

ESET PROTECT

Installation, Upgrade and Migration Guide

[Click here to display the Online help version of this document](#)

Авторське право за ©ESET, spol. s r.o., 2021

ESET PROTECT розроблено компанією ESET, spol. s r.o.

Докладніше див. на веб-сайті www.eset.ua.

Усі права захищено. Забороняється відтворювати, зберігати в інформаційно-пошуковій системі або передавати в будь-якій формі та будь-якими засобами (електронними, механічними, шляхом фотокопіювання, записування, сканування чи іншим чином) будь-яку частину цієї документації без письмового дозволу автора.

ESET, spol. s r.o. зберігає за собою право змінювати без попередження будь-яке описане програмне забезпечення.

Служба технічної підтримки: www.eset.com/support

РЕД. 30.04.2021

1	Про довідку	1
2	Інсталяція або оновлення	2
2.1	Нові функції ESET PROTECT 8.0	2
2.2	Архітектура	3
2.2.1	Сервер	4
2.2.2	Web Console	4
2.2.3	Проксі-сервер HTTP	5
2.2.4	Агент	7
2.2.5	Rogue Detection Sensor	8
2.2.6	Mobile Device Connector	9
2.2.7	Проксі-сервер Apache HTTP	10
2.3	Відмінності між проксі-сервером Apache HTTP, інструментом «Дзеркало» та прямим підключенням	14
2.3.1	Коли починати користуватися проксі-сервером Apache HTTP	15
2.3.2	Коли починати користуватись інструментом «Дзеркало»	16
3	Системні вимоги та налаштування розмірів	16
3.1	Підтримувані операційні системи	16
3.1.1	Windows	17
3.1.2	Linux	18
3.1.3	macOS	19
3.1.4	Мобільний пристрій	19
3.2	Підтримувані середовища підготовки настільних комп'ютерів	20
3.3	Обладнання та налаштування розмірів інфраструктури	21
3.3.1	Рекомендації щодо розгортання	22
3.3.2	Розгортання для 10 000 клієнтів	24
3.4	База даних	24
3.5	Підтримувані версії Apache Tomcat і Java	26
3.6	Підтримувані веб-браузери, продукти ESET для захисту та мови	26
3.7	Мережа	28
3.7.1	Використовувані порти	29
4	Процес інсталяції	32
4.1	Універсальна інсталяція у Windows	33
4.1.1	Інсталяція сервера ESET PROTECT	34
4.1.2	Інсталяція ESET PROTECT Mobile Device Connector (автономно)	46
4.2	Інсталяція в Microsoft Azure	52
4.3	Інсталяція компонентів у Windows	52
4.3.1	Інсталяція сервера	54
4.3.1.1	Попередні вимоги до сервера - Windows	60
4.3.2	Вимоги до Microsoft SQL Server	60
4.3.3	Інсталяція та конфігурація сервера MySQL	61
4.3.4	Спеціальний обліковий запис користувача бази даних	62
4.3.5	Інсталяція агента	63
4.3.5.1	Інсталяція агента з використанням сервера	65
4.3.5.2	Інсталяція агента в автономному режимі	66
4.3.5.3	Видалення агента й виправлення неполадок	66
4.3.5.4	ESET Remote Deployment Tool	67
4.3.6	Інсталяція веб-консолі	67
4.3.6.1	Інсталяція веб-консолі з використанням універсального інсталюатора	67
4.3.6.2	Інсталяція веб-консолі вручну	71
4.3.7	Інсталяція проксі-сервера HTTP	73
4.3.8	Інсталяція RD Sensor	74
4.3.8.1	Попередні вимоги до RD Sensor	74
4.3.9	Інструмент «Дзеркало» - Windows	74
4.3.10	Інсталяція Mobile Device Connector	79
4.3.10.1	Попередні вимоги до Mobile Device Connector	81

4.3.10.2 Активація Mobile Device Connector	83
4.3.10.3 Ліцензування iOS в MDM	84
4.3.10.4 Вимоги до сертифіката HTTPS	84
4.3.11 Інсталяція та кешування проксі-сервера Apache HTTP	85
4.3.11.1 Конфігурація проксі-сервера Apache HTTP	86
4.3.12 Інсталяція Squid у Windows і кешування проксі-сервера HTTP	89
4.3.13 Автономний репозиторій	89
4.3.14 Відмовостійкий кластер	91
4.4 Інсталяція компонентів у Linux	92
4.4.1 Інсталяція та конфігурація MySQL	93
4.4.2 Інсталяція та конфігурація ODBC	94
4.4.3 Інсталяція сервера – Linux	95
4.4.3.1 Попередні вимоги до сервера – Linux	98
4.4.4 Інсталяція агента – Linux	100
4.4.4.1 Попередні вимоги до агента – Linux	103
4.4.5 Інсталяція веб-консолі – Linux	104
4.4.6 Інсталяція проксі-сервера – Linux	105
4.4.7 Попередні вимоги й інсталяція RD Sensor – Linux	106
4.4.8 Інсталяція Mobile Device Connector – Linux	107
4.4.8.1 Попередні вимоги до Mobile Device Connector – Linux	109
4.4.9 Інсталяція проксі-сервера Apache HTTP – Linux	110
4.4.10 Інсталяція проксі-сервера Squid HTTP на сервері Ubuntu	114
4.4.11 Інструмент «Дзеркало» – Linux	115
4.4.12 Відмовостійкий кластер – Linux	119
4.5 Покрокова інсталяція сервера ESET PROTECT в Linux	122
4.6 Інсталяція компонентів у macOS	122
4.6.1 Інсталяція агента – macOS	122
4.7 Образ ISO	123
4.8 Запис служби DNS	124
4.9 Сценарій інсталяції ESET PROTECT в автономному режимі	124
5 Процедури оновлення, міграції та повторної інсталяції	125
5.1 Завдання з оновлення компонентів ESET PROTECT	126
5.2 Оновлення за допомогою ESET PROTECT8.0 Універсальний інстальатор	130
5.3 Оновлення інфраструктури за допомогою проксі-сервера ERA 6.5	132
5.4 Перенесення з ERA 5.x	134
5.5 Перенесення з одного сервера на інший	135
5.5.1 Чиста інсталяція – така сама IP-адреса	135
5.5.2 Перенесена база даних: інша/така сама IP-адреса	136
5.6 Створення резервної копії, оновлення сервера бази даних і перенесення бази даних ESET PROTECT	137
5.6.1 Створення резервної копії та відновлення сервера бази даних	138
5.6.2 Оновлення сервера бази даних	140
5.6.3 Процедура міграції для MS SQL Server	140
5.6.4 Процедура міграції для MySQL Server	148
5.6.5 Підключення сервера ESET PROTECT або MDM до бази даних	150
5.7 Перенесення MDM	151
5.8 Оновлення рішення ERA/ESMC, інстальованого у відмовостійкому кластері у Windows	152
5.9 Оновлення проксі-сервера Apache HTTP	152
5.9.1 Оновлення проксі-сервера Apache HTTP за допомогою універсального інстальатора (Windows)	153
5.9.2 Оновлення проксі-сервера Apache HTTP вручну (Windows)	154
5.10 Оновлення Apache Tomcat	155
5.10.1 Оновлення Apache Tomcat за допомогою універсального інстальатора (Windows)	156
5.10.2 Оновлення Apache Tomcat вручну (Windows)	159
5.10.3 Оновлення Apache Tomcat (Linux)	161
5.11 Змінення IP-адреси чи імені хоста сервера ESET PROTECT після перенесення	162
5.12 Оновлення рішення ERA/ESMC, інстальованого у відмовостійкому кластері в Linux	162

6 Видалення сервера ESET PROTECT і його компонентів	163
6.1 Windows - Видалення сервера ESET PROTECT і його компонентів	163
6.2 Linux - Оновлення, повторна інсталяція або видалення компонентів ESET PROTECT	164
6.3 macOS: видалення ESET Management Agent і продукту ESET Endpoint	165
6.4 Видалення старого сервера ERA/ESMC/ESET PROTECT/MDM після перенесення на новий сервер	166
7 Виправлення неполадок	167
7.1 Оновлення компонентів ESET PROTECT в автономному середовищі	167
7.2 Рішення поширених проблем під час інсталяції	168
7.3 Файли журналу	171
7.4 Інструмент діагностики	172
7.5 Проблеми після оновлення або перенесення сервера ESET PROTECT	174
7.6 Ведення журналів MSI	174
8 API ESET PROTECT	175
9 Питання й відповіді	175
10 Ліцензійна угода з кінцевим користувачем	181
11 Політика конфіденційності	187

Про довідку

Цей посібник з інсталяції містить допоміжні інструкції щодо інсталяції й оновлення ESET PROTECT.

Щоб забезпечити узгодженість і уникнути плутанини, у цьому посібнику використовується термінологія на основі назв параметрів ESET PROTECT. Ми також використовуємо набір символів для позначення тем, що становлять особливий інтерес або є особливо важливими.



Примітка

Примітки можуть містити важливу інформацію, зокрема інформацію щодо певних функцій або посилання на пов'язані теми.



Увага

Ця інформація потребує вашої уваги. Слід уважно ознайомитися з нею. Зазвичай це певна некритична, але важлива інформація.



Попередження

Із цією критично важливою інформацією потрібно дуже уважно ознайомитися. Попередження спеціально призначені, щоб утримати вас від потенційно небезпечних помилок. Ви маєте в повному обсязі усвідомити інформацію, наведену в дужках попередження, оскільки це стосується вразливих параметрів системи або високого ризику.



Приклад

Приклад сценарію з описом конкретної ситуації користувача, яка стосується теми з цим прикладом. Приклади використовуються для додаткового пояснення складних тем.

Позначення	Значення
Жирний текст	Назви елементів інтерфейсу, наприклад полів і кнопок опцій.
<i>Текст курсивом</i>	Заповнювачі для інформації, яку ви вказуєте. Наприклад, назва файлу або шлях означають, що ви ввели фактичну назву файлу або шлях.
Текст шрифтом Courier New	Зразки кодів і команд.
<u>Гіперпосилання</u>	Елемент для швидкого й легкого доступу до перехресних посилань і зовнішніх розташувань в Інтернеті. Гіперпосилання виділені синім кольором і можуть бути підкреслені.
%ProgramFiles%	Каталог системи Windows, у якому зберігаються інсталювані програми Windows та інших розробників.

- [Онлайн-довідка](#) — основне джерело інформації. Остання версія онлайн-довідки автоматично відобразатиметься за наявності робочого підключення до Інтернету. На сторінках онлайн-довідки ESET PROTECT розміщено чотири активні вкладки вгорі навігаційного заголовка: [Інсталяція або оновлення](#), [Адміністрування](#), [Розгортання віртуального пристрою](#) та [Посібник SMB](#).

- Теми в цьому керівництві розподілені між кількома розділами й підрозділами. Щоб знайти потрібну інформацію, скористайтеся полем "Пошук" угорі.



Увага

Коли ви відкриєте посібник користувача на панелі навігації вгорі сторінки, пошук виконуватиметься лише по вмісту посібника. Наприклад, якщо ви відкриєте посібник «Адміністратор», теми з посібників «Інсталяція або оновлення» та «Розгортання віртуального пристрою» не включатимуться в результати пошуку.

- У [базі знань ESET](#) є відповіді на найбільш поширені питання, а також рекомендовані рішення різних проблем. Регулярне оновлення, яке виконують технічні спеціалісти ESET, робить базу знань найефективнішим інструментом для вирішення різноманітних проблем.
- На [форумі ESET](#) користувачі ESET можуть легко знайти довідкову інформацію або допомогти іншим користувачам. На форумі можна звернутися за допомогою для вирішення будь-яких проблем або поставити будь-які питання, пов'язані з продуктами ESET.

Інсталяція або оновлення

ESET PROTECT (ESET PROTECT) – це програма, що дає змогу з єдиного центру керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях клієнта, які працюють у мережі. Вбудована в ESET PROTECT система керування завданнями дає змогу інсталювати рішення безпеки ESET на віддалених комп'ютерах і швидко реагувати на нові проблеми та виявлені об'єкти.

ESET PROTECT сам по собі не забезпечує захисту від шкідливого коду. Захист вашого середовища залежить від наявності рішень безпеки ESET на робочих станціях і мобільних пристроях (наприклад, ESET Endpoint Security) та серверах із Microsoft Windows Server (наприклад, ESET File Security).

ESET PROTECT базується на двох основних принципах:

1. **Централізоване керування** – можна здійснювати налаштування, керування та нагляд за системою з одного місця.
2. **Масштабованість** – систему можна розгорнути як у невеликій мережі, так і у великих корпоративних середовищах. ESET PROTECT розроблено з урахуванням можливості розширення інфраструктури.

ESET PROTECT підтримує як нове, так і [попереднє покоління продуктів ESET для захисту](#).

У довідці ESET PROTECT можна знайти повний посібник з інсталяції й оновлення:

- [Архітектура ESET PROTECT](#)
- [Процес інсталяції](#)
- [Процес оновлення](#)
- [Керування ліцензією](#)
- [Процедури розгортання й інструкція з розгортання агента за допомогою об'єкта групової політики \(GPO\) або SCCM](#)
- [Перші кроки після інсталяції ESET PROTECT](#)
- [Посібник адміністратора](#)

Нові функції ESET PROTECT 8.0

Перейменування ESET Security Management Center

ESET Security Management Center перейменовано на ESET PROTECT. Продукти й послуги постійно змінюються відповідно до потреб нових ринків і клієнтів. Ми вирішили перейменувати наше рішення, щоб його назва краще відповідала його наявним можливостям, а також тим можливостям, які ми плануємо реалізувати.

ESET Full Disk Encryption для macOS

Ми розширюємо покриття платформи та додаємо систему FileVault (власне шифрування для macOS), що дає змогу керувати безпекою й надійніше захищати дані організації. [Докладніше](#)

Розширені функції

Деякі функції призначено для великих мереж, оскільки вони дають змогу налаштовувати більше параметрів. Їх усі можна знайти в наявному інтерфейсі користувача.

Журнал аудиту

Нова функціональність допомагає адміністраторам визначати й відстежувати активність у ESET PROTECT. Зокрема, вони можуть швидко запускати завдання, змінювати політики, опрацьовувати виявлені об'єкти, додавати користувачів чи комп'ютери, а також за потреби вносити зміни та виправлення. [Докладніше](#)

Виключення загроз за допомогою брандмауера

Тепер за допомогою брандмауера можна виключати загрози зі списку виявлених об'єктів. [Докладніше](#)

Підтримка ESET Business Account Місця

Тепер можна імпортувати повну структуру ESET Business Account, зокрема розподіл робочих місць із ліцензії між [місцями](#).

Архітектура

ESET PROTECT — система віддаленого керування нового покоління. ESET PROTECT тільки частково сумісний з ERA 6 і не має зворотної сумісності з ERA 5. Проте цей продукт залишається сумісним із попередніми версіями [продуктів ESET для захисту](#).

У співпраці з ESET PROTECT компанія ESET розробила нове покоління продуктів безпеки з новою системою ліцензування.

Щоб повністю розгорнути портфель рішень безпеки ESET, мають бути інсталювані такі компоненти (для платформ Windows і Linux):

- [Сервер ESET PROTECT](#)
- [Веб-консоль ESET PROTECT](#)
- [Агент ESET Management](#)

Вказані нижче супутні компоненти не є обов'язковими, але ми рекомендуємо інсталювати їх, щоб забезпечити найкращу продуктивність роботи програми в мережі:

- [Проксі-сервер](#)
- [RD Sensor](#)
- [Проксі-сервер HTTP Apache](#)
- [Mobile Device Connector](#)

Компоненти ESET PROTECT використовують сертифікати для встановлення зв'язку із сервером ESET PROTECT. Докладніше про типи сертифікатів у ESET PROTECT можна дізнатися в нашій [статті бази знань](#).

