ESET Cloud Office Security

Посібник користувача

Натисніть тут щоб відкрити версію цього документа

Digital Security
Progress. Protected.

© ESET, spol. s r.o., 2023.

ESET Cloud Office Security розроблено компанією ESET, spol. s r.o.

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

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

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

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

REV. 20.12.2023

1 Огляд ... 1
1.1 Основні функції ... 2
1.2 Нові функції та можливості ... 5
1.3 Інтеграція ... 7
2 Специфікації ... 7
2.1 Вимоги ... 8
2.2 Підтримувані плани Microsoft 365 ... 8
2.3 Підтримувані тарифні плани Google Workspace ... 9
2.4 Підтримувані веб-браузери ... 9
2.5 Обмеження й політика збереження даних ... 10
3 Ліцензування для ESET Cloud Office Security ... 11
3.1 ESET Business Account ... 12
3.1 Створення нового облікового запису ESET Business Account ... 12
3.1 Додавання ліцензії ESET Cloud Office Security в ESET Business Account ... 13
3.1 Керувати ESET Business Account ... 14
3.2 ESET MSP Administrator ... 15
4 Активувати ESET Cloud Office Security ... 15
4.1 Деактивувати ESET Cloud Office Security ... 17
5 Керування клієнтами в меню ... 18
5.1 Додавання першого клієнта ... 20
5.2 Клієнт Microsoft 365 ... 23
5.3 Клієнт Google Workspace ... 26
5.4 Видалити клієнта з ESET Cloud Office Security ... 32
5.5 Видалення ESET Cloud Office Security з порталу Azure ... 33
6 Навігація інтерфейсом ESET Cloud Office Security ... 33
7 ESET LiveGuard Advanced ... 35
8 Панель інструментів ... 36
9 Користувачі ... 38
10 Команди й сайти ... 40
11 Виявлені об’єкти ... 41
12 Звіти ... 42
13 Карантин ... 45
14 Журнали сканування ... 47
15 Політики ... 48
15.1 Параметри захисту для Exchange Online ... 51
15.2 Параметри захисту для Gmail ... 54
15.3 Параметри захисту для OneDrive ... 57
15.4 Параметри захисту для Google Диск ... 58
15.5 Параметри захисту для груп команди ... 59
15.6 Параметри захисту для сайтів SharePoint ... 60
15.7 Параметри захисту для ESET LiveGuard Advanced ... 61
15.8 Звітність і захист на основі машинного навчання ... 62
16 Керування ліцензією ... 64
16.1 Доступ користувача ESET Cloud Office Security до певної компанії ... 66
17 Журнал аудиту ... 67
18 Надіслати відгук ... 68
19 Технічна підтримка ... 68
20 Доступність служби ... 69

20.1 Безпека для ESET Cloud Office Security 69
20.2 Умови використання 74
20.2 Ліцензійна угода з кінцевим користувачем 79
20.2 Угода про обробку даних 86
20.2 Стандартні договірні положення 89
20.3 Політика конфіденційності 112

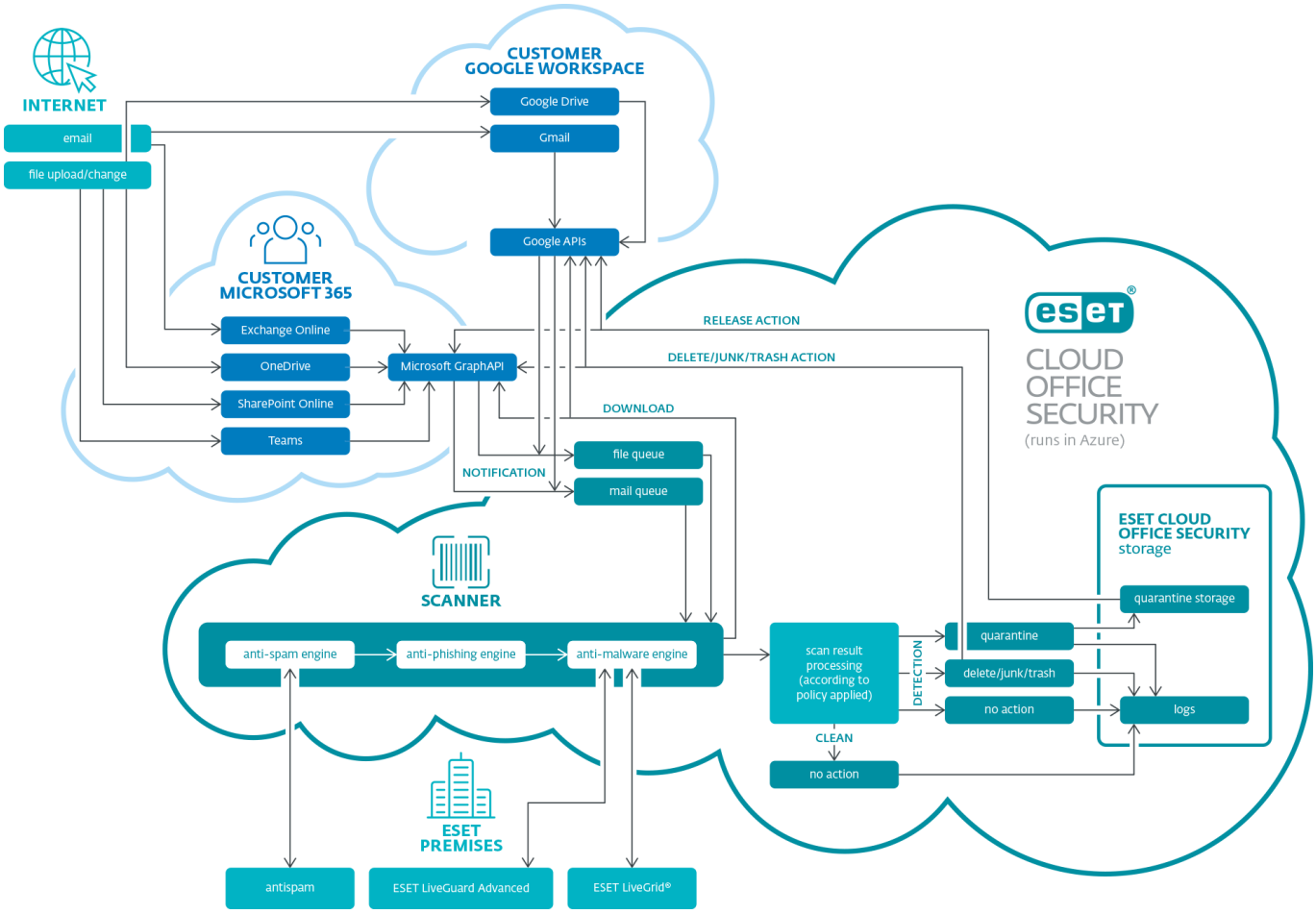
Огляд

ESET Cloud Office Security — це хмарна служба в Microsoft Azure із підтримкою мультітенантності й можливості масштабування. ESET Cloud Office Security надається як продуктSoftware-as-a-Service (SaaS), який повністю працює у хмарі, не потребуючи обладнання. Це комплексна комбінація фільтрації спаму, сканування на наявність шкідливого програмного забезпечення й захисту від фішинг-атак, яка дає змогу захистити вашу компанію від шкідливого ПЗ, мінімізує негативний вплив сторонніх повідомлень на повсякденну діяльність і блокує використання вхідних зовнішніх електронних листів як каналу для цільових атак.

Служби безпеки ESET Cloud Office Security стануть у пригоді для провідних постачальників хмарних платформ і забезпечать комплексний захист електронної пошти завдяки найсучаснішим механізмам захисту від шкідливого програмного забезпечення й ESET LiveGuard Advanced. Це рішення забезпечує розширений захист від загроз за допомогою хмарної пісочниці: підозрілі зразки аналізуються в ізольованому середовищі.

Архітектура ESET Cloud Office Security дає змогу швидко ініціювати захист через підключення до вашої хмарної платформи — Microsoft 365 і Google Workspace. Це дає вам можливість керувати захистом за допомогою веб-консолі, доступної з будь-якого місця.

ESET Cloud Office Security забезпечує розширений превентивний захист корпоративних програм Microsoft 365: Exchange Online, OneDrive, SharePoint Online і Teams. Такий самий захист надається вашим програмам Google Workspace — Gmail і Google Drive.



ESET Cloud Office Security захищає OneDrive і поштову скриньку ліцензованих користувачів, а також групи команди і сайти SharePoint. Кожне сховище цих програм Microsoft 365 захищено незалежно від того, хто передав файл або надіслав електронний лист. Вміст захищено незалежно від його автора. Автор може бути гостьовим користувачем задля забезпечення найкращого захисту.

Основні функції

У таблиці нижче наведено список доступних функцій ESET Cloud Office Security .

Мультітенантність	На одній консолі ESET Cloud Office Security можна захистити кілька клієнтів Microsoft 365 і Google Workspace та керувати ними. Azure Active Directory (Azure AD) впорядковує об’єкти (наприклад, користувачів і програми) в групи, які називаються клієнтами. Клієнти дозволяють задавати політики для користувачів і програм у вашій організації, що дозволяє забезпечити їх відповідність політикам безпеки й операційним політикам.

Антиспам	Антиспам — це важливий компонент будь-якого поштового сервера. ESET Cloud Office Security використовує найсучасніший механізм антиспаму, який захищає від спаму й фішингових повідомлень із надзвичайно високим показником виявлення. ESET Cloud Office 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 Cloud Office Security працює в хмарі, а більшість баз даних розташована в центрах обробки даних ESET. Хмарні служби антиспаму дозволяють швидко оновити дані, забезпечуючи швидку реакцію на появу нового спаму.
Захист від фішинг-атак	Ця функція не дозволяє користувачам отримувати доступ до веб-сторінок, для яких відомо, що вони розповсюджують фішингові програми. Електронні листи можуть містити посилання на веб-сайти, на яких розповсюджуються фішингові програми, а ESET Cloud Office Security використовує покращений аналізатор, який виявляє такі посилання (URL-адреси) в тілі й темі вхідних електронних листів. Посилання перевіряються в базі даних фішингових адрес, яка постійно оновлюється.
Захист від шкідливого програмного забезпечення	Відзначений нагородами та інноваційний захист від шкідливого програмного забезпечення з використанням цієї провідної технології захищає від атак. Це стосується всіх типів загроз, зокрема вірусів, програм-вимагачів, руткітів, хробаків і шпигунського програмного забезпечення. Для сканування використовуються хмарні технології, що дозволяє ще більше покращити показники виявлення. Невеликий розмір і невибагливість до ресурсів не зменшують продуктивність роботи системи. Для виявлення шкідливого програмного забезпечення використовується багаторівнева модель безпеки. На кожному рівні (етапі) застосовуються кілька основних технологій. На етапі попереднього виконання використовуються такі технології: Сканер UEFI (Unified Extensible Firmware Interface), 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 і сканер сценаріїв Script Scanner (AMSI). На рівні Post-execution (Після виконання) використовуються такі технології: захист від ботнетів, хмарна система захисту від шкідливого програмного забезпечення й пісочниця. Цей багатофункціональний набір основних технологій забезпечує неперевершений рівень захисту.
Політики	Організації більшого розміру зазвичай мають декілька відділів, і вам потрібно налаштувати різні параметри захисту для кожної організаційної одиниці. ESET Cloud Office Security дає змогу використовувати параметри захисту на основі політик, які можна призначити вибраним клієнтам, користувачам, групам команди або сайтам SharePoint. Кожну політику можна налаштувати відповідно до ваших потреб.
Диспетчер карантину	Перевірте об'єкти в карантині й виконайте потрібну дію (завантажити, видалити або розблокувати). Ця функція забезпечує просте керування електронними листами, вкладеннями, а також файлами з Exchange Online / OneDrive / груп команди / сайтів SharePoint, які були поміщені в карантин ESET Cloud Office Security. Після завантаження об'єктів, які є в карантині, їх можна проаналізувати сторонніми інструментами (за потреби), щоб визначитися з потрібною дією.

Панель інструментів зі статистикою виявлених об’єктів	Перегляньте стислі відомості про операції безпеки в Microsoft 365. На кожній оглядовій вкладці панелі інструментів (Exchange Online / OneDrive / Групи команди / Сайти SharePoint) відображається важлива інформація. На оглядовій вкладці "Користувач" відображається кількість клієнтів і дані про використання ліцензій, а також статистика для кожного клієнта — кількість користувачів, найактивніші одержувачі спаму/фішингових програм/шкідливого програмного забезпечення, найпідозріліші облікові записи OneDrive, найпідозріліші групи команди і сайти SharePoint. Можна вибрати проміжок часу й клієнта для відображення статистики. Додаткові статистичні дані й діаграми про об’єкти виявлення відображаються на оглядових вкладках Exchange Online, OneDrive, "Групи команди і Сайти SharePoint. Це статистичні дані, такі як кількість відсканованих електронних листів і файлів, а також кількість виявлених електронних листів зі спамом/фішинговими програмами/шкідливими програмами. На цих діаграмах відображається трафік для кожного типа виявлення (спам, шкідливі програми й фішингові програми).
Виявлені об’єкти з параметрами фільтрації	Ця функція містить усі записи про виявлені об’єкти. Зокрема, це журнали для кожного об’єкта, виявленого службою сканування електронної пошти (на вкладці Exchange Online), а також службою сканування файлів (на вкладці OneDrive / Групи команди / Сайти SharePoint). Це дає змогу фільтрувати й знаходити потрібні об’єкти, використовуючи додаткову інформацію про конкретне сканування (наприклад, ім’я загрози, хеш файлу тощо).
Користувачі	ESET Cloud Office Security передусім захищає обліковий запис користувача. На вкладці "Відомості" для користувача відображається корисна інформація про нього, зокрема стислі відомості, параметри, визначені політиками, список політик, призначених користувачу, і виявлені об’єкти для Exchange Online і OneDrive. Ця функція стане в пригоді, коли потрібно отримати докладні відомості про об’єкти, виявлені для певного користувача. Окрім того, можна вибрати користувачів для захисту. Користувачі розподілені на групи. Кожна група є клієнтом Microsoft 365 із його користувачами. Щоб полегшити пошук певного користувача в групі, можна застосувати фільтрацію з множинним критерієм.
Звітність і захист на основі 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. Можна налаштувати рівні звітності для таких категорій: "Шкідливе програмне забезпечення", "Потенційно небажані програми", "Потенційно підозрілі програми" й "Потенційно небезпечні програми".

Статистичні звіти та звіти про поштовий карантин	Отримуйте статистичні дані щодо захисту груп Exchange Online, OneDrive і груп команди, а також сайтів SharePoint електронною поштою або створюйте й завантажуйте звіти за потрібний проміжок часу. Можна запланувати регулярне створення звітів, які будуть надсилатися на вказані адреси електронної пошти. Для формату виводу виберіть PDF або CSV. Звіти містять дані про кількість перевірених електронних листів, виявлених шкідливих програм, фішингових посилань і спаму. Звіт у форматі PDF містить також графічне подання даних. Графічне подання є для кожної категорії даних (перевірені електронні листи, трафік шкідливого програмного забезпечення, трафік фішингової активності й трафік спаму). У звіті є також окрема статистика щодо основних одержувачів кожної категорії (шкідливе програмне забезпечення, фішингові посилання й спам). Доступно кілька параметрів створення звітів. Окрім того, можна отримувати звіти про поштовий карантин — список електронних листів, перенесених до карантину. Одержувачів таких звітів можна вибрати. Звіт про поштовий карантин надсилається у визначені дні і вказаний час, але тільки за наявності нових об'єктів, включених до звіту.
Команди й сайти	ESET Cloud Office Security забезпечує захист для груп команди або сайтів SharePoint. Це дає змогу забезпечити захист і для рішень спільної роботи Microsoft 365, адже захист SharePoint і групу команди робить можливим безпечний обмін файлами. Якщо ви використовуєте ESET Cloud Office Security, то для користування командами та сайтами вам може знадобитися ще раз надати свою згоду.
ESET LiveGuard Advanced	Додатковий рівень захисту від удосконалених загроз нульового дня. ESET LiveGuard Advanced — це хмарне рішення на основі ізольованого програмного середовища, де надіслані файли аналізуються згідно з результатами виконання підозрілого коду в ізольованому середовищі та оцінкою їхньої поведінки. ESET Cloud Office Security надсилає підозрілі поштові вкладення й файли з Exchange Online, OneDrive, груп команди і сайтів SharePoint у ESET LiveGuard Advanced для аналізу. Увімкніть і налаштуйте функцію ESET LiveGuard Advanced за допомогою політик. Результати аналізу відображаються в розділі Журнали сканування.
Журнал аудиту	Журнал аудиту дає змогу адміністратору аналізувати дії, виконані в програмі ESET Cloud Office Security. Ця функція може стати в пригоді, особливо якщо у вас є кілька користувачів консолі ESET Cloud Office Security. Записи журналу аудиту засвідчують виконані дії і показують послідовність їхнього виконання. У журналах аудиту зберігається інформація про певну операцію або подію. Журнали аудиту створюються щоразу, коли створюється або змінюється об'єкт ESET Cloud Office Security (пул ліцензій, користувач, політика, звіт, елемент карантину, наприклад вкладення).
Google Workspace (захист Gmail і Google Диск)	ESET Cloud Office Security розширює сферу застосування наших служб безпеки: тепер вони стануть у пригоді для провідних постачальників хмарних послуг електронної пошти — Google Workspace. Завдяки всім своїм функціям ESET Cloud Office Security забезпечує комплексний захист користувачів Gmail і Google Диск. Він захищає користувачів Google Workspace від шкідливого програмного забезпечення, фішингу й спаму.

Нові функції та можливості

Відомості про нові функції й удосконалення, реалізовані в кожній версії ESET Cloud Office Security:

Портал версії 353 випущено 23 листопада 2023 року

- Додано інтеграцію з Google Workspace.
- Навігатор продукту для швидкого доступу до ESET Business Account (більше консолей з'являться в найближчі місяці).
- Інші виправлення помилок і внутрішні покращення.

Портал версії 342.3 випущено 24 жовтня 2023

- Додано верифікацію облікового запису адміністратора Google Workspace.
- Додано стовпчик типу Користувач.
- Інші виправлення помилок і внутрішні покращення.

Портал версії 311.2 випущено 31 липня 2023 року

- Додано Google Workspace (захист Gmail і Google Диск): доступ до попереднього перегляду функцій у меню "Швидкі посилання".
- Додано тему Темний режим.
- Додано навігатор продукту для користувачів завчасного доступу ESET HUB.
- Інші виправлення помилок і внутрішні покращення.

Портал версії 293.7 випущено 13 липня 2023 року

- Додано зв'язок клієнтів із місцями ESET Business Account (EBA). Ця зміна потрібна для сумісності з майбутнім порталом клієнтів ESET PROTECT HUB, де більше не будуть використовуватися ESET MSP Administrator (EMA) і ESET Business Account (EBA). Це впливає лише на кількох замовників, які використовують ліцензії з кількох місць для захисту одного клієнта. У цьому разі вам буде запропоновано пов'язати своїх клієнтів із місцями EBA.
- Інші незначні покращення й виправлення помилок.

Портал версії 251.1 випущено 21 березня 2023 року

- Удосконалення відкладеного завантаження екранів, які дають змогу покращити підтримку клієнтів із десятками тисяч користувачів.
- Зміни в майстрі додавання клієнта.
- Оновлено сторінку "Про програму".
- Оновлено документ "Умови використання і політика конфіденційності" (Обмеження й політика збереження даних).

Портал версії 205 випущено 9 листопада 2022 року

- Під час першого входу в консоль ESET Cloud Office Security відображатиметься вікно "Нові функції та можливості".
- Можливість експортувати журнали сканування і журнал аудиту у файл CSV.
- Додано новий параметр під час об'єднання політик зі списками та електронними листами сповіщень.

Портал версії 180.2 випущено 27 липня 2022 року

- Нова функція Журналу аудиту.
- Розділ "Журнали" замінено розділом "Журнали сканування".

Портал версії 156.2 випущено 26 квітня 2022 року

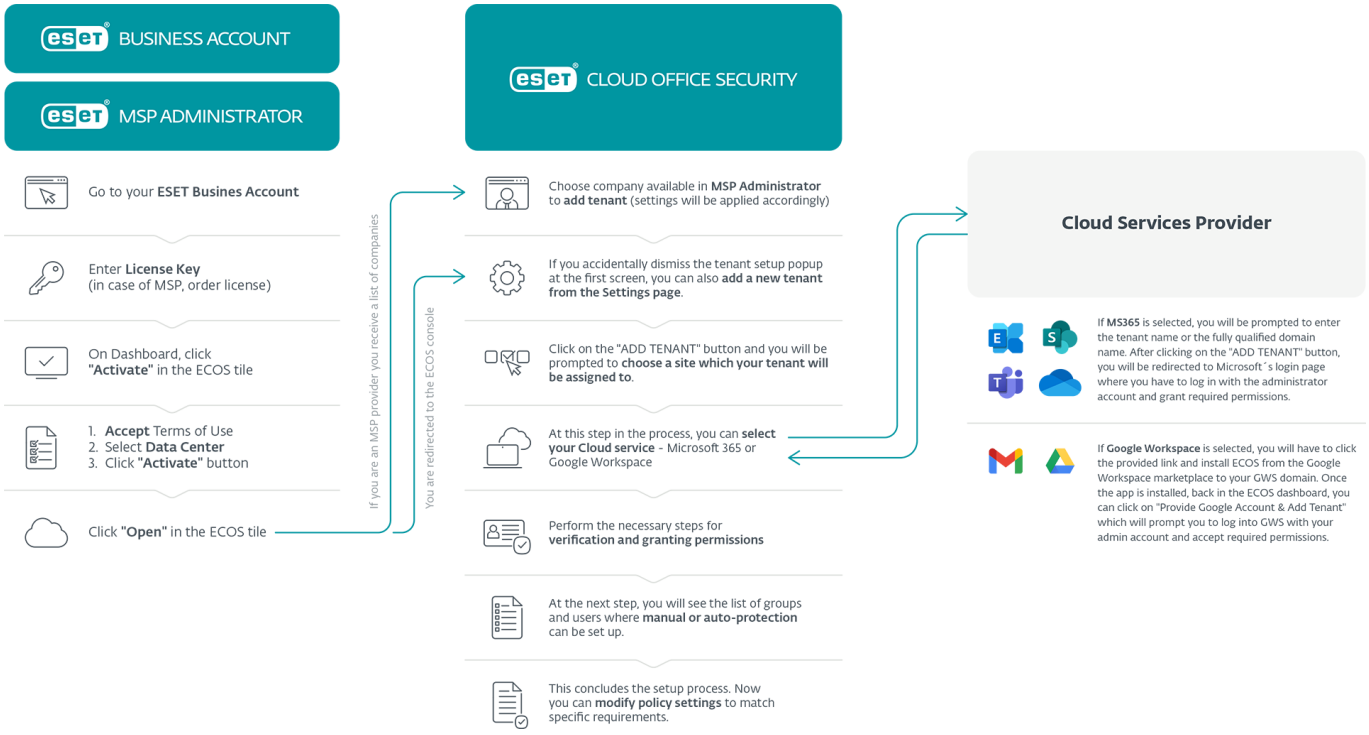
- Dynamic Threat Defense перейменовано на ESET LiveGuard Advanced.
- Надсилання зразків помилкового спрацювання / помилкового негативного результату для аналізу.
- Імпорт/Експорт списків "Затверджені", "Заблоковані" та "Ігноровані" в розділі Політики.
- На панелі інструментів на вкладці Огляд відображається кількість незахищених користувачів.
- Виправлена помилка, через яку сповіщення електронною поштою переносилися в карантин.

Портал версії 140.6 випущено 9 лютого 2022 року

• Можливість використовувати звіти за схемою white label (тільки для спільного брендингу або спеціального логотипу).
• Параметр, який визначає бажану мову сповіщень електронною поштою (сповіщення власника поштової скриньки).
• Параметр, який визначає бажану мову сповіщень електронною поштою для учасників клієнта.
• Фільтрувати електронні листи за ідентифікатором повідомлення.

Інтеграція

Процес інтеграції ESET Cloud Office Security з вашим постачальником хмарних послуг:



Специфікації

Довідкові технічні специфікації для ESET Cloud Office Security:

- Вимоги
- Підтримувані плани Microsoft 365
- Підтримувані тарифні плани Google Workspace

- Підтримувані веб-браузери
- Обмеження й політика збереження даних

Вимоги

Щоб скористатися перевагами служби ESET Cloud Office Security, яка забезпечує захист Microsoft 365, необхідно мати такі компоненти:

- Підтримуваний план підписки Microsoft 365
- Доступ адміністратора до Azure Active Directory (Azure AD)
- Azure Cloud Services: Exchange | OneDrive
- Обліковий запис на порталі ESET Business Account або ESET MSP Administrator

Підтримувані плани Microsoft 365

У ESET Cloud Office Security підтримуються вказані нижче плани Microsoft 365, Exchange Online і OneDrive.

Плани Microsoft 365 для підприємств:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Плани Microsoft 365 для бізнесу:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Плани Microsoft 365 для закладів освіти:

- Microsoft 365 A3

- Microsoft 365 A5

Плани Exchange Online:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

Плани OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Підтримувані тарифні плани Google Workspace

ESET Cloud Office Security підтримує наведені нижче тарифні плани Google Workspace.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Підтримувані веб-браузери

Щоб покращити взаємодію з ESET Cloud Office Security, рекомендуємо регулярно оновлювати веб-браузери.

Консоль ESET Cloud Office Security можна використовувати в таких веб-браузерах:

- Mozilla Firefox 69 і новіших версій
- Microsoft Edge 44 й новіших версій
- Google Chrome 77 і новіших версій
- Opera 63 й новіших версій
- Safari 13.x і новіших версій

Microsoft Internet Explorer не підтримується.

Обмеження й політика збереження даних

За певних умов є обмеження ESET Cloud Office Security, які діють для сканування. Нижче перелічені випадки, коли файл виключається зі сканування й з'являється у розділі Журнали сканування зі статусом **Не перевірено**:

- Розмір файлу перевищує 200 МБ
- Сканування займає довше 2 хвилин і завершується за тайм-аутом (минув час очікування).
- Файл архіву з глибиною 10 або більше рівнів (так звані "файлові бомби" або "ZIP-бомби")
- Архівний файл захищено паролем
- Пошкоджений файл

Обмеження карантину (під час розблокування об'єктів у карантині):

- 15 МБ для одного поштового вкладення
- 150 МБ для всього електронного листа (включно з вкладеннями)

Політика збереження даних:

Об'єкт	Період збереження	Коментар
Об'єкти в карантині	30 дні	Об'єкти, старіші за 30 день, видалятимуться остаточно.
Виявлені об'єкти	90 дні	Записи, старіші за 90 днів, видалятимуться остаточно.
Записи журналів сканування	90 дні	Записи, старіші за 90 днів, видалятимуться остаточно.
Записи журналів сканування з результатом "Очищено"	3 дні	Якщо у вас є політика "Реєструвати всі об'єкти", результати сканування зі статусом "Очищено", старіші за 3 дні, видалятимуться остаточно.
Резервне копіювання бази даних ESET Cloud Office Security	90 дні	Резервні копії, старіші за 90 днів, видалятимуться остаточно.
Журнали аудиту	90 дні	Записи, старіші за 90 днів, видалятимуться остаточно.
Журнали статистики програм	90 дні	Записи, старіші за 90 днів, видалятимуться остаточно.

Клієнта видалено з консолі ESET Cloud Office Security

Якщо видалити клієнта з консолі ESET Cloud Office Security, період збереження його даних складатиме 30 днів (через 30 днів дані карантину, журналів сканування та статистики буде видалено). Якщо протягом цих 30 днів додати видаленого клієнта, усі дані буде відновлено. Інші об'єкти (клієнти, користувачі, групи, місця, звіти, політики) остаточно видаляються через

90 днів.

ESET Cloud Office Security деактивовано в ESET Business Account або ESET MSP Administrator

Якщо деактивувати ESET Cloud Office Security у ESET Business Account або ESET MSP Administrator, цей процес також вилучить клієнтів із ESET Cloud Office Security. Видалення ESET Cloud Office Security є остаточним; видалені дані не підлягають відновленню.

Сканування на наявність спаму:

ESET Cloud Office Security сканує електронні листи, що зберігаються в поштових скриньках, на наявність спаму. Тому ESET Cloud Office Security не може запобігти надсиланню користувачем спаму на зовнішню електронну адресу. У малоймовірному сценарії спамер може скористатися викраденими обліковими даними користувача Office 365 для розсилання масових спам-повідомлень (вихідний поштовий трафік).

Ліцензування для ESET Cloud Office Security

Керування ліцензіями ESET Cloud Office Security через ESET Business Account або ESET MSP Administrator. Спробуйте ESET Cloud Office Security з 30-денною пробною ліцензією.

- Інформацію зі створення облікового запису, додавання ліцензії або керування нею див. в розділі ESET Business Account.
- Див. ESET MSP Administrator, якщо ви MSP.

ESET Business Account і ESET MSP Administrator (обліковий запис гібридного ліцензування)

Якщо в ESET MSP Administrator і ESET Business Account зареєстровано одну адресу електронної пошти (єдиний вхід), можна переключатися між поданнями ESET Business Account і ESET MSP Administrator. Захистіть користувачів або компанії в розділі Керування ліцензією для ESET Cloud Office Security.

