сервер** > **Антиспам** > **Фільтрація й перевірка**.
> Поруч із пунктом **Список ігнорованих IP-адрес** клацніть **Змінити**.
> Клацніть **Додати** та вкажіть діапазон IP-адрес мережевої інфраструктури (формат діапазону IP-адрес *1.1.1.1-1.1.1.255*). За потреби можна продовжувати додавати діапазони (або одиничні IP-адреси) в список.
> Використовуйте повзунок **Є частиною внутрішньої інфраструктури**.

Технологія сірих списків та SPF

Додайте домен у білий список IP-адрес або налаштуйте автоматичний обхід сірих списків і SPF для IP-адрес у білому списку. Файли журналів див. в журналі захисту SMTP. Щоб скористатися цими параметрами, необхідно ввімкнути параметр Технологія сірих списків або SPF. Якщо використовується SPF, потрібно ввімкнути параметр **Автоматично відхиляти повідомлення, якщо перевірка SPF неуспішна** та (або) **Автоматично обходити сірі списки, якщо перевірку SPF пройдено**.

Використовувати антиспамні списки для автоматичного обходу сірих списків та SPF

Якщо ввімкнути цей параметр, списки дозволених та ігнорованих IP-адрес використовуватимуться разом із білими списками IP-адрес і доменів для автоматичного обходу сірих списків і SPF.

Білий список IP-адрес

Можна додати IP-адресу, IP-адресу з маскою і діапазон IP-адрес. Щоб змінити список, клацніть **Додати**, **Змінити** або **Видалити**. Окрім того, можна імпортувати спеціальний список із файлу, а не додавати вручну кожен окремий запис. Для цього клацніть **Імпортувати** та знайдіть файл із записами, які потрібно додати в список. Аналогічно, якщо потрібно експортувати наявний список у файл, у контекстному меню виберіть пункт **Експорт**.

> Білі списки мають вищій пріоритет, ніж чорні списки. Наприклад, якщо електронний лист одночасно містить адреси з білого й чорного списків, він поміщається в білий список. Тільки адреса останнього відправника разом з адресами в кількості, що не перевищує задану параметром Максимальна кількість перевірених адрес із заголовків "Received:", перевіряються за білими списками. Усі адреси перевіряються за локальними чорними списками.

Білий список доменів та IP-адрес

Цей параметр дає змогу вказувати домени (наприклад, domainname.local). Для керування списком використовуйте операції **Додати**, **Видалити** або **Видалити все**. Можна імпортувати спеціальний список із файлу, а не додавати вручну кожен окремий запис. Для цього клацніть **Імпортувати** та знайдіть файл із записами, які потрібно додати в список. Аналогічно, якщо потрібно експортувати наявний список у файл, у контекстному меню виберіть пункт **Експорт**.

> Сірі списки і SPF оцінюються модулем захисту передачі пошти й дозволяють додавати IP-адреси та домени в білі списки IP-адрес, а також в списки схвалених і ігнорованих IP-адрес. Проте якщо ви використовуєте правила SPF, жоден із цих білих списків не враховуватиметься.

Додаткові параметри Антиспам

Налаштуйте ці параметри для перевірки повідомлень на зовнішніх серверах (визначених як **RBL** (Realtime Blackhole List, чорний список реального часу) і **DNSBL** (DNS Blocklist, чорний список DNS) відповідно до попередньо визначених критеріїв. Сервери RBL отримують запити щодо IP-адрес, видобутих із заголовків *Received:*, а сервери DNSBL — щодо IP-адрес й доменів, видобутих із тексту повідомлення. Детальне пояснення див. в статтях щодо RBL і DNSBL.

Максимальна кількість перевірених адрес із заголовків Received:

Можна обмежити кількість IP-адрес, для яких виконуватиметься перевірка в модулі "Антиспам". Це стосується IP-адрес, які містяться в заголовках `Received: from`. За замовчуванням використовується значення 0. Це означає, що перевіряється лише IP-адреса останнього визначеного відправника.

Перевіряти адресу відправника за чорним списком кінцевих користувачів

Електронні листи, які надіслано не з поштових серверів (комп'ютерів, які внесено до списку поштових серверів), перевіряються на відсутність відправника в чорному списку. Цей параметр

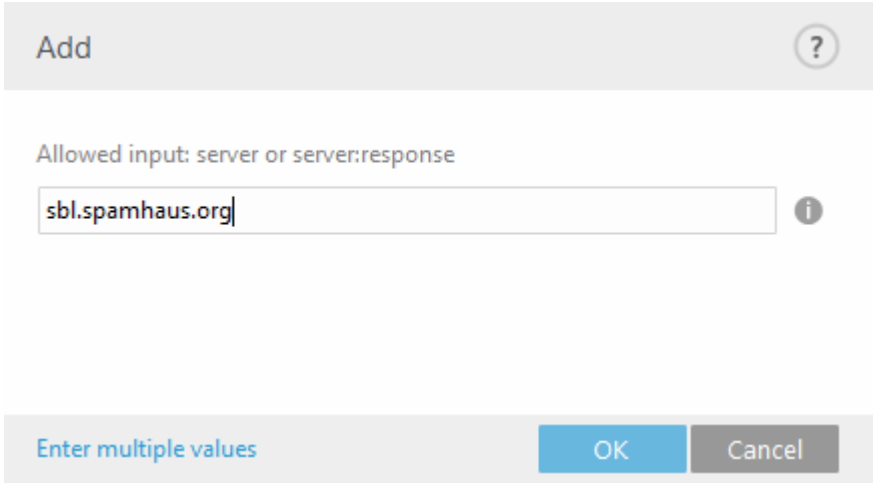
ввімкнено за замовчуванням. За потреби цей параметр можна вимкнути, проте в цьому разі повідомлення, надіслані не з поштових серверів, не перевірятимуться на відсутність відправника в чорному списку.

> Для результатів перевірки IP-адрес у заголовках `Received: from` зовнішні сторонні чорні списки мають пріоритет над чорними списками кінцевих користувачів. Усі IP-адреси (в кількості, що не перевищує вказану максимальну кількість адрес для перевірки) надсилаються для оцінки на зовнішні сторонні сервери.

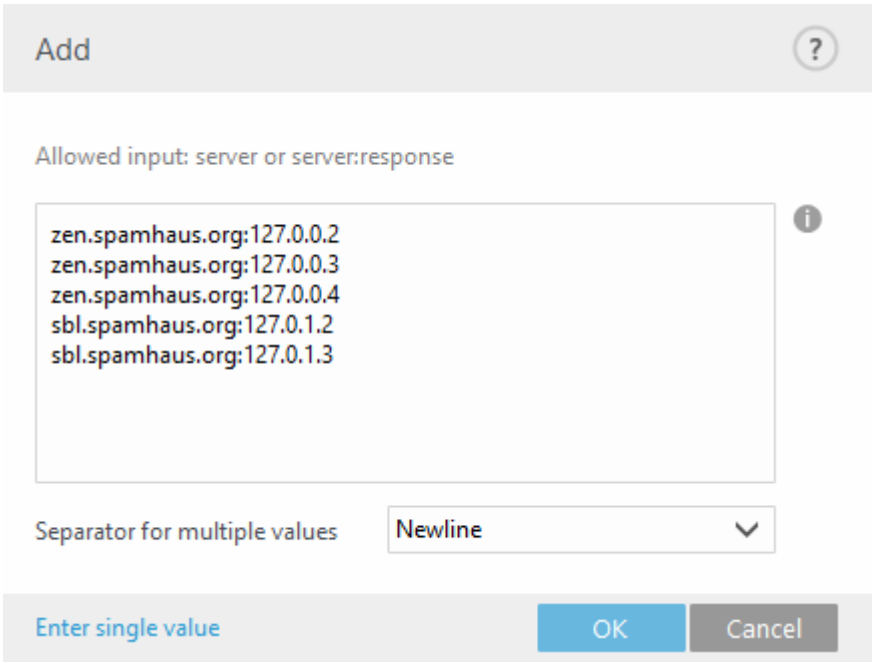
Додаткові сервери RBL

Список серверів RBL (Realtime Blackhole List, чорний список реального часу), на які надсилається запит для аналізу повідомлень.

> Під час додавання додаткових серверів RBL уведіть доменне ім'я сервера (наприклад, `sbl.spamhaus.org`). Воно працюватиме з будь-якими кодами відповіді, які підтримуються сервером.



Окрім того, можна вказати ім'я сервера з кодом відповіді у форматі `server:response` (наприклад, `zen.spamhaus.org:127.0.0.4`). Якщо ви використовуєте цей формат, рекомендуємо додавати кожне ім'я сервера й код відповіді окремо, щоб мати повний список. У вікні **Додати** клацніть **Введіть кілька значень**, щоб указати всі імена серверів з їхніми кодами відповіді. Записи мають бути подібними до наведеного нижче прикладу. Фактичні імена хостів і кодів серверів RBL можуть відрізнятися:



Обмеження виконання запиту RBL (у секундах)

Цей параметр дає змогу задавати максимальний час для запитів RBL. Використовуються відповіді RBL тільки з тих серверів RBL, які відповідають вчасно. Якщо для цього параметра задано значення "0", тайм-аут не застосовуватиметься.

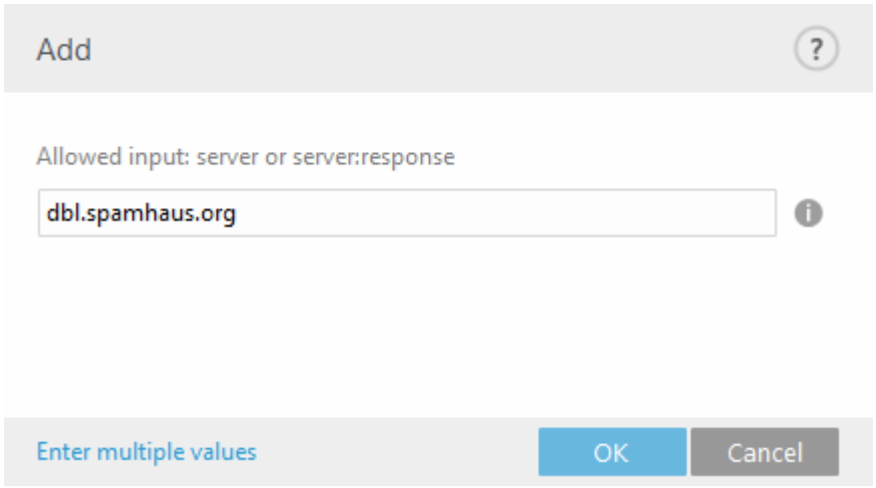
Максимальна кількість адрес, що перевіряються за RBL

Цей параметр дає змогу обмежувати кількість IP-адрес, які перевірятимуться на сервері RBL. Зверніть увагу, що загальна кількість запитів RBL дорівнюватиме кількості IP-адрес у заголовках "Received:" (але не більше максимальної кількості IP-адрес, для перевірки через запити до RBL), помноженої на кількість серверів RBL, указаних у списку RBL. Якщо для цього параметра задано значення "0", перевіряються необмежена кількість отриманих заголовків. Зверніть увагу, що для IP-адрес зі списку ігнорованих IP-адрес не враховуються обмеження кількості IP-адрес RBL.

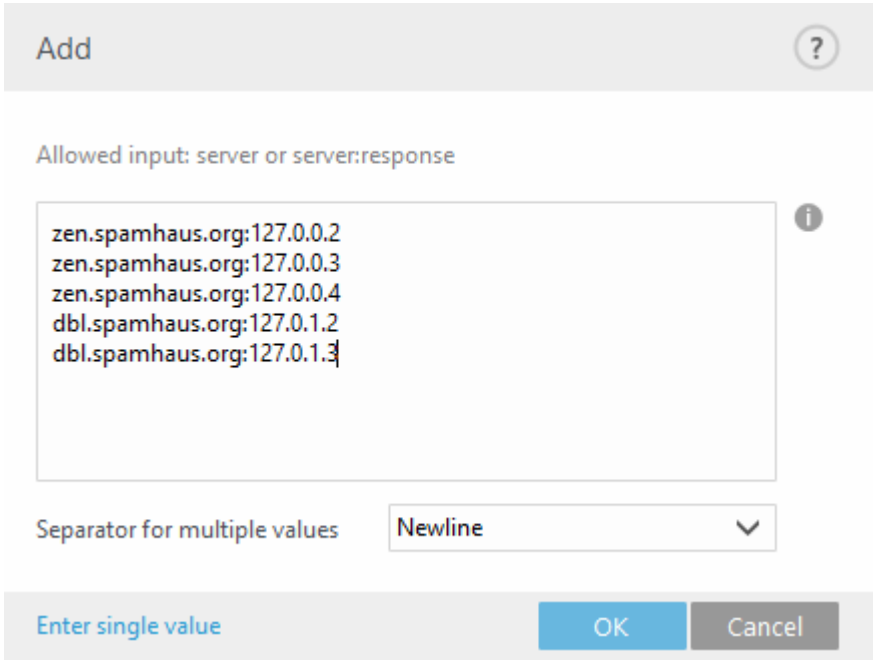
Додаткові сервери DNSBL

Список серверів DNS Blocklist (DNSBL), на які надсилаються запити щодо доменів і IP-адреси, видобуті з тексту повідомлення.

> Під час додавання додаткових серверів DNSBL уведіть доменне ім’я сервера (наприклад, `dbl.spamhaus.org`). Воно працюватиме з будь-якими кодами відповіді, які підтримуються сервером.



Окрім того, можна вказати ім’я сервера з кодом відповіді в такій формі: `server:response` (наприклад, `zen.spamhaus.org:127.0.0.4`). У цьому випадку рекомендуємо додавати кожне ім’я сервера й код відповіді окремо, щоб мати повний список. У вікні **Додати** клацніть **Введіть кілька значень**, щоб указати всі імена серверів з їхніми кодами відповіді. Записи мають бути подібними до наведеного нижче прикладу. Фактичні імена хостів і кодів серверів DNSBL можуть відрізнятися:



Обмеження виконання запиту DNSBL (у секундах)

Дає змогу задати максимальний час очікування для виконання всіх запитів DNSBL.

Максимальна кількість адрес, що перевіряються за DNSBL

Дає змогу обмежити кількість IP-адрес, які перевірятимуться за чорним списком сервера DNS.

Максимальна кількість доменів, що перевіряються за DNSBL

Дає змогу обмежити кількість доменів, які перевірятимуться за чорним списком сервера DNS.

Максимальний розмір повідомлення для сканування (кБ)

Обмежує сканування на наявність спаму для повідомлень, розмір яких більше за вказаний. Значення за замовчуванням (0) означає сканування повідомлень необмеженого розміру. Зазвичай для обмеження сканування на наявність спаму немає причин, проте якщо в деяких випадках потрібно задати обмеження, змініть значення на те, яке відповідає потрібному розміру. Якщо вибрано цей параметр, механізм антиспаму оброблятиме повідомлення, розмір яких не перебільшує вказаний, та ігноруватиме повідомлення більшого розміру.

Діє мінімальне граничне значення 12 kB. Якщо задати значення від 1 до 12, механізм антиспаму завжди зчитуватиме 12 kB.

Увімкнути тимчасове відхилення невизначених повідомлень

Якщо механізму антиспаму не вдасться визначити, чи є повідомлення спамом (повідомлення має певні підозрілі характеристики СПАМУ, яких недостатньо для його класифікації як СПАМУ, наприклад, перший електронний лист кампанії або електронний лист, надісланий з IP-адреси з діапазону адрес зі змішаними оцінками), цей параметр (якщо його ввімкнено) дає змогу ESET Mail Security тимчасово відхилити повідомлення (так само, як і у випадку застосування технології сірих списків) і продовжувати відхиляти його протягом певного періоду часу до настання однієї з таких подій:

• Після завершення вказаного періоду часу повідомлення приймається після наступної спроби доставки. Це повідомлення залишається з початковою класифікацією (СПАМ або БЕЗПЕЧНЕ ПОВІДОМЛЕННЯ).

• Хмарні служби антисмапу зберуть достатню кількість даних і можуть належним чином класифікувати повідомлення до завершення вказаного періоду часу.

Відхилене повідомлення не зберігається ESET Mail Security, оскільки його має повторно надсилати поштовий сервер відповідно до RFC SMTP.

Увімкнути надсилання тимчасово відхилених повідомлень на аналіз

Вміст повідомлення автоматично надсилається для подальшого аналізу. Це допоможе покращити класифікацію електронних листів у майбутньому.

Можливо, тимчасово відхилені повідомлення, надіслані на аналіз, фактично можуть бути безпечними. У поодиноких випадках тимчасово відхилені повідомлення можуть використовуватися для ручної оцінки. Увімкніть цю функцію, лише якщо немає ризиків несанкціонованого використання будь-яких потенційно конфіденційних даних.

Технологія сірих списків

Функція **Дозволити додавання до сірих списків** активує функцію, яка захищає користувачів від спаму за допомогою вказаного нижче методу: Транспортний агент буде повертати значення SMTP "temporarily reject" (тимчасове відхилення) (за замовчуванням 451/4.7.1) для будь-якого електронного листа, який отримано від нерозпізнаного відправника. Правомірний сервер спробує повторно надіслати повідомлення після затримки. Спам-сервери зазвичай не намагатимуться повторно надіслати повідомлення, оскільки через них переважно проходять тисячі адрес електронної пошти, тому заради економії часу повторне надсилання не виконується. Технологія сірих списків — це додатковий рівень захисту від спаму, який не впливає на можливості оцінки спаму в модулі "Антиспам".

Під час оцінювання джерела повідомлення з використанням технології сірих списків береться до уваги список затверджених IP-адрес, список ігнорованих IP-адрес, списки безпечних відправників і дозволених IP-адрес на сервері Exchange, а також параметри обходу антиспаму для поштової скриньки одержувача. Електронні листи з цих списків IP-адрес/відправників або електронні листи, доставлені в поштову скриньку з увімкненим параметром обходу антиспаму, не будуть перевірятися із застосуванням технології сірих списків.

Використовувати лише доменну частину адреси відправника

Ця функція ігнорує ім'я відправника в адресі електронної пошти. Береться до уваги тільки домен.

Синхронізувати бази даних сірих списків у кластері ESET

Сервери в кластері ESET у реальному часі обмінюються записами бази даних сірих списків. Коли на одному із серверів з'являється повідомлення, яке обробляється з використанням технології сірих списків, ця інформація розповсюджується ESET Mail Security на інші вузли в кластері.

Обмеження часу для початкової заборони підключення (хв)

Якщо повідомлення доставляється вперше й тимчасово відхиляється, цей параметр визначає період часу, протягом якого повідомлення завжди буде відхилятися (відлік починається з першого відхилення). Після завершення визначеного періоду часу повідомлення буде успішно отримано. Мінімальне значення для вводу: 1 хвилина.

Строк дії неперевірених підключень (год)

Цей параметр визначає мінімальний проміжок часу, протягом якого зберігатимуться дані триплета. Дійсний сервер має заново надіслати потрібне повідомлення до завершення цього періоду. Це значення має бути більшим, ніж значення параметра **Обмеження часу для початкової заборони підключення**.

Строк дії перевірених підключень (дн.)

Мінімальний період (у днях), протягом якого зберігатиметься інформація триплета, а електронні листи від визначеного відправника отримуватимуться без затримок. Це значення має бути більшим, ніж значення параметра **Термін дії неперевірених підключень**.

SMTP-відповідь (для тимчасово заборонених підключень)

Укажіть параметри **Код відповіді**, **Код стану** й **Текст відповіді**, які визначають відповідь тимчасової відмови SMTP, що надсилається на сервер SMTP, якщо повідомлення відхилено. Приклад відповіді SMTP про відхилення:

Код відповіді	Код стану	Повідомлення з відповіддю
451	4.7.1	Повторіть спробу пізніше

Для визначення відповіді SMTP можна також використовувати системні змінні.

Неправильний синтаксис кодів відповіді SMTP може призвести до неналежної роботи захисту з використанням технології сірих списків. У результаті, клієнтам можуть доставлятися повідомлення зі спамом або не доставлятиметься жодних повідомлень.

Усі повідомлення, оцінені з використанням технології сірих списків, записуються в журнал захисту SMTP.

SPF і DKIM

Структура політики фільтрації відправників (SPF) і DomainKeys Identified Mail (DKIM) — це методи перевірки, які перевіряють, що вхідні електронні листи з певних доменів авторизовані власником відповідного домену. Це допомагає захистити одержувачів від підроблених електронних листів. Окрім SPF і DKIM, ESET Mail Security використовує технологію DMARC (Domain-based Message (DMARC), Reporting and Conformance, ідентифікація повідомлень, створення звітів та визначення відповідності за доменним іменем).

SPF

Перевірка SPF дає змогу переконатися, що електронний лист надіслано надійним відправником. Щоб отримати список IP-адрес, у DNS виконується пошук записів SPF домену відправника. Якщо будь-яка з IP-адрес із записів SPF збігається з фактичною IP-адресою відправника, результатом перевірки SPF є **Pass**. Якщо фактична IP-адреса відправника не збігається, результатом є **Неуспішно**. Проте не для всіх доменів записи SPF указані в DNS. Якщо в DNS немає записів SPF, повертається результат **Not available**. Іноді запит DNS може завершуватися за тайм-аутом. У цьому разі повертається результат **Not available**.

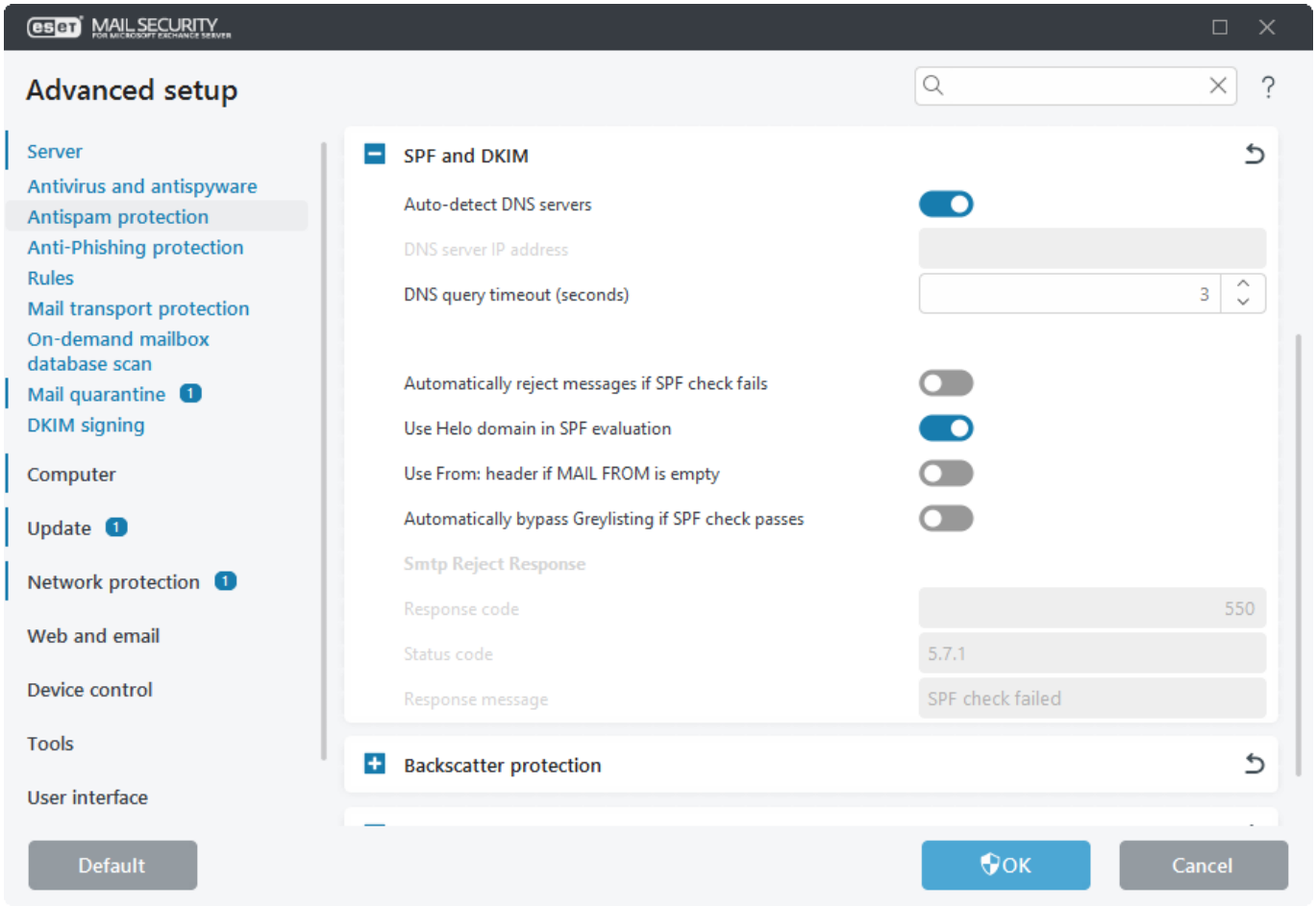
DKIM

Використовується організаціями для запобігання підробці електронних листів: у заголовки вихідних повідомлень додається цифровий підпис відповідно до стандарту DKIM. Зокрема, заголовки вихідної пошти вашого домену шифруються з використанням закритого ключа, а у записи DNS домену додається загальнодоступна версія ключа. ESET Mail Security може потім отримати загальнодоступний ключ для дешифрування вхідних заголовків і перевірки того, що повідомлення дійсно надійшло з вашого домену, а його заголовки не було змінено під час передавання.

> **i** Exchange Server 2010 і попередніх версій не повністю сумісний із DKIM, оскільки заголовки у вхідних повідомленнях із цифровим підписом можуть змінюватися під час перевірки DKIM.

DMARC

Технологію DMARC розроблено на основі наявних механізмів SPF і DKIM. Для оцінки дії **Результат DMARC** і **Застосувати політику DMARC** можна використовувати правила захисту передачі пошти.



Автоматично визначати DNS-сервери

Функція автоматичного визначення використовує параметри мережевого адаптера.

IP-адреса DNS-сервера

Щоб використовувати певні DNS-сервери для SPF та DKIM, уведіть IP-адресу (у форматі IPv4 або IPv6) потрібного DNS-сервера.

Час очікування на виконання DNS-запиту (секунди)

Укажіть тайм-аут для відповіді DNS.

Автоматично відхиляти повідомлення, якщо перевірку SPF не пройдено

Якщо відразу не вдається виконати перевірку SPF, електронний лист може бути відхилено ще до його завантаження.

Перевірка SPF виконується на рівні SMTP. Однак її можна відхилити автоматично на рівні SMTP або під час оцінювання правил.
Якщо використовується автоматичне відхилення на рівні SMTP, відхилені повідомлення неможливо записувати в журнал подій. Це зумовлено тим, що запис у журнал виконується дією правила, а автоматичне відхилення виконується безпосередньо на рівні SMTP перед оцінюванням правила. Оскільки повідомлення будуть відхилені до оцінювання правил, під час оцінювання правила немає даних для запису в журнал.
У журнал можна записувати відхилені повідомлення, але тільки якщо їх відхилено дією правила. Щоб відхилити повідомлення, які не пройшли перевірку SPF, і записувати такі відхилені повідомлення в журнал, вимкніть параметр **Автоматично відхиляти повідомлення, якщо перевірка SPF неуспішна**, і створіть таке правило для **захисту передачі пошти**:
Стан
• Тип: Результат SPF
• Операція: є
• Параметр: Невдача
Дії
• Тип: Відхилити повідомлення
• Тип: Реєструвати як подію

Використовувати домен Helo в оцінюванні SPF

Ця функція використовує домен HELO для оцінювання SPF. Якщо домен HELO не вказано, використовуйте натомість ім’я хоста комп’ютера.

Використовувати заголовок From:, якщо значення MAIL FROM пусте

Заголовок MAIL FROM може бути пустим. Його можна легко підробити. Якщо цей параметр увімкнено й заголовок MAIL FROM пустий, повідомлення завантажується і замість цього заголовка використовується заголовок From:.

Автоматично обходити сірий список, якщо перевірку SPF пройдено

Якщо перевірка SPF повернула результат "Pass", немає потреби використовувати технологію сірих списків.

Відповідь SMTP про відхилення

Можна вказати параметри **Код відповіді**, **Код стану** й **Текст відповіді**, які визначають відповідь тимчасової відмови SMTP, що надсилається на сервер SMTP, якщо повідомлення відхилено. Можна ввести текст відповіді в такому форматі:

Код відповіді	Код стану	Повідомлення з відповіддю
550	5.7.1	Не вдалося виконати перевірку SPF

Захист від несправжніх сповіщень про стан доставки

Несправжні сповіщення про стан доставки — це неправильно адресовані звіти про недоставку, які надсилаються поштовими серверами. Вона є побічним ефектом спаму. Якщо поштовий сервер одержувача відхиляє повідомлення спаму, звіт про недоставку (NDR, Non-Delivery Report)

надсилається уявному відправнику (на ту адресу електронної пошти, яку підроблено з метою видати її за адресу відправника оригінального повідомлення спаму), а не фактичному відправнику спаму. Власник адреси електронної пошти отримує повідомлення про недоставку, навіть якщо він не був пов'язаний із первісним спам-повідомленням. Саме тоді активується **захист від несправжніх сповіщень про стан доставки**. Функція захисту від несправжніх сповіщень про стан доставки в ESET Mail Security дає змогу блокувати надсилання звітів про недоставку спаму в почтові скриньки користувачів у вашій організації.

Якщо у вас **увімкнуто перевірку стану доставки**, необхідно вказати **генератор підписів** (рядок довжиною не менше 8 символів, на зразок парольної фрази). Функція захисту від несправжніх сповіщень про стан доставки в ESET Mail Security записує `X-Eset-NDR: <hash>` в заголовок кожного вихідного електронного листа. `<hash>` — це зашифрований підпис, який містить указаний вами **генератор підписів**.

Якщо не вдається доставити надійний електронний лист, поштовий сервер зазвичай отримує звіт про недоставку, який ESET Mail Security перевіряє через пошук запису `X-Eset-NDR: <hash>` у заголовках. Якщо запис `X-Eset-NDR:` присутній і підпис `<hash>` збігається, відправнику надійного електронного листа надсилається звіт про недоставку з повідомленням про помилку доставки. Якщо в заголовку немає `Eset-NDR:` або підпис `<hash>` неправильний, то повідомлення ідентифікується як несправжнє сповіщення про стан доставки. Звіт про недоставку відхиляється.

Автоматично видаляти повідомлення NDR, якщо перевірку не пройдено

Якщо відразу не вдається перевірити звіт про недоставку, електронний лист може бути відхилено ще до його завантаження.

Відомості про активність **захисту від несправжніх сповіщень про стан доставки** див. в журналі захисту SMTP.

Захист від підміни відправника

Підміна відправника електронної пошти — це поширена практика, коли зловмисник намагається обманути одержувача через підробку імені або адреси електронної пошти відправника. Для одержувача підроблений електронний лист не відрізняється від автентичного. Це становить ризик. Один із типів підробки відправника стосується випадків, коли зловмисник видає себе за директора компанії.

Зазвичай такі електронні листи не викликають підозр у співробітників, а це дає зловмиснику можливість успіху. Зловмисники видають себе не тільки за директорів. Вони можуть видавати себе за будь-якого реального відправника. Зазвичай це один із користувачів у домені Active Directory вашої організації. Підроблений електронний лист є дуже переконливим для одержувача, який не підозрює підробки. Таким чином зловмисники легко входять у довіру.

ESET Mail Security забезпечує захист від підміни відправника електронної пошти. Захист від підміни відправника кількома методами перевіряє, чи дійсна інформація про відправника.

Захист від підміни відправника шукає домен, що міститься в полі заголовка електронного листа «Від:» і відправнику конверта, а потім порівнює знайдений домен із доменами в списках. Якщо домен відрізняється, повідомлення вважається дійсним (не підробленим) і далі обробляється іншими рівнями захисту ESET Mail Security. Якщо домен знайдено в списку,

відправник може бути підробленим і потребує додаткової перевірки.

Залежно від цього параметра виконується подальша перевірка (перевірка SPF, IP-адреса конверта перевіряється за списками IP-адрес) або повідомлення автоматично вважається підробленим. Якщо перевірка SPF повернула результат "Успішно" або IP-адреса конверта збігається з IP-адресою зі списку, повідомлення вважатиметься автентичним. В іншому разі воно вважатиметься підробленим. Дія, яка виконуватиметься по відношенню до підробленого повідомлення.

Захист від підміни відправника можна використовувати двома способами:

• Увімкніть **захист від підміни відправника**, налаштуйте його параметри й за потреби вкажіть домени або списки IP-адрес. Дія за замовчуванням, що застосовуватиметься до підроблених повідомлень: **Відправити повідомлення в карантин**. Щоб змінити цю дію, відкрийте розширені параметри Захист передачі пошти.

• Використовуйте правила захисту передачі пошти: Умови **Результат перевірки SPF: заголовок From** або **Результат порівняння відправника конверта й заголовка From**, відповідно до яких застосовується вибрана дія. Правила дають вам змогу вказати додаткові параметри й комбінації, якщо потрібно визначити певну поведінку щодо підроблених електронних листів.

Якщо використовується параметр **"Захист від підміни відправника"** або вибрано тип дії правила **"Реєструвати як подію"**, усі повідомлення, оцінювані функцією **захисту від підміни відправника**, записуються у файли журналу. Аналогічним чином підроблені електронні листи можна знайти в поштовому карантині, якщо в розділі Захист передачі пошти або в правилах для дії визначено **Відправити повідомлення в карантин**.

Увімкнути захист від підміни відправника

Активуйте захист від підміни відправника, щоб запобігти атакам, які мають на меті ввести одержувачів повідомлення в оману відносно джерела повідомлення (підроблений відправник).

Увімкнути вхідні електронні листи з моїм власним доменом в адресі відправника

Дозвольте подальшу перевірку повідомлень, які в заголовку електронного листа "From:" або у відправнику конверта містять власний домен (такі повідомлення можуть бути підроблені).

• **Тільки якщо вони пройшли перевірку SPF** (має бути ввімкнуто SPF). Якщо SPF повертає результат "Pass", повідомлення вважається автентичним і оброблюється для доставки. Якщо SPF повертає результат "Неуспішно", повідомлення вважатиметься підробленим (застосовується відповідна визначена дія). Можна ввімкнути Автоматично відхиляти повідомлення, якщо перевірка SPF неуспішна.

• **Тільки якщо IP-адреса входить до списку IP-адрес інфраструктури**: IP-адреса конверта порівнюється з IP-адресами в списку (список ваших власних IP-адрес і список ігнорованих IP-адрес із позначенням **Є частиною внутрішньої інфраструктури**). Якщо IP-адреси збігаються, повідомлення є автентичним і оброблюється для доставки. Якщо IP-адреси немає в цих списках, повідомлення вважатиметься підробленим (застосовується відповідна визначена дія).

• **Ніколи**: якщо вхідне повідомлення містить власний домен у заголовку електронного

листа або відправнику конверта, воно автоматично вважається підробленим без подальшої перевірки. До повідомлення буде застосовано дію. Доступні дії див. в розділі Захист передачі пошти.

Автоматично завантажувати мої власні домени зі списку допустимих доменів

Наполегливо рекомендуємо ввімкнути цей параметр, щоб зберегти найвищий рівень захисту. Таким чином, домени та IP-адреси з вашої інфраструктури враховуються під час оцінювання функцією захисту від підміни відправника.

Список моїх власних доменів

Ці домени вважаються вашими власними. Додайте домени, які будуть використовуватися під час оцінювання, на додаток до автоматично завантажених доменів з Active Directory. Домени відправників порівнюватимуться з доменами в цих списках. Якщо не буде знайдено такого домену, повідомлення вважатиметься автентичним. Якщо домен буде знайдено в списку, подальша перевірка виконуватиметься відповідно до параметра **Увімкнути вхідні електронні листи з моїм власним доменом в адресі відправника**.

Список моїх власних IP-адрес

IP-адреси, які вважаються надійними. Додайте IP-адреси, які використовуватимуться під час оцінювання, на додаток до IP-адрес у списку ігнорованих IP-адрес, що мають позначку **Є частиною внутрішньої інфраструктури**. IP-адреса конверта відправника порівнюється з IP-адресами в цих списках. Якщо IP-адреса конверта є в цих списках, повідомлення вважатиметься дійсним. Якщо IP-адреси немає в цих списках, повідомлення вважатиметься підробленим (застосовується відповідна визначена дія).

Захист від фішинг-атак

Фішинг — це спроба отримати таку конфіденційну інформацію, як імена користувачів, паролі, дані банківського рахунку або кредитної картки, а також PIN-коди, електронною поштою або на веб-сторінках, які зловмисники намагаються представити як довірені. Зазвичай така активність пов’язана із шахрайством. Це форма соціотехнік (маніпулювання користувачами для отримання конфіденційної інформації).

ESET Mail Security містить захист від фішинг-атак, який не дозволяє користувачам отримувати доступ до веб-сторінок, для яких відомо, що вони використовуються для фішинг-атак. Якщо електронні листи містять посилання на фішингові веб-сайти, ESET Mail Security використовує покращений синтаксичний аналізатор, який виявляє такі посилання (URL-адреси) в темі й тексті вхідних електронних листів.

Посилання перевіряються в базі даних фішингових адрес. Якщо результат оцінювання є позитивним, електронний лист вважається фішинговим повідомленням. ESET Mail Security застосовує до нього дію, яка визначена в параметрі **Дія, яку потрібно виконати з фішинговим повідомленням** для кожного рівня захисту (Захист передачі пошти, Захист бази даних поштової скриньки й Сканування бази даних поштових скриньок за вимогою). Також виконуються дії правила.

Підтримувані стандарти формату електронних листів:

- Звичайний текст
- Лише HTML
- MIME
- Багатокомпонентне повідомлення MIME (електронний лист, що містить як текст у форматі HTML, так і звичайний текст)

Підтримувані об’єкти HTML:

Фішингові повідомлення можуть містити об’єкти HTML для уникнення виявлення обробником функції "Захист від фішинг-атак". Захист від фішинг-атак також аналізує і перетворює символи HTML для пошуку й правильної оцінки прихованих URL-адрес.

Один символ може бути представлений в різних формах. Наприклад, крапка може бути представлена в таких формах:

Спосіб відображення посилань в електронному листі для користувача	Значення	Приховані посилання, що містяться в тексті повідомлення	Тип
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	символ
http://www.example-phishing-domain.com/Fraud	&period;	http://www.example-phishing-domain.com/Fraud	ім’я об’єкта
http://www.example-phishing-domain.com/Fraud	&#x0002E;	http://www.example-phishing-domain.com/Fraud	шістнадцяткове число об’єкта
http://www.example-phishing-domain.com/Fraud	&#46;	http://www.example-phishing-domain.com/Fraud	десяткове число об’єкта

Щоб переглядати активність захисту електронної пошти від фішинг-атак, установіть прапорець **Файли журналу** > Журнал захисту поштового сервера. Журнал містить інформацію про фішингові посилання, знайдені в електронних листах.

Повідомити про шахрайський сайт

Щоб повідомити ESET про фішинговий або зловмисний веб-сайт, клацніть Звіт.

Правила

Правила дають змогу вручну визначати умови фільтрування електронної пошти й призначати дії, які будуть застосовуватися до відфільтрованих електронних листів. Окрім того, можна визначати різні умови й дії окремо для захисту передачі пошти, захисту бази даних поштових скриньок і сканування бази даних поштових скриньок на вимогу. Це корисно, оскільки для кожного типу захисту використовуються різні підходи для обробки повідомлень (особливо це стосується захисту передачі пошти).

> Доступність правил Захист бази даних поштової скриньки, Сканування бази даних поштових скриньок за вимогою і Захист передачі пошти у вашій системі залежить від того, яку версію Microsoft Exchange Server інстальовано на сервері з ESET Mail Security.

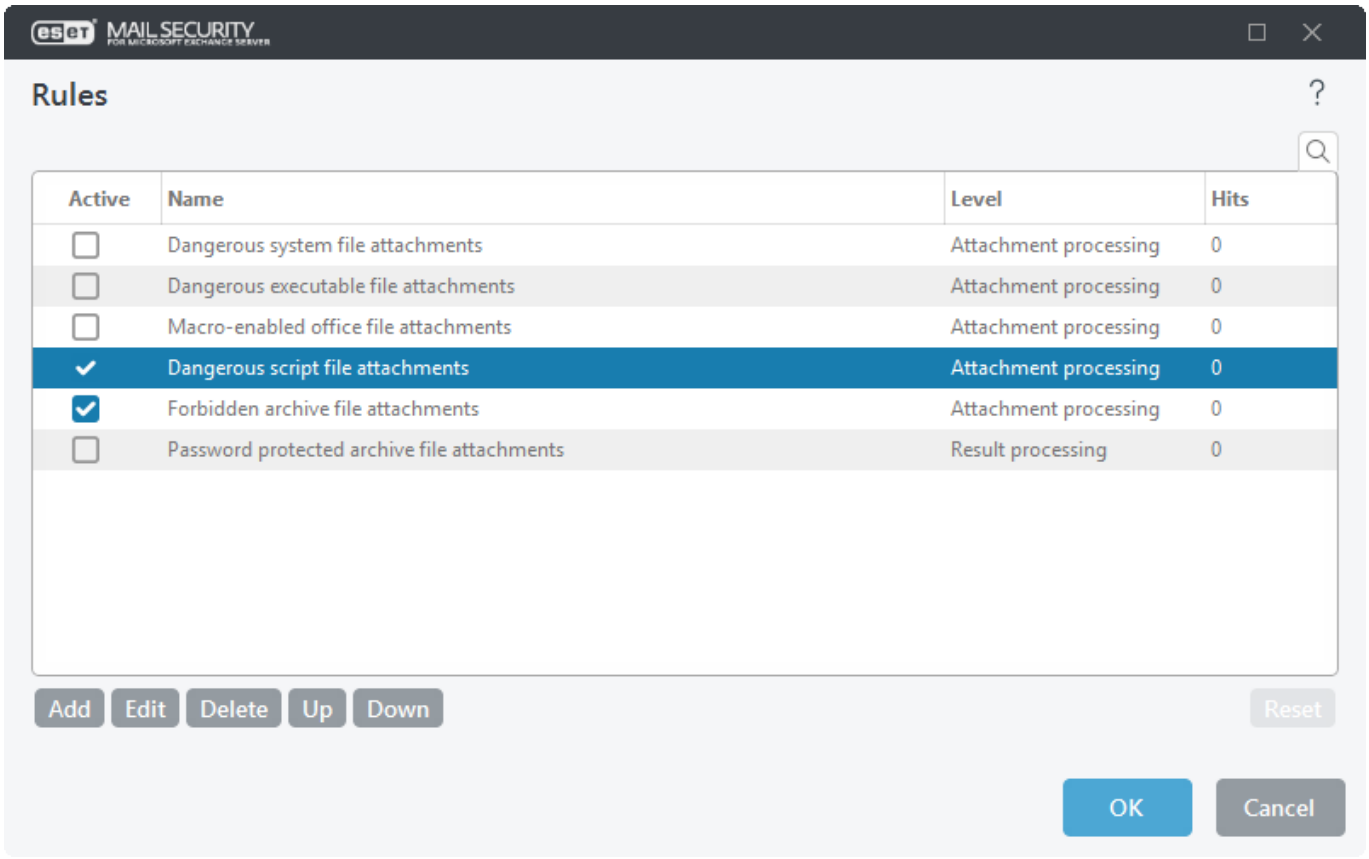
Неправильно визначені правила **сканування бази даних поштових скриньок за вимогою** можуть призвести до незворотних змін у базах даних поштових скриньок. Перед першим запуском сканування бази даних поштових скриньок на вимогу із застосуванням правил переконайтеся, що маєте найновіші резервні копії бази даних поштових скриньок. Настійно рекомендуємо перевіряти виконання правил відповідно до ваших очікувань. Для перевірки визначте правила тільки з дією **Реєструвати як подію**. Це потрібно лише тому, що інші дії можуть унести зміни до бази даних поштових скриньок. Якщо ви задоволені перевіркою, можна додати правило з дією видалення, наприклад **Видалити вкладення**.

Правила класифікуються за трьома рівнями й оцінюються в такому порядку:

- **Правила фільтрації** (1): правила, які оцінюються до сканування модулями антиспаму, антивірусом й захистом від фішинг-атак.
- **Правила обробки вкладень** (2): оцінюються під час сканування антивірусом.
- **Правила обробки результатів** (3): правила, які оцінюються до сканування модулями антиспаму, антивірусом й захистом від фішинг-атак.

Правила з однаковим рівнем оцінювання переглядаються в порядку, відображеному у вікні правил. Порядок можна змінювати лише для правил того самого рівня. Якщо є кілька правил фільтрації, можна змінити порядок їхнього застосування. Зверніть увагу, що правила **Обробка вкладень** не можна перемістити перед правилами **Фільтрація**, оскільки кнопки **Угору**/**Униз** не працюють. Не можна змішувати правила різних **рівнів**.

У стовпці **Збіги** відображається кількість успішно застосованих правил. Якщо зняти прапорець (зліва від імені кожного правила), відповідне правило деактивується, доки ви знову не встановите прапорець.



Клацніть **Скинути**, щоб скинути лічильник для вибраного правила (стовпчик **Збіги**). Пункт **Переглянути** дає змогу переглянути конфігурацію, призначену з політики ESET PROTECT.

Зазвичай, якщо умови правила виконано, то оцінювання припиняється для наступних правил, які мають нижчий пріоритет. Проте за потреби для продовження оцінювання можна скористатися спеціальною дією правила, яка називається **Оцінити інші правила**.

Правила перевіряються для повідомлення під час його обробки функціями захисту передачі пошти, захисту бази даних поштових скриньок або сканування бази даних поштових скриньок за вимогою. Кожен рівень захисту має окремий набір правил.

Якщо умови правила захисту передачі пошти або сканування бази даних поштових скриньок за вимогою збігаються, значення в лічильнику правила може підвищитися на 2 або більше. Це зумовлено тим, що ці рівні захисту мають доступ до тексту й вкладених файлів повідомлення окремо, тому правила застосовуються до кожної частини окремо. Правила захисту бази даних поштових скриньок також застосовуються під час сканування у фоновому режимі (наприклад, коли ESET Mail Security виконує сканування поштової скриньки після завантаження нового обробника виявлення), що може призвести до збільшення значення лічильника правил ("Збіги").

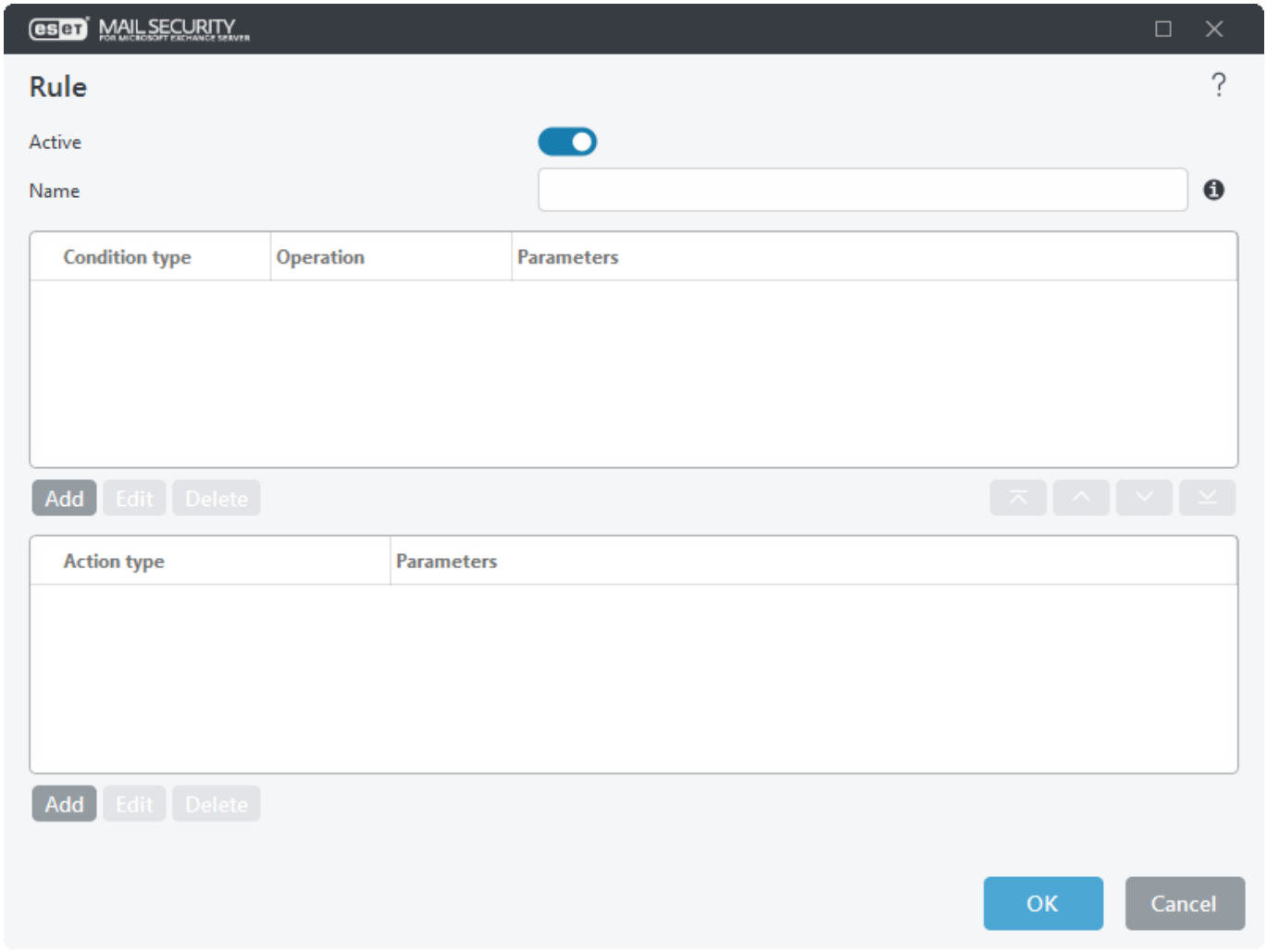
Майстер правил

1. Клацніть **Додати** (в середині). Відкриється вікно Умова правила, де можна вибрати тип умови, операцію і значення. Спочатку визначте умови, а потім дії.

Можна визначити кілька умов. Якщо ви використовуєте кілька умов, то правило застосовуватиметься тільки тоді, коли виконано всі умови. Усі умови підключаються за допомогою логічного оператора **AND**. Якщо хоча б одну умову не виконано, результат оцінки буде негативним і дія, визначена правилом, не застосовуватиметься.

2. Клацніть **Додати** (в нижній частині), щоб додати дію правила.

Для одного правила можна додати кілька дій.



3. Якщо визначено умови й дії, уведіть **ім’я** для правила (за яким ви будете розпізнавати це правило). Це ім’я відображатиметься в списку правил. "Ім’я" — це обов’язкове поле. Якщо його виділено червоним кольором, у текстовому полі введіть назву правила й клацніть **OK**, щоб створити правило. Червоне виділення не зникає, навіть якщо ім’я правила введено. Воно зникає, коли ви клацнете **OK**.

4. Щоб підготувати правила, але використовувати їх пізніше, клацніть повзунок поруч із пунктом **Активний**, щоб деактивувати правило. Щоб активувати правило, установіть прапорець поруч із правилом, яке потрібно активувати.

Якщо додати нове правило або внести зміни в наявне, під час повторного сканування повідомлення автоматично почнуть використовуватися нові або змінені правила.

Перегляньте приклади правил, щоб дізнатися про варіанти використання правил.

Умова правила

Майстер "Умова правил" дає змогу додавати умови для правила. У розкривному меню виберіть **тип** умови й **операцію**. Список операцій змінюється залежно від вибраного типу правила. Після цього виберіть **Параметр**. Поля параметрів змінюються залежно від типу правила та операції.

Наприклад, виберіть Розмір файлу > більше ніж і в полі Параметр укажіть 10 МБ. Якщо задано таке налаштування, усі файли, розмір яких перевищує 10 МБ, будуть оброблятися з

використанням указаних вами дій правила. З цієї причини потрібно вказати дію, яка виконуватиметься в разі спрацювання певного правила, якщо ви ще цього не зробили, коли вказували параметри для цього правила.

Можна імпортувати спеціальний список із файлу, а не додавати вручну кожен окремий запис. Для цього клацніть правою кнопкою миші в середині вікна і в контекстному меню виберіть пункт **Імпортувати**. Потім знайдіть файл (*.xml* або *.txt* із записами, розділеними символами нового рядка), який потрібно додати в список. Аналогічно, якщо потрібно експортувати наявний список у файл, у контекстному меню виберіть пункт **Експорт**.

Окрім того, можна вказати **Регулярний вираз** і вибрати **операція: відповідає регулярному виразу** або **не відповідає регулярному виразу**.

ESET Mail Security використовує std::regex. Інструкції зі створення регулярних виразів див. в розділі Синтаксис ECMAScript. Синтаксис регулярного виразу не є чутливим до регістру (це стосується й результатів пошуку).

Можна визначити кілька умов. У цьому разі для застосування правила мають бути виконані всі умови. Усі умови підключаються за допомогою логічного оператора **AND**. Якщо хоча б одну умову не виконано, результат оцінки буде негативним і дія, визначена правилом, не застосовуватиметься.

Указані нижче типи умов доступні для захисту передачі пошти, захисту бази даних поштових скриньок і сканування бази даних поштових скриньок за вимогою (деякі параметри можуть не відображатися залежно від раніше вибраних умов):

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Тема	✔	✔	✔	Застосовується до повідомлень, які містять або не містять певний рядок (або регулярний вираз) у темі.
Відправник	✔	✔	✔	Застосовується до повідомлень, надісланих визначеним відправником.
Відправник конверта (відправник SMTP)	✔	✔	✔	атрибут MAIL FROM конверта, який використовується під час підключення SMTP. Використовується також для перевірки SPF.
IP-адреса відправника	✔	✔	✔	Застосовується до повідомлень, надісланих із певної IP-адреси.
Домен відправника конверта або домен відправника	✔	✔	✔	Застосовується до повідомлень від відправника, який має певний домен у своїх адресах електронної пошти.
Домен SMTP-відправника	✔	✔	✔	Застосовується до повідомлень від відправника, який має певний домен у своїх адресах електронної пошти.

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Заголовок From – адреса	✔	✔	✔	значення "From:", що міститься в заголовках повідомлень. Це адреса, яка відображається для одержувача. Не виконується перевірка на предмет того, що систему, яка надіслала електронний лист, авторизовано для надсилання від імені користувача цієї адреси. Часто використовується для підміни відправника.
Заголовок From – ім’я, що відображається	✔	✔	✔	значення "From:", що міститься в заголовках повідомлень. Це ім’я, що відображається для одержувача. Не виконується перевірка на предмет того, що систему, яка надіслала електронний лист, авторизовано для надсилання від імені користувача цієї адреси. Часто використовується для підміни відправника.
Одержувач	✔	✔	✔	Застосовується до повідомлень, надісланих певному одержувачу.
Організаційні одиниці одержувача	✔	✔	✔	Застосовується до повідомлень, надісланих одержувачу певної організаційної одиниці.
Результат перевірки одержувача	✔	✔	✔	Застосовується до повідомлень, надісланих одержувачу, перевіреному в Active Directory.
Назва вкладення	✔	✔	✔	Застосовується до повідомлень, що містять вкладення з певним іменем.
Розмір вкладення	✔	✔	✔	Застосовується до повідомлень із вкладенням, яке не відповідають указаному розміру, розташовані в межах указаного діапазону розмірів або перевищують указаний розмір.
Тип вкладення[1]	✔	✔	✔	Застосовується до повідомлень із вкладеними файлами певного типу. Типи файлів розподілено за групами для полегшення вибору. Можна вибрати кілька типів файлів або цілі категорії. ESET Mail Security виявляє фактичний тип файлу незалежно від розширення. Те саме стосується вмісту архіву.

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Розмір повідомлення	✔	✔	✔	Застосовується до повідомлень із вкладеннями, які не відповідають указаному розміру, знаходяться в межах указаного діапазону розміру або перевищують указаний розмір.
Поштова скринька	✔	✔	✔	Застосовується до повідомлень, розташованих у певний поштовій скриньці.
Заголовки повідомлень	✔	✔	✔	Застосовується до повідомлень із певними даними, які містяться в заголовку повідомлення.
Тіло повідомлення	✔	✔	✔	У тілі повідомлення виконується пошук указаної фрази. Щоб видалити HTML-теги, атрибути й значення і залишити лише текст, можна скористатися функцією "Вилучити HTML-теги". Після цього буде виконано пошук у тілі повідомлення.
Внутрішнє повідомлення	✔	✔	✔	Застосовується залежно від того, чи є повідомлення внутрішнім.
Вихідне повідомлення	✔	✔	✔	Застосовується до вихідних повідомлень.
Підписане повідомлення	✔	✔	✔	Застосовується до підписаних повідомлень.
Зашифроване повідомлення	✔	✔	✔	Застосовується до зашифрованих повідомлень.
Результат сканування на наявність спаму	✔	✔	✔	Застосовується до повідомлень, позначених або не позначених як "Безпечне повідомлення" або "Спам".
Результат антивірусного сканування	✔	✔	✔	Застосовується до повідомлень, позначених як шкідливі або не шкідливі.
Результат сканування для захисту від фішинг-атак	✔	✔	✔	Застосовується до повідомлень, оцінених як фішингові.
Час отримання	✔	✔	✔	Застосовується до повідомлень, отриманих до або після певної дати або впродовж певного діапазону дат.
Містить архів, захищений паролем	✔	✔	✔	Застосовується до повідомлень із архівними вкладеннями, захищеними паролем.

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Містить пошкоджений архів	✔	✔	✔	Застосовується до повідомлень із пошкодженими архівними вкладеннями (які, найімовірніше, неможливо відкрити).
Вкладення є архівом, захищеним паролем	✔	✔	✔	Застосовується до вкладень, захищених паролем.
Вкладення є пошкодженим архівом	✔	✔	✔	Застосовується до пошкоджених вкладень (які, найімовірніше, неможливо відкрити).
Ім’я папки	✔	✔	✔	Застосовується до повідомлень, розташованих у певній папці. Якщо папка не існує, вона буде створена. Це не стосується загальнодоступних папок.
DKIM результат	✔	✔	✔	Застосовується до повідомлень, які пройшли або не пройшли перевірку DKIM (альтернативно, якщо така можливість недоступна).

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
SPF результат	✔	✔	✔	Застосовується до повідомлень, для яких отримано такий результат перевірки SPF: • **Успішно**: для цієї IP-адреси дозволено надсилати повідомлення з домену (кваліфікатор SPF: "+") • **Неуспішно**: запис SPF не містить сервера-відправника або IP-адресу надсилання (кваліфікатор SPF: "-") • **Незначна помилка**: для цієї IP-адреси може бути дозволено або не дозволено надсилати повідомлення з домену (кваліфікатор SPF: "~") • **Нейтральний**: означає, що власник домену, зазначений у записі SPF, не хоче підтвердити, що IP-адресу авторизовано для надсилання повідомлення з домену (кваліфікатор SPF: "?") • **Недоступно**: результат SPF None означає, що домен не опублікував жодного запису, або що на основі цієї ідентичності не можна визначити жодного домену відправника, доступного для перевірки. Більш докладні відомості про SPF див. в документі RFC 4408. Якщо ви використовуєте результат SPF, для правил не враховуються білі списки фільтрації та перевірки.
DMARC результат	✔	✔	✔	Застосовується до повідомлень, які пройшли або не пройшли перевірку SPF чи DKIM або з використанням обох методів (альтернативно, якщо така можливість недоступна).
Має зворотний запис DNS	✔	✔	✔	Застосовується до повідомлень із доменом відправника, який має зворотний запис DNS.
NDR результат	✔	✔	✔	Застосовується до повідомлень, які не вдалося верифікувати за допомогою NDR.

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
результат перевірки SPF: заголовок From	✔	✔	✔	Застосовується до повідомлень, для яких отримано такий результат перевірки SPF: • **Успішно**: для цієї IP-адреси дозволено надсилати повідомлення з домену (кваліфікатор SPF: "+") • **Неуспішно**: запис SPF не містить сервера-відправника або IP-адресу надсилання (кваліфікатор SPF: "-") • **Незначна помилка**: для цієї IP-адреси може бути дозволено або не дозволено надсилати повідомлення з домену (кваліфікатор SPF: "~") • **Нейтральний**: означає, що власник домену, зазначений у записі SPF, не хоче підтвердити, що IP-адресу авторизовано для надсилання повідомлення з домену (кваліфікатор SPF: "?") • **Недоступно**: результат SPF None означає, що домен не опублікував жодного запису, або що на основі цієї ідентичності не можна визначити жодного домену відправника, доступного для перевірки. Більш докладні відомості про SPF див. в документі RFC 4408. Якщо ви використовуєте результат SPF, для правил не враховуються білі списки фільтрації та перевірки.
Результат порівняння заголовків відправника конверта та From	✔	✔	✔	Порівнює домени, які містяться в полі заголовку електронного листа "From:" полі заголовка електронного листа й відправника конверта, зі списками доменів.

Назва умови	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Результат SPF HELO	✔	✔	✔	Застосовується до повідомлень, для яких отримано такий результат перевірки HELO: • **Успішно**: для цієї IP-адреси дозволено надсилати повідомлення з домену (кваліфікатор SPF: "+") • **Неуспішно**: запис SPF не містить сервера-відправника або IP-адресу надсилання (кваліфікатор SPF: "-") • **Незначна помилка**: для цієї IP-адреси може бути дозволено або не дозволено надсилати повідомлення з домену (кваліфікатор SPF: "~") • **Нейтральний**: означає, що власник домену, зазначений у записі SPF, не хоче підтвердити, що IP-адресу авторизовано для надсилання повідомлення з домену (кваліфікатор SPF: "?") • **Недоступно**: результат SPF None означає, що домен не опублікував жодного запису, або що на основі цієї ідентичності не можна визначити жодного домену відправника, доступного для перевірки. Більш докладні відомості про SPF див. в документі RFC 4408. Якщо ви використовуєте результат SPF, для правил не враховуються білі списки фільтрації та перевірки.