Огляд елементів інфраструктури

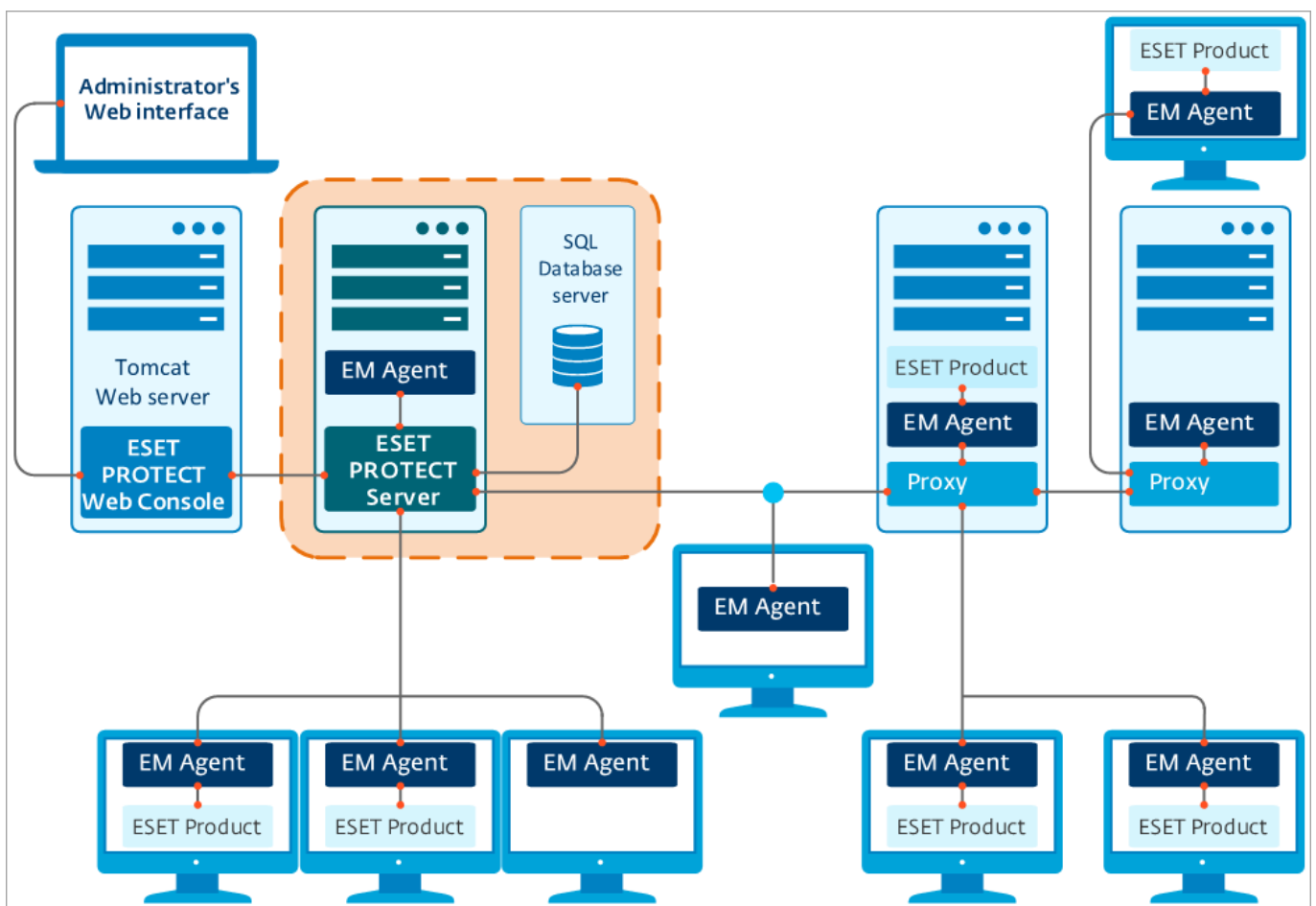
У таблиці нижче міститься огляд елементів інфраструктури ESET PROTECT та їхніх основних функцій:

Функція	Сервер ESET PROTECT	Агент ESET Management	Продукт захисту ESET	Проксі-сервер HTTP	Сервери ESET	Mobile Device Connector
Віддалене керування продуктами ESET для захисту (створення політик, завдань, звітів тощо)	✓	x	x	x	x	x
Обмін даними із сервером ESET PROTECT та керування продуктами ESET для захисту на клієнтському пристрої	x	✓	x	x	x	✓
Надання оновлень, перевірка ліцензій	x	x	x	x	✓	x

Кешування та переадресація оновлень (ядро виявлення, інсталятори, модулі)	x	x	✓	✓	x	x
Переадресація мережевого трафіку між агентом ESET Management і сервером ESET PROTECT	x	x	x	✓	x	x
Захист клієнтського пристрою	x	x	✓	x	x	x
Віддалене керування мобільними пристроями	x	x	x	x	x	✓

Сервер

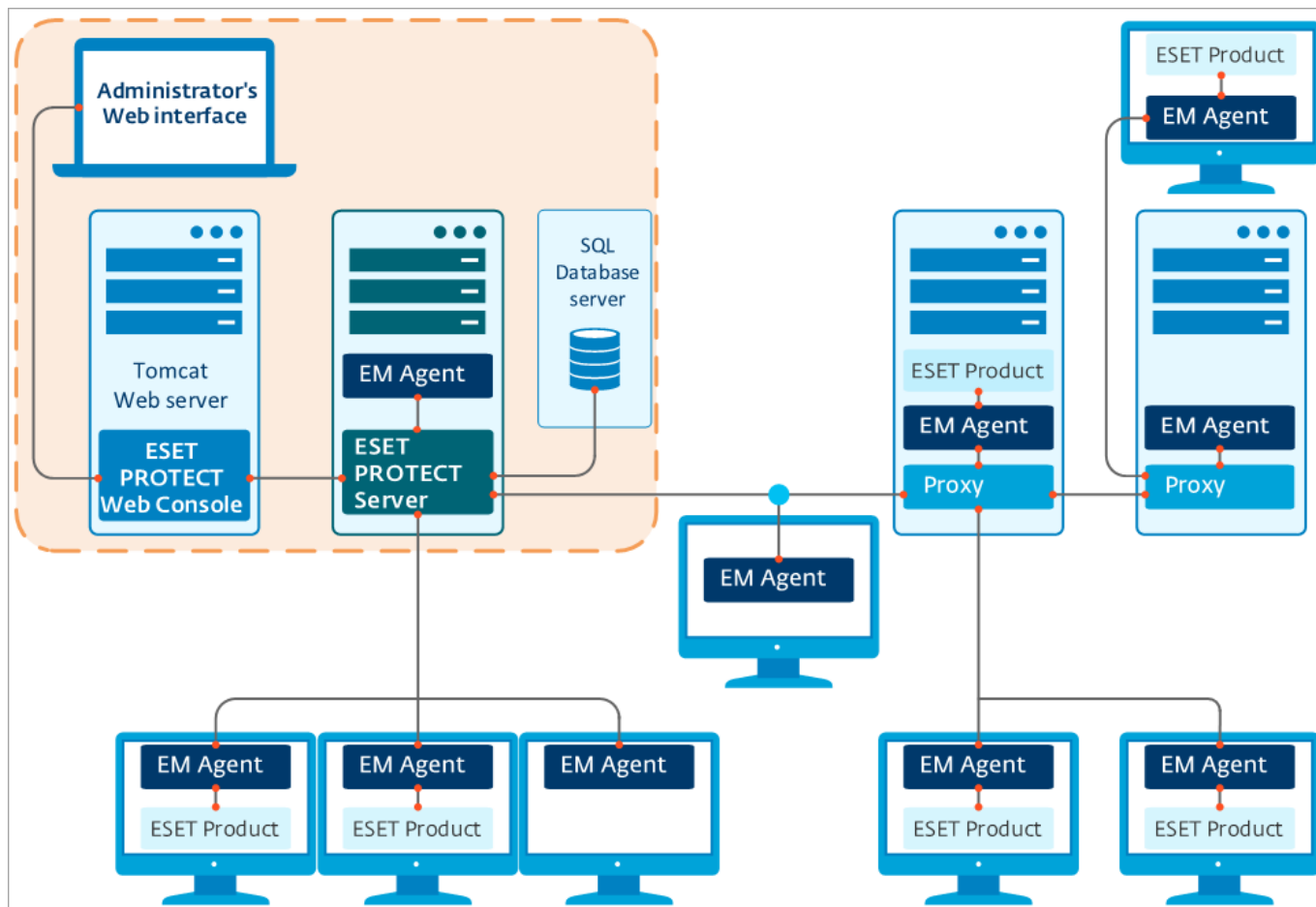
Сервер ESET PROTECT – це програма, яка обробляє всі дані, отримані від клієнтів, які підключаються до сервера (через агента ESET Management або [проксі-сервер HTTP](#)). Для належної обробки даних необхідно забезпечити стабільне підключення між цим сервером і сервером бази даних, у якій зберігаються мережеві дані. Для підвищення продуктивності рекомендується інстальовати сервер бази даних на іншому комп'ютері.



Web Console

Веб-консоль ESET PROTECT – це веб-інтерфейс користувача, який дає змогу керувати рішеннями безпеки ESET у вашому середовищі. У ньому відображається загальна інформація про статус клієнтів у мережі. Окрім того, його можна використовувати для віддаленого розгортання рішень ESET на некеровані комп'ютери. Доступ до веб-консолі здійснюється за допомогою браузера (див. список [підтримуваних браузерів](#)). Якщо зробити веб-сервер доступним з Інтернету, ESET PROTECT можна використовувати практично в будь-якому місці й на будь-якому пристрої.

Веб-консоль використовує Apache Tomcat як веб-сервер HTTP. У разі використання Tomcat з інсталятора ESET або віртуального пристрою для підключення до веб-консолі можна використовувати лише протоколи TLS 1.2 та 1.3.



Проксі-сервер HTTP

Що таке проксі-сервер HTTP та як його використовувати?

Проксі-сервер HTTP передає дані від агентів до сервера ESET PROTECT в середовищах, де агенти не можуть підключитися до сервера.

Що таке проксі-сервер ERA 6.x і чому його видалили?

Проксі-сервер ERA збирав трафік від клієнтських агентів. Таким чином кілька агентів могли підключитися до ERA Proxy, який спрямовував трафік на ERA Server. ESET PROTECT використовує новий протокол реплікації, що дає змогу спрямовувати її трафік через новий проксі-сервер. Проксі-сервер ERA 6.x не підтримує цей протокол, тому його не можна використовувати з агентами ESET Management .

Чи можна використовувати проксі-сервер ERA 6.x разом із ESET PROTECT?

В обмеженій мірі. Проксі-сервер ERA 6.x може пересилати дані від агентів версій 6.x до сервера ESET PROTECT, але агенти ESET Management не можуть підключатися до сервера/проксі-сервера ERA 6.x. Врахуйте це під час [оновлення інфраструктури](#) з версії 6.x.

Як працює проксі-сервер у ESET PROTECT?

ESET PROTECT 8 використовує спеціалізовану версію [проксі-сервера Apache HTTP](#). Після відповідного налаштування проксі-сервер Apache HTTP може діяти як проксі-сервер для агентів ESET Management. Проксі-сервер не кешує та не запускає зв'язок, а лише пересилає дані.

Чи можна використовувати інші проксі-сервери окрім [Проксі-сервер HTTP Apache](#)?

З агентом ESET Management можна використовувати будь-який проксі-сервер, яке відповідає наступним умовам:

- передача даних по SSL
- підтримка HTTP CONNECT
- робота без імені користувача та пароля

Чим відрізняється новий протокол зв'язку?

Сервер ESET PROTECT обмінюється даними з агентами ESET Management через протокол gRPC. Щоб дані могли передаватися через проксі-сервери, використовується TLS та HTTP2. Крім того, було додано нові функції самовідновлення та забезпечення стабільного з'єднання, які покращують загальну ефективність обміну даними.

Як це впливає на продуктивність?

Використання проксі-сервера HTTP не має істотного впливу на продуктивність комп'ютера.

Коли слід використовувати проксі-сервер?

Рекомендується використовувати проксі-сервер, якщо ваша інфраструктура відповідає принаймні одній із наведених нижче умов:

- Ваші агенти не можуть напряму підключитися до сервера ESET PROTECT.
- Ви обслуговуєте віддалене робоче місце або відділення компанії та хочете використовувати проксі-сервер для забезпечення зв'язку:
 - оміж сервером ESET PROTECT і проксі-сервером,
 - оміж проксі-серверами та клієнтськими комп'ютерами на віддаленому робочому місці.

Як налаштувати проксі-сервер HTTP

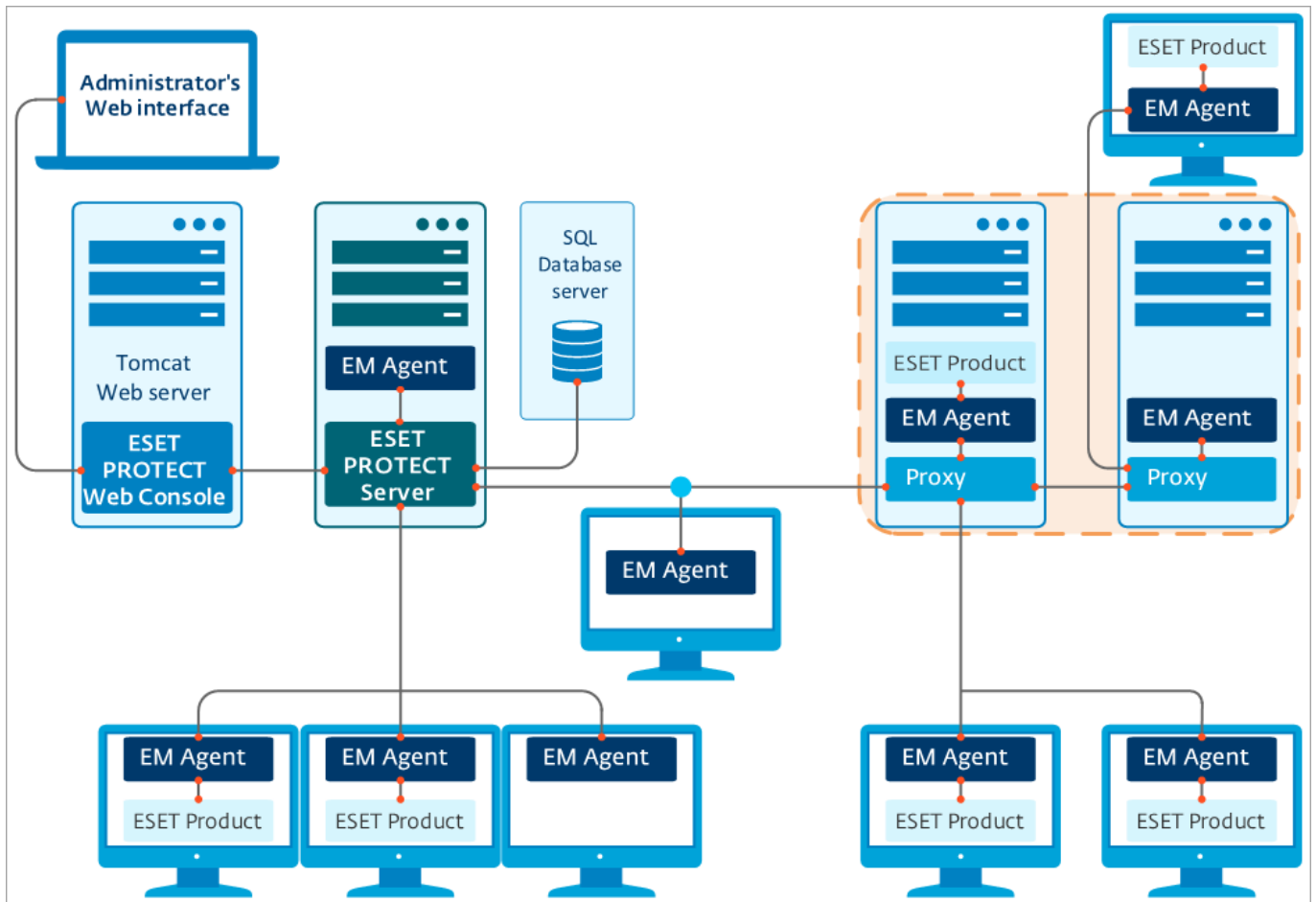
Щоб користуватися проксі-сервером, потрібно налаштувати ім'я хоста проксі-сервера HTTP в [політиці агента](#) (**Додаткові параметри > Проксі-сервер HTTP**). Для кешування та перенаправлення можна використовувати різні проксі-сервери. Перегляньте параметри політики нижче.

- **Глобальний проксі-сервер.** Один проксі-сервер використовуватиметься для кешування завантажень і перенаправлення даних агента.
- **Різні проксі-сервери для служби.** Для кешування та перенаправлення даних використовуватимуться різні проксі-сервери.



Примітка

- Які ще функції має [проксі-сервер Apache HTTP](#)?
- [Як оновити](#) інфраструктуру з проксі-сервером ERA 6.x до ESET PROTECT?



Агент

Агент ESET Management є невід'ємною частиною ESET PROTECT. Після версії 6.x (агент ERA) назву компонента було змінено, але він все ще виконує ту саму функцію. Агент ESET Management використовує новий, удосконалений [протокол зв'язку](#).

Клієнти передають дані на сервер ESET PROTECT не напряму, а через агента. Агент збирає інформацію від клієнта та надсилає її на сервер ESET PROTECT. Якщо сервер ESET PROTECT надсилає завдання клієнту, воно потрапляє до агента, який пересилає завдання до призначення.

Для спрощення розгортання захисту робочої станції до пакета ESET PROTECT входить відокремлений агент ESET Management. Це проста універсальна служба, що відрізняється невеликим розміром і забезпечує весь обмін даними між сервером ESET PROTECT та продуктами ESET чи операційною системою. Продукти ESET передають дані не на сервер ESET PROTECT, а до агента. Клієнтські комп'ютери, на яких інстальовано агент ESET Management та які можуть обмінюватися даними із сервером ESET PROTECT, називаються «керованими». Ви можете інстальовати агента на будь-який комп'ютер, навіть якщо на ньому немає іншого програмного забезпечення ESET.