Пільговий період після завершення терміну дії ліцензії в ESET Business Account

Коли термін дії ліцензії добігає до кінця, в інтерфейсі ESET Business Account відображається попередження. Якщо дата закінчення терміну дії минула й ви не поновили ліцензію або не активували нову, в ESET Business Account відображатиметься попередження про завершення терміну дії ліцензії. Якщо дійсна ліцензія відсутня, у ESET Business Account відображатиметься сповіщення про те, що термін дії ліцензії завершується через 14 днів. Ви також отримаєте електронний лист на адресу, указану в обліковому записі адміністратора.

У вас буде 14-денний пільговий період, щоб оновити ліцензію після завершення її дії. Коли мине половина пільгового періоду, ви отримаєте сповіщення в ESET Business Account і на електронну пошту. Через 14 днів ваше користування ESET Cloud Office Security буде призупинено. Обліковий запис стане недоступним і неробочим. Призупинений обліковий запис ESET Cloud Office Security зберігатиметься. Якщо додати нову ліцензію ESET Cloud Office Security у ESET Business Account, він знову стане доступним. Обліковий запис ESET Cloud Office Security може бути в призупиненому стані до 30 днів. Після завершення цього періоду його буде остаточно видалено.

Якщо обліковий запис перейшов у стан призупинення, ви отримаєте сповіщення в ESET Business

Account і електронною поштою за 14 днів до видалення облікового запису. Щоб відновити доступ до облікового запису ESET Cloud Office Security, потрібно активувати нову ліцензію ESET Cloud Office Security.

> **i** У пільговий період користувачі залишаються повністю захищеними. Після завершення пільгового періоду користувачі стануть незахищеними.

Призупинена ліцензія

Якщо в ESET Cloud Office Security немає дійсної ліцензії ESET Business Account, ваш екземпляр ESET Cloud Office Security буде призупинено. Екземпляр стане недоступний і неробочий. Екземпляр ESET Cloud Office Security може бути в призупиненому стані до 30 днів. Після завершення цього періоду його буде остаточно видалено. Щоб відновити доступ до екземпляра ESET Cloud Office Security, потрібно активувати нову дійсну ліцензію ESET Cloud Office Security.

ESET Business Account

ESET Business Account працює як уніфікована точка доступу для ESET Business Account і ESET Cloud Office Security. Для доступу до ESET Cloud Office Security використовуйте сторінку входу ESET Business Account або ESET Cloud Office Security. На обох сторінках потрібно буде виконати автентифікацію ESET Business Account для перевірки ідентичності.

- Створіть новий обліковий запис, якщо у вас немає зареєстрованого облікового запису в ESET Business Account.
- Якщо у вас є обліковий запис ESET Business Account, додайте ліцензію ESET Cloud Office Security.
- Керувати ESET Business Account.

Створення нового облікового запису ESET Business Account

1. Відкрийте сторінку входу в ESET Business Account і клацніть **Зареєструватися безкоштовно**. Уважно заповніть реєстраційну форму. Уведена адреса електронної пошти буде використовуватися для входу.

2. Пароль має містити не менше 10 символів. Заповніть поля **Ім'я** й **Дані компанії** й клацніть **Продовжити**. Ознайомтесь із документом **Умови використання ESET** і підтвердьте свою згоду з викладеними умовами. Заповніть форму reCAPTCHA й клацніть **Зареєструватися**.

3. Після успішної реєстрації ви маєте отримати електронний лист із її підтвердженням (на це може знадобитися до 15 хвилин). Клацніть посилання в електронному листі з підтвердженням, щоб відкрити нове вікно **Активувати обліковий запис**.

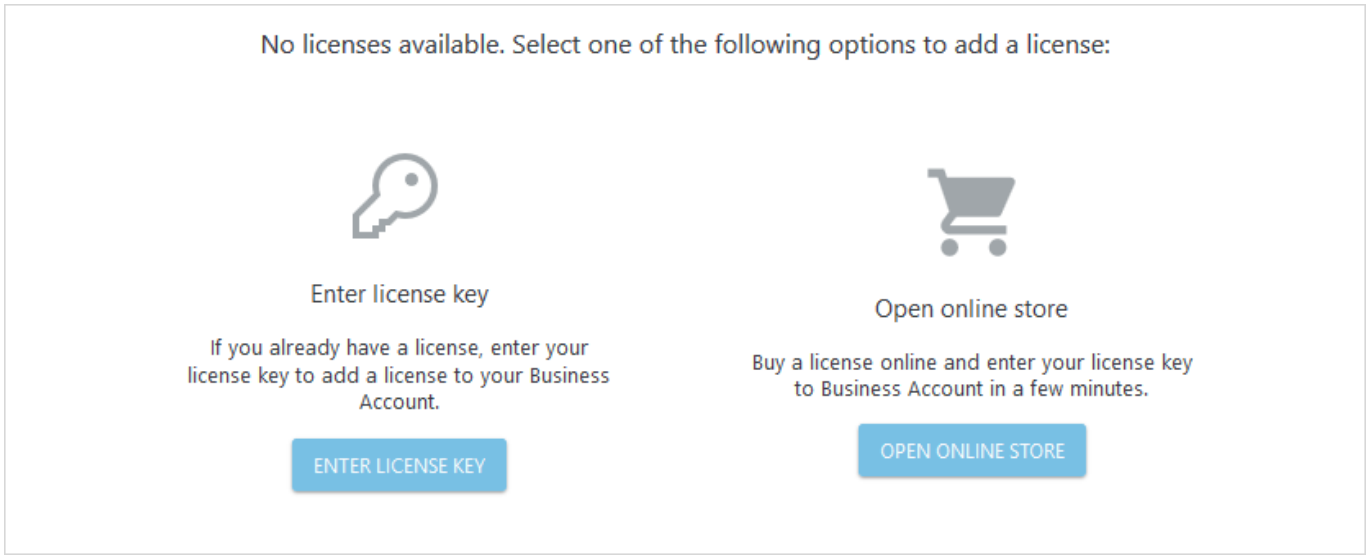
4. Уведіть пароль і клацніть **Активувати** для активації ESET Business Account. Ви отримаєте ще один електронний лист із підтвердженням створення облікового запису ESET Business Account. Тепер ви можете ввійти у свій ESET Business Account.

Після активації ESET Business Account додайте ліцензію ESET Cloud Office Security.

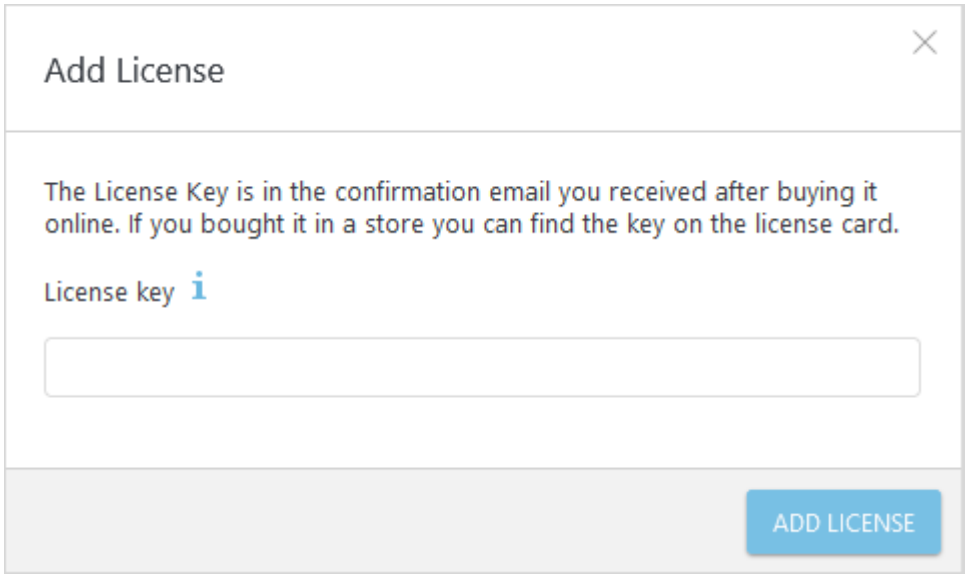
Додавання ліцензії ESET Cloud Office Security в ESET Business Account

Після успішного входу до ESET Business Account відобразиться екран привітання ESET Business Account, якщо ви вперше його використовуєте.

1. Клацніть **Додати ліцензію**, щоб відкрити вікно ліцензій. Якщо ви — постійний користувач ESET Business Account, відкрийте вкладку **Ліцензія** й клацніть **Додати ліцензію**.



2. Уведіть **ліцензійний ключ** і клацніть **Додати ліцензію**.



3. Ви отримаєте електронний лист із посиланням для підтвердження. Клацніть посилання й уведіть облікові дані порталу ESET Business Account у відповідь на запит. Додаткову інформацію про керування ліцензією, користувачами й місцями див. в посібнику ESET Business Account .

Керувати ESET Business Account

Поширені дії, пов’язані з ліцензуванням:

Місця й пул ліцензій

Ліцензії й пули ліцензій завантажуються з ESET Business Account. Пули ліцензій доступні, тільки якщо у вас є наявні місця в ESET Business Account.

Створення нового користувача в ESET Business Account

Можна створити користувача, який допоможе керувати частиною ваших ліцензій.

1. Відкрийте ESET Business Account і виконайте вхід.

2. Виберіть **Керування користувачами**, клацніть **Новий користувач** і введіть потрібну інформацію.

3. Виберіть **права доступу** до ESET Cloud Office Security для користувача:

   • **Читання**: користувач має доступ до ESET Cloud Office Security, зокрема може переглядати користувачів, журнали й виявлені об’єкти, проте не може керувати політикою, захищати користувачів або розблоковувати їх із карантину.

   • **Запис**: користувач має повний доступ до ESET Cloud Office Security, може переглядати й виконувати операції керування відносно користувачів і карантину або створювати політику.

   • **Без доступу**: у користувача немає доступу до ESET Cloud Office Security.

4. Задайте мову в **налаштуваннях** користувача для консолі ESET Cloud Office Security.

5. Клацніть **Створити**, щоб створити користувача.

Створення нового місця в ESET Business Account

Місця дозволяють розділити або об’єднати ліцензії в пули ліцензій. Місця — це окремі групи, які можуть мати власне розташування й адміністраторів.

1. Відкрийте ESET Business Account і виконайте вхід.

2. Виберіть **Відомості**, клацніть **Створити сайт** і введіть потрібні особисті дані.

3. Клацніть **Додати користувача**, виберіть користувача й клацніть **Підтвердити**.

4. У пулі ліцензій клацніть **Додати робочі одиниці** й виберіть ліцензію ESET Cloud Office Security. Можна змінити значення параметра **Робочі субодиниці** й клацнути **Підтвердити**.

5. Клацніть **Створити**, щоб створити сайт.

ESET MSP Administrator

ESET MSP Administrator — це система керування ліцензіями, яка дає змогу користувачам постачальників керованих послуг створювати кількох клієнтів MSP й генерувати специфічні ліцензії з певною кількістю робочих місць. Портал ліцензування ESET MSP Administrator підтримує ціноутворення залежно від обсягу послуг і виставлення рахунків залежно від точної кількості придбаних днів для робочих місць.

ESET Cloud Office Security доступний для всіх MSP Managers, MSPs і managed MSPs. Користувач ESET MSP Administrator із правом доступу на запис може активувати ESET Cloud Office Security. До ESET Cloud Office Security можуть отримати доступ користувачі з правами на запис, правами на читання або настроюваними правами.

- Створення нового клієнта MSP (для активації консолі ESET Cloud Office Security потрібна адреса електронної пошти клієнта).

- Активуйте ESET Cloud Office Security з ESET MSP Administrator.

Активувати ESET Cloud Office Security

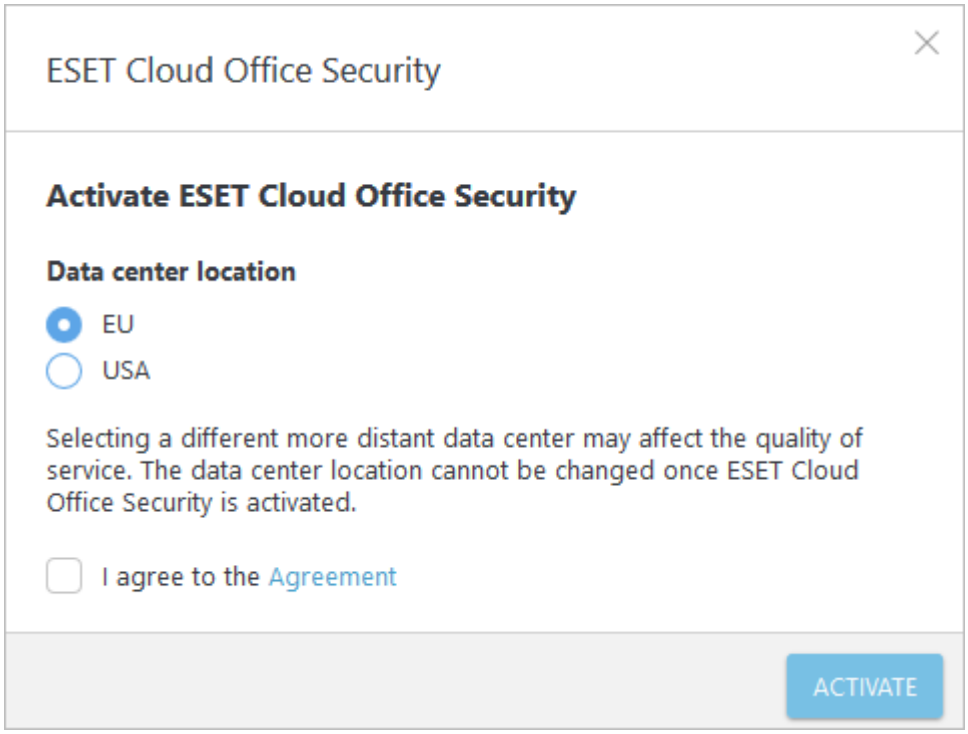
1. Увійдіть в ESET Business Account або ESET MSP Administrator і знайдіть плитку ESET Cloud Office Security на **панелі інструментів**.

2. Клацніть **Активувати** в правому верхньому куті плитки ESET Cloud Office Security.

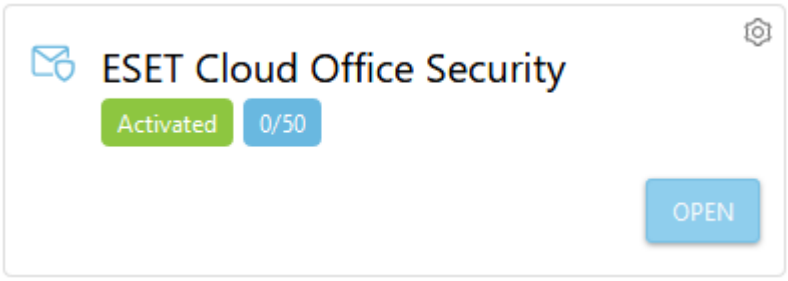


3. У майстрі активації буде відображатися посилання на документ Умови використання ESET Cloud Office Security, а також оптимальне розташування центра обробки даних залежно від вашого поточного розташування. Виберіть **Приймаю умови використання** й клацніть **Активувати**. Не рекомендуємо змінювати розташування центра обробки даних. Проте можна вибрати інше розташування, якщо його потрібно використовувати.

> Центри обробки даних є повністю відокремленими. Після вибору розташування центра обробки даних його неможливо змінити. Окрім того, центр обробки даних не можна перенести в інше розташування. Щоб змінити центр обробки даних, запустіть процес активації спочатку.

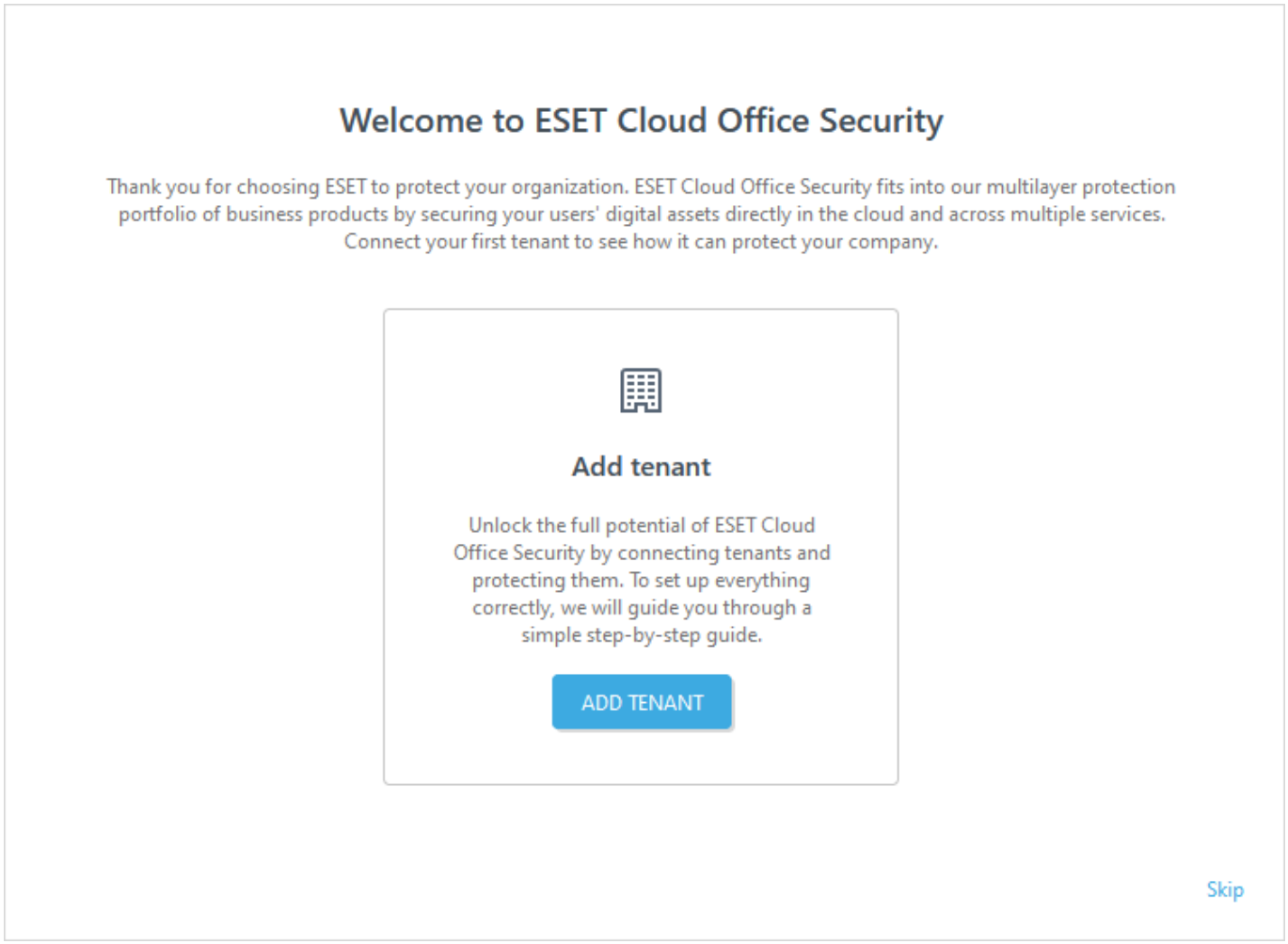


4. У плитці ESET Cloud Office Security клацніть **Відкрити**. Панель інструментів ESET Cloud Office Security відкривається в новій вкладці браузера.

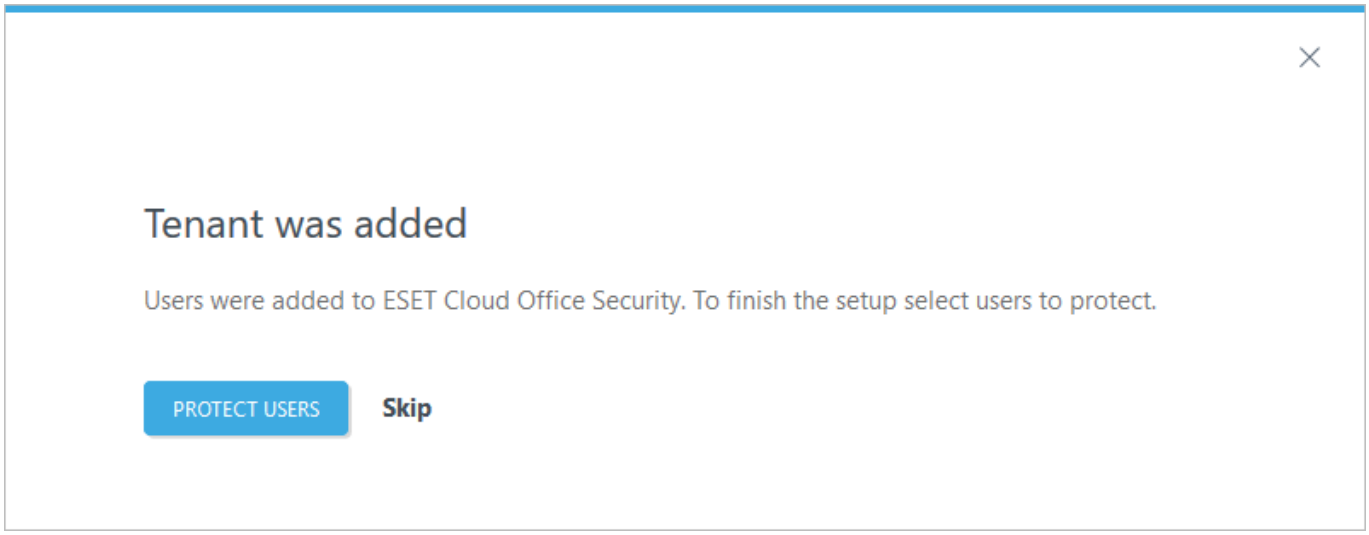


Під час першого входу в ESET Cloud Office Security відобразиться **майстер запуску**. Цей майстер допоможе покроково виконати процес початкового розгортання.

1. Додайте клієнт (Microsoft 365 або Google Workspace).



2. Захистити користувачів. Якщо ви вибрали пункт **Пропустити**, ви зможете захистити користувача або компанії пізніше в розділі Керування ліцензією для ESET Cloud Office Security.

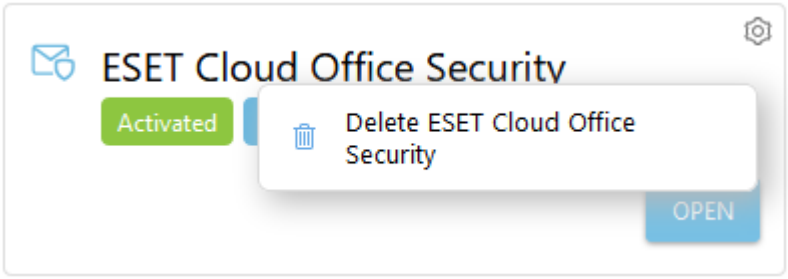


Деактивувати ESET Cloud Office Security

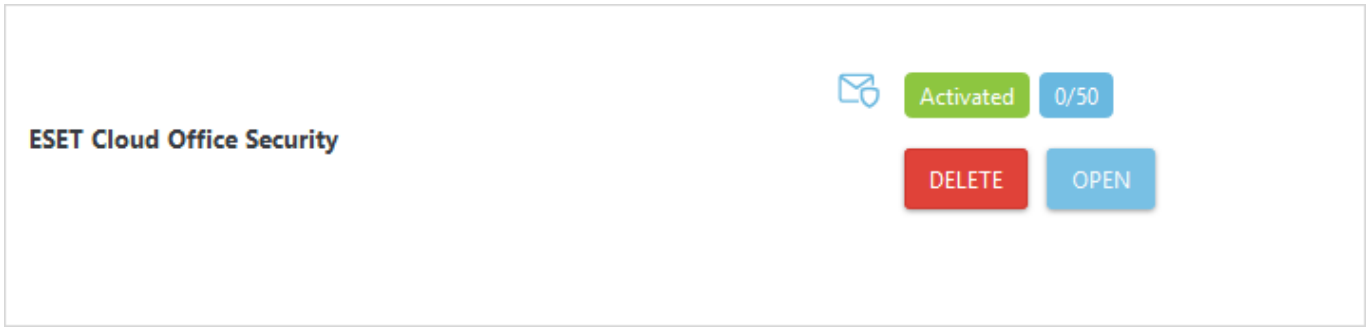
1. Увійдіть в ESET Business Account або ESET MSP Administrator і знайдіть плитку ESET Cloud Office Security на **панелі інструментів**.

2. Клацніть піктограму шестерні у верхньому правому куті плитки ESET Cloud Office Security і

виберіть **Видалити** ESET Cloud Office Security.

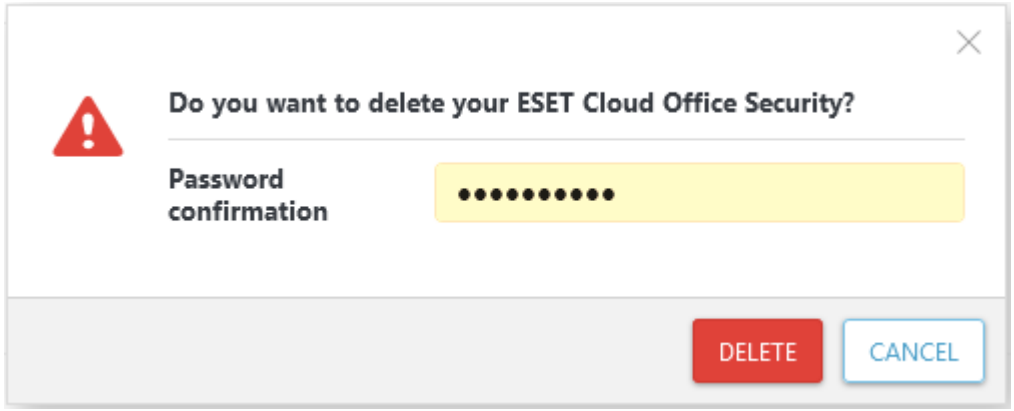


3. Крім цього, можна відкрити розділ **Відомості** й клацнути **Видалити**.



4. З'явиться вікно з попередженням про те, що всі дані будуть видалені. Уведіть пароль ESET Business Account для підтвердження й клацніть **Видалити**.

Видалення ESET Cloud Office Security остаточне. Відновити видалені дані не можна.



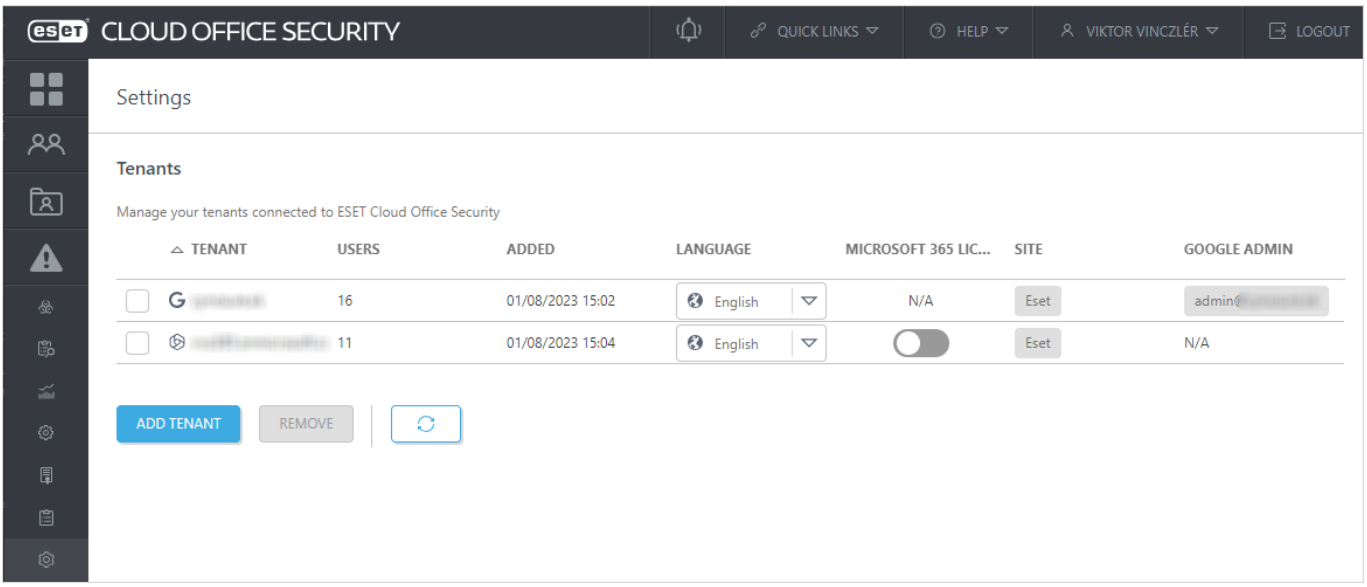
Екземпляр ESET Cloud Office Security буде видалено, і плитка продукту ESET Cloud Office Security змінить свій стан на **Не активовано**. Ви також отримаєте електронний лист із підтвердженням від ESET Business Account.

Керування клієнтами в меню "Параметри"

Керуйте клієнтами, які підключені до ESET Cloud Office Security. Можна переглянути всіх зареєстрованих клієнтів в таблиці з докладними відомостями для кожного клієнта. За допомогою кнопки Оновити можна перезавантажити таблицю з клієнтами.

Якщо потрібно додати новий клієнт, клацніть Додати клієнта й виберіть Microsoft 365 або Google Workspace залежно від хмарної платформи, яку потрібно захистити. Після завершення реєстрації клієнта ваш Microsoft 365 або Google Workspace буде захищено ESET Cloud Office Security.

Після додавання клієнта екран зміниться: на ньому відобразиться список клієнтів, пов'язаних із місцем. Можна керувати наявним клієнтом або додати інших клієнтів. У таблиці вказано ім'я клієнта, кількість користувачів, час додавання клієнта, налаштування мови, ліцензовані користувачі Microsoft 365, ім'я сайту й адміністратор Google.