[1] Умова **Тип вкладення** має відоме обмеження: обробник виявлення ESET Mail Security не може виявити додаткові невеликі текстові файли розміром менше 10 байт у кодуванні ASCII/ANSI.

Тип умови має такі **операції**:

• **Рядок:** "є", "не є", "містить", "не містить", "збігається", "не збігається", "в", "не в", "у списку", "не в списку", "відповідає регулярному виразу", "не відповідає регулярному виразу"

• **Число:** "менше", "більше", "у діапазоні"

• **Текст:** "містить", "не містить", "збігається", "не збігається"

• **Дата-час:** "менше", "більше", "у діапазоні"

• **Перелічення:** "є", "не є", "в", "не в"

Якщо **назвою вкладення** або **типом вкладення** є файл Microsoft Office, він обробляється ESET Mail Security як архів. Це означає, що його вміст видобуто, а кожен файл, що міститься у файловому архіві Office (наприклад, *.docx, .xlsx, .xltx, .pptx, .ppsx, .potx* тощо), сканується окремо.

Якщо для **захисту передачі пошти й захисту баз даних поштових скриньок** вимкнути **Захист від вірусів** у меню Параметри або в розділі **Додаткові параметри** (F5) > **Сервер** > **Антивірус і антишпигун**, це вплине на такі умови правила:

- Назва вкладення
- Розмір вкладення
- Тип вкладення
- Результат антивірусного сканування
- Вкладення захищено паролем
- Вкладення є пошкодженим архівом
- Містить пошкоджений архів
- Містить архів, захищений паролем

Дія правила

Для повідомлень і (або) вкладень можна додавати дії, які відповідають умовам правила.

Для одного правила можна додати кілька дій.

Список доступних дій для захисту передачі пошти, захисту бази даних поштових скриньок і сканування бази даних поштових скриньок за вимогою (деякі параметри можуть не відображатися залежно від вибраних умов):

Назва дії	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Відправити повідомлення в карантин	✔	✔	✔	Повідомлення не буде доставлено одержувачу, а буде переміщено в поштовий карантин. Дає змогу користувачам, які не є адміністраторами, розблоковувати з карантину електронні листи, переміщені туди за цим правилом (за допомогою веб-інтерфейсу або звітів про карантин).

Назва дії	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Відправити вкладення в карантин	✔	✔	✔	Переміщує поштові вкладення у файловий карантин. Електронний лист буде доставлено одержувачу з обнуленим вкладенням.
Видалити вкладення	✔	✔	✔	Видаляє вкладення Повідомлення буде доставлено отримувачу без вкладення.
Відхилити повідомлення	✔	✔	✔	Видаляє повідомлення. Для вхідних електронних листів, отриманих через SMTP, NDR (Non-Delivery Report) має бути згенеровано сервером-відправником.
Видалити повідомлення без попередження	✔	✔	✔	Видаляє повідомлення без створення NDR.
Встановлення значення SCL	✔	✔	✔	Змінює або встановлює певне значення SCL.
Надіслати сповіщення про подію адміністратору	✔	✔	✔	Надсилає сповіщення про події одержувачу, якого вказано в розділі Сповіщення електронною поштою. Необхідно ввімкнути функцію Відправляти сповіщення про події електронною поштою. Після цього можна налаштувати формат повідомлень про події (використовуйте підказку для пропозицій) під час створення правила. Окрім того, можна вибрати рівень детальності повідомлень про події, однак це залежить від параметра мінімального рівня детальності в розділі Сповіщення електронною поштою.
Надіслати електронна пошта сповіщення				Надсилає сповіщення про електронні листи одержувачу, якого вказано в розділі Сповіщення електронною поштою.
Пропустити сканування на наявність спаму	✔	✔	✔	Повідомлення не буде скануватися механізмом антиспаму.
Пропустити антивірусне сканування	✔	✔	✔	Повідомлення не перевірятиметься механізмом антивірусу.
Пропустити сканування для захисту від фішинг-атак	✔	✔	✔	Повідомлення не аналізуватиметься модулем захисту від фішинг-атак.

Назва дії	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Пропустити сканування ESET LiveGuard Advanced	✔	✔	✔	Повідомлення не буде перевірятися системою захисту ESET LiveGuard Advanced.
Оцінити інші правила	✔	✔	✔	Дає змогу оцінити інші правила, оскільки користувач може визначити кілька наборів умов і кілька дій, які будуть виконуватися залежно від цих умов.
Реєструвати як подію	✔	✔	✔	Записує інформацію про застосоване правило в журнал програми й визначає формат повідомлень про події (використовуйте підказку для пропозицій). Якщо налаштувати тип дії "Реєструвати як подію" для захисту бази даних поштових скриньок із параметром %IPAddress%, то стовпчик "Подія" в розділі Файли журналу буде пустим для цієї події. Це зумовлено тим, що на рівні захисту бази даних поштових скриньок немає IP-адреси. Деякі параметри доступні не на всіх рівнях захисту: %IPAddress%: ігнорується скануванням бази даних поштових скриньок за вимогою і захистом бази даних поштових скриньок %Mailbox%: ігнорується захистом передачі пошти Наведені нижче параметри застосовуються тільки до правил обробки вкладень: %Attname%: ігнорується правилами фільтрації й правилами обробки результатів %Attsize%: ігнорується правилами фільтрації й правилами обробки результатів
Додати поле заголовка	✔	✔	✔	Додає спеціальний рядок у заголовок повідомлення.
Додати префікс теми	✔	✔	✔	Додає префікс у тему.
Замінити вкладення інформацією про дію	✔	✔	✔	Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Видалити поля заголовків	✔	✔	✔	Видаляє поля із заголовка повідомлення відповідно до заданих параметрів.

Назва дії	Захист передачі пошти	Захист бази даних поштової скриньки	Сканування бази даних поштових скриньок за вимогою	Опис
Видаляє повідомлення	✔	✔	✔	Видаляє інфіковане повідомлення.
Перемістити повідомлення до папки	✔	✔	✔	Повідомлення буде переміщено у вказану папку.
Перемістити повідомлення до кошика	✔	✔	✔	Переміщує електронний лист у папку кошика на стороні поштового клієнта.
Застосування політики DMARC	✔	✔	✔	Якщо виконано умову результату DMARC, електронний лист обробляється відповідно до політики, яка визначена в записі DNS DMARC для домену відправника.

Якщо для **захисту передачі пошти** вимкнути **Захист від вірусів** у меню Параметри або в розділі **Додаткові параметри** (F5) > **Сервер** > **Антивірус і антишпигун**, це вплине на такі дії правила:

- Відправити вкладення в карантин
- Видалити вкладення

Приклади правил

Перемістити в карантин повідомлення, що містять шкідливе програмне забезпечення або захищені паролем, зашифровані чи пошкоджені вкладення

Мета: Перемістити в карантин повідомлення, що містить шкідливе програмне забезпечення або захищені паролем, зашифровані чи пошкоджені вкладення
Створіть таке правило для **захисту передачі пошти**:
Стан
- Тип: Результат антивірусного сканування
- Операція: не є
- Параметр: Очистити

Дія
Тип: Відправити повідомлення в карантин

Перемістити повідомлення, для яких не вдалося виконати перевірку SPF, до папки небажаних повідомлень

Мета: Перемістити повідомлення, для яких не вдалося виконати перевірку SPF, до папки небажаних повідомлень
Створіть таке правило для **захисту передачі пошти**:
Стан
• Тип: Результат SPF
• Операція: є
• Параметр: Невдача
Дія
• Тип: Установлення значення SCL
• Значення: 5
Установіть значення відповідно до параметра `SCLJunkThreshold` для командлета `Get-OrganizationConfig` вашого сервера Exchange. Більш докладні відомості див. в статті про дії щодо порогу SCL.

Перевірити підозрілий електронний лист на підробку відправника

Мета: перевірити підозрілий електронний лист на підробку відправника. Якщо повідомлення містить власний домен у заголовку електронного листа "From:" або у відправнику конверта, додатково перевірити за результатом SPF. Якщо перевірка SPF повернула результат "Нейтральний", перемістити повідомлення в карантин, записати в журнал подій і повідомити про це адміністратору.
Стан
• Тип: Результат порівняння заголовків відправника конверта та From
• Операція: є
• Параметр: Порівняти
• Тип: результат перевірки SPF: заголовок From
• Операція: є
• Параметр: Нейтральний
Дія
Тип: Перемістити повідомлення в карантин, записати в журнал подій і надіслати сповіщення про подію адміністратору

Видалити повідомлення від певних відправників

Мета: видалити повідомлення від певних відправників
Створіть таке правило для **захисту передачі пошти**:
Стан
• Тип: Відправник
• Операція: Є / є одним із
• Параметр: spammer1@domain.com, spammer2@domain.com
Дія
Тип: **Видалити повідомлення без попередження**

Список заблокованих IP-адрес

Мета: Перенести в карантин повідомлення, яке надійшло з IP-адреси зі списку заблокованих IP-адрес, повідомити про це адміністратора й записати подію в журнал.
Відомості: Якщо електронний лист надійшов з IP-адреси зі списку заблокованих IP-адрес, <%PM%> перенесе повідомлення в карантин і повідомить вас про це електронною поштою. Після цього можна розблокувати повідомлення з карантину або видалити його назавжди. В іншому разі <%PM%> скине повідомлення, не надавши можливості застосувати до нього будь-яку дію.
Відкрити **Захист передачі пошти**
Стан
• Тип: IP-адреса відправника
• Операція: У списку
• Список Список заблокованих IP-адрес
Дія
Тип: Перемістити повідомлення в карантин, записати в журнал подій і надіслати сповіщення про подію адміністратору

налаштувати попередньо визначене правило

Мета: налаштувати попередньо визначене правило
Відомості: Дозволити архівні вкладення в повідомленнях із визначених IP-адрес (наприклад, якщо використовуються внутрішні системи), якщо застосовано правило "Заборонені архівні файли у вкладенні"
Відкрийте набір правил **Захист передачі пошти**, виберіть **Заборонені архівні файли у вкладенні** й клацніть **Змінити**.
Стан
• Тип: IP-адреса відправника
• Операція:Не є / не є жодним із
• Параметр: 1.1.1.2, 1.1.1.50-1.1.1.99

Тіло повідомлення

Мета: Перемістити в карантин повідомлення, які містять певний рядок у тексті
Створіть таке правило для **захисту передачі пошти**:
Стан
• Тип: Тіло повідомлення
• Операція: "містить" / "містить одне з", клацніть **Додати**, уведіть URL-адресу веб-сайту або частину URL-адреси
Дія
Тип: Відправити повідомлення в карантин

Зберігати повідомлення для одержувачів, які не існують

Мета: Зберігати повідомлення для одержувачів, які не існують
Відомості: якщо потрібно переносити в карантин усі повідомлення одержувачам, які не існують (незалежно від їхнього позначення антивірусом або антиспамом)
Стан
• Тип: Результат перевірки одержувача
• Операція: є
• Параметр: Містить недійсного одержувача
Дія
Тип: Відправити повідомлення в карантин

Захист передачі пошти

Можна налаштувати дії для виявлених загроз на рівні транспорту для кожного модуля ESET Mail Security окремо ("Антивірус", "Захист від фішинг-атак" і "Антиспам").

Дії, яку потрібно виконати, якщо очищення неможливе

• **Пропустити**: зберегти інфіковані повідомлення, які не можна очистити.

• **Відправити повідомлення в карантин**: помістити інфіковані повідомлення в поштову скриньку карантину

• **Відхилити повідомлення**: відхилити інфіковане повідомлення.

• **Видалити повідомлення без попередження**: видалити повідомлення без надсилання звіту про недоставку (NDR, Non-Delivery Report).

Якщо вибрати пункт **Пропустити**, коли в параметрах ThreatSense Антивірус та антишпигун для **рівня очищення** вибрано пункт **Без очищення**, то колір статусу захисту зміниться на жовтий. Це пов'язано з ризиком для безпеки, тому не рекомендуємо використовувати цю комбінацію. Щоб забезпечити надійний рівень захисту, змініть той чи інший параметр.

Дії, які будуть застосовуватися до фішингового повідомлення:

• **Пропустити**: зберегти повідомлення

• **Відправити повідомлення в карантин**: помістити повідомлення, позначені як фішинг, у поштову скриньку карантину

• **Відхилити повідомлення**: відхилити повідомлення, позначені як фішинг.

• **Видалити повідомлення без попередження**: видалити повідомлення без надсилання звіту про недоставку (NDR, Non-Delivery Report).

Дія, яку потрібно виконувати зі спамовими повідомленнями:

• **Пропустити**: зберегти повідомлення

• **Відправити повідомлення в карантин**: помістити повідомлення, позначені як спам, у поштову скриньку карантину

• **Відхилити повідомлення**: відхилити повідомлення, позначені як спам.

• **Видалити повідомлення без попередження**: видалити повідомлення без надсилання звіту про недоставку (NDR, Non-Delivery Report).

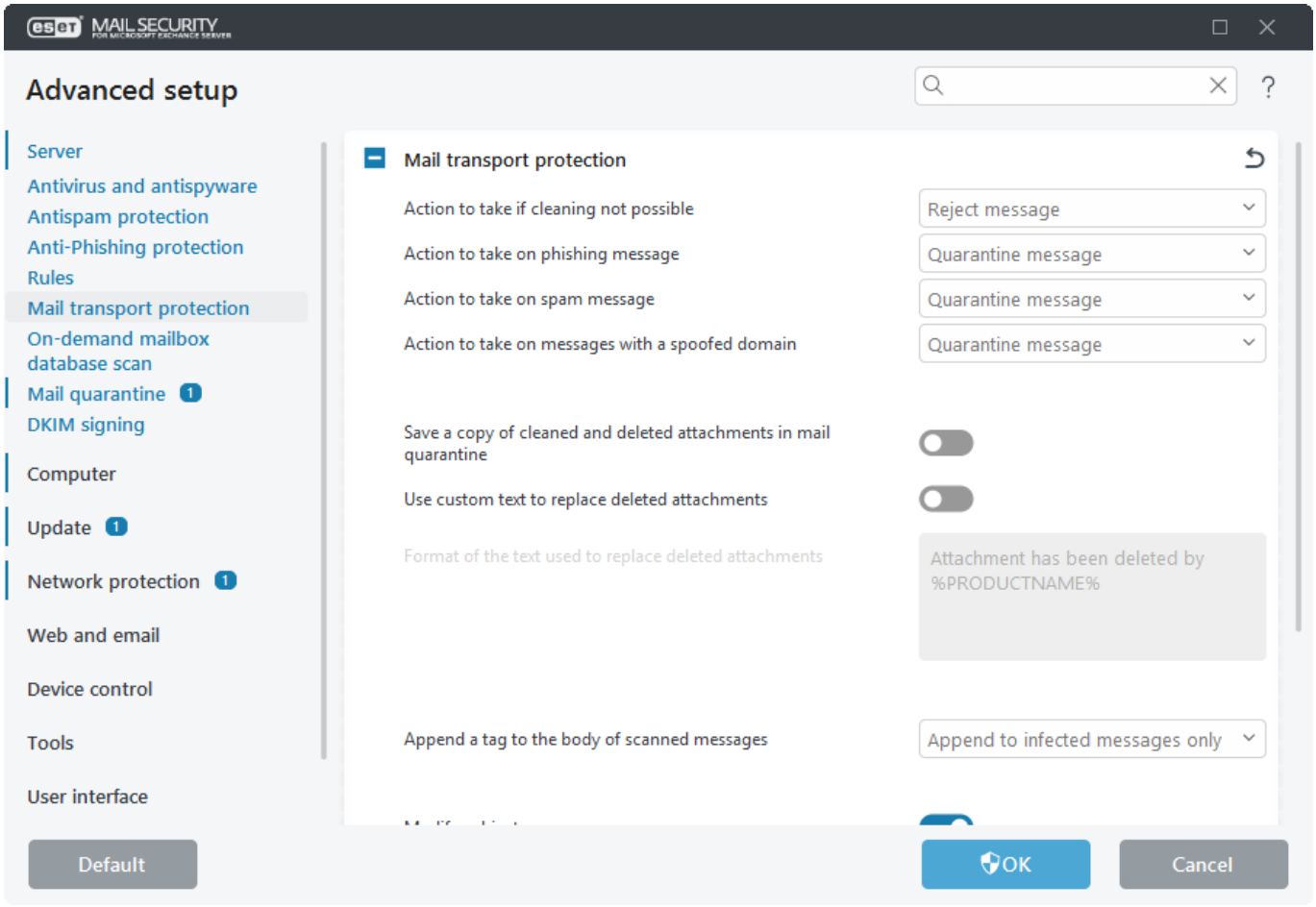
Дія, яка застосовуватиметься для повідомлень із підробленим доменом:

• **Пропустити**: зберегти повідомлення

• **Відправити повідомлення в карантин**: перемістити повідомлення, позначені як підроблені, в поштову скриньку карантину.

• **Відхилити повідомлення**: відхилити повідомлення, позначені як підроблені.

• **Видалити повідомлення без попередження**: видалити повідомлення без надсилання звіту про недоставку (NDR, Non-Delivery Report).



Зберегти копію очищених і видалених вкладень у поштовий карантин

Копію вихідного вкладеного файлу буде збережено в поштовому карантині.

Заміняти видалені вкладення за допомогою налаштовуваного тексту

Якщо цей параметр увімкнено, можна вказати спеціальний текст, який буде відображатися замість видалених вкладень.

Формат тексту, який використовується для заміни видалених вкладень

Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію. Якщо ви ввімкнули наведений вище параметр (**Використовувати налаштовуваний текст**), за потреби можна змінити текст за замовчуванням на власний розсуд.

Використовуйте змінні для налаштування тексту, який відображатиметься в електронному листі замість видалених вкладень.
%PRODUCTNAME%
%FILENAME%
%VIRUSNAME%
%DETECTIONNAME%
%FILESIZE%
Вкладення %FILENAME% розміром %FILESIZE% видалено %PRODUCTNAME% через %DETECTIONNAME%.
Налаштовуваний текст буде мати такий вигляд:
Вкладення eicar_com.zip розміром 184 Б видалено ESET Mail Security через файл Eicar test.

Відповідь SMTP про відхилення

Можна вказати параметри **Код відповіді**, **Код стану** й **Текст відповіді**, які визначають відповідь тимчасової відмови SMTP, яка надсилається на сервер SMTP, якщо повідомлення відхилено. Можна ввести текст відповіді в такому форматі:

Код відповіді	Код стану	Повідомлення з відповіддю
250	2.5.0	Запитувану дію з поштою виконано
451	4.5.1	Запитувану дію перервано: локальна помилка в процесі обробки
550	5.5.0	Запитану дію не прийнято: поштова скринька недоступна
554	5.6.0	Недійсний вміст

Під час налаштування відповідей відхилення SMTP можна також використовувати системні змінні.

Параметр **Додавати сповіщення до тіла просканованих повідомлень** має такі три варіанти для вибору:

• **Не додавати до повідомлень**: інформацію не буде додано.

• **Додавати лише до інфікованих повідомлень**: впливає лише на інфіковані повідомлення.

• **Додавати до всіх повідомлень** (не застосовується до внутрішніх повідомлень): усі повідомлення будуть позначені.

Змінити тему

Якщо цей параметр увімкнуто, можна змінювати шаблони, додані в тему інфікованих повідомлень, спаму або фішингових повідомлень.

Шаблон, який додається до теми інфікованих повідомлень

ESET Mail Security додасть тег сповіщення в тему електронного листа зі значенням, визначеним у текстовому полі **Шаблон, який додається до теми інфікованих повідомлень** (попередньо визначений текст за замовчуванням: `[found threat %VIRUSNAME%]`). Цю модифікацію можна використовувати для автоматизації фільтрації інфікованих повідомлень через фільтрацію електронних листів із певною темою, наприклад, за допомогою правил або, як альтернативний варіант, на боці клієнта (якщо це підтримується поштовим клієнтом), із подальшим перенесенням таких електронних листів в окрему папку.

Шаблон, який додається до теми повідомлень зі спамом

ESET Mail Security додасть тег сповіщення в тему електронного листа зі значенням, визначеним у текстовому полі **Шаблон, який додається до теми спамових повідомлень** (попередньо визначений текст за замовчуванням: `[SPAM]`). Цю модифікацію можна використовувати для автоматизації фільтрації спаму через фільтрацію електронних листів із певною темою, наприклад, за допомогою правил або, як альтернативний варіант, на боці клієнта (якщо це підтримується поштовим клієнтом), із подальшим перенесенням таких електронних листів в окрему папку.

Шаблон, який додається до теми фішингових повідомлень

ESET Mail Security додасть тег сповіщення в тему електронного листа зі значенням, визначеним у текстовому полі **Шаблон, який додається до теми фішингових повідомлень** (попередньо визначений текст за замовчуванням: `[PHISH]`). Цю модифікацію можна використовувати для автоматизації фільтрації спаму через фільтрацію електронних листів із певною темою, наприклад, за допомогою правил або, як альтернативний варіант, на боці клієнта (якщо це підтримується поштовим клієнтом), із подальшим перенесенням таких електронних листів в окрему папку.

> Під час редагування тексту, який додається в тему, можна використовувати системні змінні.

Додаткові параметри передавання пошти

Параметри захисту передавання пошти можна налаштувати.

Також сканувати повідомлення, отримані через автентифіковані й внутрішні підключення

Можна вибрати сканування, яке буде застосовуватися для повідомлень з автентифікованих джерел або локальних серверів. Рекомендується сканувати ці повідомлення, оскільки це підвищує рівень захисту. Обов'язково слід використовувати сканування, якщо ви використовуєте вбудований Microsoft SBS POP3 Connector для отримання електронних листів із зовнішніх серверів POP3 або поштових служб (наприклад, Gmail.com, Outlook.com, Yahoo.com, gmx.dem тощо). Докладніше див. в розділі POP3 Connector і антиспам.

У розкривному меню виберіть рівень захисту. Рекомендуємо використовувати **Антивірусний захист** (налаштовано за замовчуванням), особливо для внутрішніх підключень, оскільки навряд чи фішингові повідомлення або спам розповсюджуватимуться через локальні сервери. Проте рівень захисту для Microsoft SBS POP3 Connector можна підвищити. Для цього виберіть **Захист від вірусів і фішинг-атак** або **Захист від вірусів, фішинг-атак і спаму**.

> Цей параметр вмикає (вимикає) антиспам для автентифікованих користувачів і внутрішніх підключень. Завжди перевіряються електронні листи, надіслані з неавтентифікованих підключень (навіть якщо вибрано параметр **Не сканувати**).

Внутрішні повідомлення від Outlook усередині організації надсилаються у форматі TNEF (Transport Neutral Encapsulation Format). Антиспам не підтримує TNEF. Тому внутрішні електронні листи у форматі TNEF не перевірятимуться на наявність СПАМУ незалежно від параметра **Також сканувати повідомлення, отримані через автентифіковані та внутрішні підключення**.

Перед скануванням видалити наявний заголовок SCL

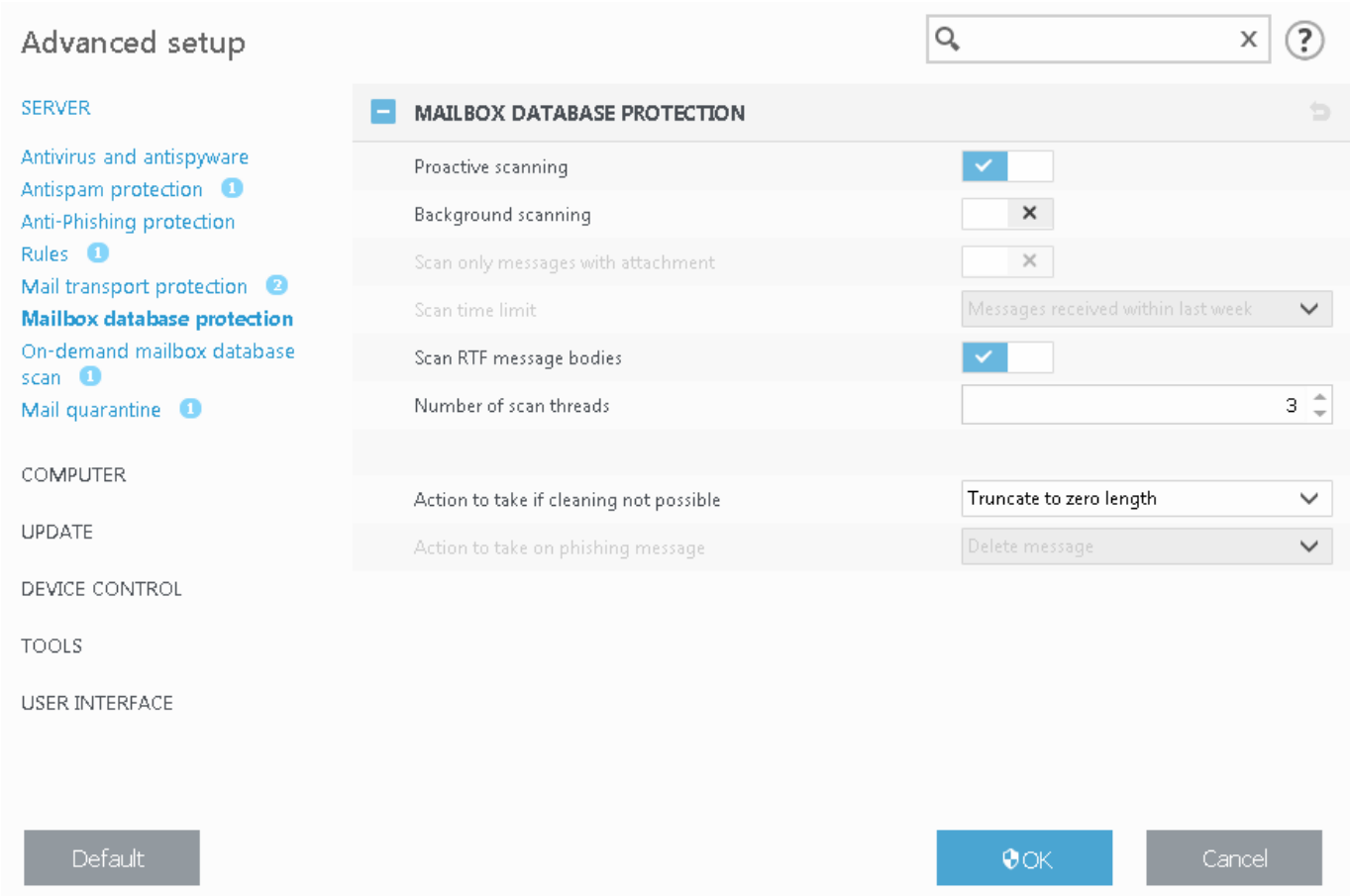
Цей параметр ввімкнено за замовчуванням. Його можна вимкнути. Проте потрібно залишити незмінним заголовок SCL (Spam Confidence Level, показник імовірності спаму).

Записувати результати сканування в заголовки повідомлень

Якщо цей параметр увімкнено, результати сканування записуються в заголовки повідомлень. Заголовки цих повідомлень починаються з `X_ESET`, тому їх легко розпізнати (наприклад, `X_EsetResult` або `X_ESET_Antispam`).

Захист бази даних поштової скриньки

Якщо ввімкнуто параметр **Проактивне сканування**, нові вхідні повідомлення скануватимуться в порядку їхнього отримання. Якщо цей параметр увімкнуто, то коли користувач відкриває повідомлення, яке ще не було просканово, воно буде просканово перед іншими повідомленнями в черзі.



Сканування у фоновому режимі

Дає змогу виконувати сканування всіх повідомлень у фоновому режимі (сканування

виконується в сховищі поштової скриньки й загальнодоступних папок, наприклад, у базі даних Exchange). Microsoft Exchange Server вирішує, чи запускати сканування у фоновому режимі, на основі різних факторів, зокрема поточного навантаження на систему, кількості активних користувачів тощо. Microsoft Exchange Server зберігає історію просканованих повідомлень і дані про використовувану версію бази даних сигнатур вірусів.

Якщо ви спробуєте відкрити повідомлення, яке ще не просканово з використанням найновішої бази даних сигнатур вірусів, Microsoft Exchange Server надішле це повідомлення ESET Mail Security для його перевірки перед відкриттям у поштовому клієнті. Можна вибрати параметр **Сканувати лише повідомлення з вкладеннями** й застосувати фільтр за часом отримання з використанням таких параметрів обмеження за часом сканування:

- Усі повідомлення
- Повідомлення, отримані за останній рік
- Повідомлення, отримані за останні 6 місяців
- Повідомлення, отримані за останні 3 місяці
- Повідомлення, отримані за останній місяць
- Повідомлення, отримані за останній тиждень

Оскільки сканування у фоновому режимі може негативно вплинути на навантаження на систему (сканування виконується після кожного оновлення обробника виявлення), ми рекомендуємо запланувати запуск сканування в неробочі години. Заплановане сканування у фоновому режимі можна налаштувати за допомогою спеціального завдання в планувальнику.

Під час планування розкладу сканування у фоновому режимі можна задати час запуску, кількість повторних запусків та інші параметри, доступні в планувальнику. Після того, як запуск завдання заплановано, воно відобразиться в списку запланованих завдань. Ви можете змінити параметри завдання, видалити або тимчасово деактивувати його.

Кількість потоків сканування

Кількість потоків сканування може бути в діапазоні від 1 до 21. Можна вказати кількість незалежних потоків сканування, які використовуватимуться одночасно. Більша кількість потоків на мультіпроцесорних комп’ютерах може підвищити частоту сканування. Для забезпечення найкращої продуктивності програми рекомендуємо використовувати однакову кількість обробників сканування ThreatSense і потоків сканування.

Сканувати тіла повідомлень RTF

Параметр активує сканування тексту повідомлень RTF. У тексті повідомлень RTF можуть бути макровіруси.

VSAPI не сканує електронні листи зі звичайним текстом.

Дії, яку потрібно виконати, якщо очищення неможливе

- **Жодних дій**: до повідомлень не застосовуватиметься жодних змін

• **Скоротити до нульової довжини**: вкладення буде скорочено до нульової довжини

• **Замінити вміст інформацією про дію**: вихідний текст буде замінено інформацією про дію. Вміст вкладення буде замінено інформацією про дію.

• **Видалити повідомлення**: повідомлення буде видалено

Дія, яку потрібно виконати з фішинговим повідомленням:

• **Жодних дій**: до повідомлень не застосовуватиметься жодних змін

• **Видалити повідомлення**: повідомлення буде видалено

> Загальнодоступні папки обробляються так само, як і поштові скриньки. Це означає, що загальнодоступні папки також скануються.

Сканування у фоновому режимі

Цей тип завдання дає змогу виконувати сканування бази даних за допомогою VSAPI у фоновому режимі. Він дає можливість Exchange Server за потреби запускати сканування у фоновому режимі. Сканування ініціюватиме сам Exchange Server. Це означає, що сервер Exchange Server може виконувати сканування в будь-який час протягом дозволеного періоду часу.

Рекомендуємо дозволити запускати це завдання в той час, коли немає високого навантаження (Exchange Server не зайнятий), наприклад уночі. Це зумовлено тим, що сканування бази даних у фоновому режимі може спричинити певне навантаження на систему. Окрім цього, щоб уникнути проблем із продуктивністю і доступністю системи, потрібно слідкувати за тим, аби виконання цього завдання не збігалося в часі з жодним процесом резервного копіювання, який може виконуватися в Exchange Server.

> Щоб заплановане завдання запустилося, захист бази даних поштових скриньок має бути ввімкнено. Цей тип захисту доступний тільки для Microsoft Exchange Server 2010, які працюють на поштових серверах.

Тайм-аут (години)

Укажіть, скільки годин із часу запуску цього запланованого завдання вашому серверу Exchange Server дозволяється виконувати сканування бази даних у фоновому режимі. Коли час очікування мине, Exchange отримає інструкцію зупинити сканування у фоновому режимі.

Сканування бази даних поштових скриньок за вимогою

> У системі Microsoft Exchange Server 2010 можна вибрати захист бази даних поштових скриньок або **сканування бази даних поштових скриньок за вимогою**. Одночасно можна активувати лише один тип захисту. Якщо ви вирішите **використовувати сканування бази даних за вимогою**, потрібно буде вимкнути інтеграцію **захисту бази даних поштових скриньок** у розділі **Додаткові параметри** (**F5**) із розділу Сервер. В іншому разі **сканування бази даних поштових скриньок за вимогою** буде недоступне.

Адреса хоста: ім'я або IP-адреса сервера, на якому запущено веб-служби EWS (Exchange Web Services).

Ім'я користувача: укажіть облікові дані користувача, який має відповідний доступ до EWS.

Пароль користувача — Клацніть **Задати** поруч із пунктом **Пароль користувача** і введіть пароль для цього облікового запису користувача.

Для можливості сканувати загальнодоступні папки в користувача, який використовується для сканування бази даних поштових скриньок за вимогою, має бути поштова скринька. В іншому разі в журналі сканування бази даних відображатиметься *Failed to load public folders* разом із більш докладним повідомленням від Exchange.

Метод доступу до поштової скриньки: дає змогу вибрати бажаний спосіб доступу до поштової скриньки:

- **Імітація користувача** — Простіше й швидше налаштувати **роль ApplicationImpersonation**, яку потрібно призначити для облікового запису сканування.

Призначення ролі ApplicationImpersonation користувачу

Якщо цей параметр недоступний, необхідно вказати **ім'я користувача**. Клацніть **Призначити**, щоб автоматично призначити роль ApplicationImpersonation вибраному користувачу. Окрім цього, для облікового запису користувача можна вручну призначити роль ApplicationImpersonation. Для облікового запису користувача створюється нова політика обмеження кількості запитів EWS, для якої не встановлено обмежень. Більш докладну інформацію див. в розділі Відомості облікового запису сканування бази даних.

- **Делегування** — Використовуйте цей тип доступу, якщо потрібно вимагати налаштування прав доступу для окремих поштових скриньок, проте ви можете забезпечити більш високу швидкість сканування великих обсягів даних.

Призначення делегованого доступу користувачу

Якщо цей параметр недоступний, необхідно вказати **ім'я користувача**. Клацніть **"Призначити"**, щоб автоматично надати вибраному користувачу повний доступ до всіх користувачів і спільних поштових скриньок. Для облікового запису користувача створюється нова політика обмеження кількості запитів EWS, для якої не встановлено обмежень. Більш докладну інформацію див. в розділі Відомості облікового запису сканування бази даних.

Використовувати SSL

SSL потрібно ввімкнути, якщо для EWS встановлено значення "Вимагати SSL" у службах IIS. Якщо SSL увімкнено, сертифікат Exchange Server потрібно імпортувати в систему з ESET Mail Security (якщо ролі Exchange Server розташовано на різних серверах). Параметри для веб-служб Exchange (EWS) можна знайти в розділі IIS Sites/Default website/EWS/SSL Settings.

Параметр **Використовувати SSL** можна вимкнути, лише якщо EWS у IIS налаштовано таким чином, що не вимагає SSL.

Ігнорувати помилку сертифіката сервера — Якщо ви використовуєте сертифікат із власним підписом, можна ігнорувати помилку сертифіката сервера.

Сертифікат клієнта: потрібно задати, лише якщо EWS вимагає сертифікат клієнта. Щоб вибрати сертифікат, клацніть **Вибрати**.

Дії, яку потрібно виконати, якщо очищення неможливе: це поле дії дає змогу блокувати інфікований вміст.

- **Пропустити**: не застосовувати жодних дій до інфікованого вмісту повідомлення.
- **"Перемістити повідомлення до кошика"** не підтримується для об’єктів із загальнодоступних папок. Натомість буде застосовано дію "Видалити об’єкт".
- **Видалити об’єкт**: видаляє інфікований вміст повідомлення.
- **Видалити повідомлення**: видалити все повідомлення, включно з інфікованим вмістом.
- **Замінити об’єкт інформацією про дію**: видаляє об’єкт і фіксує інформацію про об’єкт, який було видалено.

Дія, яку потрібно виконати з фішинговим повідомленням:

- **Пропустити**: зберегти повідомлення, навіть якщо його позначено як фішингове.
- **"Перемістити повідомлення до кошика"** не підтримується для об’єктів із загальнодоступних папок. Натомість буде застосовано дію "Видалити об’єкт".
- **Видалити повідомлення**: видалити все повідомлення, включно з інфікованим вмістом.

Кількість потоків сканування

Можна вказати кількість потоків, які ESET Mail Security має використовувати під час сканування бази даних. Що вище значення, то краще продуктивність. Однак для підвищення продуктивності використовується більше ресурсів. Точно налаштуйте для цього параметра потрібне значення відповідно до ваших вимог. За замовчуванням задано 4 потоки сканування.

> **i** Якщо для сканування бази даних поштових скриньок за вимогою налаштовано забагато потоків, це може призвести до надмірного навантаження на систему, що може сповільнити роботу інших процесів або навіть усієї системи. У повідомленні може з’явитися повідомлення про помилку Відкрито забагато паралельних підключень.

Microsoft 365

Відображається лише за наявності гібридного середовища Microsoft 365.

Обліковий запис користувача для сканування спільної папки

Щоб сканувати спільні папки, укажіть ім’я облікового запису головного користувача (пароль можна не вказувати) для імітації користувача. Переконайтеся, що цей обліковий запис користувача має доступ до всіх спільних папок.

Сканування бази даних поштових скриньок

Запуск повного сканування бази даних електронної пошти у великих середовищах може призвести до небажаних навантажень системи. Щоб уникнути цієї проблеми, запускайте сканування для окремих баз даних або поштових скриньок. Щоб додаткового мінімізувати вплив на систему сервера, відфільтруйте об’єкти сканування за допомогою позначок часу повідомлень.

Неправильно визначені правила сканування бази даних поштових скриньок за вимогою можуть призвести до незворотних змін у базах даних поштових скриньок. Перед першим запуском сканування бази даних поштових скриньок із правилами переконайтеся, що маєте найновіші резервні копії баз даних поштових скриньок. Окрім того, наполегливо рекомендуємо перевірити, чи виконуються правила відповідно до очікувань.
Для перевірки визначте правила з дією "Реєструвати як подію". Це потрібно лише тому, що інші дії можуть унести зміни до бази даних поштових скриньок. Після завершення перевірки можна додати правило з дією видалення, наприклад **Видалити вкладення**.

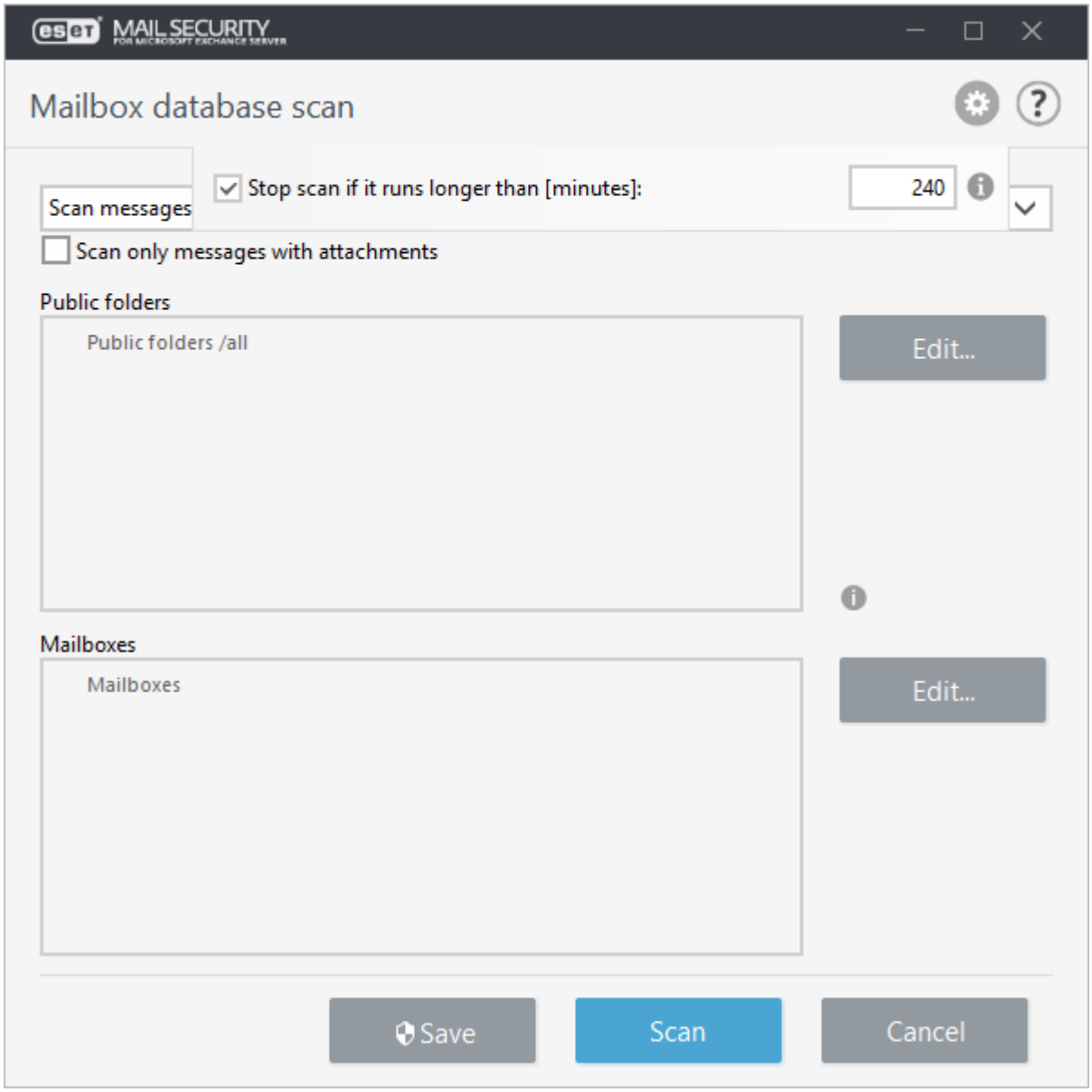
Указані нижче типи елементів скануються, як у **загальнодоступних папках**, так і в **поштових скриньках** користувача:

- Електронна пошта
- Допис
- Елементи календаря (наради/інтерв’ю)
- Завдання
- Контакти
- Журнал

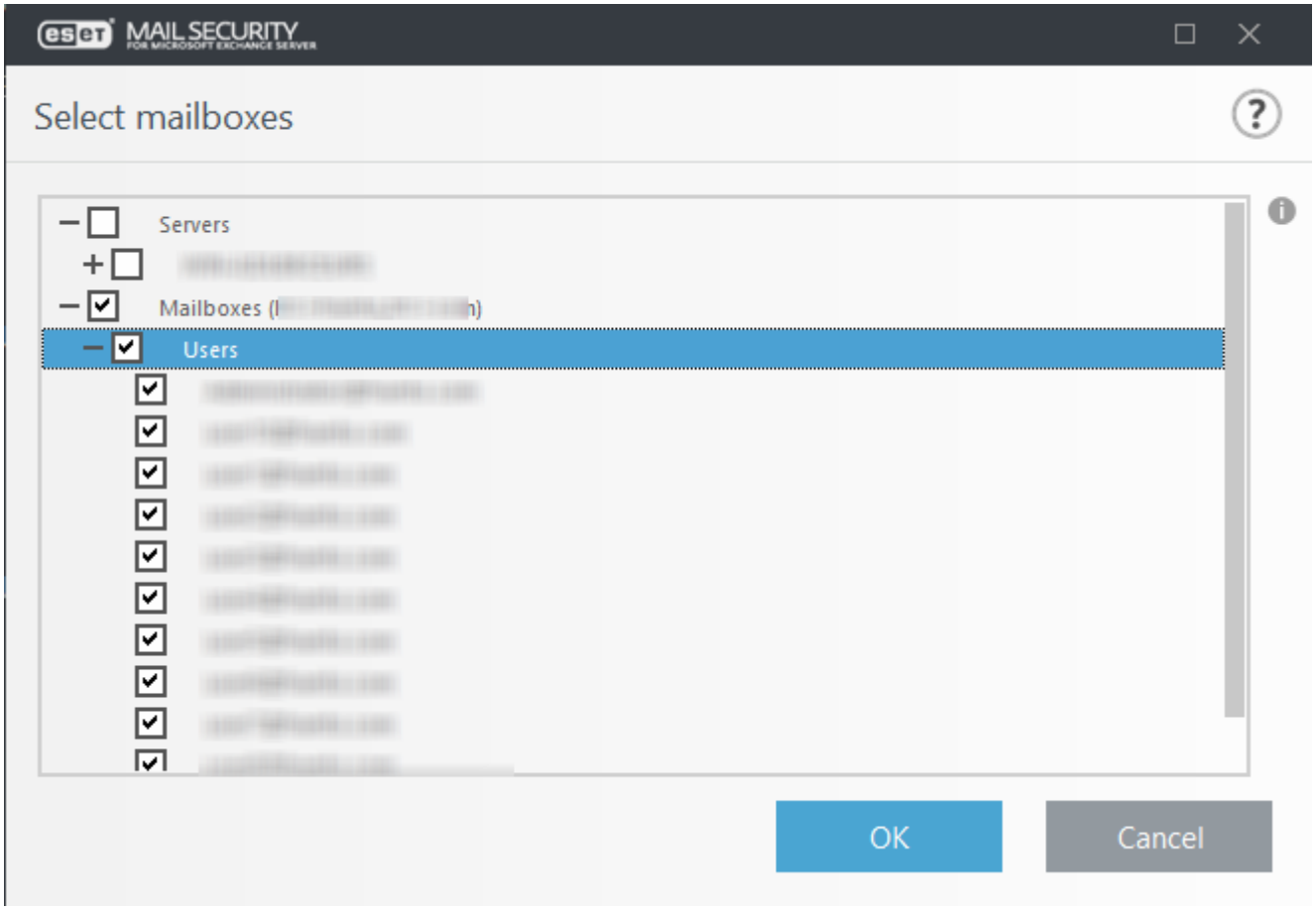
У розкривному списку виберіть параметр, що визначає повідомлення, які потрібно сканувати відповідно до їхньої мітки часу. Наприклад, **Сканувати повідомлення, змінені за останній тиждень**. За потреби можна вибрати параметр **Сканувати всі повідомлення**.

Щоб увімкнути або вимкнути сканування вкладень повідомлень, установіть прапорець **Сканувати лише повідомлення з вкладеннями**. Клацніть **Змінити**, щоб вибрати загальнодоступну папку для сканування.

Клацніть піктограму ⚙ і змініть інтервал **Зупинити сканування, якщо воно триває довше ніж (хв.)**, а потім змініть бажаний час (будь-який час від 1 до 2880 хвилин).



Установіть прапорці поруч із базами даних сервера й поштовими скриньками, які потрібно сканувати. Фільтр дає змогу швидко знаходити бази даних і поштові скриньки, особливо якщо у вашій інфраструктурі Exchange багато поштових скриньок.



Клацніть **Зберегти**, щоб зберегти вибрані об'єкти й параметри сканування в профілі сканування на вимогу. Тепер можна клацнути **Сканувати**. Якщо ви раніше не вказали відомості облікового запису сканування бази даних, відкриється спливаюче вікно з запитом на введення облікових даних. В іншому разі запуститься сканування бази даних поштових скриньок за вимогою.

Якщо вбудована поштова скринька адміністратора не відображається, переконайтеся, що цей атрибут *UserPrincipalName* не є пустим.

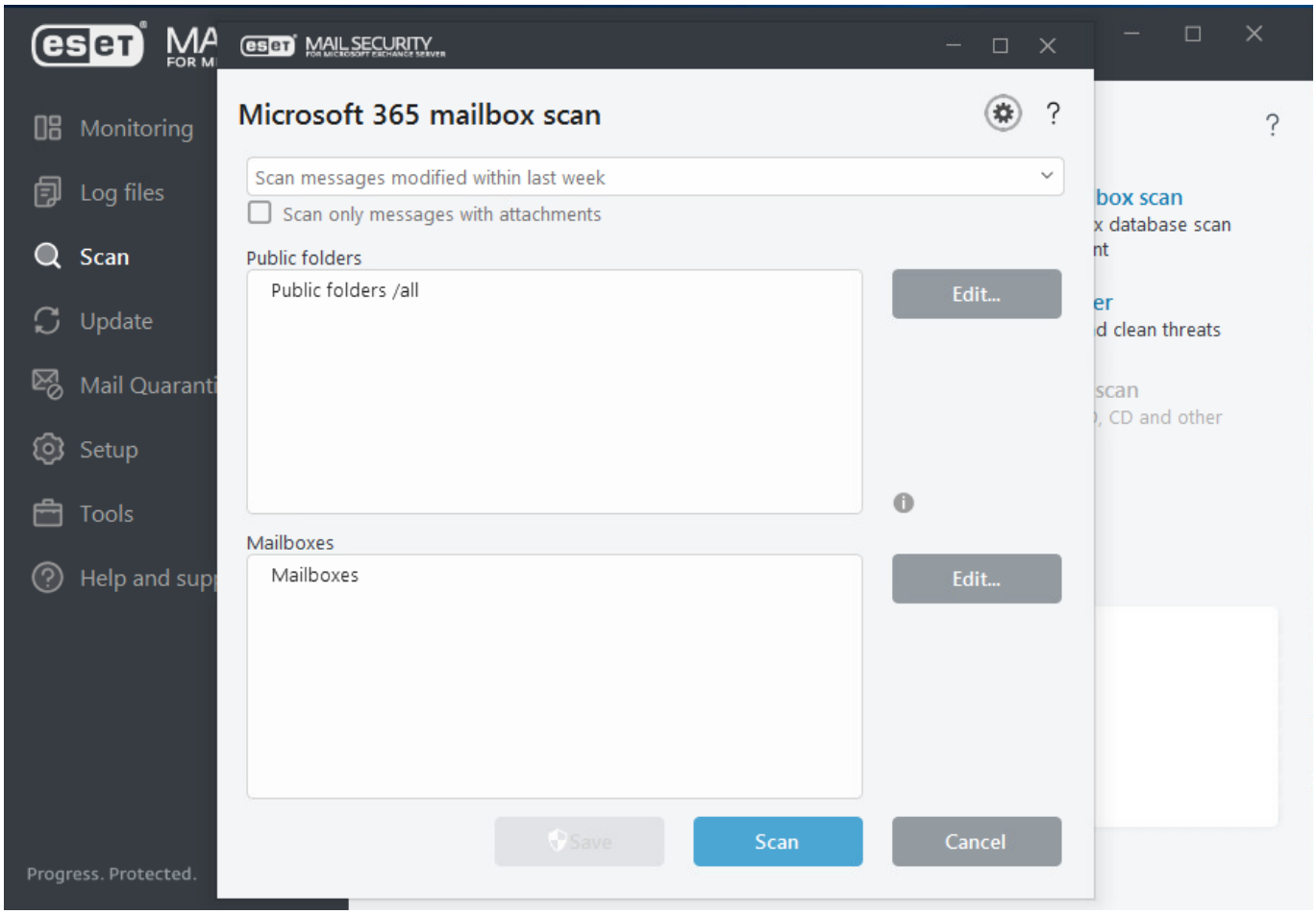
У системі Microsoft Exchange Server 2010 можна вибрати захист бази даних поштових скриньок або сканування бази даних поштових скриньок за вимогою. Одночасно можна активувати лише один тип захисту. Якщо ви вирішите **використовувати сканування бази даних за вимогою**, потрібно буде вимкнути інтеграцію **захисту бази даних поштових скриньок** у розділі **Додаткові параметри** > **Сервер**. В іншому разі сканування бази даних поштових скриньок за вимогою буде недоступне.

Сканування поштових скриньок Microsoft 365

ESET Mail Security забезпечує функцію сканування гібридних середовищ Microsoft 365. Вона доступна й відображається в ESET Mail Security тільки тоді, коли ви маєте гібридне середовище Exchange (локальний сервер і хмара). Підтримуються обидва сценарії маршрутизації: через **Exchange Online** або через **локальну** організацію. Докладніші відомості див. в розділі Transport routing in Exchange hybrid deployments (Транспортні маршрути в гібридних середовищах Exchange).

Щоб активувати цю функцію, зареєструйте сканер ESET Mail Security.

Сканування віддалених поштових скриньок Microsoft 365 і загальнодоступних папок можна використовувати так само, як і звичайне сканування бази даних поштових скриньок за вимогою.



Запуск повного сканування бази даних електронної пошти у великих середовищах може призвести до небажаних навантажень системи. Щоб уникнути цієї проблеми, запускайте сканування для окремих баз даних або поштових скриньок. Щоб додатково мінімізувати вплив на систему, використовуйте фільтр часу у верхній частині вікна. Наприклад, замість того, щоб використовувати функцію **Сканувати всі повідомлення**, можна вибрати параметр **Сканувати повідомлення, змінені за останній тиждень**.

Рекомендуємо налаштувати Microsoft 365. Натисніть клавішу **F5** і виберіть пункти **Сервер** > **Сканування бази даних поштових скриньок за вимогою**. Див. також розділ Відомості облікового запису сканування бази даних.

Щоб переглянути активність сканування поштових скриньок Office 365, установіть прапорець **Файли журналу** > **Сканування бази даних поштових скриньок**.

Додаткові елементи в поштових скриньках

Параметри сканера баз даних поштових скриньок за вимогою дають змогу ввімкнути або вимкнути сканування інших типів елементів у поштових скриньках:

- Сканувати календар
- Сканувати завдання

- Сканувати контакти
- Сканувати журнал

Якщо виникнуть проблеми з продуктивністю, можна вимкнути сканування цих елементів. Якщо ці елементи ввімкнено, сканування триватиме довше.

Проксі-сервер

Якщо ви використовуєте проксі-сервер між Exchange Server із роллю CAS і сервером Exchange Server з інстальованим ESET Mail Security, укажіть параметри проксі-сервера. Це потрібно, оскільки ESET Mail Security підключається до API веб-служб Exchange (EWS) за протоколом HTTP/HTTPS. В іншому разі карантинна поштова скринька й карантин Microsoft Exchange не працюватимуть.

Проксі-сервер

Уведіть IP-адресу або ім’я проксі-сервера, який ви використовуєте.

Порт

Уведіть номер порту проксі-сервера.

Ім’я користувача, пароль

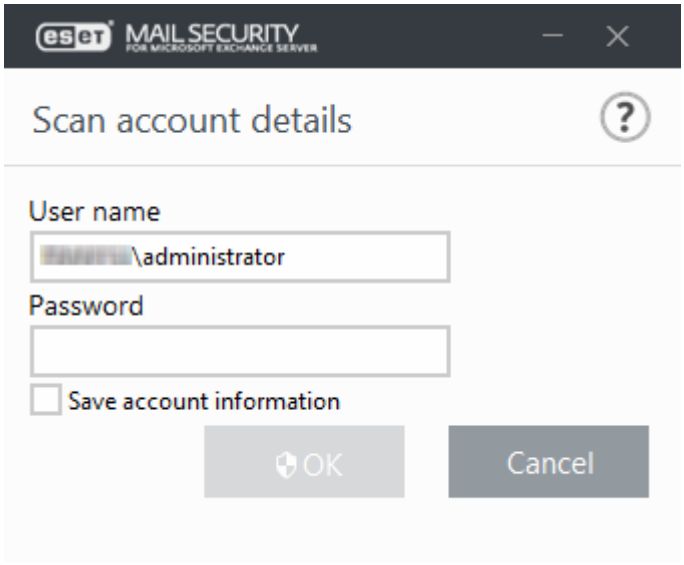
Уведіть облікові дані, якщо на проксі-сервері потрібно проходити автентифікацію.

Відомості облікового запису сканування бази даних

Це діалогове вікно відображається, якщо вам усе ще потрібно вказати ім’я користувача й пароль для сканування бази даних. У цьому вікні вкажіть облікові дані користувача, який має доступ до веб-служб Exchange (EWS) і клацніть **OK**. Як альтернативний варіант, можна відкрити розділ **Додаткові параметри** > **Сервер** > Сканування бази даних поштових скриньок за вимогою.

1. Уведіть **ім’я користувача**, клацніть **Задати**, потім уведіть пароль цього користувача й клацніть **OK**.

2. Установіть прапорець **Зберегти інформацію про обліковий запис**, щоб зберегти параметри облікового запису. В іншому разі під час кожного запуску сканування бази даних поштових скриньок за вимогою потрібно буде вводити дані облікового запису.



Якщо обліковий запис користувача не має відповідного доступу до веб-служб Exchange (EWS), можна вибрати пункт **Створити призначення ролей "ApplicationImpersonation"**, щоб призначити цю роль обліковому запису користувача. Окрім цього, **роль ApplicationImpersonation** можна призначити вручну.

Для облікових записів сканування має бути призначена **роль ApplicationImpersonation**. Це дасть змогу ввімкнути обробник сканування для сканування поштових скриньок користувача в базах даних поштових скриньок Exchange. Якщо ви використовуєте Exchange Server 2010 або новішої версії, для облікового запису користувача створюється нова необмежена політика обмеження кількості запитів EWS.
Щоб уникнути ситуацій, коли від ESET Mail Security находить дуже багато запитів на виконання операцій (це може спричинити тайм-аут для певних запитів), налаштуйте політику обмеження кількості запитів EWS для облікового запису сканування. Більш докладно про політики обмеження кількості запитів див. в статтях EWS Best Practices (Рекомендації щодо EWS) і Understanding Client Throttling Policies (Основні відомості про політики м клієнта). Додаткові відомості й приклади див. в статті Change user throttling settings for specific users (Зміна параметрів обмеження кількості запитів для конкретних користувачів).