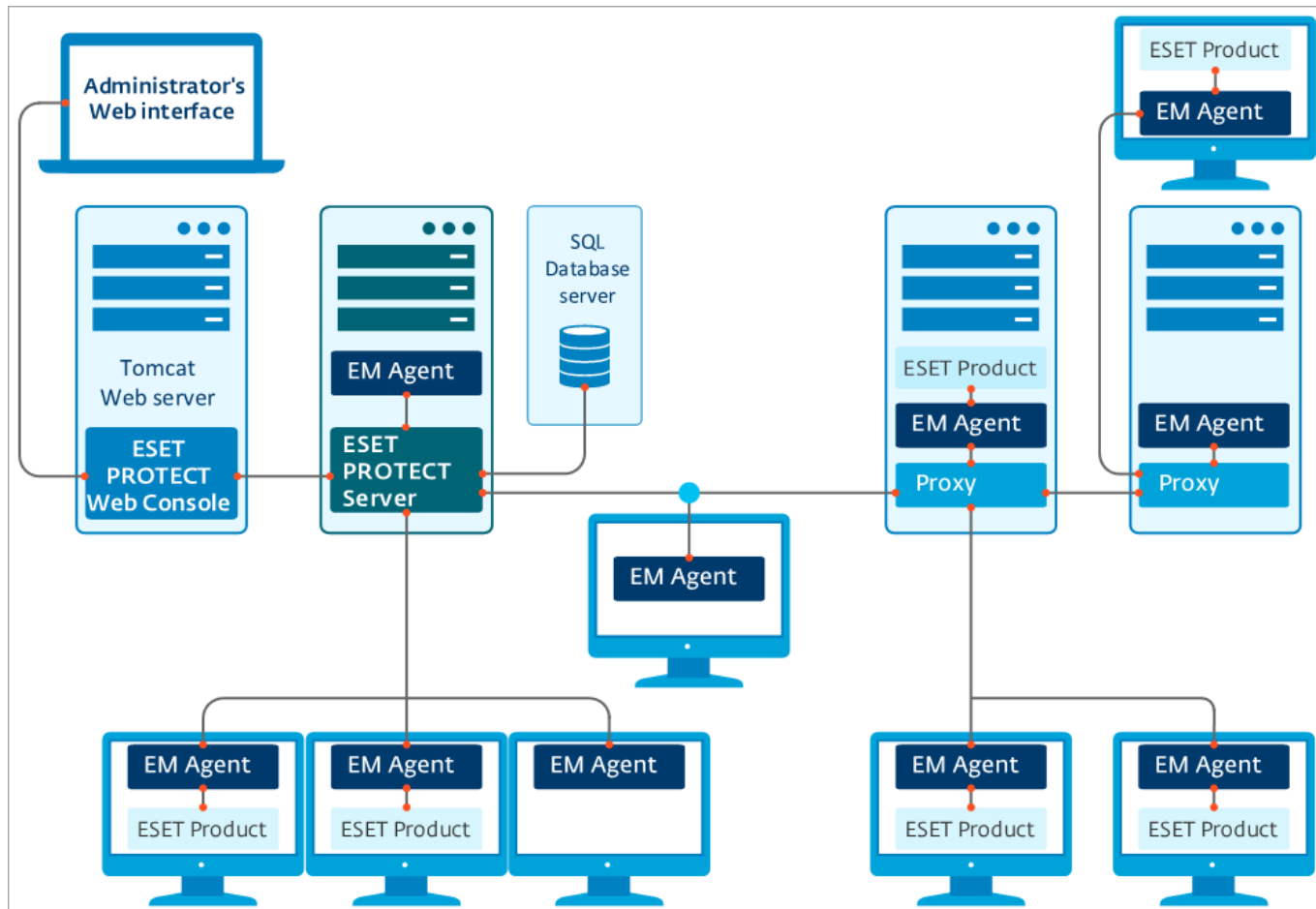
Переваги

- Просте налаштування - агента можна розгорнути під час стандартної інсталяції в корпоративному середовищі.
- Локальне керування безпекою - оскільки агент може зберігати кілька сценаріїв забезпечення безпеки, це дає змогу значно прискорити реакцію на виявлені об'єкти.
- Керування безпекою в автономному режимі - агент може реагувати на подію, навіть якщо його не підключено до сервера ESET PROTECT.



Увага

Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT, для якого потрібна автентифікація, не працюватиме. Якщо ви не виберете порт для веб-консолі або агента за замовчуванням, можливо, потрібно буде налаштувати брандмауер відповідним чином. В іншому разі інсталяція може закінчитися невдало.

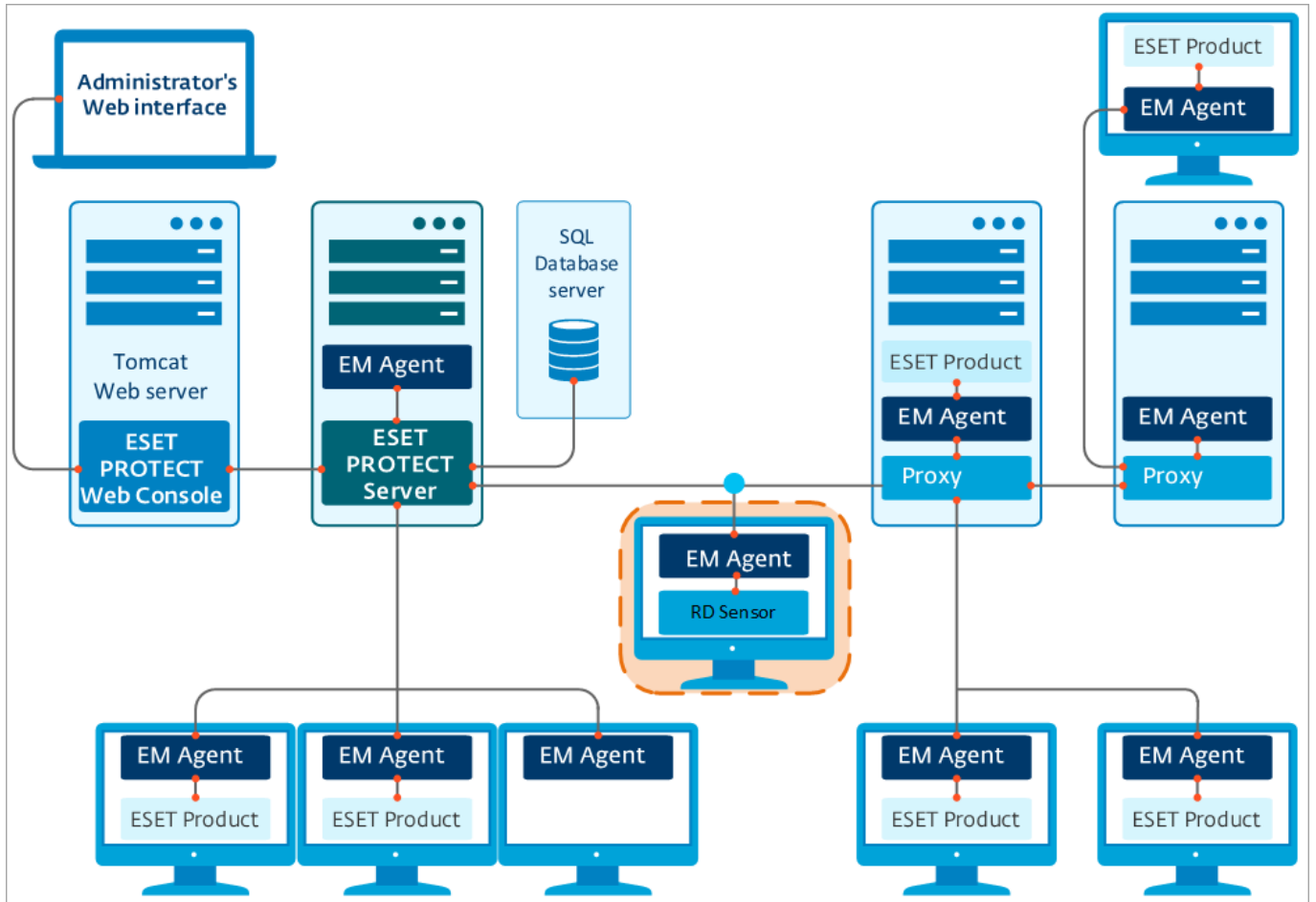


Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) – це засіб виявлення неавторизованих систем, який здійснює пошук комп'ютерів у вашій мережі. Цей засіб може знаходити нові комп'ютери з ESET PROTECT без ручного пошуку та додавання. Виявлені комп'ютери негайно вносяться до попередньо налаштованого звіту, завдяки чому ви можете переносити їх до певних статичних груп і виконувати різні завдання керування.

RD Sensor – пасивний засіб ведення обліку, що виявляє комп'ютери в мережі й надсилає інформацію про них серверу ESET PROTECT. Сервер ESET PROTECT оцінює статус виявлених ПК (невідомі для сервера ESET PROTECT чи під керуванням).

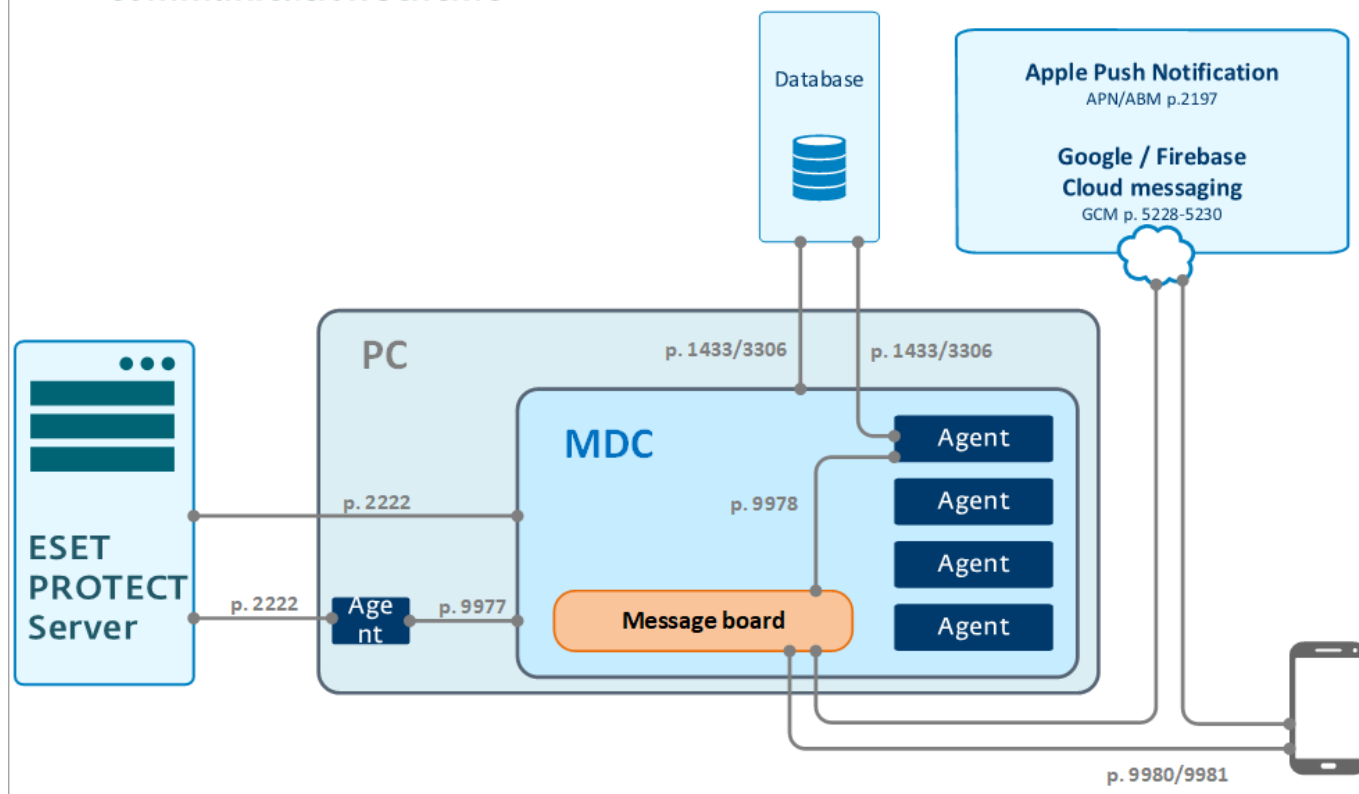
Завдяки синхронізації із сервером усі комп'ютери мережі (домену, LDAP, мережі Windows) автоматично вносяться до списку комп'ютерів сервера ESET PROTECT. RD sensor дає змогу швидко знаходити комп'ютери, що не входять до домену чи іншої мережевої структури, і додавати їх до сервера ESET PROTECT. RD Sensor зберігає дані про знайдені комп'ютери, тому ніколи не надсилає одну й ту саму інформацію двічі.



Mobile Device Connector

ESET PROTECT Mobile Device Connector. Цей компонент робить можливим керування мобільними пристроями за допомогою ESET PROTECT, дозволяючи керувати мобільними пристроями (Android та iOS) і адмініструвати ESET Endpoint Security for Android.

ESET PROTECT – MDC – Device Communication scheme



[Клацніть тут, щоб збільшити зображення](#)



Примітка

Рекомендуємо розгорнути компонент MDM на хост-пристрої, на якому не розміщено сервер ESET PROTECT.

Рекомендовані попередні вимоги до обладнання для приблизно 80 керованих мобільних пристроїв:

Обладнання	Рекомендована конфігурація
Процесор	4 ядра, 2,5 ГГц
ОЗП	4 ГБ (рекомендовано)
Жорсткий диск	100 ГБ

Вимоги до обладнання майже не відрізняються для понад 80 керованих мобільних пристроїв. Затримка між надсиланням завдання з ESET PROTECT і його виконанням на мобільному пристрої пропорційно збільшуватиметься відповідно до кількості пристроїв у середовищі.

Проксі-сервер Apache HTTP

Apache HTTP Proxy – це проксі-сервер, за допомогою якого можна розповсюджувати оновлення на клієнтські комп'ютери. Функції Apache HTTP Proxy схожі на функції дзеркального сервера, який часто використовується в ERA версії 5 і нижче.

Щоб інсталиувати Apache HTTP Proxy, ознайомтеся з інструкціями для [Windows](#), [Linux](#) або [віртуального пристрою](#).

Функції проксі-сервера Apache HTTP

Функція	Проксі-сервер, на якому доступна ця функція
Кешування завантажень і оновлень	Проксі-сервер Apache HTTP або інший проксі-сервер
Кешування результатів ESET Dynamic Threat Defense	Лише налаштований проксі-сервер Apache HTTP

Функція кешування

Apache HTTP Proху завантажує й кешує:

- оновлення модулів ESET;
- пакети інсталяцій із серверів репозиторію;
- оновлення компонентів продуктів.

Кешовані дані розповсюджуються клієнтам робочих станцій у вашій мережі. Кешування може значно зменшити інтернет-трафік у вашій мережі.

На відміну від інструмента «Дзеркало», який завантажує всі доступні на серверах оновлення ESET дані, Apache HTTP Proху зменшує навантаження на мережу, завантажуючи лише ті дані, які необхідні компонентами ESET PROTECT або продуктам ESET на робочих станціях. Якщо клієнт робочої станції запитує оновлення, Apache HTTP Proху завантажує його із серверів оновлення ESET, зберігає в кеш, а потім пересилає відповідному клієнту робочої станції. Якщо інший клієнт запитує таке саме оновлення, Apache HTTP Proху передає файли клієнту безпосередньо з кешу та не завантажує із серверів оновлення ESET додаткових даних.

Кешування для продуктів ESET для робочих станцій

Налаштування кешування агента ESET Management та робочої станції відрізняються. Агент ESET Management може керувати налаштуваннями продуктів ESET для захисту на клієнтських пристроях. Ви можете налаштувати проксі-сервер для ESET Endpoint Security:

- [локально](#) в графічному інтерфейсі,
- з веб-консолі ESET PROTECT, використовуючи відповідну політику (рекомендований спосіб [керування](#) налаштуваннями клієнтських пристроїв).

Кешування результатів від ESET Dynamic Threat Defense

Проксі-сервер Apache HTTP також може кешувати результати, надані [ESET Dynamic Threat Defense](#). Для цього необхідно застосувати певну конфігурацію, яку включено в Apache HTTP Proху від ESET. Якщо це можливо, рекомендується використовувати кешування з ESET Dynamic Threat Defense. Більш докладні відомості див. у [документації](#) служби.

Використання Apache як проксі-сервера HTTP для підключення між агентом і сервером

Правильно налаштований Apache HTTP Proху можна використовувати для збору та пересилання даних від компонентів ESET PROTECT у віддалене сховище. Таку саму функцію виконує проксі-сервер ERA 6.x. Один проксі-сервер можна використовувати для кешування оновлень (рекомендується проксі-сервер Apache HTTP), а інший – для підключення між агентом і сервером. Ви можете використовувати Apache HTTP Proху для виконання обох функцій одночасно, але в мережах, що містять більше 10 000 клієнтських машин на один проксі-сервер не рекомендується робити це. У корпоративних середовищах (що містять більше 1000 керованих комп'ютерів) рекомендується використовувати спеціальний сервер Apache HTTP Proху.

Компонент ERA 6.x Proху не сумісний з агентами ESET Management. Детальніше про [Функції проксі-сервера](#).