Мова

Цей параметр визначає мову повідомлень електронною поштою, які надсилаються учасникам клієнта. Можна окремо визначити мову для кожного клієнта, наприклад, якщо MSP керує кількома компаніями.

Щоб видалити клієнта з ESET Cloud Office Security, виберіть відповідний клієнт і клацніть Видалити. З'явиться вікно із запитом на підтвердження рішення. Після видалення клієнта всі дані користувача будуть видалені через 30 днів.

Ліцензовані користувачі Microsoft 365

Цей параметр ввімкнено за замовчуванням. Цей параметр еквівалентний списку користувачів у центрі адміністрування Microsoft 365 у розділі **Користувачі** > **Активні користувачі** > Фільтр: **Ліцензовані користувачі**.

Якщо вимкнути цей параметр, ESET Cloud Office Security буде показувати всіх користувачів, зокрема й користувачів без ліцензії Microsoft 365 (наприклад, спільні поштові скриньки). Якщо ви використовуєте автоматичний захист для груп або клієнтів, у яких є користувачі без ліцензій Microsoft 365, ці користувачі стануть видимими й захищеними, а також використовуватимуть робочі одиниці з ліцензії ESET Cloud Office Security. Нові видимі користувачі можуть мати статус захисту **Очікування** протягом 1 години. Після виконання процесу автоматичного захисту статус захисту зміниться на **Захищено** або інший можливий статус у розділі Користувачі.

> Якщо в клієнті або групі з автоматичним захистом є користувач без поштової скриньки або OneDrive, він буде використовувати робочу одиницю з ліцензії ESET Cloud Office Security. Для цього користувача відображатиметься статус захисту **Попередження**.

Якщо заново ввімкнути параметр Ліцензовані користувачі Microsoft 365, відображатимуться тільки користувачі з ліцензією Microsoft 365. Користувач без ліцензії Microsoft 365 буде виключений із розділу Користувачі, а відповідні робочі одиниці з ліцензії ESET Cloud Office Security

будуть вивільнені. Для застосування зміни може знадобитися певний час (до 1 години).

Якщо ви маєте захищених уручну користувачів без ліцензії Microsoft 365, то за умови, що було вимкнуто параметр **Ліцензовані користувачі Microsoft 365**), ці користувачі залишаться видимими й захищеними навіть після ввімкнення параметра **Ліцензовані користувачі Microsoft 365** (поки не припиниться захист користувачів).

Сайт

Якщо потрібно змінити місце, з яким пов'язано клієнта, клацніть ім'я місця, щоб відкрити вікно **Виберіть місце для захисту** й унесіть необхідні зміни.

Адміністратор Google

Для адміністратора Google має бути визначена активна електронна адреса адміністратора Google Workspace.

Якщо роль або адреса електронної пошти адміністратора незабаром зміняться, оновіть інформацію адміністратора Google, клацнувши її. Зробіть це заздалегідь, щоб забезпечити функціональність клієнта й захист місця.

Оновити згоду

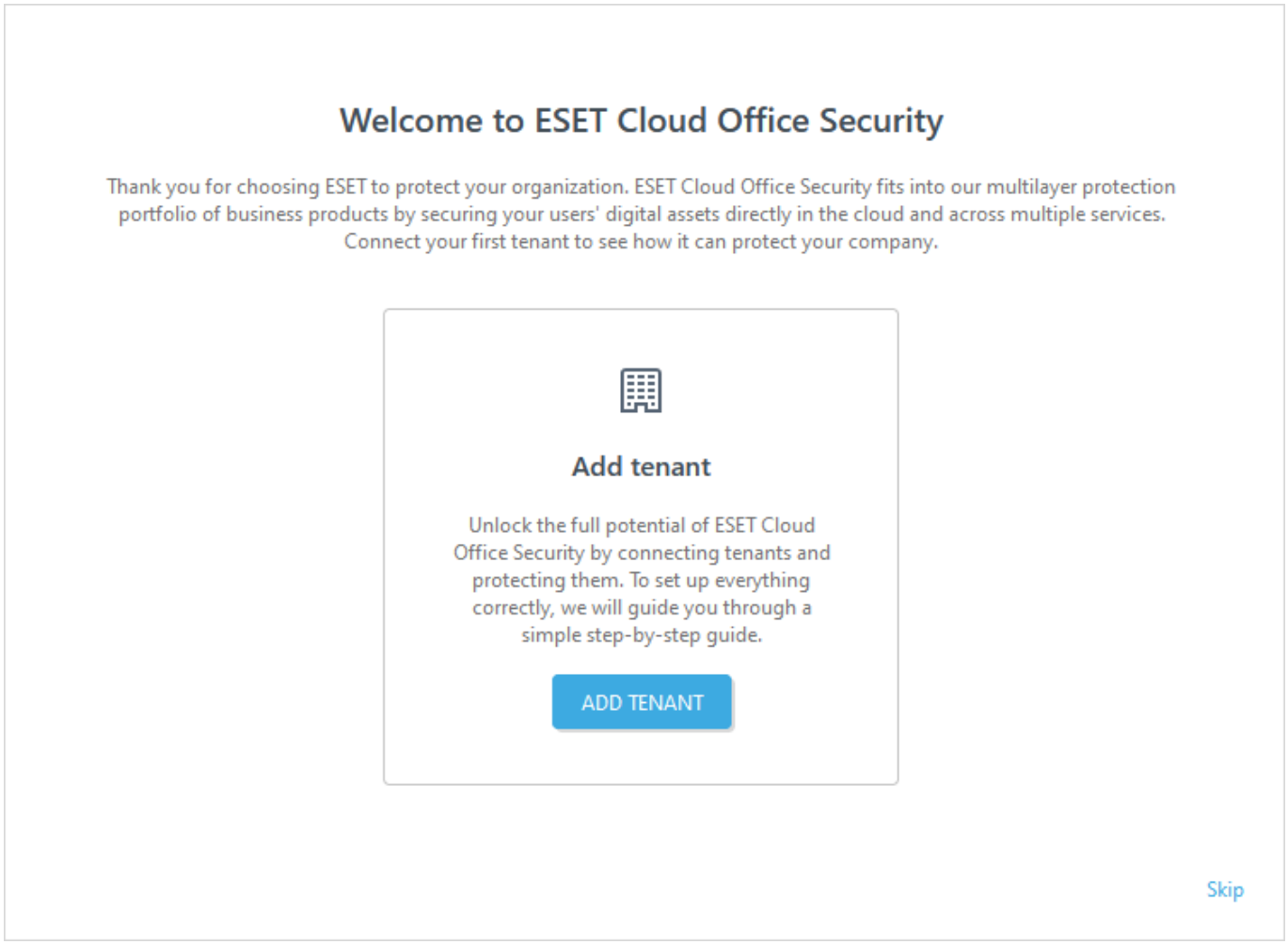
Якщо відображається жовта кнопка, ви можете оновити свою згоду. Оновлення згоди для наявного клієнта розширює дозволи ESET Cloud Office Security для вашого облікового запису Microsoft 365 завдяки активації функції, яка надає інформацію про тип користувача. Тип користувача визначається в Azure Active Directory й відображатиметься в розділі Користувачі в спеціальному стовпці. Наприклад, користувачів Microsoft 365 можна фільтрувати за типом, якщо потрібно додати список лише в спільні поштові скриньки.

Клацніть кнопку **Оновити** для кожного клієнта, для якого потрібно ввімкнути цю функцію. Оновлення типу користувача з вашого Azure AD може зайняти до 24 годин.

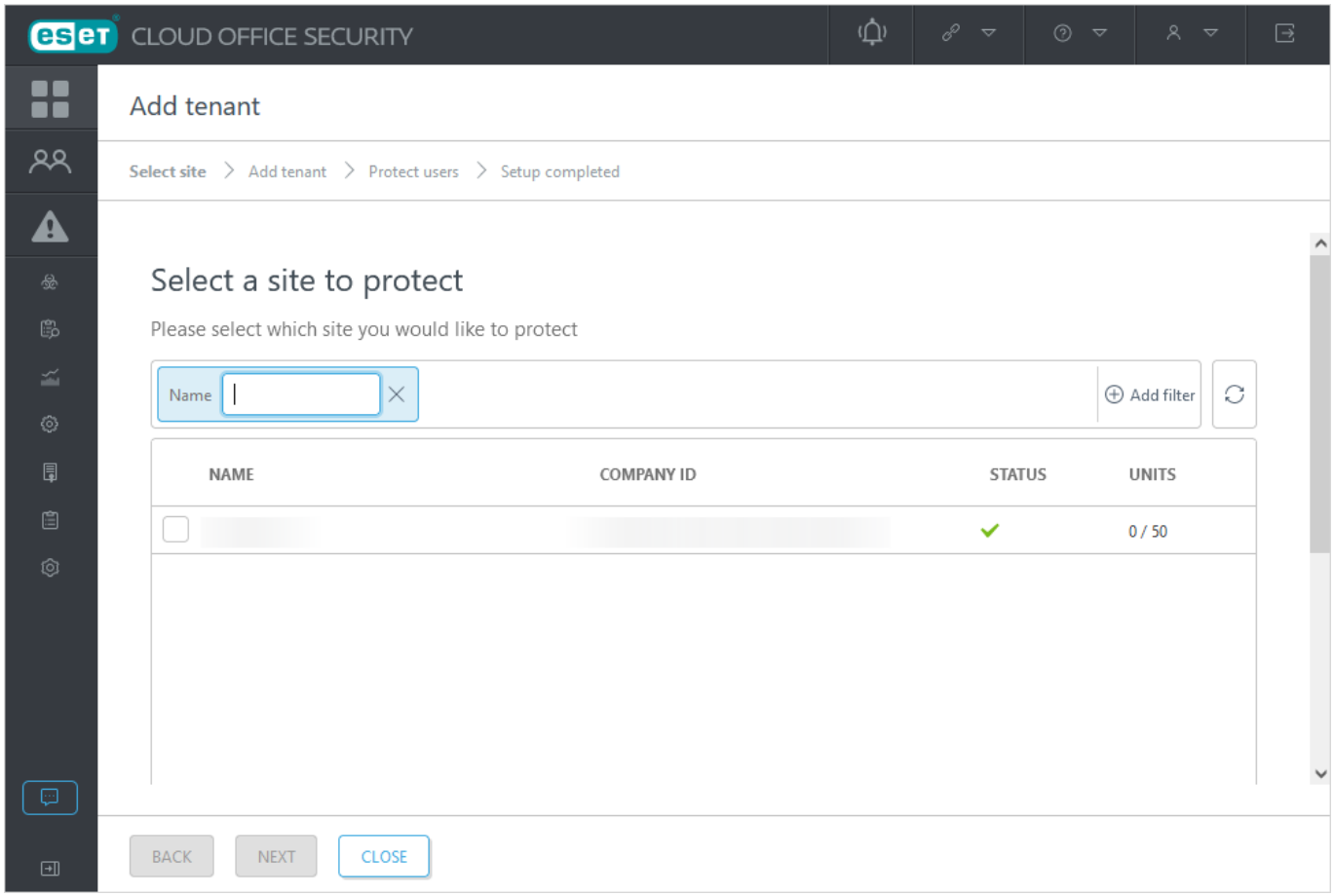
Якщо відображається червона кнопка, це означає, що згоду відкликано або внесено іншу зміну, яка вплинула на інтеграцію клієнта з ESET Cloud Office Security. Клацніть кнопку **Оновити**, щоб продовжити захищати користувачів.

Додавання першого клієнта

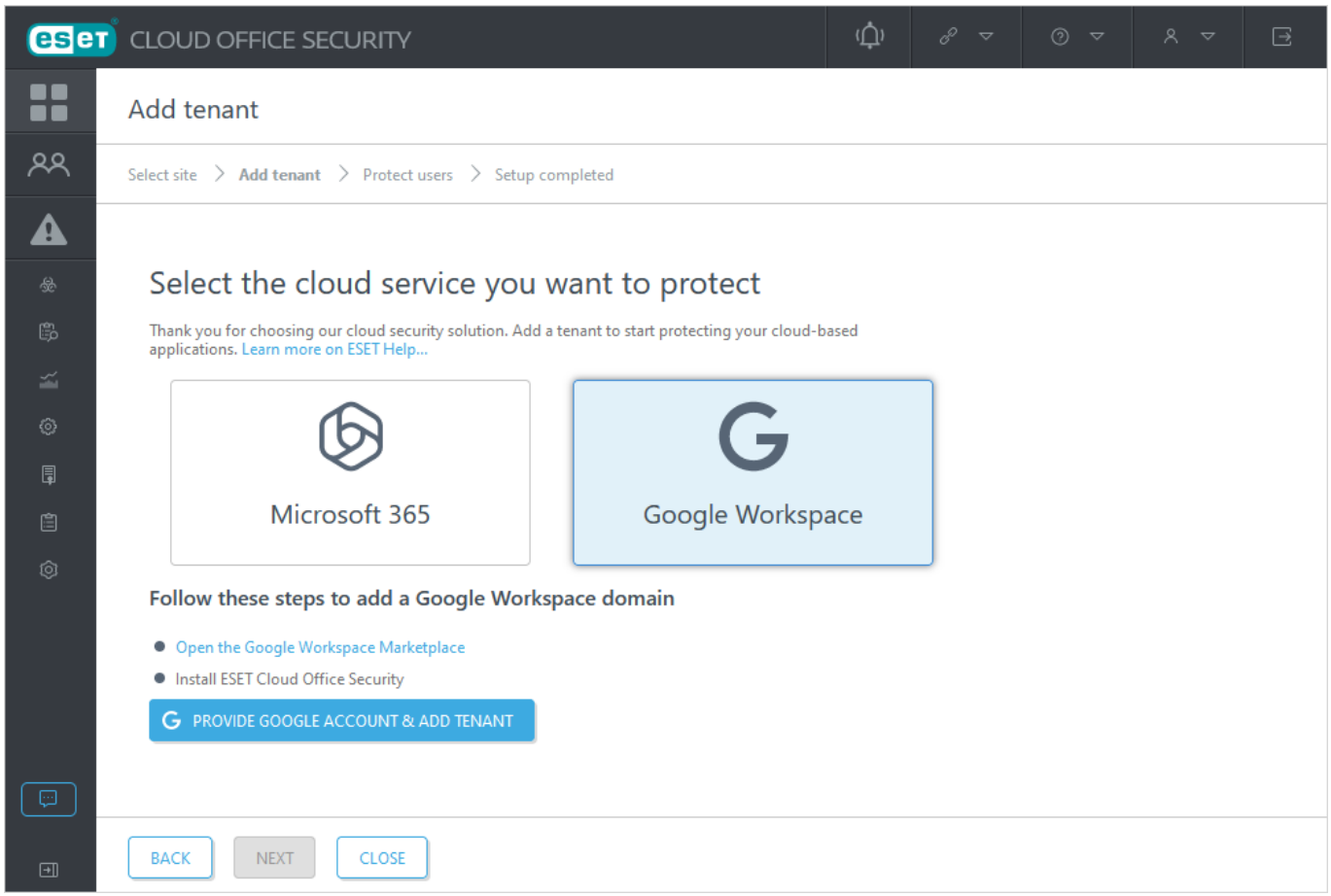
Для захисту хмарної платформи клацніть **Додати клієнта**, щоб підключити Microsoft 365 або Google Workspace до ESET Cloud Office Security.



Список доступних місць має відобразитися у вікні **Виберіть місце для захисту**. Установіть прапорець, щоб вибрати місце, яке потрібно пов’язати з клієнтом, і клацніть **Далі**.



У вікні **Виберіть хмарну службу, яку потрібно захистити** клацніть плитку Microsoft 365 або Google Workspace і дотримуйтеся наведених нижче інструкцій:



Клієнт Microsoft 365

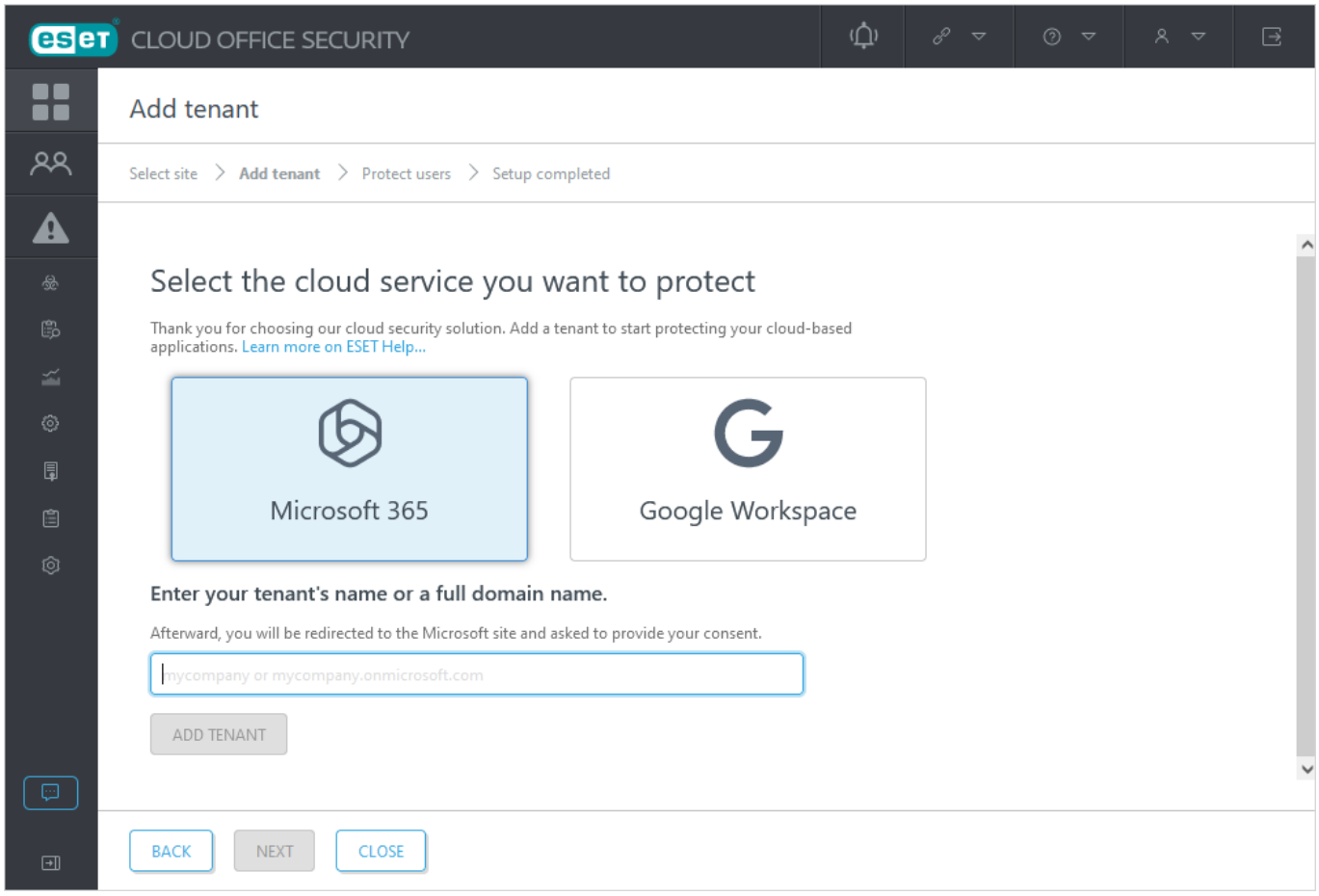
Azure Active Directory (Azure AD) впорядковує об’єкти (наприклад, користувачів і програми) в групи, які називаються клієнтами. Для ідентифікації клієнта зазвичай використовується ім’я домену. Якщо кілька користувачів мають однакове ім’я домену, ці користувачі входять до складу одного клієнта. Клієнти дозволяють задавати політики для користувачів і програм у вашій організації, що дозволяє забезпечити їх відповідність політикам безпеки й операційним політикам. Можна захистити кілька клієнтів Microsoft 365 і керувати ними з однієї консолі ESET Cloud Office Security.

Більш докладні відомості див. в статті Microsoft щодо клієнтів у Azure Active Directory.

Додати клієнта

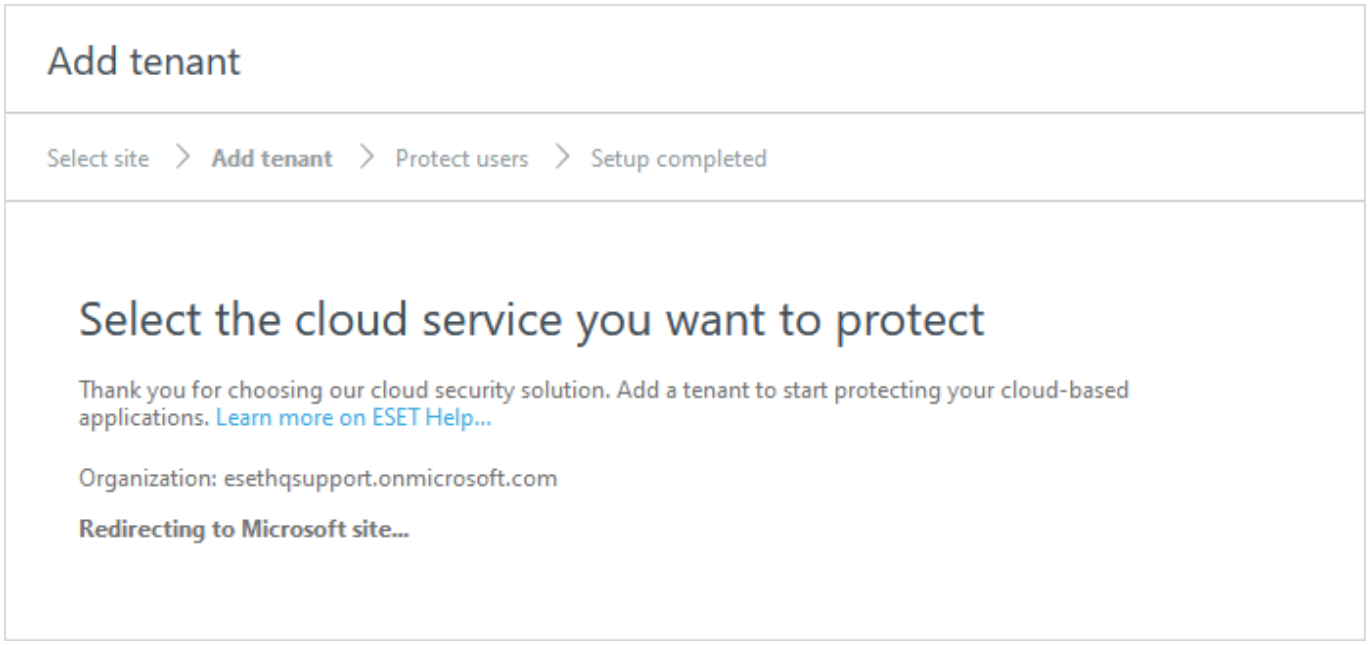
1. Відкрийте розділ **Параметри** й клацніть **Додати клієнта** (або в будь-якому місці, де є кнопка **Додати клієнта**).

2. Клацніть плитку **Microsoft 365**.

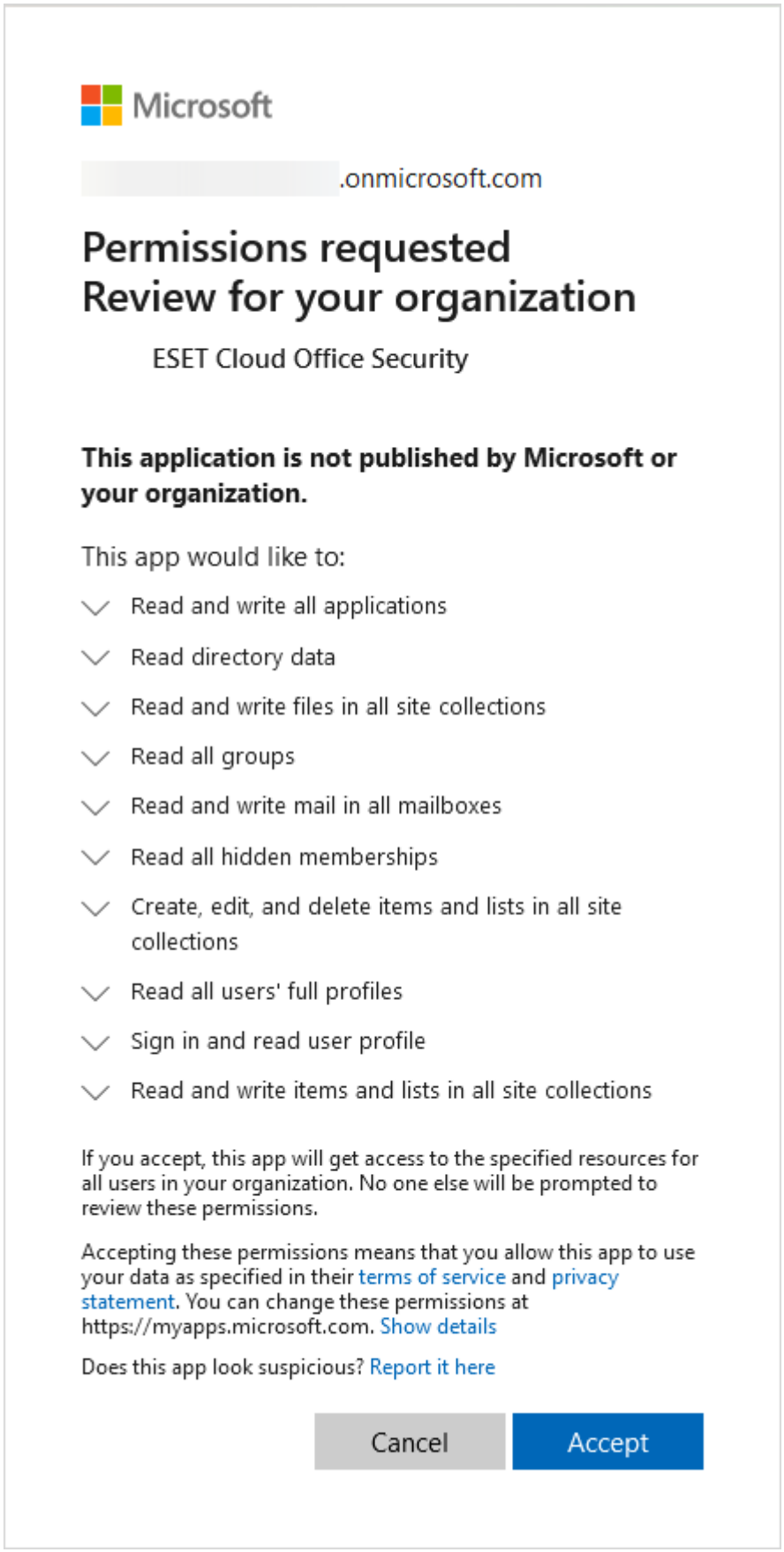


3. Уведіть ім’я клієнта Microsoft 365 або повне ім’я домену й клацніть **Додати клієнт**.

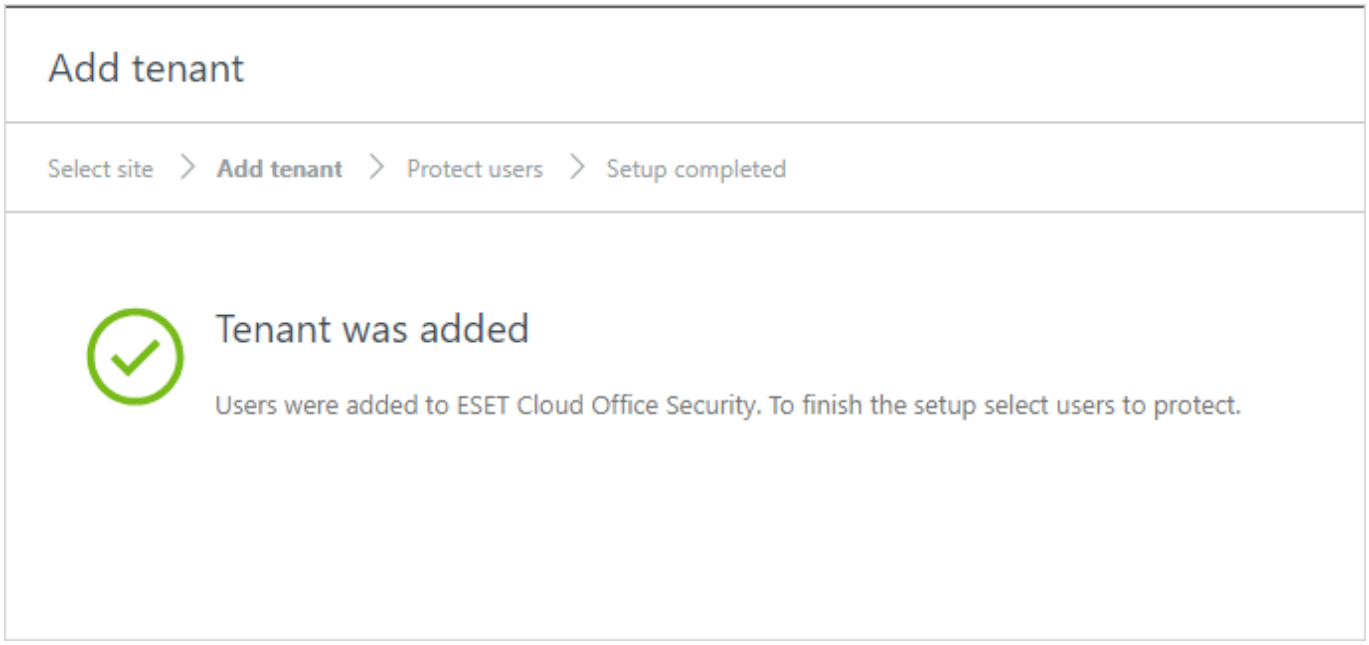
4. Відкриється сторінка Microsoft Online із пропозицією надати згоду на дозволи зі списком дозволів, що потрібні для ESET Cloud Office Security.