Щоб уручну призначити **роль ApplicationImpersonation** для облікового запису користувача й створити нову політику обмеження кількості запитів EWS для цього облікового запису, скористайтеся наведеними нижче командами (замініть `ESET-user` фактичним ім'ям облікового запису в системі; окрім того, політику обмеження кількості запитів EWS можна налаштувати, замінивши `$null` на потрібні значення):

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

На це може знадобитись певний час

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -
EWSFastSearchTimeoutInSeconds $null -EWSMaxConcurrency $null -
EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
EWSPercentTimeInMailboxRPC $null

Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-
```

```
ThrottlingPolicy
```

Exchange Server 2013, 2016 і 2019

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

На це може знадобитись певний час

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -
EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited

Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Типи поштового карантину

Диспетчер поштового карантину доступний для всіх трьох типів карантину:

- Локальний карантин
- Карантинна поштова скринька
- Карантин Microsoft Exchange

Вміст поштового карантину можна переглянути в диспетчері поштового карантину. Окрім того, локальний карантин можна переглянути у веб-інтерфейсі поштового карантину.

Зберігати повідомлення для одержувачів, які не існують

Цей параметр застосовується до повідомлень, позначених для перенесення в карантин антивірусом, антиспамом або на основі правил. Якщо цей параметр увімкнено, повідомлення, надіслані одержувачам, які не існують в Active Directory, зберігаються в поштовому карантині. Вимкніть цю функцію, якщо не потрібно зберігати такі повідомлення в поштовому карантині. Якщо цей параметр вимкнено, повідомлення невідомим одержувачам будуть автоматично видалятися.

Якщо потрібно переносити в карантин усі повідомлення одержувачам, які не існують, див. приклад.

Пропускати оцінювання правил під час розблокування електронних листів

Якщо розблокувати повідомлення з карантину, воно не буде оцінюватися за правилами. Це дасть змогу уникнути повернення повідомлення в карантин, а розблоковане повідомлення буде доставлено одержувачу. Ця функція використовується лише тоді, коли повідомлення розблоковує адміністратор. Якщо цю функцію вимкнуто або повідомлення розблоковано іншим користувачем (не адміністратором), це повідомлення оцінюватиметься за правилами.

> **i** Якщо ви розблокуєте повідомлення з карантину в кластерному середовищі, воно більше не буде переміщено в карантин іншими вузлами ESET Mail Security. Це досягається синхронізацією правил між вузлами кластера.

Генератор підписів електронних листів для багатосерверного середовища

Він дає змогу пропускати оцінку правил під час розблокування електронних листів у багатосерверному середовищі. Уведіть те саме початкове значення (рядок символів або парольну фразу) на всіх серверах, які потрібно зробити довіреними.

Формат конверта вкладення

Коли електронний лист розблоковується з карантину, він вкладається в нове повідомлення (конверт із вкладенням), яке потім доставляється одержувачу. Одержувач отримує оригінальне повідомлення, яке було розблоковано з поштового карантину як вкладення. Ви можете використовувати попередньо визначений формат конверта або змінити його відповідно до ваших вимог, використовуючи для цього доступні змінні.

Використовувати кластер ESET для зберігання всіх повідомлень у карантині на одному вузлі

Якщо ви використовуєте кластер ESET, цей параметр буде доступним. Рекомендуємо використовувати цю функцію, оскільки вона дає змогу зберігати файл локального карантину в одному місці — головному вузлі.

Головний вузол

Укажіть, який сервер є головним вузлом вашого кластера ESET. Після цього ви зможете отримати доступ до локального карантину на головному вузлі й керувати ним (для цього можна використовувати диспетчер поштового карантину в головному вікні програми або веб-інтерфейс поштового карантину).

Локальний карантин

Локальний карантин використовує локальну файлову систему для зберігання електронних листів карантину й бази даних SQLite як індексу. Збережені файли електронних листів карантину, а також файли бази даних шифруються з міркувань безпеки. Ці файли розташовані в каталозі C:\ProgramData\ESET\ESET Mail Security\MailQuarantine (у Windows Server 2012).

> **i** Шоб зберігати файли карантину на іншому диску, окрім C: (налаштовано за замовчуванням), змініть папку даних на потрібну під час інсталяції ESET Mail Security.

Функції локального карантину:

- Спам і електронні листи в карантині зберігатимуться в локальній файлової системі, а не в базі даних поштових скриньок Exchange.
- Шифрування й стискання локально збережених файлів електронних листів у карантині
- Веб-інтерфейс поштового карантину замість диспетчера карантину пошти.
- Дає змогу надсилати звіти про карантин як заплановане завдання на вказану адресу електронної пошти
- Видаляє файли електронних листів із вікна карантину (за замовчуванням через 21 день) і зберігає їх у файловій системі (поки не буде виконано автоматичне видалення після

вказаного періоду в днях).

• Автоматично видаляє старі файли електронних листів (через три дні за замовчуванням). Докладніше див. в розділі File storage settings (Параметри сховища файлів).

• Видалені файли електронних листів у карантині можна відновити з використанням eShell (якщо вони ще не були видалені з файлової системи).

• Дає змогу перевіряти електронні листи в карантині й приймати рішення про їхнє видалення або розблокування. Для перегляду електронних листів, які містяться в локальному карантині, і керування ними можна скористатися диспетчером поштового карантину в головному вікні програми або веб-інтерфейсом поштового карантину.

Недоліком використання локального карантину є те, що під час запуску кількох серверів ESET Mail Security із роллю "Транспортний сервер-концентратор" необхідно окремо керувати локальним карантином кожного сервера. Що більше поштових серверів, то більше сховищ карантину, якими потрібно керувати.

Сховище файлів

У цьому розділі можна змінити параметри сховища файлів, яке використовується локальним карантином.

Стиснути файли в карантині

Стиснуті файли в карантині займають менше місця на диску, але якщо ви вирішили не стискати файли, можна клацнути перемикач, щоб вимкнути стискання.

Очищати старі файли через (дн.)

Після утримання повідомлень протягом визначеного періоду (дні) вони видаляються з вікна карантину. Проте файли не видалятимуться з диска. Оскільки файли не видаляються з файлової системи, їх можна відновити за допомогою eShell.

Очищати видалені файли через (дн.)

Цей параметр видаляє файли з диска через зазначену кількість днів. Неможливо буде відновити їх після видалення (якщо у вас немає рішення для резервного копіювання файлової системи).

Веб-інтерфейс

Веб-інтерфейс поштового карантину є альтернативою диспетчеру поштового карантину, проте він доступний лише для локального карантину.

Веб-інтерфейс поштового карантину недоступний на сервері з роллю "Межовий транспорт", оскільки Active Directory недоступна для автентифікації.

Веб-інтерфейс поштового карантину дає змогу переглянути стан поштового карантину. Окрім того, він дає змогу керувати електронними листами в карантині. Цей веб-інтерфейс доступний

за посиланнями зі звітів про карантин або за посиланням для веб-браузера.

Щоб отримати доступ до веб-інтерфейсу поштового карантину, необхідно пройти автентифікацію за допомогою облікових даних домену. Microsoft Internet Explorer автоматично автентифікує користувача домену. Однак сертифікат веб-сторінки має бути дійсним, автоматичний вхід — ввімкнутим у Microsoft Internet Explorer, а веб-сайт із поштового карантину — доданим в місця локальної інтрамережі.

Будь-який користувач в Active Directory може отримати доступ до веб-інтерфейсу поштового карантину, але бачитиме лише елементи в карантині, надіслані на його адресу електронної пошти (включно з псевдонімами користувача). Адміністратор може переглядати всі елементи в карантині для всіх одержувачів.

ESET Mail Security не використовує IIS для запуску веб-інтерфейсу поштового карантину. Натомість використовується API HTTP-сервера, зокрема підтримка SSL. Це дає змогу обмінюватися даними через безпечні підключення HTTP.

Веб-адреса

Це URL-адреса, за якою буде доступний веб-інтерфейс поштового карантину. За замовчуванням використовується FQDN сервера з `/quarantine` (наприклад, `mailserver.company.com/quarantine`). Замість `/quarantine` можна вказати власний віртуальний каталог. URL-адресу веб-інтерфейсу можна змінити в будь-який час.

Веб-посилання має бути вказано без протоколу (HTTP, HTTPS) або номера порту; для нього використовуйте тільки форму fqdn/virtualdirectory. Окрім того, замість FQDN можна використовувати групові символи.

Після зміни URL-адреси веб-сторінки неможливо буде повернутися до стандартної веб-сторінки за допомогою піктограми відновлення налаштувань. Видаліть запис і залиште поле пустим. Перезавантажте сервер. Коли ESET Mail Security запуститься і визначить, що URL-адреса веб-інтерфейсу є пустою, вона автоматично заповнить це поле значенням за замовчуванням (`fqdn/quarantine`).

ESET Mail Security підтримує такі форми URL-адреси веб-інтерфейсу:
Явний груповий символ (+/quarantine)
Явний (mydomain.com/quarantine)
Груповий символ, прив'язаний до IP-адреси (192.168.0.0/quarantine)
Груповий символ (*/quarantine)
Докладніше див. в розділі **Host-Specifier Categories** (Категорії вказування хоста) статті UrlPrefix Strings (Рядки UrlPrefix).

Мови звітів і веб-інтерфейсу

Ця функція дає змогу задати мову веб-інтерфейсу поштового карантину й звітів про карантин.

Порт HTTPS

Для веб-інтерфейсу використовується порт HTTPS. За замовчуванням використовується порт 443.

Порт HTTP

Використовується для розблокування електронних листів із карантину через звіти електронною поштою.

> Якщо в IIS не інстальовано сертифікат SSL, налаштуйте прив'язку порту HTTPS. Якщо ви змінюєте номер порту для HTTPS або HTTP, обов'язково додайте відповідну прив'язку порту в IIS.

Реєструвати випуск з карантину як події

Під час розблокування елементів із поштового карантину ця дія записується у файли журналу.

Активувати адміністраторів за замовчуванням

За замовчуванням учасникам групи адміністраторів надається доступ для адміністрування веб-інтерфейсу поштового карантину. Для адміністраторського доступу немає обмежень. Він дає змогу адміністратору переглядати всі елементи в карантині для всіх одержувачів. Якщо вимкнути цей параметр, лише облікові записи користувачів із правами адміністратора матимуть доступ до веб-інтерфейсу поштового карантину.

Додаткові права доступу

Ця функція дає змогу користувачам керувати поштовим карантином інших користувачів. Адміністраторів карантину можна призначити, надавши користувачу (або групі) додатковий доступ до веб-інтерфейсу поштового карантину іншого користувача (або всіх учасників групи) для керування елементами в карантині.

1. Клацніть **Змінити**, щоб відкрити вікно додаткових прав доступу, а потім клацніть **Додати**.

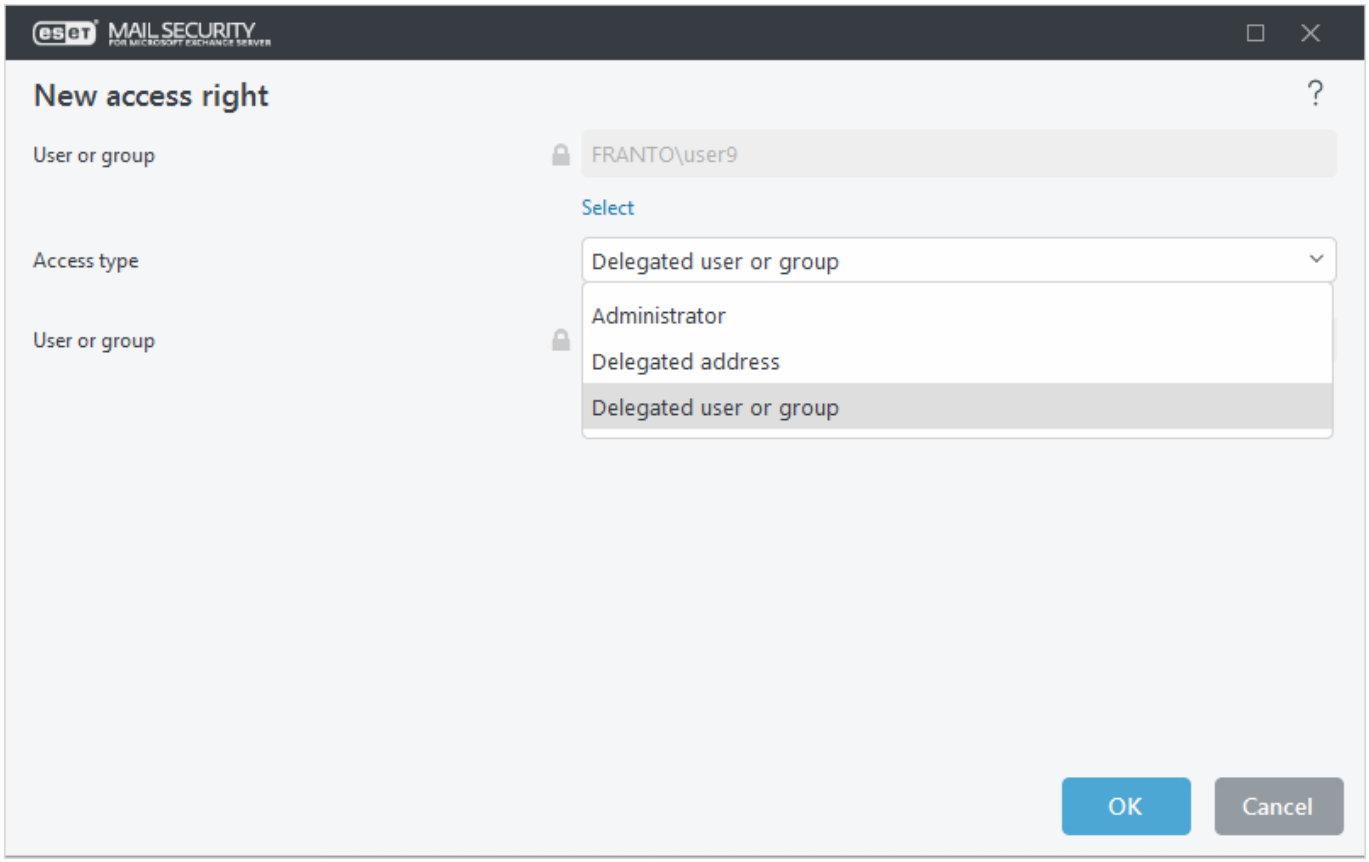
2. Клацніть **Вибрати** й скористайтеся селектором об'єктів Active Directory, щоб вибрати користувача або групу, до складу якої входить користувач, для надання доступу до поштового карантину.

3. У розкривному меню виберіть пункт **Тип доступу**:

   • **Адміністратор**: користувач має доступ адміністратора до веб-інтерфейсу поштового карантину.

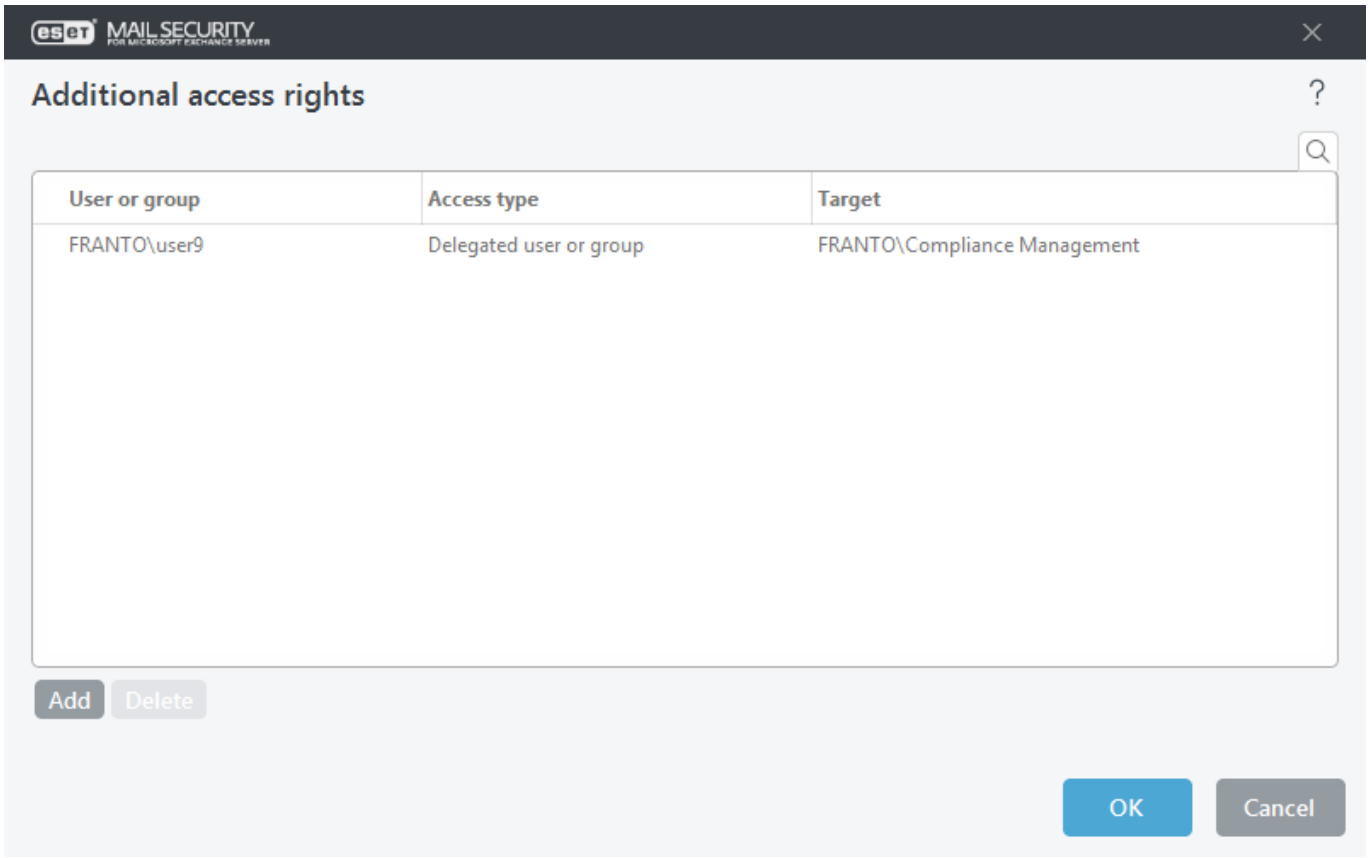
   • **Делегований доступ**: користувачу (представнику) дозволено переглядати повідомлення в карантині для іншого одержувача й керувати ними. Укажіть адресу одержувача: уведіть адресу електронної пошти користувача, карантинними повідомленнями якого буде керувати користувач із делегованим доступом. Якщо користувач має псевдоніми в Active Directory, за потреби можна додати додаткові права доступу для кожного псевдоніма.

   • **Делегований користувач або група**: те саме, що й делегований доступ; користувач також може використовувати селектор об'єктів Active Directory, щоб вибрати користувача або групу, до складу якої входить користувач, карантином якого потрібно керувати.

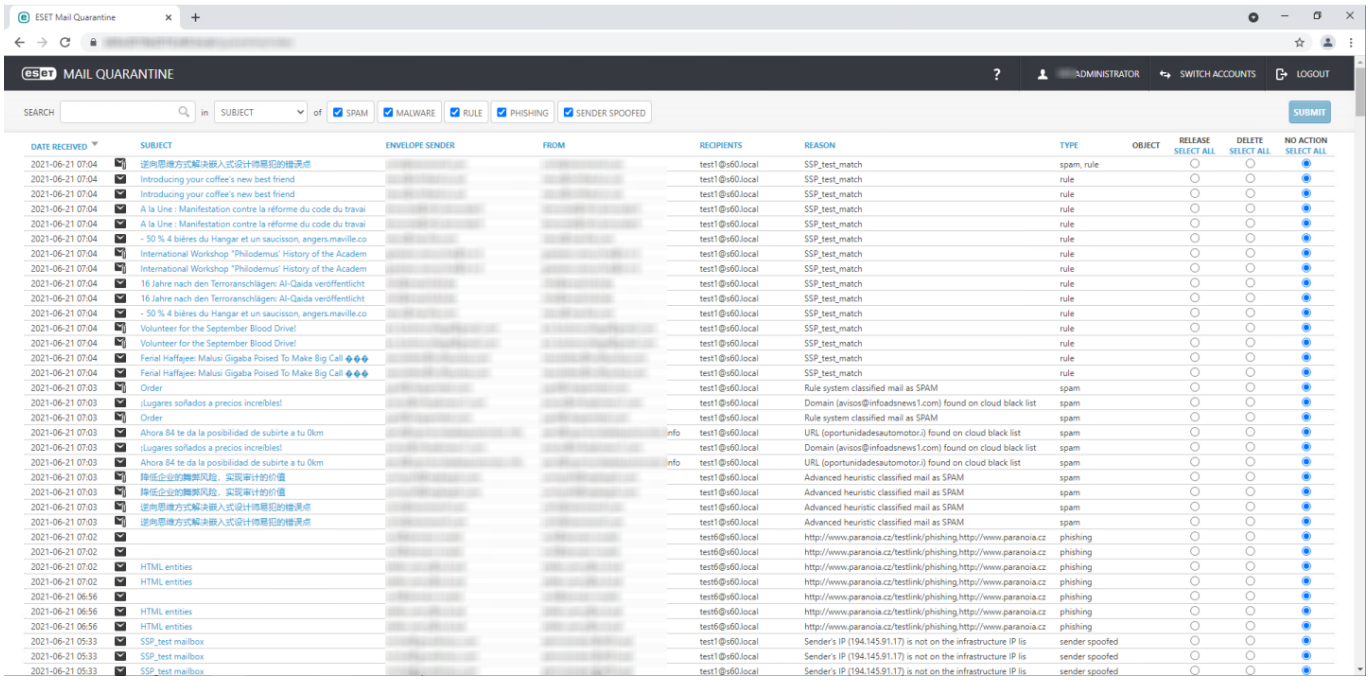


4. Клацніть **Вибрати** й виберіть користувача або групу, до складу якої входить користувач, карантином якого керуватиме делегований користувач, вибраний на кроці 2.

Приклад користувачів, яким було надано додаткові права доступу до веб-інтерфейсу поштового карантину:



Щоб отримати доступ до веб-інтерфейсу поштового карантину, відкрийте веб-браузер і скористайтеся URL-адресою, указаною в полі **Поштовий карантин** (**Додаткові параметри** (**F5**) > **Сервер** > **Поштовий карантин** > **Веб-інтерфейс**).



Реліз

Розблоковує надсилання електронних листів їхнім початковим одержувачам за допомогою каталогу відтворення і видаляє їх із карантину. Клацніть **Надіслати**, щоб підтвердити дію.

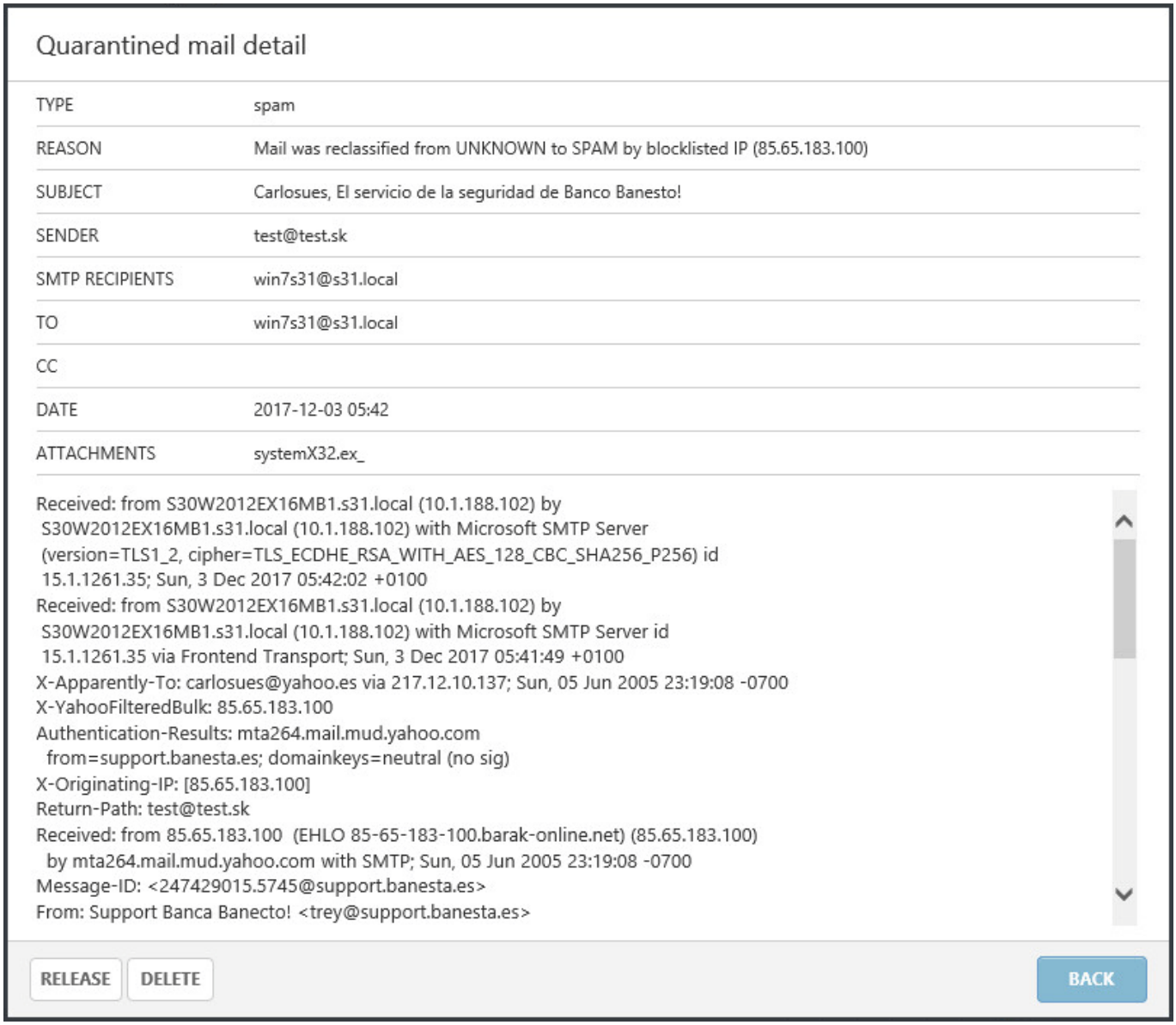
> Якщо розблокувати повідомлення електронної пошти з карантину, ESET Mail Security ігнорує заголовок MIME To:, оскільки його легко підробити. Натомість використовується вихідна інформація про одержувача з команди `RCPT TO:`, яка отримується під час SMTP-з'єднання. Це гарантує, що розблоковане з карантину повідомлення надійде потрібному одержувачу.

Видалити

Ця функція видаляє елементи з карантину. Клацніть **Надіслати**, щоб підтвердити дію.

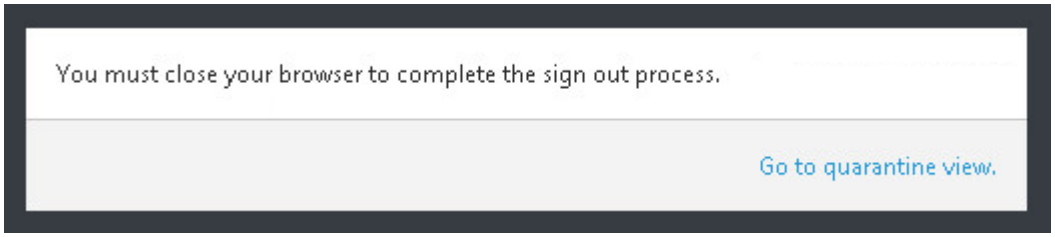
Якщо клацнути **Тема**, відкриється спливаюче вікно з докладними відомостями ("Тип", "Причина", "Відправник", "Дата", "Вкладення" тощо) про електронний лист у карантині.

Клацніть **Показати заголовки**, щоб переглянути заголовок електронного листа в карантині.



За потреби клацніть **Розблокувати** або **Видалити**, щоб вжити дію до переміщеного в карантин електронного листа.

Щоб повністю вийти з веб-інтерфейсу поштового карантину, закрийте вікно браузера. В іншому разі клацніть подання **"Перейти в карантин"**, щоб повернутися на попередній екран.



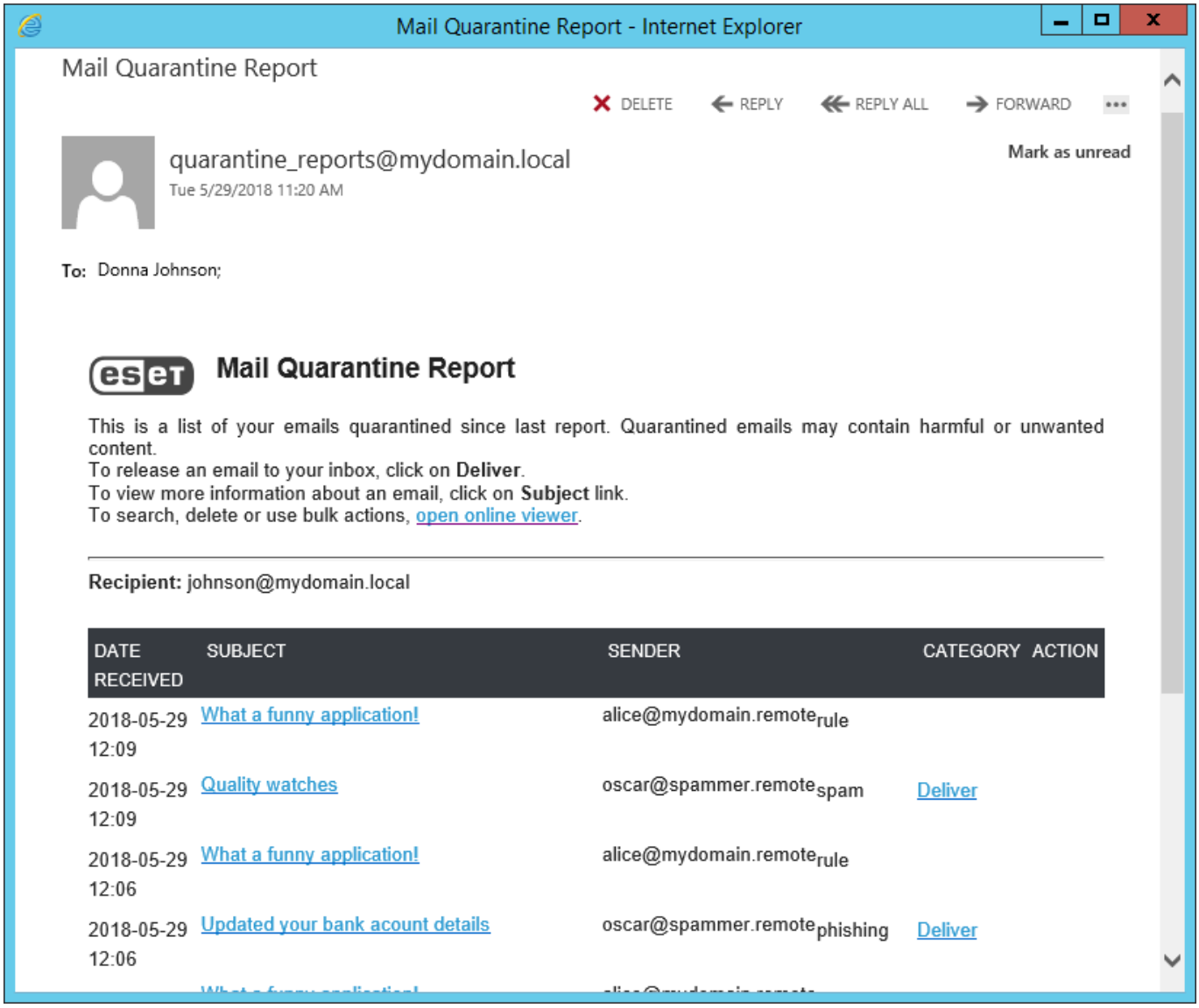
Якщо у вас виникли проблеми з доступом до веб-інтерфейсу поштового карантину в браузері або з'являється помилка, подібна до HTTP Error 403.4 - Forbidden, переконайтеся, що для типу карантину вибрано **Локальний карантин** і ввімкнено параметр **Увімкнути веб-інтерфейс**.

Надіслати звіти про поштовий карантин: заплановане завдання

Звіти про поштовий карантин — це сповіщення електронною поштою, які надсилаються вибраним користувачам і адміністраторам, з інформацією про те, що їхні електронні листи поміщено в карантин ESET Mail Security. Звіти містять посилання, які дають змогу вам, а також користувачам, які отримують звіти про поштовий карантин, безпосередньо видаляти або розблоковувати (доставляти) повідомлення електронної пошти, поміщене в карантин через помилкове спрацювання. Звичайним користувачам не дозволяється доставляти певні повідомлення, які відфільтровані за правилами або поміщені в поштовий карантин антивірусним захистом.

Щоб почати надсилати звіти про карантин, створіть заплановане завдання ("Інструменти" > Розклад > "Додати завдання") і виберіть тип завдання Надіслати звіти про поштовий карантин або Надіслати адміністраторські звіти про поштовий карантин. Під час вибору одержувачів пов'язані поштові скриньки додаються до списку доступних поштових скриньок.

Завдання "Надіслати звіти про поштовий карантин" або "Надіслати адміністраторські звіти про поштовий карантин" надсилає звіт поштового карантину електронною поштою відповідно до запланованого завдання. Нижче наведено приклад звіту про поштовий карантин:



У звіті про поштовий карантин також міститься посилання на веб-інтерфейс поштового карантину користувача (відкривається в онлайн-засобі перегляду).

Завдання "Надіслати звіти про поштовий карантин" доступне лише в разі використання **локального карантину**. Ви не зможете використовувати його з карантинною поштовою скринькою і карантином MS Exchange.

Адреса відправника

Укажіть адресу електронної пошти, яка буде відображатися як відправник звіту про поштовий карантин.

Максимальна кількість записів у звіті

Можна обмежити кількість записів у звіті. Для лічильника за замовчуванням встановлено значення 50.

Веб-адреса

Цю URL-адреса буде додано в звіт "Поштовий карантин", щоб одержувач міг просто клацнути посилання для отримання доступу до веб-інтерфейсу поштового карантину.

Одержувачі

Виберіть користувачів, які будуть отримувати звіти про поштовий карантин. Клацніть **Змінити**, щоб вибрати поштові скриньки для конкретних одержувачів (пов’язані поштові скриньки також підтримуються).

> Звіт про поштовий карантин надсилатиметься, тільки якщо є повідомлення в карантині. Якщо карантин порожній або з моменту останнього звіту в нього не було додано нових елементів, звіт не надсилатиметься. Якщо надсилається звіт про поштовий карантин, він міститиме лише елементи, нещодавно додані з часу останнього звіту (а не весь вміст карантину).

> Мета: створити заплановане завдання, щоб регулярно надсилати звіти про поштовий карантин собі як адміністратору або інформувати користувачів про їхні спамові повідомлення, які зараз зберігаються в поштовому карантині.
> Виберіть пункти **Інструменти** > **Розклад** > **Додати завдання** і відкрийте майстер.
> Уведіть **назву завдання** і в розкривному меню виберіть **тип завдання**.
> Виберіть **Надіслати звіти про поштовий карантин** (звіт буде містити тільки спамові повідомлення конкретного користувача) або **Надіслати адміністраторські звіти про поштовий карантин** (звіт буде містити всі повідомлення зі всього карантину), потім клацніть **Далі**.
> Виберіть один із параметрів, які потрібно визначити для виконання завдання. Наприклад, **Щотижня** о **10:00:00** по **п’ятницях**.
> Укажіть **адресу відправника** (administrator@mydomain.com).
> Клацніть **Змінити**, щоб додати **одержувачів** зі списку. Виберіть поштові скриньки користувача, які отримуватиме звіти про поштовий карантин.

Веб-інтерфейс поштового карантину користувача

Вам надали доступ до веб-інтерфейсу, у якому можна керувати повідомленнями в карантині, зокрема спамом, повідомленнями з підробленим відправником або фішинговими повідомленнями, а також повідомленнями, які відфільтровані правилами, заданими адміністратором. Зазвичай ви можете бачити лише ті повідомлення в карантині, які було надіслано на вашу адресу електронної пошти. Однак якщо вам делегували право керувати карантинними повідомленнями інших користувачів, для вас також відобразяться повідомлення цих користувачів. Повідомлення можна розрізняти за одержувачами. Скористайтеся функцією пошуку, щоб відфільтрувати повідомлення, наприклад, за одержувачем.

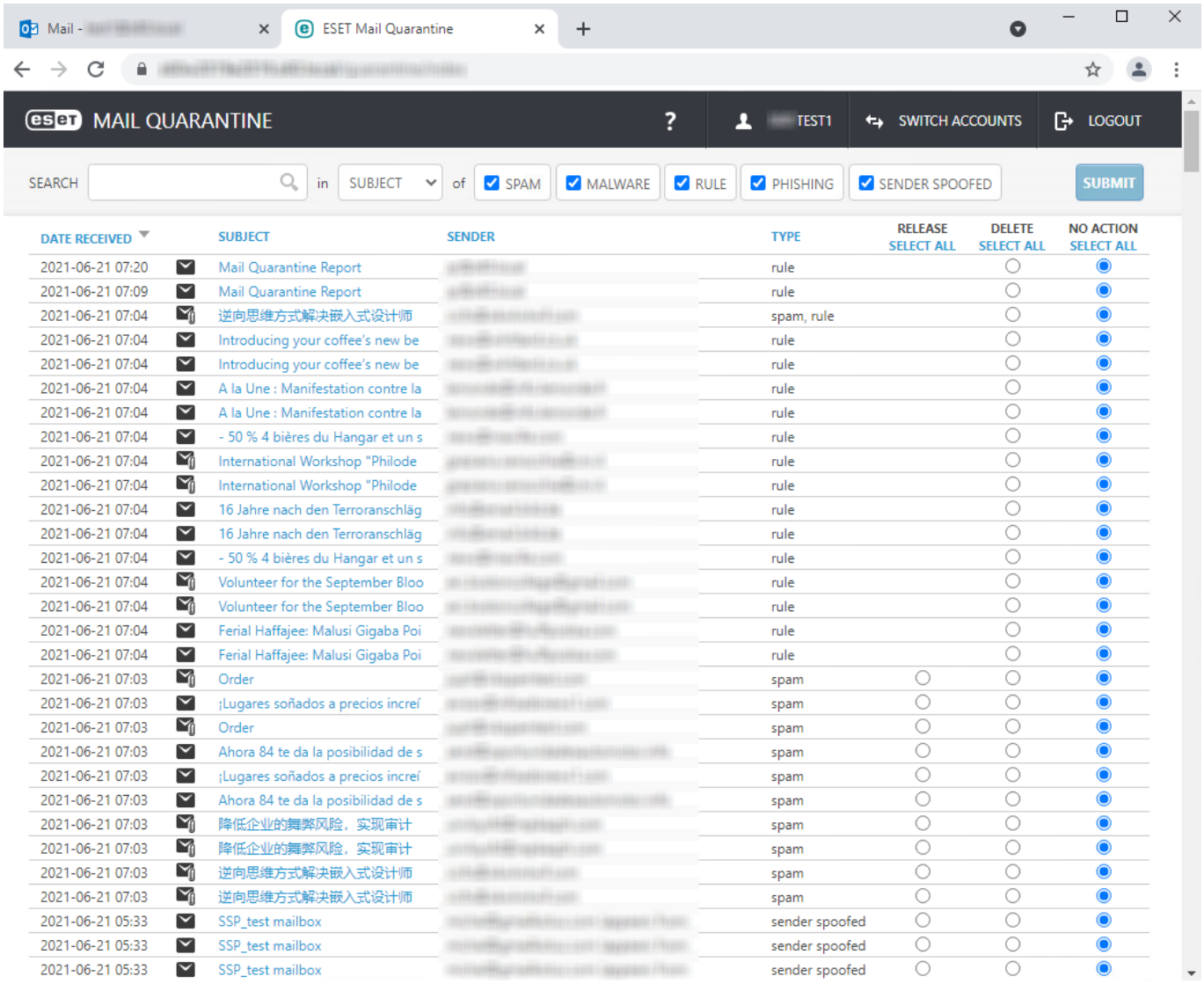
Можна вибрати дію, яка застосовуватиметься до повідомлення або кількох повідомлень (**розблокувати**, **видалити** або **жодних дій**). Доступність дій залежить від рівня доступу й параметрів правила. Наприклад, ви не зможете розблокувати або видалити повідомлення певних типів.

Якщо вам призначено права адміністратора, для вас будуть відображатися всі повідомлення в карантині для всіх користувачів; ви зможете виконати будь-яку дію.

Керування повідомленнями в карантині:

Веб-інтерфейс поштового карантину дає змогу переглядати елементи в карантині. Якщо ви делегували доступ або навіть адміністратора, для вас також відобразяться інші повідомлення з

карантину.



У нижньому лівому куті вікна можна змінити кількість записів на сторінку (розмір сторінки).

Якщо повідомлень забагато, скористайтеся функцією "Пошук" у верхньому рядку, щоб знайти конкретний електронний лист або відфільтрувати вміст за темою, відправником або одержувачем (одержувач доступний тільки для користувачів із делегованим доступом або правами адміністратора). Окрім того, можна використовувати прапорці, щоб відображати лише повідомлення певного типу (**спам**, **шкідливі повідомлення**, **відфільтровані за правилом**, **фішингові** й **повідомлення з підробленим відправником**).

Щоб розблокувати (доставити) повідомлення, поміщене в карантин через помилкове спрацювання під час класифікації, скористайтеся перемикачами праворуч і виберіть пункт **Розблокувати**. Щоб видалити повідомлення, виберіть дію **Видалити**.

Одночасно можна вибрати кілька повідомлень із відповідною дією. Коли все буде готово, клацніть **Відправити**.

Після цього повідомлення, позначені для розблокування, надсилаються в поштову скриньку або у вихідну поштову скриньку одержувача, якщо ви делегували доступ і розблоковуєте повідомлення для інших користувачів. Повідомлення, позначені для видалення, остаточно видаляються з карантину.

Обидві дії **Розблокувати** й **Видалити** стануть незворотними після натискання пункту **Надіслати**.

Після натискання пункту "Надіслати", подання оновлюється автоматично, проте його можна оновити вручну за допомогою кнопки "Оновити" у вашому веб-браузері або клавіши **F5**.

Можна розблокувати лише спам і повідомлення з підробленим відправником. Не дозволено розблоковувати шкідливе програмне забезпечення, фішингові повідомлення, а також повідомлення, заблоковані відповідно до правил. Якщо потрібно розблокувати таке повідомлення, зверніться до адміністратора.

Немає потреби регулярно видаляти повідомлення з карантину, тому що вони видаляються автоматично через певний період часу, визначений адміністратором.

Щоб повністю вийти з веб-інтерфейсу поштового карантину, закрийте вікно веб-браузера. В іншому разі клацніть подання "Перейти в карантин", щоб повернутися на попередній екран.

Карантинна поштова скринька й карантин Microsoft Exchange

Якщо ви вирішите не використовувати локальний карантин, у вас є два варіанти: карантинна поштова скринька або карантин MS Exchange. Для будь-якого варіанту потрібно створити спеціального користувача з поштовою скринькою (наприклад, main_quarantine@company.com), яка буде використовуватися для зберігання електронних листів у карантині. Диспетчер поштового карантину також буде використовувати цього користувача й поштову скриньку для перегляду елементів і керування ними в карантині. У параметрах диспетчера карантину потрібно вказати дані облікового запису цього користувача.

Перевага використання карантину поштової скриньки / карантину Microsoft Exchange у порівнянні з локальним карантином полягає в тому, що елементами поштового карантину можна керувати з одного місця незалежно від того, скільки серверів мають роль "Транспортний сервер-концентратор". На відміну від локального карантину, карантинна поштова скринька / карантин MS Exchange, спам і електронні листи в карантині зберігаються в базах даних поштових скриньок Exchange. Будь-який користувач, який має доступ до карантинної поштової скриньки, може керувати повідомленнями в карантині.

Порівнюючи карантинну поштову скриньку й карантин MS Exchange, майте на увазі, що в обох варіантах використовується спеціальна поштова скринька як основний механізм зберігання повідомлень у карантині. Ці варіанти дещо відрізняються способом доставки електронних листів у поштову скриньку. Карантинна поштова скринька й карантин MS Exchange:

Карантинна поштова скринька

ESET Mail Security створює електронний лист-обгортку з додатковою інформацією, вкладає до нього оригінальні електронні листи й доставляє в поштову скриньку.

Укажіть адресу карантину повідомлень (наприклад, main_quarantine@company.com).

Не рекомендуємо використовувати обліковий запис адміністратора як карантинну поштову скриньку.

Карантин MS Exchange

Доставка електронного листа в саму поштову скриньку повністю залежить від Microsoft Exchange Server. Поштову скриньку потрібно зробити карантинною на рівні організації в Active Directory (за допомогою наведеної нижче команди PowerShell).

За замовчуванням внутрішній карантин не активовано в Microsoft Exchange Server. Якщо ви його не активували, відкрийте оболонку керування Exchange і введіть таку команду (замініть `Name@domain.com` на фактичну адресу виділеної поштової скриньки): `Set-ContentFilterConfig -QuarantineMailbox name@domain.com`

ESET Mail Security використовує систему карантину Microsoft Exchange (це стосується Microsoft Exchange Server 2010 і новіших версій). У цьому разі для зберігання потенційно інфікованих повідомлень і СПАМУ використовується внутрішній механізм Exchange.

Параметри диспетчера карантину

Адреса хоста

Вона з'явиться автоматично, якщо в локальному середовищі є Exchange Server із роллю сервера клієнтського доступу (CAS). Якщо на сервері з інстальованим ESET Mail Security немає ролі сервера клієнтського доступу (CAS), проте вона присутня в Active Directory (AD), адреса хоста також з'явиться автоматично. Якщо вона не з'явиться, можна ввести ім'я хоста вручну. Автоматичне виявлення не працюватиме для серверної ролі "Межовий транспорт". IP-адреса не підтримується. Потрібно використовувати ім'я хоста сервера CAS.

Ім'я користувача

Спеціальний обліковий запис користувача карантину, створений для зберігання повідомлень у карантині (або обліковий запис, який має доступ до цієї поштової скриньки через механізм делегування доступу). Для серверної ролі "Межовий транспорт", яка не входить до домену, необхідно використовувати всю адресу електронної пошти (наприклад, *main_quarantine@company.com*).

Пароль

Уведіть пароль облікового запису карантину.

Використовувати SSL

Потрібно ввімкнути, якщо для веб-служб Exchange (EWS) у IIS задано значення **Вимагати SSL**. Якщо SSL увімкнено, сертифікат Exchange Server потрібно імпортувати в систему з ESET Mail Security (якщо ролі Exchange Server розташовано на різних серверах). Параметри EWS можна переглянути в IIS у розділі Sites/Default web site/EWS/SSL Settings.

Вимкніть параметр **Використовувати SSL**, лише якщо Exchange Web Services (EWS) у IIS налаштовано таким чином, щоб не вимагати SSL.

Ігнорувати помилку сертифіката сервера

Ігнорує такі стани: self-signed, wrong name in certificate, wrong usage, expired.

Проксі-сервер

Якщо ви використовуєте проксі-сервер між Exchange Server із роллю CAS і сервером Exchange Server з інстальованим ESET Mail Security, укажіть параметри проксі-сервера. Це потрібно, оскільки ESET Mail Security підключається до API веб-служб Exchange (EWS) за протоколом HTTP/HTTPS. В іншому разі карантинна поштова скринька й карантин Microsoft Exchange не працюватимуть.

Проксі-сервер

Уведіть IP-адресу або ім’я проксі-сервера, який ви використовуєте.

Порт

Уведіть номер порту проксі-сервера.

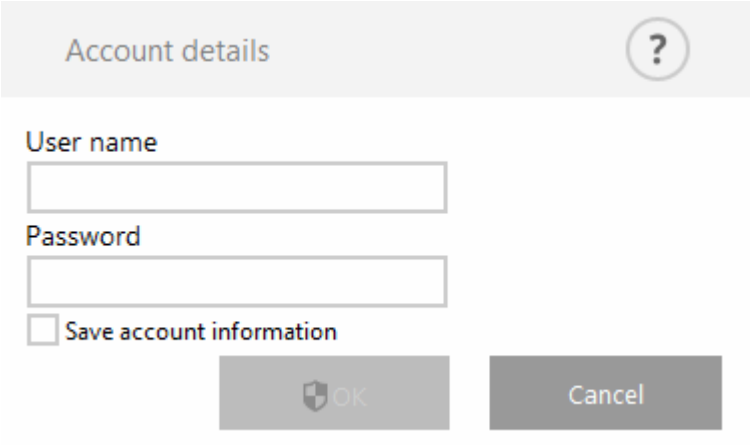
Ім’я користувача, пароль

Уведіть облікові дані, якщо на проксі-сервері потрібно проходити автентифікацію.

Відомості про обліковий запис диспетчера карантину

У цьому діалоговому вікні відображатимуться застереження в разі, якщо ви не вказали дані облікового запису (ім’я користувача й пароль) для диспетчера карантину. Укажіть облікові дані користувача, який має доступ до карантинної поштової скриньки, і клацніть **ОК**. Можна скористатися таким варіантом: натисніть клавішу **F5**, щоб відкрити розділ **Додаткові параметри** і виберіть пункти **Сервер** > **Карантин** > Параметри диспетчера карантину.

Уведіть **ім’я користувача** й **пароль** для вашої карантинної поштової скриньки.



Установіть прапорець поруч із пунктом **Зберегти інформацію про обліковий запис**, щоб зберегти параметри облікового запису для майбутнього використання під час доступу до

диспетчера карантину.

Підписання DKIM

Підписання DKIM (DomainKeys Identified Mail) — це метод, який дає змогу захистити вихідні електронні листи й полегшити перевірку. Цей метод надає поштовим серверам-одержувачам точний спосіб відрізнити автентичні повідомлення від спаму.

Автентифікація DKIM працює таким чином:

- Заголовки вихідних електронних листів підписуються за допомогою закритого ключа DKIM.
- Поштовий сервер-одержувач перевіряє запис DKIM DNS, що містить відкритий ключ.
- Якщо підпис із закритим ключем у заголовках повідомлень збігається з відкритим ключем запису DKIM DNS, лист вважається автентичним і надсилається одержувачам.
- Якщо підпис і відкритий ключ не збігаються, дія, яку буде застосовано до електронного листа, залежить від конфігурації поштового сервера-одержувача (на ньому можуть діяти певні правила, наприклад, ESET Mail Security з цією метою використовує умову правила результату DKIM).

Щоб скористатися функцією підписування DKIM у ESET Mail Security, переконайтеся, що для вашого домену налаштовано запис DKIM DNS. Більш докладну інформацію про створення запису DKIM див. в статті What is DKIM record and how to create it? (Що таке запис DKIM і як його створити?) У цій статті також наведено приклад запису DKIM. Окрім того, для створення закритих і відкритих ключів можна спробувати скористатися онлайн-генератором DKIM.

Після цього рекомендуємо скористатися інструментом DKIM Record Checker або MXToolBox для перевірки наявності відкритого ключа DKIM і правильності його синтаксису.

Налаштуйте підписування DKIM у ESET Mail Security. Для цього вкажіть домени DKIM і список заголовків електронної пошти для підписування. Підпис DKIM додається в заголовки вибраних повідомлень. Кожен підпис DKIM містить інформацію, яку поштові сервери можуть використовувати для перевірки автентичності електронного листа під час його передавання до кінцевого пункту призначення. Якщо ви використовуєте кілька доменів для вихідних повідомлень, для кожного домену підписування DKIM можна налаштувати окремо.

> У розділі **Додаткові параметри** виберіть **Сервер** > Інтеграція і ввімкніть параметр **Підписання DKIM**. Для налаштування пріоритету агента рекомендуємо не змінювати пріоритет агента ESET DKIM, залишивши його останнім у списку. Таким чином ви будете впевнені, що підписування заголовків виконуватиметься наостанок після того, як попередні агенти внесуть у них усі потрібні зміни.

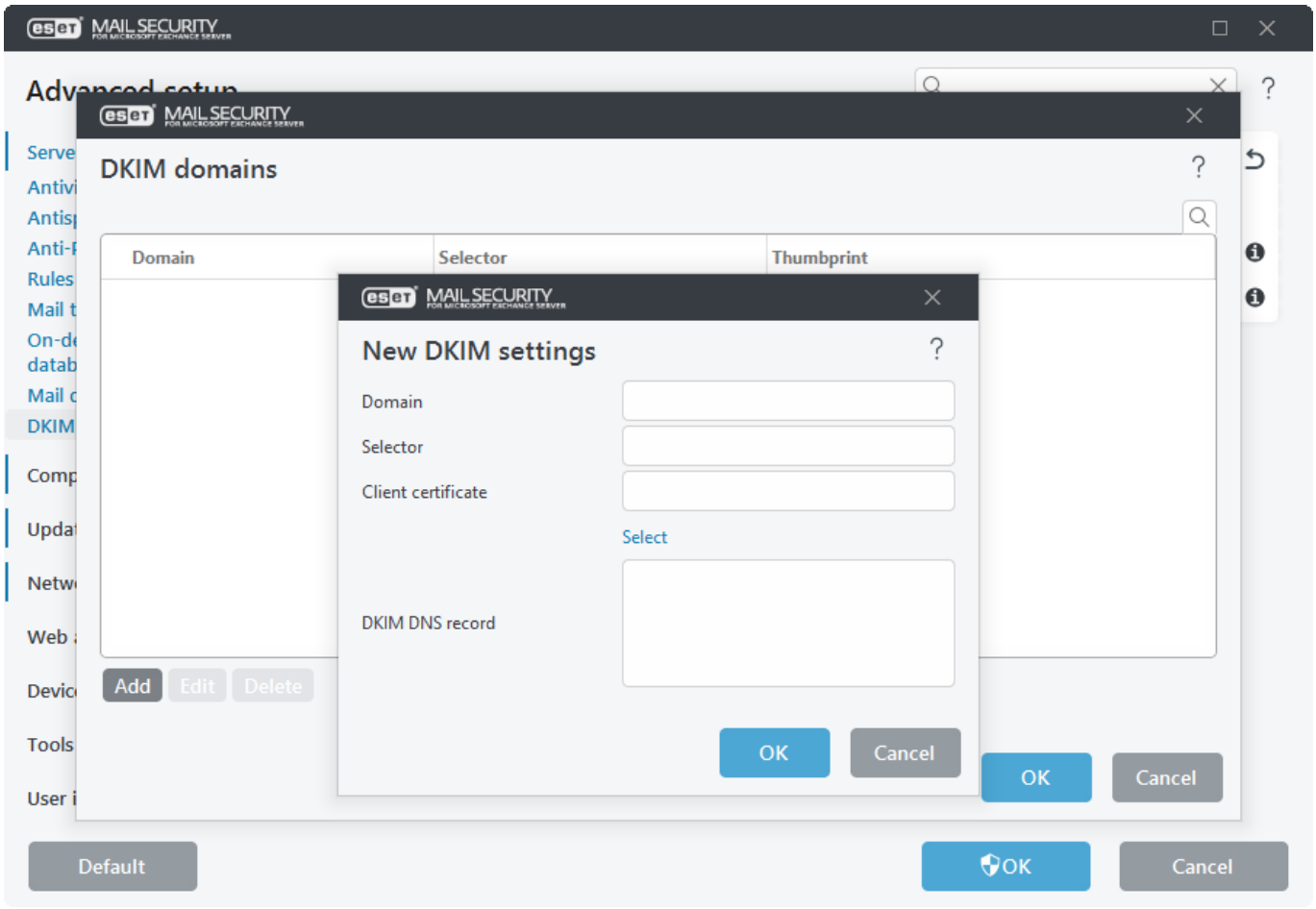
Домени DKIM

Визначте параметри для кожного домену для підписування DKIM. Клацніть **Змінити**, щоб відкрити вікно доменів DKIM. Клацніть **Додати**, щоб створити **нові параметри DKIM**, або "Змінити", щоб змінити наявні.

• **Домен**: уведіть домен (наприклад, *domainname.local*).

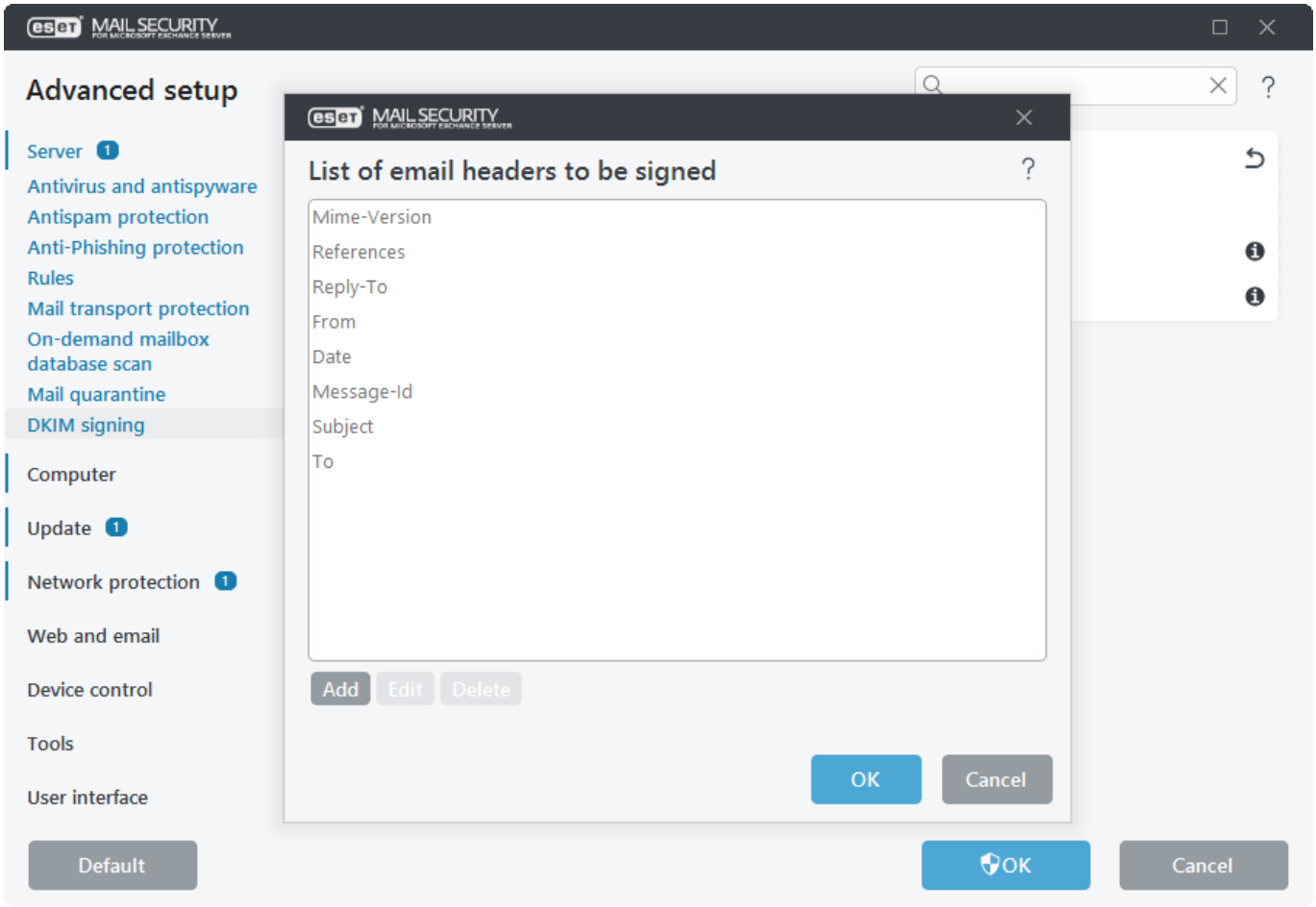
• **Селектор**: визначте селектор для атрибута підпису DKIM; потім його буде записано в поле заголовка DKIM-Signature

• **Сертифікат клієнта**: клацніть **Вибрати** й виберіть сертифікат клієнта, який використовувався для підписування DKIM.



Список заголовків електронних листів для підпису

Клацніть **Змінити**, щоб відкрити вікно "Список заголовків електронних листів для підпису". Клацніть **Додати**, щоб додати нові заголовки, або **Змінити**, щоб змінити наявні заголовки в списку.



Перевірка антивірусу

Щоб переконатися, що захист у режимі реального часу працює і виявляє віруси, скористайтеся перевірочним файлом із веб-сайту eicar.com. Цей файл створено EICAR (European Institute for Computer Antivirus Research). Він є безпечним; його виявляють усі антивірусні програми.

Щоб перевірити функціональність антивірусу, створіть текстовий файл із таким рядком:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Щоб отримати додаткову інформацію і завантажити тестові файли, відвідайте https://www.eicar.org/download-anti-malware-testfile/

Перевірка функції "Антиспам"

Тестовий рядок GTUBE (Generic Test for Unsolicited Bulk Email) дає змогу перевірити, чи виявляє функція "Антиспам" ESET Mail Security вхідні повідомлення зі спамом.

Щоб перевірити функцію антиспаму, вставте наведений нижче рядок довжиною 68 байт у текст електронного листа й надішліть його:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Використовуйте рядок так, як його наведено (на одному рядку, без пробілів і розривів рядка). Відповідний електронний лист можна завантажити у форматі RFC-822.

Перевірка функції "Захист від фішинг-атак"

Щоб перевірити функцію "Захист від фішинг-атак", вставте наведене нижче посилання (URL-адресу) в текст або тему електронного листа й надішліть його:

https://www.amtso.org/check-desktop-phishing-page/

Щоб переглядати активність захисту електронної пошти від фішинг-атак, установіть прапорець **Файли журналу** > Журнал захисту поштового сервера. Цей журнал буде містити відомості про електронні листи й знайдені фішингові посилання.

Загальні параметри

Ви можете налаштувати загальні параметри й опції залежно від ваших потреб. Меню зліва містить такі категорії:

Computer

Увімкнення або вимкнення виявлення потенційно небажаних, небезпечних, підозрілих програм і модуля "Антируткіт". Укажіть виключення процесів або файлів і папок. Налаштуйте захист файлової системи в режимі реального часу, параметри ThreatSense, захист на основі хмари (ESET LiveGrid®), сканування комп'ютера на наявність шкідливого програмного забезпечення (сканування комп'ютера за вимогою й інші варіанти сканування), сканування Hyper-V та HIPS.

Оновлення

Налаштуйте опції оновлення, як-от профілі, дату створення ядра виявлення, знімки для відкочування модуля, тип оновлення, спеціальний сервер оновлення, підключення/проксі-сервер, дзеркало оновлення, доступ до файлів оновлення, сервер HTTP, дані облікового запису користувача для мережевого підключення тощо.

Захист мережі

Керування захистом мережі: відомі мережі, зони, захист від мережевих атак (IDS), захист від атак повним перебором і захист від ботнетів.

Інтернет і електронна пошта

Дає змогу налаштувати фільтрацію протоколів і виключення (виключені програми та IP-адреси), опції фільтрації протоколів SSL/TLS, захист поштового клієнта (інтеграція, протоколи електронної пошти, сигнали й сповіщення), захист доступу до Інтернету (веб-протоколи HTTP/HTTPS і керування URL-адресами) та захист поштового клієнта від фішинг-атак.

Контроль пристроїв

Увімкніть інтеграцію й налаштуйте правила та групи контролю пристроїв.

Конфігурація інструментів

Дозволяє налаштовувати інструменти, як-от ESET CMD, ESET RMM, постачальник WMI, цільові об’єкти сканування ESET PROTECT, сповіщення Windows Update, файли журналу, проксі-сервер, сповіщення електронною поштою, діагностичні дані, кластер тощо.

Сповіщення

Дає змогу налаштувати сповіщення, які відображатимуться на робочому столі або надсилатимуться електронною поштою для статусів програм, сповіщень на робочому столі, інтерактивних сповіщень і пересилання.

Інтерфейс користувача

Дає змогу налаштувати головне вікно програми, інформацію про ліцензію, захист паролем, політику виконання eShell тощо.

Computer

Ядро виявлення захищає систему від атак шкідливого програмного забезпечення через сканування файлів, електронних листів і підключень до мережі. Якщо виявляється об’єкт, класифікований як шкідливе програмне забезпечення, запускається процес виправлення. Ядро виявлення може знешкодити такий об’єкт: заблокувати його й застосувати до нього відповідну дію (очищення, видалення або переміщення в карантин).

Захист у режимі реального часу й за допомогою машинного навчання

Удосконалене машинне навчання тепер застосовується в ядрі виявлення для підвищення рівня захисту, що покращує виявлення на основі машинного навчання. Дізнайтеся більше про цей тип захисту в глосарії. Рівні звітування та захисту можна налаштувати для таких категорій:

Шкідливе програмне забезпечення

Комп’ютерний вірус – це шкідливий код, який додається на початок або в кінець файлів на комп’ютері. Проте термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення". Виявлення шкідливого програмного забезпечення здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Дізнайтеся більше про ці типи програм у глосарії.

Потенційно небажані програми

Потенційно небажана програма — це програмне забезпечення, яке не обов’язково має бути зловмисним, однак може інсталювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, виконувати неочікувані для користувача дії, не підтверджені ним операції чи мати інші неясні цілі.

До таких програм належать такі: ПЗ, що показує рекламу або завантажує інші програми, різноманітні браузерні панелі інструментів, ПЗ з оманливою поведінкою, пакетне ПЗ, ПЗ для відстеження користувацьких операцій тощо. Дізнайтеся більше про ці типи програм у глосарії.

Потенційно підозрілі програми

Це програмне забезпечення, стиснуте упаковані шкідливі програми або протектором, щоб завадити аналізу його структури або приховати вміст виконуваного файлу (наприклад, шкідливого ПЗ). Для стискання або шифрування при цьому використовуються засоби із закритим вихідним кодом.До цієї категорії належать усі відомі програми, стиснуті за допомогою пакувальника або протектора, який часто використовується для стискання шкідливого ПЗ.

До цієї категорії належать усі відомі програми, стиснуті за допомогою пакувальника або протектора, який часто використовується для стискання шкідливого ПЗ.

Потенційно небезпечні програми

До цієї групи належать комерційні легальні програми, які можуть використовуватися неналежним чином зі зловмисною метою. Небезпечна програма — це легальне комерційне програмне забезпечення, яке може використовуватися зі зловмисною метою.

До таких програм належать інструменти для зламу захисту ПЗ і систем, генератори ліцензійних ключів, інструменти зламу, інструменти віддаленого доступу та керування, програми для зламу паролів, клавіатурні шпигуни (програми, що записують натискання клавіш користувачем). Цей параметр вимкнуто за замовчуванням.
Дізнайтеся більше про ці типи програм у глосарії.

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) звітування або захисту для категорії.

Звітування

Складання звітів здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Можна задати порогове значення для генерації звітності на власний розсуд. Немає такого поняття, як "правильна конфігурація". Тому ми рекомендуємо відстежувати поведінку у вашій мережі й самим вирішувати, чи потрібно вносити зміни до налаштувань генерації звітності.
Система звітності не виконує жодних дій з об’єктами, вона лише передає інформацію на відповідний рівень захисту, а рівень захисту застосовує відповідну дію.

Агресивний вміст	**Максимальна чутливість звітності. Програма буде повідомляти про більшу кількість виявлених об’єктів. Хоча параметр "Агресивний вміст" із певної точки зору є найнадійнішим, проте його використання може буди контрпродуктивним через високу чутливість.** Якщо вибрано параметр "Агресивний вміст", об’єкти можуть помилково визначатися як шкідливі із застосуванням відповідної дії до них (залежно від налаштувань захисту).
Збалансований	Цей параметр забезпечує оптимальний баланс між продуктивністю й точністю виявлення та кількістю помилкового виявлених об’єктів.
Помірний	Для звітування про шкідливе програмне забезпечення налаштовано мінімізацію кількості помилково визначених об’єктів зі збереженням достатнього рівня захисту. Об’єкти реєструються тільки тоді, коли ймовірність очевидна й відповідає поведінці шкідливого програмного забезпечення.
Вимкнуто	Функція "Звітність" неактивна. Пошук (очищення) об’єктів цього типа не виконується. Звітність про шкідливе програмне забезпечення неможливо вимкнути. Проте налаштування Вимкнуто недоступно для шкідливого програмного забезпечення.

Щоб відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.

Захист

Об’єкт, у якому виявлено потенційну загрозу на основі конфігурації вище й результатів машинного навчання, блокується до подальшої дії (очищення, видалення або переміщення в карантин).

Агресивний вміст	**Об’єкти, виявлені із застосуванням агресивного (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).**
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).
Вимкнуто	Виявлення неактивне, пошук і очищення об’єктів не проводяться. Звітність про шкідливе програмне забезпечення неможливо вимкнути. Проте налаштування Вимкнуто недоступно для шкідливого програмного забезпечення.

Щоб Відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.

За замовчуванням наведені вище параметри захисту на основі машинного навчання застосовуються також до сканування комп’ютера за вимогою. За потреби можна окремо налаштувати параметри **захисту за вимогою й на основі машинного навчання**. Натисніть піктограму перемикача, щоб вимкнути опцію **Використання параметрів захисту в режимі реального часу** й перейти до налаштувань.

Захист на основі машинного навчання

Ядро виявлення захищає систему від атак шкідливого програмного забезпечення через сканування файлів, електронних листів і підключень до мережі. Якщо виявляється об’єкт, класифікований як шкідливе програмне забезпечення, запускається процес виправлення. Ядро виявлення може знешкодити такий об’єкт: заблокувати його й застосувати до нього відповідну дію (очищення, видалення або переміщення в карантин).

Захист у режимі реального часу й за допомогою машинного навчання

Удосконалене машинне навчання тепер застосовується в ядрі виявлення для підвищення рівня захисту, що покращує виявлення на основі машинного навчання. Дізнайтеся більше про цей тип захисту в глосарії. Рівні звітування та захисту можна налаштувати для таких категорій:

Шкідливе програмне забезпечення

Комп’ютерний вірус – це шкідливий код, який додається на початок або в кінець файлів на комп’ютері. Проте термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення". Виявлення шкідливого програмного забезпечення здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Дізнайтеся більше про ці типи програм у глосарії.

Потенційно небажані програми

Потенційно небажана програма — це програмне забезпечення, яке не обов’язково має бути зловмисним, однак може інсталювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, виконувати неочікувані для користувача дії, не підтверджені ним операції чи мати інші неясні цілі.

До таких програм належать такі: ПЗ, що показує рекламу або завантажує інші програми, різноманітні браузерні панелі інструментів, ПЗ з оманливою поведінкою, пакетне ПЗ, ПЗ для відстеження користувацьких операцій тощо. Дізнайтеся більше про ці типи програм у глосарії.

Потенційно підозрілі програми

Це програмне забезпечення, стиснуте упаковані шкідливі програми або протектором, щоб завадити аналізу його структури або приховати вміст виконуваного файлу (наприклад, шкідливого ПЗ). Для стискання або шифрування при цьому використовуються засоби із закритим вихідним кодом.До цієї категорії належать усі відомі програми, стиснуті за допомогою пакувальника або протектора, який часто використовується для стискання шкідливого ПЗ.

До цієї категорії належать усі відомі програми, стиснуті за допомогою пакувальника або протектора, який часто використовується для стискання шкідливого ПЗ.

Потенційно небезпечні програми

До цієї групи належать комерційні легальні програми, які можуть використовуватися неналежним чином зі зловмисною метою. Небезпечна програма — це легальне комерційне програмне забезпечення, яке може використовуватися зі зловмисною метою.

До таких програм належать інструменти для зламу захисту ПЗ і систем, генератори ліцензійних ключів, інструменти зламу, інструменти віддаленого доступу та керування, програми для зламу паролів, клавіатурні шпигуни (програми, що записують натискання клавіш користувачем). Цей параметр вимкнуто за замовчуванням.
Дізнайтеся більше про ці типи програм у глосарії.

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) звітування або захисту для категорії.

Звітування

Складання звітів здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Можна задати порогове значення для генерації звітності на власний розсуд. Немає такого поняття, як "правильна конфігурація". Тому ми рекомендуємо відстежувати поведінку у вашій мережі й самим вирішувати, чи потрібно вносити зміни до налаштувань генерації звітності.
Система звітності не виконує жодних дій з об’єктами, вона лише передає інформацію на відповідний рівень захисту, а рівень захисту застосовує відповідну дію.

Агресивний вміст	**Максимальна чутливість звітності. Програма буде повідомляти про більшу кількість виявлених об’єктів. Хоча параметр "Агресивний вміст" із певної точки зору є найнадійнішим, проте його використання може буди контрпродуктивним через високу чутливість.** Якщо вибрано параметр "Агресивний вміст", об’єкти можуть помилково визначатися як шкідливі із застосуванням відповідної дії до них (залежно від налаштувань захисту).
Збалансований	Цей параметр забезпечує оптимальний баланс між продуктивністю й точністю виявлення та кількістю помилкового виявлених об’єктів.
Помірний	Для звітування про шкідливе програмне забезпечення налаштовано мінімізацію кількості помилково визначених об’єктів зі збереженням достатнього рівня захисту. Об’єкти реєструються тільки тоді, коли ймовірність очевидна й відповідає поведінці шкідливого програмного забезпечення.
Вимкнуто	Функція "Звітність" неактивна. Пошук (очищення) об’єктів цього типа не виконується. Звітність про шкідливе програмне забезпечення неможливо вимкнути. Проте налаштування Вимкнуто недоступно для шкідливого програмного забезпечення.

Щоб відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.

Захист передачі пошти й захист на основі машинного навчання

Звітування
Здійснюється ядром виявлення й компонентом машинного навчання. Система звітування не виконує жодних дій з об'єктами (це робиться відповідним рівнем захисту).
Захист
Налаштуйте параметри захисту передачі пошти, щоб визначити дії щодо виявлених об'єктів. Крім того, ви можете налаштувати спеціальне правило:

Приклад базової інсталяції:
Мета: Перемістити в карантин повідомлення, що містить шкідливе програмне забезпечення або захищені паролем, зашифровані чи пошкоджені вкладення
Створіть таке правило для **захисту передачі пошти**:
Стан
Тип: **Результат антивірусного сканування**
Операція: **є**
Параметр: **Інфіковано, не очищено**
Дія
Тип: **Відправити повідомлення в карантин**

Щоб Відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.

Налаштуйте захист на основі машинного навчання за допомогою eShell. Ім'я контексту в eShell – **MLP**. Відкрийте eShell в інтерактивному режимі й перейдіть до MLP:

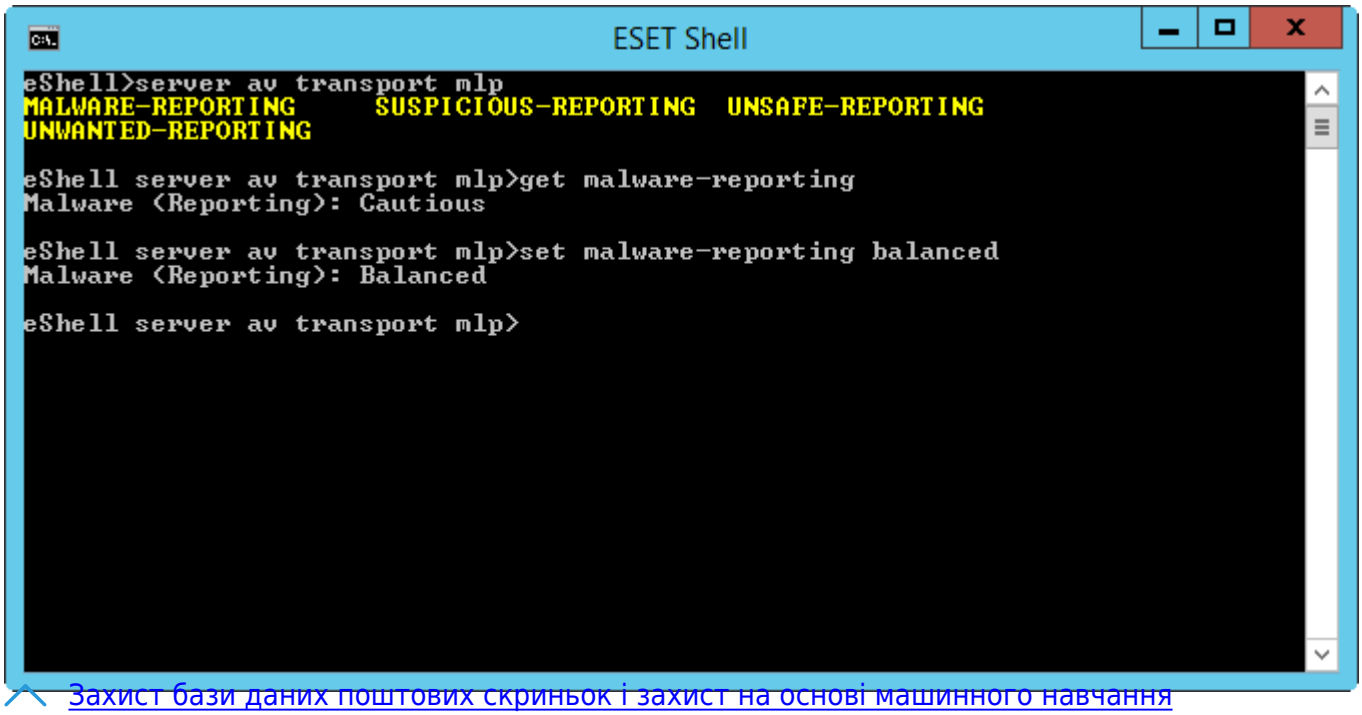
```
server av transport mlp
```

Дізнайтеся поточний параметр звітування для підозрілих програм:

```
get suspicious-reporting
```

Якщо звітування має бути менш ретельним, змініть параметр на "Помірний":

```
set suspicious-reporting cautious
```



Захист бази даних поштових скриньок і захист на основі машинного навчання

Звітування
Здійснюється ядром виявлення й компонентом машинного навчання. Система звітування не виконує жодних дій з об’єктами (це робиться відповідним рівнем захисту).
Захист
Налаштуйте параметри захисту бази даних поштової скриньки, щоб визначити дії щодо виявлених об’єктів.
Щоб Відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.
Налаштуйте захист на основі машинного навчання за допомогою eShell. Ім’я контексту в eShell – **MLP**. Відкрийте eShell в інтерактивному режимі й перейдіть до MLP:

```
server av database mlp
```

Дізнайтеся поточний параметр звітування для підозрілих програм:

```
get suspicious-reporting
```

Якщо звітування має бути менш ретельним, змініть параметр на "Помірний":

```
set suspicious-reporting cautious
```

Сканування бази даних поштових скриньок за вимогою й захист на основі машинного навчання

Звітування
Здійснюється ядром виявлення й компонентом машинного навчання. Система звітування не виконує жодних дій з об’єктами (це робиться відповідним рівнем захисту).
Захист
Налаштуйте параметри сканування бази даних поштових скриньок за вимогою, щоб визначити дії щодо виявлених об’єктів.
Щоб Відновити значення за замовчуванням у цьому розділі, натисніть стрілку поруч із його заголовком. Усі зміни, внесені в цей розділ, буде втрачено.
Налаштуйте захист на основі машинного навчання за допомогою eShell. Ім’я контексту в eShell – **MLP**. Відкрийте eShell в інтерактивному режимі й перейдіть до MLP:

```
server av on-demand mlp
```

Дізнайтеся поточний параметр звітування для підозрілих програм:

```
get suspicious-reporting
```

Якщо звітування має бути менш ретельним, змініть параметр на "Помірний":

```
set suspicious-reporting cautious
```

Виключення

Ця функція дає змогу виключати файли й папки зі сканування. Щоб усі об’єкти перевірялися на наявність можливих загроз, рекомендуємо створювати виключення лише тоді, коли це абсолютно необхідно. Випадки, коли вам може знадобитися виключити об’єкт, можуть охоплювати сканування великих записів бази даних, які можуть уповільнити роботу вашого сервера під час сканування, або програмне забезпечення, яке конфліктує зі скануванням (наприклад, програмне забезпечення для резервного копіювання).

Не плутати виключення розширень, виключення процесів або фільтр виключення.

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.

Виберіть тип виключень і натисніть **Змінити**, щоб додати нові або змінити наявні налаштування, зазначені далі.

- Виключення продуктивності: виключення файлів і папок зі сканування.
- Виключення об'єктів виявлення: виключити об'єкти зі сканування за певними критеріями (шлях, хеш файлу або назва виявленого об'єкта).

Виключення в роботі

Ця функція дає змогу виключати файли та папки зі сканування. Виключення для продуктивності доцільно вживати, щоб виключити сканування на рівні файлів критично важливих програм або коли сканування призводить до неналежної роботи системи чи зниження продуктивності.

Шлях

Виключає певний шлях (файл або каталог) для цього комп'ютера. Не використовуйте груповий символ зірочку (*) у середині шляху. Щоб дізнатися більше, перегляньте цю статтю бази знань.

Щоб виключити вміст папки, додайте зірочку (*) у кінці шляху (*C:\Tools**).
Шлях *C:\Tools* не виключатиметься, оскільки з погляду модуля сканування *Tools* також може бути іменем файлу.

Коментар

Ви можете додати коментар, щоб легко розпізнавати виключення в майбутньому.

Виключення шляху за допомогою зірочки.
C:\Tools*: шлях має закінчуватися зворотною скісною рискою (\) і зірочкою (*), указуючи на те, що це папка, і весь її вміст (файли й підпапки) буде виключено
C:\Tools*.*: така сама поведінка, як і з C:\Tools*. Це означає, що дія виконується рекурсивно.
C:\Tools*.dat: буде виключено файли dat у папці Tools.
C:\Tools\sg.dat: буде виключено цей конкретний файл, розташований за вказаним шляхом.

Щоб виключити всі файли в папці, введіть шлях до папки й скористайтеся маскою *.*.
Щоб виключити лише файли з розширенням DOC, використовуйте маску *.doc.
Якщо ім'я виконуваного файлу містить певну кількість символів (які можуть змінюватися), і точно відома лише перша літера (наприклад, D), використовуйте такий формат: D????.exe (знаки питання замінюють відсутні або невідомі символи).

Щоб визначити виключення сканування, використовуйте системні змінні, наприклад %PROGRAMFILES%.
Щоб виключити папку Program Files ("Файли програм") за допомогою цієї системної змінної, скористайтеся шляхом %PROGRAMFILES%\ (обов'язково додайте зворотну скісну риску в кінці шляху під час додавання до виключень).
Щоб виключити всі файли в підкаталозі %HOMEDRIVE%, скористайтеся шляхом %HOMEDRIVE%\Excluded_Directory*.*.
Указані нижче змінні можна використовувати у форматі виключення шляху:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Користувацькі системні змінні (наприклад, %TEMP% чи %USERPROFILE%) або змінні середовища (наприклад, %PATH%) не підтримуються.

Виключення об'єктів виявлення

Це ще один метод виключення об'єктів зі сканування за допомогою імені виявленого об'єкта, шляху або його хешу. Виключення виявлених об'єктів не виключають файли й папки зі сканування (наприклад, виключення щодо продуктивності). Виключення об'єктів виявлення виключають об'єкти лише тоді, коли об'єкти виявлено ядром виявлення, а відповідне правило є в списку виключень.

Найпростіший спосіб створити виключення на основі виявлених об'єктів – використовувати наявне виявлення на основі **виявлених файлів** у файлах журналу. Клацніть правою кнопкою миші запис журналу (виявлений об'єкт) і виберіть пункт **Створити виключення**. Відкриється майстер виключень із попередньо визначеними критеріями.

Щоб створити виключення виявленого об'єкта вручну, натисніть **Редагувати** > **Додати** (або **Редагувати** під час змінення наявного об'єкта) і вкажіть один або кілька з указаних нижче критеріїв (можна об'єднати).

Шлях

Виключає певний шлях (файл або каталог). Можна знайти певне розташування/файл або ввести рядок уручну. Не використовуйте груповий символ зірочку (*) у середині шляху. Щоб дізнатися більше, перегляньте цю статтю бази знань.

Щоб виключити вміст папки, додайте зірочку (*) у кінці шляху (C:\Tools*).
Шлях *C:\Tools* не виключатиметься, оскільки з погляду модуля сканування *Tools* також може бути іменем файлу.

Хеш

Виключає файл на основі заданого хешу (SHA1), незалежно від типу файлу, місця розташування, назви або його розширення.

Ім’я виявленого об’єкта

Укажіть дійсну назву виявленого об’єкта (загрози). Створення виключення на основі однієї лише назви виявлення може призвести до загрози безпеці. Рекомендуємо комбінувати назву виявленого об’єкта зі шляхом. Цей критерій виключення можна використовувати лише для певних типів виявлених об’єктів.

Коментар

Ви можете додати **коментар**, щоб легко розпізнавати виключення в майбутньому.

ESET PROTECT містить керування виключеннями об’єктами виявлення, щоб створити виключення виявлених об’єктів і застосувати їх до кількох комп’ютерів/груп.

Щоб охопити групу файлів, використовуйте групові символи. Знак запитання (*?*) позначає окремий змінний символ, а зірочка (*) — змінний рядок, який містить або не містить символи.

- Виключення шляху за допомогою зірочки.
  C:\Tools*: шлях має закінчуватися зворотною скісною рискою (\) і зірочкою (*), указуючи на те, що це папка, і весь її вміст (файли й підпапки) буде виключено
  C:\Tools*.*: така сама поведінка, як і з C:\Tools*. Це означає, що дія виконується рекурсивно.
  C:\Tools*.dat: буде виключено файли dat у папці Tools.
  C:\Tools\sg.dat: буде виключено цей конкретний файл, розташований за вказаним шляхом.

- Щоб виключити загрозу, введіть дійсну назву виявленого об’єкта в такому форматі:
  @NAME=Win32/Adware.Optmedia
  @NAME=Win32/TrojanDownloader.Delf.QQI
  @NAME=Win32/Bagle.D

- Щоб виключити всі файли в папці, введіть шлях до папки й скористайтеся маскою *.*.
  Щоб виключити лише файли з розширенням DOC, використовуйте маску *.doc.
  Якщо ім’я виконуваного файлу містить певну кількість символів (які можуть змінюватися), і точно відома лише перша літера (наприклад, "D"), використовуйте такий формат: D????.exe (знаки питання замінюють відсутні або невідомі символи).

Щоб визначити виключення сканування, використовуйте системні змінні, наприклад *%PROGRAMFILES%*.
Щоб виключити папку Program Files ("Файли програм") за допомогою цієї системної змінної, скористайтеся шляхом %PROGRAMFILES%\ (обов'язково додайте зворотну скісну риску в кінці шляху під час додавання до виключень).
Щоб виключити всі файли в підкаталозі %HOMEDRIVE%, скористайтеся шляхом %HOMEDRIVE%\Excluded_Directory*.*
Указані нижче змінні можна використовувати у форматі виключення шляху:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Користувацькі системні змінні (наприклад, %TEMP% чи %USERPROFILE%) або змінні середовища (наприклад, %PATH%) не підтримуються.

Майстер створення виключень

Рекомендоване виключення попередньо вибране на основі типу виявленого об'єкта, але ви також можете вказати критерії виключення для виявлених об'єктів. Натисніть **Змінити критерії**:

- **Точні файли:** виключити кожен файл за його хешем SHA-1
- **Виявлений об'єкт**: укажіть назву виявленого об'єкта, щоб виключити кожен файл, який містить такий виявлений об'єкт.
- **Шлях + виявлений об'єкт**: назву виявленого об'єкта й шлях (зокрема, назву файлу), щоб виключити кожен файл із виявленим об'єктом у вказаному розташуванні.

Ви можете додати **коментар**, щоб легко розпізнавати виключення в майбутньому.

Додаткові параметри

Активувати технологію Anti-Stealth

Найсучасніша система виявлення небезпечних програм, наприклад руткітів, які можуть приховатися в операційній системі. Зазвичай ці типи програм не виявляються стандартними методами.

AMSI

Microsoft Antimalware Scan Interface (AMSI) сканує сценарії PowerShell, що виконуються Windows Script Host.

Автоматичні виключення

Розробники серверних програм та операційних систем для більшості своїх продуктів рекомендують виключати набори критично важливих робочих файлів і папок зі сканування на наявність шкідливого програмного забезпечення. Така перевірка може мати негативний вплив на продуктивність сервера, що може призвести до конфліктів і навіть завадити запуску деяких програм на сервері. Виключення допомагають мінімізувати ризик виникнення потенційних конфліктів і підвищити загальну продуктивність сервера під час роботи захисту від шкідливого програмного забезпечення. Перегляньте повний список файлів, виключених зі сканування серверних продуктів ESET.

Функція автоматичних виключень вмикається після того, як ви активуєте ESET Mail Security за допомогою дійсної ліцензії й виконаєте початкове оновлення, яке містить усі найновіші модулі.

Функція автоматичних виключень для файлів бази даних Microsoft SQL Server працює для розташувань за замовчуванням. Якщо у вас є бази даних Microsoft SQL Server у різних розташуваннях (відмінних від стандартних), у вас є два варіанти. Додавати виключення вручну або ввімкнути автоматичне виключення файлів бази даних. Для автоматичного виключення ESET Mail Security потрібен доступ на читання екземпляра Microsoft SQL Server, який дасть змогу виконувати пошук шляхів, що використовуються для файлів бази даних. Якщо ESET Mail Security повертає помилку з повідомленням про недостатній обсяг прав, усуньте її. Для цього надайте обліковому запису NO_AUTHORITY\SYSTEM дозвіл **Перегляд усіх визначень** щодо кожного екземпляра Microsoft SQL Server, який виконується на сервері з ESET Mail Security.
Докладніше див. в статті бази знань Add permission to get database data locations to generate automatic exclusions for Microsoft SQL Server (Додавання дозволу на отримання розташувань даних бази даних для створення автоматичних виключень для Microsoft SQL Server).

ESET Mail Security визначає критичні серверні програми та файли операційної системи сервера й автоматично додає їх до списку виключень. Усі автоматичні виключення ввімкнено за замовчуванням. Виключення для кожної серверної програми можна вимкнути/ввімкнути за допомогою повзунка.

- Якщо виключення ввімкнено, усі критичні файли й папки буде додано до списку файлів, виключених зі сканування. Після кожного перезавантаження сервера система виконує автоматичну перевірку виключень та оновлює список у разі виявлення змін (наприклад, після встановлення нової серверної програми). Цей параметр забезпечує постійне застосування рекомендованих автоматичних виключень.

- Якщо виключення вимкнено, автоматично виключені файли й папки будуть видалені зі списку. Це не вплине на виключення, внесені користувачами вручну.

Автоматичні виключення для Exchange Server вибираються на основі рекомендацій Microsoft. ESET Mail Security застосовує лише "Виключення каталогів/папок" ("Виключення процесу" й "Виключення розширень файлів" не застосовуються). Щоб дізнатися більше, перегляньте наведені нижче статті бази знань Microsoft.

Update on the Exchange Server Antivirus Exclusions (Актуальна інформація щодо виключень антивірусу в Exchange Server)

Рекомендації щодо перевірки на віруси корпоративних комп’ютерів, які працюють під управлінням підтримуваних версій Windows

Антивірусна перевірка на рівні файлів (Exchange 2010)

Антивірусне програмне забезпечення в операційній системі Exchange Server (Exchange 2013)

Використання антивірусного програмного забезпечення Windows на серверах Exchange 2016

> **i** На локальному сервері також розміщені виключення файлів бази даних Exchange для активних і пасивних баз даних у DAG. Список автоматичних виключень оновлюється що 30 хвилин. Щойно створений файл бази даних Exchange буде автоматично виключено незалежно від стану (активного чи пасивного).

Для ідентифікації та створення автоматичних виключень ESET Mail Security використовує спеціальну програму eAutoExclusions.exe, розміщену в папці інсталяції. Жодні дії з вашого боку не потрібні, але ви можете скористатися командою eAutoExclusions.exe -servers у командному рядку, щоб переглянути список виявлених серверних програм у системі. Щоб відобразити повний синтаксис, введіть `eAutoExclusions.exe -?`.

Виявлено зараження

Зараження можуть потрапити в систему з різних джерел, наприклад веб-сайтів, спільних папок, електронної пошти або знімних носіїв (пристроїв USB, зовнішніх дисків, компакт- або DVD-дисків, дискет тощо).

Стандартна поведінка

Зазвичай ESET Mail Security виявляє зараження за допомогою наведених нижче модулів.

- Захист файлової системи в режимі реального часу
- Захист доступу до Інтернету
- Захист поштового клієнта
- Сканування комп'ютера за вимогою

Кожен із цих модулів використовує стандартний рівень очищення й намагається очистити файл і перемістити його в карантин або розірвати підключення. Вікно сповіщень відображається в області сповіщень у нижньому правому куті екрана. Щоб дізнатися більше про рівні очищення та поведінку, перегляньте статтю Очищення.

Очищення та видалення

Якщо для модуля захисту файлової системи в режимі реального часу немає попередньо визначеної дії, користувачу буде запропоновано вибрати її у вікні оповіщення. Зазвичай доступні такі опції: **Очистити**, **Видалити** та **Пропустити**. Не радимо вибирати опцію **Пропустити**, оскільки в такому разі заражені файли не буде очищено. Виключення можна зробити, якщо ви впевнені, що файл нешкідливий і його було виявлено помилково.

Очищення слід застосовувати, якщо файл атаковано вірусом, який додав у нього шкідливий код. У такому разі програма спробує очистити заражений файл, щоб відновити його початковий стан до очищення. Якщо файл містить лише шкідливий код, файл буде видалено.

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

Багато загроз

Якщо якісь заражені файли не очищено під час сканування комп'ютера (або для рівня очищення вибрано значення **Без очищення**), з'явиться вікно оповіщень із проханням вибрати дії для цих файлів.

Виберіть дію окремо для кожної загрози в списку або скористайтеся параметром **Вибрати дію для всіх загроз у списку** та виберіть одну дію, яку потрібно застосувати до всіх загроз у списку, після чого натисніть **Готово**.

Видалення файлів з архівів

У режимі очищення за замовчуванням архів буде видалено повністю, лише якщо всі файли в ньому заражені. Іншими словами, архіви, які містять нешкідливі чисті файли, не видаляються.

Будьте обережні, коли виконуєте сканування з ретельним очищенням, оскільки в цьому режимі архів буде видалено, якщо він міститиме принаймні один заражений файл (незалежно від стану інших файлів у ньому).

Захист файлової системи в режимі реального часу

Захист файлової системи в режимі реального часу контролює всі події, пов'язані зі шкідливим програмним забезпеченням у системі. Усі файли скануються на наявність шкідливого коду під час відкриття, створення або запуску на комп'ютері. За замовчуванням захист файлової системи в режимі реального часу запускається під час стартового завантаження системи й забезпечує безперервне сканування.

У деяких випадках (наприклад, якщо існують конфлікти з іншим сканером, що працює в режимі реального часу), захист у режимі реального часу можна вимкнути, вимкнувши параметр **Автоматично запускати захист файлової системи в режимі реального часу** у меню **Додаткові параметри** (**F5**) у розділі **Захист файлової системи в режимі реального часу** > **Базовий**.

ESET Mail Security сумісно з комп'ютерами, на яких використовується агент Azure File Sync з увімкненим розподілом за рівнями в хмарі. ESET Mail Security розпізнає файли з атрибутом *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Носії для перевірки

За замовчуванням на наявність потенційних загроз скануються всі типи носіїв.

- **Локальні диски** — Контроль усіх жорстких дисків у системі.
- **Змінні носії** — Контроль CD/DVD-дисків, USB-пристроїв, пристроїв Bluetooth тощо.
- **Мережеві диски** – сканування всіх підключених мережевих дисків.

Рекомендовано використовувати параметри за замовчуванням і змінювати їх лише в деяких випадках, наприклад, якщо під час сканування певних носіїв значно сповільнюється обмін даними.

Перевіряти під час

За замовчуванням усі файли скануються під час відкриття, створення або виконання. Рекомендовано не змінювати ці параметри за замовчуванням, оскільки вони забезпечують максимальний рівень захисту комп'ютера в режимі реального часу.

- **Відкриття файлу** – сканування під час відкриття й доступу до файлів.
- **Створення файлу** – сканування, коли файли створюються або змінюються.
- **Виконання файлу** – сканування під час виконання файлів.
- **Доступ до змінних носіїв** – сканування під час доступу до змінних носіїв. Коли до пристрою додається змінний носій, що містить завантажувальний сектор, такий сектор негайно сканується. Ця опція не запускає сканування файлів на змінних носіях. Параметри сканування файлів на змінних носіях містяться в розділі **Носії для сканування** > **Змінні носії**. Щоб доступ до завантажувального сектору змінного носія працював належним чином, не вимикайте пункт "Завантажувальні сектори / UEFI" в параметрах ThreatSense.

Виключення процесів

Дозволяє виключити певні процеси. Приклад – процеси резервного копіювання. У такому разі всі операції з файлами, пов'язані з виключеним процесом, ігноруються та вважаються безпечними, що мінімізує втручання в процес резервного копіювання.

ThreatSense параметри

Захист файлової системи в режимі реального часу перевіряє всі типи носіїв і запускається різними системними подіями, як-от доступ до файлу. Захист файлової системи в режимі реального часу можна налаштувати для новостворених і наявних файлів по-різному. Наприклад, можна налаштувати захист файлової системи в режимі реального часу таким чином, щоб він уважніше відстежував новостворені файли.

Щоб мінімізувати використання ресурсів системи під час роботи захисту в режимі реального часу, файли, які вже було скановано, повторно не скануються (якщо їх не було змінено). Файли скануються знову відразу після кожного оновлення бази даних ядра виявлення. Така поведінка керується за допомогою **Smart-оптимізації**. Якщо **Smart-оптимізацію** вимкнено, усі файли скануються під час кожного доступу до них.

Щоб змінити цей параметр, натисніть **F5**, щоб відкрити меню **Додаткові параметри** й розгорнути розділ **Computer** > **Захист файлової системи в режимі реального часу**. Натисніть **Параметри ThreatSense** > **Інше** та встановіть або зніміть прапорець **Увімкнути Smart-оптимізацію**.

Додаткові параметри ThreatSense

Додаткові опції можна змінювати в розділі **Додаткові параметри ThreatSense для нових і змінених файлів** або **Додаткові параметри ThreatSense для виконуваних файлів**.

ThreatSense параметри

ThreatSense – це технологія, у якій використовується багато складних методів виявлення загрози. Вона проактивна, тобто забезпечує захист під час раннього розповсюдження нової загрози. Технологія використовує поєднання аналізу коду, емуляції коду, загальних і вірусних сигнатур, що працюють разом заради значного поліпшення безпеки системи. Ядро сканування може одночасно керувати кількома потоками даних, що підвищує ефективність і частоту виявлення. Технологія ThreatSense також успішно усуває руткіти.

> Щоб дізнатися більше про автоматичну перевірку файлів під час запуску системи, перегляньте статтю Сканування під час запуску.

У налаштуваннях ядра ThreatSense можна задати кілька параметрів сканування:

- Типи й розширення файлів, які потрібно сканувати
- Комбінації різних методів виявлення
- Рівні очистки тощо

Щоб відкрити вікно налаштувань, клацніть налаштування **параметрів модуля ThreatSense** у вікні **Додаткові параметри** (**F5**) будь-якого модуля, що використовує технологію ThreatSense (див. нижче). Різні сценарії безпеки можуть потребувати різних конфігурацій. Пам'ятайте: ThreatSense можна налаштувати окремо для наведених нижче модулів захисту.

- Захист передачі пошти
- Захист бази даних поштових скриньок
- Захист бази даних поштової скриньки
- Сканування Hyper-V
- Захист файлової системи в режимі реального часу
- Сканування шкідливого ПЗ
- Сканування в неактивному стані
- Сканування під час запуску
- Захист документів
- Захист поштового клієнта
- Захист доступу до Інтернету

Параметри ThreatSense максимально оптимізовані для кожного модуля, а їх зміна може істотно вплинути на роботу системи. Наприклад, якщо змінити параметри на постійне сканування упакованих програм або ввімкнути розширену евристику в модулі захисту файлової системи в режимі реального часу, це може призвести до сповільнення роботи системи (за допомогою цих методів зазвичай скануються лише нові файли). Рекомендуємо не змінювати параметри

ThreatSense за замовчуванням для всіх модулів, крім сканування комп'ютера.

Перевірити об'єкти

У цьому розділі можна визначити компоненти комп'ютера й файли, які скануватимуться на наявність заражень.

Оперативна пам'ять
Перевірка на наявність загроз, орієнтованих на оперативну пам'ять комп'ютера.

Завантажувальні сектори/UEFI
Перевірка завантажувальних секторів на наявність вірусів у головному завантажувальному записі (MBR). MBR диска віртуальної машини Hyper-V сканується в режимі лише для читання.

База даних WMI
Сканування всієї бази даних WMI, пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване у вигляді даних.

Системний реєстр
Сканування всього системного реєстру, усіх розділів і підрозділів, пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване у вигляді даних.

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

Архіви
Програма підтримує такі 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
Саморозпакувальні архіви (SFX) – це архіви, для розпакування яких не потрібні спеціальні програми.

Упаковані програми
Після виконання упаковані програми (на відміну від стандартних типів архіву) розпаковуються в пам'яті. Крім стандартних статичних пакувальників (UPX, yoda, ASPack, FSG тощо), сканер може розпізнати кілька додаткових типів пакувальників завдяки емуляції коду.

> **i** З функцією захисту бази даних поштових скриньок вкладені файли електронної пошти (наприклад, *.eml files*) скануються незалежно від налаштувань у розділі **Об'єкти для сканування**. Це зумовлено тим, що Exchange Server аналізує вкладений файл .eml перед надсиланням ESET Mail Security для сканування. Плагін VSAPI отримує видобуті файли з вкладення .eml, а не вихідний файл .eml.

Опції сканування

Виберіть методи сканування системи на наявність заражень. Доступні вказані нижче опції:

Евристичний аналіз
Евристика – це алгоритм, який аналізує зловмисні дії програм. Основна перевага цієї технології – здатність виявляти шкідливе програмне забезпечення, якого не існувало за попереднього ядра виявлення або про яке нічого не було відомо.

Розширений евристичний аналіз/Родові сигнатури
У розширеному евристичному аналізі реалізовано унікальний евристичний алгоритм, розроблений компанією ESET та оптимізований для виявлення комп'ютерних черв'яків і троянських програм, написаних мовами програмування високого рівня. Використання розширеного евристичного аналізу значно збільшує можливості продуктів ESET із виявлення загроз. Сигнатури можуть надійно виявляти й ідентифікувати віруси. Завдяки автоматичній системі оновлення нові сигнатури стають доступні протягом кількох годин після виявлення загрози. Недоліком сигнатур є те, що вони виявляють лише відомі їм віруси (або трохи змінені версії цих вірусів).

Очистка

Параметри очистки визначають поведінку сканера під час очистки інфікованих файлів. Модулі захисту в режимі реального часу й інших типів захисту мають наведені нижче рівні виправлення (очистки).

Завжди виправляти виявлені об’єкти
Спробувати виправити виявлений об’єкт під час очистки без втручання користувача. Виключення – системні файли. Такі об’єкти залишаються у вихідному розташуванні, якщо виявлений об’єкт неможливо виправити.

Виправляти виявлений об’єкт, якщо він безпечний, а в іншому разі – залишати
Спробувати виправити виявлений об’єкт під час очистки без втручання користувача. Якщо виявлений об’єкт не вдається виправити для системних файлів або архівів (із чистими й інфікованими файлами), він залишається у вихідному розташуванні.

Виправляти виявлений об’єкт, якщо він безпечний, а в іншому разі – запитувати
Спробувати виправити виявлений об’єкт під час очистки. У деяких випадках, коли ESET Mail Security не може виконати автоматичну дію, вам буде запропоновано вибрати дію (видалити або ігнорувати). Цей параметр рекомендовано в більшості випадків.

Завжди запитувати кінцевого користувача
ESET Mail Security не виконуватиме автоматичну дію. Вам буде запропоновано вибрати дію.

Виключення

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст файлу. У цьому розділі налаштування параметрів ThreatSense можна визначити типи файлів, які потрібно виключити зі сканування.

Інше
Під час налаштування параметрів ядра ThreatSense для сканування комп’ютера за вимогою доступні також наведені нижче опції в розділі **Інше**.

Перевіряти альтернативні потоки даних (ADS)
Файлова система NTFS використовує альтернативні потоки даних, тобто асоціації файлів і папок, невидимі для звичайних методик перевірки. Багато загроз намагаються уникнути виявлення, маскуючись під альтернативні потоки даних.

Запуск фонової перевірки з низьким пріоритетом
Кожна послідовність сканування потребує 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
Якщо вибрано цю опцію, у журналі відображатимуться всі скановані файли, навіть неінфіковані.

Увімкнути Smart-оптимізацію
Якщо Smart-оптимізацію ввімкнено, то для забезпечення найефективнішого рівня сканування та підтримання максимальної швидкості сканування використовуватимуться оптимальні параметри. Модулі захисту використовують різні розумні методи сканування й застосовують їх до певних типів файлів. Якщо Smart-оптимізацію вимкнено, під час сканування застосовуватимуться лише визначені користувачем параметри ядра ThreatSense певних модулів.

Зберегти час останнього доступу
Виберіть цю опцію, щоб зафіксувати час першого доступу до сканованих файлів, а не час їх оновлення (наприклад, для використання в системах резервного копіювання).

Обмеження

У розділі "Обмеження" можна вказати максимальний розмір об’єктів і рівнів вкладених архівів, які потрібно сканувати:

Параметри об'єкта за замовчуванням

Увімкніть, щоб використовувати параметри за замовчуванням (без обмежень). ESET Mail Security ігноруватиме спеціальні параметри.

Максимальний розмір об'єкта

Визначає максимальний розмір об’єктів, які потрібно сканувати. Після цього модуль захисту скануватиме лише ті об’єкти, розмір яких не перевищує визначений. Цю опцію слід змінювати лише досвідченим користувачам, які можуть мати особливі причини для виключення зі сканування більших об’єктів. Значення за замовчуванням – необмежено.

Максимальний час перевірки об’єкта (сек.)

Визначає максимальний час сканування об’єкта. Якщо тут указано значення, визначене користувачем, модуль захисту перестане перевіряти об’єкт після закінчення відповідного періоду часу, незалежно від того, чи було завершено сканування. Значення за замовчуванням – необмежено.

Параметри перевірки архівів

Щоб змінити параметри сканування архівів, зніміть прапорець **Параметри сканування архівів за замовчуванням**.

Глибина архіву

Визначає максимальну глибину сканування архіву. За замовчуванням використовується файл: 10. Для об’єктів, виявлених захистом передавання пошти, фактичний рівень вкладення становить +1, оскільки архівні вкладення в електронному листі вважаються першим рівнем.

Якщо встановлено рівень вкладення 3, файл архіву з таким рівнем вкладення скануватиметься лише на рівні передавання до фактичного рівня 2. Тому, щоб архіви сканувалися захистом передавання пошти до рівня 3, установіть значення 4 для параметра **Рівень вкладення архіву**.

Максимальний розмір файлу в архіві

Цей параметр дає змогу вказати максимальний розмір файлів, що містяться в архівах (після видобування), які потрібно просканувати. Значення за замовчуванням – необмежено.

Не рекомендуємо змінювати значення за замовчуванням – за нормальних умов для цього немає потреби.

Додаткові параметри ThreatSense

Додаткові параметри ThreatSense для нових і змінених файлів

Імовірність зараження в новостворених або змінених файлах порівняно вища, ніж у наявних файлах. Тому програма перевіряє ці файли з додатковими параметрами сканування. Окрім поширених методів сканування на основі сигнатур, також використовуються розширена евристика, яка може виявляти нові загрози перед випуском оновлення модуля. Окрім новостворених файлів, сканування виконується на саморозпакувальних файлах (.sfx) та упакованих програмах (внутрішньо стиснутих виконуваних файлах).

За замовчуванням архіви перевіряються до 10-го рівня вкладення, причому сканування виконується незалежно від їх фактичного розміру. Щоб змінити параметри сканування архівів, приберіть прапорець **Параметри сканування архівів за замовчуванням**.

Додаткові параметри ThreatSense для виконуваних файлів

За замовчуванням під час виконання файлів використовується розширена евристика. Якщо цей параметр увімкнено, настійно рекомендуємо не вимикати Smart-оптимізацію та ESET LiveGrid®, щоб запобігти впливу на продуктивність системи.

Список розширень файлів, виключених із перевірки

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип файлу. Зазвичай перевіряються всі файли. Якщо потрібно виключити зі сканування файли з певним розширенням, параметр ThreatSense дає змогу робити це на його основі. Виключення може бути корисним, якщо сканування певних типів файлів заважає належному виконанню програми.

Щоб додати в список нове розширення, натисніть **Додати**. Введіть розширення в текстове поле (наприклад, tmp) і натисніть **ОК**. Якщо вибрано **Введіть кілька значень**, ви можете додати кілька розширень файлів, розділених рядками, комами або крапками з комами (наприклад, виберіть **Крапка з комою** в розкривному меню як розділювач і тип `edb;eml;tmp`).
Можна використовувати спеціальний символ ? (знак питання). Знак питання позначає будь-який символ (наприклад, `?db`).

Щоб відобразити розширення (тип файлу) для всіх файлів в операційній системі Windows, зніміть прапорець **Сховати розширення для відомих типів файлів** у розділі **Панель керування** > **Параметри папки** > **Вид**.

Виключення процесів

Функція виключення процесів дає змогу виключити програмні процеси лише зі сканування за доступом на наявність шкідливого програмного забезпечення. Оскільки виділені сервери (сервер програм, сервер зберігання даних тощо) відіграють критично важливу роль, регулярне резервне копіювання гарантуватиме своєчасне відновлення після будь-якого інциденту.

Щоб підвищити швидкість резервного копіювання, цілісність процесів і доступність служби, використовуються деякі методи, відомі конфліктами із захистом від шкідливого програмного забезпечення на рівні файлів. Подібні проблеми можуть виникати під час перенесення віртуальних машин.

Єдиний ефективний спосіб уникнути обох ситуацій – деактивувати захист від шкідливого програмного забезпечення. Якщо виключити його для певного процесу, як-от резервного копіювання, усі операції з файлами, пов’язані із цим процесом, ігноруватимуться та вважатимуться безпечними, що мінімізує втручання в процес резервного копіювання. Рекомендуємо діяти обережно під час створення виключень, оскільки виключений інструмент резервного копіювання може отримати доступ до інфікованих файлів без попередження. Тому розширені дозволи можна надавати лише в модулі захисту в режимі реального часу.

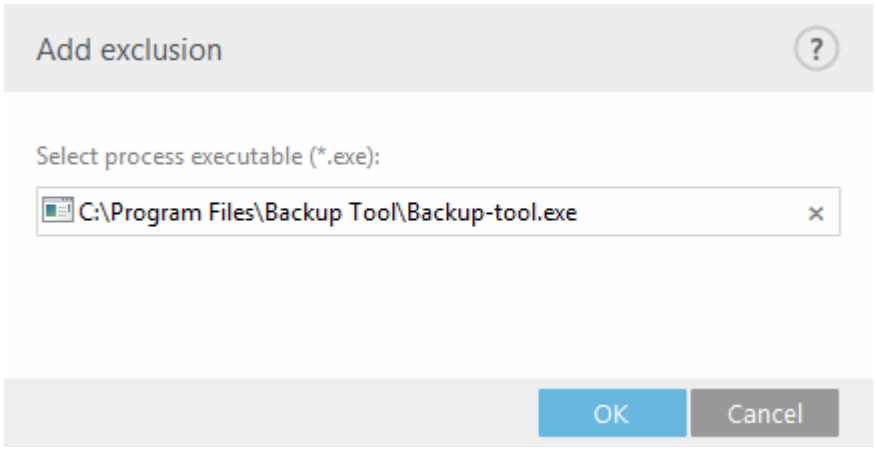
Виключення процесів допомагають мінімізувати ризик потенційних конфліктів та підвищити продуктивність виключених програм, що позитивно впливає на загальну продуктивність і стабільність операційної системи. Виключення процесу/програми означає виключення відповідного виконуваного файлу (*.exe*).

Ви можете додати виконувані файли в список виключених процесів у розділі **Додаткові параметри** (**F5**) > **Computer** > **Захист файлової системи в режимі реального часу** > **Базовий** > **Виключення процесів** або за допомогою списку запущених процесів у головному меню **Інструменти** > **Запущені процеси**.

Ця функція призначена для виключення інструментів резервного копіювання. Виключення інструменту резервного копіювання зі сканування не лише забезпечує стабільність системи, але й не впливає на продуктивність резервного копіювання, адже цей процес під час виконання не сповільнюватиметься.

Натисніть **Редагувати**, щоб відкрити вікно керування **Виключення процесів**, де можна **Додати** виключення й знайти виконуваний файл (наприклад, Backup-tool.exe), який буде виключено зі сканування.
Щойно файл *.exe* буде додано до виключень, ESET Mail Security більше не відстежуватиме активність цього процесу, а сканування не виконуватиметься для жодних операцій із файлами, виконуваних цим процесом.

Якщо для вибору виконуваного файлу ви не використовуєте функцію пошуку, введіть повний шлях до нього вручну. В іншому разі виключення працюватиме неправильно, а HIPS може повідомляти про помилки.



Також можна **Редагувати** наявні процеси або **Видаляти** їх із виключень.

Захист доступу до Інтернету не враховуватиме це виключення, тому якщо виключити виконуваний файл веб-браузера, завантажені файли однаково скануватимуться. Це допоможе й надалі виявляти загрози. Цей сценарій наведено лише для прикладу. Ми не рекомендуємо створювати виключення для веб-браузерів.

Захист на основі хмари

ESET LiveGrid® – це сучасна система завчасного попередження, що працює на основі кількох хмарних технологій. Вона виявляє нові загрози на основі репутаційних даних і підвищує ефективність сканування за допомогою білих списків. Відомості про нову загрозу передаються в хмару в режимі реального часу, що дозволяє лабораторії ESET Malware Research Lab забезпечити оперативне реагування та стабільно високий рівень захисту. Користувачі можуть перевіряти репутаційні дані запущених процесів і файлів безпосередньо в інтерфейсі програми або контекстному меню за допомогою додаткової інформації, яка отримується від ESET LiveGrid®.

Під час інсталяції ESET Mail Security виберіть один із варіантів нижче.

- Можна не вмикати ESET LiveGrid®. Функційні можливості програмного забезпечення не буде втрачено, проте в деяких випадках система ESET Mail Security може повільніше реагувати на нові загрози, ніж оновлення бази даних ядра виявлення.

• Можна налаштувати ESET LiveGrid® для надсилання анонімних даних про нові загрози й місце виявлення нового загрозливого коду. Цей файл можна надіслати до ESET для докладного аналізу. Вивчення цих загроз допоможе ESET оновити свої засоби виявлення загроз.

ESET LiveGrid® збиратиме інформацію про комп'ютер, пов'язану з новими виявленими загрозами. Ця інформація може містити зразок або копію файлу, у якому виявлено загрозу, шлях до нього, ім'я файлу, дату й час, процес, з яким пов'язана поява загрози на комп'ютері, а також інформацію про операційну систему комп'ютера.

За замовчуванням ESET Mail Security налаштовано на надсилання підозрілих файлів до лабораторії ESET Virus Lab для аналізу. Файли з певними розширеннями, наприклад .docx або .xlsx, завжди виключені. Якщо ви або ваша організація хочете уникнути надсилання певних файлів, можна додати також інші розширення.

Увімкнути систему репутації ESET LiveGrid® (рекомендовано)

Система репутації ESET LiveGrid® підвищує ефективність рішень ESET для захисту від шкідливого ПЗ, порівнюючи перевірені файли з хмарною базою даних об'єктів, доданих до білих і чорних списків.

Увімкнути систему зворотного зв'язку ESET LiveGrid®

Дані надсилатимуться в ESET Research Lab для подальшого аналізу.

Надсилати звіти про аварійне завершення роботи і дані діагностики

Надсилати дані, зокрема звіти про аварійне завершення роботи, модулі або дампи пам'яті.

Надіслати анонімну статистику

Дозволяє ESET збирати інформацію про нові виявлені загрози, зокрема їхні назви, дати й час виявлення, методи виявлення та пов'язані метадані, скановані файли (хеш, ім'я файлу, походження файлу, дані телеметрії), заблоковані та підозрілі URL-адреси, 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.

Надсилання зразків

Автоматичне надсилання виявлених зразків
Усі виявлені зразки будуть надіслані команді ESET для подальшого аналізу й удосконалення системи виявлення.
• Усі виявлені зразки
• Усі зразки за винятком документів
• Не відправляти
Автоматичне надсилання підозрілих зразків
Підозрілі зразки, які за вмістом або поведінкою схожі на загрози, відправляються для аналізу в ESET.
• **Виконувані файли** – охоплює виконувані файли: .exe, .dll, .sys
• **Архіви** – охоплює типи файлів архіву: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
• **Сценарії** – охоплює типи файлів сценаріїв: .bat, .cmd, .hta, .js, .vbs, .js, .ps1
• **Інше** – охоплює такі типи файлів: .jar, .reg, .msi, .swf, .lnk
• **Повідомлення електронної пошти з підозрою на спам** – поліпшує глобальне виявлення спаму.
• **Документи** — Містить документи Microsoft Office або PDF-файли з активним вмістом
Виключення
Натисніть опцію Редагувати поруч із пунктом "Виключення" у ESET LiveGrid®, щоб налаштувати спосіб надсилання загроз до лабораторій ESET Virus Lab для аналізу.
Максимальний розмір зразків (МБ)
Визначає максимальний розмір зразків, які потрібно сканувати.

ESET LiveGuard Advanced

Вмикає службу ESET LiveGuard Advanced на клієнтському комп’ютері за допомогою веб-консолі ESET PROTECT. У веб-консолі ESET PROTECT створіть нову політику або відредагуйте наявну й призначте її на комп’ютерах, де вона має використовуватися ESET LiveGuard Advanced.

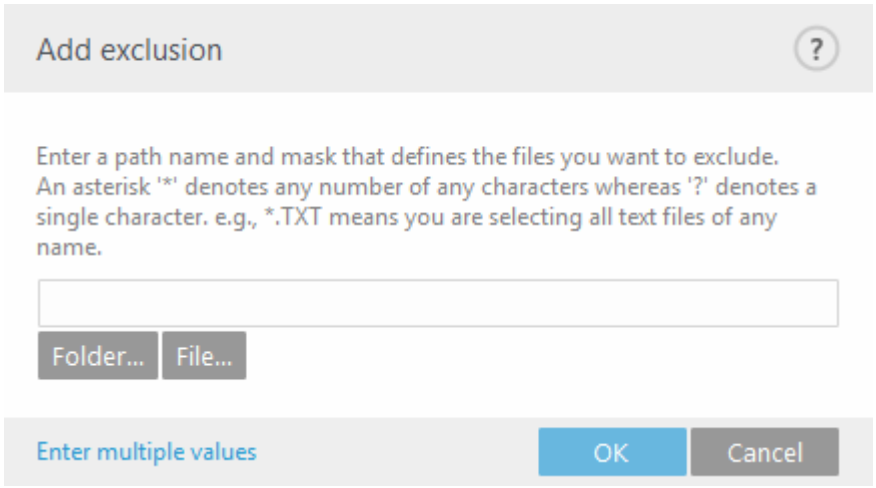
Фільтр виключення

Фільтр виключення дозволяє запобігати відправленню певних файлів або папок (наприклад, доцільно виключити файли, які можуть містити конфіденційну інформацію, як-от документи або електронні таблиці).

Перелічені файли ніколи не надсилатимуться до лабораторії ESET для аналізу, навіть якщо вони містять підозрілий код.

Найпоширеніші типи файлів виключено за замовчуванням (*.doc*). За потреби список виключених файлів можна доповнити.

Якщо ви раніше користувалися ESET LiveGrid®, а потім вимкнули її, можуть залишатися пакети даних для надсилання. Навіть після деактивації програми ці пакети буде надіслано в ESET. Після надсилання всієї поточної інформації пакети більше не створюються.



Якщо ви виявите підозрілий файл, його можна надіслати для аналізу до наших лабораторій ThreatLabs. Якщо це шкідлива програма, виявлений об’єкт буде додано до наступного оновлення модуля виявлення.

Сканування шкідливого ПЗ

У цьому розділі можна вибрати параметри сканування.

> Цей перемикач профілів сканування застосовується до **Сканування за вимогою** та Сканування Hyper-V.

Вибраний профіль

Певний набір параметрів, які використовуються сканером за вимогою. Можна скористатись одним із попередньо визначених профілів сканування або створити новий. У профілях сканування використовуються різні параметри модуля ThreatSense.

Список профілів

Щоб створити новий профіль, натисніть **Редагувати**. Введіть ім’я профілю й натисніть **Додати**. Новий профіль відображатиметься в розкривному меню **Вибраний профіль**, що містить наявні профілі сканування.

Об’єкти сканування

Щоб просканувати певний об’єкт, натисніть **Редагувати** й виберіть відповідну опцію в розкривному меню або потрібні об’єкти зі структури (дерева) папок.

ThreatSense параметри

Змініть параметри сканування для сканера комп’ютера за вимогою.

Захист за вимогою та за допомогою машинного навчання

Звіти генеруються ядром виявлення й компонентом машинного навчання.

Диспетчер профілів

У розкривному меню "Профіль сканування" можна вибрати попередньо визначені профілі сканування.

- Інтелектуальне сканування
- Сканування з контекстного меню
- Детальне сканування
- Мій профіль (застосовується до сканування Hyper-V, профілів оновлення)

Щоб створити профіль сканування відповідно до потреб, перегляньте опис кожного параметра налаштування сканування в розділі Налаштування параметрів модуля ThreatSense.

Диспетчер профілів використовується в трьох розділах ESET Mail Security.

Сканування комп'ютера за вимогою

Вибрані параметри сканування можна зберегти для використання в майбутньому. Радимо створити окремий профіль для кожного сканування, що використовується регулярно (з різними об’єктами та способами сканування й іншими параметрами).

Оновлення

Редактор профілів дає користувачам змогу створювати нові профілі оновлення. Користувацькі профілі оновлення потрібні, лише якщо комп’ютер підключається до серверів оновлень за допомогою різних засобів.

Сканування Hyper-V

Створіть новий профіль і виберіть **Редагувати** поруч із пунктом **Список профілів**. Новий профіль відображатиметься в розкривному меню **Вибраний профіль**, що містить наявні профілі сканування.

Цілі профілю

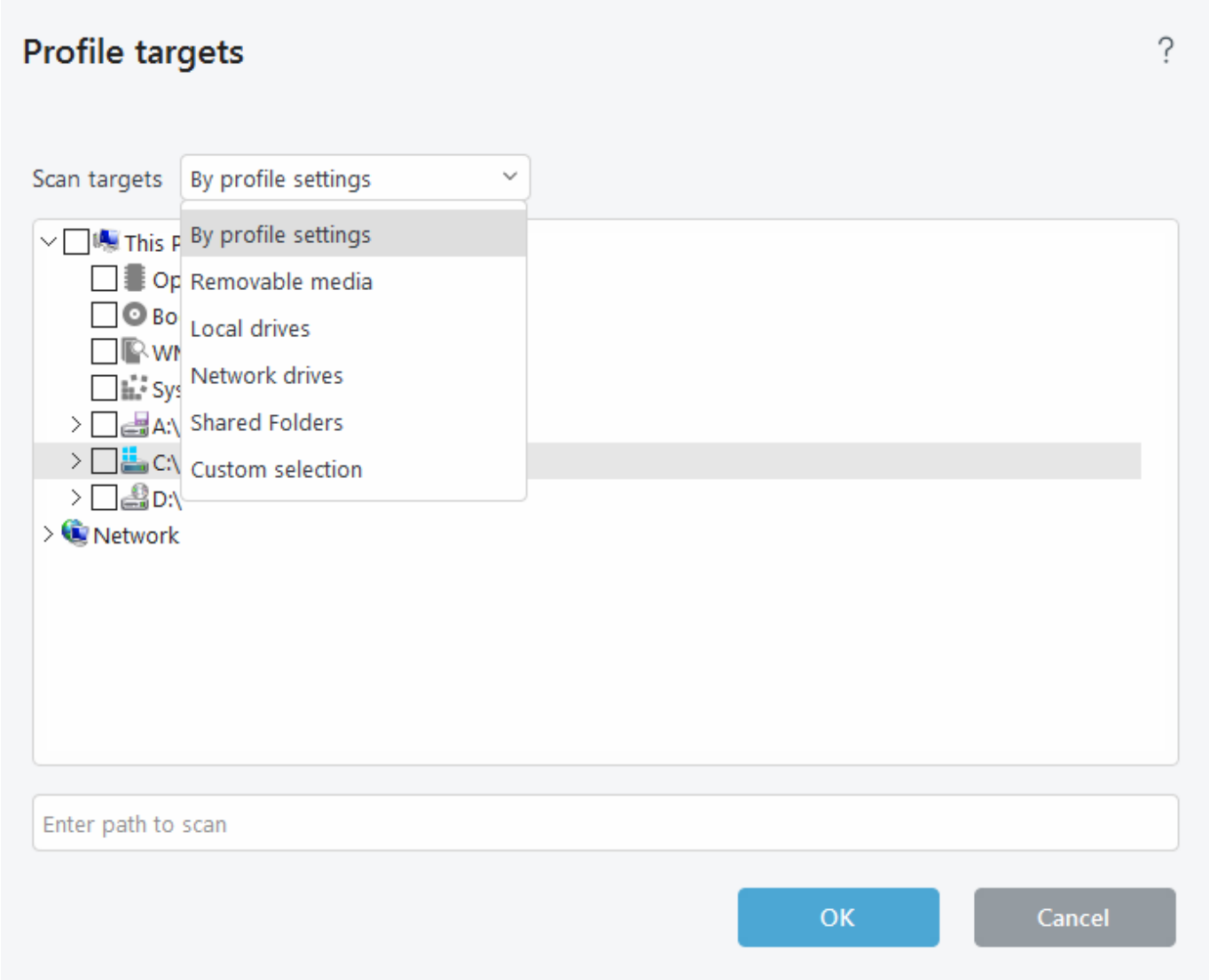
Ви можете вказати, що потрібно сканувати на наявність заражень. Виберіть об’єкти (пам’ять, завантажувальні сектори та UEFI, диски, файли й папки, мережа) у структурі дерева, що містить усі доступні об’єкти в системі. Натисніть піктограму шестерні у верхньому лівому куті, щоб отримати доступ до розкривних меню **Об’єкти сканування** та **Профіль сканування**.

Цей перемикач профілів сканування застосовується до сканування на вимогу та сканування Hyper-V.

Оперативна пам’ять	Сканування всіх процесів і даних, які зараз використовує оперативна пам’ять.
Завантажувальні сектори/UEFI	Сканування завантажувальних секторів і UEFI на наявність шкідливого програмного забезпечення. Дізнатися більше про сканер UEFI можна в глосарії.

Оперативна пам’ять	Сканування всіх процесів і даних, які зараз використовує оперативна пам’ять.
База даних WMI	Сканування всієї бази даних інструментарію керування Windows (WMI), усіх просторів імен, екземплярів класу та властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване як дані.
Системний реєстр	Сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване як дані. Під час очищення виявлених об’єктів посилання залишається в реєстрі, щоб уникнути втрати важливих даних.

Щоб швидко перейти до об’єкта сканування або додати цільову папку чи файли, введіть цільовий каталог у порожньому полі під списком папок.



У розкривному меню **Об’єкти сканування** можна вибрати попередньо визначені об’єкти сканування.

За параметрами профілю	Вибираються об’єкти, указані у вибраному профілі сканування.
Змінні носії	Вибираються дискети, пристрої USB для зберігання даних, компакт- і DVD-диски.

За параметрами профілю	Вибираються об’єкти, указані у вибраному профілі сканування.
Локальні диски	Вибираються всі жорсткі диски системи.
Мережеві диски	Вибираються всі підключені мережеві диски.
Спільні папки	Вибираються всі папки на локальному сервері, до яких надано спільний доступ.
Спеціальний вибір	Скасовується вибір усіх об’єктів. Після цього можна самостійно вибрати потрібні об’єкти.

Щоб швидко перейти до об’єкта сканування (файлу або папки) та додати його в список сканування, введіть шлях до нього в текстовому полі під деревовидною структурою. Шлях до об’єкта вказується з урахуванням регістру.

У розкривному меню **Профіль сканування** можна вибрати попередньо визначені профілі сканування.

- Інтелектуальне сканування
- Сканування з контекстного меню
- Детальне сканування
- Сканування комп'ютера

Ці профілі сканування використовують різні параметри модуля ThreatSense.

Сканувати без очищення

Якщо потрібно просканувати систему без додаткових дій з очищення, виберіть **Сканувати без очищення**. Ця функція корисна, якщо потрібно лише отримати загальну інформацію про інфіковані елементи та дізнатися більше про ці зараження (якщо є). Можна вибрати один із трьох рівнів очистки, натиснувши послідовно **Параметри** > **Параметри ThreatSense** > **Очищення**. Інформація про сканування зберігається в журналі сканування.

Ігнорувати виключення

Якщо вибрати "Ігнорувати виключення", під час сканування ігноруються виключення, які застосовуються.

Об’єкти сканування

Щоб просканувати лише певний об’єкт, можна скористатися **вибірковим скануванням** і вибрати потрібну опцію в розкривному меню **Об’єкти сканування** або вибрати певні об’єкти в дереві папок.

Засіб вибору профілю об’єктів сканування застосовується до:

- Сканування за вимогою
- Сканування Hyper-V

Щоб швидко перейти до об’єкта сканування або додати новий цільовий файл чи папку, введіть

їхнє ім’я в порожнє поле під списком папок. Це можливо, лише якщо в деревовидній структурі не вибрано жодного об’єкта, а в меню **Об’єкти сканування** вибрано значення **Нічого не вибирати**.

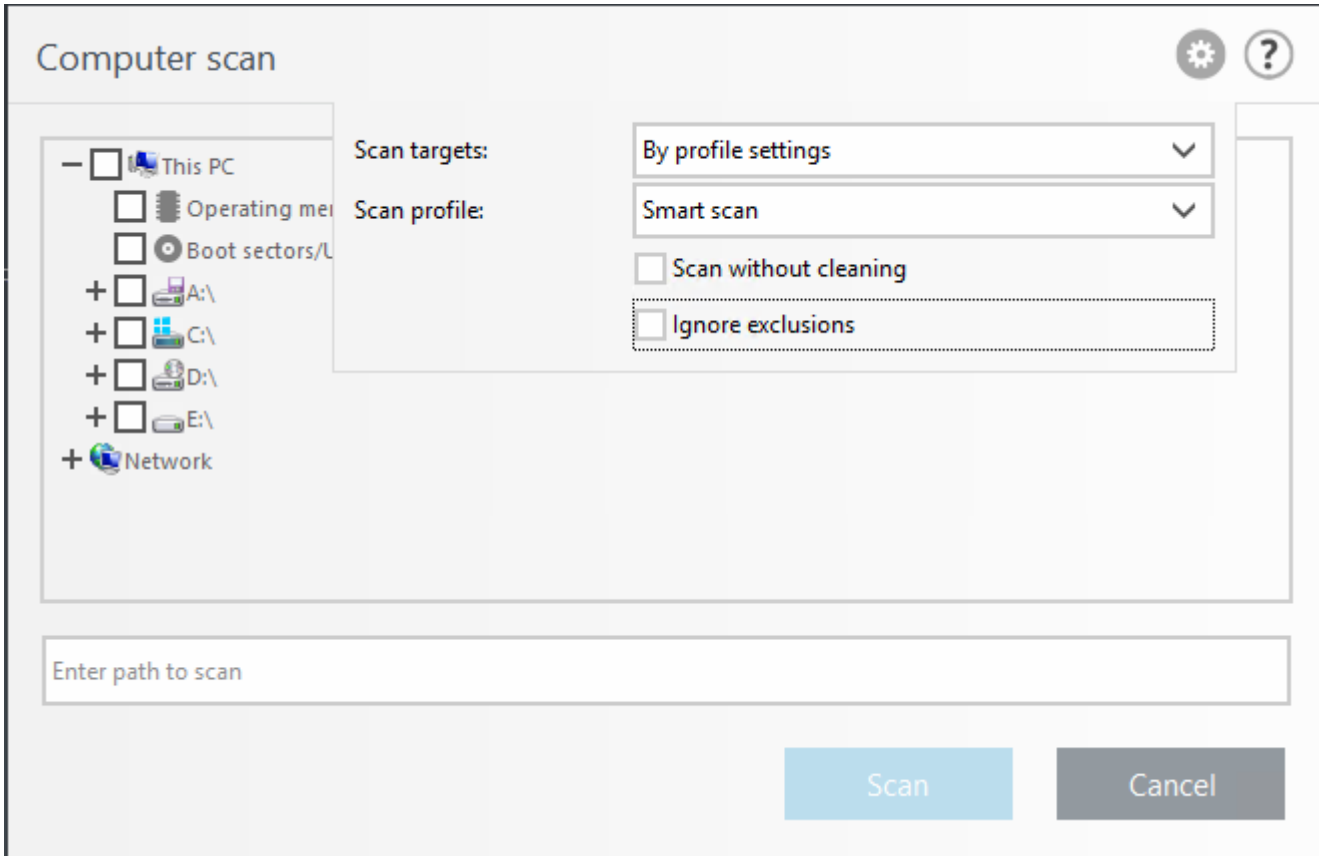
Оперативна пам’ять	Сканування всіх процесів і даних, які зараз використовує оперативна пам’ять.
Завантажувальні сектори/UEFI	Сканування завантажувальних секторів і UEFI на наявність шкідливого програмного забезпечення. Дізнатися більше про сканер UEFI можна в глосарії.
База даних WMI	Сканування всієї бази даних інструментарію керування Windows (WMI), усіх просторів імен, екземплярів класу та властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване як дані.
Системний реєстр	Сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване як дані. Під час очищення виявлених об’єктів посилання залишається в реєстрі, щоб уникнути втрати важливих даних.

У розкривному меню **Об’єкти сканування** можна вибрати попередньо визначені об’єкти сканування.

За параметрами профілю	Вибираються об’єкти, указані у вибраному профілі сканування.
Змінні носії	Вибираються дискети, пристрої USB для зберігання даних, компакт- і DVD-диски.
Локальні диски	Вибираються всі жорсткі диски системи.
Мережеві диски	Вибираються всі підключені мережеві диски.
Спільні папки	Вибираються всі папки на локальному сервері, до яких надано спільний доступ.
Спеціальний вибір	Скасовується вибір усіх об’єктів. Після цього можна самостійно вибрати потрібні об’єкти.

У розкривному меню Профіль сканування можна вибрати профіль, який використовуватиметься для сканування визначених об’єктів. За замовчуванням використовується профіль **Smart-сканування**. Є ще два попередньо визначені профілі сканування: детальне сканування та **сканування з контекстного меню**. Ці профілі сканування використовують різні параметри модуля ThreatSense.

Вікно **Вибіркове сканування**:



Сканувати без очищення — Якщо потрібно просканувати систему без додаткових дій з очищення, виберіть Сканувати без очищення. Ця функція корисна, якщо потрібно лише отримати загальну інформацію про інфіковані елементи та дізнатися більше про ці зараження (якщо є). Можна вибрати один із трьох рівнів очистки, натиснувши послідовно Параметри > Параметри ThreatSense > Очищення. Інформація про сканування зберігається в журналі сканування.

Ігнорувати виключення — Можна вибрати сканування з ігноруванням виключень, які застосовуються.

Дія після сканування: у розкривному меню виберіть дію, яку потрібно виконати після завершення сканування.

Не вдається перервати сканування: дає змогу позбавити непривілейованих користувачів можливості зупиняти дії, які виконуються після сканування.

Перевірка може бути зупинена користувачем на (хв.): дає змогу користувачу з обмеженими правами призупинити сканування комп’ютера на вказаний проміжок часу.

Перервати сканування автоматично через (хв): дає змогу перервати сканування, якщо воно виконується довше за вказаний ліміт часу.

Сканування як адміністратор — Дає змогу виконати сканування з облікового запису адміністратора. Скористайтеся цією функцією, якщо в поточного користувача немає прав доступу до відповідних файлів, які потрібно просканувати. Зверніть увагу, що ця кнопка недоступна, якщо поточний користувач не може викликати операції служби захисту користувачів як адміністратор.

Сканування в режимі очікування

Коли комп’ютер перебуває в режимі очікування, на всіх локальних дисках виконується сканування. **Виявлення режиму очікування** виконуватиметься в таких випадках:

- Вимкнений екран або заставка
- Блокування комп’ютера
- Вихід користувача із системи

Запускати, навіть якщо комп'ютер живиться від батареї

За замовчуванням сканування в режимі очікування не виконується, якщо комп’ютер (ноутбук) працює від батареї.

Вести журнал

Запис результатів сканування комп’ютера в розділі Файли журналу (у головному вікні програми натисніть "Файли журналу" й виберіть тип журналу "Сканування комп’ютера" в розкривному меню).

ThreatSense параметри

Зміна параметрів сканування в режимі очікування.

Сканування під час запуску

За замовчуванням автоматична перевірка файлу виконується під час запуску системи (входу користувача в систему) й успішного оновлення модуля. Це сканування контролюється конфігурацією та завданнями розкладу.

Параметри сканування під час запуску є частиною завдання розкладу **Перевірка файлів під час запуску системи**.

Щоб змінити параметри сканування під час запуску, перейдіть у розділ **Інструменти** > **Розклад**, виберіть завдання **Автоматична перевірка файлів під час запуску** (вхід користувача в систему або оновлення модуля) і натисніть **Редагувати**. На останньому кроці майстра можна змінити параметри опції Автоматична перевірка файлів під час запуску системи.

Автоматична перевірка файлів під час запуску системи

Створюючи заплановане завдання "Перевірка файлів під час запуску системи", можна змінити вказані нижче параметри.

У розкривному меню **"Об’єкт сканування"** вказується глибина сканування файлів, що виконуються під час запуску системи. Файли розташуються за зростанням відповідно до

наведених нижче критеріїв.

- Усі зареєстровані файли (перевіряється більшість файлів)
- Файли, які рідко використовуються
- Файли, які зазвичай використовуються
- Файли, які часто використовуються
- Лише файли, які використовуються найчастіше (перевіряється мінімальна кількість файлів)

Включено також дві конкретні цільові групи.

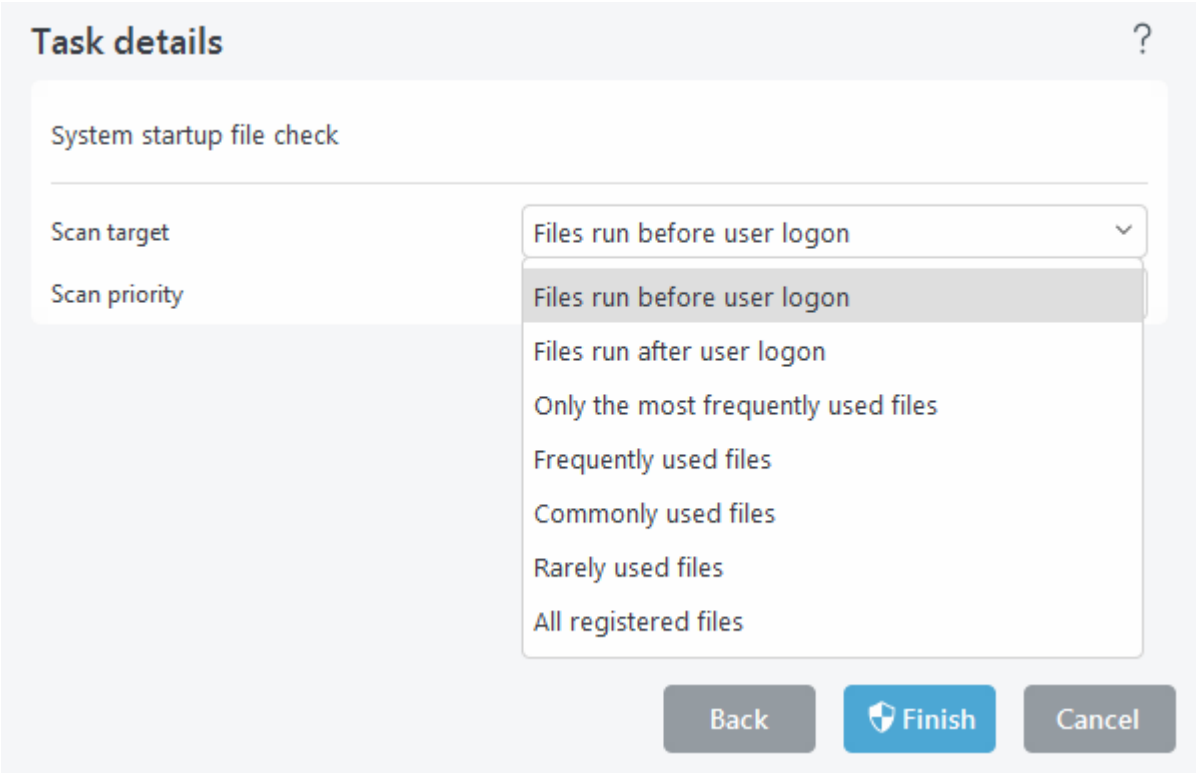
Файли, що запускаються перед входом користувача в систему

Містить файли з розташувань, до яких можна отримати доступ без входу користувача в систему (зокрема більшість елементів, що виконуються під час запуску: служби, об'єкти модуля підтримки браузера, сповіщення Winlogon, записи в інструменті "Планувальник завдань Windows", відомі бібліотеки DLL тощо).

Файли, що запускаються після входу користувача в систему

Містить файли з розташувань, до яких можна отримати доступ лише після входу користувача в систему (зокрема файли, які запускає лише певний користувач, зазвичай файли з папки *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

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



Пріоритет сканування

Рівень пріоритетності, який визначається перед початком сканування.

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

Змінні носії

ESET Mail Security дає змогу автоматично сканувати змінні носії (CD/DVD/USB). За допомогою цього модуля можна сканувати вставлений носій. Це може бути корисним, якщо адміністратор комп'ютера хоче запобігти використанню змінних носіїв із небажаним вмістом.

Після вставлення змінного носія з'явиться таке діалогове вікно:

- **Сканувати зараз**: ініціює сканування змінного носія.
- **Не сканувати**: змінні носії не скануватимуться.
- **Налаштування**: відкриває додаткові параметри.
- **Завжди використовувати вибрані параметри**: якщо вибрано цей параметр, після вставлення змінного носія завжди виконуватиметься та сама дія.

Окрім цього, ESET Mail Security забезпечує контроль пристроїв, який дає змогу визначати правила використання зовнішніх пристроїв на певному комп'ютері.

Щоб отримати доступ до параметрів сканування змінних носіїв, відкрийте **Додаткові параметри** (**F5**) > **Сповіщення** > **Інтерактивні сповіщення** > **Змінити**. Якщо параметр **Запитувати користувача** не вибрано, виберіть дію, яку буде виконано після вставлення змінного носія в комп'ютер:

- **Не сканувати**: не виконуватимуться жодні дії, а вікно з виявленим **новим пристроєм** буде закрито.
- **Автоматичне сканування пристроїв**: виконуватиметься сканування вставленого змінного носія на вимогу.
- **Примусове сканування пристрою**: виконуватиметься сканування вставленого змінного носія, яке неможливо скасувати.
- **Показати параметри сканування**: відкриває розділ налаштувань **Інтерактивні сповіщення**.

Захист документів

Функція захисту документів перевіряє документи Microsoft Office перед відкриттям і сканує файли, автоматично завантажувані в Internet Explorer (наприклад, елементи Microsoft ActiveX).

Функція захисту документів надає ще один рівень безпеки додатково до функції захисту файлової системи в реальному часі. Її можна вимкнути, щоб поліпшити продуктивність у системах, які не містять великої кількості документів Microsoft Office.

Інтегрувати до системи

Цей параметр забезпечує посилений захист документів Microsoft Office (не потрібний за нормальних умов).

ThreatSense параметри

Зміна параметрів захисту документів.

> Цю функцію активують програми, у яких використовується Microsoft Antivirus API (наприклад, Microsoft Office 2000 та новіші версії або Microsoft Internet Explorer 5.0 і новіші версії).

Сканування Hyper-V

Поточна версія модуля сканування Hyper-V підтримує сканування онлайнової й автономної віртуальної систем у Hyper-V. Нижче наведено підтримувані типи сканування відповідно до розміщеної системи Windows Hyper-V та стану віртуальної системи:

Віртуальні системи з функцією Hyper-V	Онлайнова віртуальна машина	Автономна віртуальна машина
Windows Server 2022 Hyper-V	лише для читання	лише для читання/очищення
Windows Server 2019 Hyper-V	лише для читання	лише для читання/очищення
Windows Server 2016 Hyper-V	лише для читання	лише для читання/очищення
Windows Server 2012 R2 Hyper-V	лише для читання	лише для читання/очищення
Windows Server 2012 Hyper-V	лише для читання	лише для читання/очищення

Вимоги до обладнання

На сервері не має виникати проблем із роботою віртуальних машин. Сканування насамперед використовує ресурси ЦП. Для сканування онлайнових віртуальних машин потрібне місце на диску. Доступне місце має бути принаймні вдвічі більше за те, що використовується для контрольних точок/знімків і віртуальних дисків.

Спеціальні обмеження

- Сканування в сховищі RAID, складених томах і динамічних дисках не підтримується через особливості динамічних дисків. Через це ми рекомендуємо за можливості не використовувати динамічні диски у віртуальних машинах.

- Сканування завжди виконується на поточній віртуальній машині й не впливає на контрольні точки або знімки системи.

- Hyper-V, що працює на хості в кластері, наразі не підтримується в ESET Mail Security.

Хоча ESET Security допускає сканування MBR-секторів віртуального диска, єдиний підтримуваний метод їх сканування – лише для читання. Цей параметр можна змінити в розділі **Додаткові параметри** (**F5**) > **Computer** > **Сканування Hyper-V** > Параметри ThreatSense > **Завантажувальні сектори**.

Сканується автономна віртуальна машина: стан "Вимкнено"

ESET Mail Security використовує Hyper-V Management для виявлення віртуальних дисків і підключення до них. Таким чином, ESET Mail Security має такий самий доступ до вмісту віртуальних дисків, що й під час роботи зі звичайним диском.

Сканується віртуальна машина, що працює в мережі: стани "Виконується", "Призупинено", "Збережено"

ESET Mail Security використовує Hyper-V Management для виявлення віртуальних дисків. Фактичне підключення до цих дисків неможливе. Таким чином, ESET Mail Security створює контрольну точку чи знімок віртуальної машини, а потім підключається до цієї контрольної точки чи знімка. Після завершення сканування контрольна точка чи знімок видаляється. Це означає, що можна виконати сканування в режимі лише для читання, оскільки воно не впливатиме на роботу запущених віртуальних машин.

Щоб створити знімок або контрольну точку під час сканування, ESET Mail Security потрібно до однієї хвилини. Це допоможе, якщо ви застосуєте це під час сканування Hyper-V на більшій кількості віртуальних машин.

Правила іменування

Іменування в модулі сканування Hyper-V здійснюється за таким правилом:

```
VirtualMachineName\DiskX\VolumeY
```

Де X – кількість дисків, а Y – кількість томів. Приклад:

```
Computer\Disk0\Volume1
```

Номерний суфікс додається залежно від порядку виявлення об’єктів і збігається з тим, що відображається в Disk Manager віртуальної машини. Правило іменування використовується в деревоподібному розкривному меню сканованих об’єктів, на індикаторі перебігу виконання процедури, а також у файлах журналу.

Виконання сканування

- За вимогою: клацніть **Сканування Hyper-V**, щоб переглянути список віртуальних машин і томів, доступних для сканування. Виберіть віртуальні машини, диски або томи, які потрібно просканувати, і натисніть **Сканувати**.
- Створення завдання в розкладі.
- Через ESET PROTECT як клієнтське завдання під назвою Сканування сервера.
- Сканування Hyper-V можна налаштовувати й запускати за допомогою eShell.

Одночасно можна виконувати кілька сканувань Hyper-V. Після завершення сканування ви

отримаєте сповіщення з посиланням на файли журналу.

Можливі проблеми

• Під час сканування віртуальної машини, яка працює в мережі, необхідно створити контрольну точку/знімок цієї віртуальної машини. Під час створення контрольної точки/знімка деякі загальні дії операції машини можуть бути обмежені або вимкнуті.

• Якщо сканується автономна віртуальна машина, її неможливо ввімкнути до завершення сканування.

• Диспетчер Hyper-V дає змогу ідентично назвати дві різні віртуальні машини, через що їх можна сплутати в журналах сканування.

Щоб створити новий профіль, виберіть **Редагувати** поруч із пунктом **Список профілів**, укажіть власну **назву профілю** й натисніть **Додати**. Новий профіль відображатиметься в розкривному меню **Вибраний профіль**, що містить наявні профілі сканування.

У розкривному меню **Об'єкти сканування** для **Hyper-V** можна вибрати попередньо визначені об'єкти сканування:

За параметрами профілю	Вибирає об'єкти, установлені у вибраному профілі сканування.
Усі віртуальні машини	Вибирає всі віртуальні машини.
Мережеві віртуальні машини	Вибирає всі мережеві віртуальні машини.
Автономні віртуальні машини	Вибирає всі автономні віртуальні машини.
Без вибору	Скасовується вибір усіх об'єктів.

Клацніть піктограму  і змініть інтервал **Зупинити сканування, якщо воно триває довше ніж (хв.)**, а потім змініть бажаний час (будь-який час від 1 до 2880 хвилин).

Натисніть **Сканувати**, щоб виконати сканування зі встановленими спеціальними параметрами. Після завершення сканування перегляньте **Файли журналу** > Сканування Hyper-V.

Захист Hyper-V й захист на основі машинного навчання

Звіти генеруються ядром виявлення й компонентом машинного навчання.

ThreatSense параметри

Змінення параметрів сканування Hyper-V.

HIPS

Система виявлення втручання (HIPS) захищає вашу систему від шкідливого програмного забезпечення й небажаної активності, які можуть негативно позначатися на вашому комп'ютері. Система HIPS використовує передовий поведінковий аналіз у поєднанні з можливостями мережевої фільтрації для моніторингу запущених процесів, файлів і ключів реєстру. Система HIPS відокремлена від захисту файлової системи в режимі реального часу й не

є брандмауером; вона лише відстежує процеси, що виконуються в операційній системі.

Зміни до параметрів системи HIPS має вносити лише досвідчений користувач. Неправильна конфігурація параметрів HIPS може призвести до нестабільності системи.

Увімкнути самозахист

ESET Mail Security має вбудовану технологію самозахисту, яка не дає змоги шкідливому програмному забезпеченню пошкодити або вимкнути захист від шкідливого програмного забезпечення, тому ви можете бути впевнені, що ваша система завжди захищена. Зміни параметрів "Увімкнути HIPS" та "Увімкнути SD (самозахист)" наберуть сили після перезапуску операційної системи Windows. Якщо вимкнути всю систему HIPS, необхідно перезавантажити комп'ютер.

Увімкнути захищену службу

Компанія Microsoft представила концепцію захищених сервісів у Microsoft Windows Server 2012 R2. Це захищає сервіс від атак шкідливого програмного забезпечення. Ядро ESET Mail Security працює як захищений сервіс за замовчуванням. Ця функція доступна в Microsoft Windows Server 2012 R2 і новіших серверних операційних системах.

Увімкнути розширений сканер пам'яті

У поєданні з модулем захисту від експлойтів удосконалений сканер пам'яті посилює захист від шкідливого ПЗ, призначеного для обходу продуктів для захисту за допомогою обфускації та/або шифрування. Розширений сканер пам'яті увімкнено за замовчуванням. Дізнайтеся більше про цей тип захисту в глосарії.

Увімкнути захист від експлойтів

Служить для захисту програм, які, зазвичай, використовуються для зараження системи, зокрема веб-браузерів, PDF-читачів, клієнтів електронної пошти й компонентів MS Office. Функцію "Блокування експлойтів" увімкнено за замовчуванням. Дізнайтеся більше про цей тип захисту в глосарії.

Увімкнути захист від програм-вимагачів

Щоб користуватися цією функцією, увімкніть HIPS і ESET Live Grid. Дізнайтеся більше про програми-вимагачі в глосарії.

Режим фільтрації

Можна вибрати один із таких режимів фільтрації:

• **Автоматичний режим**: операції ввімкнено (окрім заблокованих попередньо визначеними правилами, які захищають систему). Усі дозволені, за винятком дій, відхилених правилом.

• **Інтелектуальний режим**: користувач отримає сповіщення лише про дуже підозрілі події.

• **Інтерактивний режим**: користувачу пропонується підтверджувати операції. Дозволити/відхилити доступ, створити правило, тимчасово запам'ятати цю дію.

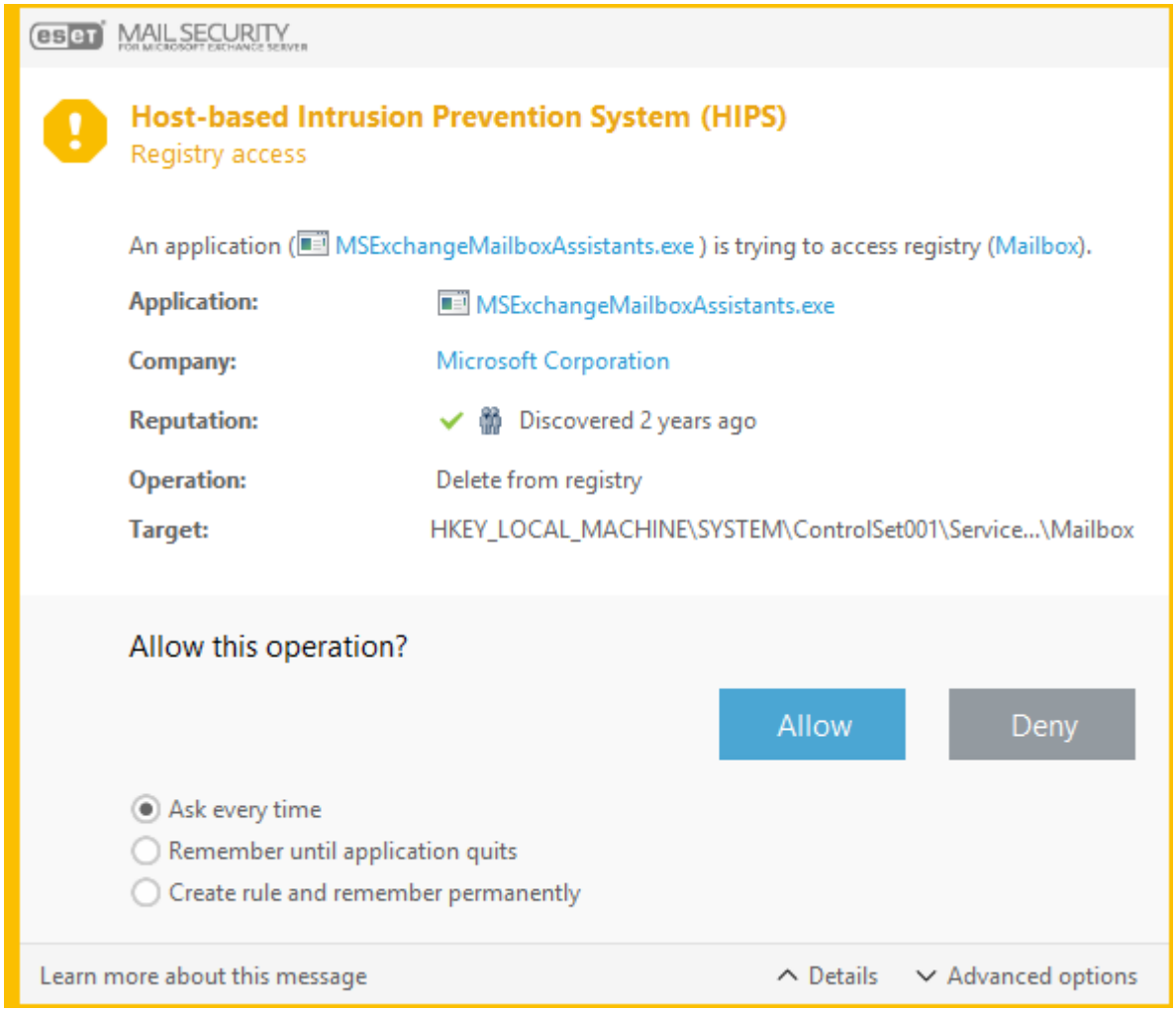
• **Режим на основі політик**: операції заблоковано. Приймає лише користувача / попередньо визначені правила.

• **Режим навчання**: операції ввімкнено, а після кожної операції створюється правило. Правила, створені в цьому режимі, можна переглядати в редакторі правил, проте їхній пріоритет нижчий за пріоритет правил, створених уручну або в автоматичному режимі. Якщо вибрати "Режим навчання" в розкривному меню "Режим фільтрації HIPS", параметр "Режим навчання" стане доступним. Виберіть тривалість використання режиму навчання (максимальний час складає 14 днів). Коли вказаний час мине, з’явиться запит на зміну правил, створених HIPS у режимі навчання. Також можна вибрати інший режим фільтрації або продовжити користуватися режимом навчання.

Правила

Правила визначають, до яких файлів, розділів реєстру чи інших програм матимуть доступ програми. Система HIPS контролює події в операційній системі й реагує на неї відповідно до правил, подібних до правил персонального брандмауера. Натисніть Редагувати, щоб відкрити вікно керування правилами HIPS. Якщо для правила за замовчуванням установлено параметр **Запитувати**, під час кожного його виконання відображатиметься діалогове вікно. Ви можете **заблокувати** або **дозволити** операцію. Якщо в цей час не вибирати дію, вибирається нова дія на основі правил.

У діалоговому вікні можна створити правило на основі будь-якої нової дії, яку HIPS виявляє, а потім визначити умови, за яких потрібно **дозволити** або **заблокувати** цю дію. Натисніть **Подробиці**, щоб переглянути додаткову інформацію. Правила, створені таким чином, вважаються рівносильними правилам, створеним вручну, тому правило, створене з діалогового вікна, може бути менш конкретним, ніж правило, яке викликало це діалогове вікно. Це означає, що після створення такого правила та сама операція може ініціювати те саме вікно.



Запитувати щоразу

Діалогове вікно відображатиметься щоразу, коли правило ініціюватиметься. Ви можете **відхилити** або **дозволити** операцію.

Запам’ятати до закриття програми

Якщо вибрати дію **Відхилити** або **Дозволити**, буде створено тимчасове правило HIPS, яке використовуватиметься до закриття відповідної програми. Крім того, якщо змінити режим фільтрації, змінити правила або оновити модуль HIPS, після перезапуску системи тимчасові правила видалятимуться.

Створити правило та запам’ятати безстроково

Створіть нове правило HIPS. Пізніше це правило можна змінити в розділі керування правилами HIPS.

Параметри правила системи HIPS

У цьому вікні можна переглянути наявні правила HIPS.

Правило	Визначена користувачем або автоматично вибрана назва правила.
Увімкнено	Вимкніть цей перемикач, щоб зберегти правило в списку, але не використовувати його.

Правило	Визначена користувачем або автоматично вибрана назва правила.
Дія	Правило визначає дію ("Дозволити", "Блокувати" або «Запитати"), яка має виконуватися в разі правильності умов.
Джерела	Правило використовуватиметься лише в тому разі, якщо подію ініціюватиме програма.
Цілі	Правило використовуватиметься лише в тому разі, якщо операція пов’язана з певним файлом, програмою або записом реєстру.
Рівень критичності журналу	Якщо ввімкнути цей параметр, інформацію про це правило буде записано в журналі HIPS.
Сповістити	У разі спрацювання події в області сповіщень Windows з’являється невелике вікно.

Створіть нове правило й клацніть **Додати** нові правила HIPS або **Редагувати** вибрані записи.

Ім’я правила

Визначена користувачем або автоматично вибрана назва правила.

Дія

Правило визначає дію (**Дозволити**, **Блокувати** або **Запитати**), яка має виконуватися в разі правильності умов.

Задіяні операції

Необхідно вибрати тип операції, до якої буде застосовано правило. Правило використовуватиметься лише для цього типу операцій і для вибраного об’єкта. Правило складається із частин, що описують умови, які його ініціюють.

Програми-джерела

Правило використовуватиметься лише в тому разі, якщо подію ініціюватиме програма. Виберіть **окремі програми** з розкривного меню й натисніть **Додати**, щоб додати нові файли або папки, або виберіть **усі програми** з розкривного меню.

> Деякі операції певних правил, попередньо визначених HIPS, не можна блокувати й дозволяти за замовчуванням. Крім того, не всі операції системи контролюються HIPS. Система HIPS відстежує операції, які можуть вважатися небезпечними.

Опис важливих операцій:

Операції з файлами

Видалити файл	Програма запитує дозвіл на видалення цільового файлу.
Записати у файл	Програма запитує дозвіл на запис у цільовий файл.

Видалити файл	Програма запитує дозвіл на видалення цільового файлу.
Безпосередній доступ до диска	Програма намагається прочитати диск або записати на нього в нестандартний спосіб, щоб обійти звичайні процедури Windows. Це може призвести до того, що файли будуть змінені без застосування відповідних правил. Ця операція може бути спричинена шкідливим програмним забезпеченням, яке намагається уникнути виявлення, програмою резервного копіювання, яка намагається зробити точну копію диска, або менеджером розділів, який намагається реорганізувати томи диска.
Установити глобальне перехоплення	Стосується виклику функції SetWindowsHookEx із бібліотеки MSDN.
Завантажити драйвер	Інсталяція та завантаження драйверів у систему.

Правило використовуватиметься лише в тому випадку, якщо операція пов’язана із цим об’єктом. Виберіть **певні файли** з розкривного меню й натисніть **Додати**, щоб додати нові файли або папки. Крім того, ви можете вибрати **всі файли** з розкривного меню, щоб додати всі програми.

Операції з програмами

Налагодити іншу програму	Приєднання до процесу засобу налагодження. Під час налагодження програми можна переглядати й змінювати багато відомостей про її поведінку, а також отримати доступ до її даних.
Зупиняти події від іншої програми	Програма-джерело намагається перехопити події, спрямовані на певну програму (наприклад, програма для зчитування натиснень клавіатури намагається перехопити події браузера).
Припинити/призупинити роботу іншої програми	Призупинення, відновлення або припинення процесу (доступ можна отримати безпосередньо з провідника процесів або у вікні "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 код від її імені. Ця функція може бути корисною для захисту важливої програми. Для цього потрібно налаштувати її як цільову програму в правилі, що блокує використання цієї операції.

Правило використовуватиметься лише в тому разі, якщо операція пов’язана із цим об’єктом. Виберіть **певні програми** з розкривного меню й натисніть **Додати**, щоб додати нові файли або папки. Крім того, ви можете вибрати **всі програми** з розкривного меню, щоб додати всі програми.

Операції з реєстром

Змінити параметри запуску	Будь-які зміни в параметрах, які визначають, які програми будуть запускатися під час запуску Windows. Їх можна знайти, наприклад, за допомогою пошуку ключа "Виконати" в реєстрі Windows.
Видалити з реєстру	Видалення розділу реєстру або його значення.
Перейменувати розділ реєстру	Перейменування розділу реєстру

Змінити параметри запуску	Будь-які зміни в параметрах, які визначають, які програми будуть запускатися під час запуску Windows. Їх можна знайти, наприклад, за допомогою пошуку ключа "Виконати" в реєстрі Windows.
Внести зміни до реєстру	Створення нових значень розділів реєстру, зміна наявних значень, переміщення даних у дереві бази даних або налаштування прав користувача або груп для розділів реєстру.

Правило використовуватиметься лише в тому разі, якщо операція пов'язана із цим об'єктом. Виберіть **певні записи** з розкривного меню й натисніть **Додати**, щоб додати нові файли або папки. Крім того, ви можете вибрати **всі записи** з розкривного меню, щоб додати всі програми.

Під час введення об'єкта можна використовувати групові символи з певними обмеженнями. Замість певного розділу в шляхах реєстру можна використовувати символ "*" (зірочка). Наприклад, *HKEY_USERS*\software can mean HKEY_USER\.default\software*, але не *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** не є коректним шляхом до розділу реєстру. Шлях до розділу реєстру, що містить ***, означає цей шлях або будь-який шлях на будь-якому рівні після цього символу. Це єдиний спосіб використовувати групові символи для цілей файлів. Спершу оцінюється конкретна частина шляху, а потім шлях, який слідуватиме за груповим символом (*).

Якщо створити перевизначене загальне правило, ви можете отримати сповіщення.

Додаткові параметри HIPS

Нижче наведено корисні варіанти для налагодження та аналізу поведінки програми.

Драйвери, які дозволено завжди завантажувати

Вибрані драйвери завжди дозволено завантажувати незалежно від налаштованого режиму фільтрації, якщо вони явно не заблоковані правилом користувача. Завантаження драйверів, зазначених у цьому списку, завжди дозволятиметься незалежно від режиму фільтрації HIPS, якщо їх не блокує правило користувача. У списку можна **додати** новий драйвер, **змінити** або **видалити** вибраний.

Натисніть **Скинути**, якщо ви не хочете включати драйвери, додані вручну. Це може бути корисно, якщо ви додали кілька драйверів, і їх не можна видалити зі списку вручну.

Реєструвати всі заблоковані операції

Усі заблоковані операції буде записано в журнал HIPS. Цю функцію можна використовувати тільки для виправлення неполадок або в разі отримання відповідних інструкцій від служби технічної підтримки ESET, оскільки це може призвести до створення файлу журналу великого розміру й сповільнити роботу системи.

Повідомляти, коли в автоматично виконувані програми вносяться зміни

Відображає сповіщення на робочому столі щоразу, коли програма додається до списку завантажуваних під час запуску системи або видаляється з нього.

Оновити конфігурацію

У цьому розділі вказується інформація про оновлення, наприклад сервери оновлень, а також дані автентифікації для цих серверів.

Щоб оновлення завантажилося належним чином, важливо правильно вказувати всі параметри оновлення. Якщо ви використовуєте брандмауер, переконайтеся, що програмі ESET дозволено обмінюватися даними з Інтернетом (наприклад, через протокол HTTP).

Основна

Вибрати профіль оновлення за замовчуванням
Виберіть наявний або створіть новий профіль, який застосовуватиметься за замовчуванням для оновлення.
Автоматичне переключення профілів
Призначте профіль оновлення відповідно до відомих мереж у брандмауері. Автоматичне переключення профілів дає змогу змінювати профіль для певної мережі залежно від налаштування в розділі "Розклад". Щоб дізнатися більше, перегляньте довідку.
Налаштування сповіщень про оновлення
Клацніть **Змінити**, щоб вибрати сповіщення програми, які будуть відображатися. Виберіть один із таких параметрів для сповіщень: "Показувати на робочому столі" або "Пересилати на електронну пошту".
Очистити кеш оновлення
Якщо виникнуть проблеми з оновленням, натисніть **Очистити**, щоб очистити тимчасовий кеш оновлення.

Оновлення продукту

Автоматичні оновлення
Увімкнено за замовчуванням. За допомогою повзунка можна вимикати автоматичні оновлення, якщо потрібно тимчасово припинити оновлення ESET Mail Security. Рекомендуємо не вимикати цей параметр, щоб гарантувати, що ESET Mail Security має найновіші оновлення програмних компонентів (PCU) та оновлення мікропрограмних компонентів (µPCU), які застосовуються, коли доступне нове оновлення.

> Оновлення застосуються після наступного перезапуску сервера.

Сповіщення про застаріле ядро виявлення

Автоматично встановлювати термін дії ядра виявлення / максимальний термін дії ядра виявлення (дн.)
За допомогою повзунка вимкніть термін дії автоматичного ядра виявлення й установіть максимальний час вручну (у днях), після завершення якого термін дії ядра виявлення буде позначено як застарілий. Значення за замовчуванням: 7.

Відкочування модуля

Якщо ви підозрюєте, що нове оновлення ядра виявлення та/або програмних модулів може бути нестабільним або пошкодженим, ви можете відкотитися до попередньої версії та відключити оновлення на певний період часу. Крім того, можна ввімкнути раніше вимкнуті оновлення, якщо їх було відтерміновано на невизначений час. ESET Mail Security записує знімки ядра виявлення та модулів програми для використання з функцією відкочування. Щоб створити знімки обробника виявлення, не вимикайте параметр **Створити знімки модулів**.
Кількість локально збережених знімків
Визначає кількість попередньо збережених знімків модулів.
Повернутися до попередніх модулів
Виберіть Відкочування, щоб повернути модулі програми до попередньої версії, і тимчасово вимкніть оновлення.

Профілі
Щоб створити спеціальний профіль оновлення, виберіть **Редагувати** поруч із пунктом **Список профілів**. Введіть власну **назву профілю** й натисніть **Додати**. Виберіть профіль, щоб змінити параметри для типів оновлень модулів, або створіть **дзеркало оновлення**.

Оновлення

У розкривному меню виберіть тип оновлення.
• **Регулярне оновлення**: за замовчуванням для параметра "Тип оновлення" задано значення "Регулярне оновлення", щоб забезпечити автоматичне завантаження файлів оновлень із сервера ESET із найменшими витратами мережевого трафіку.
• **Пре-реліз оновлення**: пройшли повну внутрішню перевірку й незабаром будуть доступні для широкого загалу. Перевага попередніх оновлень – це доступ до інноваційних методів виявлення загроз і найновіших функцій продукту. Однак попередні оновлення можуть бути недостатньо стабільними в будь-який час і НЕ повинні використовуватися на виробничих серверах та робочих станціях, де потрібна максимальна доступність і стабільність.
• **Відкладені оновлення**: дають змогу виконувати оновлення зі спеціальних серверів, що забезпечують нові версії вірусних баз даних із затримкою принаймні X год (тобто, бази даних протестовано в реальному середовищі, тому вони вважаються стабільними).

Увімкнути оптимізацію доставки оновлення
Якщо цей параметр увімкнено, файли оновлень завантажуються із CDN (мережа доставки вмісту). Вимкнення цього параметра може спричинити переривання завантаження та уповільнення роботи, коли виділені сервери оновлень ESET перевантажені. Вимкнення корисне, коли брандмауер обмежується доступом лише до IP-адрес сервера оновлення ESET або підключення до сервісів CDN не працює.

Запитувати перед завантаженням оновлення
Коли стане доступним нове оновлення, з'явиться запит на його завантаження.

Запитувати, якщо розмір файлу оновлення більший за (КБ)
Якщо розмір файлу оновлення більший за значення, указане в полі, з'явиться сповіщення.

Оновлення модулів

За замовчуванням для оновлень модулів установлено **автоматичний вибір**. Сервер оновлень – це розташування, у якому зберігаються оновлення. Якщо ви використовуєте сервер ESET, рекомендуємо не вимикати параметр за замовчуванням.

У разі використання локального HTTP-сервера (також відомого як дзеркало) параметри сервера оновлення потрібно вказати таким чином: **http://computer_name_or_its_IP_address:2221**
У разі використання локального HTTP-сервера з протоколом SSL параметри сервера оновлення потрібно вказати таким чином: https://computer_name_or_its_IP_address:2221
У разі використання спільної папки параметри сервера оновлення потрібно вказати таким чином: \\computer_name_or_its_IP_address\shared_folder

Увімкнути частіші оновлення модулів
Ядра виявлення буде оновлено за короткі проміжки часу. Вимкнення цього параметра може негативно вплинути на частоту виявлення.

Дозволити оновлення модулів зі змінного носія
Оновлення зі змінного носія, якщо містить створене дзеркало. Якщо вибрано **Автоматично**, оновлення будуть виконуватися у фоновому режимі. Щоб показати діалогові вікна оновлення, виберіть **Завжди запитувати**.

Оновлення продукту

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.

У деяких випадках для оновлення може знадобитися перезавантажити сервер.

Параметри підключення

Проксі-сервер
Щоб отримати доступ до параметрів проксі-сервера для певного профілю оновлення, натисніть режим проксі-сервера й виберіть одну з трьох наведених нижче опцій.
• **Не використовувати проксі-сервер**: під час оновлення ESET Mail Security не використовуватиметься проксі-сервер.
• **Використовувати глобальні параметри проксі-сервера**: використовуватиметься конфігурація проксі-сервера, указана в розділі "Додаткові параметри" (F5) > Інструменти > Проксі-сервер.
• **Підключення через проксі-сервер**: використовуйте цей параметр у наведених нижче випадках.

для оновлення ESET Mail Security слід використовувати проксі-сервер, відмінний від проксі-сервера, зазначеного в глобальних налаштуваннях (Інструменти > Проксі-сервер). Якщо це так, слід указати тут параметри: За потреби для проксі-сервера використовується адреса проксі-сервера, порт обміну даними (за замовчуванням – 3128), а також ім'я користувача й пароль для проксі-сервера.

Параметри проксі-сервера не було встановлено глобально, але ESET Mail Security підключатиметься до проксі-сервера для оновлення.

Ваш комп'ютер підключено до Інтернету через проксі-сервер. Під час інсталяції програми параметри беруться з конфігурації Internet Explorer, але якщо згодом вони змінюються (наприклад, ви згодні змінити постачальника послуг Інтернету), перевірте, чи правильні параметри проксі-сервера HTTP, указані в цьому вікні. В іншому разі програма не зможе підключитися до серверів оновлень.

Дані автентифікації, наприклад **ім'я користувача** й **пароль**, призначені для доступу до проксі-сервера. Заповніть ці поля, лише якщо потрібно вказувати ім'я користувача й пароль. Зверніть увагу, що ці поля не вказують на ім'я користувача / пароль для програми ESET Mail Security, тому їх слід заповнити, лише якщо вам відомо, що для доступу до Інтернету через проксі-сервер потрібно вказувати пароль.

Використовувати пряме підключення, якщо проксі-сервер недоступний
Якщо продукт налаштувати для використання проксі-сервера HTTP, проте проксі-сервер буде недоступним, продукт обійде проксі-сервер та обмінюватиметься даними безпосередньо із серверами ESET.
Спільні папки Windows
Під час оновлення з локального сервера, на якому запущено Windows, автентифікація кожного мережевого підключення вимагається за замовчуванням.
Підключатися до локальної мережі як
Щоб налаштувати обліковий запис, виберіть одну з наведених нижче опцій.
• **Системний обліковий запис (за замовчуванням)**: використання системного облікового запису для автентифікації. Зазвичай процес автентифікації не відбувається, якщо в розділі основних параметрів оновлення не вказано дані автентифікації.
• **Поточний користувач**: виберіть цей параметр, щоб програма виконувала автентифікацію з використанням облікового запису користувача, який увійшов у систему. Недоліком такого рішення є те, що програма не може підключитися до сервера оновлень, якщо наразі жоден користувач не увійшов до системи.
• **Указаний користувач**: виберіть цей параметр, щоб використовувати для автентифікації обліковий запис конкретного користувача. Використовуйте цей метод, якщо не вдається виконати підключення до системного облікового запису за замовчуванням. Пам'ятайте, що обліковий запис указаного користувача повинен мати доступ до каталогу файлів оновлення на локальному сервері. Якщо користувач не має доступу, програма не зможе встановити підключення або завантажити оновлення.

Якщо вибрано параметр **Поточний користувач** або **Зазначений користувач**, під час зміни ідентифікатора програми на потрібного користувача може виникати помилка. Рекомендуємо вказати дані автентифікації локальної мережі в головному розділі параметрів оновлення. У цьому розділі параметрів оновлення слід указати дані автентифікації таким чином: domain_name\user (якщо це робоча група, укажіть workgroup_name\name) і пароль. Під час оновлення з http-версії локального сервера автентифікація не потрібна.

Відключатися від сервера після оновлення
Примусове відключення, якщо підключення до сервера залишається активним навіть після завантаження оновлень.

Дзеркало оновлень

Параметри конфігурації для локального сервера дзеркала розташовані в розділі **Додаткові параметри** (F5) на вкладці > **Оновлення Профілі** > Дзеркало оновлення.

Відкочування оновлення

Якщо ви вважаєте, що нещодавнє оновлення обробника виявлення або модулів програми може бути нестабільним або пошкодженим, можна виконати відкочування до попередньої версії й тимчасово вимкнути оновлення. Окрім того, можна ввімкнути раніше вимкнуті оновлення, якщо їх було відтерміновано на невизначений час.

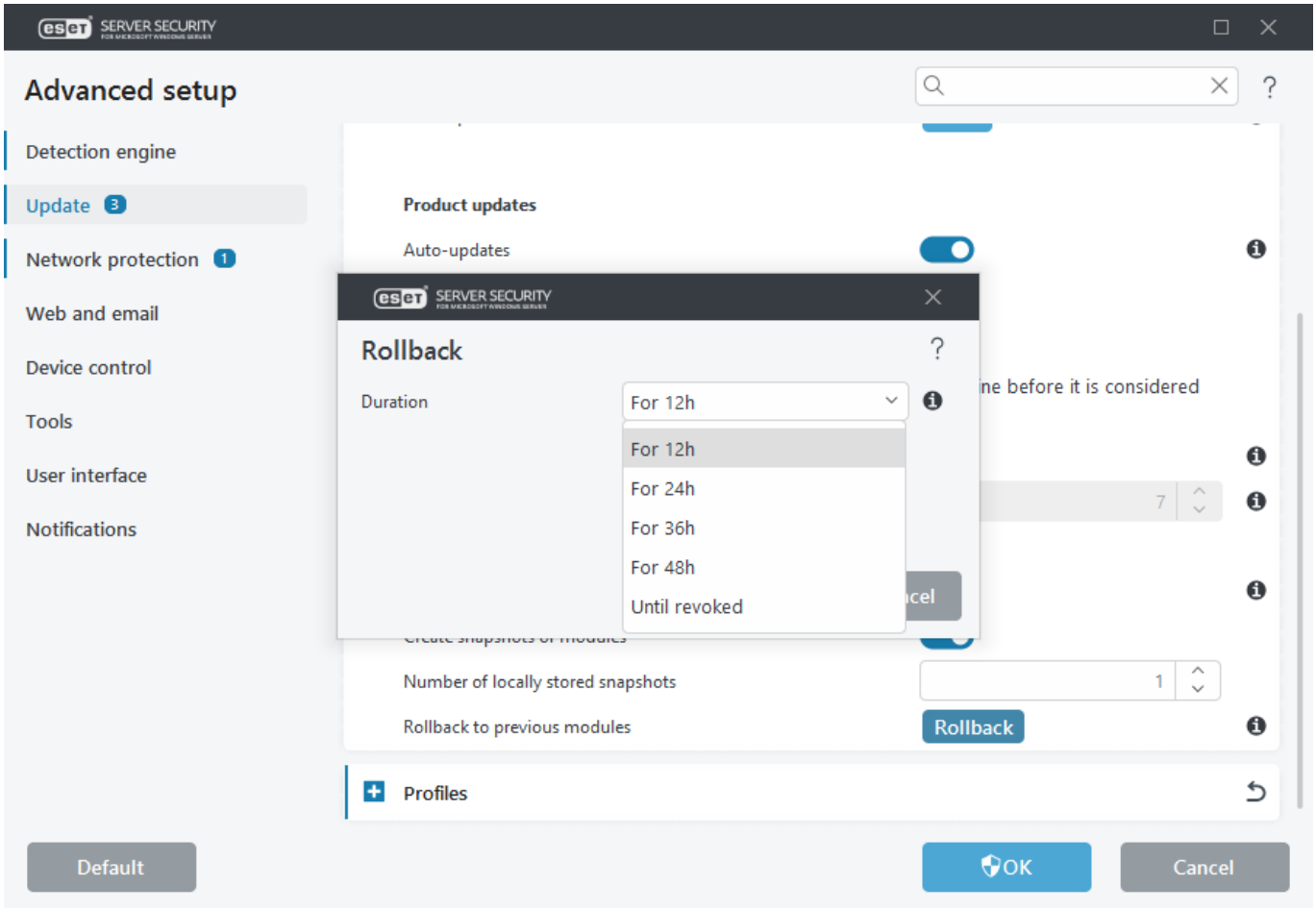
ESET Mail Security записує знімки обробника виявлення й модулів програми, які можна використовувати з функцією відкочування. Щоб створювати знімки бази даних вірусів, не вимикайте параметр **Створити знімки модулів**.

Якщо параметр **Створити знімки модулів** увімкнуто, під час першого оновлення створюється перший знімок. Наступний знімок створюється через 48 годин.

У полі **Кількість локально збережених знімків** визначається кількість збережених знімків обробника виявлення.

> Коли досягнуто максимальної кількості знімків (наприклад, три), найстаріший знімок замінюється новим знімком кожні 48 годин. ESET Mail Security відкочує оновлення обробника виявлення й модуля програми до найстарішого знімка.

Якщо натиснути **Відкочування**, у розкривному меню потрібно вибрати проміжок часу, протягом якого буде призупинено оновлення бази даних обробника виявлення й модулів програми.



Виберіть **До відкликання**, щоб відкласти регулярні оновлення на невизначений час, доки не відновите їх вручну. Рекомендується не вибирати цей параметр, оскільки це становить потенційну загрозу безпеці.

Якщо виконано відкочування, замість кнопки **Відкочування** відображатиметься кнопка **Дозволити оновлення**. Оновлення не будуть дозволені протягом проміжку часу, вибраного в розкривному меню **Призупинити оновлення**.

Версію бази даних ядра виявлення буде понижено до найстарішої з доступних. Вона зберігатиметься як знімок у файловій системі локального комп'ютера.

Заплановане завдання: оновлення

Якщо потрібно оновити програму з двох серверів оновлень, необхідно створити два різних профілі оновлення. Якщо першому не вдається завантажити файли оновлення, програма автоматично переключається на альтернативний. Це зручно, наприклад, для ноутбуків, які зазвичай оновлюються із сервера оновлення локальної мережі, але їхні власники часто підключаються до Інтернету через інші мережі. Тому, якщо перший профіль не вдається завантажити, другий автоматично завантажить файли оновлення із серверів оновлень ESET.

Нижче наведено інструкції щодо того, як відредагувати наявне **регулярне автоматичне оновлення**.
1. На головному екрані **розкладу** виберіть завдання **оновлення** з назвою **Регулярне автоматичне оновлення** й натисніть **Редагувати**. Відкриється майстер налаштування.
2. Задайте заплановане завдання та виберіть одну з наведених нижче опцій часу, щоб визначити час запуску запланованої задачі.
3. Щоб заборонити виконання завдання, коли система працює від акумулятора (наприклад, джерела безперебійного живлення), натисніть перемикач поруч із пунктом **Не запускати завдання під час роботи від акумулятора**.
4. Виберіть профіль для оновлення. Виберіть дію, яку потрібно виконати, якщо виконання запланованого завдання неможливе з будь-якої причини.
5. Натисніть **Готово**, щоб застосувати завдання.

Дзеркало оновлень

ESET Mail Security дає змогу створювати копії файлів оновлень, які можна використовувати для оновлення інших робочих станцій у мережі. Використовувати "дзеркало", копію файлів оновлення в середовищі локальної мережі, зручно, оскільки ці файли не доведеться постійно завантажувати із сервера оновлень постачальника на кожну робочу станцію. Щоб уникнути ризику перевантаження мережевого трафіку, оновлення завантажуються на локальний сервер-дзеркало, а потім розповсюджуються на всі робочі станції.

Оновлення робочих станцій клієнта із дзеркала дає змогу оптимізувати баланс навантаження на мережу й заощадити пропускну здатність підключення до Інтернету.

Щоб мінімізувати інтернет-трафік у мережах, де ESET PROTECT використовується для керування великою кількістю клієнтів, рекомендуємо використовувати ESET Bridge, а не налаштовувати клієнт як дзеркало. ESET Bridge можна інсталювати разом із ESET PROTECT за допомогою універсального інсталятора або як окремий компонент. Докладніші відомості, а також відомості про відмінності між ESET Bridge, проксі-сервером Apache HTTP, Mirror Tool і прямим підключенням див. на сторінці онлайн-довідки ESET PROTECT.

Дзеркало оновлень

Створити дзеркало оновлення
Активує параметри конфігурації дзеркала.

Доступ до файлів оновлення

Увімкнути HTTP-сервер
Якщо цей параметр увімкнуто, доступ до файлів оновлень можна отримати через протокол HTTP без облікових даних.

Папка для зберігання
Натисніть **Змінити**, щоб знайти папку на локальному комп’ютері або спільну мережеву папку. Якщо для вказаної папки необхідна авторизація, введіть дані автентифікації в поля "Ім’я користувача" й "Пароль".
Клацніть **Очистити**, щоб змінити визначену папку за замовчуванням для зберігання дзеркальних дублікатів файлів (*C:\ProgramData\ESET\ESET Security\mirror*).

HTTP-сервер

Порт сервера
Порт за замовчуванням – 2221. Змініть це значення, якщо використовуєте інший порт.
Аутентифікація
Визначає метод автентифікації, що використовується для доступу до файлів оновлень. Доступні такі опції: **Немає**, **Базова** та **NTLM**.
• Виберіть **Базова**, щоб використовувати кодування base64 з базовою автентифікацією за допомогою імені користувача й пароля.
• Опція **NTLM** забезпечує використання безпечного методу кодування. Для автентифікації використовується користувач, створений на робочій станції, що надає спільний доступ до файлів оновлення.
• За замовчуванням використовується параметр **Немає**, тобто доступ до файлів оновлень не потребує автентифікації.

> ⚠ Щоб надати доступ до файлів оновлень через HTTP-сервер, розмістіть папку дзеркала на тому самому комп'ютері, що й екземпляр ESET Mail Security, який її створив.

SSL для HTTP-сервера
Додайте **файл ланцюжка сертифікатів** або створіть самопідписаний сертифікат, щоб забезпечити підтримку сервера HTTP через протокол SSL. Доступні такі типи сертифікатів: PEM, PFX та ASN. Щоб забезпечити додатковий рівень захисту, завантажуйте файли оновлення за допомогою протоколу HTTPS. У такому разі буде майже неможливо відстежити передання даних і облікові дані для входу.
За замовчуванням для параметра **Тип закритого ключа** встановлено значення **Інтегрований** (тому за замовчуванням опцію "Файл закритого ключа" вимкнено). Це означає, що закритий ключ є частиною вибраного файлу ланцюжка сертифікатів.
Параметри підключення

Спільні папки Windows
Під час оновлення з локального сервера, на якому запущено Windows, автентифікація кожного мережевого підключення вимагається за замовчуванням.
Підключатися до локальної мережі як
Щоб налаштувати обліковий запис, виберіть одну з наведених нижче опцій.
• **Системний обліковий запис** (за замовчуванням): для автентифікації використовуватиметься системний обліковий запис. Зазвичай процес автентифікації не відбувається, якщо в розділі основних параметрів оновлення не вказано дані автентифікації.
• **Поточний користувач**: програма буде виконувати автентифікацію з використанням облікового запису користувача, який увійшов у систему. Недоліком такого рішення є те, що програма не зможе підключитися до сервера оновлень, якщо жоден користувач не увійшов у систему.
• **Вказаний користувач**: виберіть, щоб використовувати для автентифікації обліковий запис користувача. Використовуйте цей метод, якщо не вдається виконати підключення до системного облікового запису за замовчуванням. Пам'ятайте, що обліковий запис указаного користувача повинен мати доступ до каталогу файлів оновлень на локальному сервері. Якщо користувач не має доступу, програма не зможе встановити підключення й завантажити оновлення.

> ⚠ Якщо вибрано параметр **Поточний користувач** або **Зазначений користувач**, під час зміни ідентифікатора програми на потрібного користувача може виникати помилка. Рекомендуємо внести дані автентифікації локальної мережі в головному розділі параметрів оновлення. У цьому розділі параметрів оновлення слід указати дані автентифікації таким чином: *domain_name**user* (якщо це робоча група, укажіть *workgroup_name**name*) і пароль. Під час оновлення з HTTP-версії локального сервера автентифікація не потрібна.

Відключатися від сервера після оновлення
Примусове відключення, якщо підключення до сервера залишається активним навіть після завантаження оновлень.

Захист мережі

Керуйте захистом мережі, натисніть **"Змінити"**, щоб додати нові або змінити наявні налаштування, зазначені далі.

- Відомі мережі
- Зони

Відомі мережі

У разі частого підключення комп'ютера до загальнодоступних мереж або до інших мереж, окрім робочої, рекомендовано перевіряти їхню надійність. Після визначення мережі ESET Mail Security може розпізнати довірені (домашні або робочі) мережі, використовуючи різні параметри, задані в розділі Ідентифікаційні дані мережі.

Комп'ютери часто підключаються до мереж з IP-адресами, подібними до адреси надійної мережі. У таких випадках ESET Mail Security може віднести невідому мережу до довіреної (домашньої чи робочої). Щоб уникнути цього, рекомендовано використовувати функцію автентифікації мережі.

Коли мережевий адаптер підключається до мережі або його налаштування змінюються, ESET Mail Security здійснюватиме пошук у списку відомих мереж запису, що збігатиметься з параметрами нової мережі. Якщо параметри в розділах "Ідентифікаційні дані мережі" й "Автентифікація мережі" (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 "Загальнодоступна мережа".

У новому діалоговому вікні "Виявлено мережеве підключення" можна вибрати тип захисту "Загальнодоступна мережа", "Домашня або корпоративна мережа" чи "Використовувати параметр Windows". Якщо мережевий адаптер підключено до відомої мережі, яку позначено як "Домашня або корпоративна мережа", локальні підмережі адаптера додаються до довіреної зони.

Тип захисту нових мереж

Виберіть один із варіантів нижче. **Використовувати параметр Windows**, **Запитувати користувача** або **Позначити як загальнодоступну** використовується за замовчуванням для нових мереж. Якщо вибрати **Використовувати параметр Windows**, діалогове вікно не з'являтиметься, а мережу, до якої ви підключені, буде автоматично позначено відповідно до параметрів Windows. Через це певні функції (наприклад, обмін файлами й віддалений робочий стіл) будуть доступні в разі підключення до нових мереж.

Відомі мережі можна налаштувати вручну у вікні Редактор відомих мереж.

Додати мережу

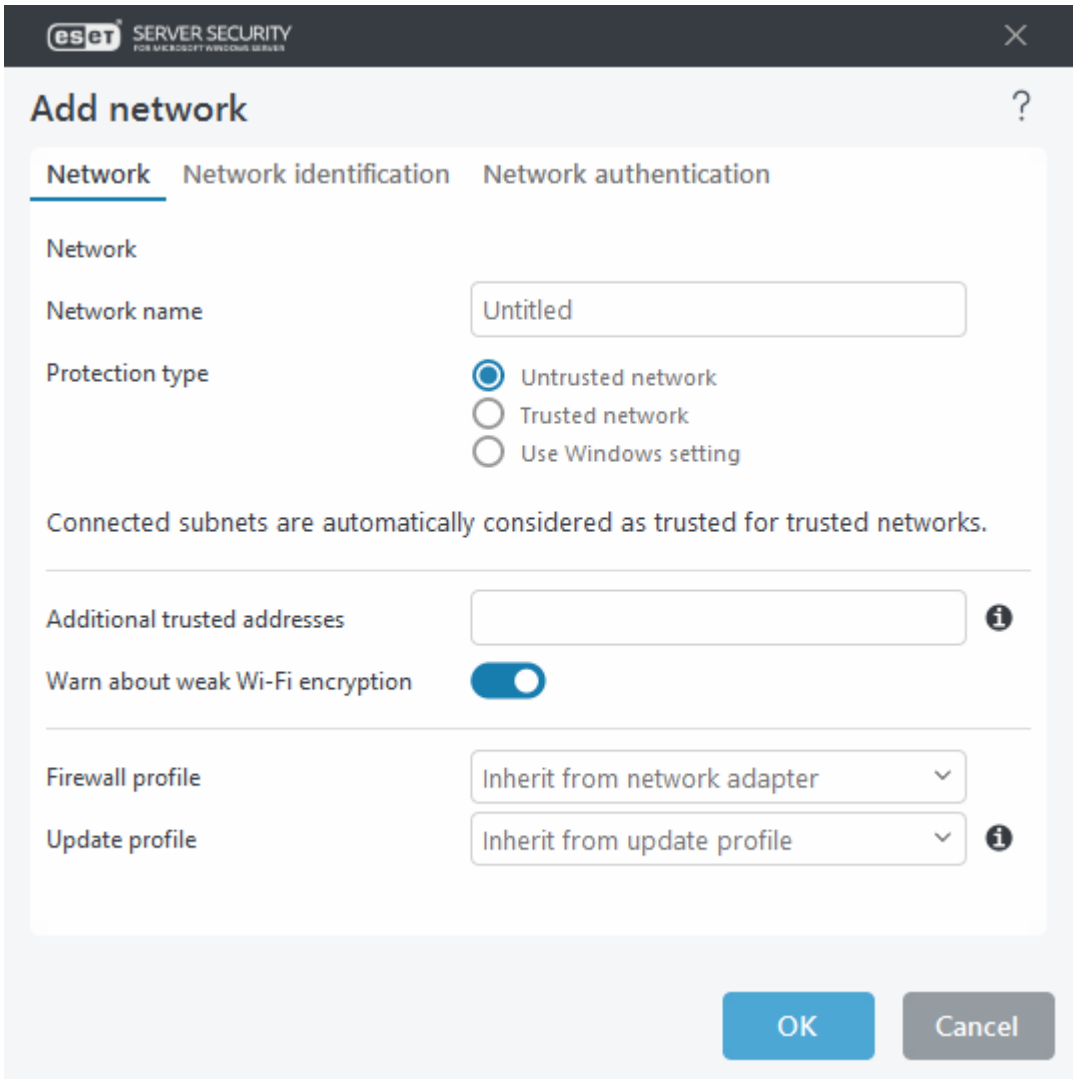
Параметри конфігурації мережі розташовано на таких указаних нижче вкладках.

Мережа

Тут можна задати **ім'я** й вибрати **тип захисту** для мережі. Показує, який параметр вибрано для мережі (**Надійна мережа**, **Ненадійна мережа** або **Використовувати параметр Windows**).

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

- **Попереджати про слабке шифрування Wi-Fi**: ESET Mail Security сповістить вас про підключення до незахищеної бездротової мережі або мережі зі слабким захистом.
- **Профіль брандмауера** буде отримано від мережевого адаптера.
- **Профіль оновлення**: дає змогу вибрати профіль оновлення, який буде використовуватися під час підключення до цієї мережі.



Ідентифікаційні дані мережі

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

Аутентифікація мережі

Ця функція 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 й відкритий ключ, який відповідає закритому ключу сервера. Ім’я сервера можна ввести як IP-адресу, DNS або ім’я NetBios разом зі шляхом розташування ключа на сервері (наприклад, *server_name_/directory1/directory2/authentication*). Можна вказати альтернативні сервери для використання, додаючи їх до шляху й розділяючи крапкою з комою.

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.
- Зашифрований відкритий ключ
- Файл сертифіката відкритого ключа (.crt)

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.

Помилка автентифікації на сервері. Неприпустимий або невідповідний підпис.	**Підпис сервера не збігається із введеним відкритим ключем.**
Помилка автентифікації на сервері. Невідповідність імені мережі.	Вимкніть цей перемикач, щоб зберегти правило в списку, але не використовувати його.
Помилка автентифікації на сервері. Неприпустима відповідь сервера або немає відповіді.	Відповідь не надійде, якщо сервер не працює або він недоступний. Якщо за вказаною адресою працює інший HTTP-сервер, може надійти неприпустима відповідь.
Введено недійсний відкритий ключ.	Переконайтеся, що файл відкритого ключа не пошкоджено.

Зони

Зона — це набір мережевих адрес, які створюють одну логічну групу IP-адрес, що стає в пригоді, коли потрібно повторно використовувати однаковий набір адрес у кількох правилах. Кожній адресі в певній групі призначаються аналогічні правила, визначені централізовано для всієї групи. Одним із прикладів такої групи є **довірена зона**. Довірена зона – це група мережевих адрес, які не блокує брандмауер.

Порядок додавання довіреної зони

1. Відкрийте **Додаткові параметри** (**F5**) > **Захист мережі** > **Основна** > **Зони**.

2. Клацніть **Змінити** поруч із розділом **Зони**.

3. Клацніть **Додати**, уведіть **назву** й **опис** для нової зони, а також додайте IP-адресу віддаленого комп’ютера в поле **Адреса віддаленого комп’ютера (IPv4/IPv6, діапазон, маска)**.

4. Клацніть **OK**.

Стовпці

- **Ім’я**: ім’я групи віддалених комп’ютерів.
- **IP-адреси**: віддалені IP-адреси, що належать зоні.

Елементи контролю

Під час додавання або зміни зони доступні наведені нижче поля:

- **Ім’я**: ім’я групи віддалених комп’ютерів.
- **Опис**: загальний опис групи.
- **Адреса віддаленого комп'ютера (IPv4, IPv6, діапазон, маска)**: віддалена адреса, діапазон адрес або підмережа.
- **Видалити**: видалення зони зі списку.

Попередньо визначені зони неможливо видалити.

Захист мережі від атак

Увімкнути захист мережі від атак (IDS)

Дозволяє налаштувати доступ до деяких служб, запущених на комп’ютері з довіреної зони, і ввімкнути або вимкнути виявлення кількох типів атак та експлойтів, які можуть бути використані, щоб нашкодити комп'ютеру.

Увімкнути захист від ботнетів

Виявляє й блокує обмін даними зі шкідливими командними та керівними серверами відповідно до звичних шаблонів, які вказують на зараження комп’ютера та спробу бота обмінюватися даними.

Виключення IDS

Виключення системи виявлення вторгнень (IDS) можна сприймати як правила захисту мережі. Натисніть Змінити, щоб визначити виключення IDS.

У разі наявності середовища з високошвидкісною мережею (10 Гбіт/с і вище) радимо ознайомитися з інформацією в статті бази знань про швидкість роботи мережі та ESET Mail Security.

Захист від атак повним перебором

ESET Mail Security перевіряє вміст мережевого трафіку й блокує спроби атак, які передбачають угадування пароля.

Додаткові параметри

Дає змогу налаштувати додаткові опції фільтрації, щоб виявляти різні типи атак і вразливостей, які може бути застосовано до комп'ютера.

Виявлення вторгнення:

Протокол SMB – виявляє та блокує різні проблеми з безпекою в протоколі SMB.
Протокол RPC – виявляє та блокує різноманітні CVE в системі віддаленого виклику процедур, розробленій для розподіленого обчислювального середовища (DCE).
Протокол RDP – виявляє та блокує різноманітні CVE в протоколі RDP (див. вище).
Блокувати небезпечну адресу після виявлення атаки – перегляд списку IP-адрес, які визначені як джерела атак і додані до чорного списку, щоб блокувати з'єднання протягом певного періоду часу.
Відображати сповіщення після виявлення атаки – вмикає область сповіщень Windows у нижньому правому куті екрана.
Також відображати сповіщення про атаки, спрямовані на слабкі місця в системі безпеки – відображає сповіщення, якщо виявлено атаки на вразливості в системі або спроби ввійти в систему таким чином, що створюється загроза.

Перевірка пакетів:

Дозволити вхідні запити спільних адміністративних ресурсів у протоколі SMB – спільні адміністративні ресурси (адмінресурси) є за замовчуванням мережевими папками, які спільно використовують розділи жорсткого диска (C$, D$, ...) у системі разом із системною папкою (ADMIN$). Заборона підключення до спільних адміністративних ресурсів дає змогу мінімізувати багато ризиків безпеки. Наприклад, черв'як Conficker виконує словникові атаки, щоб підключитися до спільних адміністративних ресурсів.
Відхилити застарілі (непідтримувані) діалекти SMB – відмова від сеансів SMB, які використовують застарілий діалект SMB, що не підтримується IDS. Сучасні операційні системи Windows підтримують застарілі діалекти SMB, щоб гарантувати зворотну сумісність зі старими операційними системами, як-от Windows 95. Зловмисник може використати застарілий діалект під час сеансу SMB, щоб обійти перевірку трафіку. Відмовтеся від старих діалектів SMB, якщо комп'ютеру не потрібно обмінюватися файлами (або використовувати SMB-з'єднання взагалі) з комп'ютером зі старою версією Windows.
Відхилити SMB без розширення функцій безпеки – розширена безпека може використовуватися під час узгодження сеансу SMB, щоб забезпечити безпечніший механізм автентифікації, ніж автентифікація LAN Manager Challenge або Response (LM). Схема LM вважається слабкою, тому використовувати її не рекомендовано.
Дозволити обмін даними із службою диспетчера облікових записів – додаткові відомості про цю службу див. у розділі [MS-SAMR].
Дозволити обмін даними із службою локального центру безпеки – додаткові відомості про цю службу див. у розділах [MS-LSAD] та [MS-LSAT].

Дозволити вхідні запити спільних адміністративних ресурсів у протоколі SMB – спільні адміністративні ресурси (адмінресурси) є за замовчуванням мережевими папками, які спільно використовують розділи жорсткого диска (C$, D$, ...) у системі разом із системною папкою (ADMIN$). Заборона підключення до спільних адміністративних ресурсів дає змогу мінімізувати багато ризиків безпеки. Наприклад, черв'як Conficker виконує словникові атаки, щоб підключитися до спільних адміністративних ресурсів.
Дозволити обмін даними із службою віддаленого реєстру. Щоб дізнатися більше про цю службу, див. у розділі [MS-RRP].
Дозволити обмін даними із службою диспетчера керування службами – докладніше про цю службу див. у розділі [MS-SCMR].
Дозволити обмін даними із службою сервера – інформацію про цю службу див. у розділі [MS-SRVS].
Дозволити обмін даними з іншими службами – інші служби MSRPC.

Виключення IDS

Виключення системи виявлення вторгнень (IDS) – це фактично правила захисту мережі. Виключення аналізуються за списком згори донизу. Редактор виключень IDS дозволяє налаштувати поведінку захисту мережі за наявності різних виключень IDS. Перше виключення, з яким установлюється відповідність, застосовується для кожного типу дії (блокування, сповіщення, реєстрація в журналі) окремо. Натискайте **зверху**, **угору**, **униз**, **знизу**, щоб задати рівень пріоритету виключень. Щоб створити нове виключення IDS, натисніть **Додати**. Натисніть **Змінити**, щоб змінити наявне виключення IDS, або **Видалити**, щоб видалити його.

Виберіть тип **сповіщення** з розкривного списку. Укажіть **Ім'я загрози** та її **Напрямок**. Знайдіть **програму,** для якої необхідно створити виключення. Укажіть список IP-адрес (IPv4 чи IPv6) або підмереж. Кілька записів розділяйте комами.

Налаштуйте **дію** для виключення IDS, вибравши одну з опцій у розкривному меню (**За замовчуванням**, **Так**, **Ні**). Виконайте це для кожного типу дії (**Блокувати**, **Сповіщати**, **Реєструвати в журналі**).

✓ Якщо ви хочете, щоб у разі виключення IDS відображалось сповіщення й щоб час події реєструвався в журналі, залиште для типу дії **Блокувати** значення **За замовчуванням**, а для інших двох типів дій (**Сповіщати** й **Реєструвати в журналі**) у розкривному меню виберіть **Так**.

Підозрілу бот-мережу заблоковано

Така ситуація може виникнути, коли програма на вашому комп'ютері намагається передати шкідливий трафік на інший комп'ютер у мережі, використовуючи вразливість системи безпеки, або якщо хтось намагається сканувати порти у вашій мережі.

- Загроза: назва загрози.
- Джерело: мережева адреса джерела.
- Об'єкт: цільова мережева адреса.

• Припинити блокування: створення правила IDS для можливої загрози з параметрами, що дають змогу обмінюватися даними.

• Продовжувати блокування: блокування виявленої загрози. 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. Щоб дізнатися більше про загрози й інші пов'язані умови, перегляньте типи віддалених атак або типи виявлених об'єктів.

Тимчасовий чорний список IP-адрес

Переглянути список IP-адрес, визначених як джерело атак і доданих до чорного списку, що блокує підключення до них протягом певного періоду часу (до однієї години). Показує заблоковану **IP-адресу**.

Причина блокування

Показує тип атаки, яку було попереджено із цієї адреси (наприклад, атака із використанням сканування портів TCP).

Час очікування

Показує час і дату завершення терміну дії адреси із чорного списку.

Видалити / видалити все

Видаляє вибрану IP-адресу з тимчасового чорного списку, перш ніж його термін дії мине, або негайно видаляє всі адреси із чорного списку.

Додати винятки

Додає виключення брандмауера у фільтрування IDS для вибраної IP-адреси.

Захист від атак повним перебором

Захист від атак повним перебором блокує атаки, які передбачають вгадування пароля для служб RDP та SMB. Атака повним перебором — це метод добору потрібного пароля через систематичний перебір усіх можливих комбінацій букв, цифр і символів.

• **Увімкнути захист від атак повним перебором** – ESET Mail Security перевіряє вміст мережевого трафіку й блокує спроби атак, які передбачають вгадування пароля.

• Правила – створення, редагування й перегляд правил для вхідних і вихідних мережевих з'єднань.

• Виключення – список виключених виявлених об'єктів, заданих за допомогою IP-адреси або шляхом програми. Створювати й редагувати виключення можна у веб-консолі ESET PROTECT.

Правила захисту від атак повним перебором

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

Натисніть **Додати**, щоб створити правило захисту від атак повним підбором, або виберіть **Змінити**, щоб змінити вибрані записи.

У цьому вікні можна переглянути наявні правила захисту від атак повним перебором.

Назва	Визначена користувачем або автоматично вибрана назва правила.
Увімкнено	Вимкніть цей перемикач, щоб зберегти правило в списку, але не використовувати його.
Дія	Правило визначає дію ("Дозволити" чи "Заборонити"), яку потрібно виконати за певних умов.
Протокол	Протокол зв'язку, який перевірятиметься цим правилом.
Профіль	Для певних профілів можна задати й застосувати спеціальні правила.
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. За замовчуванням для підрахунку кількості спроб використовується період часу 30 хвилин.
IP-адреса джерела	Список IP-адрес, діапазонів або підмереж. Кілька адрес потрібно розділяти комами.
Зони джерел	Дає змогу додати попередньо визначену або створену зону з діапазоном IP-адрес. Для цього потрібно клацнути "Додати".

Винятки в захисті від атак повним перебором

Винятки в захисті від атак методом повного підбору можуть використовуватися, щоб уникнути виявлення таких атак за певних умов. Ці винятки створюються в ESET PROTECT на основі виявлених випадків атак методом повного підбору. Винятки в захисті від атак повним перебором відображатимуться, якщо адміністратор створив їх у веб-консолі ESET PROTECT. Винятки можуть містити лише правила дозволів та аналізуються перед правилами IDS.

- **Виявлений об’єкт** – тип виявлених об’єктів.

- **Програма** – виберіть шлях до файлу програми, що виключається, натиснувши "..." (наприклад, *C:\Program Files\Firefox\Firefox.exe*). Не вводьте ім’я програми.

- **Віддалена IP-адреса** – список віддалених IPv4- або IPv6-адрес, діапазонів або підмереж. Кілька адрес потрібно розділяти комами.

Інтернет і електронна пошта

Щоб захистити сервер під час інтернет-з'єднання, можна налаштувати фільтрацію протоколів, захист поштового клієнта, захист доступу до інтернету й захист від фішинг-атак.

Захист поштового клієнта

Контролює весь обмін даними електронною поштою, захищає від шкідливого коду й дає змогу вибрати дії, які потрібно виконати в разі виявлення зараження.

Захист доступу до Інтернету

Відстежує обмін даними між веб-браузерами й віддаленими серверами та забезпечує відповідність правилам протоколів HTTP та HTTPS. Ця функція також дає змогу блокувати, дозволяти або виключати певні URL-адреси.

Фільтрація протоколів

Пропонує розширений захист протоколів програм, який надає ядро сканування ThreatSense. Ця функція працює автоматично незалежно від того, використовується веб-браузер чи поштовий клієнт. Вона також працює для зашифрованих з'єднань (SSL/TLS).

Захист від фішинг-атак

Дозволяє блокувати відомі веб-сторінки, через які розповсюджується фішинговий вміст.

Фільтрація протоколів

Захист протоколів від шкідливих програм забезпечує ядро сканування ThreatSense, у якому поєднано кілька сучасних методів виявлення шкідливого програмного забезпечення. Модуль фільтрації протоколів працює автоматично, незалежно від веб-браузера й поштового клієнта. Якщо фільтрацію протоколів увімкнено, ESET Mail Security перевірятиме з'єднання, що використовують протокол SSL або TLS. Виберіть **Інтернет та електронна пошта** > SSL/TLS.

Увімкнути фільтрацію вмісту програмних протоколів

Зверніть увагу, що від функції фільтрації протоколів залежать багато компонентів ESET Mail Security (захист доступу до Інтернету, захист протоколів електронної пошти й захист від фішинг-атак). Тому в разі вимкнення модуля фільтрації протоколів не всі їхні функції будуть доступні.

Виключені програми

Щоб виключити з'єднання певних мережевих програм із процесу фільтрації вмісту, виберіть їх у списку. Обмін даними за протоколом HTTP/POP3 для вибраних програм не перевірятиметься на наявність загроз. Це дає змогу виключити певні програми з фільтрації протоколів. Натисніть **Змінити** й **Додати**, щоб вибрати виконуваний файл зі списку програм і виключити його з фільтрації протоколів.

Рекомендовано використовувати цю опцію лише для тих програм, які працюють некоректно під час перевірки їхнього з'єднання.

Виключені IP-адреси

Дозволяє виключити певні віддалені адреси з фільтрації протоколів. IP-адреси зі списку буде виключено з фільтрування вмісту протоколу. Обмін даними за протоколом HTTP/POP3/IMAP між вибраними адресами не перевірятиметься на наявність загроз.

Рекомендовано використовувати цю опцію лише для довірених адрес.

Натисніть **Змінити** й **Додати**, щоб вказати IP-адреси, діапазон адрес або підмережу для застосування до них правила виключення. Якщо вибрано **Введіть кілька значень**, ви можете додати кілька IP-адрес, розділених новими рядками, комами або крапками з комами. Якщо увімкнено множинний вибір, адреси будуть відображатися у списку виключених IP-адрес.

Виключення можуть знадобитися, коли фільтрація протоколів спричиняє проблеми із сумісністю.

Інтернет і поштові клієнти

Через велику кількість зловмисного коду, що циркулює в Інтернеті, дуже важливим аспектом захисту комп'ютера є безпечний перегляд веб-сторінок. Уразливості веб-браузера й посилання на шахрайські програми допомагають зловмисному коду потрапити в систему непомічено, ось чому ESET Mail Security приділяє особливу увагу безпеці веб-браузера. Будь-яку програму, яка має доступ до мережі, можна позначити як веб-браузер. Програми, які вже використовують певні протоколи для обміну даними, або програми з вибраних шляхів можна додати до списку веб- і поштових клієнтів.

SSL/TLS

ESET Mail Security може перевіряти на наявність загроз з'єднання, у яких використовуються протоколи Secure Sockets Layer (SSL) / Transport Layer Security (TLS).

Можна використовувати різні режими сканування захищених SSL-з'єднань з довіреними сертифікатами, невідомими сертифікатами або сертифікатами, виключеними з перевірки захищених SSL-з'єднань.

Увімкнути фільтрацію протоколу SSL/TLS

Якщо фільтрацію протоколів вимкнено, програма не сканuватиме з'єднання SSL/TLS. Режим фільтрації протоколів Secure Sockets Layer (SSL) / Transport Layer Security (TLS) доступний у наведених нижче випадках.

- **Автоматичний режим**: виберіть цей варіант, щоб сканувати всі захищені SSL/TLS-з'єднання за винятком тих, які захищено сертифікатами, виключеними з перевірки. Якщо встановлюється нове з'єднання, яке використовує невідомий підписаний сертифікат, користувач не отримає повідомлення, а саме з'єднання автоматично фільтруватиметься. Під час доступу до сервера з ненадійним сертифікатом, який користувач позначив як довірений (доданий до списку довірених сертифікатів), з'єднання із цим сервером дозволяється, а вміст з'єднання фільтрується.

• **Інтерактивний режим**: під час переходу на новий захищений протоколами SSL/TLS сайт (з невідомим сертифікатом) на екран виводиться діалогове вікно вибору дій. Цей режим дозволяє створювати список сертифікатів SSL/TLS, які будуть виключені зі сканування.

• **Режим політики**: фільтруються всі з'єднання SSL/TLS за винятком налаштованих виключень.

Список програм, до яких застосовуються фільтри SSL/TLS

Дає змогу додавати програми, до яких застосовуються фільтри, і встановлювати одну з дій сканування. Список програм, до яких застосовуються фільтри SSL/TLS, можна використовувати, щоб налаштувати поведінку ESET Mail Security відносно окремих програм і запам'ятати дії, вибрані, якщо в **режимі фільтрації протоколів TCP/TLS** вибрано **Інтерактивний режим**.

Список відомих сертифікатів

Налаштування поведінки ESET Mail Security відносно певних сертифікатів SSL. Список можна переглянути й керувати ним, натиснувши Змінити поруч із елементом **Список відомих сертифікатів**.

Виключити зв'язок із довіреними доменами

Виключення з'єднань з перевірки протоколів (інтернет-банкінг) за допомогою розширених сертифікатів перевірки.

Блокувати зашифрований зв'язок, що використовує застарілий протокол SSL v2

З'єднання за допомогою цієї попередньої версії протоколу SSL буде автоматично заблоковано.

Кореневий сертифікат

Для нормальної роботи SSL/TLS-з'єднань у браузерах і поштових клієнтах необхідно додати кореневий сертифікат ESET до списку відомих кореневих сертифікатів (видавців). Параметр додавання кореневого сертифіката до відомих браузерів має бути активовано.

Виберіть цю опцію, щоб автоматично додавати кореневий сертифікат ESET у відомі браузери (наприклад, Opera та Firefox). Для браузерів, які використовують системне сховище сертифікатів (наприклад, Internet Explorer), сертифікат додається автоматично.

Щоб застосувати сертифікат у непідтримуваних браузерах, виберіть пункт **Переглянути сертифікат** > **Деталі** > **Копіювати до файлу**, а потім імпортуйте його в браузер вручну.

Дійсність сертифікатів

Якщо сертифікат не вдається перевірити за допомогою сховища сертифікатів TRCA

У деяких випадках сертифікат неможливо перевірити за допомогою сховища **довірених кореневих центрів сертифікації**. Це означає, що сертифікат уже підписаний (наприклад, адміністратором веб-сервера або невеликої компанії) й ухвалення рішення про вибір такого сертифіката як довіреного не завжди становить небезпеку. Більшість великих компаній (наприклад, банки) використовують сертифікати, підписані сховищем довірених кореневих центрів сертифікації.

Якщо встановлено прапорець **Запитувати термін дії сертифіката** (за замовчуванням), користувачеві буде запропоновано вибрати дію, яку слід виконати під час установлення зашифрованого з'єднання. Можна вибрати опцію **Блокувати з'єднання, які використовують цей сертифікат**, щоб завжди розривати зашифровані з'єднання із сайтами, які використовують неперевірені сертифікати.

Якщо сертифікат недійсний або пошкоджений

Це означає, що термін дії сертифіката закінчився, або використовується неприпустимий підпис. У цьому разі рекомендовано вибрати елемент **Блокувати з'єднання, які використовують цей сертифікат**.

Список відомих сертифікатів

Існує можливість налаштовувати поведінку ESET Mail Security відносно певних сертифікатів Secure Sockets Layer (SSL) / Transport Layer Security (TLS) і запам'ятовувати задані дії, якщо в режимі фільтрації протоколів SSL/TLS вибрано **Інтерактивний режим**. Можна налаштувати вибраний сертифікат, або ж **додати** сертифікат із URL-адреси або файлу.

Після відкриття вікна **Додати сертифікат** натисніть **URL-адреса** або **Файл** і вкажіть URL-адресу сертифіката або знайдіть файл сертифіката. На основі даних цього сертифіката автоматично заповнюються нижченаведені поля.

- **Ім'я сертифіката** – власне ім'я сертифіката.
- **Видавець сертифіката** – ім'я автора сертифіката.
- **Суб'єкт сертифіката** – у цьому полі можна вказати організацію, якій належить відкритий ключ, що міститься в полі відкритого ключа суб'єкта.

Доступ

- **Автоматично** – дозволити довірені сертифікати й запитувати про дії щодо ненадійних.
- **Дозволити або заблокувати** – дозволяти або блокувати з'єднання, захищені цим сертифікатом незалежно від його надійності.
- **Запитувати** – запитувати в разі виявлення певного сертифіката.

Перевірка

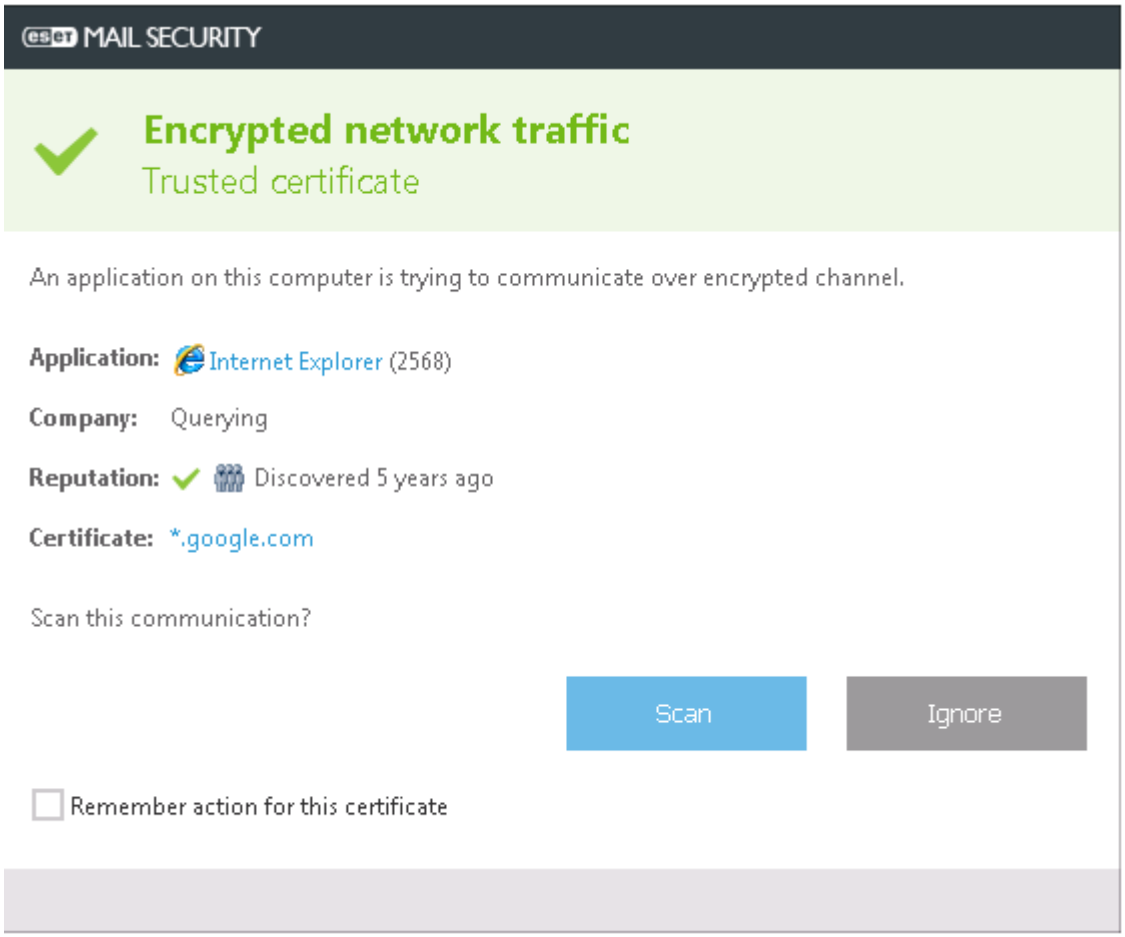
- **Автоматично** – сканування в автоматичному режимі й запитування в інтерактивному режимі.
- **Сканувати або пропустити** – сканувати або ігнорувати з'єднання, захищене цим сертифікатом.
- **Запитувати** – запитувати в разі виявлення певного сертифіката.

Зашифрований SSL-зв’язок

Якщо систему налаштовано на використання сканування протоколу SSL, у двох ситуаціях відображатиметься діалогове вікно з пропозицією вибрати дію.

По-перше, якщо веб-сайт використовує невизначений або недійсний сертифікат, а ESET Mail Security налаштовано на запит користувача, у таких випадках (за замовчуванням "так" – для неперевірених сертифікатів, "ні" – для недійсних), з’явиться діалогове вікно із запитом **Дозволити** або **Блокувати підключення**.