Як налаштувати проксі-сервер HTTP

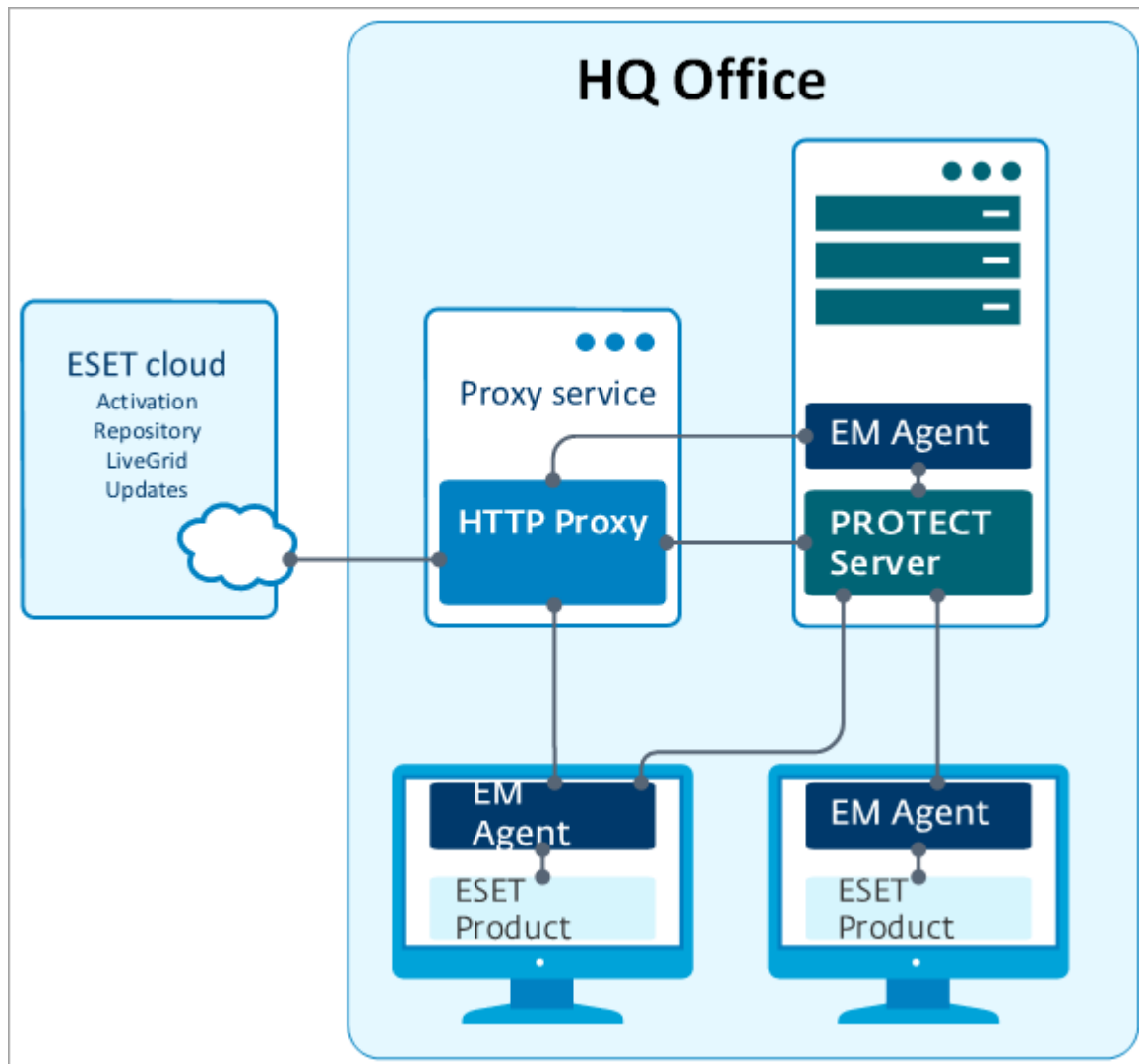
Щоб користуватися проксі-сервером, потрібно налаштувати ім'я хоста проксі-сервера HTTP в [політиці агента](#) (**Додаткові параметри > Проксі-сервер HTTP**). Для кешування та перенаправлення можна використовувати різні проксі-сервери. Перегляньте параметри політики нижче.

- **Глобальний проксі-сервер.** Один проксі-сервер використовуватиметься для кешування завантажень і перенаправлення даних агента.

- **Різні проксі-сервери для служби.** Для кешування та перенаправлення даних використовуватимуться різні проксі-сервери.

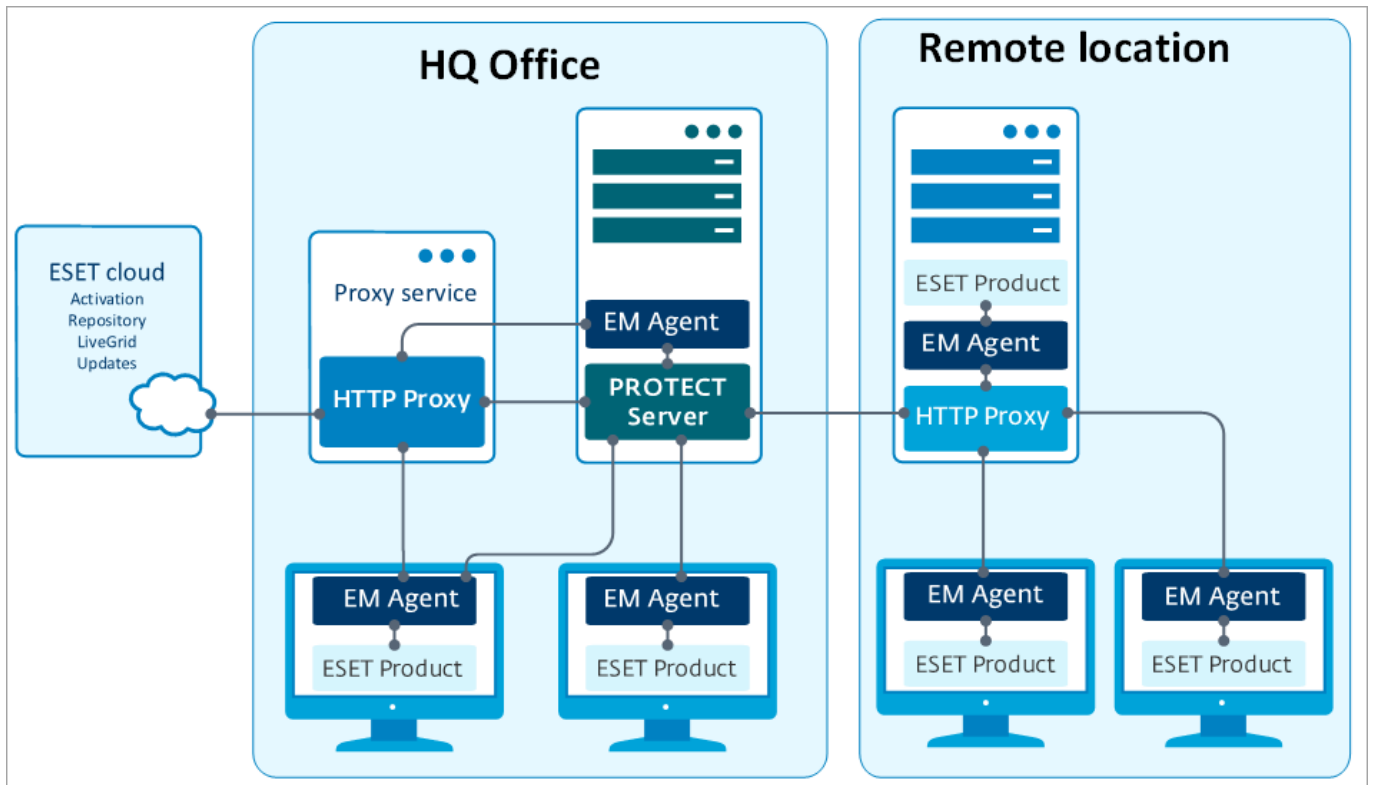
Проксі-сервер Apache HTTP в інфраструктурі

Нижче показано проксі-сервер (Apache HTTP), який використовується для розповсюдження хмарного трафіку ESET на всі компоненти ESET PROTECT та продукти ESET для робочих станцій.



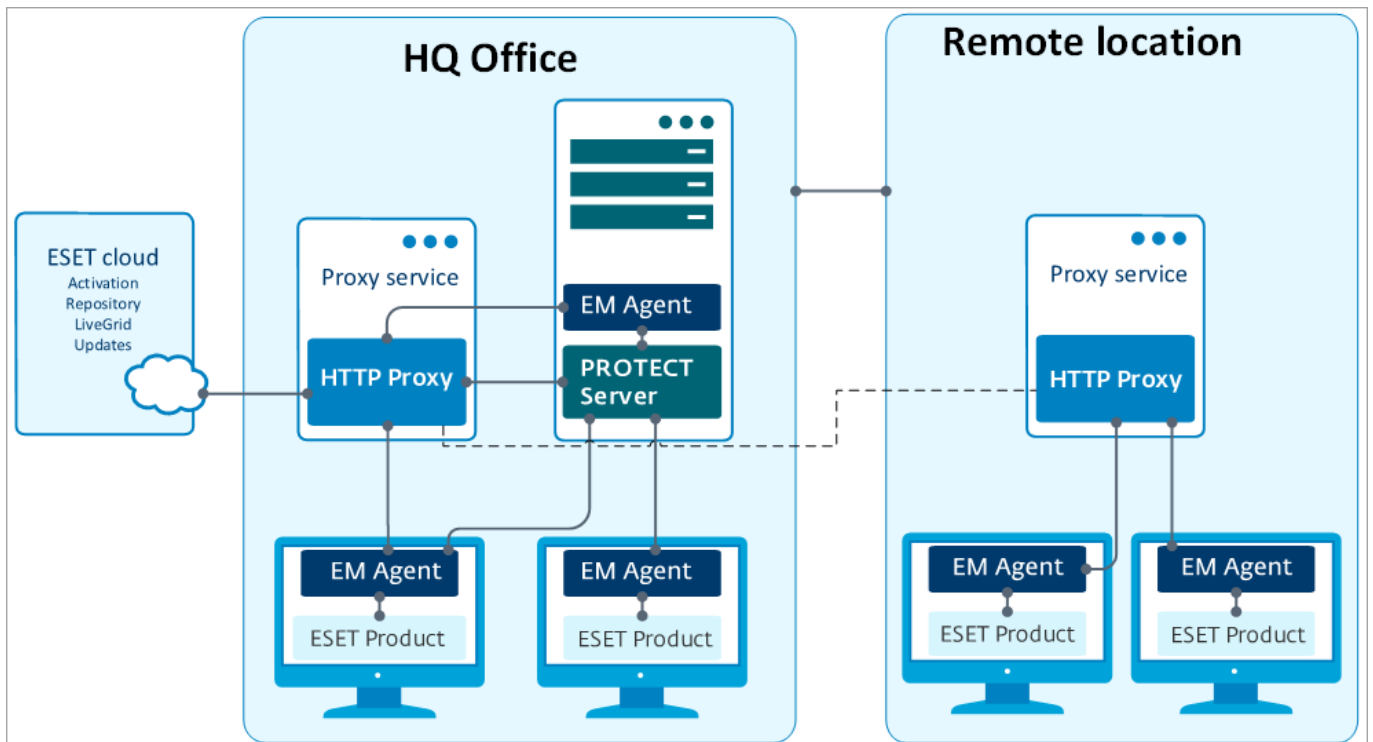
Примітка

[Чим відрізняються різні проксі-сервери?](#)



Увага

Ви можете використовувати [ланцюжок проксі-серверів](#), щоб додати ще один проксі-сервер до віддаленого сховища. Зауважте, що ESET PROTECT не може використовувати такі ланцюжки, якщо проксі-сервери вимагають автентифікації. Ви можете використовувати власний прозорий проксі-сервер, однак він може потребувати додаткового налаштування.



Примітка

Для автономних оновлень ядра виявлення використовуйте інструмент «Дзеркало» (доступний для [Windows](#) і [Linux](#)) замість проксі-сервера HTTP Apache.

Відмінності між проксі-сервером Apache HTTP, інструментом «Дзеркало» та прямим підключенням

Продукти ESET отримують оновлення ядра виявлення та модуля програми, а також обмінюються даними [ESET LiveGrid®](#) (див. [Таблицю](#) нижче) і відомостями про ліцензії.

ESET PROTECT завантажує з репозиторія останні версії продуктів для розповсюдження на клієнтські комп'ютери. Після розповсюдження продукти готові до розгортання на цільовому комп'ютері.

Після інсталяції продукту ESET для захисту його потрібно активувати, тобто продукт повинен перевірити інформацію про вашу ліцензію на сервері ліцензій. Активовані ядро виявлення та модуль програми регулярно оновлюються.

[Система раннього попередження ESET LiveGrid®](#) дає ESET змогу негайно дізнаватися про нові проникнення, щоб надійно захищати своїх клієнтів. Система дає змогу надсилати нові виявлені об'єкти на аналіз і обробку до дослідницької лабораторії ESET.

Оновлення модулів продукту споживають більшість мережевого трафіку. Загалом продукт ESET для захисту завантажує приблизно 23,9 МБ оновлень модулів за місяць.

Дані [ESET LiveGrid®](#) (приблизно 22,3 МБ) і файл з оновленою версією продукту (до 11 КБ) – це єдині файли, що розповсюджуються, які не можна кешувати.

Існує два види оновлень: *оновлення рівнів* і *нанооновлення*. [Щоб дізнатися більше, перегляньте статтю бази знань про види оновлень.](#)

Зменшити навантаження на мережу під час розподілу оновлень у комп'ютерній мережі можна двома способами: за допомогою [проксі-сервера HTTP Apache](#) або інструменту «Дзеркало» (доступний для [Windows](#) і [Linux](#)).



Примітка

Щоб налаштувати ланцюг інструмента «Дзеркало», прочитайте [цю статтю бази знань](#) (налаштування інструмента «Дзеркало» для завантаження оновлень з іншого інструмента «Дзеркало»).

Типи підключення продуктів ESET

Тип підключення	Частота підключення	Споживання мережевого трафіка	Передача даних через проксі-сервер	Кешування за допомогою проксі-сервера ¹	Інструмент «Дзеркало» ²	Варіант з автономним середовищем
Розгортання агента (з репозиторія за допомогою Push-сповіщень/Live Installer)	Один раз	Приблизно 50 МБ на клієнта	ТАК	ТАК ³	НІ	ТАК (GPO / SCCM, змінений Live Installer) ⁴
Інсталяція на робочій станції (інсталяція програмного забезпечення з репозиторія)	Один раз	Приблизно 100 МБ на клієнта	ТАК	ТАК ³	НІ	ТАК (GPO / SCCM, інсталяція за допомогою URL-адреси пакета) ⁴
Оновлення модулю ядра виявлення/модулю програми	Понад 6 разів на день	23,9 МБ на місяць ⁵	ТАК	ТАК	ТАК	ТАК (Mirror Tool в автономному режимі та користувацький сервер HTTP) ⁶
Файл з версією для оновлення update.ver	Прибл. 8 разів на день	2,6 МБ на місяць ⁷	ТАК	НІ	-	-

Тип підключення	Частота підключення	Споживання мережевого трафіка	Передача даних через проксі-сервер	Кешування за допомогою проксі-сервера ¹	Інструмент «Дзеркало» ²	Варіант з автономним середовищем
Активіація/перевірка ліцензії	4 рази на день	незначне	ТАК	НІ	НІ	ТАК (автономні файли, створені в ESET Business Account) ⁸
ESET LiveGrid® (репутація в хмарі)	На ходу	11 МБ на місяць	ТАК	НІ	НІ	НІ

1. Особливості/переваги кешування за допомогою проксі-сервера описано в розділі [Коли починати користуватися проксі-сервером Apache HTTP?](#)
2. Особливості використання інструмента «Дзеркало» описано в розділі [Коли починати користуватись інструментом «Дзеркало»?](#)
3. Під час інсталяції/оновлення продуктів рекомендується спочатку розгорнути один агент (по одному на кожну версію, що використовується) і робочу станцію, щоб здійснити кешування інсталятора.
4. У разі розгортання агента ESET Management у великій мережі див. розділ [Розгортання агента за допомогою GPO та SCCM](#).
5. Якщо ви використовуєте застарілий пакет інсталяції, розмір першого оновлення ядра виявлення може бути більшим, ніж зазвичай, оскільки необхідно буде завантажити останні оновлення ядра виявлення та модулів. Рекомендується спочатку інсталювати й оновити один клієнт, щоб здійснити кешування необхідних оновлень ядра виявлення та модулів програм.
6. Без підключення до Інтернету Mirror Tool не може завантажити оновлення для ядра виявлення. Ви можете використати Apache Tomcat як сервер HTTP для завантаження оновлень у каталог, доступний для інструменту «Дзеркало» (доступний для [Windows](#) і [Linux](#)).
7. Для перевірки наявності оновлень ядра виявлення завантажується й аналізується файл *update.ver*. За замовчуванням планувальник продуктів ESET для робочих станцій перевіряє наявність оновлень щогодини. Припускається, що робоча станція клієнта працює протягом 8 годин на день. Розмір файлу *update.ver* становить приблизно 11 КБ.
8. [Щоб завантажити файли автономної ліцензії, використовуйте обліковий запис власника ліцензії або адміністратора безпеки.](#)



Примітка

Функція кешування оновлень для версій продуктів 4 та 5 за допомогою проксі-сервера Apache HTTP не підтримується. Для розповсюдження оновлень для цих продуктів використовуйте інструмент «Дзеркало».

Коли починати користуватися проксі-сервером Apache HTTP

Згідно з результатами наших практичних тестів, ми рекомендуємо розгортати проксі-сервер Apache HTTP, якщо у вашій мережі понад 37 комп'ютерів включно.