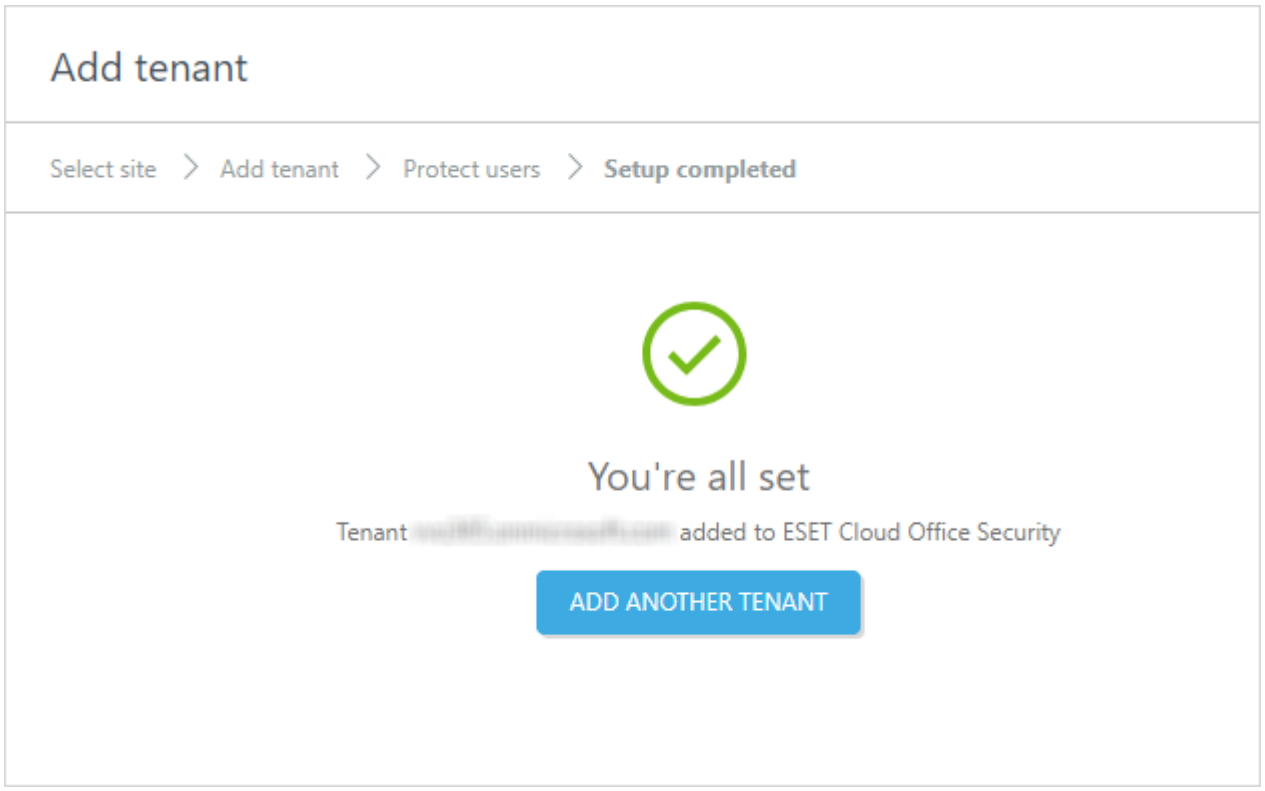
5. Уведіть облікові дані облікового запису адміністратора Microsoft 365, щоб дозволити ESET Cloud Office Security доступ до даних, розташованих в обліковому записі Microsoft, і клацніть **Прийняти**.



6. Ваш клієнт Microsoft 365 було додано разом із користувачами.



7. Щоб завершити налаштування, клацніть **Далі** й виберіть користувачів для ввімкнення **захисту**.



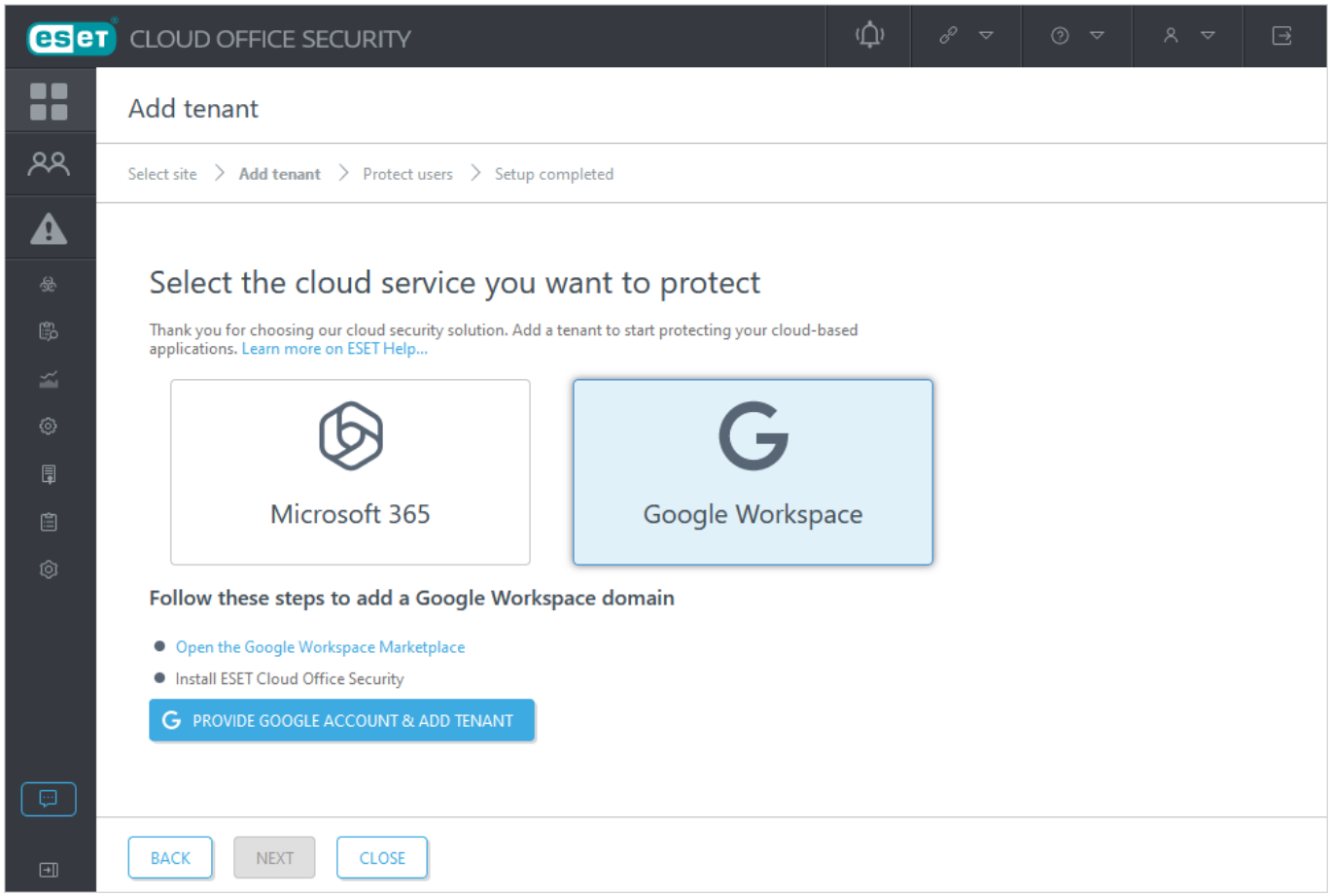
Клієнт Google Workspace

Інтегруйте клієнт Google Workspace із ESET Cloud Office Security, щоб забезпечити захист користувачів Google Workspace.

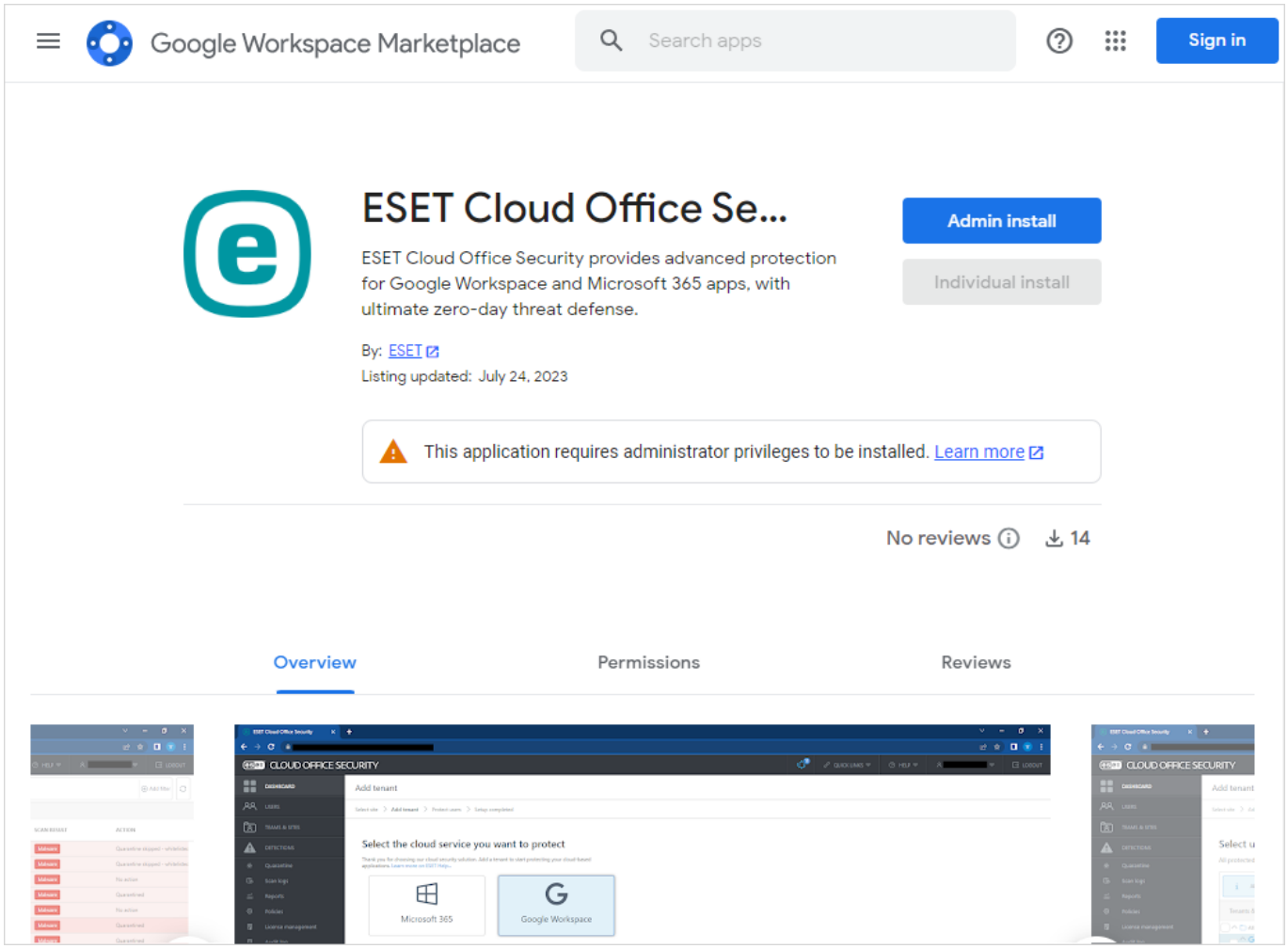
Додати клієнта

1. Відкрийте розділ **Параметри** й клацніть **Додати клієнта** (або в будь-якому місці, де є кнопка **Додати клієнта**).

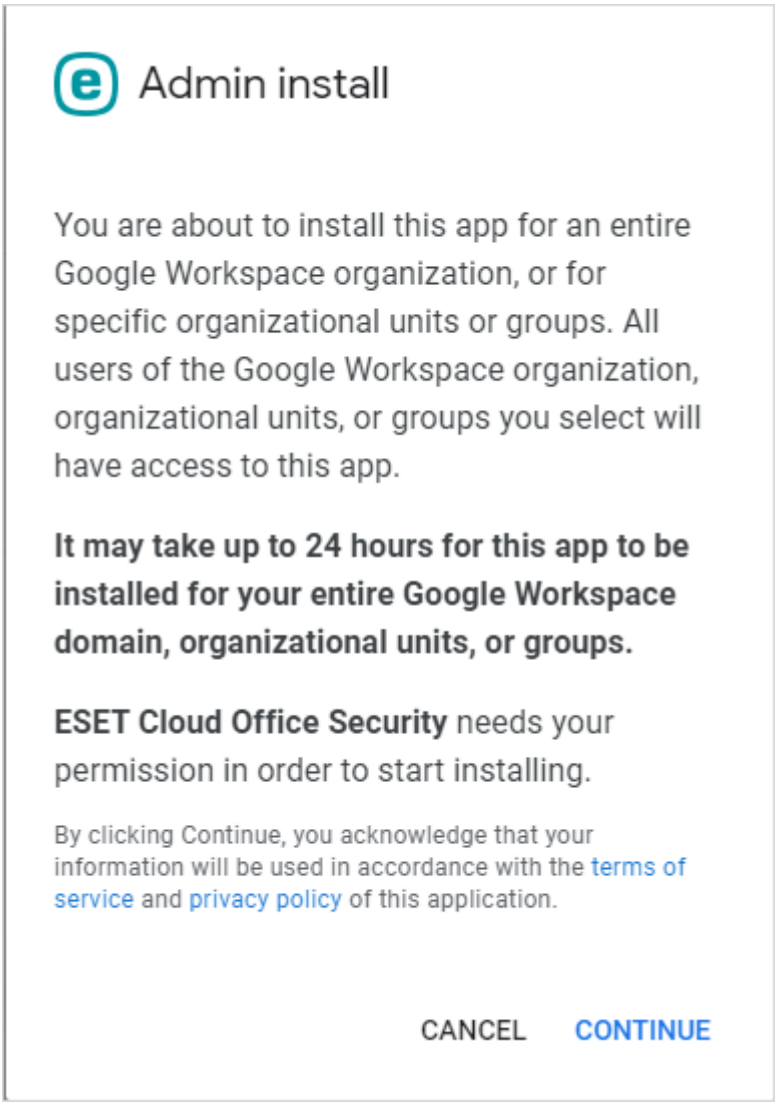
2. Клацніть плитку **Google Workspace**.



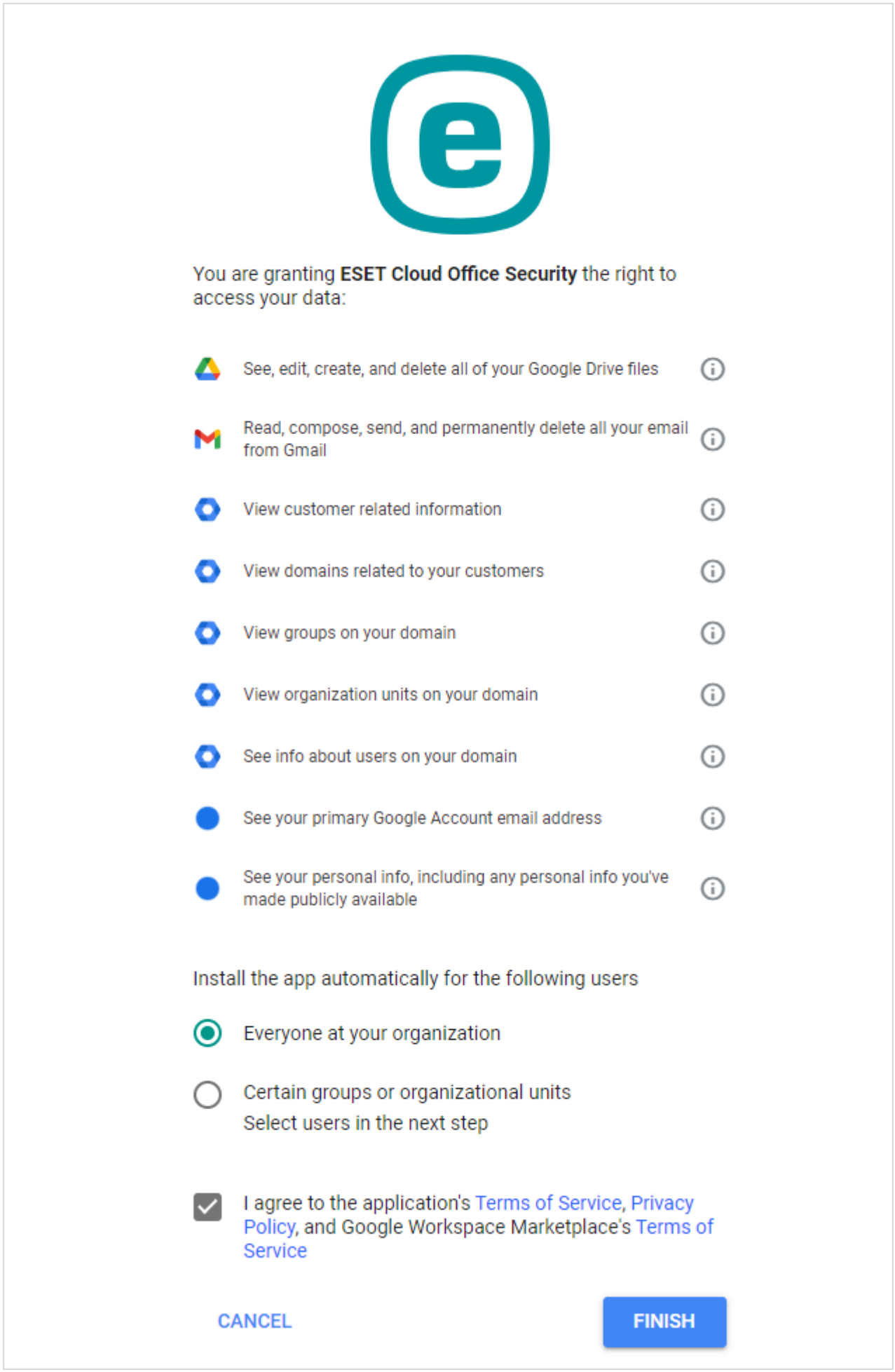
3. Клацніть Відкрити Google Workspace Marketplaceта інсталюйте програму ESET Cloud Office Security з використанням облікового запису адміністратора. Наразі програма ESET Cloud Office Security доступна в Google Workspace Marketplace лише за прямим посиланням із цього майстра.



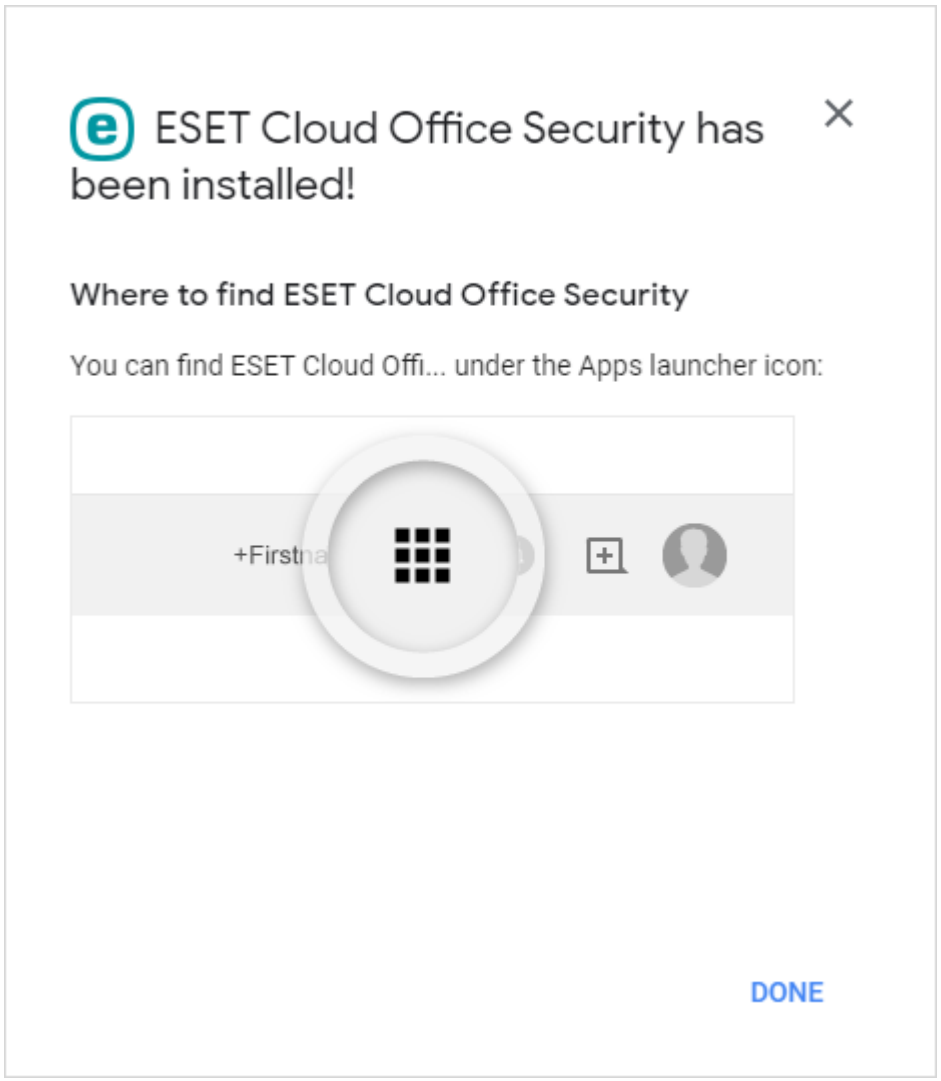
4. На екрані **Admin install** (Інсталяція адміністрування) клацніть **Продовжити**.



5. Переконайтеся, що на екрані прав доступу вибрано параметр **Everyone at your organization** (Усі у вашій організації). Окрім того, кнопка **Готово** стане доступною після встановлення прапорця згоди з умовами надання послуг і політикою конфіденційності.

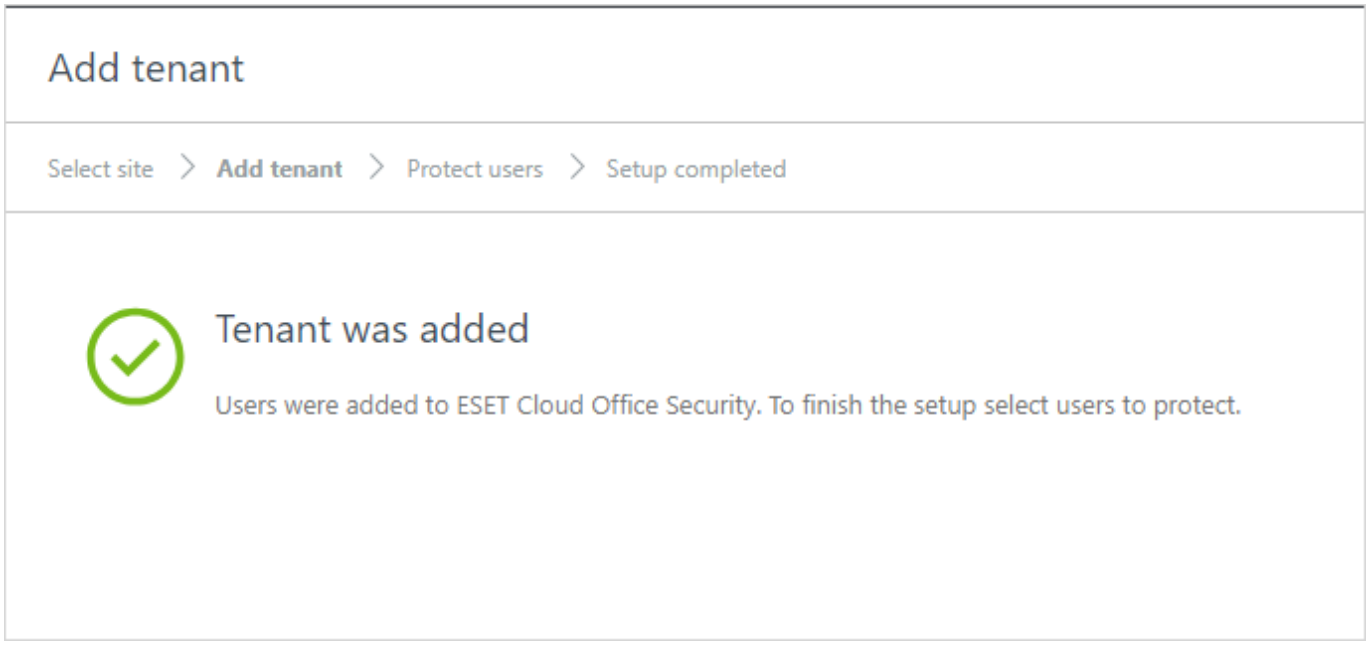

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your domain
View organization units on your domain
See info about users on your domain
See your primary Google Account email address
See your personal info, including any personal info you've made publicly available
Install the app automatically for the following users
Everyone at your organization
Certain groups or organizational units
Select users in the next step
I agree to the application's Terms of Service, Privacy Policy, and Google Workspace Marketplace's Terms of Service
CANCEL
FINISH

6. Програму ESET Cloud Office Security інстальовано, клацніть **Готово**.

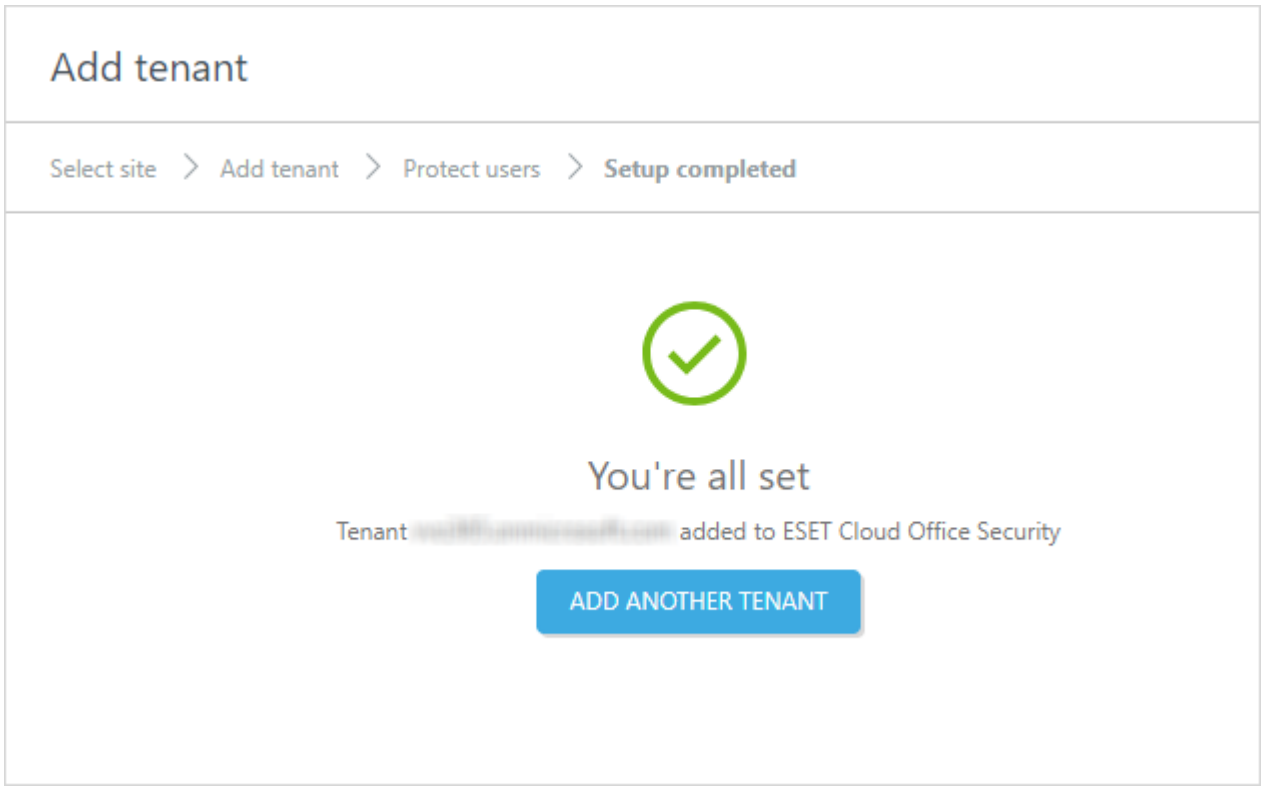


7. Після завершення роботи програми ESET Cloud Office Security поверніться на консоль ESET Cloud Office Security. Клацніть **Надати обліковий запис Google і додати клієнта**, щоб підтвердити право власності й продовжити роботу.

8. Клієнт Google Workspace було додано разом із користувачами.



9. Щоб завершити налаштування, клацніть **Далі** й виберіть користувачів для ввімкнення **захисту**. Усе готово.