По-друге, якщо вибрано **інтерактивний** режим **фільтрації протоколу SSL**, для кожного веб-сайту відображатиметься діалогове вікно із запитом про **сканування** чи **ігнорування** трафіку. Деякі програми перевіряють, щоб їхній SSL-трафік ніхто не змінював і не перевіряв; у таких випадках ESET Mail Security має **ігнорувати** цей трафік, щоб програма продовжувала працювати.



В обох випадках користувач може запам’ятати вибрану дію. Збережені дії зберігаються в списку відомих сертифікатів.

Захист поштового клієнта

Інтеграція ESET Mail Security з поштовими клієнтами збільшує рівень активного захисту від шкідливого коду в повідомленнях електронної пошти. Якщо поштовий клієнт підтримується, можна налаштувати його інтеграцію в ESET Mail Security. Якщо інтеграцію активовано, панель інструментів ESET Mail Security вставляється безпосередньо в поштовий клієнт, забезпечуючи

ефективніший захист електронної пошти (панель інструментів для останніх версій Windows Live Mail не вставляється).

Інтеграція з поштовими клієнтами

Наразі підтримуються такі клієнти електронної пошти: Microsoft Outlook, Outlook Express, Windows Mail і Windows Live Mail. Захист електронної пошти реалізовано в цих програмах як плагін. Головна перевага плагіна полягає в тому, що він не залежить від протоколу, який використовується. Коли поштовий клієнт отримує зашифроване повідомлення, воно розшифровується й надсилається до антивірусного сканера. Навіть якщо інтеграцію вимкнено, поштові клієнти залишаються захищеними відповідним модулем (для протоколів POP3, IMAP).

Повний список підтримуваних поштових клієнтів і їхніх версій див. у цій статті бази знань.

Не перевіряти під час зміни вмісту поштової скриньки

Якщо під час роботи з поштовим клієнтом робота системи вповільнюється, скористайтеся цим параметром (тільки для MS Outlook). Це може статися, наприклад, під час отримання електронної пошти з Kerio Outlook Connector Store.

Увімкнути захист електронної пошти за допомогою плагінів клієнта

Дає змогу вимкнути захист поштового клієнта без видалення інтеграції із цим клієнтом. Можна вимкнути всі плагіни відразу або ж вибірково вимкнути плагіни, перелічені нижче.

- **Отримані листи**: вмикає або вимикає перевірку вхідних електронних листів.
- **Відправлені листи**: вмикає або вимикає перевірку надісланих електронних листів.
- **Прочитані листи**: вмикає або вимикає перевірку прочитаних електронних листів.

Дія, яку потрібно виконати з інфікованим електронним листом

- **Пропустити**: якщо цей параметр увімкнуто, програма виявлятиме інфіковані вкладення, але не виконуватиме жодних дій з електронними листами.
- **Видалити лист**: програма сповіщатиме користувача про інфікування й видалятиме електронний лист.
- **Перемістити лист до папки "Видалені"**: інфіковані електронні листи будуть автоматично переміщатися в папку "Видалені".
- **Перемістити лист до папки**: інфіковані електронні листи будуть автоматично переміщатися у вказану папку.
- **Папка**: укажіть спеціальну папку, куди потрібно переміщувати інфіковані електронні листи.

Повторити перевірку після оновлення

Вмикає або вимикає повторне сканування після оновлення обробника виявлення.

Прийняти результати сканування іншими модулями

Якщо вибрано цей параметр, модуль захисту електронної пошти прийматиме результати сканування іншими модулями захисту (сканування даних, отриманих за допомогою протоколів POP3, IMAP).

Протоколи електронної пошти

Увімкнути захист електронної пошти за допомогою фільтрації протоколів

IMAP і POP3 – це найпоширеніші протоколи, які використовуються програмами поштових клієнтів для роботи з електронною поштою. ESET Mail Security забезпечує захист цих протоколів незалежно від поштового клієнта, який використовується.

ESET Mail Security також підтримує сканування даних, отриманих із використанням протоколів IMAPS і POP3S, які для передання інформації між сервером та клієнтом використовують зашифрований канал. ESET Mail Security перевіряє з'єднання, які використовують протоколи шифрування SSL (Secure Socket Layer) і TLS (Transport Layer Security). Програма виконуватиме сканування трафіку тільки на портах, які вказано як такі, що використовують **протокол IMAPS/POP3S**, незалежно від версії операційної системи.

Налаштування сканера IMAPS/POP3S

Зашифровані з'єднання не скануватимуться, якщо використовуються параметри за замовчуванням. Щоб увімкнути сканування зашифрованих з'єднань, перейдіть до пункту Перевірка протоколів SSL/TLS.

Номер порту визначає його тип. Нижче наведено порти електронної пошти, які використовуються за замовчуванням.

Ім'я порту	Номер порту	Опис
POP3	110	Порт POP3 без шифрування, який використовується за замовчуванням.
IMAP	143	Порт IMAP без шифрування, який використовується за замовчуванням.
Secure IMAP (IMAP4-SSL)	585	Увімкнути фільтрацію протоколу SSL/TLS. Номери портів необхідно розділяти комами.
IMAP4 over SSL (IMAPS)	993	Увімкнути фільтрацію протоколу SSL/TLS. Номери портів необхідно розділяти комами.
Secure POP3 (SSL-POP)	995	Увімкнути фільтрацію протоколу SSL/TLS. Номери портів необхідно розділяти комами.

Теги електронної пошти

Захист електронної пошти забезпечує контроль повідомлень електронної пошти, отриманих через протоколи POP3 й IMAP. За допомогою плагіна для Microsoft Outlook та інших поштових клієнтів ESET Mail Security може контролювати всі повідомлення поштового клієнта (POP3, MAPI, IMAP, HTTP).

Під час перевірки вхідних повідомлень програма використовує всі методи розширеного

сканування, включені в ядро сканування ThreatSense. Це означає, що виявлення шкідливих програм відбувається ще до зіставлення з базою даних виявлення вірусів. Сканування повідомлень за протоколами POP3 й IMAP не залежить від наявного поштового клієнта.

Після перевірки електронного листа до нього може додаватися сповіщення з результатом сканування. Можна вибрати параметр **Додавати повідомлення-ознаку до отриманих і прочитаних електронних листів** або **Додавати повідомлення-ознаку до відправлених електронних листів**.

Пам'ятайте, що в поодиноких випадках повідомлення-позначки можуть бути пропущені в проблемних HTML-повідомленнях або повідомленнях, уражених шкідливим програмним забезпеченням. Повідомлення-позначки можуть додаватися до отриманих і прочитаних електронних листів, надісланих електронних листів або в обох випадках.

Доступні вказані нижче опції:

- **Ніколи**: повідомлення-позначки взагалі не додаватимуться.
- **Коли з'являється виявлений об'єкт**: перевіреними позначатимуться лише повідомлення, які містять шкідливе програмне забезпечення (використовується за замовчуванням).
- **До усіх перевірених електронних листів**: програма додаватиме повідомлення до всіх просканованих електронних листів.

Текст для додавання до теми виявленого повідомлення електронної пошти

Відредагувавши цей шаблон, ви можете змінити формат префікса теми інфікованого електронного листа. Ця функція замінить формат теми повідомлення `Hello` на такий: `"[detection %DETECTIONNAME%] Hello`. Змінна `%DETECTIONNAME%` представляє виявлений об'єкт.

Панель інструментів Microsoft Outlook

Захист Microsoft Outlook працює як компонент плагіна. Після інсталяції ESET Mail Security панель інструментів із параметрами захисту від шкідливого програмного забезпечення додається в Microsoft Outlook.

ESET Mail Security

Клацніть піктограму, щоб відкрити головне вікно програми ESET Mail Security.

Повторна перевірка повідомлень

Дає змогу вручну запустити перевірку електронної пошти. Ви можете вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Щоб дізнатися більше, перегляньте інформацію про захист поштового клієнта.

Параметри сканера

Відображає параметри захисту поштового клієнта.

Панель інструментів Outlook Express і Windows Mail

Захист Outlook Express і Windows Mail працює як модуль плагіна. Після інсталяції ESET Mail Security панель інструментів із параметрами захисту від шкідливого програмного забезпечення додається в Outlook Express або Windows Mail.

ESET Mail Security

Клацніть піктограму, щоб відкрити головне вікно програми ESET Mail Security.

Повторна перевірка повідомлень

Дає змогу вручну запустити перевірку електронної пошти. Ви можете вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Щоб дізнатися більше, перегляньте інформацію про захист поштового клієнта.

Параметри сканера

Відображає параметри захисту поштового клієнта.

Настройка вигляду

Вигляд панелі інструментів для поштового клієнта можна змінити. Зніміть цей прапорець, щоб налаштувати вигляд незалежно від параметрів програми електронної пошти.

- **Показувати текст**: відображає опис піктограм.
- **Текст праворуч**: описи параметрів переміщуються знизу в праву сторону піктограм.
- **Великі піктограми**: відображаються великі піктограми для опцій меню.

Діалогове вікно підтвердження

Це сповіщення слугує для перевірки того, що користувач справді хоче виконати вибрану дію, що має виключити можливі помилки. У цьому діалоговому вікні також можна вимкнути підтвердження.

Повторна перевірка повідомлень

Панель інструментів ESET Mail Security, інтегрована в поштові клієнти, дає користувачам змогу вказати кілька варіантів перевірки електронної пошти. Опція **Повторне сканування повідомлень** пропонує два режими сканування:

- **Усі повідомлення в поточній папці**: сканування повідомлень у поточній папці, що відображається.
- **Лише вибрані повідомлення**: сканування лише повідомлень, позначених користувачем.

• **Повторне сканування вже просканованих повідомлень**: дає користувачу змогу запустити інше сканування повідомлень, які вже було просканово раніше.

Захист доступу до Інтернету

Захист доступу до Інтернету здійснюється за допомогою контролю зв'язків між веб-браузерами й віддаленими серверами для захисту від онлайн-загроз і виконання правил протоколів HTTP (протокол передавання гіпертексту) і HTTPS (зашифрований зв'язок).

Доступ до відомих веб-сторінок зі шкідливим вмістом блокується до завантаження вмісту. Якщо виявлено шкідливий вміст, ядро сканування ThreatSense перевіряє всі інші веб-сторінки під час завантаження та блокує їх. Захист доступу до Інтернету забезпечує два рівні захисту, блокування за чорним списоком і блокування за вмістом.

Основна

Наполегливо рекомендуємо не вимикати функцію **захисту доступу до Інтернету**. Доступ до цієї опції також можна отримати з головного вікна програми ESET Mail Security. Для цього перейдіть у меню **Налаштування** > **Інтернет та електронна пошта** > **Захист доступу до Інтернету**.

Увімкнути розширену перевірку сценаріїв браузера
За замовчуванням усі програми JavaScript, що їх виконують веб-браузери, перевірятиме ядро виявлення.

Веб-протоколи

Дає змогу налаштувати моніторинг для стандартних протоколів, які використовує більшість веб-браузерів. За замовчуванням у ESET Mail Security налаштовано відстеження протоколу HTTP, який використовує більшість веб-браузерів.
ESET Mail Security також підтримує перевірку протоколу HTTPS. Підключення HTTPS використовує зашифрований канал для передання інформації між сервером і клієнтом. ESET Mail Security перевіряє зв'язок, що підтримує протоколи SSL і протоколи Transport Layer Security (TLS). Програма виконуватиме сканування трафіку тільки на портах, які вказано як такі, що використовують **протокол HTTPS**, незалежно від версії операційної системи.
Зашифрований зв'язок не перевірятимуть, коли використовуються параметри за замовчуванням. Щоб увімкнути сканування зашифрованих з'єднань, перейдіть до пункту **Додаткові параметри** (**F5**) > **Інтернет та електронна пошта** > SSL/TLS.

ThreatSense параметри

Налаштуйте параметри, зокрема типи сканування (електронна пошта, архіви, виключення, обмеження тощо) і методи виявлення для захисту доступу до Інтернету.

Управління URL-адресами

Управління URL-адресами дає змогу вказувати HTTP-адреси для блокування, дозволу або виключення з перевірки. Веб-сайти зі списку заблокованих адрес будуть недоступні, якщо їх також не додано до списку дозволених адрес. Веб-сайти зі списку адрес, виключених із перевірки, під час доступу до них не скануватимуться на наявність шкідливого коду. Для фільтрації адрес HTTPS додатково до веб-сторінок HTTP необхідно увімкнути фільтрацію протоколів SSL/TLS. В іншому разі додаватимуться лише домени відвіданих сайтів HTTPS, а не повна URL-адреса.

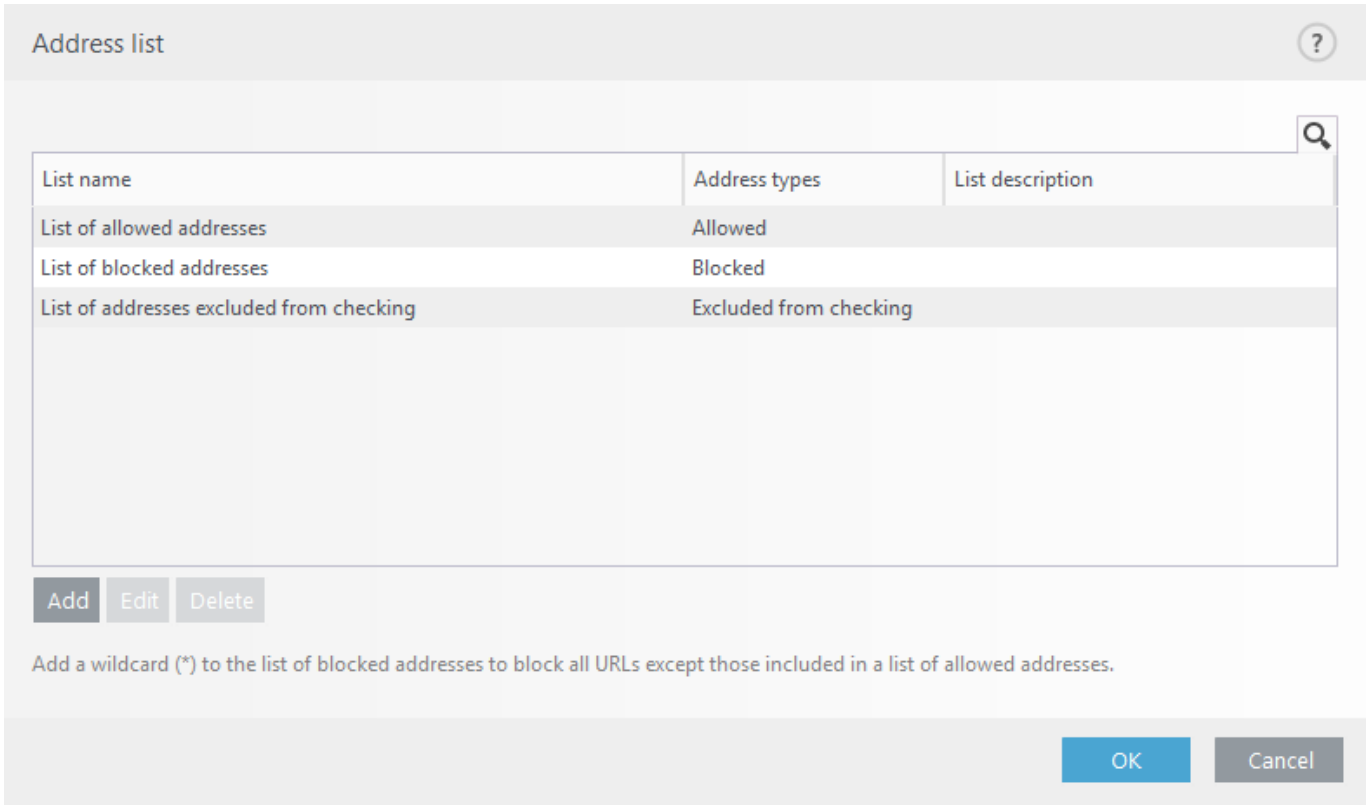
Один список заблокованих адрес може містити адреси, отримані з певного зовнішнього загальнодоступного чорного списку, а другий – бути вашим власним чорним списком. Таким чином зовнішній список можна легко оновлювати без внесення змін до вашого списку.

Щоб створити новий список адрес додатково до попередньо визначених, натисніть **Змінити** й **Додати**. Це може бути корисно, якщо потрібно логічно розділити різні групи адрес. За замовчуванням доступні три нижченаведені списки.

• **Список адрес, виключених із перевірки**: для будь-якої адреси, доданої до цього списку, перевірка на наявність шкідливого коду не виконуватиметься.

• **Список дозволених адрес**: якщо встановлено прапорець "Надавати доступ лише до адрес HTTP зі списку дозволених адрес", а в списку заблокованих адрес вказано символ зірочки (блокувати всі адреси без винятків), користувачу буде надано доступ лише до дозволених адрес. Адреси з цього списку залишаються доступними, навіть якщо їх включено до списку заблокованих адрес.

• **Список заблокованих адрес**: користувач не зможе отримати доступ до адрес із цього списку, якщо їх не додано до списку дозволених адрес.



До списку можна **додати** нову URL-адресу. Можна також ввести кілька значень за допомогою роздільника. Натисніть **Змінити**, щоб змінити наявну адресу в списку, або **Видалити**, щоб видалити її. Видаляти можна лише адреси, створені за допомогою команди **Додати**, а не імпортовані.

У всіх списках можна використовувати символи "*" (зірочка) та "?" (знак питання). Зірочка означає будь-яку кількість символів, а знак питання – лише один символ. Працювати з умістом списку виключених адрес слід особливо уважно, оскільки він повинен містити тільки довірені й безпечні адреси. Так само потрібно переконатися, що символи "*" і "?" у списку використовуються правильно.

Щоб заблокувати всі HTTP-адреси, окрім доданих до активного списку дозволених адрес, додайте "*" до активного списку заблокованих адрес.

Створити новий список

У списку відображатимуться потрібні URL-адреси/маски домену, які будуть заблоковані, дозволені або виключені з перевірки. Під час створення нового списку вкажіть такі параметри:

• **Тип списку адрес**: виберіть тип із розкривного списку ("Виключено з перевірки", "Заблоковано" або "Дозволено").

• **Назва списку**: укажіть назву списку. Це поле буде недоступним під час редагування одного з трьох попередньо визначених списків.

• **Опис списку**: введіть короткий опис списку (необов'язково). Буде недоступним під час редагування одного з трьох попередньо визначених списків.

• **Список активний**: використовуйте перемикач, щоб деактивувати список. Ви можете активувати його пізніше за необхідності.

• **Сповіщати про застосування**: якщо ви хочете отримувати сповіщення, коли певний список використовується під час оцінки відвіданого сайту HTTP/HTTPS. Сповіщення надходитимуть, якщо веб-сайт заблоковано або дозволено, оскільки його включено до списку заблокованих або дозволених адрес. Сповіщення міститиме назву списку з указаним веб-сайтом.

• **Рівень серйозності**: виберіть із розкривного списку рівень серйозності журналювання ("Немає", "Діагностика", "Інформація" або "Попередження"). Записи з попередженням може збирати ESET PROTECT.

ESET Mail Security дає змогу користувачу блокувати доступ до вказаних веб-сайтів та унеможливити відображення їх вмісту у веб-браузері. Крім того, це дає змогу користувачу вказати адреси, які слід виключити з перевірки. Якщо повне ім'я віддаленого сервера невідоме або користувач хоче вказати всю групу віддалених серверів, так звані маски можна використовувати для ідентифікації такої групи.

Маски містять символи ? та *:

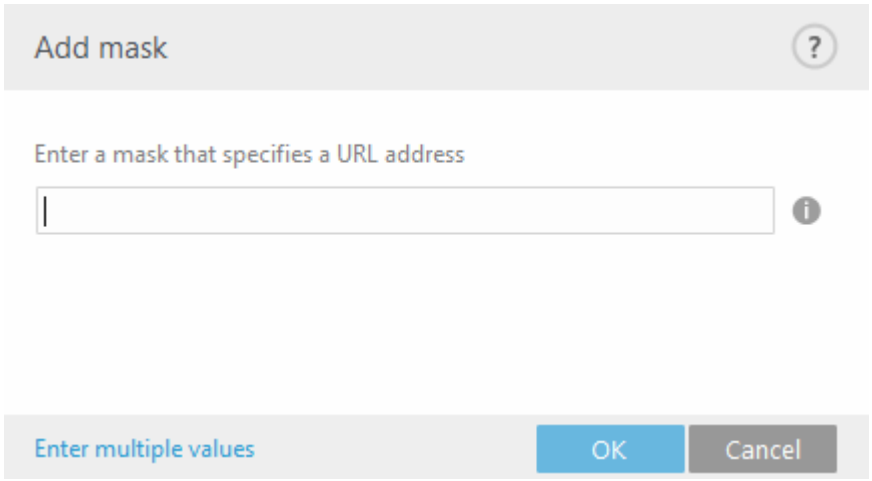
• Використайте ?, щоб замінити символ.

• Використайте ?, щоб замінити текстовий рядок.

.c?m застосовується до всіх адрес, остання частина яких починається літерою c, закінчується літерою m і містить невідомий символ (.com*, *.cam* тощо).

"*" на початку. Послідовність використовується спеціально на початку доменного імені. У такому разі груповий символ "*" не може представляти скісну риску ("/"). Щоб уникнути обходу маски, наприклад маска *.domain.com не збігається з *https://anydomain.com/anypath#.domain.com* (такий суфікс можна додати до будь-якої URL-адреси без впливу на завантаження). І по-друге, *. у цьому випадку також збігається з порожнім рядком. Це необхідно, щоб він міг збігатися з усім доменом, включно з будь-яким дочірнім доменом за допомогою однієї маски. Наприклад,

маска *.domain.com відповідає *https://domain.com*. Використання *domain.com буде неправильним, оскільки назва також збігається з https://anotherdomain.com.



Введіть кілька значень

Додайте кілька URL-адрес, розділених новими рядками, комами або крапкою з комою. Якщо увімкнено множинний вибір, адреси будуть відображатися у списку.

Імпортувати

Текстовий файл з URL-адресами для імпорту (окремі значення з розривом рядка, наприклад, `*.txt` з використанням кодування UTF-8).

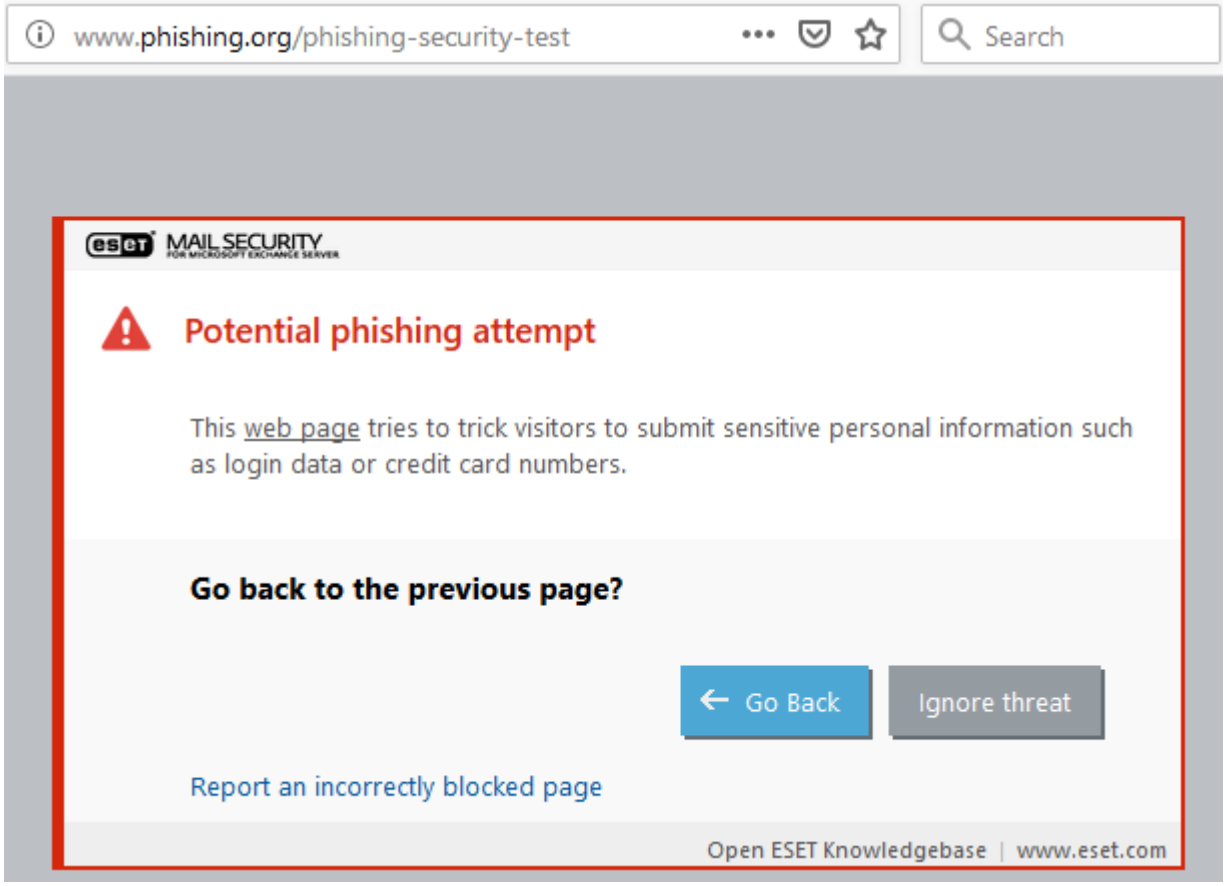
Веб-захист від фішинг-атак

Терміном фішинг називається злочинна діяльність із використанням соціотехнік (маніпулювання користувачами для отримання конфіденційної інформації). Зазвичай мета фішингу – отримати доступ до конфіденційних даних, як-от номери банківських рахунків, PIN-коди тощо.

ESET Mail Security містить захист від фішинг-атак, що блокує веб-сторінки, про які відомо, що вони розповсюджують цей тип вмісту. Наполегливо рекомендуємо ввімкнути захист від фішинг-атак у ESET Mail Security. Додаткову інформацію про захист ESET Mail Security від фішинг-атак див. у нашій статті бази знань.

Якщо відкрити фішинговий сайт, у веб-браузері відобразиться наведене нижче діалогове вікно.

Якщо ви все одно бажаєте отримати доступ до веб-сайту, виберіть **Ігнорувати загрозу** (не рекомендовано).



Тривалість віднесення потенційно фішингових сайтів до білого списку за замовчуванням обмежується кількома годинами. Щоб дозволити доступ до веб-сайту безстроково, скористайтеся інструментом керування URL-адресами.

Повідомити про шахрайський сайт

Якщо ви зустрінете підозрілий веб-сайт, який схожий на фішинговий або шкідливий іншим чином, про це можна повідомити ESET для аналізу. Перш ніж надсилати дані про веб-сайт до ESET, упевніться, що він відповідає одному або кільком переліченим нижче критеріям.

- Веб-сайт узагалі не виявляється.
- Веб-сайт неправильно виявляється як загроза. У цьому разі можна повідомити про помилкове віднесення сайту до категорії фішингових.

Про веб-сайт також можна повідомити електронною поштою. Надішліть електронного листа на адресу samples@eset.com. Пам'ятайте, що тема листа повинна бути інформативною. Надайте також якомога більше інформації про веб-сайт (наприклад, укажіть веб-сайт, з якого ви перейшли на цей веб-сайт тощо).

Контроль пристроїв

ESET Mail Security містить модуль автоматичного контролю пристроїв (CD- та DVD-дисків, а також USB-пристроїв). За допомогою цього модуля можна сканувати, блокувати та налаштовувати

розширені фільтри й дозволи, а також указати, чи може користувач отримувати доступ до пристрою та працювати з ним. Він може бути корисним, якщо адміністратор комп'ютера хоче запобігти використанню пристроїв із небажаним вмістом.

> Якщо ввімкнути контроль пристроїв за допомогою перемикача **Інтегрувати в систему**, функцію контролю пристроїв ESET Mail Security буде активовано. Однак щоб цю зміну було активовано, потрібно перезавантажити систему.

Контроль пристроїв активується, що дозволить редагувати їхні параметри. Якщо буде виявлено пристрій, заблокований наявним правилом, на екрані відобразиться вікно сповіщення, а доступ до пристрою буде заблоковано.

Правила

Правило контролю пристроїв визначає дію, яка буде виконуватися після підключення до комп'ютера пристрою, що відповідає критеріям такого правила.

Групи

Якщо натиснути Редагувати, групами пристроїв можна буде керувати. Створіть нову групу пристроїв або виберіть наявну, щоб додати пристрої до списку або видалити їх із нього.

> Записи журналу контролю пристроїв можна переглядати у файлах журналу.

Правила пристроїв

Можна дозволити або заблокувати певні пристрої для окремих користувачів чи груп користувачів, або ж відповідно до будь-яких із додаткових параметрів, які можна вказати в конфігурації правил. Список правил містить кілька описів для кожного правила, зокрема його ім'я, тип зовнішнього пристрою, дію, яку потрібно виконувати в разі виявлення пристрою, а також інформацію про рівень критичності для запису до журналу.

Можна **додати** нове правило або змінити параметри наявного. Щоб спростити ідентифікацію правила, введіть його опис у поле **Ім'я**. Натисніть перемикач поруч із пунктом **Правило ввімкнено**, щоб вимкнути або ввімкнути правило. Ця можливість може бути корисною, якщо потрібно зберегти правило.

Застосовувати протягом

Правила можна обмежувати за допомогою часових інтервалів. Спочатку створіть часовий інтервал, після чого він з'явиться в розкривному меню.

Тип пристрою

Виберіть тип зовнішнього пристрою в розкривному меню (дисковий накопичувач, портативний пристрій, Bluetooth, FireWire тощо). Перелік типів пристроїв надає операційна система, тому їх можна переглянути в диспетчері пристроїв системи, якщо пристрій підключено до комп'ютера. До накопичувачів належать зовнішні диски й традиційні пристрої для читання карт пам'яті, підключені через інтерфейс USB або FireWire. До пристроїв читання смарт-карт належать усі зчитувачі карт з убудованою мікросхемою, наприклад SIM-карт або карт автентифікації. Прикладами пристроїв формування зображень є сканери й камери, які не надають інформацію

про користувачів, а лише інформацію про їхні дії. Це означає, що пристрої формування зображень можна блокувати лише глобально.

Дія

Доступ до пристроїв, не призначених для зберігання даних, можна лише дозволити або заблокувати. На відміну від них, для пристроїв зберігання даних можна вибрати одне з наведених нижче прав.

- **Читання та запис** – повний доступ до пристрою.
- **Блокувати** – доступ до пристрою буде заблоковано.
- **Лише читання** – доступ до пристрою буде дозволено лише для читання.
- **Попереджати** – під час кожного підключення пристрою користувач отримає сповіщення про стан пристрою (дозволений чи заблокований), після чого буде створено запис у журналі. Пристрої не запам’ятовуються, тож сповіщення відображаються під час кожного нового підключення пристрою.

> Повний список прав (дій) доступний не для всіх пристроїв. Якщо пристрій має простір для зберігання даних, доступні всі чотири дії. Якщо пристрої не призначено для зберігання даних, доступні лише дві дії (наприклад, право **Лише читання** не застосовується до Bluetooth-пристроїв; доступ до них можна лише дозволити або заблокувати).

Тип критеріїв

За допомогою наведених нижче додаткових параметрів можна налаштовувати й змінювати правила для конкретних пристроїв. Усі параметри чутливі до регістру й підтримують групові символи (*, ?):

- **Виробник** – фільтрування за назвою або ідентифікатором виробника.
- **Модель** – назва пристрою.
- **Серійний номер** – зовнішні пристрої зазвичай мають серійні номери. У випадку CD- або DVD-дисків, це серійний номер носія, а не оптичного приводу.

> Якщо ці параметри не вказано, правило ігноруватиме ці поля під час зіставлення. Параметри фільтрації в усіх текстових полях чутливі до регістру й підтримують групові символи (знак запитання (?) позначає один символ, а зірочка (*) позначає рядок, який містить нуль або більше символів).

Щоб визначити параметри пристрою, створіть правило, що дозволяє доступ до такого типу пристроїв, підключіть пристрій до комп’ютера, а потім перегляньте відомості про пристрій у журналі контролю пристроїв.

У розкривному списку виберіть пункт **Рівень критичності**:

- **Завжди** – запис усіх подій.
- **Діагностика** – запис інформації, необхідної для налаштування програми.
- **Інформація** – запис інформаційних повідомлень, включно з повідомленнями про успішні

оновлення, а також усі зазначені вище записи.

- **Попередження** – запис про критичні помилки й попереджувальні повідомлення.
- **Немає** – ніякі журнали не створюються.

Можна обмежувати правила певними користувачами або групами, додаючи їх до списку користувачів. Натисніть **Змінити**, щоб керувати **списком користувачів**.

- **Додати** – відкриває вікно типів об’єктів: з користувачами й групами для вибору.
- **Видалити** – видаляє вибраного користувача зі списку фільтрування.

> За допомогою правил користувача можна фільтрувати всі пристрої (наприклад, пристрої формування зображення не надають інформацію про користувачів, а лише про викликані дії).

Доступні вказані нижче функції.

Змінити

Дає змогу змінити ім’я вибраного правила або параметри пристроїв, які містяться в ньому (виробник, модель, серійний номер).

Копіювати

Створює нове правило на основі параметрів вибраного правила.

Видалити

Видалення вибраного правила. Також можна скористатися прапорцем поруч із певним правилом, щоб вимкнути його. Ця можливість може бути корисною, якщо потрібно зберегти правило, щоб його можна було використовувати в майбутньому.

Заповнити

Надає огляд усіх наразі підключених пристроїв із такими відомостями: тип пристрою, виробник пристрою, модель і серійний номер (якщо доступно). Якщо вибрати пристрій (у списку виявлених пристроїв) і натиснути **ОК**, відкриється вікно редактора правил із попередньо налаштованою інформацією (усі параметри можна змінювати).

Правила наведено в порядку їхнього пріоритету: правила з вищим пріоритетом розташовуються вгорі. Можна вибрати кілька правил і застосувати до них певні дії одночасно, наприклад видалити або перемістити їх угору або вниз списком. Для цього натискайте **зверху**, **угору**, **униз**, **знизу** (кнопки зі стрілками).

Групи пристроїв

Вікно "Групи пристроїв" розділено на дві частини. У правій частині вікна міститься список пристроїв, які належать до відповідної групи, а в лівій – список наявних груп. Виберіть групу з пристроями, які потрібно відобразити на панелі справа.

Можна створювати різні групи пристроїв, до яких застосовуватимуться різні правила. Також можна створити одну групу пристроїв, для яких установлено значення **Читання** та/або **запис** або **Лише для читання**. Таким чином, модуль контролю пристроїв блокуватиме нерозпізнані пристрої в разі їхнього підключення до комп’ютера.

⚠ Підключення зовнішнього пристрою до комп’ютера може створити загрозу безпеці.

Доступні вказані нижче функції.

Додати

Створює нову групу пристроїв. Для цього введіть її ім’я або додайте пристрій до наявної групи (за потреби можна вказати відомості, як-от назва виробника, модель і серійний номер) залежно від того, де у вікні натиснуто кнопку.

Змінити

Дає змогу змінити ім’я вибраної групи або параметрів пристроїв, що містяться в ній (виробник, модель, серійний номер).

Видалити

Видаляє вибрану групу або пристрій залежно від того, де у вікні натиснуто кнопку. Також можна скористатися прапорцем поруч із певним правилом, щоб вимкнути його. Ця можливість може бути корисною, якщо потрібно зберегти правило, щоб його можна було використовувати в майбутньому.

Імпортувати

Імпортує список серійних номерів пристроїв із файлу. Кожен пристрій починається з нового рядка.

Для кожного пристрою мають бути вказані такі відомості (через кому): **виробник**, **модель** і **серійний номер**.

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

Заповнити

Надає огляд усіх наразі підключених пристроїв із такими відомостями: тип пристрою, виробник пристрою, модель і серійний номер (якщо доступно). Якщо вибрати пристрій (у списку виявлених пристроїв) і натиснути **ОК**, відкриється вікно редактора правил із попередньо налаштованою інформацією (усі параметри можна змінювати).

Додати пристрій

Клацніть "Додати" в правому вікні, щоб додати пристрій у наявну групу. За допомогою наведених нижче додаткових параметрів можна гнучко налаштувати правила для різних пристроїв. Усі параметри чутливі до регістру й підтримують групові символи (*, ?):

- **Виробник**: фільтрування за назвою або ідентифікатором виробника.

• **Модель**: назва пристрою.

• **Серійний номер**: зовнішні пристрої зазвичай мають власні серійні номери. У випадку CD- або DVD-дисків, це серійний номер носія, а не оптичного приводу.

• **Опис**: опис пристрою як додаткові відомості про нього.

Якщо ці параметри не вказано, правило ігноруватиме ці поля під час зіставлення. Параметри фільтрації в усіх текстових полях чутливі до регістру й підтримують групові символи (знак запитання (?) позначає один символ, а зірочка (*) позначає рядок, який містить нуль або більше символів).

Після створення групи пристроїв необхідно додати нове правило контролю пристроїв для створеної групи пристроїв і вибрати дію, яку потрібно виконати.

Завершивши налаштування, натисніть **ОК**. Натисніть **Скасувати**, щоб вийти з вікна **Групи пристроїв** без збереження змін.

Повний список прав (дій) доступний не для всіх пристроїв. Якщо пристрій має простір для зберігання даних, доступні всі чотири дії. Якщо пристрої не призначено для зберігання даних, доступні лише дві дії (наприклад, право "Лише читання" не застосовується до Bluetooth-пристроїв; доступ до них можна лише дозволити або заблокувати).

Конфігурація інструментів

Можна налаштувати додаткові параметри для нижченаведених інструментів.

- Часові проміжки
- Microsoft Windows® Update
- ESET CMD
- ESET RMM
- Ліцензія
- Постачальник WMI
- Об’єкти сканування консолі керування ESET
- Файли журналу
- Проксі-сервер
- Режим презентації
- Діагностичні дані
- Кластер

Часові проміжки

У правилах контролю пристроїв використовуються часові проміжки, що обмежують застосування цих правил. Створіть часовий проміжок і виберіть його під час додавання нових або зміни наявних правил (параметр **Застосовувати під час**). Це дасть змогу визначити часто використовувані часові проміжки (робочий час, вихідні дні тощо) і легко використовувати їх, не уточнюючи діапазони часу для кожного правила. Часовий проміжок слід застосовувати до будь-якого відповідного типу правил, що підтримує контроль на основі часу.

Microsoft Windows® Update

Оновлення Windows надають важливі виправлення потенційно небезпечних вразливостей і поліпшують загальний рівень безпеки комп'ютера. Тому важливо інсталювати оновлення Microsoft Windows, щойно вони з'являться. ESET Mail Security повідомлятиме про відсутні оновлення згідно з вибраним рівнем сповіщення. Доступні наведені нижче рівні.

- **Жодних оновлень**: жодні оновлення системи не пропонуватимуться для завантаження.
- **Необов'язкові оновлення**: оновлення з низьким і високим пріоритетом будуть пропонуватися для завантаження.
- **Рекомендовані оновлення**: оновлення зі звичайним і високим пріоритетом будуть пропонуватися для завантаження.
- **Важливі оновлення**: важливі оновлення та оновлення з високим пріоритетом будуть пропонуватися для завантаження.
- **Критичні оновлення**: для завантаження пропонуватиуються лише критичні оновлення.

Натисніть **ОК**, щоб зберегти зміни. Вікно "Оновлення системи" відобразиться після перевірки стану на сервері оновлень. Інформація про оновлення системи може бути доступна не відразу після збереження змін.

Сканер командного рядку

Окрім eShell, сканер за вимогою можна ESET Mail Security запускати за допомогою командного рядка, ввівши `ecls.exe`. Ця програма міститься в папці інсталяції.

Нижче наведено список параметрів і ключів.

Параметри:

`/base-dir=FOLDER`	завантажити модулі з ПАПКИ
`/quar-dir=FOLDER`	ПАПКА карантину
`/exclude=MASK`	виключити МАСКУ відповідності файлів із перевірки
`/subdir`	перевіряти підпапки (за замовчуванням)
`/no-subdir`	не перевіряти підпапки

/max-subdir-level=LEVEL	максимальний підрівень папок, вкладених у папки для перевірки
/symlink	дотримуватись символьних посилань (за замовчуванням)
/no-symlink	пропускати символьні посилання
/ads	перевіряти ADS (за замовчуванням)
/no-ads	не перевіряти ADS
/log-file=FILE	вивід з журналу у ФАЙЛ
/log-rewrite	Перезаписувати вихідний файл (за замовчуванням - дозаписувати)
/log-console	виводити журнал на консоль (за замовчуванням)
/no-log-console	не виводити журнал на консоль
/log-all	також реєструвати чисті файли
/no-log-all	не реєструвати чисті файли (за замовчуванням)
/aind	показати індикатор активності
/auto	Сканування всіх локальних дисків та автоматична очистка інфекций

Параметри сканеру:

/files	перевіряти файли (за замовчуванням)
/no-files	не перевіряти файли
/memory	перевірка пам'яті
/boots	перевіряти завантажувальні сектори
/no-boots	не перевіряти завантажувальні сектори (за замовчуванням)
/arch	перевіряти архіви (за замовчуванням)
/no-arch	не перевіряти архіви
/max-obj-size=SIZE	перевіряти лише файли, розмір яких не перевищує SIZE мегабайт (за промовчанням 0 = необмежено)
/max-arch-level=LEVEL	максимальний підрівень архівів в архівах (вкладених архівів) для перевірки
/scan-timeout=LIMIT	перевіряти архіви не довше LIMIT секунд
/max-arch-size=SIZE	перевіряти тільки файли в архівах, розмір яких не перевищує SIZE (за промовчанням 0 = необмежено)
/max-sfx-size=SIZE	перевіряти лише файли в саморозпакувальних архівах, якщо їх розмір не перевищує SIZE мегабайт (за промовчанням 0 = необмежено)
/mail	перевіряти файли електронної пошти (за замовчуванням)
/no-mail	не перевіряти файли електронної пошти
/mailbox	перевіряти поштові скриньки (за замовчуванням)
/no-mailbox	не сканувати поштові скриньки
/sfx	перевіряти саморозпакувальні архіви (за замовчуванням)
/no-sfx	не перевіряти саморозпаковувані архіви
/rtp	перевіряти упаковані програми (за замовчуванням)
/no-rtp	не перевіряти упаковані програми
/unsafe	шукати потенційно небезпечні програми

/no-unsafe	не перевіряти на наявність потенційно небезпечних програм (за замовчуванням)
/unwanted	шукати потенційно небажані програми
/no-unwanted	не перевіряти 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=EXTENSIONS	не сканувати файли з РОЗШИРЕННЯМИ, розділеними двокрапкою
/clean-mode=MODE	використовувати РЕЖИМ очищення для інфікованих об’єктів Доступні вказані нижче опції: • none (за замовчуванням) – автоматичне очищення не відбувається. • standard – ecls.exe спробує автоматично очистити або видалити інфіковані файли. • strict – ecls.exe спробує автоматично очистити або видалити інфіковані файли без втручання користувача (перед видаленням запит не відображатиметься). • rigorous – ecls.exe видалятиме файли без спроби очищення незалежно від їхнього типу. • delete – ecls.exe видалятиме файли без спроби очищення, але не видалятиме важливі файли, як-от системні файли Windows.
/quarantine	копіювати інфіковані файли до карантину (доповнення до дії, що виконується під час очищення)
/no-quarantine	не копіювати інфіковані файли до карантину

Загальні параметри:

/help	відкрити довідку й вийти
/version	показати інформацію про версію й вийти
/preserve-time	зберегти час останнього доступу

Коди виходу:

0	загрози не знайдено
1	загрозу знайдено й очищено
10	деякі файли не вдається сканувати (можуть бути загрозами)
50	знайдено загрозу
100	помилка (коди виходу понад 100 означають, що файл не було перевірено, тому його не можна вважати чистим)

ESET CMD

Ця функція активує додаткові команди ecmd. Вони дозволяють експортувати й імпортувати параметри за допомогою командного рядка (ecmd.exe). До цього часу експорт та імпорт параметрів був можливий лише за допомогою графічного інтерфейсу користувача. Конфігурацію ESET Mail Security можна експортувати у файл формату *.xml*.

Якщо ESET CMD ввімкнено, доступні два методи авторизації.

- **Немає** – без авторизації. Не рекомендовано використовувати 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 потрібен пароль; цей файл має бути підписаним (див. файл конфігурації .xml нижче). Для імпорту нової конфігурації спочатку необхідно вказати пароль, введений у розділі Параметри доступу. Якщо параметри доступу не активовано, пароль указано неправильно, або файл конфігурації у форматі .xml не підписано, конфігурація не імпортуватиметься.

Якщо ESET CMD ввімкнено, то для імпорту або експорту конфігурацій ESET Mail Security можна використовувати командний рядок. Це можна зробити вручну або створити сценарій для автоматизації.

Щоб використовувати додаткові команди ecmd, потрібно запустити їх із правами адміністратора або відкрити командний рядок Windows (cmd), вибравши пункт **У режимі адміністратора**. В іншому разі з'явиться повідомлення про **помилку виконання команди**. Крім того, щоб експортувати конфігурацію, потрібна цільова папка. Команда експорту працює, навіть якщо параметр ESET CMD вимкнено.

Команда параметрів експорту:
`ecmd /getcfg c:\config\settings.xml`

Команда параметрів імпорту:
`ecmd /setcfg c:\config\settings.xml`

Додаткові команди ecmd можна виконати лише локально. Виконати клієнтське завдання **Виконати команду** за допомогою ESET PROTECT не можна.

Підписання файлу конфігурації у форматі *.xml*.

1. Завантажте виконуваний файл XmlSignTool.

2. Відкрийте командний рядок Windows (cmd), вибравши параметр **У режимі адміністратора**.

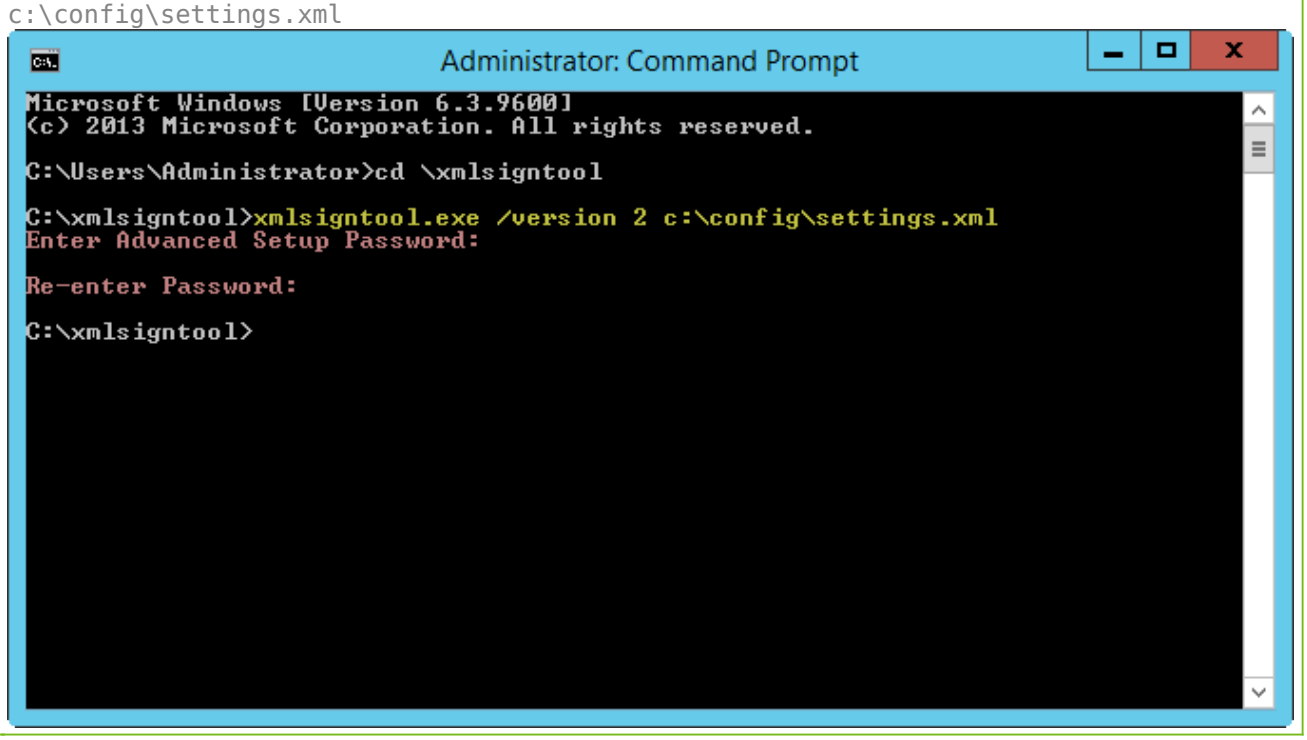
3. Перейдіть до місця розташування файлу `xmlsigntool.exe`.

4. Щоб підписати файл конфігурації у форматі *.xml*, виконайте команду `xmlsigntool /version 1|2 <xml_file_path>`.

Значення параметра `/version` залежить від версії ESET Mail Security. Використовуйте параметр `/version 2` для ESET Mail Security версії 7 і новіших.

5. Коли з'явиться відповідний запит XmlSignTool, введіть пароль для додаткових параметрів, а потім введіть його повторно. Тепер файл конфігурації у форматі *.xml* підписано, тож його можна використовувати для імпорту іншого екземпляра ESET Mail Security за допомогою ESET CMD з використанням пароля для авторизації.

Команда для підпису експортованого файлу конфігурації: `xmlsigntool /version 2 c:\config\settings.xml`



Якщо пароль у розділі Параметри доступу буде змінено й необхідно імпортувати файл конфігурації, підписаний раніше старим паролем, потрібно підписати файл конфігурації *.xml*, використовуючи поточний пароль. Це дозволяє використовувати старий файл конфігурації, не експортуючи його на інший комп'ютер з ESET Mail Security перед імпортом.

ESET RMM

Віддалене відстеження й керування (RMM) – процес нагляду та контролю за системами програмного забезпечення (зокрема встановленого на настільних ПК, серверах і мобільних пристроях) за допомогою локально інстальованого агента, до якого може отримати доступ постачальник послуг управління.

Увімкнути RMM

Вмикає функцію віддаленого відстеження й керування (RMM). Для використання утиліти RMM необхідні права адміністратора.

Робочий режим

Виберіть робочий режим RMM у розкривному меню:

- **Лише безпечне розділення** – якщо потрібно ввімкнути інтерфейс RMM для безпечних операцій лише для читання
- **Лише безпечне розділення** – якщо потрібно ввімкнути інтерфейс RMM для всіх

операцій

Метод авторизації

Виберіть метод авторизації RMM у розкривному меню:

- **Немає** — перевірка шляху програми не виконуватиметься. Ви можете запустити ermm.exe з будь-якої програми
- **Шлях програми** — укажіть програму, якій буде дозволено запускати ermm.exe

Інсталяція ESET Mail Security за замовчуванням містить файл *ermm.exe* у ESET Mail Security (шлях за замовчуванням *c:\Program Files\ESET\ESET Mail Security*). *ermm.exe* обмінюється даними з плагіном RMM, що передає їх агенту RMM, пов'язаному із сервером RMM.

- *ermm.exe* — це утиліта командного рядка, розроблена компанією ESET, яка дозволяє керувати продуктами робочої станції й обмінюватися даними з будь-яким плагіном RMM.
- Плагін RMM – це програма стороннього виробника, запущена локально на робочій станції із системою Windows. Плагін розробляється для обміну даними з певним агентом RMM (наприклад, лише Kaseya) і *ermm.exe*.
- Агент RMM – це програма стороннього виробника (наприклад, Kaseya), запущена локально на робочій станції із системою Windows. Агент обмінюється даними з плагіном RMM і сервером RMM.
- Сервер RMM запускається як служба на сторонньому сервері. Підтримувані системи RMM: Kaseya, Labtech, Autotask, Max Focus і Solarwinds N-able.

Щоб дізнатися більше про ESET RMM у ESET Mail Security, перегляньте нашу статтю бази знань.

Плагіни ESET Direct Endpoint Management для RMM сторонніх виробників

Сервер RMM запускається як служба на сторонньому сервері. Щоб дізнатися більше, перегляньте наведені нижче посібники користувача ESET Direct Endpoint Management:

- Плагін ESET Direct Endpoint Management для ConnectWise Automate
- Плагін ESET Direct Endpoint Management для DattoRMM
- Плагін ESET Direct Endpoint Management для Solarwinds N-Central
- ESET Direct Endpoint Management для NinjaRMM

Ліцензія

ESET Mail Security підключається до сервера ліцензій ESET кілька разів на годину для проведення перевірок. За замовчуванням для параметра **Перевірка інтервалу** встановлено значення **Автоматично**. Щоб зменшити мережевий трафік, що виникає внаслідок перевірок ліцензування, змініть значення "Перевірка інтервалу" на **Обмежено**, і тоді перевірка ліцензування виконуватиметься лише раз на день (а також після перезавантаження сервера).

Якщо для параметра "Перевірка інтервалу" встановлено значення **Обмежено**, на застосування всіх змін, пов'язаних із ліцензуванням ESET Mail Security за допомогою ESET Business Account та ESET MSP Administrator, може знадобитися до одного дня.

Постачальник WMI

Інструментарій керування Windows (WMI) – це реалізація Microsoft Web-Based Enterprise Management (WBEM), яка є галузевою основою для розробки стандартної технології доступу до інформації про керування в корпоративному середовищі.

Щоб дізнатися більше про WMI, перегляньте сторінку http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Постачальник ESET WMI

Мета ESET постачальника ESET WMI – дозволити віддалений моніторинг продуктів ESET у корпоративному середовищі без потреби використання будь-якого програмного забезпечення або інструментів ESET. Надаючи основну інформацію про продукт, стан і статистику через WMI, ми значно розширюємо можливості адміністраторів підприємств під час моніторингу продуктів ESET.

Адміністратори можуть скористатися низкою методів доступу, пропонованих WMI (командний рядок, сценарії та сторонні інструменти моніторингу корпоративних продуктів), щоб відстежувати стан своїх продуктів ESET.

Поточна реалізація забезпечує доступ лише для читання до основної інформації про продукт, інстальовані компоненти та їхній статус захисту, статистику окремих сканерів і файлів журналу продуктів.

Постачальник WMI дає змогу використовувати стандартну інфраструктуру й інструменти Windows WMI для читання стану продукту та його журналів.

Надані дані

Усі класи WMI, пов'язані з продуктом ESET, розташовані в просторі імен root\ESET. Нижче наведено класи, які зараз використовуються. Докладну інформацію про них можна переглянути під їх переліком.

Загальні

- ESET_Product
- ESET_Features
- ESET_Statistics

Журнали

- ESET_ThreatLog
- ESET_EventLog

- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

Клас ESET_Product

Клас ESET_Product може існувати лише в одному екземплярі. Властивості цього класу стосуються основної інформації про інстальований продукт ESET.

- ID – ідентифікатор типу продукту, наприклад "emsl".
- Name – назва продукту, наприклад "ESET Mail Security".
- FullName – повна назва продукту, наприклад "ESET Mail Security для IBM Domino".
- Version – версія продукту, наприклад "6.5.14003.0".
- VirusDBVersion – версія бази даних вірусів, наприклад "14533 (20161201)".
- VirusDBLastUpdate – мітка часу останнього оновлення бази даних вірусів. Рядок містить мітку часу у форматі дати й часу WMI, наприклад "20161201095245.000000+060".
- LicenseExpiration – час завершення терміну дії. Рядок містить мітку часу у форматі дати й часу WMI.
- KernelRunning – логічне значення, що вказує, чи запущена служба ekrn на комп’ютері, наприклад "TRUE".
- StatusCode – номер, що вказує на статус захисту продукту: 0 – зелений (OK), 1 – жовтий (попередження), 2 – червоний (помилка).
- StatusText – повідомлення, що пояснює, чому код статусу не дорівнює нулю (це повідомлення не з’являється, якщо код статусу дорівнює нулю).

Клас ESET_Features

Клас ESET_Features має кілька екземплярів. Їх кількість залежить від кількості функцій продукту. Кожен екземпляр містить указану нижче інформацію.

- Name – ім’я функції (список імен наведено нижче).
- Status – статус функції: 0 – неактивно, 1 – вимкнено, 2 – увімкнено.

Нижче наведено список рядків із функціями продукту, які зараз розпізнаються.

- CLIENT_FILE_AV – захист файлової системи від вірусів у режимі реального часу.
- CLIENT_WEB_AV – захист клієнта від вірусів під час інтернет-з’єднання.
- CLIENT_DOC_AV – захист документів клієнта від вірусів.
- CLIENT_NET_FW – персональний брандмауер клієнта.
- CLIENT_EMAIL_AV – захист електронної пошти клієнта від вірусів.
- CLIENT_EMAIL_AS – захист електронної пошти клієнта від спаму.
- SERVER_FILE_AV – захист файлів, що зберігаються в захищених файлових серверних продуктах, від вірусів у режимі реального часу, наприклад файлів у базі даних вмісту SharePoint, коли використовується ESET Mail Security.
- SERVER_EMAIL_AV – захист від вірусів повідомлень електронної пошти, що зберігаються в захищених серверних продуктах (наприклад, повідомлення електронної пошти в Microsoft Exchange або IBM Domino).
- SERVER_EMAIL_AS – захист від спаму повідомлень електронної пошти, що зберігаються в захищених серверних продуктах (наприклад, повідомлення електронної пошти в Microsoft Exchange або IBM Domino).
- SERVER_GATEWAY_AV – антивірусний захист захищених мережевих протоколів у шлюзі.
- SERVER_GATEWAY_AS – захист від спаму захищених мережевих протоколів у шлюзі.

Клас ESET_Statistics

Клас ESET_Statistics має кілька екземплярів. Їх кількість залежить від кількості сканерів у продукті. Кожен екземпляр містить указану нижче інформацію.

- Scanner – код рядка, що стосується певного сканера, наприклад "CLIENT_FILE".
- Total – загальна кількість просканованих файлів.
- Infected – кількість знайдених заражених файлів.
- Cleaned – кількість очищених файлів.
- Timestamp – мітка часу останньої зміни цієї статистики. У форматі дати й часу WMI ця мітка має такий вигляд: "2013011815511.000000+060".
- ResetTime – мітка часу останнього скидання лічильника статистики. У форматі дати й часу

WMI ця мітка має такий вигляд: "20130118155511.000000+060".

Нижче наведено список рядків зі сканерами, які зараз розпізнаються.

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Клас ESET_ThreatLog

Клас ESET_ThreatLog має кілька екземплярів, кожен із яких представляє запис із журналу "Виявлені загрози". Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу сканування.
- Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).
- LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.
- Scanner – ім’я сканера, який створив цю подію журналу.
- ObjectType – тип об’єкта, що згенерував цю подію журналу.
- ObjectName – ім’я об’єкта, що згенерував цю подію журналу.
- Threat – ім’я загрози, виявленої в об’єкті, описаному властивостями ObjectName і ObjectType.
- Action – дія, виконана після виявлення загрози.
- User – обліковий запис користувача, що спричинив створення цієї події журналу.
- Information – додатковий опис події.
- Hash – хеш об’єкта, що згенерував цю подію журналу.

ESET_EventLog

Клас ESET_EventLog має кілька екземплярів, кожен із яких представляє запис із журналу "Події". Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу сканування.
- Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Module – ім’я модуля, який створив цю подію журналу.

• Event – опис події.

• User – обліковий запис користувача, що спричинив створення цієї події журналу.

ESET_ODFileScanLogs

Клас ESET_ODFileScanLogs має кілька екземплярів, кожен із яких представляє запис про сканування файлів на вимогу. Цей список ідентичний списку журналів "Сканування комп’ютера на вимогу", що показується в графічному інтерфейсі. Кожен екземпляр містить указану нижче інформацію.

• ID – унікальний ідентифікатор запису журналу сканування.

• Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).

• Targets – цільові папки й об’єкти сканування.

• TotalScanned – загальна кількість просканованих об’єктів.

• Infected – кількість знайдених заражених об’єктів.

• Cleaned – кількість очищених об’єктів.

• Status – статус процесу сканування.

ESET_ODFileScanLogRecords

Клас ESET_ODFileScanLogRecords має кілька екземплярів, кожен із яких представляє запис в одному з журналів сканування, представлених екземплярами класу ESET_ODFileScanLogs. Екземпляри цього класу містять записи всіх журналів або сканувань на вимогу. Якщо потрібен екземпляр певного журналу сканування, необхідно виконати фільтрацію за властивістю LogID. Кожен екземпляр класу містить указану нижче інформацію.

• LogID — ідентифікатор журналу сканування, до якого належить цей запис (ідентифікатор одного з екземплярів класу ESET_ODFileScanLogs).

• ID – унікальний ідентифікатор запису журналу сканування.

• Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Log — фактичне повідомлення журналу.

ESET_ODServerScanLogs

Клас ESET_ODServerScanLogs має кілька екземплярів, кожен із яких представляє запуск сканування сервера на вимогу. Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу сканування.
- Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).
- Targets – цільові папки й об’єкти сканування.
- TotalScanned – загальна кількість просканованих об’єктів.
- Infected – кількість знайдених заражених об’єктів.
- Cleaned – кількість очищених об’єктів.
- RuleHits — загальна кількість спрацювань правила.
- Status – статус процесу сканування.

ESET_ODServerScanLogRecords

Клас ESET_ODServerScanLogRecords має кілька екземплярів, кожен із яких представляє запис в одному з журналів сканування, представлених екземплярами класу ESET_ODServerScanLogs. Екземпляри цього класу містять записи всіх журналів або сканувань на вимогу. Якщо потрібен екземпляр певного журналу сканування, необхідно виконати фільтрацію за властивістю LogID. Кожен екземпляр класу містить указану нижче інформацію.

- LogID – ідентифікатор журналу сканування, до якого належить цей запис (ідентифікатор одного з екземплярів класу ESET_ODServerScanLogs).
- ID – унікальний ідентифікатор запису журналу сканування.
- Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).
- LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.
- Log – фактичне повідомлення журналу.

ESET_SmtpProtectionLog

Клас ESET_SmtpProtectionLog має кілька екземплярів, кожен із яких представляє запис із журналу "Захист SMTP". Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу сканування.
- Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).
- LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація,

важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

- HELODomain – ім’я домену HELO.
- IP – IP-адреса джерела.
- Sender – відправник повідомлення електронної пошти.
- Recipient – одержувач повідомлення електронної пошти.
- ProtectionType – тип захисту, що використовується.
- Action – виконана дія.
- Reason – причина дії.
- TimeToAccept – кількість хвилин, після яких буде прийнято повідомлення електронної пошти.

ESET_HIPSLog

Клас ESET_HIPSLog має кілька екземплярів, кожен із яких представляє запис із журналу "HIPS". Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу.
- Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).
- LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.
- Application – вихідна програма.
- Target – тип операції.
- Action – дія, яку вживає система запобігання вторгненням (HIPS), наприклад дозвіл, заборона тощо.
- Rule – ім’я правила, відповідального за дію.
- AdditionalInfo

ESET_URLLog

Клас ESET_URLLog має кілька екземплярів, кожен із яких представляє запис із журналу "Відфільтровані веб-сайти". Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу.
- Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• URL – URL-адреса.

• Status – які дії було вжито до URL-адреси, наприклад «Заблоковано за допомогою веб-контролю»

• Application – програма, яка намагалась отримати доступ до URL-адреси.

• User – обліковий запис користувача, від імені якого запускалася програма.

ESET_DevCtrlLog

Клас ESET_DevCtrlLog має кілька екземплярів, кожен із яких представляє запис із журналу "Контроль пристроїв". Кожен екземпляр містить указану нижче інформацію.

• ID – унікальний ідентифікатор запису журналу.

• Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Device – ім’я пристрою.

• User – ім’я облікового запису користувача.

• UserSID – ідентифікатор безпеки облікового запису користувача.

• Group – ім’я групи користувачів.

• GroupSID – ідентифікатор безпеки групи користувачів.

• Status – які дії було вжито до пристрою, наприклад «Запис заблоковано»

• DeviceDetails – додаткова інформація про пристрій.

• EventDetails – додаткова інформація про подію.

ESET_MailServerLog

Клас ESET_MailServerLog має кілька екземплярів, кожен із яких представляє запис із журналу "Поштовий сервер". Кожен екземпляр містить указану нижче інформацію.

• ID – унікальний ідентифікатор запису журналу.

• Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8].

Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

- IPAddr – IP-адреса джерела.
- HELODomain – ім’я домену HELO.
- Sender – відправник повідомлення електронної пошти.
- Recipient – одержувач повідомлення електронної пошти.
- Subject – тема повідомлення електронної пошти.
- ProtectionType – тип захисту, який виконав дію, описану в поточному записі журналу, наприклад захист від шкідливого програмного забезпечення, захист від спаму або правила.
- Action – виконана дія.
- Reason – причина виконання дії над об’єктом за поточним типом захисту ProtectionType.

ESET_HyperVScanLogs

Клас ESET_HyperVScanLogs має кілька екземплярів, кожен із яких представляє запуск сканування файлів Hyper-V. Цей список ідентичний списку журналів "Сканування Hyper-V", що показується в графічному інтерфейсі. Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор запису журналу.
- Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).
- Targets – цільові комп’ютери, диски, томи для сканування.
- TotalScanned – загальна кількість просканованих об’єктів.
- Infected – кількість знайдених заражених об’єктів.
- Cleaned – кількість очищених об’єктів.
- Status – статус процесу сканування.

ESET_HyperVScanLogRecords

Клас ESET_HyperVScanLogRecords має кілька екземплярів, кожен із яких представляє запис в одному із журналів сканування, представлених екземплярами класу ESET_HyperVScanLogs. Екземпляри цього класу містять записи всіх журналів або сканувань Hyper-V. Якщо потрібен екземпляр певного журналу сканування, необхідно виконати фільтрацію за властивістю LogID. Кожен екземпляр класу містить указану нижче інформацію.

- LogID – ідентифікатор журналу сканування, до якого належить цей запис (ідентифікатор одного з екземплярів класу ESET_HyperVScanLogs).
- ID – унікальний ідентифікатор запису журналу.

• Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Log – фактичне повідомлення журналу.

ESET_NetworkProtectionLog

Клас ESET_NetworkProtectionLog має кілька екземплярів, кожен із яких представляє запис із журналу "Захист мережі". Кожен екземпляр містить указану нижче інформацію.

• ID – унікальний ідентифікатор запису журналу.

• Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Event – подія, яка активує дію захисту мережі.

• Action – дія, яку виконує захист мережі.

• Source – вихідна адреса мережевого пристрою.

• Target – цільова адреса мережевого пристрою.

• Protocol – протокол мережевого підключення.

• RuleOrWormName – ім’я правила або черв’яка, пов’язаного з подією.

• Application – програма, яка ініціювала мережеве підключення.

• User – обліковий запис користувача, що спричинив створення цієї події журналу.

ESET_SentFilesLog

Клас ESET_SentFilesLog має кілька екземплярів, кожен із яких представляє запис із журналу "Надіслані файли". Кожен екземпляр містить указану нижче інформацію.

• ID – унікальний ідентифікатор запису журналу.

• Timestamp – мітка часу створення запису журналу (у форматі дати й часу WMI).

• LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.

• Sha1 – хеш Sha-1 надісланого файлу.

- File – надісланий файл.
- Size – розмір надісланого файлу.
- Category – категорія надісланого файлу.
- Reason – причина надсилання файлу.
- SentTo – відділ ESET, якому надіслано файл.
- User – обліковий запис користувача, що спричинив створення цієї події журналу.

ESET_OneDriveScanLogs

Клас ESET_OneDriveScanLogs має кілька екземплярів, кожен із яких представляє запуск сканування OneDrive. Цей список ідентичний списку журналів "Сканування OneDrive", що відображається в графічному інтерфейсі. Кожен екземпляр містить указану нижче інформацію.

- ID – унікальний ідентифікатор журналу OneDrive.
- Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).
- Targets – цільові папки й об’єкти сканування.
- TotalScanned – загальна кількість просканованих об’єктів.
- Infected – кількість знайдених заражених об’єктів.
- Cleaned – кількість очищених об’єктів.
- Status – статус процесу сканування.

ESET_OneDriveScanLogRecords

Клас ESET_OneDriveScanLogRecords має кілька екземплярів, кожен із яких представляє запис в одному з журналів сканування, представлених екземплярами класу ESET_OneDriveScanLogs. Екземпляри цього класу містять записи всіх журналів або сканувань OneDrive. Якщо потрібен екземпляр певного журналу сканування, необхідно виконати фільтрацію за властивістю LogID. Кожен екземпляр містить указану нижче інформацію.

- LogID – ідентифікатор журналу сканування, до якого належить цей запис (ідентифікатор одного з екземплярів класу ESET_OneDriveScanLogs).
- ID – унікальний ідентифікатор журналу OneDrive.
- Timestamp – мітка часу створення журналу (у форматі дати й часу WMI).
- LogLevel – рівень серйозності запису журналу, виражений як число в діапазоні [0–8]. Значення відповідають таким рівням: налагодження, інформаційна виноска, інформація, важлива інформація, попередження, помилка, попередження про безпеку, критична помилка, критичне попередження про безпеку.
- Log – фактичне повідомлення журналу.

Доступ до наданих даних

Нижче наведено кілька прикладів, як можна отримати доступ до даних ESET WMI із командного рядка Windows та оболонки PowerShell, які мають працювати з будь-якою поточною операційною системою Windows. Однак існує багато інших способів доступу до даних за допомогою інших мов сценаріїв та інструментів.

Командний рядок без сценаріїв

Інструмент `wmic` командного рядка можна використовувати для доступу до різних попередньо визначених або спеціальних класів WMI.

Щоб показати на локальному комп'ютері повну інформацію про продукт:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Щоб відобразити номер версії лише продукту на локальному комп'ютері:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Щоб показати повну інформацію про продукт на віддаленому комп'ютері з IP-адресою 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Отримати й показати повну інформацію про продукт на локальному комп'ютері:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Отримати й показати повну інформацію про продукт на віддаленому комп'ютері з IP-адресою 10.1.118.180:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
cred $cred
```