Увага

Для ефективного кешування вкрай важливо, щоб на проксі-сервері HTTP було задано правильну дату й правильний час. Різниця в кілька хвилин погіршить ефективність механізму кешування: може завантажуватися більше файлів, ніж потрібно.

Аналіз пропускну здатності мережі, що використовувалася виключно оновленнями в тестовій мережі з 1000 комп'ютерів, де виконувалося кілька інсталяцій і видалень, показав такі результати:

- один комп'ютер завантажує в середньому 23,9 МБ на місяць [оновлень](#) при прямому підключенні до Інтернету (проксі-сервер Apache HTTP не використовується);
- при використанні проксі-сервера Apache HTTP завантаження для всієї мережі загалом складає 900 МБ на місяць.

Нижче наведено звичайне порівняння завантажених даних оновлень на місяць через пряме підключення до Інтернету або проксі-сервер Apache HTTP в мережі комп'ютерів.

Кількість ПК в корпоративній мережі	25	36	50	100	500	1.000
Пряме підключення до Інтернету (МБ/місяць)	375	900	1.250	2.500	12.500	25.000
Проксі-сервер Apache HTTP (МБ/місяць)	30	50	60	150	600	900

Коли починати користуватись Mirror Tool?

Якщо у вас автономне середовище (тобто комп'ютери у вашій мережі не підключаються до Інтернету протягом тривалого періоду (місяців, року)), інструмент «Дзеркало» (доступний для [Windows](#) і [Linux](#)) — єдиний спосіб розповсюдити оновлення модулів продукту, оскільки він завантажує всі доступні оновлення рівнів і нанооновлення після кожного відповідного запиту (якщо оновлення доступне).



Примітка

Щоб налаштувати ланцюг інструмента «Дзеркало», прочитайте [цю статтю бази знань](#) (налаштування інструмента «Дзеркало» для завантаження оновлень з іншого інструмента «Дзеркало»).

Основна відмінність між проксі-сервером Apache HTTP й інструментом «Дзеркало» в тому, що проксі-сервер Apache HTTP завантажує лише відсутні оновлення (наприклад, нанооновлення 3), коли Mirror Tool завантажує всі доступні [оновлення рівнів і нанооновлення](#) (чи лише оновлення рівнів, якщо таке вказано) незалежно від того, яке оновлення відсутнє в модулі продукту.



Примітка

Потокові оновлення недоступні для інструменту «Дзеркало». У всіх випадках, коли це можливо, рекомендуємо використовувати для оновлення проксі-сервер HTTP замість інструменту «Дзеркало». Навіть якщо на комп'ютері немає зв'язку з мережею, але є доступ до іншого комп'ютера, який підключений до Інтернету і може виконувати проксі-сервер HTTP для кешування файлів оновлення, виберіть цей параметр.

У вищезгаданій мережі з 1000 комп'ютерів ми протестували інструмент «Дзеркало» замість [проксі-сервера Apache HTTP](#). За результатами аналізу за місяць було завантажено 5500 МБ оновлень. Після додавання інших комп'ютерів у мережу розмір завантажених оновлень не збільшився. Це все ще досить велике зменшення навантаження порівняно з конфігурацією, де клієнти напряму підключаються до Інтернету, однак покращення продуктивності не настільки значне, як при використанні проксі-сервера HTTP.

Кількість ПК в корпоративній мережі	25	36	50	100	500	1.000
Пряме підключення до Інтернету (МБ/місяць)	375	900	1.250	2.500	12.500	25.000
Інструмент «Дзеркало» (МБ/місяць)	5.500	5.500	5.500	5.500	5.500	5.500



Примітка

Навіть якщо б у мережі було понад 1000 комп'ютерів, використання пропускної здатності для оновлень не збільшилося би значно при застосуванні проксі-сервера Apache HTTP чи інструмента «Дзеркало».

Системні вимоги та налаштування розмірів

Щоб інсталиувати ESET PROTECT і працювати з цим продуктом, потрібно виконати попередні вимоги до [обладнання](#), [бази даних](#), [мережі](#) та [програмного забезпечення](#).

Підтримувані операційні системи

У розділах нижче описано, які версії операційних систем [Windows](#), [Linux](#), [macOS](#) і [мобільних телефонів](#) підтримують конкретні компоненти ESET PROTECT.

Windows

У таблиці нижче вказано підтримувані операційні системи Windows для кожного компонента ESET PROTECT.

Операційна система	Сервер	Агент	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1 з інстальованим оновленням KB4474419 або KB4490628		✓	✓	
Windows Server 2008 R2 CORE x64 з інстальованим оновленням KB4474419 або KB4490628		✓	✓	
Windows Server 2008 SP2 (x86 і x64) з інстальованими оновленнями KB4493730 і KB4039648		✓	✓	
Windows Storage Server 2008 R2 x64 з інстальованим оновленням KB4474419 або KB4490628		✓	✓	
Windows Server 2012 x64	✓	✓	✓	✓
Windows Server 2012 CORE x64	✓	✓	✓	✓
Windows Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2012 R2 CORE x64	✓	✓	✓	✓
Windows Storage Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2016 x64	✓	✓	✓	✓
Windows Storage Server 2016 x64	✓	✓	✓	✓
Windows Server 2019 x64	✓	✓	✓	✓
Microsoft SBS 2008 x64 SP2 з інстальованими оновленнями KB4493730 і KB4039648		✓	✓	✓
Microsoft SBS 2011 Standard x64	✓	✓	✓	✓
Microsoft SBS 2011 Essentials x64	✓	✓	✓	✓
Операційна система	Сервер	Агент	RD Sensor	MDM
Windows 7 x86 SP1 з останніми оновленнями Windows (принаймні KB4474419 і KB4490628)		✓	✓	
Windows 7 x64 SP1 з останніми оновленнями Windows (принаймні KB4474419 і KB4490628)		✓	✓	
Windows 8 x86		✓	✓	
Windows 8 x64	✓*	✓	✓	✓*
Windows 8.1 x86		✓	✓	
Windows 8.1 x64	✓*	✓	✓	✓*
Windows 10 x86		✓	✓	
Windows 10 x64 (усі офіційні випуски)	✓*	✓	✓	✓*

* Інсталяція компонентів ESET PROTECT в ОС клієнта може суперечити політиці ліцензування корпорації Майкрософт. Перевірте умови цієї політики або зверніться за допомогою до постачальника програмного забезпечення. У середовищах малого/середнього бізнесу чи невеликих мережевих середовищах рекомендуємо інстальувати ESET PROTECT для Linux або [віртуальний пристрій](#), де це можливо.



Увага

- **Старіші системи MS Windows:** у вас завжди має бути інстальовано останню версію пакета оновлень, особливо в старіших системах, таких як Server 2003, 2008, Windows XP та Windows Vista.
- Ми не підтримуємо нелегальні чи піратські операційні системи.
- З 24 березня 2020 року ESET більше не підтримуватиме (офіційно) продукти ESET PROTECT (Server і MDM), інстальовані в таких операційних системах Microsoft Windows: Windows 7, Windows Server 2008 (усі версії). Технічна підтримка для цих продуктів не надаватиметься.



Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інстальувати один із підтримуваних випусків Java.



Примітка

[VMware Player](#) можна інстальувати в операційній системі для настільних комп'ютерів і розгорнути [віртуальний пристрій ESET PROTECT](#). Це дасть змогу запускати ESET PROTECT в несерверній ОС без використання гіпервізора ESXi.

Linux

У таблиці нижче перелічено підтримувані операційні системи Linux для кожного компонента ESET PROTECT.

Операційна система	Сервер	Агент	RD Sensor	MDM
Ubuntu 16.04.1 LTS x86 Desktop		✓	✓	
Ubuntu 16.04.1 LTS x86 Server		✓	✓	
Ubuntu 16.04.1 LTS x64 Desktop	✓	✓	✓	✓
Ubuntu 16.04.1 LTS x64 Server	✓	✓	✓	✓
Ubuntu 18.04.1 LTS x64 Desktop	✓	✓	✓	✓
Ubuntu 18.04.1 LTS x64 Server	✓	✓	✓	✓
Ubuntu 20.04 LTS x64	✓	✓	✓	✓
RHEL Server 7 x86		✓	✓	
RHEL Server 7 x64	✓	✓	✓	✓
RHEL Server 8 x64	✓	✓		✓
CentOS 7 x86		✓	✓	
CentOS 7 x64	✓	✓	✓	✓
CentOS 8 x64	✓	✓		✓
SLED 15 x86		✓	✓	
SLED 15 x64	✓	✓	✓	✓
SLES 11 x86		✓	✓	
SLES 11 x64	✓	✓	✓	✓
SLES 12 x86		✓	✓	
SLES 12 x64	✓	✓	✓	✓
SLES 15 x86		✓	✓	
SLES 15 x64	✓	✓	✓	✓
OpenSUSE Leap 15.2 x64	✓	✓	✓	✓
Debian 9 x86		✓	✓	

Debian 9 x64	✓	✓	✓	✓
Debian 10 x64	✓	✓	✓	✓
Fedora 31 x64		✓		
Fedora 32 x64		✓		

macOS

Операційна система	Агент
macOS 10.12 Sierra	✓
macOS 10.13 High Sierra	✓
macOS 10.14 Mojave	✓
macOS 10.15 Catalina	✓
macOS 11.0 Big Sur	✓



Примітка

macOS підтримується лише як клієнт. [Агент ESET Management](#) і [продукти ESET для macOS](#) можна інсталиувати в macOS, однак не можна інсталиувати сервер ESET PROTECT.

Мобільний пристрій

Операційна система	EESA	Власник пристрою EESA	MDM iOS	MDM iOS DEP
Android v5.x+	✓			
Android v6.x+	✓			
Android v7.x+	✓	✓		
Android v8.x+	✓	✓		
Android v9.0	✓	✓		
Android v10.0	✓	✓		
Android v11	✓	✓		
iOS 9.x+			✓	✓*
iOS 10.x+			✓	✓*
iOS 11.x+			✓	✓*
iOS 12.0.x			✓	✓*
iOS 13.x+			✓	✓
iOS 14.x+			✓	✓
iPadOS 13.x+			✓	✓
iPadOS 14.x+			✓	✓

* Програма iOS DEP доступна лише у [вибраних країнах](#).



Увага

Рекомендуємо оновити ОС мобільного пристрою до останньої версії, щоб і надалі отримувати важливі виправлення системи безпеки.

[-] [Вимоги до iOS 10.3 і новіших версій](#)

Після виходу iOS 10.3 центр сертифікації, інстальований як частина профілю реєстрації, може не отримати статус надійного автоматично. Щоб вирішити цю проблему, виконайте вказані нижче дії.

а) Скористайтеся сертифікатом, що надав [видавець сертифіката, якому довіряє Apple](#).

б) Призначте надійність сертифіката вручну перед реєстрацією. Це означає, що перед реєстрацією потрібно інсталиувати кореневий ЦС вручну на мобільному пристрої й [увімкнути повну довіру](#) для встановленого сертифіката.

☐ [Вимоги до iOS 12](#)

Перегляньте вимоги до iOS 10.3 і новіших версій.

- Потрібно використовувати підключення **TLS 1.2** або **новіших версій**.
- Підключення має використовувати **симетричне шифрування AES-256** або **AES-128**. Комплект шифрів установленого підключення TLS має підтримувати **повну безпеку пересилання (PFS)** через **обмін ефемерними ключами за протоколом Діффі-Геллмана на еліптичних кривих (ECDHE)**.

Крім цього, це має бути комплект шифрів із цього переліку:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

- Має бути підпис **ключем RSA** довжиною **щонайменше 2048 біт**. Для хешування сертифіката має використовуватись алгоритм **SHA-2 з довжиною дайджеста** (іноді називається «відбитком») не менше 256 (тобто **SHA-256** або **вище**). Ви можете створити сертифікат за цими вимогами в ESET PROTECT, коли ввімкнено параметр [Додаткова безпека](#).

- Сертифікати мають містити **повний ланцюг сертифікатів, зокрема кореневий центр сертифікації**. Кореневий ЦС, включений у сертифікат, використовується для встановлення довіри з пристроями й інсталюється як частина профілю реєстрації MDM.

☐ [Вимоги до iOS 13](#)

- Щоб керувати мобільними пристроями з iOS 13, потрібно відповідати новим [вимогам](#) Apple до сертифіката обміну даними (MDM HTTPS). Сертифікати, видані до 1 липня 2019 року, теж повинні відповідати цим вимогам.
- Сертифікат HTTPS, підписаний ЦС ESMC, не відповідає цим вимогам.
- **Рекомендуємо не оновлювати мобільні пристрої до iOS 13, доки не виконаєте [вимоги](#) Apple до сертифіката обміну даними. В іншому разі пристрої перестануть підключатися до ESET PROTECT MDM.**
- Якщо ви вже інстальювали оновлення без належного сертифіката й пристрої перестали підключатися до ESET PROTECT MDM, спершу потрібно змінити поточний сертифікат HTTPS, який використовувався для обміну даними з пристроями iOS, на сертифікат, який відповідає [вимогам](#) Apple до сертифіката обміну даними (MDM HTTPS), а потім повторно зареєструвати пристрої iOS.
- Якщо ви ще не оновилися до iOS 13, переконайтеся, що поточний сертифікат MDM HTTPS, який використовується для обміну даними з пристроями iOS, відповідає [вимогам](#) Apple до сертифіката обміну даними (MDM HTTPS). Якщо відповідає, можете оновити пристрої до iOS 13. В іншому разі змініть поточний сертифікат MDM HTTPS на сертифікат HTTPS, який відповідає [вимогам](#) Apple до сертифіката обміну даними (MDM HTTPS), а потім оновіть пристрої до iOS 13.

Підтримувані середовища підготовки настільних комп'ютерів

Підготовка настільних комп'ютерів полегшує керування пристроями й пришвидшує передачу цих комп'ютерів кінцевим користувачам.

Підготовані настільні комп'ютери зазвичай бувають фізичні або віртуальні. Для віртуалізованих середовищ, що використовують ОС, яка передається потоково (служби підготовки Citrix), перегляньте список [підтримуваних гіпервізорів](#).

ESET PROTECT [підтримка](#):

- системи з непостійними дисками;
- середовища VDI;
- ідентифікацію клонованих комп'ютерів.

Підтримувані гіпервізори

- Citrix XenServer
- Microsoft Hyper-V
- VMware vSphere
- VMware ESXi
- VMware Workstation
- VMware View
- Oracle VirtualBox

Підтримувані розширення гіпервізора

- Citrix VDI-in-a-box
- Citrix XenDesktop

Інструменти (застосовуються до віртуальних і фізичних комп'ютерів)

- Microsoft SCCM
- Диспетчер сервера Windows Server 2012/2016/2019
- Центр адміністрування Windows

Обладнання та налаштування розмірів інфраструктури

Характеристики комп'ютера із сервером ESET PROTECT повинні відповідати рекомендаціям щодо апаратного забезпечення з таблиці нижче.

Екземпляр SQL Server може надавати серверу ESET PROTECT доступ до власних ресурсів для забезпечення максимальної продуктивності та мінімізації затримок. Щоб збільшити продуктивність ESET PROTECT, запускайте сервер ESET PROTECT і сервер бази даних на одному комп'ютері.

Кількість клієнтів	Сервер ESET PROTECT + сервер бази даних SQL		
	Ядра ЦП	ОЗП (ГБ)	Диск IOPS ²
До 1000	4	4	Одиночний
5.000	8	8	Окремий
10,000 ³	8	16	
50.000	16	32	
100.000	16	32+	20.000

Рекомендації щодо використання диска

- ¹ одиночний/окремий диск: Якщо до системи входить понад 10 000 клієнтів, рекомендується інсталиувати [базу даних](#) на окремий диск.
ОПродуктивність сервера SQL зростає, якщо розмістити базу даних і файли журналу транзакцій на окремих дисках (бажано використовувати окремі фізичні накопичувачі SSD).
ОВикористовуйте SSD корпоративного класу з високим значенням IOPS f або іншу високопродуктивну систему.
- Мінімальне необхідне значення: 2 IOPS (операцій вводу/виводу на секунду).
- З Див. [зразок сценарію](#) для середовища з 10 000 клієнтами.
- Рекомендується забезпечити приблизно 0,2 IOPS на кожний підключений клієнт (не менше 500 IOPS загалом).
- Ви можете перевірити значення IOPS свого диска, запустивши наступну команду в інструменті [diskspd](#):

Кількість клієнтів	Команда
До 5000	diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat
Понад 5000	diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat

- Використовуйте твердотільні накопичувачі (SSD), оскільки вони працюють набагато швидше, ніж

звичайні.

- Ємності в 100 ГБ достатньо для будь-якої кількості клієнтів. Якщо ви часто створюєте резервні копії бази даних, використовуйте накопичувач більшої ємності.
- Не використовуйте мережеві накопичувачі, оскільки їхня продуктивність уповільнить роботу ESET PROTECT.



Увага

Продуктивність ESET PROTECT дуже сильно залежить від типу накопичувача, що використовується.