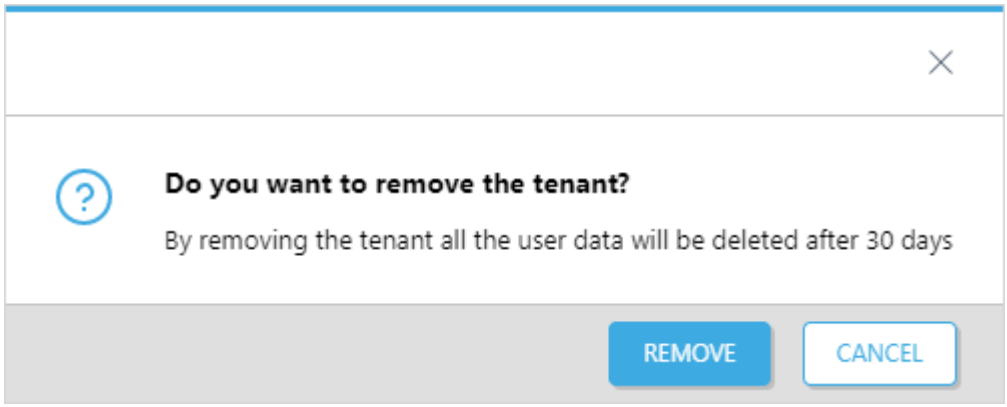


Видалити клієнта з ESET Cloud Office Security

1. Виберіть **Параметри**.

2. Виберіть потрібного клієнта й клацніть **Видалити**.

3. У вікні сповіщення зазначатиметься, що ця операція призведе до видалення всіх даних, які описані в документі Обмеження й політика збереження даних, а користувачі залишаться незахищеними. Натисніть **Видалити** для підтвердження.



Якщо видалити клієнт із консолі ESET Cloud Office Security, період збереження його даних складатиме 30 днів (через 30 днів дані карантину, журналів сканування й статистики буде видалено). Якщо протягом цих 30 днів додати видаленого клієнта, усі дані буде відновлено. Інші об'єкти (клієнти, користувачі, групи, місця, звіти, політики) остаточно видаляються через 90 днів. Докладніше див. в розділі Обмеження й політика збереження даних.

Видалення ESET Cloud Office Security з порталу Azure

1. Увійдіть на портал Azure з обліковим записом адміністратора.

Щоб видалити програму, необхідно бути власником програми або мати права адміністратора.

2. Перейдіть до служби **Azure Active Directory** й виберіть **Корпоративні програми**.

3. Знайдіть і клацніть програму **ESET Cloud Office Security** на сторінці огляду, відкрийте **Властивості** й клацніть **Видалити**.

Навігація інтерфейсом ESET Cloud Office Security

У цьому розділі описана навігація інтерфейсом ESET Cloud Office Security. Ви швидко ознайомитеся з навігаційними елементами та інструментами ESET Cloud Office Security, оскільки вони прості й зрозумілі, а також мають інтерактивну поведінку.

Панель переходів із лівого боку дозволяє переходити між розділами консолі ESET Cloud Office Security:

- Користувачі
- Команди й місця
- Виявлені об'єкти
- Карантин

Журнали сканування

Звіти

Політики

Керування ліцензією

Журнал аудиту

Налаштування

Згорнути: розкрийте й згорніть меню навігації. Згортання панелі дозволяє забезпечити додаткове місце на екрані для панелі інструментів. Щоб розгорнути панель навігації, клацніть піктограму .

Панель інструментів угорі доступна завжди:



Навігатор продукту: швидкий доступ до консолей ESET та інші корисні посилання. (Відповідні продукти можна переглядати на основі вашої ліцензії та прав доступу).

ESET Business Account і **ESET MSP Administrator** (обліковий запис гібридного ліцензування): якщо в ESET MSP Administrator і ESET Business Account зареєстровано одну адресу електронної пошти (єдиний вхід), можна переключатися між поданнями ESET Business Account і ESET MSP Administrator.

Показати сповіщення: Щоб переглянути всі сповіщення, клацніть піктограму дзвоника на панелі вгорі.

Швидкі посилання: забезпечує швидкий і простий доступ до команд Додати клієнта, Нова політика, ESET Business Account або ESET MSP Administrator.

Довідка: перше посилання цього меню завжди веде з поточного екрана до онлайн-довідки. Якщо не вдається вирішити проблему, виконайте пошук у базі знань ESET або на форумі підтримки. Крім цього, можна надіслати відгук або **надати зразок на аналіз**. Відкрийте сторінку Про програму з докладними відомостями про версію ESET Cloud Office Security і посиланнями на офіційні документи.

Користувач (наразі в системі) — Показує ім'я користувача. Клацніть **Налаштувати тему** й виберіть потрібну тему в розкривному меню:

- **Тема за замовчуванням (світла)**: ESET Cloud Office Security використовуватиметься світла колірна схема (стандартна).

- **Темна тема**: для ESET Cloud Office Security використовуватиметься темна колірна схема (темний режим).

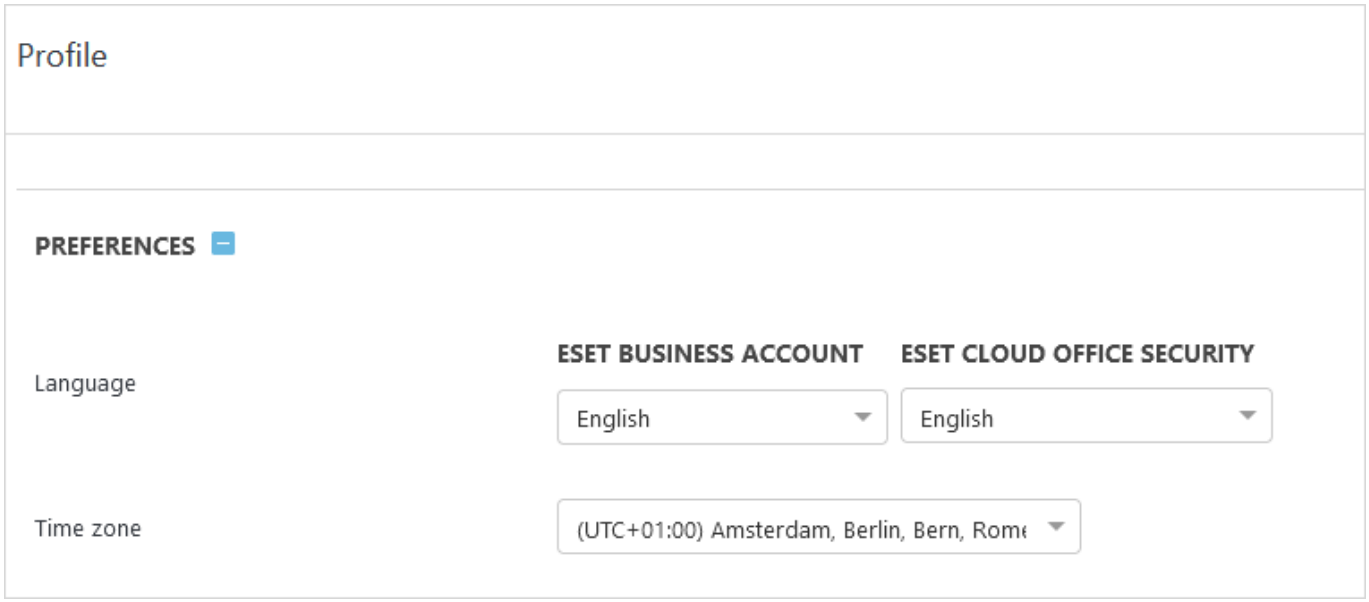
- **Тема операційної системи**: ESET Cloud Office Security буде мати колірну схему на основі

параметрів операційної системи.

Вихід: клацніть цю глобальну піктограму, щоб вийти з консолі ESET Cloud Office Security.

Зміна мови порталу ESET Cloud Office Security

Увійдіть у ESET Business Account або ESET MSP Administrator, відкрийте розділ **Керування користувачами** й клацніть **Змінити** для відповідного користувача. Перейдіть до параметри мови ESET Cloud Office Security, змініть задану мову на потрібну, клацніть **Зберегти**, а потім закрийте екран **Профіль**.



ESET LiveGuard Advanced

ESET LiveGuard Advanced забезпечує додатковий рівень безпеки завдяки використанню вдосконаленої хмарної технології ESET для виявлення нових загроз, які ще не були відомі. ESET LiveGuard Advanced захищає від можливих наслідків, спричинених новими загрозами. Якщо ESET LiveGuard Advanced виявить підозрілий код або поведінку, підозрілі об’єкти тимчасово переносяться до карантину, тому шкідливу активність буде відразу заблоковано.

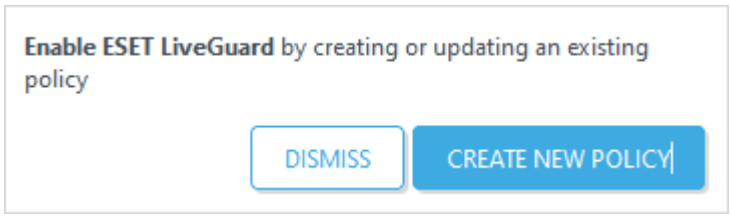
Підозрілий зразок (файл або електронний лист) автоматично надсилається в хмару ESET, де сервер ESET LiveGuard Advanced аналізує зразок із використанням найсучасніших ядер виявлення шкідливого програмного забезпечення. Поки файли або електронні листи заблоковані в карантині, ESET Cloud Office Security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

Після завершення аналізу ESET Cloud Office Security отримає звіт зі зведеною інформацією про поведінку зразка. Якщо буде встановлено, що зразок не є шкідливим, його буде розблоковано з карантину. В іншому разі він залишиться в карантині.

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 одну хвилину).

Ліцензія ESET Cloud Office Security надає право безкоштовно використовувати функцію ESET LiveGuard Advanced. У розділі Керування ліцензією поруч із ідентифікатором ліцензії відображатиметься позначка ELG.

Коли з'явиться невелике спливаюче вікно, можна активувати ESET LiveGuard Advanced. Для цього створіть нову політику або оновіть наявну.



Більш докладну інформацію про ESET LiveGuard Advanced див. в розділі Принцип роботи рівнів виявлення ESET LiveGuard Advanced .

Панель інструментів

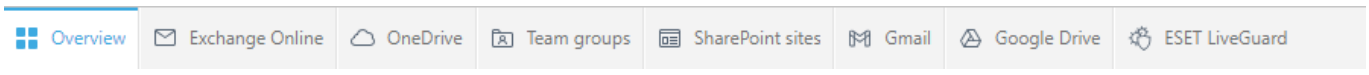
Панель інструментів — це колекція віджетів з основними відомостями про дії, пов'язані з безпекою Microsoft 365. На кожній оглядовій вкладці панелі інструментів (Огляд / Exchange Online / OneDrive / Групи команди / Сайти SharePoint, Gmail, Google Drive і ESET LiveGuard Advanced) відображається важлива інформація. **Огляд** — це основний екран панелі інструментів, який відображається під час кожного входу на консоль ESET Cloud Office Security. На цій вкладці відображається загальна й статистична інформація.

Інформація на панелі інструментів оновлюється кожні 10 хвилин. Якщо інформація на панелі інструментів не є актуальною, натисніть клавішу **F5**, щоб оновити її вручну.

Для перегляду статистику панелі інструментів скористайтеся фільтрами вгорі, щоб вибрати потрібний **період часу** ("Останні 24 години", "Останні 7 днів", "Останні 30 днів" або "Останні 90 днів") і **клієнта**. На оглядових вкладках **Exchange Online**, **OneDrive**, **Групи команди**, **Сайти SharePoint**, **Gmail**, **Google Drive** і **ESET LiveGuard Advanced** відображається додаткова статистична інформація та діаграмами щодо об'єктів виявлення. Це статистичні дані, такі як кількість відсканованих електронних листів і файлів, а також кількість виявлених електронних листів зі спамом/фішинговими програмами/шкідливими програмами. На цих діаграмах відображається трафік для кожного типа виявлення (спам, шкідливі програми й фішингові програми).

Час від часу на екрані може з'являтися панель оголошень. Колір оголошення вказує на його тип (для новин — темно-блакитний, для інформаційних повідомлень — жовтий, для попереджень — червоний).

Вкладки панелі інструментів дозволяють переходити між панелями подання:



Огляд

показує такі відомості:
• кількість клієнтів і використання ліцензій
• статистика для кожного клієнта:
oУсього користувачів / незахищених користувачів
oНайактивніші одержувачі спаму / фішингових повідомлень / шкідливого програмного забезпечення
oНайпідозріліші облікові записи OneDrive
oНайпідозріліші групи команди
oНайпідозріліші сайти SharePoint
деталізація
• Клацніть плитку Загальна кількість користувачів, щоб відкрити розділ Користувачі
• Клацніть користувача в розділі статистики (спам/фішингові програми/шкідливі програми/OneDrive), щоб переглянути відповідні виявлені об'єкти, або клацніть групу або сайт, щоб переглянути виявлені об'єкти й отримати додаткові відомості про підозрілу групу команди або підозрілий сайт SharePoint.

 Exchange Online

показує такі відомості:
• загальна кількість просканованих електронних листів
• статистика виявлених електронних листів зі спамом, шкідливими й фішинговими програмами
• окремі діаграми для спаму, шкідливих і фішингових програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

 OneDrive

показує такі відомості:
• кількість захищених користувачів
• загальна кількість відсканованих файлів
• статистика виявлених шкідливих програм
• графік із трафіком для шкідливих програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

 Групи команди

показує такі відомості:
• кількість захищених груп
• загальна кількість відсканованих файлів
• статистика виявлених шкідливих програм
• графік із трафіком для шкідливих програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

 Сайти SharePoint

показує такі відомості:
• кількість захищених сайтів
• загальна кількість відсканованих файлів
• статистика виявлених шкідливих програм
• графік із трафіком для шкідливих програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

Gmail

показує такі відомості:
• загальна кількість просканованих електронних листів
• статистика виявлених електронних листів зі спамом, шкідливими й фішинговими програмами
• окремі діаграми для спаму, шкідливих і фішингових програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

Google Диск

показує такі відомості:
• кількість захищених користувачів
• загальна кількість відсканованих файлів
• статистика виявлених шкідливих програм
• графік із трафіком для шкідливих програм
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

ESET LiveGuard Advanced

показує такі відомості:
• надіслані файли (зокрема, дублікати; тому відображувана кількість може перевищувати кількість унікальних файлів)
• виявлено об’єктів
• середній час аналізу
• графік із надісланими файлами
• власники з найбільшою кількістю переданих файлів
• типи надісланих файлів
Плитки є інтерактивними. Клацніть потрібну плитку, щоб перейти до відповідного розділу на консолі ESET Cloud Office Security. Наприклад, відкриється розділ Журнали сканування з відповідними записами журналу.

Користувачі

ESET Cloud Office Security передусім захищає обліковий запис користувача. Двічі клацніть користувача, щоб знайти корисну інформацію про нього, зокрема стислі відомості, параметри, визначені політиками, список політик, призначених користувачу, і виявлені об’єкти для Gmail, Google Диск, Exchange Online і OneDrive. Окрім того, можна вибрати користувачів, які матимуть статус "Захищено" або "Не захищено". Користувачі відсортовані за групами, кожна група є клієнтом Microsoft 365 із його користувачами. Щоб полегшити пошук певного вибраного користувача в групі, можна застосувати фільтр із множинним критерієм.

Користувачі без ліцензії Microsoft 365 не відображатимуться на консолі ESET Cloud Office Security за замовчуванням. До них належать спільні поштові скриньки без ліцензії Microsoft 365.
Щоб переглядати всіх користувачів і керувати ними в середовищі Microsoft 365, відкрийте розділ Параметри й вимкніть параметр Ліцензовані користувачі Microsoft 365.

Статус захисту:

Статус	Опис
Незахищено	Користувач наразі незахищений.
Захищено автоматично	Захищений користувач із автоматичним захистом.
Очікування	Перехідний стан, який має місце в процесі захисту користувача. Щойно він завершиться, стан користувача зміниться на "Захищено".
Захищено	Поштова скринька й OneDrive користувача наразі захищені політикою за замовчуванням або налаштовуваною політикою.
Попередження	Помилка процесу ввімкнення захисту для користувача. Могла статися помилка для ресурсів, поштової скриньки або OneDrive. Імовірно, обидва ресурси недоступні для користувача. Перевірте, чи призначено користувачу дійсну ліцензію Microsoft 365.

У дереві можна переглянути користувачів для певного клієнта або для певної групи. Щоб переглянути всіх користувачів у кожному клієнті й групі, клацніть **Усі**.

Щоб отримати більш докладну інформацію, двічі клацніть користувача або клацніть піктограму і виберіть дію (**Показати подробиці**, **Захистити** або **Зняти захист**). Клацніть користувача, щоб відкрити вікно **Показати подробиці**, яке має чотири частини:

Дія	Використання
Огляд	Показує основну інформацію про користувача, завантажену з Microsoft 365 (адреса електронної пошти, група, профіль завдання тощо). Відображається поточний статус захисту для поштової скриньки й OneDrive.
Конфігурація	Містить список параметрів і призначених політик для цього користувача (список із доступом тільки для читання). Переходьте між вкладками для перегляду конфігурації або списку призначених політик. Не можна змінювати параметри або призначати політики користувачам. Замість цього скористайтеся розділом Політики.
Виявлені об’єкти	Показати всі об’єкти, виявлені для цього облікового запису (Gmail, Google Диск, Exchange Online або OneDrive).
Карантин	Показати всі електронні листи й файли в карантині для цього користувача. Окрім того, можна виконати одну з таких дій: Розблокувати, завантажити або видалити електронні листи або файли в карантині.

Користувачів можна фільтрувати за кількома критеріями. Клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть цю дію, якщо застосовуєте декілька критеріїв):

Додати фільтр	Використання
Статус захисту	Виберіть статус користувача "Захищено", "Не захищено", "Попередження" або "Очікування".
Захищено автоматично	Показувати тільки автоматично захищених користувачів.

Додати фільтр	Використання
Назва	Уведіть дійсне ім’я користувача.
Електронна пошта	Уведіть дійсну адресу електронної пошти користувача.
Тип	Виберіть тип користувача ("Невідомий", "Користувач", "Пов’язані", "Спільна поштова скринька", "Кімната", "Обладнання", "Інші").

Захистити користувачів

1. Виберіть **користувачів**, для яких потрібно ввімкнути захист, і клацніть **Захистити**.
2. Виберіть **Пул ліцензій**, що завантажується з ESET Business Account, і клацніть **OK**. Вибрані користувачі будуть захищені з використанням політики за замовчуванням.
3. За потреби в розділіПолітики вкажіть налаштовувану політику для користувачів.

Зняти захист із користувачів

Виберіть **користувачів**, для яких потрібно скасувати захист, і клацніть **Зняти захист**.

Команди й сайти

ESET Cloud Office Security забезпечує захист для груп команди або сайтів SharePoint.

Вкладки дають змогу переключатися між групами команди і сайтами SharePoint. На них відображаються групи команди або сайти SharePoint для кожного клієнта.

Групи команди

показує об'єкти, які відносяться до типу групи Microsoft 365, зокрема сайт групи SharePoint за замовчуванням і OneDrive:

- назва
- статус
- поштове повідомлення
- клієнт

Щоб захистити розділи групи команди, переконайтеся, що принаймні один учасник групи є захищеним користувачем ESET Cloud Office Security. Кожна група Microsoft 365 має сайт групи SharePoint за замовчуванням і OneDrive, які також захищені.

Сайти SharePoint

показує всі кореневі сайти SharePoint, не пов'язані з групою Microsoft 365:

- назва
- статус
- URL-адреса
- клієнт

Сайти SharePoint, зокрема й підсайти (не показано), автоматично захищені.

Для отримання докладніших відомостей клацніть групу команди або сайт SharePoint, щоб відкрити вікно **Показати подробиці**, яке має чотири частини:

Дія	Використання
Огляд	Відображає основну інформацію про групи команди або сайти SharePoint, завантажені з Microsoft 365 (електронна пошта, власник, учасники, автор, URL-адреса тощо). Окрім того, відображається поточний статус захисту для групи команди або сайту SharePoint.
Конфігурація	Містить список параметрів і призначених політик (список із доступом тільки для читання). Переходьте між вкладками для перегляду конфігурації або списку призначених політик. У цій частині неможливо змінити налаштування або призначити політики. Це можна зробити в розділі Політики.
Виявлені об’єкти	Відображає всі виявлені об’єкти для групи команди або сайту SharePoint.
Карантин	Показати всі файли в карантині Окрім того, можна виконати одну з таких дій: Розблокувати, завантажити або видалити файли в карантині.

Клацніть **Додати фільтр**, щоб відфільтрувати групи команди або сайти SharePoint.

Виявлені об’єкти

Виводить усі об’єкти, виявлені ESET Cloud Office Security. Вкладки дозволяють переключатися між розділами Gmail, Google Диск, Exchange Online, OneDrive, Групи команди і Сайти SharePoint. Переглядайте інформацію про кожний виявлений об’єкт, наприклад про виявлені файли, які були додані до групи команди на вкладці Групи команди.

Клацніть піктограму , щоб відкрити бічну панель зі зведеними даними про певний запис журналу (виявлений об’єкт). Щоб отримати більш докладну інформацію, клацніть піктограму й виберіть **Показати подробиці**.

У дереві можна переглянути виявлені об’єкти тільки для певного клієнта або для певної групи. Щоб переглянути виявлені об’єкти в кожному клієнті або групі, клацніть **Усі**. Щоб полегшити пошук певного вибраного об’єкта, можна застосувати фільтр із множинним критерієм. Клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть, якщо застосовуєте критеріїв):

Додати фільтр	Використання
Початок періоду події	Укажіть початкову дату діапазону.
Закінчення періоду події	Укажіть кінцеву дату діапазону.
Тема	Застосовується до повідомлень, які містять або не містять певний рядок (або регулярний вираз) у темі.
Повідомлення	Фільтруйте електронні листи за унікальним ідентифікатором повідомлення під час пошуку певного повідомлення, особливо у великих журналах, які містять багато повідомлень або дані про числені спроби доставки.
Від	Фільтрувати повідомлення за відправником.
До	Фільтрувати повідомлення за отримувачами.
Поштова скринька	Застосовується до повідомлень, розташованих у певний поштовій скриньці.

Додати фільтр	Використання
Результат сканування	Виберіть один із варіантів нижче. "Шкідливе програмне забезпечення", "Шкідливе програмне забезпечення" (виявлене ESET LiveGuard Advanced), "Фішинг" або "Спам".
Дія	Виберіть одну з доступних дій.
Команда	Уведіть дійсне ім’я команди.
Сайт	Уведіть дійсне ім’я сайту.
Об’єкт	Уведіть дійсне ім’я об’єкта.
Виявлений об’єкт	Уведіть дійсне ім’я виявленого об’єкта.
Хеш	Уведіть дійсний хеш виявленого об’єкта.

Після клацання піктограми параметр **Видалити об’єкти, що належать до білого списку** буде доступний, якщо ви помістили до білого списку файл, раніше розблокований із карантину для того ж самого користувача. Використовуйте цей параметр для видалння файлу з білого списку. Усі подібні файлу надалі будуть поміщатися в карантин.

> Період зберігання для виявлених об’єктів складає 90 днів. Записи, старіші за 90 днів, видалятимуться остаточно.

Повідомити про помилкове спрацювання (FP) / помилковий негативний результат (FN)

Можна вручну повідомити про помилкові спрацювання й помилкові негативні результати в категоріях "Спам", "Фішинг" або "Шкідливе програмне забезпечення", надіславши відповідні зразки до лабораторій ESET для аналізу. Адреса електронної пошти для надсилання зразків:

Спам: електронні листи, помилково визначені як спам, надішліть нам на адресу nospam_ecos@eset.com; електронні листи категорії "спам", які не було визначено як спам, надішліть нам на адресу spam_ecos@eset.com. Оригінальні електронні листи надішліть як вкладення у форматі *.eml* або *.msg*.

Фішинг: щоб повідомити про помилкове спрацювання або про помилковий негативний результат щодо фішингових повідомлень, надішліть електронного листа на адресу samples@eset.com. У темі електронного листа вкажіть *'phishing email'*. Фішингові повідомлення надайте як вкладення у форматі *.eml* або *.msg*.

Шкідливе програмне забезпечення: щоб повідомити про помилкове спрацювання або про помилковий негативний результат щодо шкідливого програмного забезпечення, надішліть електронного листа на адресу samples@eset.com. У темі електронного листа вкажіть *'False positive'* або *'Suspected infection'*. Шкідливе програмне забезпечення надайте як вкладення у форматі *.zip* або *.rar*.

Звіти

У звітах ESET Cloud Office Security надається огляд статистики захисту ESET Cloud Office Security. Можна вибрати один із двох типів звітів (статичні або звіти про поштовий карантин).

Статистичні звіти містять інформацію про захист Gmail, Google Диск, Exchange Online, OneDrive, груп команди і сайтів SharePoint: кількість перевірених електронних листів, файлів, виявлених шкідливих програм, фішингових посилань і спаму за вказаний проміжок часу. Звіти можна

створювати вручну й завантажувати у форматах *PDF* або *CSV*. Окрім того, можна запланувати надіслання звітів вибраним одержувачам електронною поштою. Звіти у форматі *PDF* містять графічне подання даних, довгострокові середні показники для порівняння, дані про трафік для кожного типу захисту, а також відомості про основних отримувачів шкідливого програмного забезпечення, фішингових посилань і спаму.

Звіт про поштовий карантин містить список нових об'єктів, перенесених в карантин. Цей звіт надсилається вибраним одержувачам електронною поштою. Одержувачі можуть розблокувати повідомлення зі спамом (якщо вони вважають їх безпечними). Для цього потрібно клацнути посилання **Розблокувати**. Застосовується тільки до спаму. Інші типи об'єктів у карантині неможливо розблокувати.

Можна налаштувати отримання статистичних даних електронною поштою, щоб не входити на консоль ESET Cloud Office Security. Налаштуйте й заплануйте повторювані звіти й вкажіть адреси отримувачів. Окрім цього, можна створити статистичний звіт прямо на консолі ESET Cloud Office Security. Виберіть наявний звіт (зокрема, це може бути запланований звіт) і клацніть **Створити й завантажити**. Окрім того, звіт можна клацнути правою кнопкою миші й вибрати відповідний пункт в розкривному меню. Можна легко створити новий шаблон звіту зі спеціальними параметрами.

Новий звіт

Натисніть Новий звіт, щоб відкрити майстер шаблонів звітів і вказати налаштовувані параметри. Уведіть назву й опис звіту.

Мова

У розкривному меню виберіть потрібну мову. Буде створено звіт вибраною мовою.

Тип

Виберіть, які типи слід включати в статистику.

Статистичні звіти

Створіть заплановані звіти або звіти за вимогою, в яких буде міститися інформація відповідно до вибраних вами параметрів.

Надіслати звіти про поштовий карантин

Щоб інформувати користувачів про нові електронні листи в карантині, надсилайте вибраним користувачам сповіщення електронною поштою. Можна призначити одного або кількох одержувачів або групу одержувачів. Виберіть інтервал для звітів, а також початкову дату й час. Якщо налаштовано повторюваний звіт, виберіть, коли має завершуватися його надсилання (на певну дату, через певну кількість повторних надсилань або ніколи). Надсилання звіту про поштовий карантин активується тільки за наявності нових елементів для включення в нього. Одержувачі звіту можуть розблокувати повідомлення зі спамом (якщо вони вважають їх безпечними). Для цього потрібно клацнути посилання Розблокувати (після цього у веб-браузері відкриється вікно підтвердження). Розблоковане повідомлення зі спамом надсилається окремим електронним листом як вкладення.

Клієнт

Цей параметр доступний тільки для середовища з кількома клієнтами. Можна вибрати кількох клієнтів, для яких буде згенеровано статистичні звіти. Звіти створюються для кожного клієнта окремо й надсилаються одним електронним листом ESET Cloud Office Security із кількома вкладеннями.

Проміжок часу

Укажіть проміжок часу для відображення результатів (останні 24 години, тиждень, місяць). Якщо вибрати параметр Спеціальний, можна вказати діапазон ("Дата від" і "Дата до").

Вивід

Виберіть потрібний формат файлу (можна вибрати *PDF* або *CSV*). У звіті формату *PDF* міститься графічне подання даних. У звіті формату *CSV* містяться необроблені дані. Звіти збираються відповідно до вказаних параметрів. Якщо ви вибрали дані Gmail, Google Диск, Exchange Online і дані OneDrive, груп команди або сайтів SharePoint, вихідний файл буде архівним файлом у форматі ZIP зі звітом у файлі *PDF* або *CSV*.

Біла мітка

Якщо потрібно, щоб у звіті був логотип вашої компанії, увімкніть цю функцію. Для відображення ви можете вибрати два варіанти: показувати в заголовку ваш логотип разом із логотипом ESET або показувати тільки ваш логотип. Передайте логотип у форматі *PNG* або *JPEG*.

За розкладом

Планувальник дозволяє створити звіти на певну дату й час, а також налаштувати регулярне створення звітів. Заплановані звіти доставляються до вибраних одержувачів у вкладеннях електронних листів від ESET Cloud Office Security.

Повторювати

Виберіть частоту створення звітів (один раз або регулярне створення):

- **Одноразово**: звіт буде створено один раз.
- **Щодня**: звіти регулярно створюються й надсилаються кожного дня (якщо не задано граничну кількість звітів для надсилання).
- **Щотижня**: звіти створюються й надсилаються щотижня у вибрані дні.
- **Щомісячно**: звіти створюються й надсилаються раз на місяць у вибраний день.

Починаючи з

Виберіть початкову дату для звітів.

Завершується

Виберіть час завершення регулярного створення звітів.

Одержувачі

Укажіть адресу електронної пошти одержувача. Натисніть клавішу ENTER для підтвердження.