Об'єкти сканування консолі керування ESET

Ця функція дає змогу ESET PROTECT використовувати об'єкт сканування (сканування бази даних поштових скриньок за вимогою та сканування Hyper-V) під час виконання клієнтського завдання "Сканування сервера" на сервері з ESET Mail Security. Налаштування об'єктів сканування ESET PROTECT можливе, лише якщо у вас встановлено ESET Management Agent. В іншому разі воно буде недоступне.

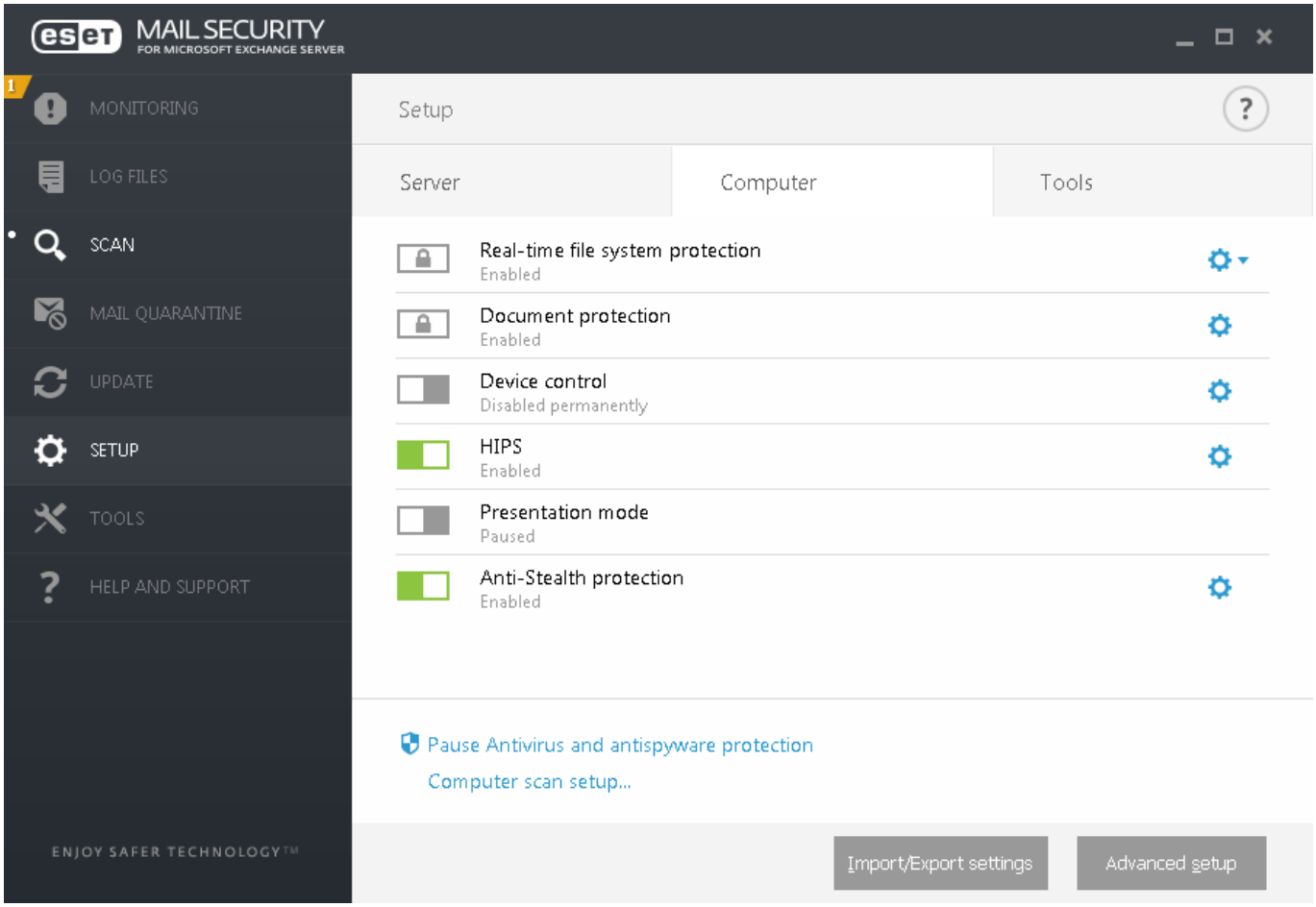
Якщо ввімкнути функцію **Створити список об'єктів**, ESET Mail Security створить список доступних об'єктів сканування. Цей список генеруватиметься відповідно до **Періоду оновлення**.

Якщо функцію **Створити список об'єктів** увімкнено вперше, для отримання цього списку ESET PROTECT знадобиться приблизно половина визначеного **Періоду оновлення**. Тому якщо для **Періоду оновлення** задано 60 хвилин, ESET PROTECT отримає список об'єктів сканування приблизно за 30 хвилин. Щоб ESET PROTECT отримав список швидше, задайте менше значення для періоду оновлення. Його завжди можна збільшити пізніше.

Коли ESET PROTECT запускає клієнтське завдання **Сканування сервера**, то отримує список, а вам буде запропоновано вибрати об'єкти для сканування Hyper-V на цьому сервері.

Режим заміщення

Якщо до ESET Mail Security застосовано політику ESET PROTECT, на сторінці Налаштування відображатиметься піктограма блокування , а не перемикач увімкнення/вимкнення, а у вікні **Додаткові параметри** – піктограма блокування поруч із перемикачем.

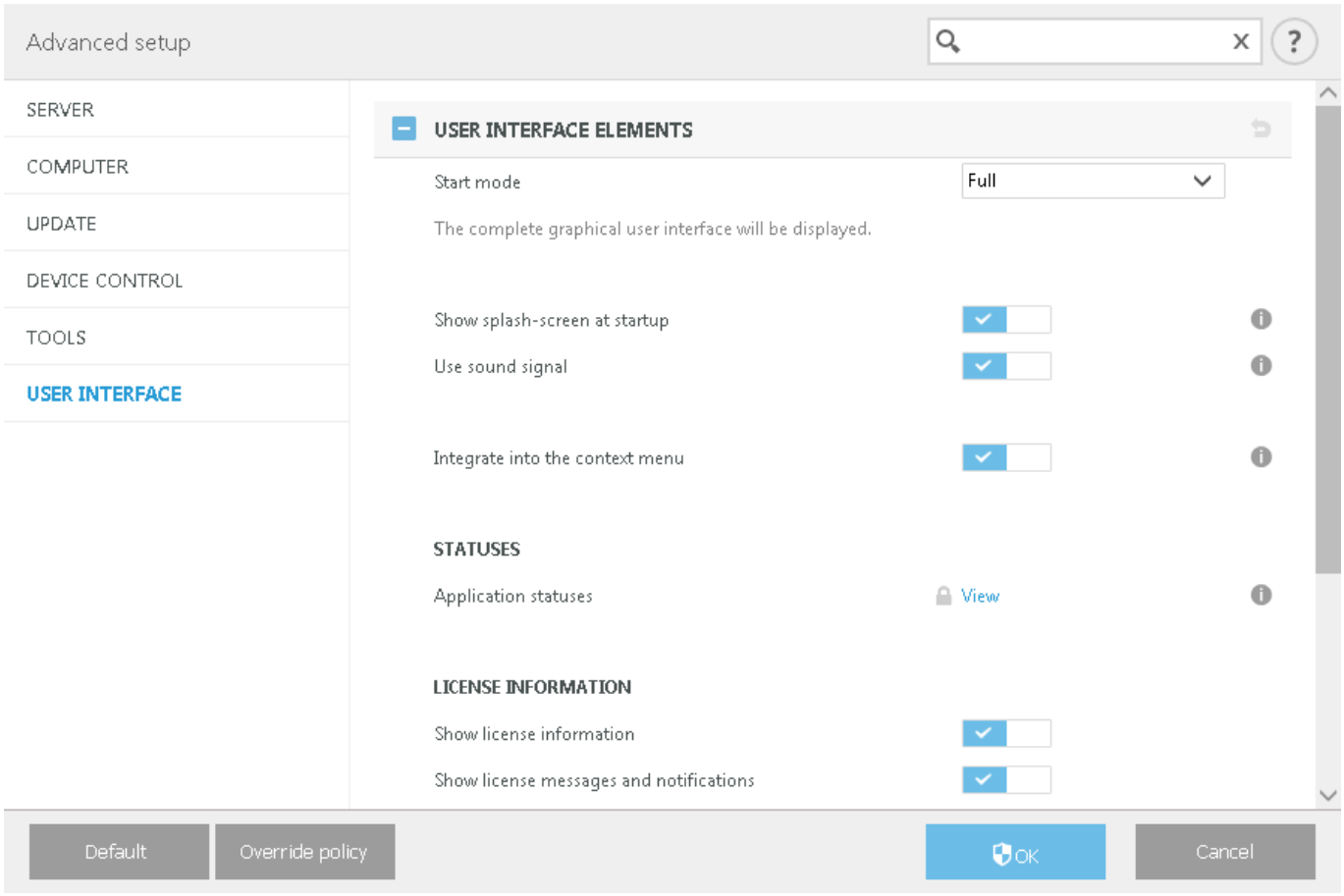


Зазвичай параметри, налаштовані за допомогою політики ESET PROTECT, не можна змінювати. Режим заміщення дозволяє тимчасово розблокувати ці параметри. Однак потрібно ввімкнути **режим заміщення** за допомогою політики ESET PROTECT.

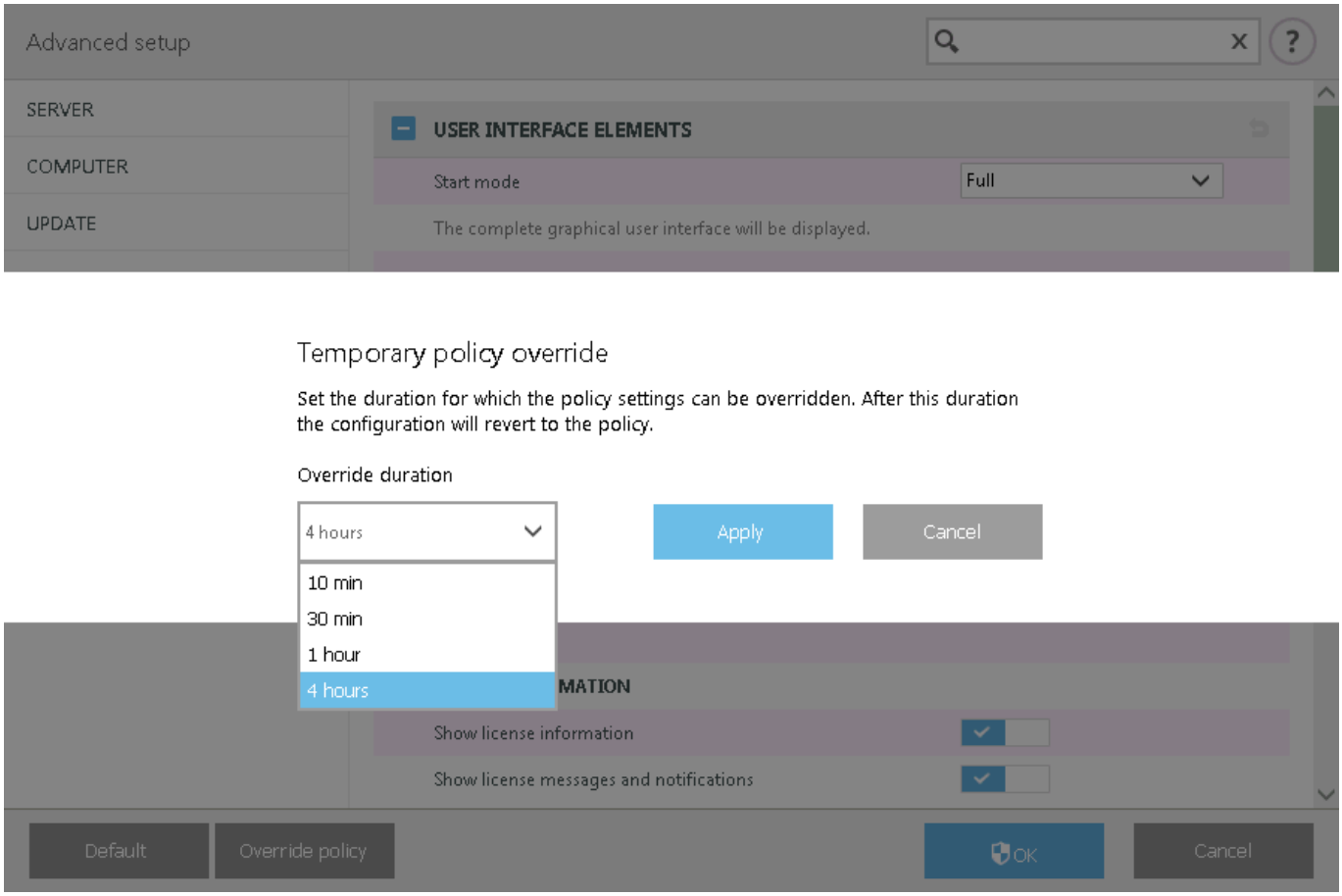
Увійдіть у ESET PROTECT веб-консоль, перейдіть до пункту **Політики**, виберіть і змініть наявну політику, яка застосовується до ESET Mail Security, або створіть нову. У розділі **Параметри** клацніть **Режим заміщення**, увімкніть його й налаштуйте інші параметри, зокрема тип автентифікації (користувач Active Directory або пароль).

Після змінення політики або застосування нової політики до ESET Mail Security у вікні **Додаткові**

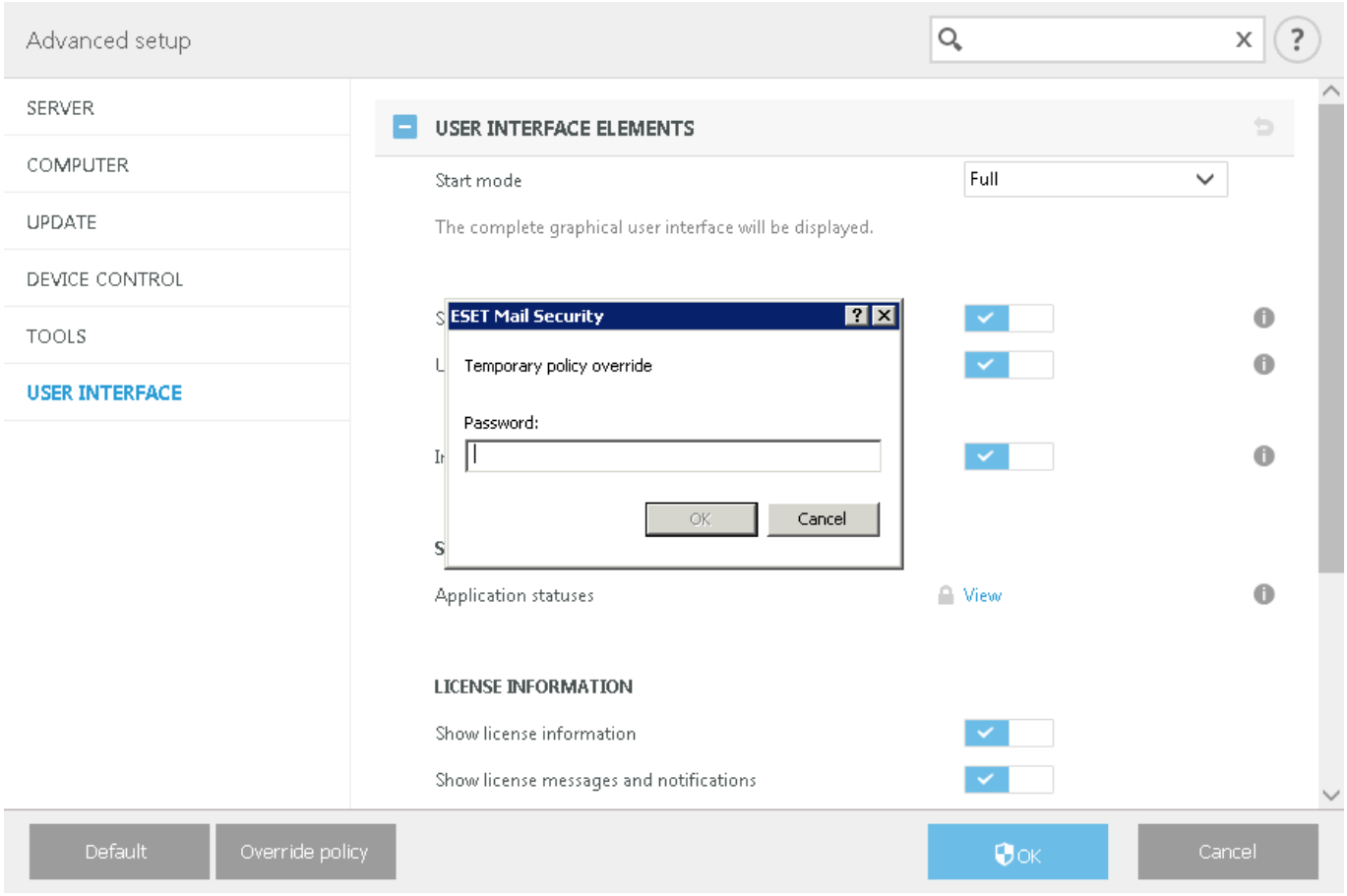
параметри з’явиться кнопка заміщення політики.



Натисніть кнопку **Замістити політику**, виберіть тривалість і натисніть **Застосувати**.



Якщо як тип автентифікації вибрано **Пароль**, введіть пароль заміни політики.



Після завершення роботи режиму заміщення всі внесені зміни в конфігурації повернуться до початкових параметрів політики ESET PROTECT. Ви побачите сповіщення до завершення заміщення.

Режим заміщення можна **завершити** в будь-який час до закінчення строку його дії на сторінці моніторингу або у вікні додаткових параметрів.

Файли журналу

У цьому розділі можна змінювати параметри ведення журналів ESET Mail Security.

Записи журналу

Записи вносяться в журнал подій (*C:\ProgramData\ESET\ESET Security\Logs*). Їх можна переглянути в засобі для перегляду файлів журналу. Щоб увімкнути або вимкнути певну функцію, скористайтеся перемикачами:

Вести журнал помилок передавання електронних листів
Якщо цю опцію ввімкнено, то під час виникнення проблем на рівні передавання електронних листів повідомлення про помилки записуватимуться в журнал подій.

Вести журнал виключень передавання електронних листів
Якщо на рівні передавання електронних листів є виключення, інформація про них записується в журнал подій.

Фільтр ведення журналів

Створює значний обсяг даних, оскільки всі опції ведення журналів ввімкнено за замовчуванням. Рекомендуємо вибірково вимкнути ведення журналів для компонентів, які не допоможуть у вирішенні проблеми або взагалі не пов'язані з нею.

> Щоб розпочати фактичне ведення журналів, потрібно ввімкнути загальне **ведення журналу діагностики** на рівні продукту в головному меню **Налаштування** > Інструменти. Щойно ви ввімкнете ведення журналів, ESET Mail Security почне збирати докладні журнали відповідно до функцій, увімкнених у цьому розділі.

Щоб увімкнути або вимкнути певну функцію, скористайтеся перемикачами. Ці опції можна поєднувати залежно від доступності окремих компонентів у ESET Mail Security.

• Ведення журналу діагностики передавання електронних листів

> У разі вирішення проблем зі скануванням бази даних, що виконується за звичайних умов, рекомендуємо вимкнути **ведення журналу діагностики передавання електронних листів**. В іншому разі це може призвести до перевантаження отриманого журналу й зробити його складним для аналізу.

- **Ведення журналу діагностики сканування баз даних на вимогу** – записує докладну інформацію в журнали, зокрема необхідну для виправлення помилок.
- **Ведення журналу діагностики кластерів** – ведення журналу кластерів буде включено в загальне ведення журналу діагностики.
- **Ведення журналу діагностики OneDrive**: ведення журналу OneDrive буде складовим загального ведення журналу діагностики.
- **Ведення журналу діагностики антиспам-модуля** – відображатиме в журналах докладну інформацію про антиспам-модуль, необхідну для виправлення помилок. Записує докладну діагностичну інформацію про антиспам-модуль у файл журналу. Антиспам-модуль не використовує журнал подій (файл warnlog.dat), тому його неможливо переглянути в засобі для перегляду файлів журналу. Записи вносяться безпосередньо в спеціальний текстовий файл (наприклад, C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log), тож усі діагностичні дані про антиспам-модуль зберігаються в одному місці. Завдяки цьому великий поштовий трафік не впливатиме на продуктивність ESET Mail Security.

Файли журналу

Визначте спосіб керування журналами. Це важливо здебільшого для того, щоб запобігти використанню диска. Параметри за замовчуванням дають змогу автоматично видаляти старіші журнали, щоб заощадити місце на диску.

Автоматично видаляти записи

Записи журналу, старіші за вказану нижче кількість днів, буде видалено.

Видаляти записи, старіші за (дн.)

Укажіть кількість днів.

Автоматично видаляти старі записи, коли розмір журналу перевищує обмеження

Якщо розмір файлу журналу перевищить **Максимальний розмір журналу [МБ]**, старі записи буде видалено, щоб зменшити файл до значення, установленого в параметрі **Розмір скороченого журналу [МБ]**.

Робити резервні копії автоматично видалених записів

Автоматично видалені файли та записи із журналів завантажуватимуться до вибраного каталогу й за потреби стискатимуться в ZIP-файл.

Робити резервні копії діагностичних журналів

Робитиме резервні копії автоматично видалених діагностичних журналів. Якщо цей параметр не ввімкнено, резервні копії записів журналу діагностики не робитимуться.

Папка для резервних копій

Папка, у якій зберігатимуться резервні копії журналу. Ви можете ввімкнути стискання резервних копій журналу в ZIP.

Автоматично оптимізувати файли журналу

Якщо цей прапорець встановлено, файли журналу автоматично дефрагментуються, коли відсоток фрагментації перевищує значення, вказане в полі **"Якщо кількість невикористаних записів перевищує (%)"**. Натисніть **Оптимізувати**, щоб розпочати дефрагментацію файлів журналу. Усі порожні записи журналу видаляються для підвищення продуктивності й швидкості опрацювання журналів. Це вдосконалення буде особливо помітним, якщо журнали містять велику кількість записів.