Рекомендації щодо розгортання

Практичні поради з розгортання ESET PROTECT

Кількість клієнтів	До 1000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	100.000+
Сервер ESET PROTECT і сервер баз даних інстальовано на один комп'ютер	✓	✓	✓	x	x	x
Використання MS SQL Express	✓	✓	x	x	x	x
Використання MS SQL	✓	✓	✓	✓	✓	✓
Використання MySQL	✓	✓	✓	x	x	x
Використання віртуального пристрою ESET PROTECT	✓	✓	Не рекомендовано	x	x	x
Використання сервера на віртуальній машині	✓	✓	✓	Необов'язкова	x	x
Рекомендований інтервал підключення (під час розгортання)	60 секунд	5 хвилин	10 хвилин	15 хвилин	20 хвилин	25 хвилин
Рекомендований інтервал підключення (після розгортання, під час звичайного використання)	10 хвилин	10 хвилин	20 хвилин	30 хвилин	40 хвилин	60 хвилин

Інтервал підключення

Сервер ESET PROTECT підключено до агентів ESET Management шляхом постійного підключення. Незважаючи на це, передача даних відбувається лише один раз протягом інтервалу підключення. Наприклад, якщо інтервал реплікації на 5000 клієнтів становить вісім хвилин, відбувається 5000 передач даних за 480 секунд, тобто 10,4 за секунду. Обов'язково налаштуйте відповідний [інтервал підключення клієнта](#). Загальна кількість підключень між агентом і сервером не має перевищувати 1000 на секунду навіть на високопродуктивному обладнанні.

Якщо сервер буде перевантажено або атаковано зловмисним програмним забезпеченням (наприклад, ми підключили 20 000 клієнтів до сервера, що може обслуговувати лише 10 000 клієнтів з інтервалом у 10 хвилин), він не буде встановлювати зв'язок із деякими підключеними клієнтами. Не підключені клієнти спробують підключитися до сервера ESET PROTECT пізніше.

Єдиний сервер (малий бізнес)

Для керування невеликими мережами (до 1000 клієнтів) використовуйте один комп'ютер із сервером ESET PROTECT та всіма компонентами ESET PROTECT. У середовищах малого/середнього бізнесу чи невеликих мережевих середовищах рекомендуємо інстальувати ESET PROTECT для Linux або [віртуальний пристрій](#), де це можливо.

Віддалені офіси з проксі-серверами

Якщо клієнтські машини не мають можливості напряму підключатися до сервера ESET PROTECT, використовуйте [проксі-сервер](#) для пересилання даних від продуктів ESET. Проксі-сервер HTTP не збирає дані та не обмежує трафік під час реплікації.

Висока доступність (корпоративні рішення)

У разі керування корпоративним середовищем (понад 10 000 клієнтів) враховуйте наступне:

- [RD Sensor](#) допомагає знаходити нові комп'ютери у вашій мережі.
- Сервер ESET PROTECT можна налаштувати на відмовостійкому кластері.
- Налаштуйте свій [проксі-сервер HTTP](#) з урахуванням великої кількості клієнтів.

Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи

За замовчуванням ESET PROTECT Web Console, яку інстальовано з використанням універсального інсталятора для Windows, резервує оперативну пам'ять в обсязі 1024 МБ для Apache Tomcat.

Конфігурацію Web Console за замовчуванням можна змінити в залежності від інфраструктури:

- У корпоративному середовищі конфігурація веб-консолі за замовчуванням може бути нестабільною під час роботи з великою кількістю об'єктів. Змініть налаштування Tomcat, щоб уникнути нестачі пам'яті. Перш ніж вносити зміни, переконайтеся, що в системі достатньо оперативної пам'яті (не менше 16 ГБ).
- Якщо ваша система має низьку продуктивність через обмежену потужність апаратних ресурсів, можна зменшити використання пам'яті Tomcat.



Примітка

Указані нижче значення обсягу оперативної пам'яті наведено лише для довідки. Параметри пам'яті Tomcat можна налаштувати залежно від апаратних ресурсів.

Windows

1. Відкрийте файл tomcat9w.exe або запустіть програму Configure Tomcat.
2. Відкрийте вкладку **Java**.
3. Змініть використання пам'яті:
 - a. Збільшити (для корпоративних рішень): Змініть значення параметра **Початковий пул пам'яті** на 2048 МБ, а **Максимальний пул пам'яті** – на 16 384 МБ.
 - b. Зменшити (для систем із низькою продуктивністю): Змініть значення параметра **Початковий пул пам'яті** на 256 МБ, а **Максимальний пул пам'яті** – на 2 048 МБ.
4. Перезавантаження службу Tomcat.

Linux і віртуальний пристрій ESET PROTECT

1. Відкрийте термінал із правами користувача root або за допомогою sudo.
2. Відкрийте файл:
 - a. Віртуальний пристрій ESET PROTECT / CentOS: /etc/sysconfig/tomcat
 - b. Debian: /etc/default/tomcat9
3. Додайте у файл такий рядок:
 - a. Збільшити використання пам'яті (для корпоративних рішень): JAVA_OPTS=" -Xms2048m -Xmx16384m"

b.Зменшити використання пам'яті (для систем із низькою продуктивністю): JAVA_OPTS=" -Xms256m -Xmx2048m"

4. Збережіть файл і перезавантажте службу Tomcat.
service tomcat restart

Розгортання для 10 000 клієнтів

Нижче наведено результати роботи для віртуального середовища, в якому протягом року працюють 10 000 клієнтів.

Конфігурація сервера Hypervisor

Компонент	Значення
VMware	ESXi 6.7 Update 2 й новіших версій (VM версії 15)
Гіпервізор	VMware ESXi, 6.7.0
Логічні процесори	112
Тип процесора	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz



Тестове виконання на виділених машинах

База даних і ESET PROTECT виконуються на окремих віртуальних машинах з ідентичними конфігураціями обладнання.

Програмне забезпечення, яке використовується на віртуальних машинах

ESET PROTECT:

- OS: Microsoft Windows Server 2016 Standard (64-bit)

База даних:

- Database server: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- OS: Microsoft Windows Server 2016 Standard (64-bit)

Опис середовища ESET PROTECT

- 10 000 клієнтів, що підключаються
- Приблизно 2 000 динамічних груп і 2 000 шаблонів для динамічних груп
- Приблизно 255 статичних груп
- 20 користувачів
- 15-хвилинний інтервал підключення для агентів ESET Management
- Після роботи середовища протягом одного року розмір бази даних складає 15 ГБ.

Кількість ЦП	ОЗП (ГБ)	Ефективність
8	64	Висока
4	32	Звичайна
2	16	Низька
2	8	Дуже низька (не рекомендовано)

База даних

Укажіть сервер бази даних і з'єднувач, який слід використовувати під час інсталяції сервера ESET PROTECT. Ви можете використовувати наявний сервер бази даних, що працює у вашому середовищі; однак він має відповідати наведеним нижче вимогам.



Примітка

ESET PROTECT 8.0 [Універсальний інсталятор](#) за замовчуванням інсталює Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інсталюватиметься за замовчуванням.

Підтримувані сервери баз даних і з'єднувачі з базою даних

ESET PROTECT підтримує два типи серверів баз даних: Microsoft SQL Server і MySQL.



Попередження

MariaDB не підтримується ESET PROTECT. MariaDB — це база даних, що за замовчуванням використовується в більшості сучасних середовищ Linux та інсталюється разом із MySQL.

Підтримуваний сервер бази даних	Підтримувані версії бази даних	Підтримувані з'єднувачі бази даних
Microsoft SQL Server	<ul style="list-style-type: none"> Випуски Express і випуски, відмінні від Express 2012, 2014, 2016, 2017, 2019 	<ul style="list-style-type: none"> Сервер SQL SQL Server Native Client 10.0 Драйвер ODBC для SQL Server 11, 13, 17
MySQL	<ul style="list-style-type: none"> 5.6 5.7 8.0 	Версії драйвера ODBC для MySQL: <ul style="list-style-type: none"> 5.1, 5.2 5.3.0-5.3.10 8.0.16, 8.0.17



Попередження

Указані нижче версії драйвера ODBC для MySQL не підтримуються:

- 5.3.11 і новіших версій (5.3.x)
- 8.0.0-8.0.15
- 8.0.18 і більш пізніх версій

Вимоги до апаратного забезпечення сервера бази даних

Див. інструкції з налаштування [обладнання](#) та розмірів.

Рекомендації в роботі

Для забезпечення найвищої продуктивності рекомендується використовувати останню підтримувану версію Microsoft SQL Server як базу даних ESET PROTECT. Хоча ESET PROTECT підтримує MySQL, використання MySQL може негативно вплинути на продуктивність системи під час обробки великих обсягів даних, зокрема панелі інструментів, виявлені об'єкти та клієнтів. Те саме обладнання з Microsoft SQL Server здатне обробляти значно більшу кількість клієнтів.

Ви можете інсталювати сервер бази даних SQL на:

- той самий комп'ютер, на якому інсталювано сервер ESET PROTECT, окремий диск на тому самому сервері,
- спеціальний сервер для сервера бази даних SQL.

Якщо кількість клієнтів перевищує 10 000, рекомендується використовувати виділені комп'ютери із зарезервованими ресурсами.

База даних	Клієнт SMB	Корпоративний клієнт	Обмеження щодо клієнтів	Windows	Linux
MS SQL Express	✓	(необов'язково)	5.000	✓	
MS SQL Server	✓	✓	Немає	✓	

База даних	Клієнт SMB	Корпоративний клієнт	Обмеження щодо клієнтів	Windows	Linux
MySQL	✓	✓	10.000	✓	✓

Додаткова інформація

- ESET PROTECT 8.0 [Універсальний інсталятор](#) за замовчуванням інсталує Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інстальоватиметься за замовчуванням.
- Розмір однієї реляційної бази даних у Microsoft SQL Server Express не може перевищувати 10 ГБ. Не рекомендується використовувати Microsoft SQL Server Express у корпоративних середовищах і великих мережах.
- Рекомендуємо [не інстальювати SQL Server в контролері домену](#) (наприклад, якщо ви використовуєте Windows SBS / Essentials). Рекомендуємо інстальювати ESET PROTECT на іншому сервері або не вибирати компонент SQL Server Express під час інсталяції (щоб запустити базу даних ESET PROTECT, потрібно скористатися наявним сервером SQL Server або MySQL Server).
- Якщо ви бажаєте використовувати спеціальний обліковий запис користувача бази даних, що матиме доступ лише до бази даних ESET PROTECT, перед інсталяцією створіть обліковий запис користувача з певними правами. Докладніші відомості наведено в розділі [Спеціальний обліковий запис користувача бази даних](#). Крім того, вам знадобиться створити порожню базу даних для використання ESET PROTECT.
- Для забезпечення належної роботи ESET PROTECT див. інструкції щодо інсталяції та налаштування [MySQL для Windows](#) і [MySQL для Linux](#).
- [MS SQL Server в Linux](#) не підтримується. Однак ви можете [підключити сервер ESET PROTECT у Linux до MS SQL Server у Windows](#).
- У разі інсталяції ESET PROTECT Server та MS SQL Server [на окремі комп'ютери](#) ви можете [використовувати зашифроване підключення до бази даних](#).
- Сервер **ESET PROTECT не використовує вбудовану функцію резервного копіювання**. Настійно рекомендується [створити резервну копію](#) сервера бази даних, щоб запобігти втраті даних.
- Налаштування кластера баз даних у середовищі Windows підтримується лише для MS SQL Server, а не для MySQL.

Підтримувані версії Apache Tomcat і Java

Apache Tomcat

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT.

ESET PROTECT підтримує Apache Tomcat 9.x (64-розрядна версія). Рекомендуємо використовувати Apache Tomcat 9.0.40 або новішої версії.

ESET PROTECT не підтримує альфа-, бета-версії та версії-кандидати Apache Tomcat.

Java

Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.



Примітка

Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримуванна версія – Java 8) і залишити лише останню версію Java.



Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інстальювати один із підтримуваних випусків Java.

Підтримувані веб-браузери, продукти ESET для захисту та мови

Нижче перераховано операційні системи, які підтримує ESET PROTECT.

- [Windows](#), [Linux](#) і [macOS](#)

Веб-консоль ESET PROTECT можна запускати в указаних нижче веб-браузерах.

Веб-браузер
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera



Примітка

- Щоб покращити взаємодію з веб-консоллю ESET PROTECT, рекомендуємо стежити за оновленням веб-браузерів.
- Якщо ви використовуєте Internet Explorer, веб-консоль ESET PROTECT сповістить вас, що ви використовуєте непідтримуваний веб-браузер.

Останні версії продуктів ESET, якими можна керувати за допомогою ESET PROTECT 8.0

Продукт	Версія продукту
ESET Endpoint Security для Windows	7.x, 8.x
ESET Endpoint Antivirus для Windows	7.x, 8.x
ESET Endpoint Security для macOS	6.8+
ESET Endpoint Antivirus для macOS	6.8+
ESET Endpoint Security для Android	2.x
ESET File Security для Windows Server	7.x
ESET File Security для Microsoft Azure	7.x
ESET Mail Security для Microsoft Exchange Server	7.x
ESET Security для Microsoft SharePoint Server	7.x
ESET Mail Security для IBM Domino Server	7.x
ESET File Security для Linux	7.x, 8.x
ESET Endpoint Antivirus для Linux	7.x, 8.x
ESET Dynamic Threat Defense	
ESET Enterprise Inspector	1.x
ESET Full Disk Encryption для Windows	
ESET Full Disk Encryption для macOS	

Старіші версії продуктів ESET, якими можна керувати за допомогою ESET PROTECT 8.0

Продукт	Версія продукту
ESET Endpoint Security для Windows	6.5+
ESET Endpoint Antivirus для Windows	6.5+
ESET File Security для Microsoft Windows Server	6.5
ESET File Security для Microsoft Azure	6.5
ESET Mail Security для Microsoft Exchange Server	6.5
ESET Mail Security для IBM Lotus Domino	6.5
ESET Security для Microsoft SharePoint Server	6.5
ESET Mail Security для Linux/FreeBSD	4.5.x
ESET File Security для Linux/FreeBSD	4.5.x
ESET Gateway Security для Linux/FreeBSD	4.5.x



Примітка

- ESET PROTECT 8 не керує продуктами захисту ESET, версія яких є старішою за версію, указану в таблиці вище.
- Докладніші відомості про сумісність див. в статті [Політика завершення життєвого циклу для продуктів ESET для бізнесу](#).

Продукти, які підтримують активацію за допомогою передплаченої ліцензії

Продукт ESET	Доступно з версії
ESET Endpoint Antivirus / Security для Windows	7.0
ESET Endpoint Antivirus / Security для macOS	6.8.x
ESET Endpoint Security для Android	2.0.158
ESET Mobile Device Management для Apple iOS	7.0
ESET File Security для Microsoft Windows Server	7.0
ESET Mail Security для Microsoft Exchange	7.0
ESET File Security для Windows Server	7.0
ESET Mail Security для IBM Domino	7.0
ESET Security для Microsoft SharePoint Server	7.0
ESET File Security для Linux	7.0
ESET Endpoint Antivirus для Linux	7.0
ESET Dynamic Threat Defense	
ESET Enterprise Inspector (з ESET Endpoint для Windows 7.3 та новіших версій)	1.5

Підтримувані мови

Мова	Код
Англійська (США)	en-US
Арабська (Єгипет)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Latin)	hr-HR
Чеська (Чеська Республіка)	cs-CZ
Французька (Франція)	fr-FR
Французька (Канада)	fr-CA
Німецька (Німеччина)	de-DE
Грецька (Греція)	el-GR
Угорська (Угорщина)*	hu-HU
Індонезійська (Індонезія)*	id-ID
Італійська (Італія)	it-IT
Японська (Японія)	ja-JP
Корейська (Корея)	ko-KR
Польська (Польща)	pl-PL
Португальська (Бразилія)	pt-BR
Російська (Росія)	ru-RU
Іспанська (Чилі)	es-CL
Іспанська (Іспанія)	es-ES
Словацька (Словаччина)	sk-SK
Турецька (Туреччина)	tr-TR
Українська (Україна)	uk-UA

* Цією мовою доступний лише продукт; онлайн-довідка недоступна.

Мережа

Сервер ESET PROTECT і клієнтські комп'ютери, якими керує ESET PROTECT, повинні бути підключені до Інтернету, щоб мати доступ до репозиторію ESET та серверів активації. Якщо ви не плануєте підключати клієнти безпосередньо до Інтернету, то для з'єднання мережі з Інтернетом можна скористатися проксі-

сервером (не плутати з Apache HTTP Proxy).

Комп'ютери, якими керує ESET PROTECT, і сервер ESET PROTECT мають бути підключені до однієї локальної мережі та мають бути в тому самому домені *Active Directory*. Сервер ESET PROTECT має бути видимий для клієнтських комп'ютерів. Крім цього, потрібно, щоб клієнтські комп'ютери могли обмінюватися даними із сервером ESET PROTECT. Таким чином можна застосовувати віддалене розгортання та функцію сигналу пробудження.

ESET PROTECT для Windows/Linux працює з інтернет-протоколами IPv4 і IPv6. Віртуальний пристрій ESET PROTECT працює лише з IPv4.

Використовувані порти

Якщо в мережі використовується брандмауер, див. список можливих [портів мережевого зв'язку](#), які використовуються, коли у вашій інфраструктурі встановлено продукт ESET PROTECT із його компонентами.