За потреби додайте таким чином кількох одержувачів.

Щоб отримати докладнішу інформацію або виконати певну дію, клацніть піктограму і виберіть дію:

Дія	Використання
Показати подробиці	Відображає докладні відомості про звіт.
Створити й завантажити	Клацніть Створити й завантажити й виберіть *PDF* або *CSV*. У звіті формату *PDF* міститься графічне подання даних. У звіті формату *CSV* містяться необроблені дані. Звіти збираються відповідно до вказаних параметрів. Якщо ви вибрали дані Exchange Online і дані OneDrive, груп команди або сайтів SharePoint, вихідний файл буде архівним файлом у форматі *ZIP* зі звітом у файлі PDF або *CSV*
Змінити	Дозволяє змінювати конфігурацію наявного звіту.
Видалити	Дозволяє повністю видалити вибраний звіт.

Щоб фільтрувати звіти, клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть цю дію, якщо застосовуєте декілька критеріїв):

Додати фільтр	Використання
Назва	Уведіть назву звіту (частково або повністю).
За розкладом	Виберіть параметр "Не заплановано", "Одноразово", "Щодня", "Щотижня" або "Щомісячно".
Дані	Виберіть Exchange Online, OneDrive, групи команди або сайти SharePoint, які потрібно фільтрувати за даними.

Карантин

Просте керування об’єктами (електронні листи й файли), які поміщені ESET Cloud Office Security в карантин. Вкладки дають змогу переключатися між розділами Gmail, Google Диск, Exchange Online, OneDrive, "Групи команди" і "Сайти SharePoint". Виводяться докладні відомості про кожний об’єкт.

Клацніть піктограму , щоб відкрити бічну панель зі зведеними даними про певний об’єкт. Щоб отримати більш докладну інформацію, клацніть піктограму й виберіть **Показати подробиці**.

У дереві можна переглянути виявлені об’єкти тільки для певного клієнта або для певної групи. Щоб переглянути виявлені об’єкти в кожному клієнті або групі, клацніть **Усі**.

Перевірте електронні листи або файли в карантині й виконайте відповідну дію (**Видалити** або **Розблокувати**). Окрім того, можна **завантажити** оригінальний файл або файл, захищений паролем у форматі *.zip*.

Якщо виявлений об’єкт не є шкідливим (помилкове спрацювання), можна **розблокувати** файл із карантину. Розблокований файл автоматично поміщається до білого списку (на основі хешу). Усі майбутні виявлення цього файлу для цього користувача не будуть розглядатися як підозрілі, і не будуть поміщатися в карантин. Автоматичне внесення в білий список виконується для кожного окремого користувача. Для інших користувачів той самий файл буде виявлятися як підозрілий і поміщатися в карантин.
Для видалення файлу з білого списку в списку Виявлені об’єкти можна скористатися параметром **Видалити об’єкти, що належать до білого списку**.

Клацніть піктограму ⋮ й виберіть дію:

Дія	Використання
Показати подробиці	Показує більш докладну інформацію про електронний лист у карантині.
Розблокувати (електронні листи або файли)	Дозволяє розблокувати надсилання електронних листів їх отримувачам у формі електронних листів зі сповіщенням, вкладеннями до яких будуть оригінальні повідомлення. Якщо йдеться про елемент OneDrive, файл передаватиметься в оригінальне розташування у OneDrive цього користувача. Якщо випустити файл із групи команди або сайту SharePoint, він знову з’явиться у вихідному розташуванні. Розблокований файл автоматично поміщається до білого списку (на основі хешу). Це запобігає повторному потраплянню файлу в карантин.
Видалити	Видаляє елемент із карантину.
Завантажити оригінальний файл	Дозволяє завантажити незахищений файл у його оригінальній формі.
Завантажити архів, захищений паролем	Дозволяє завантажити архів, захищений паролем.
Надіслати зразок	У діалоговому вікні надсилання зразків можна надіслати підозрілий файл або спам для аналізу в ESET. У розкривному меню виберіть пункт Причини надсилання.

Щоб полегшити пошук певного об’єкта в карантині, можна застосувати фільтр із множинним критерієм. Клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть, якщо застосовуєте критеріїв):

Додати фільтр	Використання
Початок періоду події	Укажіть початкову дату діапазону.
Закінчення періоду події	Укажіть кінцеву дату діапазону.
Тема	Застосовується до повідомлень, які містять або не містять певний рядок (або регулярний вираз) у темі.
Повідомлення	Фільтруйте електронні листи за унікальним ідентифікатором повідомлення під час пошуку певного повідомлення, особливо у великих журналах, які містять багато повідомлень або дані про числені спроби доставки.
Від	Фільтрувати повідомлення за відправником.
До	Фільтрувати повідомлення за отримувачами.
Поштова скринька	Застосовується до повідомлень, розташованих у певний поштовій скриньці.

Додати фільтр	Використання
Результат сканування	Виберіть один із варіантів нижче. "Шкідливе програмне забезпечення", "Шкідливе програмне забезпечення" (виявлене ESET LiveGuard Advanced), "Фішинг" або "Спам".
Команда	Уведіть дійсне ім’я команди.
Об’єкт	Уведіть дійсне ім’я об’єкта.
Сайт	Уведіть дійсне ім’я сайту.

Період зберігання об’єктів у карантині складає 30 день. Об’єкти, старіші за 30 день, будуть видалятися з карантину остаточно.

Журнали сканування

У цьому розділі виводяться всі результати сканування ESET Cloud Office Security. Журнали подібні до розділу Виявлені об'єкти, але ви також можете додавати до списку очищені об'єкти (увімкніть параметр «Реєструвати всі об'єкти» в налаштуваннях політик). Вкладки дозволяють переключатися між розділами Gmail, Google Диск, Exchange Online, OneDrive, Групи команди, Сайти SharePoint і Надіслані файли. Кожний виявлений об’єкт містить значну кількість інформації. У розділі "Надіслані файли" відображається список файлів, надісланих у ESET LiveGuard Advanced для аналізу.

Клацніть піктограму , щоб відкрити бічну панель зі зведеними даними про певний запис журналу. Щоб отримати більш докладну інформацію, клацніть піктограму й виберіть **Показати подробиці**.

У дереві можна переглянути записи журналу тільки для певного клієнта або для певної групи. Щоб переглянути виявлені об’єкти в кожному клієнті або групі, клацніть **Усі**.

Якщо результатом сканування є **Не перевірено**, причина може бути іншою. Більш докладні відомості див. в розділі Обмеження.

Якщо клацнути піктограму шестерні у верхньому правому куті, щоб скористатися можливістю **Експортувати в CSV** в контекстному меню, можна експортувати сітку таблиці у формат *CSV* та використовувати її в інших програмах для роботи зі списками.

Щоб полегшити пошук певного запису журналу, можна застосувати фільтр із множинним критерієм. Клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть, якщо застосовуєте критеріїв):

Додати фільтр	Використання
Початок періоду події	Укажіть початкову дату діапазону.
Закінчення періоду події	Укажіть кінцеву дату діапазону.
Джерело даних	Виберіть один із варіантів нижче. Exchange Online, OneDrive, Група команди і Сайт SharePoint.
Поштова скринька	Застосовується до повідомлень, розташованих у певний поштовій скриньці.
Від	Фільтрувати повідомлення за відправником.

Додати фільтр	Використання
До	Фільтрувати повідомлення за отримувачами.
Тема	Застосовується до повідомлень, що містять або не містять певний рядок у темі.
Повідомлення	Фільтруйте електронні листи за унікальним ідентифікатором повідомлення під час пошуку певного повідомлення, особливо у великих журналах, які містять багато повідомлень або дані про числені спроби доставки.
Результат сканування	Виберіть один із варіантів нижче. "Шкідливе програмне забезпечення", "Шкідливе програмне забезпечення" (виявлене ESET LiveGuard Advanced), "Фішинг", "Спам", "Очищено", "Не перевірено", "Помилка" або "Вимкнуто".
Дія	Виберіть одну з доступних дій.
Власники	Уведіть дійсне ім’я власника.
Об’єкт	Уведіть дійсне ім’я об’єкта.
Виявлений об’єкт	Уведіть дійсне ім’я виявленого об’єкта.
Хеш	Уведіть дійсний хеш виявленого об’єкта.
Команда	Уведіть дійсне ім’я команди.
Сайт	Уведіть дійсне ім’я сайту.

Записи журналів зберігаються 90 днів. Записи, старіші за 90 днів, видалятимуться остаточно. Якщо у вас є політика, що використовує параметр **Реєструвати всі об’єкти**, записи журналу з результатом сканування **Очищено** зберігатимуться протягом 3 днів. Результати сканування зі статусом "Очищено", старіші за 3 дні, видалятимуться остаточно.

Політики

Організації більшого розміру зазвичай мають декілька відділів, і вам потрібно налаштувати різні параметри захисту для кожної організаційної одиниці. ESET Cloud Office Security дає змогу застосовувати параметри захисту на основі політик, які можна налаштувати й призначити вибраним користувачам і групам користувачів, клієнтам, групам команди або сайтам SharePoint.

Щоб додати критерій фільтрації, клацніть **Додати фільтр** і виберіть застосовний елемент **Ім’я** й уведіть дійсне ім’я політики. У дереві "Політики" відображаються клієнти та їхні групи користувачів, групи команди або сайти SharePoint, зокрема група **Не призначено**, що містить налаштовувані політики, які не призначені жодному користувачу.

Можна додати нову політику або змінити наявну політику та її параметри:

1. Натисніть **Політики** > **Створити політику**.

2. Уведіть **ім’я** й **опис** нової політики.

3. Виберіть цільовий об’єкт і налаштуйте політику для таких категорій:

   • **Клієнти** – Дозволяє налаштувати захист Gmail, Google Диск, Exchange Online, OneDrive, сайтів SharePoint і груп команди, а також призначити їх вибраним клієнтам

   • **Користувачі**: дає змогу налаштувати захист Gmail, Google Диск, Exchange Online і OneDrive, а

також призначити його вибраним користувачам або групам користувачів

• **Групи команди**: дає змогу налаштувати захист груп команди і призначити його вибраним групам команди

• **Сайти SharePoint**: дає змогу налаштувати захист сайтів SharePoint і призначити його вибраним сайтам

4. Налаштуйте параметри **захисту** для Exchange Online, Gmail, OneDrive, Google Drive, Team groups, SharePoint sites або ESET LiveGuard Advanced і клацніть **Далі**.

5. Натисніть **Призначити** й виберіть цільовий об'єкт, якому буде призначено політику.

6. Клацніть **Зберегти зміни**, щоб зберегти налаштування політики.

Основи політики

Політика за замовчуванням • Застосовується до всіх користувачів (захищених і не захищених) • Неможливо змінити або видалити
Налаштовувану політику можна призначити таким цільовим елементам: • **Користувачі**: застосовується до окремих користувачів, вибраних уручну • **Групи**: політика застосовується до всіх учасників групи користувачів • **Клієнти**: політика, яка застосовується до всіх об'єктів у клієнті • **Групи команд**: політика застосовується до групи команди. • **Сайти SharePoint**: політика застосовується до сайту SharePoint.
Налаштовувана політика, призначена **клієнту** або **групі**, зливається з політикою за замовчуванням Налаштовувана **політика клієнта**, **політика групи**, **політика груп команди** або **політика сайтів SharePoint** має пріоритет над політикою за замовчуванням Налаштовувана політика, призначена **користувачу**, об'єднується з політикою **клієнта**, **групи**,**груп команди**, **сайтів SharePoint**, а також політикою за замовчуванням Налаштовувана політика **користувача** має пріоритет по відношенню до політики клієнта або групи й політики за замовчуванням. Проте коли користувач завантажує файл у групу команди або на сайт SharePoint, застосовується політика для групи команди або сайту SharePoint.
Для користувачів і клієнтів можна призначити кілька **настроюваних політик**, проте ефективна політика визначається на основі пріоритету (порядку).

Налаштування для списків антиспаму під час об'єднання політик

Об’єднання застосовується до параметрів Списки антиспаму й Сповіщати адміністратора (адреси для електронних листів зі сповіщеннями від модулів "Захист від шкідливого програмного забезпечення" і "Захист від фішинг-атак").
Якщо у вас кілька політик зі списками антиспаму (списки дозволених, заблокованих та ігнорованих IP-адрес, доменів або адрес електронної пошти) або кілька адрес адміністраторів модулів "Захист від шкідливого програмного забезпечення" і "Захист від фішинг-атак", виберіть стратегію об’єднання:
Замінити: зберегти тільки нові записи списку (за замовчуванням). Усі списки з попередніх політик замінюються новими списками поточної політики.
Додати в кінець: розширити списки попередніх політик через додавання нових записів. Об’єднати списки з попередніх політик із новими записами поточної політики. Нові записи розміщуються в кінці (внизу) наявних списків попередніх політик.



Раніше (ще до того, як з’явилася можливість вибору варіанта об’єднання) за замовчуванням використовувалася стратегія **заміни**. Якщо ви вже використовуєте політики з певними списками антиспаму, можна залишити варіант **Замінити**. Проте за потреби його можна змінити на **Додати в кінець**.

Створіть нову політику з визначеним списком антиспаму й виберіть варіант об’єднання (за умови наявності політик зі списками антиспаму).
1. Натисніть **Політики** > **Створити політику**.
2. Уведіть **ім’я** й **опис** для нової політики, виберіть для цільового об’єкта параметр **Клієнти** й клацніть **Далі**.
3. Розгорніть **Exchange Online – Антиспам** і клацніть **Змінити** поруч із пунктом "Список заблокованих IP-адрес".
4. Клацніть **Додати**, уведіть IP-адресу, натисніть клавішу **ENTER** для завершення дії (або імпортуйте список із файлу), потім клацніть **Зберегти зміни**.
5. У розкривному меню для варіанта об’єднання виберіть **Додати в кінець** і клацніть **Далі**.
6. Клацніть **Призначити**, у розкривному меню виберіть пункт **Призначити клієнтам**, установіть прапорець поруч із клієнтом і клацніть **OK**.
7. Клацніть **Зберегти зміни**, щоб завершити процес.

Щоб змінити пріоритет політики, клацніть **Змінити порядок**. Виберіть політику або кілька політик і клацніть **Застосувати швидше** або **Застосувати пізніше**, щоб змінити їх пріоритет. Політики застосовуються глобально (незалежно від того, кому вони призначені — клієнту, групі або користувачу) в указаному порядку згори донизу. Найпершою завжди застосовується політика за замовчуванням.

Щоб виконати вказані нижче дії, виберіть політику й клацніть піктограму :

Дія	Використання
Показати подробиці	Виводьте докладну інформацію про створену політику, налаштування й об’єкти, яким призначено політики.
Змінити	Змініть конфігурацію наявної політики.
Призначити	Виберіть користувачів, клієнтів, групи команди або сайти SharePoint, до яких застосовується політика.

Дія	Використання
Копіювати	Створіть нову політику на основі вибраного шаблону. Для дубльованої політики необхідно вказати нове ім’я.
Видалити	Повністю видаляє вибрану політику.

Створіть налаштовувану політику клієнта, щоб переглянути всі результати сканування (зокрема, безпечні об’єкти) в розділі Журнали сканування. Політика клієнта застосовується до всіх користувачів (захищених і не захищених).
1. Натисніть **Політики** > **Створити політику**.
2. Уведіть **ім’я** й **опис** для нової політики, виберіть для цільового об’єкта параметр **Клієнти** й клацніть **Далі**.
3. Розгорніть розділ **Exchange Online – Загальні налаштування** й за допомогою повзунка ввімкніть параметр **Реєструвати всі об’єкти**.
4. Розгорніть розділ **OneDrive – Загальні налаштування** й за допомогою повзунка ввімкніть параметр **Реєструвати всі об’єкти**.
5. Розгорніть розділ **Групи команди - Загальні налаштування** й за допомогою повзунка ввімкніть параметр **Реєструвати всі об’єкти**.
6. Розгорніть розділ **Сайти SharePoint – Загальні налаштування** й за допомогою повзунка ввімкніть параметр **Реєструвати всі об’єкти**, а потім клацніть **Далі**.
7. Клацніть **Призначити**, установіть прапорець поруч із клієнтом, потім клацніть **OK**.
8. Клацніть **Зберегти зміни**, щоб завершити процес.

Створіть налаштовувану політику для певних користувачів із додатковими параметрами, які визначають операції, що будуть виконуватися для шкідливого програмного забезпечення, спаму й фішингових програм. Якщо діє ця політика, поштові вкладення зі шкідливим програмним забезпеченням будуть видалятися, спам буде переміщуватися в папку спаму цього користувача, тема фішингових повідомлень буде відповідним чином помічена, а вони будуть поміщені в карантин, вміст шкідливих файлів, розташованих у OneDrive, буде замінений звичайним текстом, щоб виключити завдання шкоди.
1. Натисніть **Політики** > **Створити політику**.
2. Уведіть **ім’я** й **опис** для нової політики, виберіть для цільового об’єкта параметр **Користувачі** й клацніть **Далі**.
3. Розгорніть **Exchange Online – Захист від шкідливого програмного забезпечення**. У розкривному меню поруч із параметром **Під час повідомлення про елементи** виберіть пункт **Видалити вкладення**.
4. Розгорніть **Exchange Online – Антиспам** і у розкривному меню поруч із параметром "**У разі виявлення елементів**" виберіть пункт **Перемістити в спам**.
5. Розгорніть розділ **Exchange Online – Захист від фішинг-атак** і за допомогою повзунка ввімкніть параметр **Додавати до теми тег**. Окрім того, можна змінити текст, указаний у параметрі **Додавати до теми тег**.
6. Розгорніть **OneDrive – Захист від шкідливого програмного забезпечення** і в розкривному меню поруч із пунктом **Якщо про елементи повідомлено** виберіть **Замінити** й клацніть **Далі**.
7. Клацніть **Призначити**, установіть прапорці поруч із користувачами, до яких потрібно застосувати політику, і клацніть **OK**. Якщо для користувача застосована наявна налаштовувана політика, її буде перевизначено новою.
8. Клацніть **Зберегти зміни**, щоб завершити процес.

Параметри захисту для Exchange Online

У цьому розділі наведено відомості про зміну параметрів "Exchange Online – Загальні налаштування", "Захист від шкідливого програмного забезпечення", "Антиспам" або "Захист від фішинг-атак".

Exchange Online – Загальні налаштування

ESET LiveGrid®Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Докладніше про ESET LiveGrid® див. в глосарії .
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Політикою зберігання для очищення результатів сканування задано термін три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

Exchange Online – Захист від шкідливого програмного забезпечення

Увімкнути Exchange Online – захист від шкідливого програмного забезпечення
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, надіслати листа одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
• **Видалити вкладення**: вкладення повідомлення буде видалено й доставлено одержувачу без вкладення.
• **Замінити вкладення**: вкладення замінюється текстовим файлом, що містить докладні відомості про виконану дію.
• **Відправити вкладення в карантин**: вкладення видаляється з електронного листа й переміщається в карантин файлів.
Текст, яким потрібно замінювати вкладення
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
Сповіщати власника поштової скриньки
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Мова
У розкривному меню виберіть потрібну мову. Власник поштової скриньки отримуватиме електронні листи зі сповіщеннями вибраною мовою, коли об’єкт вилучається з карантину Exchange Online. Цей параметр перевизначає мову клієнта за замовчуванням у налаштуваннях.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, скористайтеся клавішею ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Exchange Online – Антиспам

Увімкнути Exchange Online – Антиспам
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, надіслати листа одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
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. Окрім того, можна імпортувати спеціальний список із файлу, а не додавати вручну кожен окремий запис. Для цього клацніть **Імпортувати** й знайдіть файл (*.txt*) із записами, які потрібно додати в список. Аналогічно, якщо потрібно експортувати наявний список у файл (*.txt*), у контекстному меню виберіть пункт **Експорт**.

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.
Список дозволених відправників	Додає в білий список електронні листи від указаного відправника або домену. Тільки одна адреса відправника або цілий домен використовується для верифікації на основі такого пріоритету: 1.Адреса SMTP "MAIL FROM" 2."Return-Path:" поле заголовка електронного листа 3."X-Env-Sender:" поле заголовка електронного листа 4."From:" поле заголовка електронного листа 5."Sender:" поле заголовка електронного листа 6."X-Apparently-From:" поле заголовка електронного листа
Список заблокованих відправників	Блокує електронні листи від указаного відправника або домену. Усі ідентифіковані адреси відправника або цілі домени використовуються для верифікації таких атрибутів: Адреса SMTP "MAIL FROM" "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:" поле заголовка електронного листа

Exchange Online – Захист від фішинг-атак

Увімкнути Exchange Online – Захист від фішинг-атак
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Під час повідомлення про елементи
• **Пропустити**: нічого не робити, надіслати електронні листи зі шкідливими вкладеннями одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
Сповіщати власника поштової скриньки
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти для будь-якого користувача Exchange Online.

Параметри захисту для Gmail

У цьому розділі надано інформацію про зміну параметрів "Загальні налаштування Gmail", "Захист від шкідливого програмного забезпечення", "Антиспам" або "Захист від фішинг-атак".

Загальні налаштування Gmail

ESET LiveGrid®Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Докладніше про ESET LiveGrid® див. в глосарії .
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Політикою зберігання для очищення результатів сканування задано термін три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

Захист від шкідливого програмного забезпечення у Gmail

Увімкнути захист від шкідливого програмного забезпечення для Gmail
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, надіслати листа одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
• **Видалити вкладення**: вкладення повідомлення буде видалено; повідомлення буде доставлено одержувачу без вкладення.
• **Замінити вкладення**: вкладення замінюється текстовим файлом, що містить докладні відомості про виконану дію.
• **Відправити вкладення в карантин**: вкладення видаляється з електронного листа й переміщається в карантин файлів.
Текст, яким потрібно замінювати вкладення
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
Сповіщати власника поштової скриньки
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Мова
У розкривному меню виберіть потрібну мову. Власник поштової скриньки отримуватиме електронні листи зі сповіщеннями вибраною мовою, коли об’єкт вилучається з карантину. Цей параметр перевизначає мову клієнта за замовчуванням у налаштуваннях.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, скористайтеся клавішею ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Захист від спаму в Gmail

Увімкніть захист від спаму для Gmail
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, надіслати листа одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
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. Окрім того, можна імпортувати спеціальний список із файлу, а не додавати вручну кожен окремий запис. Для цього клацніть **Імпортувати** й знайдіть файл (*.txt*) із записами, які потрібно додати в список. Аналогічно, якщо потрібно експортувати наявний список у файл (*.txt*), у контекстному меню виберіть пункт **Експорт**.

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.
Список дозволених відправників	Додає в білий список електронні листи від указаного відправника або домену. Тільки одна адреса відправника або цілий домен використовується для верифікації на основі такого пріоритету: 1.Адреса SMTP "MAIL FROM" 2."Return-Path:" поле заголовка електронного листа 3."X-Env-Sender:" поле заголовка електронного листа 4."From:" поле заголовка електронного листа 5."Sender:" поле заголовка електронного листа 6."X-Apparently-From:" поле заголовка електронного листа
Список заблокованих відправників	Блокує електронні листи від указаного відправника або домену. Усі ідентифіковані адреси відправника або цілі домени використовуються для верифікації таких атрибутів: Адреса SMTP "MAIL FROM" "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:" поле заголовка електронного листа

Захист від фішингу в Gmail

Увімкнути захист від фішинг-атак для Gmail
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Під час повідомлення про елементи
• **Пропустити**: нічого не робити, надіслати електронні листи зі шкідливими вкладеннями одержувачу.
• **Перемістити в спам** – відправити лист у папку "Спам".
• **Перемістити в кошик** – відправити лист у папку "Кошик".
• **Видалити повідомлення**: електронний лист видалено
• **Відправити повідомлення в карантин**: оригінальний електронний лист видалятиметься, а його копія поміщатиметься в карантин. Якщо ви вирішите розблокувати електронний лист із карантину, він надсилатиметься отримувачу як вкладення в новому електронному листі.
Додавати до теми тег
Якщо цей параметр увімкнено, можна змінювати шаблони, додані в тему інфікованих повідомлень.
Текст тега, який потрібно додавати до теми
Можна додати налаштовувану позначку в теми інфікованих повідомлень.
Сповіщати власника поштової скриньки
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Параметри захисту для OneDrive

У цьому розділі надано інформацію про зміну параметрів "OneDrive – Загальні налаштування" або "OneDrive – захист від шкідливого програмного забезпечення".

OneDrive – Загальні налаштування

ESET LiveGrid®Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Дізнайтеся більше про ці програми в глосарії.
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Політикою зберігання для очищення результатів сканування задано термін три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

OneDrive – Захист від шкідливого програмного забезпечення

OneDrive – Захист від шкідливого програмного забезпечення
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, залишити файл у OneDrive.
• **Перемістити в кошик**: файл переміщається в кошик.
• **Замінити**: вміст вихідного файлу замінюється визначеним нижче текстом (у вікні "Текст, яким потрібно замінювати файл").
• **Помістити на карантин** – вихідний файл переміщується в кошик, а його копія відправляється в карантин. Коли файл розблоковується, раніше видалений файл залишається в кошику, а нова копія передається в оригінальну папку OneDrive.
Текст, яким потрібно замінювати файл
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Сповіщати власника
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Параметри захисту для Google Диск

У цьому розділі надано інформацію про зміну параметрів "Загальні налаштування Google Диск" або "Захист від шкідливого програмного забезпечення на Google Диск".

Загальні налаштування Google Диск

ESET LiveGrid®Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Дізнайтеся більше про ці програми в глосарії.
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Політикою зберігання для очищення результатів сканування задано термін три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

Захист від шкідливого програмного забезпечення на Google Диск

Захист від шкідливого програмного забезпечення на Google Диск
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити** – нічого не робити, залишити файл у Google Drive
• **Перемістити в кошик**: файл переміщається в кошик.
• **Замінити**: вміст вихідного файлу замінюється визначеним нижче текстом (у вікні "Текст, яким потрібно замінювати файл").
• **Помістити на карантин** – вихідний файл переміщується в кошик, а його копія відправляється в карантин.
• **Видалити**: вихідний файл безповоротно видаляється зі сховища Google Диск.
Текст, яким потрібно замінювати файл
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Сповіщати власника
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Параметри захисту для груп команди

У цьому розділі надано інформацію про зміну параметрів "Групи команди – Загальні налаштування" або "Групи команди – Захист від шкідливого програмного забезпечення".

Групи команди – Загальні налаштування

ESET LiveGrid®Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Дізнайтеся більше про ці типи програм у глосарії.
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Відповідно до політики зберігання результати сканування зі статусом "Очищено" зберігаються три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

Налаштування захисту від шкідливого програмного забезпечення для груп команди

Налаштування захисту від шкідливого програмного забезпечення для груп команди
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити**: жодна дія не виконується, файл залишатиметься незмінним.
• **Перемістити в кошик**: файл переміщається в кошик команд.
• **Замінити**: замінити вміст вихідного файлу визначеним нижче вікні (поле "Текст, яким потрібно замінювати файл").
• **Карантин**: вихідний файл переміщається в кошик команд і копіюється в карантин. Коли файл розблоковується, раніше видалений файл залишається в кошику, а нова копія передається в оригінальну папку.
Текст, яким потрібно замінювати файл
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Сповіщати власника
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Параметри захисту для сайтів SharePoint

У цьому розділі надано інформацію про зміну параметрів "Сайти Sharepoint – Загальні налаштування" або "Сайти Sharepoint – Захист від шкідливого програмного забезпечення".

Сайти SharePoint – Загальні налаштування

ESET LiveGrid® Відгук про
Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Дізнайтеся більше про ці типи програм у глосарії.
Реєструвати всі об'єкти
Якщо цей параметр вибрано, усі результати сканування (зокрема, безпечні об’єкти) будуть відображатися в розділі Журнали сканування. Відповідно до політики зберігання результати сканування зі статусом "Очищено" зберігаються три дні. Результати сканування, старіші за 3 дні, видалятимуться остаточно.

Налаштування захисту від шкідливого програмного забезпечення для сайтів SharePoint

Налаштування захисту від шкідливого програмного забезпечення для сайтів SharePoint
Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.
Звітність і захист на основі машинного навчання
Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для категорії Звітність.
Під час повідомлення про елементи
• **Пропустити**: жодна дія не виконується, файл залишатиметься незмінним.
• **Перемістити в кошик**: файл переміщається в кошик SharePoint.
• **Замінити**: замінити вміст вихідного файлу визначеним нижче вікні (поле "Текст, яким потрібно замінювати файл").
• **Карантин**: вихідний файл переміщається в кошик SharePoint і копіюється в карантин. Коли файл розблоковується, раніше видалений файл залишається в кошику, а нова копія передається в оригінальну папку.
Текст, яким потрібно замінювати файл
Заміняє вкладення текстовим файлом, що містить докладні відомості про виконану дію.
Сповіщати власника
Якщо цей параметр увімкнуто, користувач отримуватиме електронні листи зі сповіщеннями про виявлені об’єкти.
Сповіщати адміністратора
Укажіть адресу електронної пошти (щоб додати декілька адрес, утримуйте клавішу ENTER), на яку будуть надходити електронні листи зі сповіщеннями про виявлені об’єкти.

Параметри захисту для ESET LiveGuard Advanced

Щоб скористатися функцією ESET LiveGuard Advanced, налаштуйте політику, яка активує аналіз ESET LiveGuard Advanced. Користувачі або групи, яким призначено цю політику, матимуть додатковий захист. Файли, надіслані в ESET LiveGuard Advanced для аналізу, відображаються на вкладці Надіслані файли. Це стосується підозрілих зразків, які ще не були відомі. Відомі шкідливі файли (на основі хешу) не надсилаються в ESET LiveGuard Advanced для аналізу.