Увімкнути текстовий протокол

Щоб увімкнути зберігання журналів у файлах іншого формату окремо від файлів журналу:

- **Цільовий каталог** — це каталог, у якому зберігатимуться файли журналу (застосовується лише до **текстових** і **CSV-файлів**). У кожному розділі журналу міститься окремий файл із попередньо визначеним іменем файлу (наприклад, *virlog.txt* для розділу "Виявлені загрози" у файлах журналу, якщо для їх зберігання використовується звичайний текстовий файл).
- **Тип** – якщо вибрати формат **текстового** файлу, журнали зберігатимуться в текстовому файлі, а дані розділятимуться вкладками. Те саме стосується формату **CSV-файлу**, у якому дані розділяються крапками з комами. Якщо вибрати тип **Подія**, журнали зберігатимуться не у файлах, а в журналі подій Windows (можна переглядати за допомогою засобу перегляду подій на Панелі керування).
- **Видалити всі файли журналу** – видаляє всі збережені журнали, вибрані в розкривному меню **Тип**.

> Щоб швидше вирішити проблеми, служба технічної підтримки ESET може попросити вас надати журнали з вашого комп'ютера. ESET Log Collector полегшує збір потрібної інформації. Щоб дізнатися більше про ESET Log Collector, перегляньте нашу статтю бази знань.

Журнал аудиту

Відстежує зміни в конфігурації або захисті. Оскільки зміна конфігурації продукту може негативно вплинути на його роботу, вам може знадобитися відстежувати зміни для проведення аудиту. Журнал записів про зміни відображатиметься в розділі **Файли журналу** > Журнал аудиту.

Експортувати журнал

Експорт до журналів програм і служб Windows
Дає змогу копіювати записи із журналу захисту поштового сервера в журнали програм і служб. Щоб переглянути журнал захисту поштового сервера, відкрийте **засіб перегляду подій** Windows і перейдіть у розділ **Журнали програм і служб** > **ESET** > **Безпека** > **Exchange Server** > **Захист електронної пошти**. Журнали програм і служб підтримуються в Microsoft Windows Server 2012 або новішої версії.
Експортувати на сервер syslog
Журнали захисту поштового сервера можна копіювати на сервер syslog у форматі Common Event Format (CEF). CEF – це стандартизований розширюваний текстовий формат, який може полегшити збір і впорядкування даних для подальшого аналізу корпоративною системою керування. Його можна використовувати разом із Security Information and Event Management (SIEM) і рішеннями для керування журналами, як-от Micro Focus ArcSight. Щоб дізнатися більше про експортовані поля й опис подій, перегляньте статтю Зіставлення подій syslog.
Адреса сервера
Уведіть IP-адресу або ім'я хоста сервера. Якщо використовується ArcSight, укажіть сервер зі встановленим SmartConnector.
Протокол
Виберіть потрібний протокол (TCP або UDP).
Порт
За замовчуванням для обох протоколів використовується порт 514.
Експортувати у файл
Дає змогу локально експортувати журнали у файл формату CEF. Ємність сховища журналів обмежена, тому використовується циклічне ведення журналів. Записи вносяться у файли послідовно (від `mailserver.0.log` до `mailserver.9.log`). Найновіші записи зберігаються в `mailserver.0.log`. Щойно його буде заповнено, найстаріший файл `mailserver.9.log` видалиться, а решта файлів журналу послідовно перейменуються (`mailserver.0.log` перейменується в `mailserver.1.log` і так далі).
Шлях до файлу
Шлях за замовчуванням – C:\ProgramData\ESET\ESET Security\Logs. За потреби його можна змінити.

Зіставлення подій syslog

У таблицях нижче показано зіставлення подій ESET Mail Security із полями даних ArcSight. У цих таблицях можна дізнаватися про те, які дані передаються в ArcSight через SmartConnector.

Header		
Device Vendor	"ESET"	
Device Product	"EMSX"	"EMSX" or "ESET Mail Security for MS Exchange Server"
Device Version	e.g. "7.1.10005.0"	
Device Event Class ID	e.g. "101"	Device Event Category unique identifier: 100-199 malware 200-299 phish 300-399 spam 400-499 policy
Event Name	e.g. "MailScanResult: malware"	A brief description of what happened in the event: MailScanResult: malware MailScanResult: phishing link MailScanResult: spam MailScanResult: policy

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
rt	deviceReceiptTime	Time event was generated	The time at which the event was generated, in milliseconds since Jan 1st 1970
src	sourceAddress	Sender's IP	IP address of the sending mail server
shost	sourceHostName (1023)	Sender's HELO domain	HELO domain of the sending mail server
flexString1	flexString1	Message-ID	Message-ID header from the email
dhost	destinationHostName (1023)	Receiving server	Hostname of the machine that received the communication
msg	message (1023)	Message subject	Subject of the message, from the RFC5233 header "Subject:"
suser	sourceUserName (1023)	SMTP sender	SMTP sender of the email (MAIL FROM)
duser	destinationUserName (1023)	SMTP recipient(s)	SMTP recipient(s) of the email (RCPT TO)
act	deviceAction (63)	Action taken	Action taken (cleaned, quarantined, etc.)
cat	deviceEventCategory (1023)	Detection category	Most significant detection (malware >> phish >> spam >> SPF/DKIM >> policy)
sourceServiceName	sourceServiceName	Type of protection	SMTP Transport agent, On-demand database scan
deviceExternalId	deviceExternalId	Engine version	Anti-Malware engine version, Antispam engine version, e.g. "18620,7730"
cs1	deviceCustomString1	Anti-Malware result	Result of Anti-Malware scan, including threat name
cs1Label	deviceCustomString1Label	"Anti-Malware result"	
cs2	deviceCustomString2	Antispam result	Result of Antispam scan, including reason for marking as spam
cs2Label	deviceCustomString2Label	"Antispam result"	
cs3	deviceCustomString3	Anti-Phishing result	Result of Anti-Phishing scan, including detected URL
cs3Label	deviceCustomString3Label	"Anti-Phishing result"	
cs4	deviceCustomString4	SPF/DKIM/DMARC result	Result of SPF/DKIM/DMARC check, in RFC7601 format
cs4Label	deviceCustomString4Label	"SPF/DKIM/DMARC result"	
cs5	deviceCustomString5	"From:" sender	Sender address from RFC5322 header "From:"
cs5Label	deviceCustomString5Label	"From header"	
cs6	deviceCustomString6	"To:" and "Cc:" recipients	Recipients addresses from RFC5322 headers "To:" and "Cc:"
cs6Label	deviceCustomString6Label	"To and Cc headers"	
fname	filename (1023)	Attachment name	Name of the first detected attachment

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
fileHash	fileHash (255)	Attachment hash	Hash of the first detected attachment
fsize	fileSize	Attachment size	Size of the first detected attachment
reason	reason (1023)	Rule/policy activated	Name of the policy triggered by the email or it's content
ESETEMSXFileDetails	ESETEMSXFileDetails	File details	Information about all detected attachments, their names, hashes and sizes

Optional

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
end	endTime	Time event has ended	The time at which the activity ended, in milliseconds since Jan 1st 1970. Useful only if sand boxing technology is used ESET LiveGuard Advanced.
dtz	deviceTimeZone (255)	Timezone of the server	
request	requestURL	Detected URL	Malign or blacklisted URL extracted from mail body or mail headers. ESET Mail Security does not provide single URL in logs due to the fact that multiple URL's can be detected in email messages by various detection components.

Проксі-сервер

У великих локальних мережах підключення комп'ютера до Інтернету може здійснюватися через проксі-сервер. У такому разі потрібно задати наведені нижче параметри. Без цих параметрів програма не зможе виконувати автоматичне оновлення. У ESET Mail Security параметри проксі-сервера доступні у двох наведених нижче розділах вікна **Додаткові параметри** (**F5**).

1. **Додаткові параметри** (F5) > **Оновлення** > **Профілі** > **Оновлення** > **Параметри підключення** > Проксі-сервер HTTP. Це налаштування застосовується для вказаного профілю оновлення й рекомендовано для ноутбуків, які часто отримують модулі з різних місць.

2. **Додаткові параметри** (F5) > **Інструменти** > **Проксі-сервер**. Налаштування проксі-сервера на цьому рівні визначає глобальні параметри проксі-сервера для всього ESET Mail Security. Ці параметри будуть використовувати всі модулі, підключені до Інтернету.

Щоб задати параметри проксі-сервера на цьому рівні, увімкніть перемикач **Використовувати проксі-сервер**, а потім введіть адресу проксі-сервера в полі **Проксі-сервер**, а також номер **порту** проксі-сервера.

Проксі-сервер потребує автентифікації

Якщо мережевий зв'язок через проксі-сервер потребує автентифікації, увімкніть цю опцію та вкажіть **ім'я користувача** і **пароль**.

Виявити проксі-сервер

Натисніть **Виявляти**, щоб автоматично виявляти й заповнювати параметри проксі-сервера. Параметри, указані в Internet Explorer, буде скопійовано.

> Ця функція не отримує даних автентифікації (ім'я користувача й пароль); їх потрібно вказати.

Використовувати пряме підключення, якщо проксі-сервер недоступний

Якщо продукт налаштувати для використання проксі-сервера HTTP, проте проксі-сервер буде недоступним, продукт обійде проксі-сервер та обмінюватиметься даними безпосередньо із серверами ESET.

Режим презентації

Режим презентації – це функція для користувачів, які потребують безперервного використання програмного забезпечення й відсутності відволікальних вікон сповіщень, а також хочуть мінімізувати споживання ресурсів процесора. Режим презентації також буде корисним під час презентацій, які не можна перервати активністю ESET Mail Security. Якщо цей режим увімкнено, усі вікна сповіщень вимикаються, а заплановані завдання не запускаються. Захист системи продовжує працювати у фоновому режимі, але не потребує втручання користувача.

Автоматично вмикати режим презентації під час запуску програм у повноекранному режимі

Режим презентації автоматично активується щоразу, коли запускається повноекранна програма. Якщо задіяно режим презентації, ви не зможете переглядати сповіщення або змінювати статус ESET Mail Security.

Автоматично вимкнути режим презентації через

Визначення періоду часу у хвилинах, після якого режим презентації автоматично вимкнеться.

Діагностичні дані

Модуль діагностики створює дампи робочих процесів ESET (наприклад, *ekrn*). Якщо програма аварійно завершує роботу, може бути створений дамп. Це може допомогти розробникам налагодити й усунути різні проблеми ESET Mail Security.

Відкрийте розкривне меню поруч із пунктом **Тип дампу** й виберіть один із трьох доступних параметрів, указаних нижче:

- **Вимкнути** – вимикає функцію.
- **Мінімальний** – (за замовчуванням) збирає найменший обсяг корисної інформації, яка може допомогти визначити причину аварійного завершення роботи програми. Цей тип файлу дампу може бути корисним, якщо дисковий простір обмежений. Проте аналіз цього файлу може не виявити помилок, які не було безпосередньо спричинено виконуваним потоком, оскільки зібрана інформація є неповною.

- **Повний** – записує весь уміст 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 створити файли дампу з даними діагностики в цільовому каталозі.

Розширене ведення журналів

Розширене ведення журналів для сканера — Записувати всі події, що виникають під час перевірки файлів і папок за допомогою функцій "Сканування комп’ютера" або "Захист файлової системи в режимі реального часу".
Увімкнути розширене ведення журналів для контролю пристроїв — Записувати всі події контролю пристроїв для діагностування та вирішення проблем.
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 служби ядра ESET (ekrn) для діагностики й вирішення проблем.
Увімкнути розширене ведення журналів для ліцензування: записувати всі сеанси обміну даними між продуктом і сервером ліцензій.
Увімкнути відстеження пам’яті — Записувати всі події, які допоможуть розробникам діагностувати втрати пам’яті.
Увімкнути розширене ведення журналів для модуля захисту мережі — Записувати всі мережеві дані, що проходять через модуль захисту мережі у форматі PCAP, щоб допомогти розробникам діагностувати й усувати проблеми, пов’язані з модулем захисту мережі.
Увімкнути ведення журналів для операційної системи — Буде збиратися додаткова інформація про операційну систему, зокрема інформація про запущені процеси, активність процесора, операції з диском. Це допоможе розробникам діагностувати й усувати проблеми з продуктом ESET у вашій операційній системі.
Увімкнути розширене ведення журналів для фільтрації протоколів — Записувати всі дані, що проходять через механізм фільтрації протоколів у форматі PCAP, щоб допомогти розробникам 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 допомогти в діагностиці й вирішенні проблем.
Увімкнути розширене ведення журналів 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 ведення журналів для підсистеми оновлення — Записувати всі події, які відбуваються під час оновлення, щоб допомогти розробникам діагностувати й усувати проблеми, пов’язані з підсистемою оновлення.

Розташування файлів журналу

C:\ProgramData\ESET\ESET Security\Diagnostics

Технічна підтримка

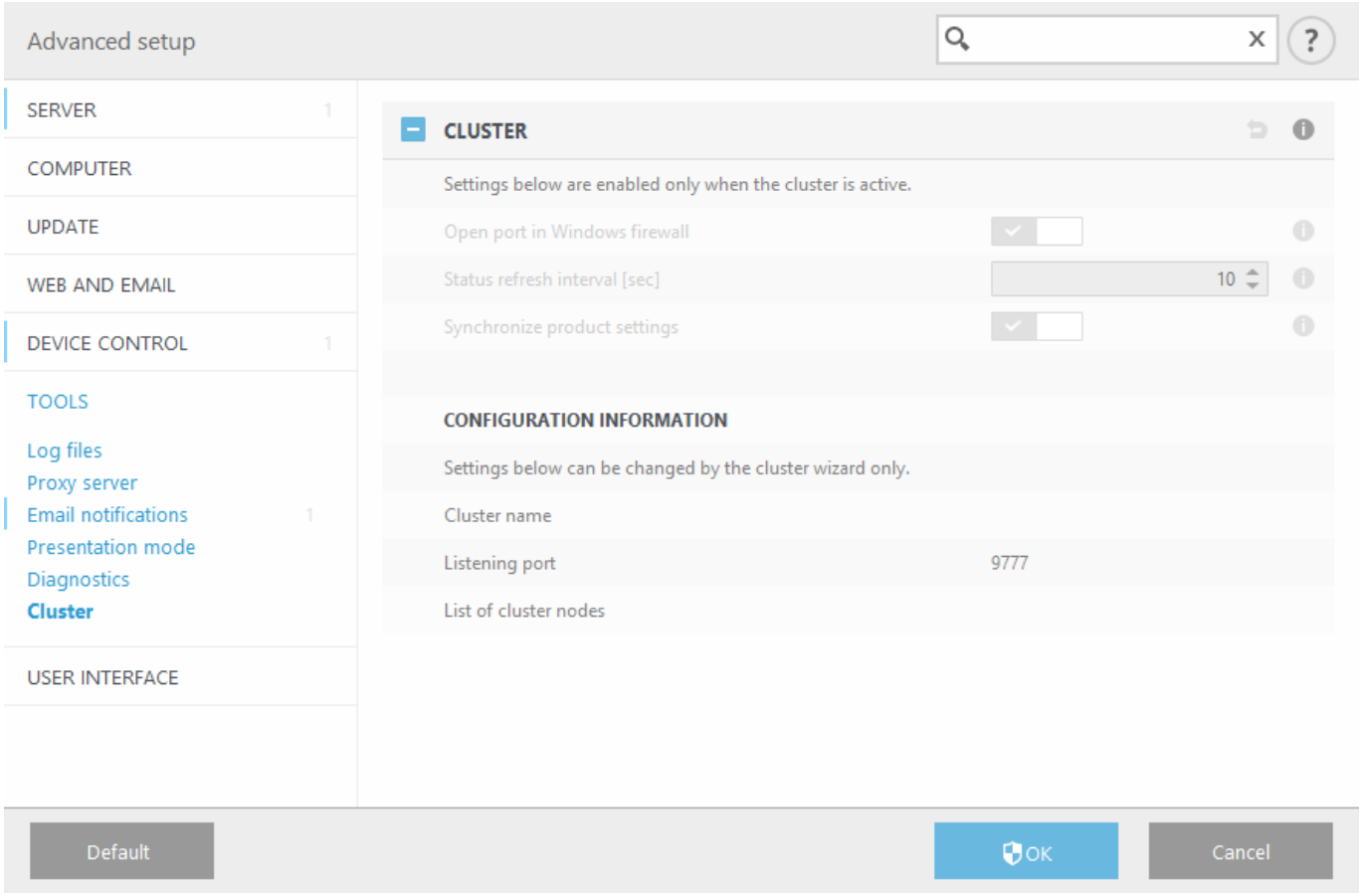
Надіслати дані про конфігурацію системи

Виберіть **Завжди надсилати**, щоб перед надсиланням даних конфігурації ESET Mail Security до служби технічної підтримки не вимагати підтвердження, або ж скористайтеся варіантом **Запитувати перед надсиланням**, якщо підтвердження необхідно.

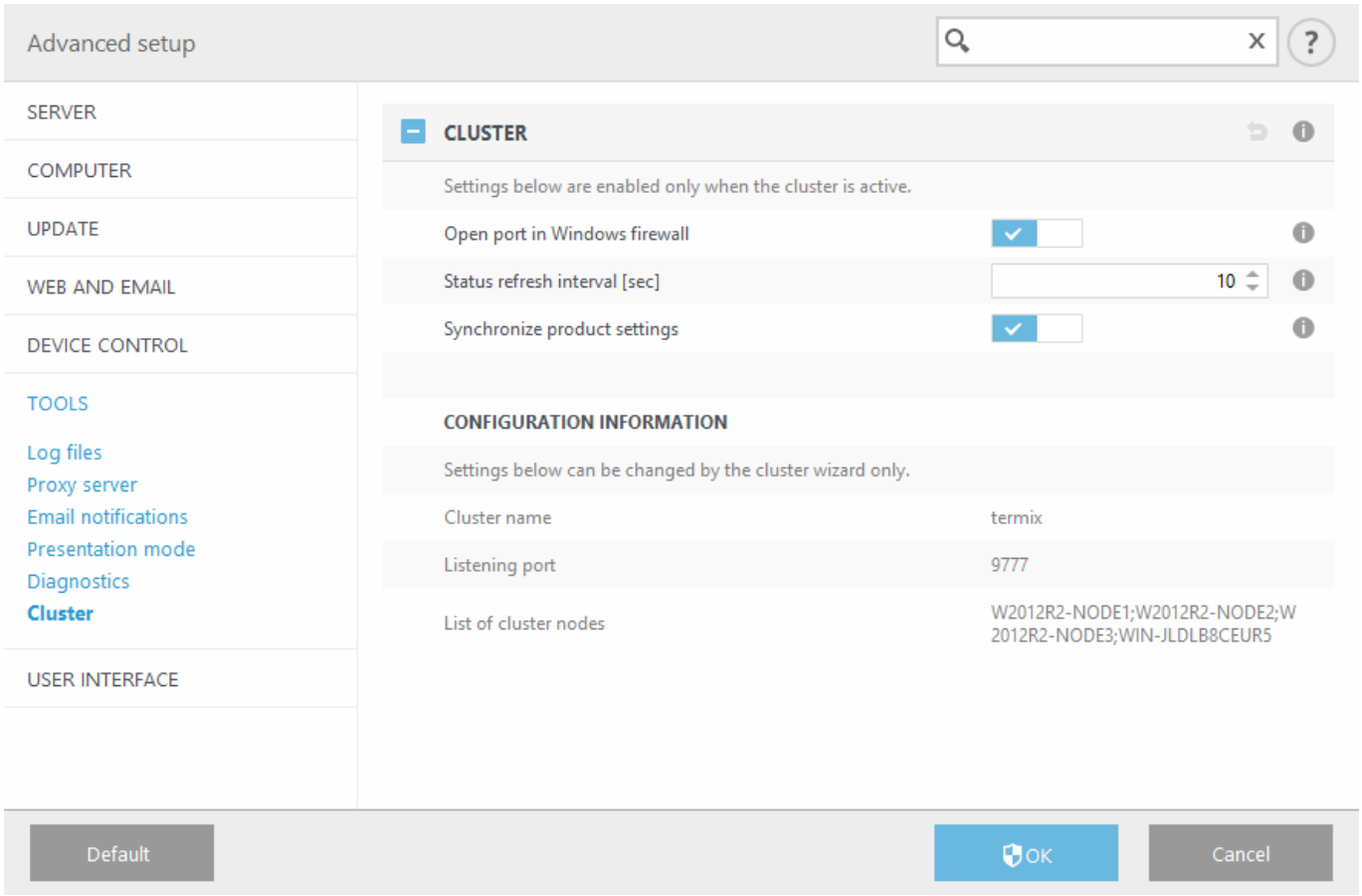
Кластер

Якщо налаштовано кластер ESET, він активується автоматично. Щоб вимкнути його вручну, у вікні **Додаткові параметри** (F5) натисніть піктограму перемикача (наприклад, якщо потрібно змінити конфігурацію без впливу на інші вузли кластера ESET). Цей перемикач вмикає або вимикає функції кластера ESET. Щоб налаштувати або знищити кластер, скористайтеся майстром кластера або **знищте** кластер, розташований у розділі "Інструменти" > "Кластер" головного вікна програми.

Кластер ESET не налаштовано й вимкнуто:



Дані й параметри кластера ESET правильно налаштовані:



Інтерфейс користувача

Налаштуйте поведінку графічного інтерфейсу користувача ESET Mail Security. Тут можна змінити зовнішній вигляд програми й ефекти, що використовуються.

У розкривному меню "Режим запуску графічного інтерфейсу користувача" виберіть один із наведених нижче режимів запуску графічного інтерфейсу користувача.

- **Повний**: графічний інтерфейс користувача відображатиметься повністю.

- **Термінал** – ніякі сповіщення й попередження не відображаються. Графічний інтерфейс користувача може запустити лише адміністратор. Якщо графічні елементи знижують продуктивність комп'ютера або спричиняють інші проблеми, для інтерфейсу користувача слід установити значення "Термінал". Також можна вимкнути графічний інтерфейс користувача на сервері терміналів. Щоб дізнатися більше про програму ESET Mail Security, інстальовану на сервері терміналів, див. розділ Вимкнути графічний інтерфейс користувача на сервері терміналів.

Режим кольору

У розкривному меню виберіть колірну схему графічного інтерфейсу користувача ESET Mail Security:

- **Той самий, що й колір системи**: колірна схема ESET Mail Security заснована на параметрах операційної системи.

- **Темна**: для ESET Mail Security використовуватиметься темна колірна схема (темний режим).

- **Світла**: для ESET Mail Security використовуватиметься світла колірна схема (стандартна).

Відображати стартовий екран під час запуску — Вимкніть цей параметр, якщо не потрібно показувати стартовий екран під час запуску головного вікна ESET Mail Security, наприклад, під час входу в систему.

Використовувати звуковий сигнал — ESET Mail Security відтворюватиме звукове попередження про важливі події, що трапляються під час сканування (наприклад, коли виявляється загроза або завершується перевірка).

Додати до контекстного меню: якщо цей параметр увімкнуто, елементи керування ESET Mail Security буде додано в контекстне меню. Контекстне меню відображається, якщо натиснути об'єкт (файл) правою кнопкою миші. Меню містить перелік усіх дій, які можна виконати з об'єктом.

Відомості про ліцензію

Якщо цей параметр увімкнено, відображатимуться повідомлення та сповіщення щодо ліцензії.

Показати інформацію про ліцензію — Якщо цей параметр вимкнуто, дата завершення терміну дії ліцензії не буде відображатися на екранах **Статус захисту** й **Довідка та підтримка**.

Налаштування статусів програми, пов'язаних із ліцензією: відкриває список статусів програми, пов'язаних із ліцензією.

Налаштування сповіщень про ліцензію — Якщо цей параметр вимкнуто, сповіщення й повідомлення відображатимуться лише після завершення терміну дії ліцензії.

Параметри доступу — Щоб забезпечити високий рівень безпеки, можна запобігти несанкційованим змінам за допомогою засобу **"Параметри доступу"**.

Оболонка ESET — Щоб налаштувати права доступу до параметрів продукту, функцій і даних, потрібно змінити політику виконання оболонки ESET у eShell.

Піктограма в області сповіщень Windows

Відновити всі параметри у цьому розділі?

Параметри доступу

Для максимальної безпеки системи важливо правильно налаштувати ESET Mail Security. Будь-які некваліфіковані зміни можуть призвести до проблем або навіть утрати важливих даних. Щоб уникнути внесення таких змін, конфігурацію ESET Mail Security можна захистити паролем.

Щоб видалити ESET Mail Security, доступ до якої захищено паролем, необхідно ввести цей пароль. Якщо цього не зробити, ви не зможете видалити ESET Mail Security.

Параметри захисту паролем

Блокує/розблоковує параметри налаштування програми. Натисніть, щоб відкрити вікно **Налаштування пароля**.

Установити пароль

Щоб установити або змінити пароль для захисту параметрів налаштування, натисніть **Установити**. Щоб захистити параметри налаштування ESET Mail Security та запобігти несанкційованим змінам, необхідно встановити новий пароль. Щоб змінити наявний пароль, уведіть його в полі **Старий пароль**, двічі введіть новий пароль у полях **Новий пароль** і **Підтвердити пароль**, а тоді натисніть **ОК**. Цей пароль потрібно буде вказувати для внесення будь-яких подальших змін ESET Mail Security.

Вимагати повних прав адміністратора для обмежених облікових записів адміністраторів

Виберіть цю опцію, щоб поточний користувач (без прав адміністратора) мав указати облікові дані адміністратора для зміни певних параметрів, як-от вимкнення модулів захисту.

Якщо пароль у розділі "Параметри доступу" буде змінено, а вам необхідно імпортувати файл конфігурації у форматі XML (підписаний раніше старим паролем) за допомогою командного рядка ESET CMD, підпишіть його знову, використовуючи поточний пароль. Так ви зможете використовувати старий файл конфігурації, не експортуючи його на інший комп'ютер з ESET Mail Security перед імпортом.

Оболонка ESET

Щоб налаштувати права доступу до параметрів продукту, функцій і даних, потрібно змінити **політику виконання оболонки ESET** у eShell. За замовчуванням використовується параметр **Обмежене використання сценаріїв**, але за потреби його можна змінити на "Вимкнуто", "Лише для читання" або "Повний доступ".

Вимкнуто

eShell узагалі не можна використовувати. У контексті ui eshell дозволено лише конфігурацію самої eShell. Ви можете налаштовувати зовнішній вигляд eShell, але не матимете доступу до параметрів продукту або даних.

Лише для читання

eShell можна використовувати як інструмент моніторингу. Ви можете переглядати всі параметри в інтерактивному й пакетному режимах, але без можливості змінювати будь-які параметри, функції або дані.

Обмежене використання сценаріїв

В інтерактивному режимі ви можете переглядати й змінювати всі параметри, функції та дані. У пакетному режимі eShell працюватиме так, ніби ви перебуваєте в режимі лише для читання. Проте якщо ви використовуєте підписані пакетні файли, то можете змінювати параметри й дані.

Повний доступ

Доступ до всіх параметрів необмежений в інтерактивному й пакетному режимах (під час виконання пакетних файлів). Ви можете переглядати й змінювати будь-які параметри. Щоб

запустити eShell з повним доступом, потрібно використовувати обліковий запис адміністратора. Якщо ввімкнено службу захисту користувачів (UAC), вищий рівень доступу також знадобиться.

Вимкнення графічного інтерфейсу на сервері терміналів

У цьому розділі описано, як вимкнути графічний інтерфейс програми ESET Mail Security, запущеної на сервері терміналів Windows для роботи із сеансами користувача.

Зазвичай графічний інтерфейс ESET Mail Security запускається щоразу, коли віддалений користувач входить на сервер і створює сеанс термінала. Це, зазвичай, небажано на серверах терміналів. Якщо потрібно вимкнути графічний інтерфейс для сеансів термінала, це можна зробити за допомогою eShell, виконавши команду `set ui ui gui-start-mode none`. Це переведе графічний інтерфейс у режим термінала. Нижче наведено два доступні режими запуску графічного інтерфейсу.

```
set ui ui gui-start-mode full

set ui ui gui-start-mode none
```

Щоб дізнатися, який режим зараз використовується, виконайте команду `get ui ui gui-start-mode`.

> Якщо ви інсталювали ESET Mail Security на сервері Citrix, радимо використовувати параметри, описані в статті бази знань.

Піктограма в області сповіщень Windows

Щоб відкрити найважливіші параметри налаштування й функції, клацніть правою кнопкою миші піктограму в системному треї (в області сповіщень Windows).

> Щоб мати доступ до меню в системному треї (область сповіщень Windows), переконайтеся, що для режиму запуску елементів інтерфейсу користувача вибрано значення "Повний".

Додаткова інформація

Відкриється сторінка моніторингу, на якій відображатимуться поточні статуси захисту й повідомлення.

Тимчасово вимкнути захист

Відкриється діалогове вікно з підтвердженням, у якому можна вимкнути захист від вірусів і шпигунських програм, який попереджає атаки, контролює обмін даними між файлами, Інтернетом та електронною поштою. У розкривному меню **Часовий інтервал** можна вказати, скільки часу буде вимкнено захист.

Додаткові параметри

Відкрийте додаткові параметри ESET Mail Security.

Файли журналу

Містить інформацію про важливі програмні події та зведені дані про виявлені загрози.

Відновити розташування вікна

Відновити стандартний розмір вікна ESET Mail Security і його розміщення на екрані.

Режим кольору

Відкриває параметри інтерфейсу користувача, де можна змінити колір графічного інтерфейсу користувача.

Перевірити наявність оновлень

Запускає оновлення модулів, щоб забезпечити достатній рівень захисту від шкідливого коду.

Про програму

Надає інформацію про систему, інстальовану версію й інстальовані модулі програми ESET Mail Security, а також дату завершення терміну дії ліцензії. Інформацію про операційну систему й системні ресурси див. унизу сторінки.

Сповіщення

Сповіщення на робочому столі й спливні підказки призначені лише для інформування та не потребують взаємодії з користувачем. Вони відображаються в області сповіщень у нижньому правому куті екрана. Додаткові параметри, як-от час відображення сповіщень і прозорість вікна, можна змінити нижче.

Для керування сповіщеннями ESET Mail Security, відкрийте розділ **Додаткові параметри** (**F5**) > **Сповіщення**. Можна налаштувати такі типи сповіщень:

Статуси програми: клацніть **Змінити**, щоб вибрати статуси програм, які відображатимуться в домашньому розділі головного вікна програми.

Сповіщення на робочому столі: невеликі спливаючі вікна поруч із панеллю завдань системи.

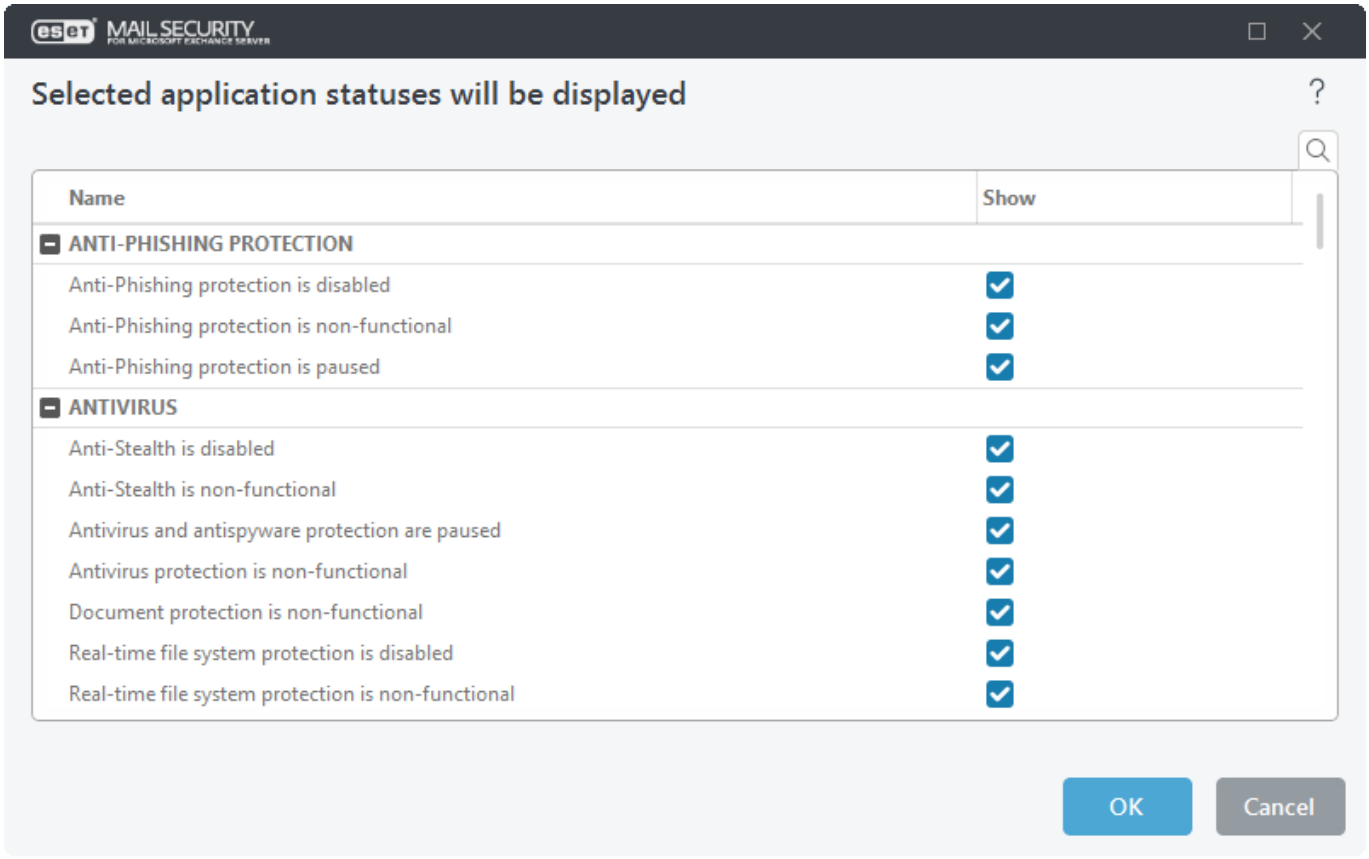
Інтерактивні сповіщення: вікна сповіщень і вікна повідомлень, які потребують втручання користувача.

Пересилання (сповіщення електронною поштою): сповіщення надсилаються на вказану адресу електронної пошти.

Статуси програми

У цьому діалоговому вікні можна вибрати або скасувати вибір відображення статусів програм. Наприклад, якщо призупинити використання захисту від вірусів і шпигунських програм, це призведе до зміни статусу захисту, і цей статус з’явиться на сторінці Моніторинг. Статус

програми також відображатиметься, якщо продукт не активовано, або термін дії ліцензії завершиться. Статусами програм можна керувати за допомогою політик ESET PROTECT.



Вимкнені повідомлення та статуси

Повідомлення з підтвердженням

Показує список повідомлень із підтвердженням, відображення яких можна ввімкнути або вимкнути.

Статуси програми

Дає змогу ввімкнути або вимкнути відображення статусу на сторінці Моніторинг у головному меню.

Сповіщення на робочому столі

Сповіщення на робочому столі відображаються в невеликих вікнах сповіщень поруч із панеллю завдань системи. За замовчуванням вікно відображається протягом 10 секунд, а потім поступово зникає. ESET Mail Security повідомляє користувачу про успішні оновлення продукту, нові підключені пристрої, сканування на віруси, завершення виконання завдання або нові виявлені об’єкти.

Показувати сповіщення на робочому столі

Рекомендуємо не вимикати цей параметр, щоб постійно отримувати інформацію про виникнення нових подій.

Сповіщення на робочому столі

Клацніть **Змінити**, щоб вибрати сповіщення на робочому столі, які будуть відображатися для різних подій.

Увімкніть опцію **Не показувати сповіщення під час роботи програм у повноекранному режимі**, щоб заборонити відображення всіх неінтерактивних сповіщень.

Показувати час у секундах

Установіть тривалість відображення сповіщень. Значення має бути в діапазоні від 3 до 30 секунд.

Прозорість

Дає змогу задати відсоток прозорості сповіщень. Підтримуваний діапазон: від 0 (без прозорості) до 80 (дуже високий рівень прозорості).

У розкривному меню**Мінімальна детальність подій для відображення** можна вибрати рівень важливості повідомлень про загрози та сповіщень. Доступні вказані нижче опції.

- **Діагностика** – запис інформації, необхідної для налаштування програми й усіх зазначених вище записів.
- **Інформація** – запис інформаційних повідомлень, зокрема повідомлень про успішні оновлення, а також усіх зазначених вище записів.
- **Попередження** – запис критичних помилок і попереджувальних повідомлень.
- **Помилки** – запис критичних та інших помилок (як-от "Помилка завантаження файлу").
- **Критичні помилки** – запис лише критичних помилок.

У **системах із багатьма користувачами**, які дозволяють їх одночасне підключення, можна вказати, хто з них отримуватиме системні й інші сповіщення. Зазвичай це буде системний або мережевий адміністратор. Ця опція буде особливо корисною для серверів терміналів, для яких усі системні сповіщення надсилатимуться адміністратору.

Дозволити показ сповіщень на екрані – сповіщення показуватимуться на екрані; для їх перегляду потрібно натиснути комбінацію клавіш Alt+Tab.

Налаштування

У цьому вікні можна налаштувати повідомлення, які використовуватимуться в сповіщеннях.

Повідомлення в сповіщенні — Повідомлення, яке відображається за замовчуванням у підписі сповіщень.

Виявлений об’єкт

Не закривати сповіщення про виявлений об’єкт автоматично

Вмикає сповіщення про виявлені об’єкти, які залишатимуться на екрані, доки ви не закриєте їх

уручну.

Використовувати повідомлення за замовчуванням

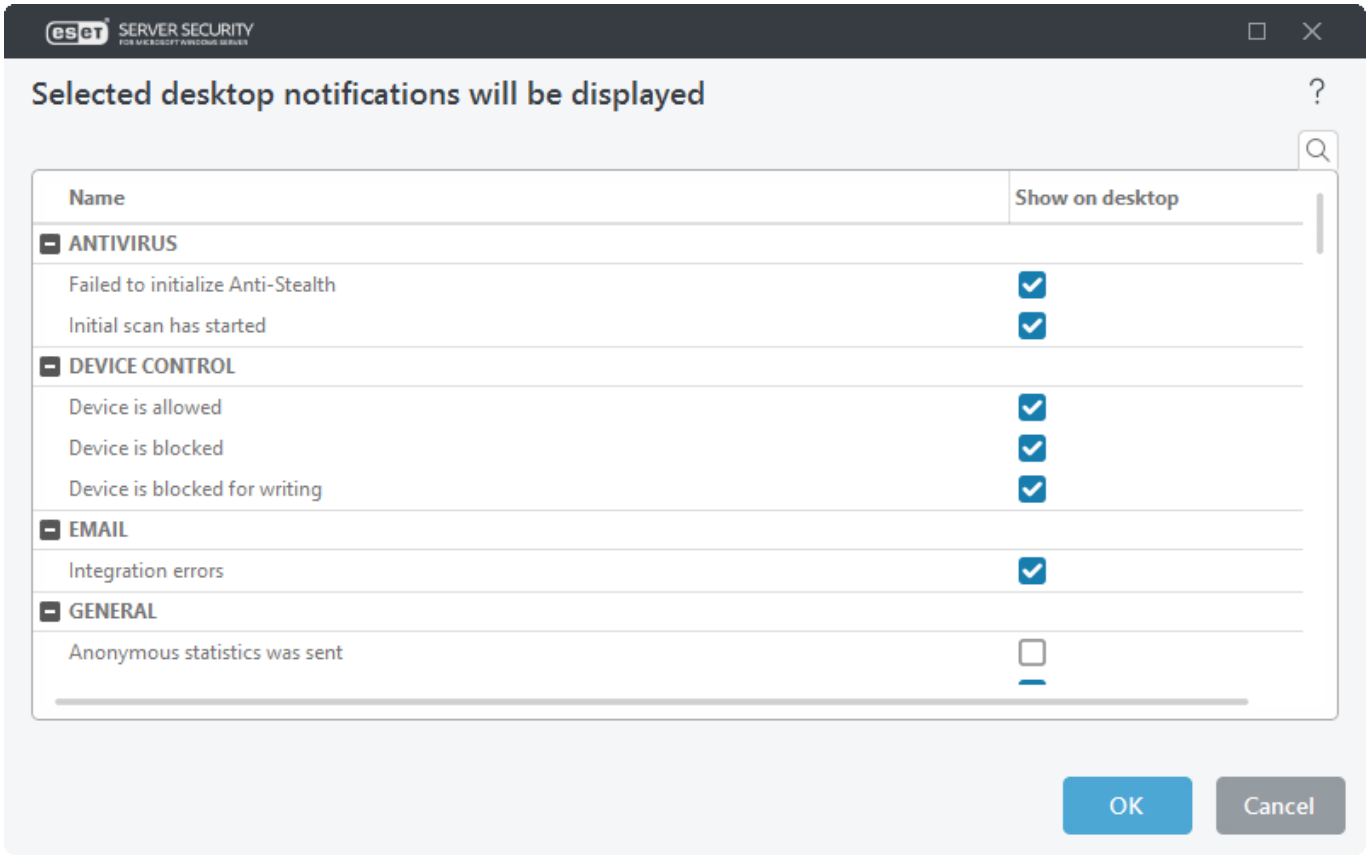
Можна вимкнути повідомлення за замовчуванням і налаштувати власне сповіщення про виявлений об’єкт, яке відображатиметься в разі блокування загрози.

Повідомлення в сповіщенні про виявлений об’єкт

Уведіть текст повідомлення, яке відображатиметься в разі блокування виявленого об’єкта.

Сповіщення на робочому столі

Можна налаштувати сповіщення ESET Mail Security, які відображатимуться на робочому столі.



Інтерактивні сповіщення

Ви можете налаштувати, як ESET Mail Security опрацьовуватиме повідомлення про загрози й системні сповіщення (як-от повідомлення про успішні оновлення). Наприклад, **тривалість** відображення цих повідомлень в області сповіщень Windows і їхню **прозорість** (це стосується лише систем, які підтримують сповіщення).

Показати інтерактивні сповіщення

Вимкніть цю функцію, щоб заборонити ESET Mail Security відображення сповіщень в області сповіщень Windows.

Список інтерактивних сповіщень

Корисно для автоматизації. Зніміть прапорець **Запитувати користувача** для елементів, які необхідно автоматизувати, і виберіть дію для виконання замість відтворення вікна сповіщення, що очікує на взаємодію.

Вікна повідомлень використовуються для відображення коротких текстових повідомлень або запитань.

Автоматично закривати вікна повідомлень

Автоматичне закриття вікон сповіщень через певний проміжок часу. Якщо вікна сповіщень не закрито вручну, їх буде закрито автоматично після завершення вказаного періоду часу.

Повідомлення з підтвердженням

Якщо натиснути **Змінити**, відкриється вікно зі списком повідомлень із підтвердженнями, які ESET Mail Security відображатиме перед виконанням дії. Установіть прапорці, щоб налаштувати повідомлення з підтвердженнями.

Пересилання

ESET Mail Security може автоматично надсилати сповіщення електронною поштою, коли ставатимуться події з вибраним рівнем деталізації.

Пересилати на електронну пошту

Щоб активувати сповіщення електронною поштою, увімкніть параметр "Пересилати сповіщення на електронну пошту".

Переадресовані сповіщення

Виберіть сповіщення на робочому столі, які пересилатимуться на електронну пошту.

Параметри електронної пошти

Мінімальна детальність повідомлень: визначає мінімальний рівень детальності сповіщень, які потрібно надсилати.

• **Діагностика**: запис у журнал інформації, необхідної для налаштування програми й усіх зазначених вище записів.

• **Інформаційні записи**: запис інформаційних повідомлень (наприклад, щодо нестандартних подій у мережі), зокрема повідомлень про успішні оновлення, а також усіх зазначених вище записів.

• **Попередження**: запис критичних помилок і попереджень (наприклад, повідомлення про те, що модуль Anti-Stealth працює неправильно або не вдалося виконати оновлення).

• **Помилки** – запис критичних та інших помилок (як-от "Помилка завантаження файлу").

• **Критичні помилки** – запис лише критичних помилок.

Надсилати кожне сповіщення окремим електронним листом

Якщо цю опцію ввімкнено, із кожним сповіщенням одержувач отримуватиме новий електронний лист. Це може призвести до отримання чималої кількості електронних листів за короткий проміжок часу.

Інтервал, через який будуть надсилатися нові сповіщення електронною поштою (хв.)

Після завершення часу, заданого інтервалом у хвилинах, електронною поштою буде надіслано нове сповіщення. Якщо вибрати значення 0, сповіщення надходитимуть миттєво.

Адреса відправника

Уведіть адресу відправника, яка відображатиметься в заголовку сповіщень електронною поштою. Одержувач бачитиме її в полі **Від**.

Адреса одержувача

Укажіть адресу електронної пошти одержувача, яка відображатиметься в заголовку електронних листів із сповіщеннями. Щоб відокремити кілька адрес електронної пошти, використовуйте крапку з комою ";".

Сервер SMTP

Ім’я сервера SMTP, що використовується для надсилання попереджень про загрози й сповіщень. Зазвичай це ім’я вашого Microsoft Exchange Server.

ESET Mail Security підтримує сервери SMTP з протоколом шифрування TLS.

Ім’я користувача та пароль

Якщо сервер SMTP потребує автентифікації, у цих полях слід указати дійсне ім’я користувача та пароль, які забезпечують доступ до сервера.

Увімкнути TLS

Увімкніть попередження про загрози й сповіщення, що підтримують шифрування TLS.

Перевірка підключення до SMTP-сервера

На електронну адресу одержувача буде надіслано перевірочний електронний лист.

Формат повідомлень

Обмін повідомленнями між програмою й віддаленим користувачем або системним адміністратором здійснюється через електронну пошту або локальну мережу (за допомогою служби Windows Messenger). Формат попереджень про загрози й сповіщень за замовчуванням є оптимальним для більшості ситуацій. За певних обставин може виникнути необхідність змінити формат повідомлень про події.

Формат повідомлень про події

Укажіть формат сповіщень про події, що надсилаються електронною поштою.

Формат попереджень про загрози

Попередження про загрози й сповіщення мають попередньо визначений формат за замовчуванням. Радимо не змінювати цей формат. Проте за певних обставин (наприклад, якщо у вас автоматична система опрацювання електронної пошти) може виникнути необхідність змінити формат повідомлень.

Ключові слова (рядки, розділені символами %) замінюються в повідомленні визначеною фактичною інформацією. Доступні такі ключові слова:

- %TimeStamp%: дата й час реєстрації події.
- %Scanner%: залучений модуль.
- %ComputerName%: ім’я комп’ютера, на якому зареєстровано оповіщення.
- %ProgramName%: програма, робота якої призвела до оповіщення.
- %DetectionObject%: ім’я інфікованого файлу, повідомлення тощо.
- %DetectionName%: ідентифікатор вірусу.
- %ErrorDescription%: опис події, не пов’язаної з вірусами.

Ключові слова **%DetectionObject%** і **%DetectionName%** використовуються лише в попередженнях про загрози, а **%ErrorDescription%** – лише в повідомленнях про події.

Набір символів

У розкривному меню можна вибрати тип кодування. Повідомлення електронної пошти буде перетворено відповідно до вибраного кодування символів. Перетворює вміст електронного листа в кодування ANSI відповідно до регіональних параметрів Windows (наприклад, windows-1250, Юнікод (UTF-8), ACSII (7 біт) або японська (ISO-2022-JP)). У результаті "á" буде замінено на "a", а невідомий символ — на "?".

Використовувати кодування даних у формат Quoted-printable

Джерело електронного листа кодується у форматі Quoted-Printable (QP), який використовує символи ASCII та може правильно передавати електронною поштою національні спеціальні символи у 8-бітному форматі (áéíóú).

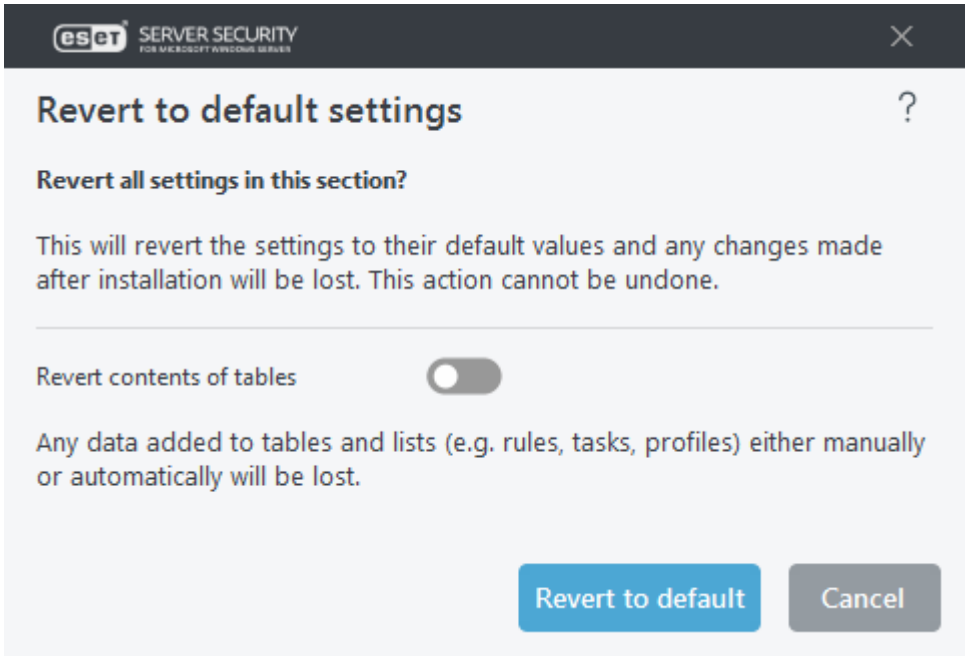
Відновити параметри за замовчуванням

Ви можете відновити параметри до значень за замовчуванням у меню **Додаткові параметри**. Є два варіанти. Можна відновити значення за замовчуванням всіх параметрів або лише для певного розділу (параметри в інших розділах не зміняться).

Відновити всі параметри — Усі параметри з усіх розділів меню "Додаткові параметри" буде відновлено до значень, які вони мали після інсталяції ESET Mail Security. Цю опцію можна описати як відновлення заводських налаштувань.

Коли ви натиснете **Відновити значення за замовчуванням**, усі внесені зміни буде втрачено. Цю дію неможливо скасувати.

Відновити всі параметри у цьому розділі: відновлення параметрів модуля у вибраному розділі до значень. Усі зміни, внесені в цей розділ, буде втрачено.



Відновити вміст таблиць — Якщо цей параметр увімкнено, додані вручну чи автоматично правила, завдання або профілі буде втрачено.

Довідка та підтримка

ESET Mail Security містить інструменти для виправлення неполадок і технічну інформацію, що допоможе у вирішенні проблем, які можуть виникнути.

Інстальований продукт

Інформація про продукт і ліцензію

- Про ESET Mail Security. Показує інформацію про вашу копію ESET Mail Security.
- Виправлення неполадок із продуктом. Пошук вирішень найпоширеніших проблем. Перш ніж звертатися до служби технічної підтримки, радимо прочитати цей розділ.
- Виправлення неполадок із ліцензією. Пошук вирішень проблем з активацією або зміною ліцензії.
- Змінити ліцензію. Натисніть, щоб відкрити вікно активації й активувати продукт.

Довідкні сторінки

Відкриває сторінки онлайн-довідки для продукту ESET Mail Security.

База знань

Пошук у базі знань ESET. База знань ESET містить відповіді на найпоширеніші запитання та рекомендовані вирішення різних проблем. Технічні спеціалісти ESET регулярно оновлюють базу знань, завдяки чому вона є найпотужнішим інструментом для вирішення різних проблем.

Служба технічної підтримки

• Розширене ведення журналів. Створення розширених журналів для всіх доступних функцій, які допомагають розробникам діагностувати й вирішувати проблеми.

• Звернутися до служби підтримки. Якщо ви не можете знайти відповідь на своє запитання, зверніться до нашої служби технічної підтримки.

• Інформація для служби технічної підтримки. Показує інформацію про продукт (назву, версію тощо) для служби технічної підтримки.

• ESET Log Collector. ESET Log Collector – це програма, яка автоматично збирає інформацію, зокрема дані про конфігурацію й журнали із сервера, щоб допомогти швидше вирішувати проблеми.

Надіслати запит до служби технічної підтримки

Для надання максимально швидкої та якісної допомоги ESET потрібні інформація про вашу конфігурацію ESET Mail Security, докладна інформація про систему, запущені процеси (файл журналу ESET SysInspector) і дані реєстру. ESET використовуватиме ці дані лише для надання технічної підтримки клієнту. Цей параметр також можна налаштувати в меню **Додаткові параметри** (**F5**) > **Інструменти** > **Діагностика** > **Технічна підтримка**.

Якщо ви вирішите надати дані про систему, заповніть і надішліть веб-форму, інакше ваш запит не буде створено, а дані про систему буде втрачено.

Під час надсилання веб-форми дані про налаштування системи надсилатимуться в ESET. Виберіть **Завжди надсилати ці дані**, щоб запам’ятати дію для цього процесу.

Не надсилати дані: Використайте цю опцію, якщо не хочете надсилати дані. Вас буде переспрямовано на веб-сторінку служби технічної підтримки ESET.

Про ESET Mail Security

У цьому вікні наведено докладні відомості про інстальовану версію ESET Mail Security. У верхній частині вікна міститься інформація про операційну систему та системні ресурси, поточного користувача й повне ім’я комп’ютера.

Інстальовані компоненти

Містить інформацію про модулі, де можна переглянути список інстальованих компонентів і їхні деталі. Натисніть **Копіювати**, щоб скопіювати список у буфер обміну. Це може бути корисно під час виправлення неполадок або звернення до служби технічної підтримки.

Глосарій

Щоб дізнатися більше про технічні умови, загрози й безпеку Інтернету, відвідайте сторінку Глосарій.

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 погоджуєтеся 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 ЦІЄЇ УГОДИ, РОЗУМІННЯ ЇЇ УМОВ І ПОЛОЖЕНЬ ТА ВАШУ ЗГОДУ НА ЇХ 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 інсталювати. Ви маєте інсталювати 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 інсталюєте 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 інсталюватися 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 погоджуєтеся 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 інсталювати 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.

c) **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.

e) **OEM-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.

f) **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.

g) **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 потрібне 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:

a) **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 інсталюються 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. Оновлення Програмного забезпечення не надаватимуться після завершення терміну служби будь-яких його функцій, визначених у Політиці EOL.

b) **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 ("Загроз"). 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 Інофрмації. 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’язуєтеся 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’язуєтеся дотримуватися наведених нижче обмежень.

a) 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 погоджуєтеся 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 погоджуєтеся 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 погоджуєтеся 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 договірного 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 (a) 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 погоджуєтеся, 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, НЕДБАЛІСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ІНСТАЛЯЦІЇ, ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ

ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНІМ 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 ДОЧІРНІХ 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**.

a) 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 a) Угоди; або

ii. Користувач і (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 погоджуєтеся 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 письмовий 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 погоджуєтеся, 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, сповіщенням 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 припинете 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

Захист персональних даних має особливо важливе значення для компанії ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic, запис № 3586/B у комерційному реєстрі окружного суду м. Братислави I, розділ Sro, реєстраційний номер: 31333532) як Контролера даних (далі — "ESET" або "Ми"). Ми прагнемо забезпечити відповідність вимогам до прозорості, установленим у Загальному регламенті ЄС щодо захисту даних (далі — "GDPR"). З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів (далі — "Кінцевий користувач" або "Ви") як суб'єктів даних про наведені нижче аспекти захисту персональних даних.

- Правові основи для обробки персональних даних.
- Обмін даними та конфіденційність.
- Безпека даних.
- Права суб'єкта даних.
- Обробка персональних даних.

- Контактна інформація.

Обробка персональних даних

Служби компанії ESET реалізовані в нашому продукті й надаються згідно з EULA, однак деякі з них потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов'язаний із наданням наших послуг. Ми надаємо різні служби, описані в Ліцензійній угоді та документації. 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:
    - загрози, 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;
    - інформація про пристрої в локальній мережі, зокрема їх тип, виробник, модель і (або) імена;
    - інформація щодо використання Інтернету, зокрема IP-адреса й географічні дані, IP-пакети, URL-адреси й кадри Ethernet;
    - файли 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.

Обмін даними та конфіденційність

Ми не передаємо Ваші дані третім сторонам. Однак ESET — це компанія, яка працює в усьому світі через афілійовані компанії або партнерів, які входять до нашої мережі розповсюдження, обслуговування та підтримки. Інформація про ліцензування, розрахунки й технічну підтримку, яка оброблюється ESET, може передаватись афілійованим компаніям чи партнерам або надходити від них. Це необхідно для виконання положень Ліцензійної угоди з кінцевим користувачем, таких як надання послуг або підтримки.

У компанії ESET ми віддаємо перевагу обробці даних на території Європейського Союзу (ЄС). Однак, залежно від Вашого місцезнаходження (використання наших продуктів і/або служб за межами ЄС) та (або) вибраної Вами служби, нам, можливо, доведеться передати Ваші дані в країну за межами ЄС. Наприклад, ми використовуємо служби третіх сторін для виконання обчислень у хмарі. У таких випадках Ми ретельно вибираємо наших постачальників послуг і забезпечуємо належний рівень захисту даних шляхом укладення договорів, а також за допомогою технічних та організаційних заходів. Як правило, Ми діємо згідно зі стандартними та додатковими (за потреби) договірними положеннями ЄС.

Для деяких країн за межами ЄС, наприклад Великобританії та Швейцарії, уже визначено аналогічний рівень захисту даних. Завдяки відповідному рівню захисту для передачі даних у ці країни не потрібен спеціальний дозвіл або угода.

Права суб’єкта захисту персональних даних

Права кожного Кінцевого користувача мають велике значення, і Ми хотіли б повідомити Вам, що всі Кінцеві користувачі (з будь-якої країни ЄС або за його межами) мають наведені нижче права, гарантовані ESET. Щоб скористатися своїми правами суб’єкта даних, зв’яжіться з нами за допомогою форми служби підтримки або електронною поштою за адресою dpo@eset.sk. Для ідентифікації Ми попросимо надати таку інформацію: ім’я, адресу електронної пошти та, за наявності, ліцензійний ключ або номер клієнта й місце роботи. Не надсилайте нам будь-які інші персональні дані, наприклад дату народження. Хочемо зазначити, що для обробки Вашого запиту, а також для ідентифікації Ми оброблятимемо Ваші персональні дані.

Право відкликати згоду. Право відкликати згоду застосовується до даних, які обробляються лише за згодою. Якщо Ми обробляємо персональні дані на підставі Вашої згоди, Ви маєте право відкликати її в будь-який час без пояснення причин. Відкликання згоди застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до відкликання.

Право на заперечення. Право на заперечення застосовується, коли обробка даних здійснюється на основі законних інтересів компанії ESET або третьої сторони. Якщо Ми обробляємо персональні дані для захисту законного інтересу, Ви, як суб’єкт даних, маєте право в будь-який час заперечити проти зазначеного нами законного інтересу й обробки Ваших персональних даних. Заперечення застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до заперечення. Якщо Ми обробляємо Ваші персональні дані в цілях прямого маркетингу, наводити причини для заперечення не потрібно. Це також стосується формування профілів, оскільки воно пов’язане з прямим маркетингом. У всіх інших випадках Ми просимо Вас коротко повідомити нам, чому Ви не згодні із законним інтересом компанії ESET до обробки Ваших персональних даних.

Зверніть увагу, що в деяких випадках, незважаючи на відкликання Вашої згоди, Ми маємо право на подальшу обробку Ваших персональних даних на іншій правовій основі, наприклад

для виконання умов договору.

Право на доступ. Як суб’єкт даних Ви маєте право в будь-який час безкоштовно отримати інформацію про свої дані, що зберігаються компанією ESET.

Право на виправлення. Якщо Ваші персональні дані, які перебувають у нашому розпорядженні, містять помилку, Ви маєте право на її виправлення.

Право на видалення й обмеження обробки. Як суб’єкт даних Ви маєте право вимагати видалення чи обмеження обробки Ваших персональних даних. Якщо для обробки Ваших персональних даних не залишиться правових підстав (наприклад, договору чи Вашої згоди), ми негайно видалимо їх. Ваші персональні дані також буде видалено в кінці терміну зберігання, щойно вони більше не будуть потрібні для вказаних для них цілей.

Якщо Ми використовуємо Ваші персональні дані виключно з метою прямого маркетингу, і Ви відкликали свою згоду або заперечили проти основного законного інтересу компанії ESET, Ми обмежимо обробку Ваших персональних даних шляхом включення Ваших контактних даних у наш внутрішній чорний список із метою уникнення небажаних контактів. Інакше Ваші персональні дані буде видалено.

Зверніть увагу, що Ми можемо бути зобов’язані дотримуватись умов і термінів зберігання даних, установлених законодавчими або наглядовими органами. Умови й терміни зберігання даних також може бути визначено в законодавстві Словаччини. Після завершення відповідного періоду часу дані видалятимуться звичайним чином.

Право забезпечити можливість переносу даних. Як суб’єкт даних Ви можете отримати Ваші персональні дані, які обробляє компанія ESET, у форматі XLS.

Право на подання скарги. Як суб’єкт даних Ви маєте право в будь-який час звертатися зі скаргою до наглядових органів влади. ESET є суб'єктом регулювання відповідно до законів Словацької Республіки. Відповідним наглядовим органом є Управління з питань захисту персональних даних Словацької Республіки, розташованим за адресою Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Контактна інформація

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