Вплив обміну даними між сервером ESET PROTECT і агентом ESET Management на мережевий трафік

Програми на клієнтських комп'ютерах обмінюються даними із сервером ESET PROTECT не напряму, а через агент ESET Management. Цим рішенням легше керувати й воно має менше вимог до даних, які передаються через мережу. Мережевий трафік залежить від інтервалу підключення до клієнта й типу завдань, які виконують клієнти. Навіть якщо в клієнті не виконуються та не заплановано завдання, агент ESET Management обмінюється даними із сервером ESET PROTECT один раз кожного інтервалу підключення. Кожне підключення створює трафік. Приклади трафіку наведено в таблиці нижче.

Тип дії	Трафік в одному інтервалі підключення
Завдання клієнта: Сканувати без очищення	4 КБ
Завдання клієнта: Оновити модулі	4 КБ
Завдання клієнта: Запит журналу SysInspector	300 КБ
Політика: Антивірус — максимальний захист	26 КБ

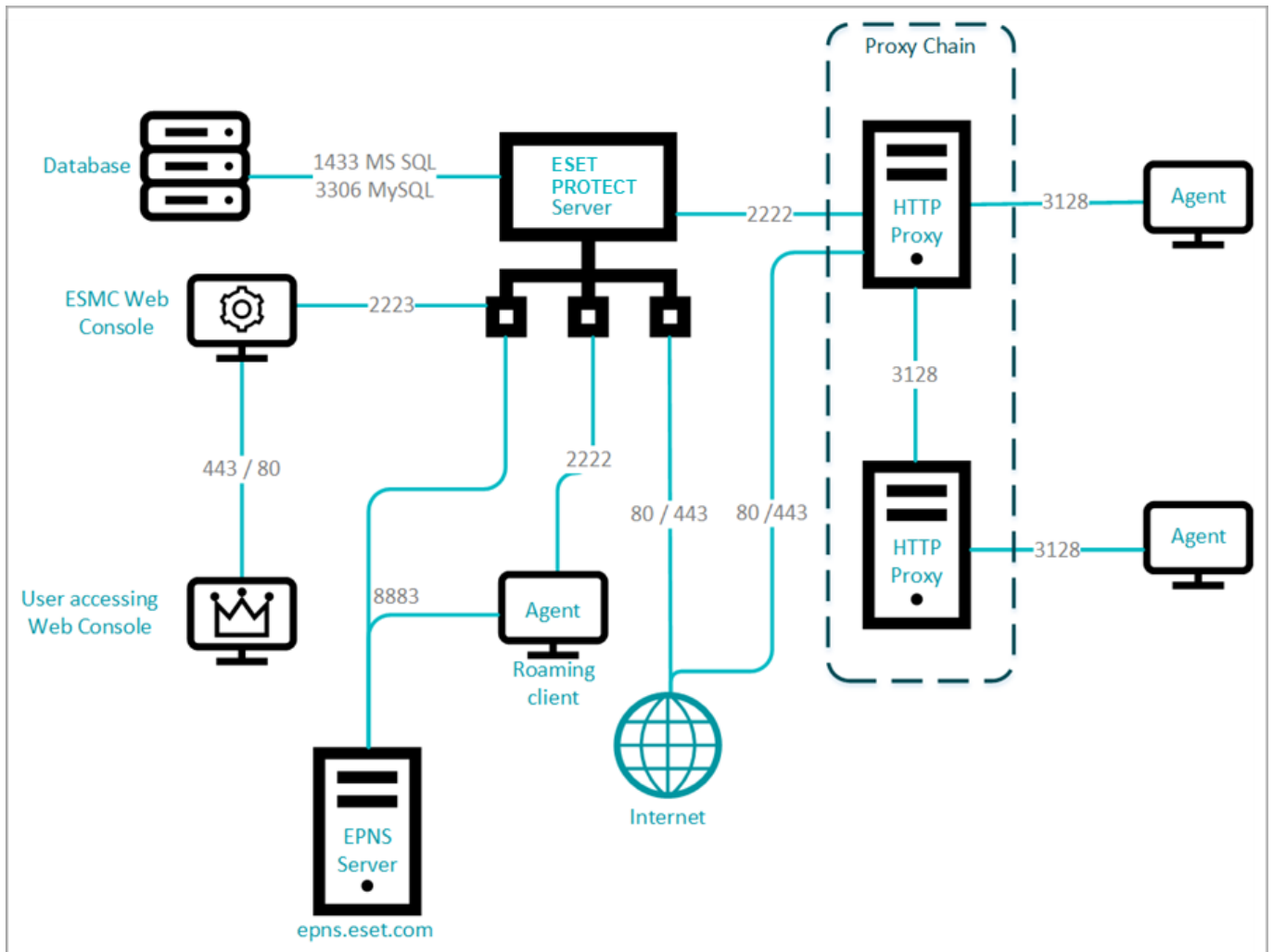
Інтервал реплікації агента ESET Management	Щоденний трафік, створений неактивним агентом ESET Management
1 хвилина	16 МБ
15 хвилин	1 МБ
30 хвилин	0.5 МБ
1 год.	144 КБ
1 день	12 КБ

Щоб вирахувати загальний трафік, створений агентами ESET Management, скористайтеся цією формулою:

*Кількість клієнтів * (щоденний трафік неактивного агента + (трафік для конкретного завдання * повторення завдання на день))*

Використовувані порти

Сервер ESET PROTECT можна інсталиувати на той самий комп'ютер, де є база даних, веб-консоль ESET PROTECT і проксі-сервер Apache HTTP. На діаграмі нижче показано окрему інсталяцію та використовувані порти.



У таблицях нижче наведено перелік усіх можливих портів обміну даних, які використовуються, коли ESET PROTECT і компоненти інсталювано в інфраструктурі. Інші процеси обміну даними виконуються за допомогою рідних процесів операційної системи (наприклад, NetBIOS over TCP/IP).

☐ **Клієнтський комп'ютер (агент ESET Management) або комп'ютер із проксі-сервером Apache HTTP**

Протокол	Порт	Описи
TCP	2222	Обмін даними між агентами ESET Management і сервером ESET PROTECT
TCP	80	Підключення до репозиторію ESET
MQTT	8883, 443	Служба push-сповіщень ESET : сигнали пробудження між сервером ESET PROTECT і агентом ESET Management. Порт відновлення після відмови – 443.
TCP	3128	Обмін даними з проксі-сервером Apache HTTP
TCP	443	Обмін даними з ESET Dynamic Threat Defense (тільки проксі-сервер)

Агент ESET Management: порти, які використовуються для віддаленого розгортання на цільовий комп'ютер з ОС Windows

Протокол	Порт	Описи
TCP	139	Використання спільного ресурсу ADMIN\$
TCP	445	Прямий доступ до спільних ресурсів за допомогою TCP/IP під час віддаленої інсталяції (замість TCP 139)
UDP	137	Визначення назви під час віддаленої інсталяції
UDP	138	Огляд під час віддаленої інсталяції

☐ **Комп'ютер із веб-консоллю ESET PROTECT (якщо це не той самий комп'ютер, на якому встановлено сервер ESET PROTECT)**

Протокол	Порт	Описи
TCP	2223	Обмін даними між веб-консоллю ESET PROTECT і сервером ESET PROTECT (використовується під час інсталяції)
TCP	443/80	Tomcat транслює веб-консоль
TCP	443	RSS-канал для новин служби підтримки: <ul style="list-style-type: none"> • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

[-] **Комп'ютер із сервером ESET PROTECT**

Протокол	Порт	Описи
TCP	2222	Обмін даними між агентом ESET Management і сервером ESET PROTECT
TCP	80	Підключення до репозиторію ESET
MQTT	8883	Служба push-сповіщень ESET : сигнали пробудження між сервером ESET PROTECT і агентом ESET Management
TCP	2223	Обробка імен DNS і резерв MQTT
TCP	3128	Обмін даними з проксі-сервером Apache HTTP
TCP	1433 (MS SQL) 3306 (MySQL)	Підключення до зовнішньої бази даних (лише якщо база даних розташована на іншому комп'ютері).
TCP	389	Синхронізація LDAP. Відкрити цей порт також на контролері AD.
UDP	88	Квитки Kerberos (стосується тільки віртуального пристрою ESET PROTECT)

[-] **Комп'ютер, на якому інстальовано ESET PROTECT MDC**

Протокол	Порт	Описи
TCP	9977 9978	Внутрішній обмін даними між Mobile Device Connector й агентом ESET Management
TCP	9980	Реєстрація мобільних пристроїв
TCP	9981	Обмін даними з мобільним пристроєм
TCP	2195	Надсилання сповіщень у службу push-сповіщень Apple (<i>gateway.push.apple.com</i>) ESMC версій до 7.2.11.1 (включно)
TCP	2196	Служба Apple Feedback (<i>feedback.push.apple.com</i>) ESMC версій до 7.2.11.1 (включно)
HTTPS	2197	• Сповіщення й відповідь Apple Push (<i>api.push.apple.com</i>) ESMC версії 7.2.11.3 та вище
TCP	2222	Обмін даними (реплікація) між агентом ESET Management, MDC та сервером ESET PROTECT
TCP	1433 (MS SQL) 3306 (MySQL)	Підключення до зовнішньої бази даних (лише якщо база даних розташована на іншому комп'ютері)

[-] **Пристрій під керівництвом MDM**

Протокол	Порт	Описи
TCP	9980	Реєстрація мобільних пристроїв
TCP	9981	Обмін даними з мобільним пристроєм
TCP	5223	Зовнішній обмін даними зі службою push-сповіщень Apple (iOS)
TCP	443	<ul style="list-style-type: none"> • Коли пристрої не можуть зв'язатися з точками доступу порту 5223, як резерв використовується лише Wi-Fi (iOS) • Підключення пристрою Android до сервера GCM. • Підключення до порталу ліцензування ESET. • ESET LiveGrid® (Android) (вхідні: https://i1.c.eset.com; вихідні: https://i3.c.eset.com) • Анонімні статистичні дані надсилаються в дослідницьку лабораторію ESET (Android) (https://ts.eset.com) • На пристрої встановлено засіб категоризації програм. Використовується для керування програмою, коли виявлено блокування деяких категорій програми. (Android) (https://play.eset.com) • Надсилання запиту на підтримку за допомогою функції «Запит на підтримку» (Android) (https://suppreq.eset.eu)
TCP	5228 5229 5230	Надсилання сповіщень у Google Cloud Messaging (Android)* Надсилання сповіщень у Firebase Cloud Messaging (Android)*
TCP	80	<ul style="list-style-type: none"> • Оновлення модулів (Android) (http://update.eset.com) • Використовується лише у веб-версії. Інформація про останнє оновлення версії програми й завантаження нової версії. (Android) (http://go.eset.eu)

* Служба Google Cloud Messaging (GCM) більше не підтримується й буде видалена 11 квітня 2019 року. Її замінила служба Firebase Cloud Messaging (FCM). До цієї дати у версію MDM 7 замість GCM буде включено FCM, і вам потрібно буде лише дозволити обмін даними для служби FCM.

За потреби можна змінити попередньо задані порти 2222 та 2223.



Примітка

- Для належної роботи ESET PROTECT інші програми не мають використовувати вказані вище порти.
- Щоб дозволити обмін даними через зазначені вище порти, обов'язково налаштуйте брандмауер мережі.

Процес інсталяції



Увага

Інструкції щодо оновлення наявної інсталяції ESET PROTECT див. у розділі [Процедури оновлення](#). Посібник з інсталяції описує багато способів інсталяції ESET PROTECT. Як правило, його призначено для корпоративних клієнтів. Див. [Посібник для підприємств малого й середнього бізнесу](#), якщо ви хочете інсталювати ESET PROTECT на платформу Windows, щоб керувати продуктами ESET для робочих станцій на Windows (до 250 продуктів).

Інсталювальники ESET PROTECT доступні в розділі [Завантажити ESET PROTECT](#) на сайті ESET. Для різних способів інсталяції доступні різні формати інсталювальників. За замовчуванням обрано вкладку **Універсальний інсталювальник**. Перейдіть на потрібну вкладку, щоб завантажити віртуальний пристрій або окремий інсталювальник. Доступні наступні файли:

- [Універсальний інсталювальник ESET PROTECT](#) для Windows у форматі ZIP.
- Образ у форматі ISO, що містить усі інсталювальники ESET PROTECT (окрім віртуального пристрою ESET PROTECT).
- Віртуальні пристрої (файли у форматі OVA). Віртуальний пристрій ESET PROTECT призначено для

користувачів, які планують запускати ESET PROTECT у віртуалізованому середовищі або бажають спростити процес інсталяції. Покрокові інструкції див. у повному [Посібнику з розгортання віртуального пристрою ESET PROTECT](#).

- Окремі інсталятори для кожного компонента на платформах [Windows](#) і [Linux](#).

Додаткові способи інсталяції:

- [Інсталяція в Microsoft Azure](#)
- Покрокова [інсталяція з інсталяції для Linux](#)



Увага

Не змінюйте ім'я комп'ютера вашого сервера ESET PROTECT після інсталяції. Для отримання додаткової інформації див. розділ [Змінення IP-адреси чи імені хоста сервера ESET PROTECT](#).

Огляд способів інсталяції



Примітка

Див. також розділ [Обладнання та налаштування розмірів інфраструктури](#).

Щоб дізнатися, який тип інсталяції ESET PROTECT підходить для вашого середовища, перегляньте наступну таблицю з рекомендаціями:

Приклад: Не використовуйте повільне підключення до Інтернету для ESET PROTECT у хмарі.

Приклад: Виберіть універсальний інсталятор, якщо ви працюєте в малому чи середньому бізнесі.

Метод інсталяції	Тип клієнта		Міграція		Середовище інсталяції ESET PROTECT					Підключення до Інтернету		
	SMB	Корпоративне рішення	Так	Ні	Немає сервера	Спеціальний сервер	Спільний сервер	Платформа для віртуалізації	Хмарний сервер	Немає	Добре	Погане
Універсальний інсталятор на сервері з Windows	✓	✓	✓			✓	✓		✓	✓	✓	✓
Універсальний інсталятор на ПК із Windows	✓		✓		✓					✓	✓	✓
Віртуальний пристрій	✓		✓					✓		✓	✓	✓
Віртуальна машина Microsoft Azure	✓			✓					✓		✓	
Компонент Linux		✓	✓			✓	✓		✓	✓	✓	✓
Компонент Windows		✓	✓			✓	✓		✓	✓	✓	✓

Універсальна інсталяція у Windows

Є кілька способів інсталювати ESET PROTECT. Виберіть тип інсталяції, яка найкраще підходить вашим потребам і середовищу. Найпростіший спосіб – скористатись універсальним інсталятором ESET PROTECT. За цим способом можна інсталювати ESET PROTECT і компоненти продукту на одному комп'ютері.

Інсталяція компонентів використовується тоді, коли потрібно інсталювати різні компоненти ESET PROTECT на кількох комп'ютерах. Цей спосіб надає більше можливостей для налаштування інсталяції – можна інсталювати кожен компонент на будь-якому комп'ютері, якщо його система відповідає вимогам.

Існує два способи інсталяції ESET PROTECT:

- Інсталяція [сервера ESET PROTECT](#), [проксі-сервера Apache HTTP](#) або [Mobile Device Connector](#) за допомогою універсального інсталятора
- Інсталяція компонентів ESET PROTECT за допомогою [відокремлених інсталяторів](#)

Спеціальні сценарії інсталяції:

- Інсталяція з використанням [налаштовуваних сертифікатів](#)
- Інсталяція на [відмовостійкий кластер](#)

У багатьох сценаріях інсталяції передбачено встановлення різних компонентів ESET PROTECT на різних комп'ютерах, щоб пристосувати мережеві архітектури, дотриматися вимог щодо ефективності тощо. Для окремих компонентів ESET PROTECT доступні вказані нижче пакети інсталяції.