Результати аналізу ESET LiveGuard Advanced відображатимуться в розділі Журнали сканування (для Exchange Online, OneDrive, груп команди або сайтів SharePoint) із поміткою "Шкідливе програмне забезпечення" .

ESET LiveGuard Advanced

Якщо цей параметр увімкнено, ця функція буде активною, і ви зможете налаштувати додаткові параметри.

ESET LiveGuard Advanced автоматично ввімкне зворотний зв’язок ESET LiveGrid®. Дані надсилатимуться в ESET Research Lab для подальшого аналізу. Докладніше про ESET LiveGrid® див. в глосарії .

Граничне значення оцінки виявлення

Об’єкти, оцінка яких дорівнює вказаному значенню або перевищує його, вважатимуться загрозами.

Автоматичне надсилання підозрілих зразків (розкривне меню)

Цей параметр пов’язаний із ESET LiveGrid®. Для нього можна вибрати такі варіанти: "Усі", "Усі за винятком документів", "Немає".

Автоматичне надсилання підозрілих зразків (повзунки)

Виберіть типи файлів, які надсилатимуться в ESET LiveGuard Advanced у разі, якщо вони містять підозрілий код, схожий на загрози, або мають незвичні характеристики чи поведінку.

- **Виконувані файли** — .exe, .dll, .sys
- **Архіви** — .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Сценарії** — .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Інше** — .jar, .reg, .msi, .swf, .lnk

Видаляти підозрілі зразки із серверів ESET

Виберіть, коли видаляти зразки, надіслані для аналізу. Для видалення зразків із хмари ESET LiveGuard Advanced можна вибрати один із таких параметрів: "Ніколи", "Після 30 днів", "Відразу після аналізу".

Документи

За допомогою повзунка виберіть типи документів, які дозволено надсилати в ESET LiveGuard Advanced для аналізу: документи Microsoft Office, PDF або інших типів.

Видалити документи із серверів ESET

Для видалення зразків документів певного формату з хмари ESET LiveGuard Advanced можна вибрати один із таких параметрів: "Ніколи", "Після 30 днів", "Відразу після аналізу".

Звітність і 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 обробнику виявлення для підвищення рівня захисту, що покращує виявлення. Дізнайтеся більше про цей тип захисту в глосарії. Можна налаштувати рівні звітності для таких категорій:

Шкідливе програмне забезпечення

Комп’ютерний вірус — це певний шкідливий код, який додається на початок або кінець коду наявних файлів на комп’ютері. Проте термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення". 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 є 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.
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.

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.

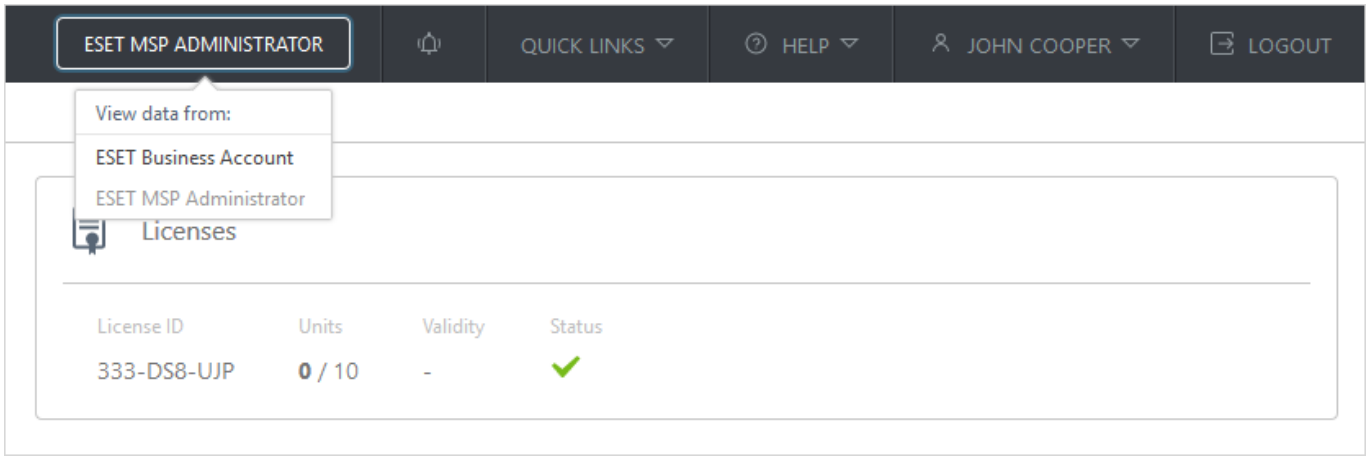
Система звітності не виконує жодних дій з об’єктами. Вона лише передає інформацію на відповідний рівень захисту, а рівень захисту передбачає застосування певної дії.

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.

Керування ліцензією

У головному вікні відображаються зведені дані про ті ліцензії, які витягнуто з ESET Business Account або ESET MSP Administrator. Тут відображаються всі пули ліцензій, сайти або компанії, доступні на порталі ESET Business Account або ESET MSP Administrator. Керування ліцензією дозволяє вмикати або вимикати захист для користувачів.

Якщо в ESET MSP Administrator та ESET Business Account зареєстровано одну адресу електронної пошти (єдиний вхід), можна переключатися між поданнями ESET Business Account та ESET MSP Administrator (обліковий запис гібридного ліцензування).



Ліцензія ESET Cloud Office Security дає змогу використовувати функцію ESET LiveGuard Advanced без додаткової плати. Поруч з ідентифікатором ліцензії відображатиметься позначка ELG.

Керування ліцензією в ESET Business Account

Відображає інформацію про ліцензію та її використання (ім'я пулу ліцензій, ідентифікатор ліцензії, робочі одиниці, термін дії й стан). Ліцензії й пули ліцензій завантажуються з ESET Business Account. Пули ліцензій доступні, тільки якщо у вас є наявні місця в ESET Business Account (місця стануть в пригоді для класифікації за категоріями). Один підрозділ — захист ESET Cloud Office Security для одного користувача Exchange Online і OneDrive.

> Кожен захищений користувач використовує одну робочу одиницю з ліцензії. Це не залежить від того, які служби Microsoft 365 використовуються. Користувач з Exchange Online і (або) OneDrive завжди використовує одну робочу одиницю з ліцензії. Робоча одиниця ліцензії не використовується групами команд або сайтами SharePoint.

Усі нові користувачі з'являтимуться в розділі Користувачі зі статусом Незахищені. Якщо використовується автоматичний захист за клієнтом або групою, для нових користувачів захист умикатиметься автоматично, і вони матимуть статус Захищені.
Для захисту користувачів ви маєте два варіанти:

• **Автоматичний захист за клієнтом або за групою (рекомендується)**: для кожного нового доданого користувача, що входить у групу Azure AD або належить до клієнта, доступ умикається автоматично. Якщо використовується цей метод, потреби в обслуговуванні немає. Більш докладну інформацію див. в примітці нижче.

• **Захист окремих користувачів**: потребує дій із керування; ви маєте вручну вмикати захист для кожного нового користувача.

Захист користувачів (без пулу ліцензій)

1. Клацніть **Захистити**.
2. Виберіть клієнта або групу для автоматичного захисту користувача й клацніть **Захистити**. Щоб захистити окремих користувачів, виберіть користувачів, для яких потрібно ввімкнути захист, і клацніть **Захистити**. Користувачі будуть захищені з використанням політики за замовчуванням.
3. За потреби вкажіть налаштовувану політику для користувачів у розділі Політики.

Захист користувачів (із використанням пулу ліцензій)

1. Виберіть пул ліцензій, поруч із ним клацніть піктограму з трьома крапками й виберіть **Показати подробиці**.
2. Клацніть **Захистити**.
3. Виберіть клієнта або групу для автоматичного захисту користувача й клацніть **Захистити**. Щоб захистити окремих користувачів, виберіть користувачів, для яких потрібно ввімкнути захист, і клацніть **Захистити**. Користувачі будуть захищені з використанням політики за замовчуванням.
4. За потреби вкажіть налаштовувану політику для користувачів у розділі Політики.

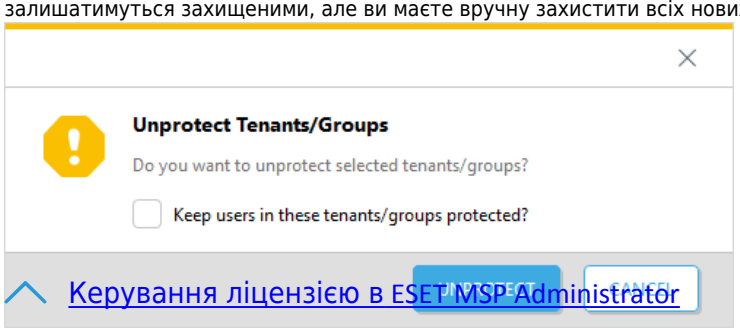
> Переконайтеся, що у вашій ліцензії достатньо робочих одиниць, особливо з увімкненим автоматичним захистом, коли кількість користувачів зростає. Після використання всіх робочих одиниць із ліцензії жоден користувач, який вступатиме в клієнт або групу, не буде захищений. Захист наявних користувачів залишиться незмінним.
> Якщо вам тимчасово не вистачає робочих одиниць у ліцензії та потрібно захистити певних користувачів, використовуйте незахищені групи (не використовуйте автоматичний захист) і ввімкніть захист для користувачів уручну. Після поповнення пулу ліцензії додатковими робочими одиницями можна повернутися до автоматичного захисту, щоб полегшити керування.

Перемістити

Щоб перемістити користувачів між пулами ліцензій і виконати більш складні операції з ліцензіями, клацніть ESET Business Account .

Зняти захист

1. Виберіть окремих користувачів, клієнт або групу й клацніть **Вимкнути захист**.
2. Якщо ви вимикаєте автоматичний захист для клієнта або групи, з'явиться запит **Залишити користувачів із цих клієнтів/груп під захистом?**. Якщо ви не будете використовувати цей параметр, користувачі втратять захист. Якщо встановити цей прапорець, автоматичний захист клієнта або групи буде деактивований і змінений на захист окремих користувачів. Користувачі залишатимуться захищеними, але ви маєте вручну захистити всіх нових доданих користувачів.



Керування ліцензією в ESET MSP Administrator

Відображає інформацію про ліцензію та її використання (компанія клієнта, ідентифікатор ліцензії, робочі одиниці й стан).

> Кожен захищений користувач використовує одну робочу одиницю з ліцензії. Це не залежить від того, які служби Microsoft 365 використовуються. Користувач з Exchange Online і (або) OneDrive завжди використовує одну робочу одиницю з ліцензії.
> Робоча одиниця ліцензії не використовується групами команд або сайтами SharePoint.

Усі нові користувачі з'являтимуться в розділі Користувачі зі статусом **Незахищені**. Якщо використовується автоматичний захист за клієнтом або групою, для нових користувачів захист умикатиметься автоматично, і вони матимуть статус **Захищені**.
Для захисту користувачів ви маєте два варіанти:
• **Автоматичний захист за клієнтом або за групою (рекомендується)**: для кожного нового доданого користувача, що входить у групу Azure AD або належить до клієнта, доступ умикається автоматично. Якщо використовується цей метод, потреби в обслуговуванні немає. Більш докладну інформацію див. в примітці нижче.
• **Захист окремих користувачів**: потребує дій із керування; вам потрібно буде вручну вмикати захист для кожного нового користувача.

Захистити користувачів

1. Клацніть **Захистити**.
2. Виберіть клієнта або групу для автоматичного захисту користувача й клацніть **Захистити**. Щоб захистити окремих користувачів, виберіть користувачів, для яких потрібно ввімкнути захист, і клацніть **Захистити**. Користувачі будуть захищені з використанням політики за замовчуванням.
3. За потреби вкажіть налаштовувану політику для користувачів у розділі Політики.

> Переконайтеся, що у вашій ліцензії достатньо робочих одиниць, особливо з увімкненим автоматичним захистом, коли кількість користувачів зростає. Після використання всіх робочих одиниць із ліцензії жоден користувач, який вступатиме в клієнт або групу, не буде захищений. Захист наявних користувачів залишиться незмінним.
> Якщо вам тимчасово не вистачає робочих одиниць у ліцензії та потрібно захистити певних користувачів, використовуйте незахищені групи (не використовуйте автоматичний захист) і ввімкніть захист для користувачів уручну. Після поповнення пулу ліцензії додатковими робочими одиницями можна повернутися до автоматичного захисту, щоб полегшити керування.

Зняти захист

1. Виберіть окремих користувачів, клієнт або групу й клацніть **Вимкнути захист**.
2. Якщо ви вимикаєте автоматичний захист для клієнта або групи, з'явиться запит **Залишити користувачів із цих клієнтів/груп під захистом?**. Якщо ви не будете використовувати цей параметр, користувачі втратять захист. Якщо встановити цей прапорець, автоматичний захист клієнта або групи буде деактивований і змінений на захист окремих користувачів. Користувачі залишатимуться захищеними, але ви маєте вручну захистити всіх нових доданих користувачів.

Доступ користувача ESET Cloud Office Security до певної компанії

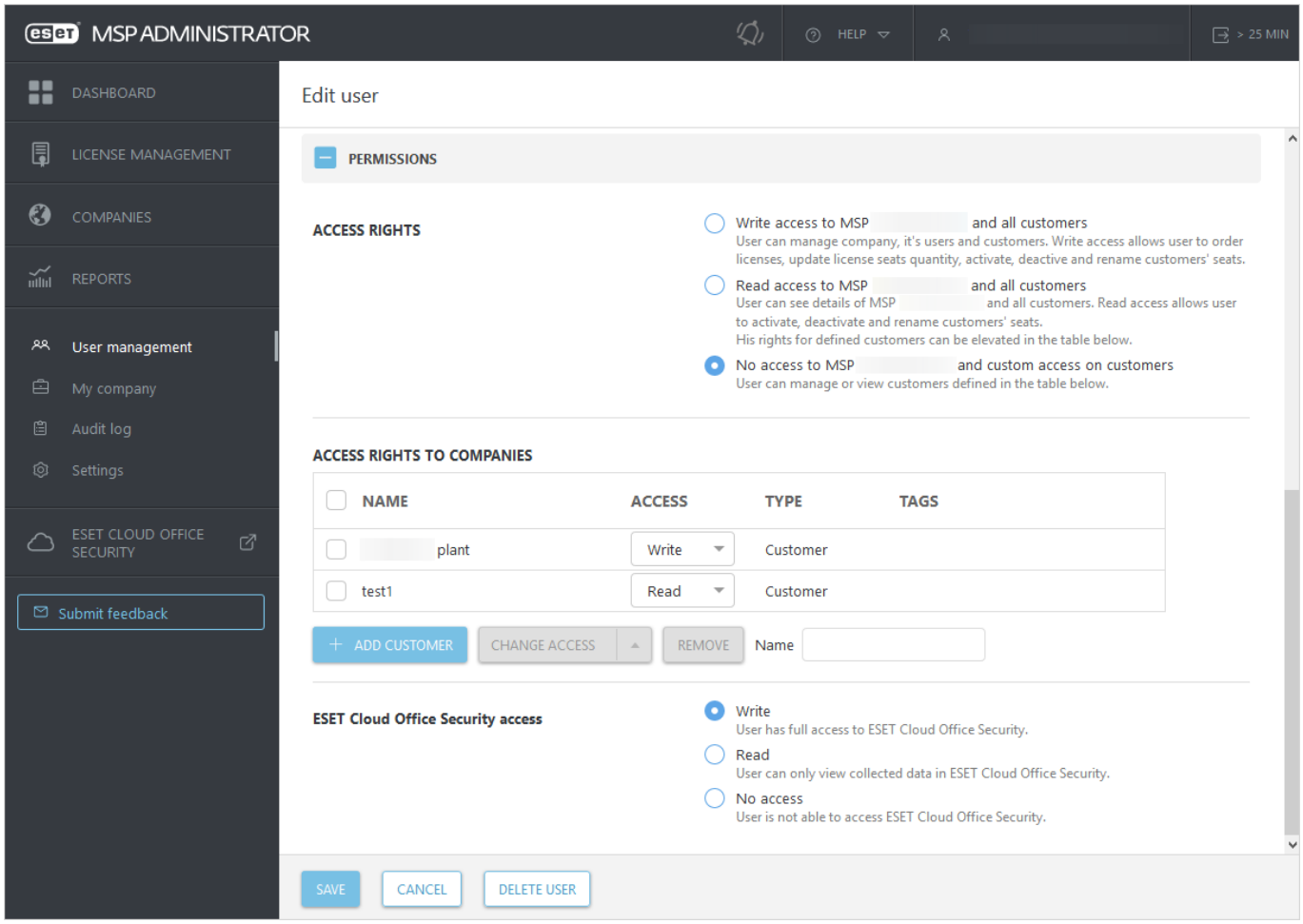
У середовищі з кількома клієнтами можна надати користувачу доступ до ESET Cloud Office Security, завдяки чому той зможе переглядати лише певні компанії (з правами на читання або запис). Зазвичай цим користуються постачальники керованих послуг.

Налаштуйте права доступу користувача в ESET MSP Administrator. Для цього призначте для нього компанію, яка має права **Запис** і доступ **Запис** для ESET Cloud Office Security:

1. Увійдіть ESET MSP Administrator від імені адміністратора.

2. Змініть користувача та налаштуйте параметр **Права доступу для компаній** у розділі «Дозволи» й виберіть доступ до **Запису**. Користувач може переглядати лише призначені до його пулу ліцензій компанії.

3. Надайте доступ до **Запису** в ESET Cloud Office Security, щоб користувач міг захистити компанію, додавши клієнта. Користувач із правом на читання не може додавати й видаляти клієнтів.



Лише один тип доступу до ESET Cloud Office Security можна встановити як глобальний параметр, який застосовується до всіх компаній (якщо користувачу призначено кілька компаній).

Журнал аудиту

Відстежує зміни в конфігурації або захисті ESET Cloud Office Security. Записи журналу аудиту засвідчують виконані дії і показують послідовність їхнього виконання. У журналах аудиту зберігається інформація про певну операцію або подію. Журнали аудиту створюються щоразу, коли створюється або змінюється об'єкт ESET Cloud Office Security (пул ліцензій, користувач, політика, звіт, елемент карантину, наприклад вкладення).

Якщо клацнути піктограму шестерні у верхньому правому куті, щоб скористатися можливістю **Експортувати в CSV** в контекстному меню, можна експортувати сітку таблиці у формат *CSV* та використовувати її в інших програмах для роботи зі списками.

Клацніть піктограму , щоб відкрити бічну панель зі зведеними даними про певний запис

журналу аудиту. Щоб отримати більш докладну інформацію, клацніть піктограму й виберіть **Показати подробиці**.

Плитка	Відомості
Основна інформація	Показує загальні дані журналу аудиту ("Відбулося", "Дія", "Критичність", "Результат", "Розділ").
Користувач	Інформація про користувача, який виконав дію або вніс зміну, зокрема його адреса електронної пошти й IP-адреса.
Зміни	Докладні відомості про внесені зміни.
Старі параметри	Показує параметри політики, які використовувалися раніше.
Нові параметри	Показує поточні параметри політики.
Об'єкти	Містить список об’єктів, на які вплинула внесена зміна або виконана дія (користувачі, політики, вкладення тощо).

Користувачів можна фільтрувати за кількома критеріями. Клацніть **Додати фільтр** і виберіть тип фільтра в розкривному меню або введіть рядок (повторіть цю дію, якщо застосовуєте декілька критеріїв):

Додати фільтр	Використання
Дія	Виберіть одну з доступних дій.
Об’єкт	Уведіть дійсне ім’я об’єкта.
Статус	Виберіть один із варіантів нижче. Виконано, не виконано, запущено або частково виконано
Користувач	Уведіть користувача, який уніс зміни.
Критичність	Виберіть рівень критичності: Низька, середня або висока
Початок періоду події / Закінчення періоду події	Фільтрація за часом виникнення. Скористайтеся параметром "Початок періоду події" і виберіть дату, щоб показати записи, створені після неї. Скористайтеся параметром "Закінчення періоду події", щоб показати записи, створені до вибраної дати. Щоб задати проміжок часу, скористайтеся обома параметрами.
Ініційовано системою	Фільтрує записи, створені системою.

Надіслати відгук

Щоб надіслати відгук, на консолі ESET Cloud Office Security відкрийте панель інструментів у верхньому правому куті, наведіть вказівник миші на розділ **Довідка** й клацніть **Надіслати відгук**, виберіть **Поділіться з нами своєю думкою** (щоб повідомити про свої міркування або досвід роботи з програмою) або **Повідомити проблему або помилку**.

Технічна підтримка

За наведеними нижче посиланнями міститься технічна інформація, що допоможе вирішити проблеми, які можуть виникнути.

Шукати в базі знань ESET

База знань ESET містить відповіді на найпоширеніші запитання й рекомендовані вирішення різних проблем. Технічні спеціалісти ESET регулярно оновлюють базу знань, завдяки чому вона є

найпотужнішим інструментом для вирішення різних проблем.

Перегляньте форум із безпеки ESET

Форум підтримки: форум ESET надає користувачам ESET простий спосіб отримати допомогу й допомогти іншим. Ви можете опублікувати повідомлення про будь-які проблеми або поставити запитання, пов’язані з продуктами ESET.

Зверніться до служби технічної підтримки

Форма технічної підтримки ESET: заповніть форму, щоб надати докладні відомості (зокрема, опис проблеми).

Зверніться за допомогою до місцевого партнера ESET

Зверніться до місцевої служби підтримки ESET: контактна інформацію служби підтримки ESET у вашому регіоні міститься в електронному листі з відомостями про ліцензію ESET.

Надіслати відгук

Надіслати відгук: поділіться з нами своєю думкою (щоб повідомити про свої міркування або досвід роботи з програмою) або повідомте про проблему або помилку.

Запропонувати вдосконалення онлайн-довідки

Щоб опублікувати оцінку й надіслати відгук на певну тему в онлайн-довідці, клацніть посилання **Ця інформація корисна?** під сторінкою довідки. Повідомте нам, чи допоміг вміст або яким чином, на вашу думку, технічний письменник може його покращити.

Доступність служби

На порталі стану ESET відображається поточний стан хмарних служб ESET, заплановані перерви в роботі й минулі інциденти. Якщо у вас виникла проблема з підтримуваною службою ESET, але вона не відображається на порталі стану, зверніться в службу технічної підтримки ESET.

Моніторингові групи перевіряють потенційні проблеми всередині компанії. Підтверджені інциденти публікуються й оновлюються вручну для підтримки достовірності та точності. Тому вони з’являтимуться на порталі стану з невеликою затримкою. Ми можемо не публікувати короткі інциденти, якщо їх було вирішено до підтвердження вручну.

Security for ESET Cloud Office Security

Вступ

Мета цього документа — узагальнити методи захисту й елементи керування безпекою, які застосовуються в програмі ESET Cloud Office Security. Методи захисту й елементи керування призначені для захисту конфіденційності, цілісності й доступності інформації клієнта. Зауважте, що методи захисту та елементи керування можуть змінюватися.

Область

У цьому документі узагальнено методи захисту й елементи керування безпекою для інфраструктури ESET Cloud Office Security, ESET Business Account (далі "EBA"), ESET Data Framework, ESET LiveGrid, модулів "Оновлення", "Антиспам", а також для інфраструктури, організації, персоналу й операційних процесів ESET Dynamic Threat Defense. Методи захисту й елементи керування безпекою:

1. Політики інформаційної безпеки
2. Організація інформаційної безпеки
3. Безпека, пов’язана з роботою персоналу
4. Керування ресурсами
5. Керування доступом
6. Криптографія
7. Фізична безпека й безпека середовища
8. Безпека операцій
9. Безпека обміну даними
10. Придбання, розробка й обслуговування системи
11. Відносини з постачальниками
12. Керування інцидентами, які стосуються інформаційної безпеки
13. Аспекти інформаційної безпеки керування безперервністю бізнесу
14. Відповідність нормативним вимогам

Концепція безпеки

Компанія ESET s.r.o. має сертифікат ISO 27001:2013 та інтегровану систему керування, яка розповсюджується на ESET Cloud Office Security, EBA та інші служби.

Тому в концепції інформаційної безпеки використовується інфраструктура ISO 27001, яка дає змогу впровадити багатошарову стратегію захисту для засобів безпеки на рівні мережі, операційних систем, баз даних, програм, персоналу та операційних процесів. Застосовувані методи захисту й елементи керування безпекою призначені для доповнення один одного й дублювання певних функцій.

Методи захисту й елементи керування безпекою

1. Політики інформаційної безпеки

ESET використовує політики інформаційної безпеки для забезпечення відповідності всім аспектам стандарту ISO 27001, зокрема в питаннях управління безпекою інформації, а також контролю за безпекою й практиками. Політики переглядаються щорічно та оновлюються після суттєвих змін, що гарантує їхню актуальність.

ESET щорічно переглядає цю політику й внутрішні процедури перевірки безпеки, щоб забезпечити їхню узгодженість із цією політикою. Недотримання політик щодо інформаційної безпеки призводить до дисциплінарних стягнень для співробітників ESET або до передбачених контрактом штрафів аж до розірвання контракту для постачальників.

2. Організація інформаційної безпеки

Організацією інформаційної безпеки для ESET Cloud Office Security займаються кілька груп і осіб із відділів інформаційної безпеки та IT, зокрема:

- Керівництво ESET
- Команди внутрішньої безпеки ESET
- IT-команди, які працюють із бізнес-програмами
- Інші команди підтримки

Обов'язки щодо безпеки інформації розподіляються відповідно до чинних політик інформаційної безпеки. Внутрішні процеси визначаються та оцінюються на наявність будь-якого ризику несанкціонованої чи ненавмисної модифікації або неналежного використання ресурсів ESET. Для тих операцій внутрішніх процесів, які пов'язані з ризиком або конфіденційними даними, діє принцип розподілення обов'язків. Це дає змогу знизити ризик.

Юридична команда ESET несе відповідальність за контакти з органами державної влади, зокрема словацькими регуляторами в галузі кібербезпеки й захисту персональних даних. Команди внутрішньої безпеки ESET несе відповідальність за контакти з групами певних інтересів, зокрема ISACA. Команда дослідницької лабораторії ESET відповідає за обмін даними з іншими компаніями з безпеки й спільнотою кібербезпеки.

Для керування проектами враховуються складові інформаційної безпеки з використанням структури керування проектами (від початку до завершення).

На віддалену роботу розповсюджується політика, реалізована на мобільних пристроях, зокрема використання надійного криптографічного захисту даних на мобільних пристроях під час роботи в недовірених мережах. Елементи керування безпекою на мобільних пристроях працюють незалежно від внутрішніх мереж ESET і внутрішніх систем.

3. Безпека, пов'язана з роботою персоналу

ESET використовує стандартні практики щодо персоналу, зокрема політики, призначені для забезпечення інформаційної безпеки. Ці методи розповсюджуються на весь термін роботи працівника, і вони застосовуються до всіх груп, які мають доступ до середовища ESET Cloud Office Security.

4. Керування ресурсами

Інфраструктура ESET Cloud Office Security входить до складу наявних ресурсів ESET із чітко визначеним правами власності й правилами, які застосовуються відповідно до типу й рівня конфіденційності ресурсу. У ESET є визначена внутрішня схема класифікації. Усі дані й конфігурації ESET Cloud Office Security класифікуються як конфіденційні.

5. Керування доступом

Політика ESET щодо керування доступом регламентує кожну спробу доступу в ESET Cloud Office Security. Керування доступом можна задати на рівні інфраструктури, мережевих служб, операційної системи, бази даних і програми. Керування повним доступом користувача на рівні програми є автономним. Керування єдиним входом ESET Cloud Office Security і ESET Business Account здійснюється централізованим постачальником ідентифікаційних даних, який гарантує, що користувач має доступ тільки до авторизованого клієнта. Для впровадження керування

доступом на основі ролей для клієнта в програмі використовуються стандартні дозволи ESET Cloud Office Security.

Доступ до серверів ESET відкрито виключно для вповноважених користувачів і користувачів із певними ролями. Для керування доступом працівників ESET до інфраструктури й мереж ESET Cloud Office Security використовуються стандартні процеси ESET щодо реєстрації (скасування реєстрації), підготовки (відкату підготовки), керування привілеями й огляду прав доступу користувача.

Доступ до всіх даних ESET Cloud Office Security захищено з використанням надійної автентифікації.

6. Криптографія

Дані ESET Cloud Office Security (постійні й транзитні) захищено шифруванням із використанням надійної криптографії. Сертифікати для загальнодоступних служб зазвичай випускаються довіреним центром сертифікації. Для керування ключами в інфраструктурі ESET Cloud Office Security використовується внутрішня інфраструктура відкритих ключів ESET. Дані, які зберігаються в базі даних, захищені ключами шифрування, згенерованими у хмарі. Усі резервні дані захищені керованими ключами ESET.

7. Фізична безпека й безпека середовища

ESET Cloud Office Security і ESET Business Account працюють на основі хмари. Щоб забезпечити належний рівень фізичної безпеки й безпеки інфраструктури, ми використовуємо Microsoft Azure. Microsoft Azure використовує сертифіковані центри обробки даних із надійним захистом. Фізичне розташування центру обробки даних залежить від регіону, який вибирає клієнт.

8. Безпека операцій

Служба ESET Cloud Office Security працює з використанням автоматичних засобів на основі чітко визначених операційних процедур і шаблонів конфігурації. Перед робочим розгортанням усі зміни, зокрема зміни конфігурації та розгортання нових пакетів, затверджуються й тестуються в спеціально виділеному тестовому середовищі. Середовища розгортання, тестові й робочі середовища відокремлені одне від одного. Дані ESET Cloud Office Security розташовані тільки в робочому середовищі.

Нагляд за середовищем ESET Cloud Office Security здійснюється в режимі операційного моніторингу. Це дає змогу швидко виявляти проблеми й надавати достатні ресурси всім службам на рівні мережі й рівні хостів.

Усі дані конфігурації зберігаються в наших репозиторіях, для яких регулярно створюються резервні копії. Це дає змогу автоматично відновлювати конфігурацію середовища. Резервні копії даних ESET Cloud Office Security зберігаються як на майданчику, так і поза ним.

Резервні копії шифруються й регулярно перевіряються на можливість використання для відновлення (один з етапів тестування безперервності бізнесу).

Аудит систем проводиться відповідно до внутрішніх стандартів і вказівок. Постійно збираються журнали й події інфраструктури, операційної системи, бази даних, серверів програм і елементів керування безпекою. Після збору журнали обробляються IT-фахівцями й внутрішніми командами безпеки для виявлення нетипових операцій та аномалій безпеки, а також інцидентів інформаційної безпеки.

Для усунення вразливостей в інфраструктурі ESET, зокрема в ESET Cloud Office Security та інших продуктах, ESET дотримується загального процесу роботи з технічними вразливостями. Складовими цього процесу є проактивне сканування на наявність уразливостей, а також тестування інфраструктури, продуктів і програм на стійкість до проникнення.

ESET впроваджує внутрішні керівні принципи щодо безпеки внутрішньої інфраструктури, мереж, операційних систем, баз даних, серверів програм і програм. Ці рекомендації перевіряються через моніторинг дотримання технічних вимог і нашу внутрішню програму аудиту безпеки.

9. Безпека обміну даними

Середовище ESET Cloud Office Security сегментоване за власною схемою сегментації хмари. Мережевий доступ надається тільки для необхідних служб серед сегментів мережі. Доступність мережевих служб реалізована за допомогою власних елементів керування хмари (зони доступності, балансування навантаження й надлишковість). Розгорнуто окремі компоненти балансування навантаження, які забезпечують певні кінцеві точки для маршрутизації екземплярів ESET Cloud Office Security з авторизацію трафіку й балансуванням навантаження. Мережевий трафік постійно відстежується на наявність нетипових операцій та аномалій безпеки. Потенційні атаки можуть нейтралізуватися з використанням власних елементів керування хмарою або розгорнутих рішень для захисту. Усі мережеві з'єднання зашифровано за допомогою загальнодоступних технологій, зокрема IPsec і TLS.

10. Придбання, розробка й обслуговування системи

Розробка систем ESET Cloud Office Security виконується відповідно до політики безпечної розробки програмного забезпечення ESET. Команди внутрішньої безпеки беруть участь у проекті розробки ESET Cloud Office Security з його початкового етапу й відстежують усі операції з розробки й обслуговування. Внутрішня команда з безпеки визначає й перевіряє виконання вимог щодо безпеки на різних етапах розробки програмного забезпечення. Безпека всіх служб, зокрема й розроблених нових, постійно перевіряється після випуску.

11. Відносини з постачальниками

Відповідні відносини з постачальниками регламентуються відповідно до дійсних керівних принципів ESET, які чинні для керування всіма відносинами і розповсюджуються на всі договірні вимоги з точки зору безпеки інформації та конфіденційності. Якість і безпека послуг, що надаються критично важливим постачальником послуг, регулярно оцінюються.

12. Керування інформаційною безпекою

Керування інцидентами, які стосуються інформаційної безпеки, в ESET Cloud Office Security виконується так само, як і в інших інфраструктурах ESET, на основі визначених процедур реагування на інциденти. Ролі реагування на інциденти визначаються й виділяються для кількох команд (IT, безпека, юридичний відділ, відділ кадрів, PR і керівництво). Команда реагування на інцидент формується на основі класифікації інциденту спеціалістами внутрішньої команди безпеки. Ця команда в подальшому координує інші команди, які займатимуться цим інцидентом. Команда внутрішньої безпеки також відповідає за збір доказів і робить висновки. Дані про всі інциденти й застосовані заходи надсилаються всім сторонам, які мають до цього відношення. Юридична команда ESET несе відповідальність за повідомлення про інциденти в регуляторні органи (за потреби) відповідно до вимог документів General Data Protection Regulation (GDPR) і Cybersecurity Act transposing Network and Information Security Directive (NIS).

13. Аспекти інформаційної безпеки керування безперервністю бізнесу

Безперервність роботи служби ESET Cloud Office Security передбачено в надійній архітектурі, яка використовується для забезпечення максимальної доступності служб. Повне відновлення з даних резервної копії поза майданчиком і даних конфігурації можливе в разі непереборного збою всіх вузлів надлишковості для компонентів ESET Cloud Office Security або служби ESET Cloud Office Security. Процес відновлення перевіряється регулярно.

14. Відповідність нормативним вимогам

Відповідність нормативним вимогам і умовам угоди ESET Cloud Office Security регулярно оцінюється та перевіряється, як й інші елементи інфраструктури й процеси ESET. ESET уживає необхідних кроків для їх дотримання на постійній основі. Компанію ESET зареєстровано як постачальник цифрових послуг для хмарних обчислень. Ця класифікація розповсюджується на кілька служб ESET, зокрема ESET Cloud Office Security. Зауважте, що дії ESET щодо забезпечення відповідності нормативним вимогам не обов’язково означають, що ці вимоги в повному обсязі виконуються клієнтами.

Умови використання

Набуває чинності 23 жовтня 2023 року | Переглянути попередню версію Умов використання | Порівняти зміни

Ця Угода ESET Cloud Office Security (далі "Умови") — окрема угода, яка укладається між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 85101 Bratislava, Slovak Republic, внесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532) (далі "ESET" або "Постачальник") і Вами, фізичною або юридичною особою (далі "Ви" або "Користувач"), яка використовує обліковий запис для адміністрування, ESET Cloud Office Security і веб-портал, що контролюється ESET (далі "Обліковий запис"), під час користування ESET Cloud Office Security. Якщо Ви користуєтеся цим Обліковим записом і ESET Cloud Office Security (сукупність яких далі вживається як "Продукт") від імені організації, то погоджуєтеся з цими умовами від її імені й підтверджуєте, що маєте всі повноваження на це. У такому випадку під "Користувачем" і "Вами" матиметься на увазі організація. Уважно ознайомтеся з цими Умовами, оскільки вони мають відношення до служб, які надаються ESET безпосередньо через цей Продукт або як супутні до нього. Спеціальні положення, що регулюють використання служб, на які не розповсюджуються ці Умови, окремо наводяться в інтерфейсі кожної служби, і Користувач має прийняти їх під час активації. Вкладені додатки доповнюють ці Умови.

Безпека і захист даних

Обліковий запис дає змогу користуватися продуктами й службами, що надаються компанією ESET. Для реєстрації й використання Облікового запису, а також для надання послуг через нього нам потрібні такі дані: повне ім’я користувача, назва компанії, країна, дійсна адреса електронної пошти, номер телефону, дані про ліцензію й статистична інформація. Ви погоджуєтесь, що дані будуть збиратися й передаватися на сервери Постачальника або його партнерів. Це необхідно виключно для забезпечення функціональних можливостей Програмного забезпечення й авторизації на його використання, а також захисту прав Постачальника. Після укладання угоди з цими Умовами Постачальник та (або) його місцеві партнери, що входять до його мережі збуту, отримують право на збір, обробку, передачу та зберігання Ваших основних ідентифікаційних даних, що необхідно для надання підтримки та

забезпечення виконання цих Умов. Ви маєте право використовувати Обліковий запис виключно з тією метою та в такий спосіб, які передбачені цими Умовами, умовами індивідуального обслуговування та документацією.

Відповідальність за безпеку Облікового запису та облікових даних для входу несе Користувач. Компанія ESET не несе жодної відповідальності за шкоду чи збитки, спричинені невиконанням цих зобов'язань. Користувач також несе відповідальність за будь-які дії з Обліковим записом ESET, санкціоновані чи ні. У разі виявлення несанкціонованого доступу до Облікового запису ESET негайно повідомте про це Постачальника.

З метою надання послуг адміністрування Облікового запису нам необхідно збирати дані, які відносяться до керованих пристроїв, а також інформацію адміністрування (далі "Дані"). Дані надаються Вами до ESET виключено з метою надання адміністративних послуг щодо Облікового запису. Дані оброблюються і зберігаються у відповідності до політик безпеки і практик ESET, а також у відповідності до положень Політики конфіденційності.

Докладні відомості про конфіденційність, захист персональних даних і ваші права як суб'єкта даних можна знайти в документі Політика конфіденційності.

Правила добросовісного використання

Ви зобов'язуєтеся дотримуватися всіх технічних обмежень, передбачених у документації. Ви погоджуєтеся використовувати Обліковий запис та його функції лише в такий спосіб, що не заважає доступу до них інших Користувачів. Постачальник зберігає за собою право обмежити перелік послуг, що надаються окремим Користувачам, з метою надання своїх послуг максимальній кількості Користувачів. Обмеження переліку доступних послуг також передбачає повну заборону використання будь-яких функцій Облікового запису та видалення відомостей та інформації.

Детально про технічні обмеження можна прочитати в розділі Обмеження.

Розташування

Постачальник може дозволити Вам вибрати одне з доступних розташувань для Облікового запису, включно з розташуванням, рекомендованим Постачальником. Ви визнаєте, що вибір розташування, відмінного від рекомендованого, може призвести до погіршення роботи. У залежності від вибраного місцезнаходження можуть діяти положення розділів "Data Protection Agreement (Угоди про захист даних)" (у додатку 2) або "Стандартні положення угоди" (у додатку 3) цієї Угоди. ESET залишає за собою право змінювати певне розташування в будь-який час без попереднього повідомлення з метою вдосконалення якості послуг, що надаються ESET відповідно до Вашого налаштованого розташування (наприклад, Європейський Союз).

Прорамне забезпечення

Компанія ESET або її постачальники володіють авторськими правами на все програмне забезпечення, яке є складовою продукту (далі "Програмне забезпечення"), чи можуть користуватися ними. Програмне забезпечення можна використовувати тільки в суворій відповідності до умов Ліцензійної угоди з кінцевим користувачем (додаток 1 до цієї Угоди). Інші відомості стосовно ліцензування, авторських прав, документації та товарних знаків див. у документі з юридичною інформацією.

Обмеження

Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Облікового запису. Використовуючи Обліковий запис забезпечення, Ви зобов’язуєтеся дотримуватися наведених нижче обмежень.

(a) Ви не маєте права використовувати, змінювати, перебудовувати або відтворювати Обліковий запис або передавати права на використання Облікового запису або його компонентів будь-яким способом, окрім чітко передбачених цими Умовами.

(b) Вам забороняється продавати, надавати в оренду, позичати Обліковий запис, передавати право на його користування чи використовувати його з комерційною метою.

(c) Ви не маєте права виконувати зворотне проектування, декомпілювати або дезасемблювати Обліковий запис чи застосувати будь-які інші засоби виявлення його вихідного коду, крім випадків, коли таке обмеження прямо заборонене законодавством.

(d) Ви погоджуєтеся використовувати Обліковий запис 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.

Застереження

ЯК КОРИСТУВАЧ ВИ ВИЗНАЄТЕ, ЩО ОБЛІКОВИЙ ЗАПИС ТА СЛУЖБИ НАДАЮТЬСЯ НА УМОВАХ "ЯК Є" БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОЗВОЛЕНО 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 ОБЛІКОВИЙ ЗАПИС АБО СЛУЖБИ НЕ ПОРУШУЮТЬ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЮТЬ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ОБЛІКОВИЙ ЗАПИС АБО СЛУЖБИ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ, АБО ЩО ВОНИ ПРАЦЮВАТИМУТЬ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ’ЯЗАНІ З ВИБОРОМ І ВИКОРИСТАННЯМ ОБЛІКОВОГО ЗАПИСУ ТА СЛУЖБ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ ТА ЗА ПОВ’ЯЗАНІ З ЙОГО ЗАСТОСУВАННЯМ НАСЛІДКИ.

Ці Умови не створюють жодних зобов’язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

Обмеження відповідальності

У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ПІДРЯДНИКИ 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, УТРАТУ 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 ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ОБЛІКОВОГО ЗАПИСУ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ПІДРЯДНИКАМ 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, ПІДРЯДНИКІВ АБО ДОЧІРНІХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ВІДПОВІДНУ СЛУЖБУ АБО ОБЛІКОВИЙ ЗАПИС.

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 цими Умовами, 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 цими Умовами, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії (законні акти, зазначені в пунктах i та ii вище, разом використовуються під назвою "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 пункту (a) розділу "Дотримання процедур із контролю за торгівлею" цих Умов.

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 цими Умовами 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.

Застосовний закон та основна мова

Ці Умови регулюються та тлумачаться 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. Якщо Ви є споживачем, що мешкає в ЄС, обов'язкові положення законодавства, що діють у вашій країні мешкання, надають вам додатковий захист.

Ви явно погоджуєтеся, що розгляд будь-яких позовів до Постачальника чи суперечок із ним або позовів чи суперечок, будь-яким чином пов’язаних із використанням програмного забезпечення, Облікового запису та Служб або таких, що базуються на цих Умовах або Спецальних умовах (за наявності), і прийняття відповідних рішень здійснюється окружним судом м. Братислава I (Словаччина), а також погоджуєтеся, що всі такі позови й суперечки підлягають юрисдикції вказаного суду. Якщо Ви є споживачем, що мешкає в ЄС, Ви також можете подати заяву щодо використання своїх прав споживача за місцем виключної юрисдикції або в країні ЄС, де Ви мешкаєте. Крім цього, ви також можете скористатися платформою для вирішення спорів в Інтернеті, доступною за адресою https://ec.europa.eu/consumers/odr/. Однак перш ніж офіційно подавати будь-які претензії, розгляньте можливість зв'язатися з нами.

У разі розбіжностей між англійською й перекладеною версією Угоди перевага надається документу англійською мовою, доступному тут.

Загальні положення

Компанія ESET залишає за собою право в будь-який час змінювати текст Умов і документації або будь-яких їхніх складових шляхом оновлення відповідних документів відповідно до змін, внесених до законодавства або правил функціонування Облікового запису. Ми сповістимо Вас про будь-яку зміну цих умов в Обліковому записі. Якщо Ви не згодні зі змінами, внесеними в Умови, Ви можете скасувати дію свого Облікового запису. Якщо Ви не видалите Обліковий запис після сповіщення про зміни, це означатиме, що Ви приймаєте всі доповнення й зміни цих Умов. Рекомендуємо регулярно відвідувати цю сторінку, щоб мати актуальну інформацію про будь-які зміни, які можуть вноситися до Умов використання Облікового запису.

Примітки

Усі зауваження слід надсилати за такою адресою: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Додаток 1

Ліцензійна угода з кінцевим користувачем

Додаток 2

Угода про обробку даних

Додаток 3

Стандартні положення угоди

Ліцензійна угода з кінцевим користувачем

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 УМОВАМИ ДОКУМЕНТА ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ.**

Ліцензійна угода з кінцевим користувачем

Ця ліцензійна угода з кінцевим користувачем (далі "Угода"), укладена між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic, унесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532) (далі "ESET" або "Постачальник") і Вами, фізичною або юридичною особою (далі "Ви" або "Користувач"), надає Вам право використовувати Програмне забезпечення, визначене в розділі 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. Якщо Ви не погоджуєтеся з будь-якими положеннями або умовами Угоди, 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 (далі "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 (далі «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 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.

в) **Business Edition.** Для використання 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.

ґ) **OEM-версія Програмного забезпечення.** Використання OEM-версії Програмного забезпечення має обмежуватися використанням на комп'ютері, з яким воно постачається. Його заборонено передавати для використання на іншому комп'ютері.

д) **ЛІЦЕНЗІЯ НЕ ДЛЯ ПРОДАЖУ 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.

е) **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 до компанії ESET або торгової точки, 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:

а) **Оновлення Програмного забезпечення.** Постачальник може час від часу випускати оновлення Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення 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.

б) Надсилання Постачальнику Інформації про загрози. Програмне забезпечення має функції, які збирають зразки вірусів та інших шкідливих комп'ютерних програм, а також підозрілих, проблемних, потенційно небажаних або небезпечних об'єктів: файлів, URL-адрес, IP-пакетів і Ethernet-фреймів (далі "Загроз"). Ці відомості (далі "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.

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. Ви погоджуєтесь отримувати повідомлення та сповіщення про продукт, зокрема маркетингову інформацію.

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.

а) Ви можете створити одну копію Програмного забезпечення на носії для постійного збереження даних за умови, що така архівна резервна копія не буде інсталюватися та використовуватися на будь-якому іншому комп'ютері. Створення будь-яких інших копій Програмного забезпечення вважається підставою для скасування цієї Угоди.

б) 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.

в) Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, передавати право на його користування чи використовувати його з комерційною метою.

г) 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.

ґ) 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.

д) 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.

е) 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 (а) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосовуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то 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. 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 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. 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 (далі "Закони експортного контролю").

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 (далі "Санкційні закони").

б) 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.

в) 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, Програмне забезпечення та Документацію слід надсилати на адресу: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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. У разі розбіжностей між англійською й перекладеною версією Угоди перевага надається документу англійською мовою. Внесення змін до положень цієї Угоди може виконуватися лише в письмовій формі. Засвідчення здійснюється підписом уповноваженого представника Постачальника чи особи, якій у прямій формі юридично надано право виконувати такі обов'язки.

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.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

Відповідно до вимог Регламенту ЄС 2016/679, затвердженого Європейським парламентом і Радою ЄС 27 квітня 2016 року, про захист фізичних осіб під час обробки персональних даних і про вільний обмін такими даними, який скасував дію Директиви 95/46/ЄС (далі — "GDPR"), Постачальник (далі — "Оператор") і Ви (далі сканувати — "Контролер") вступаєте в договірні відносини з метою визначити умови обробки персональних даних, спосіб їх захисту, а також

обумовити інші права й обов’язки обох сторін під час обробки персональних даних третіх сторін від імені Контролера під час виконання умов цієї Угоди, яка є основним договором.

1. **Обробка персональних даних.** До послуг, що надаються відповідно до цих Умов, входить обробка даних, які ідентифікують фізичну особу прямо чи опосередковано. Ці дані вказано в документі Політика конфіденційності (далі — "Персональні дані").

2. **Уповноваження.** Контролер уповноважує Оператора обробляти Персональні дані, зокрема згідно з такими інструкціями:

(i) "Мета обробки" — надання послуг відповідно до Умов цієї Угоди. Оператору дозволяється обробляти лише ті Персональні дані, які пов’язані з наданням послуг, запитаних Контролером, і лише від імені Контролера. На обробку всіх даних, які збираються в інших цілях, не розповсюджуються договірні відносини між Контролером і Оператором.

(ii) "Період обробки" — час між початком співпраці за цією Угодою та припиненням надання послуг;

(iii) Обсяг і категорії Персональних даних. Служби призначені лише для обробки загальних персональних даних. Однак Контролер несе повну відповідальність за визначення обсягу персональних даних.

(iv) "Суб’єкт даних" — фізична особа, яка є вповноваженим користувачем пристроїв Контролера;

(v) "Операції з обробки" — усі процеси, необхідні для обробки даних;

(vi) "Письмові вказівки" — інструкції в цій Угоді, Додатках, Політиці конфіденційності та документації з обслуговування. Контролер відповідає за правову допустимість обробки Персональних даних Оператором з огляду на відповідні норми законодавства про захист даних.

3. **Обов’язки Оператора**. Оператор зобов’язаний:

(i) Обробляти Персональні дані виключно на підставі задокументованих інструкцій і виключно в цілях, визначених в Умовах, Додатках до них, Політиці конфіденційності й документації з обслуговування.

(ii) Надати вказівки особам, уповноваженим обробляти Персональні дані (далі — "Уповноважені особи"), щодо їхніх прав і обов’язків відповідно до закону GDPR й відповідальності в разі його порушення, а також забезпечити, щоб Уповноважені особи взяли на себе зобов’язання зберігати конфіденційність і дотримуватися задокументованих інструкцій.

(iii) Вживати заходів, які описані в Умовах, Додатках до них, Політиці конфіденційності й документації з обслуговування.

(iv) Допомагати Контролеру надавати відповіді на запити від Суб’єктів даних щодо їхніх прав. Обробник не може виправляти, видаляти або обмежувати обробку Персональних даних без відповідних інструкцій від Контролера. Усі запити від Суб’єкта даних щодо Персональних даних, які обробляються від імені Контролера, мають негайно надсилатися Контролеру.

(v) Допомагати Контролеру повідомляти про порушення захисту Персональних даних наглядовим органам і Суб’єкту даних. Оператор повинен повідомити Контролера про будь-яке порушення, що стосується обробки або безпеки персональних даних, негайно після виявлення.

Оператор зобов'язаний належним чином сприяти дослідженню й усуненню такого порушення та вживати розумних заходів для обмеження подальших негативних наслідків.

(vi) На розсуд Контролера видаляти всі Персональні дані або повертати їх Контролеру після завершення періоду обробки. Контролер зобов'язується повідомити Оператора про своє рішення протягом десяти (10) днів після закінчення Періоду обробки. Це положення не впливає на право Оператора зберігати Персональні дані в необхідному обсязі для архівних цілей з міркувань суспільного інтересу, для наукових досліджень, з метою збору статистики або для подання, виконання й захисту позовних заяв.

(vii) Вести актуальний реєстр усіх категорій обробки, які він здійснював від імені Контролера,

(viii) Надавати всю необхідну інформацію, що засвідчує дотримання положень Умов, Додатків до них, Політики конфіденційності й документації з обслуговування, доступних для Контролера. Якщо Контролер проводитиме перевірку або аудит процесу обробки Персональних даних, Контролер зобов'язаний повідомити про це Оператора в письмовій формі принаймні за десять (30) днів до запланованої перевірки або аудиту.

4. **Залучення стороннього оператора.** Оператор має право залучати сторонніх операторів для певних процедур обробки, зокрема для надання хмарного сховища даних і хмарної інфраструктури з метою виконання положень цих Умов, Додатків до них, Політики конфіденційності й документації з обслуговування. Наразі Microsoft надає хмарне сховище даних і хмарну інфраструктуру в складі Azure Cloud Service. Але навіть у цьому разі Оператор лишається єдиною контактною особою та стороною, відповідальною за виконання вимог Угоди. Цим Оператор зобов'язується інформувати Контролера про нових або заміну старих операторів, щоб такі зміни можна було оскаржити.

5. **Територія, на якій здійснюється обробка.** Оператор докладатиме всіх зусиль, щоб обробка відбувалася в Європейській економічній зоні або країні, визначеній як безпечна за рішенням Європейської комісії, на підставі рішення Контролера. Стандартні договірні положення застосовуються в разі передачі й обробки даних за межами Європейської економічної зони або країни, визначеної як безпечна згідно з рішенням Європейської комісії за запитом Оператора.

6. **Безпека.** Оператор отримав сертифікат ISO 27001:2013 і використовує інфраструктуру ISO 27001, щоб упровадити багатошарову стратегію захисту для засобів безпеки на рівні мережі, операційних систем, баз даних, додатків, персоналу й операційних процесів. Відповідність нормативним вимогам і умовам Угоди регулярно оцінюється та перевіряється, як й інші елементи інфраструктури й операції Оператора. Оператор уживає необхідних кроків для їх дотримання на постійній основі. Оператор організував засоби безпеки даних за допомогою ISMS на основі ISO 27001. Документація з безпеки охоплює в основному політики щодо захисту інформації, фізичної безпеки та безпеки обладнання, запобігання порушенням, усунення витоків даних й порушень безпеки тощо.

7. **Технічні й організаційні заходи**. Оператор захищає Персональні дані від випадкового та незаконного пошкодження та знищення, випадкової втрати, зміни, несанкціонованого доступу й розголошення. З цією метою Оператор вживає відповідних технічних і організаційних заходів, які відповідають режиму обробки й ризику, який становить обробка для прав Суб'єктів даних відповідно до вимог GDPR. Детальний опис технічних і організаційних заходів викладено в Політиці безпеки.

8. **Контактна інформація Оператора.** Усі сповіщення, запити, претензії й інші повідомлення

щодо захисту персональних даних надсилаються на адресу ESET, spol. s.r.o., до уваги: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due

account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach

(including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities

covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any

complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory

authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in

line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on

the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by

the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic

origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Політика конфіденційності

Набуває чинності з 21 березня 2023 року | Переглянути попередню версію Політики конфіденційності | Порівняти зміни

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.

Правові основи для обробки персональних даних

Є лише декілька законних підстав для обробки даних, які ми використовуємо відповідно до чинної законодавчої бази, пов’язаної із захистом персональних даних. Компанії ESET в основному необхідно обробляти персональні дані з метою виконання положень документа Умови використання (далі — "Умови") з Кінцевим користувачем (ст. 6 (1) (b) GDPR), що застосовується для надання продуктів або служб ESET, якщо явно не зазначено інше, наприклад:

- Правові підстави законних інтересів (ст. 6 (1) (f) GDPR), які дозволяють нам обробляти дані про спосіб використання Служб нашими клієнтами й про ступінь їхнього задоволення, що дає змогу надавати нашим користувачам найкращий захист і підтримку, а також забезпечувати найвищий рівень обслуговування. Навіть маркетингові комунікації згідно з чинним законодавством визнаються законним інтересом, тому ми спираємося на це, коли надсилаємо повідомлення маркетингового характеру нашим клієнтам.
- Згода (ст. 6 (1) (a) GDPR), яку Ми можемо просити Вас надати в певних випадках, коли вважатимемо таку правову підставу найбільш відповідною, або якщо це необхідно згідно із законодавством.
- Виконання правових зобов’язань (ст. 6 (1) (c) GDPR), наприклад визначення вимог до електронних комунікацій і зберігання рахунків-фактур або документів, пов’язаних із розрахунками.

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.

Ми використовуємо служби третіх сторін, пов’язані з хмарними обчисленнями, які надаються Microsoft як постачальником хмарних послуг.

Безпека даних

ESET впроваджує відповідні технічні та організаційні заходи, щоб забезпечити безпеку на тому рівні, якій відповідає потенційним ризикам. Ми докладаємо всіх зусиль, щоб постійно забезпечувати конфіденційність, цілісність, доступність і стійкість систем обробки і сервісів.

Однак у випадку витоку конфіденційної інформації, що загрожує Вашим правам і свободам, ми готові сповістити про це відповідний наглядовий орган, а також Кінцевих користувачів як суб'єктів даних.

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.

Обробка персональних даних.

Сервіси від ESET реалізовані в наших веб-продуктах та надаються на умовах, визначених у документі «Умови використання» (далі — «УВ»), 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, як передбачено умовами та в документації. Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

Дані про ліцензії та розрахунки. Відповідно до чинного законодавства або за Вашою згодою компанія ESET збирає й обробляє такі відомості, як ім’я, адресу електронної пошти, ліцензійний ключ і (якщо застосовно) адресу, місце роботи та платіжні дані з метою проведення таких заходів: активація ліцензії, доставка ліцензійного ключа, нагадування про закінчення терміну дії, обробка запитів на підтримку, перевірка справжності ліцензії, надання служби й надсилання сповіщень, включаючи маркетингові повідомлення. За законом компанія ESET зобов’язана зберігати платіжну інформацію протягом 10 років, проте інформацію про ліцензію буде анонімізовано не пізніше ніж через 12 місяців після закінчення терміну дії ліцензії.

Оновлення й інші статистичні дані. З метою впровадження оновлень, обслуговування, захисту безпеки та поліпшення нашої серверної інфраструктури ми обробляємо інформацію, пов’язану з процесом інсталяції й вашим комп’ютером, зокрема платформою, у якій інстальовано продукт, а також інформацію про операції й функціональність наших продуктів, зокрема відомості про операційну систему й обладнання, ідентифікатори інсталяції та ліцензії, IP-адреси, MAC-адреси та параметри конфігурації продукту.

Ця інформація зберігається окремо від ідентифікаційних даних, необхідних для цілей ліцензування та виставлення рахунків, оскільки в цьому випадку ідентифікація Кінцевого користувача не потрібна. Період зберігання: до 4 років.

Система репутації ESET LiveGrid®. Односторонні хеші, пов’язані із загрозами, обробляються для забезпечення роботи системи репутації ESET LiveGrid®, яка підвищує ефективність рішень для захисту від шкідливого ПЗ, здійснюючи перевірку файлів за білим і чорним списками в хмарній базі даних об’єктів. Цей процес не передбачає ідентифікацію Кінцевого користувача.

Система зворотного зв’язку ESET LiveGrid®. 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 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.

Уся інформація, отримана й оброблена через систему зворотного зв’язку ESET LiveGrid®, призначена для використання без ідентифікації Кінцевого користувача.

Технічна підтримка. Контактна інформація, відомості про ліцензію та 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. Дані, що оброблялися з метою надання технічної підтримки, зберігаються протягом 4 років.

Зверніть увагу, що якщо особа, яка використовує наші продукти та служби, не є Кінцевим користувачем, який придбав продукт або службу й уклав із Нами Умови (наприклад, співробітник Кінцевого користувача, член сім’ї або інша особа, уповноважена використовувати продукт або службу Кінцевим користувачем відповідно до Ліцензійної угоди), обробка даних здійснюється в законних інтересах компанії ESET у розумінні ст. 6 (1) (f) GDPR, щоб дати змогу користувачу, уповноваженому Кінцевим користувачем, використовувати продукти та служби, що надаються Нами відповідно до Умов.

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