Основні компоненти

- [Сервер ESET PROTECT](#)
- [Веб-консоль ESET PROTECT](#)
- [Агент ESET Management](#) (має бути інстальовано на клієнтських комп'ютерах, за бажанням також на сервері ESET PROTECT)

Додаткові компоненти

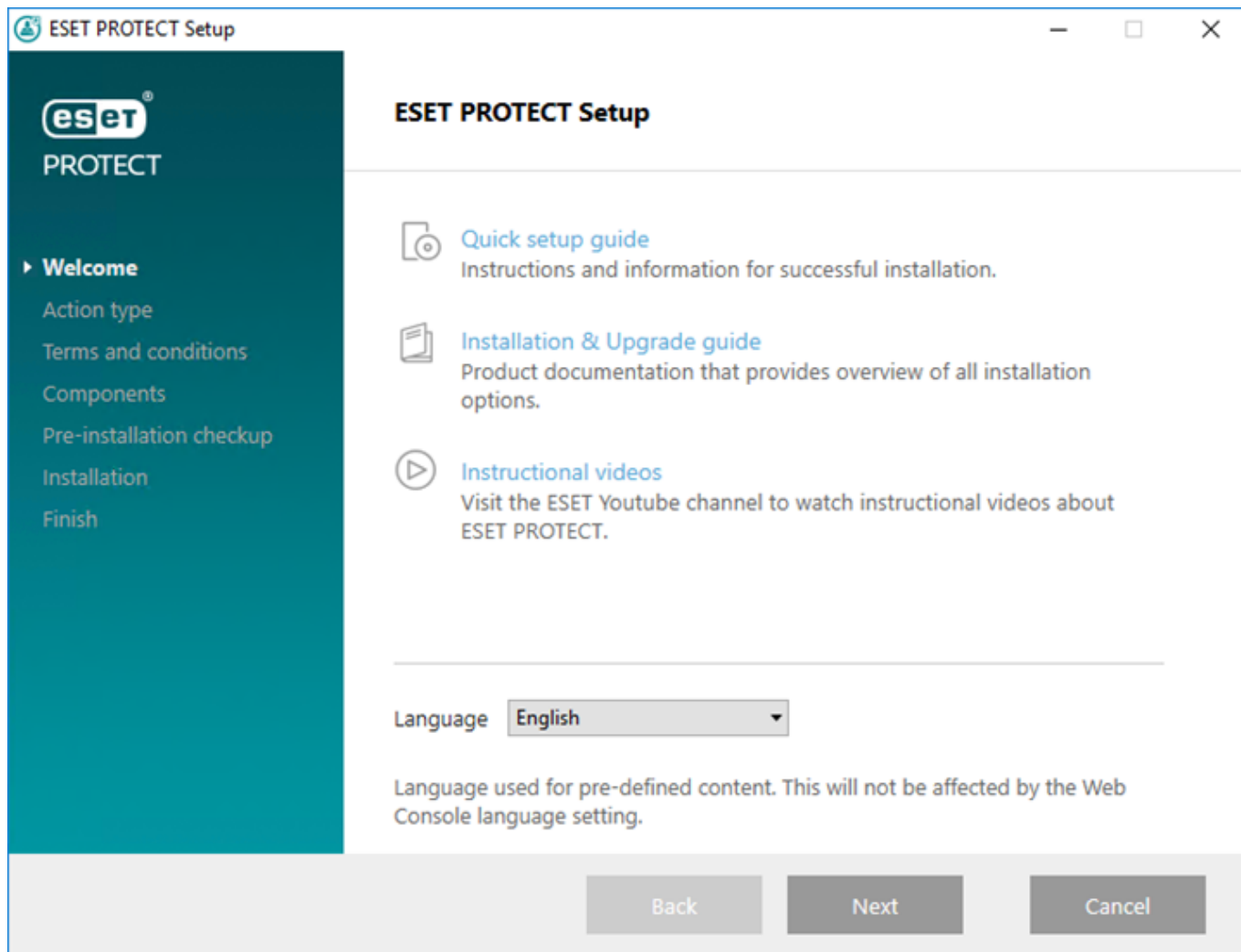
- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Проксі-сервер HTTP Apache](#)
- [Інструмент «Дзеркало»](#)

Інструкції з оновлення ERA до останньої версії ESET PROTECT 8.0 див. в нашій [статті бази знань](#).

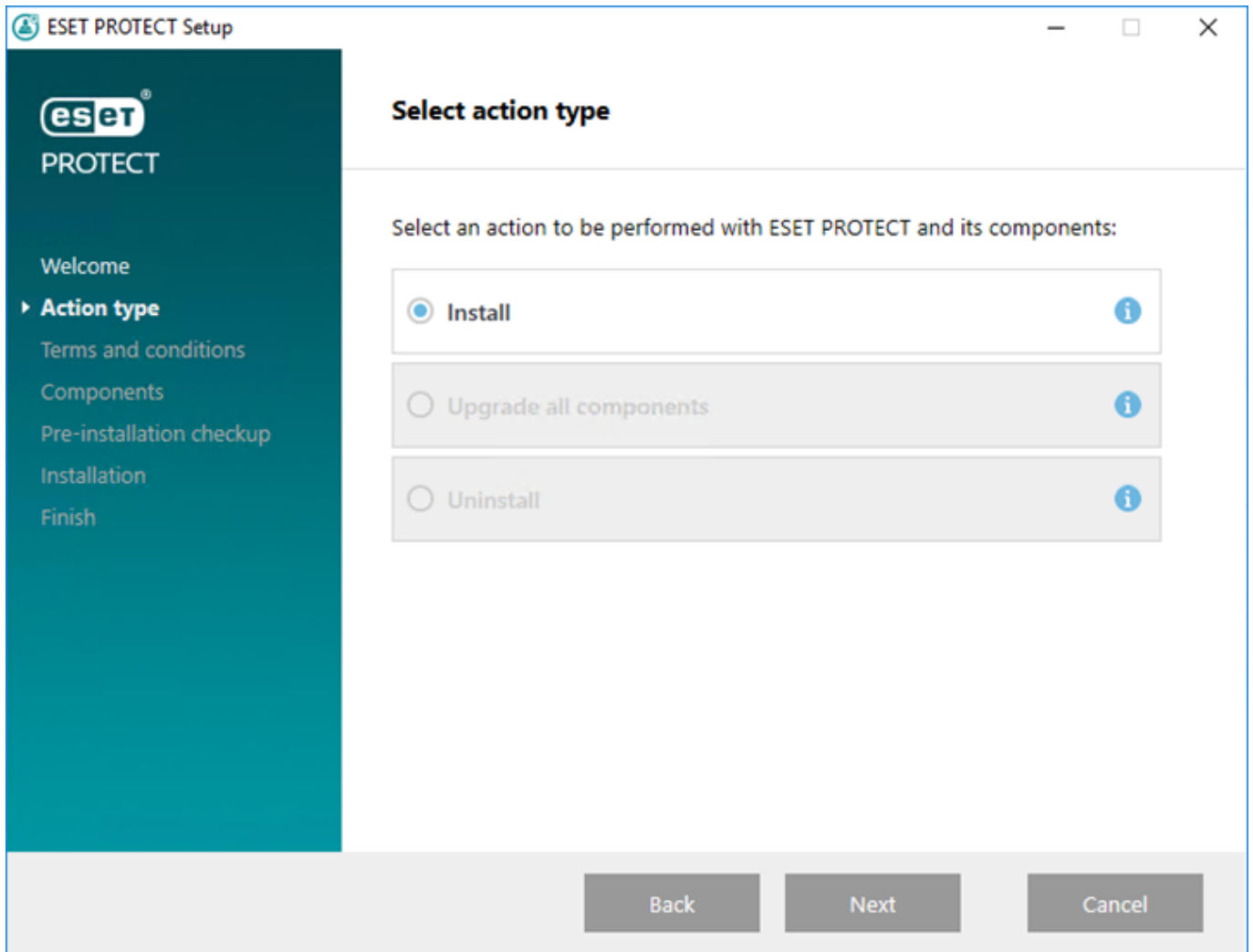
Інсталяція сервера ESET PROTECT

[Універсальний інсталятор ESET PROTECT](#) доступний лише для операційних систем Windows. Він дає змогу інстальувати всі компоненти ESET PROTECT за допомогою майстра інсталяції ESET PROTECT.

1. Відкрийте пакет інсталяції. На екрані привітання відкрийте розкривне меню **Мова** та налаштуйте параметри мови. Щоб продовжити, натисніть **Далі**.



2. Виберіть **Інсталювати** й натисніть **Далі**.



3. Якщо ви не хочете надсилати в ESET звіти про аварійне завершення роботи та дані телеметрії, зніміть прапорець **Узяти участь у програмі покращення продукту**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

4. Виберіть компоненти, які потрібно інсталювати, і натисніть **Далі**.

[-] [Microsoft SQL Server Express](#)

- ESET PROTECT 8.0 [Універсальний інсталятор](#) за замовчуванням інсталює Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інсталюватиметься за замовчуванням.
- Якщо в системі вже інсталювано іншу [підтримувану версію](#) Microsoft SQL Server чи MySQL або ви плануєте підключитися до іншого сервера SQL Server, зніміть прапорець **Microsoft SQL Server Express**.
- Рекомендуємо [не інсталювати SQL Server в контролері домену](#) (наприклад, якщо ви використовуєте Windows SBS / Essentials). Рекомендуємо інсталювати ESET PROTECT на іншому сервері або не вибирати компонент SQL Server Express під час інсталяції (щоб запустити базу даних ESET PROTECT, потрібно скористатися наявним сервером SQL Server або MySQL Server).

[-] [Додати користувацький HTTPS сертифікат для Webconsole](#)

- Виберіть цю опцію, якщо хочете використовувати користувацький сертифікат HTTPS для веб-консолі ESET PROTECT.
- Якщо ви не виберете цю опцію, для Tomcat буде автоматично створено сховище ключів.

[-] [Проксі-сервер Apache HTTP](#)



Увага

Опцію **Проксі-сервер Apache HTTP** призначено лише для невеликих або централізованих мереж без переміщуваних клієнтів. Якщо вибрати цю опцію, клієнти за замовчуванням буде налаштовано на тунельний обмін даними з ESET через проксі-сервер, інстальований на тому самому комп'ютері, що сервер ESET PROTECT. Якщо між клієнтами та сервером ESET PROTECT немає безпосередньої мережевої видимості, таке підключення не працюватиме.

- Використання проксі-сервера HTTP може суттєво зменшити навантаження на смугу пропускання під час завантаження даних з Інтернету й пришвидшити завантаження оновлень продуктів. Якщо ESET PROTECT вам потрібно керувати більш ніж 37 комп'ютерами, рекомендуємо встановити прапорець **Проксі-сервер HTTP Apache**. За бажанням можна також [інстальювати проксі-сервер Apache HTTP пізніше](#).

- Щоб дізнатися більше, перегляньте розділи [Що таке проксі-сервер Apache HTTP?](#) і [Відмінності між проксі-сервером Apache HTTP, інструментом «Дзеркало» та прямим підключенням](#).

- Виберіть опцію **Проксі-сервер Apache HTTP**, щоб інстальювати проксі-сервер Apache HTTP, а також створити й застосувати політики (під назвою **Використання проксі-сервера HTTP**; застосовуються до групи **Усі**) для таких продуктів:

oESET Endpoint для Windows

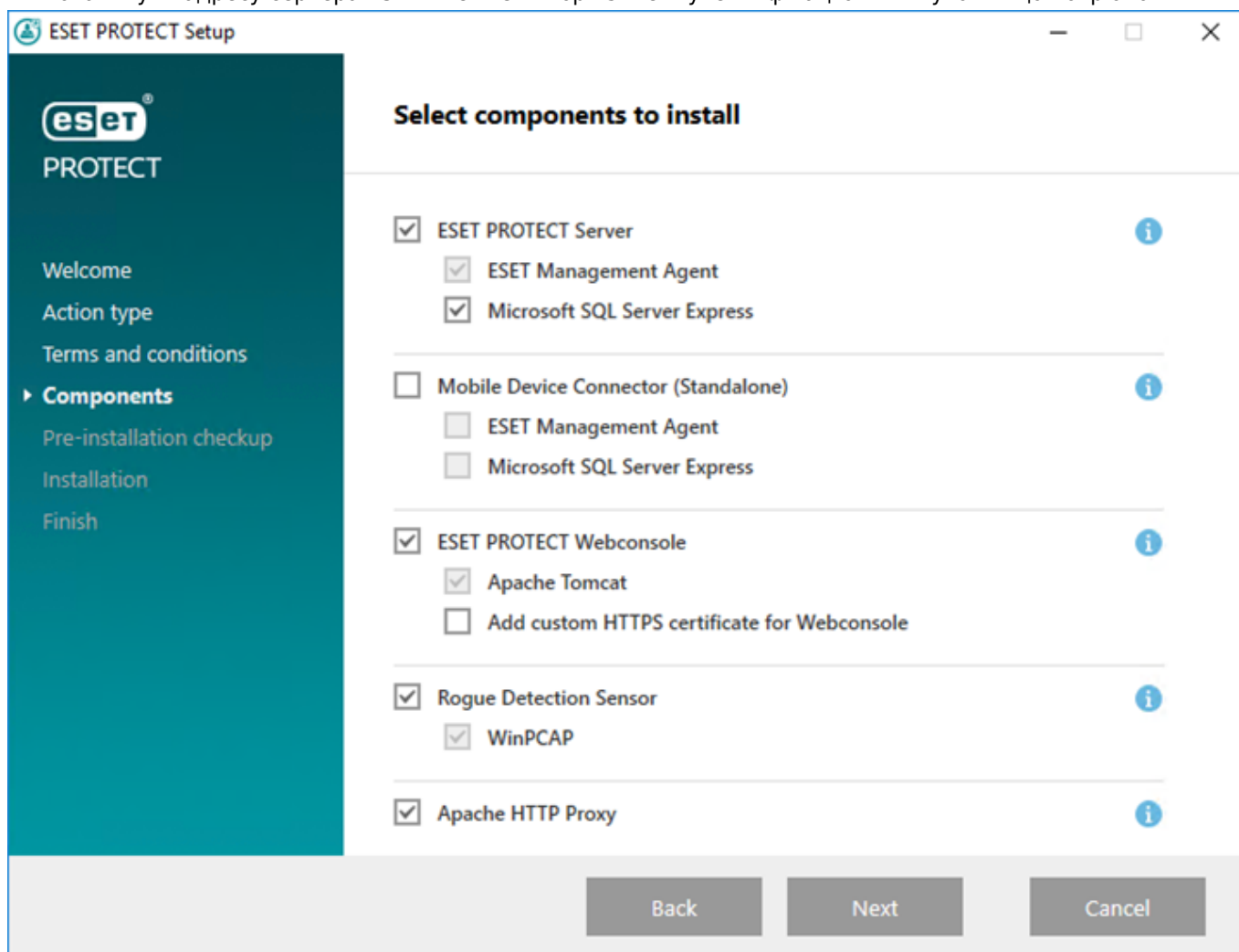
oESET Endpoint для macOS (OS X) і Linux

oESET Management Agent

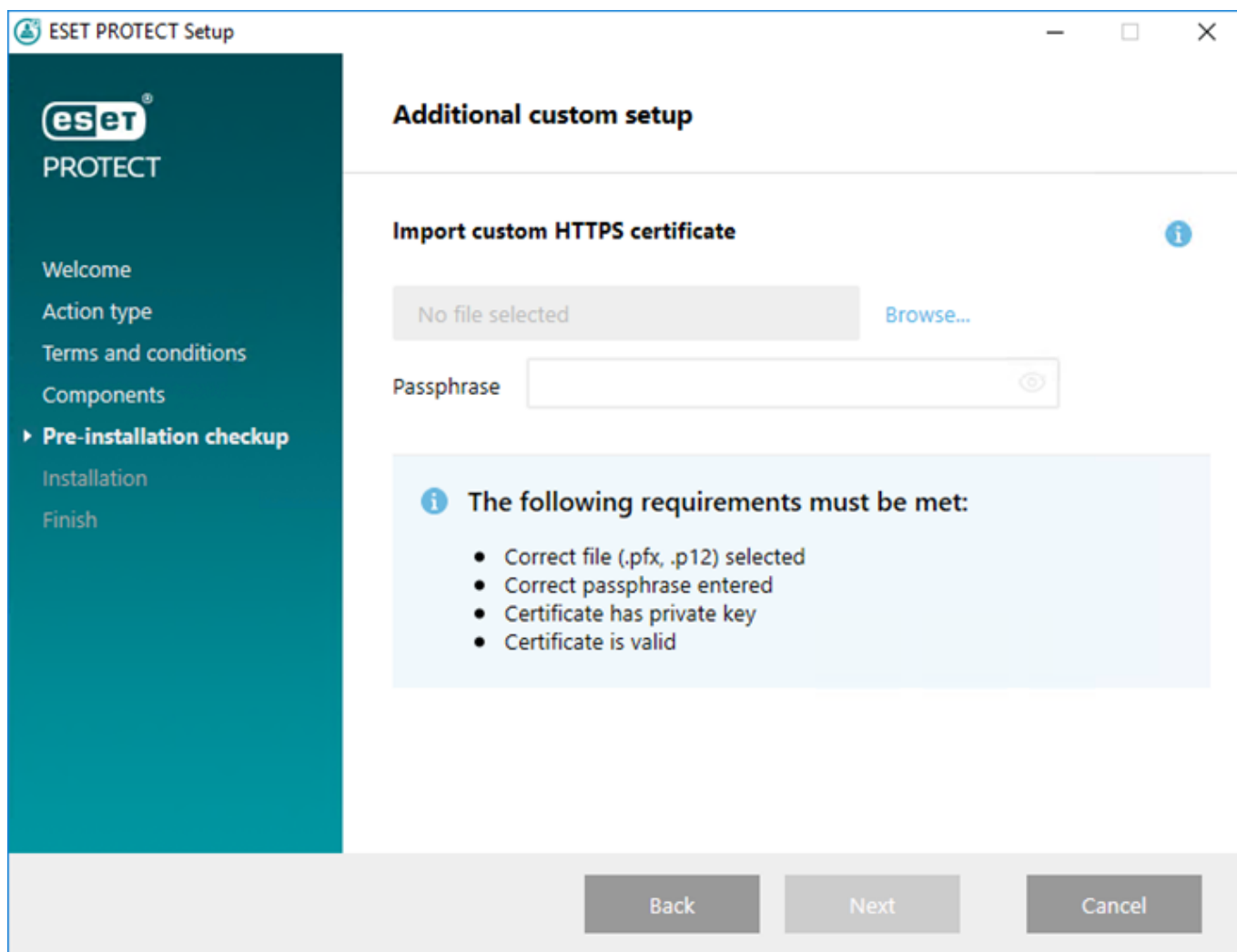
oESET File Security для Windows Server (V6+)

oESET Shared Local Cache

Політика вмикає проксі-сервер HTTP для відповідних продуктів. Хост проксі-сервера використовує локальну IP-адресу сервера ESET PROTECT і порт 3128. Аутентифікацію вимкнено. Якщо потрібно

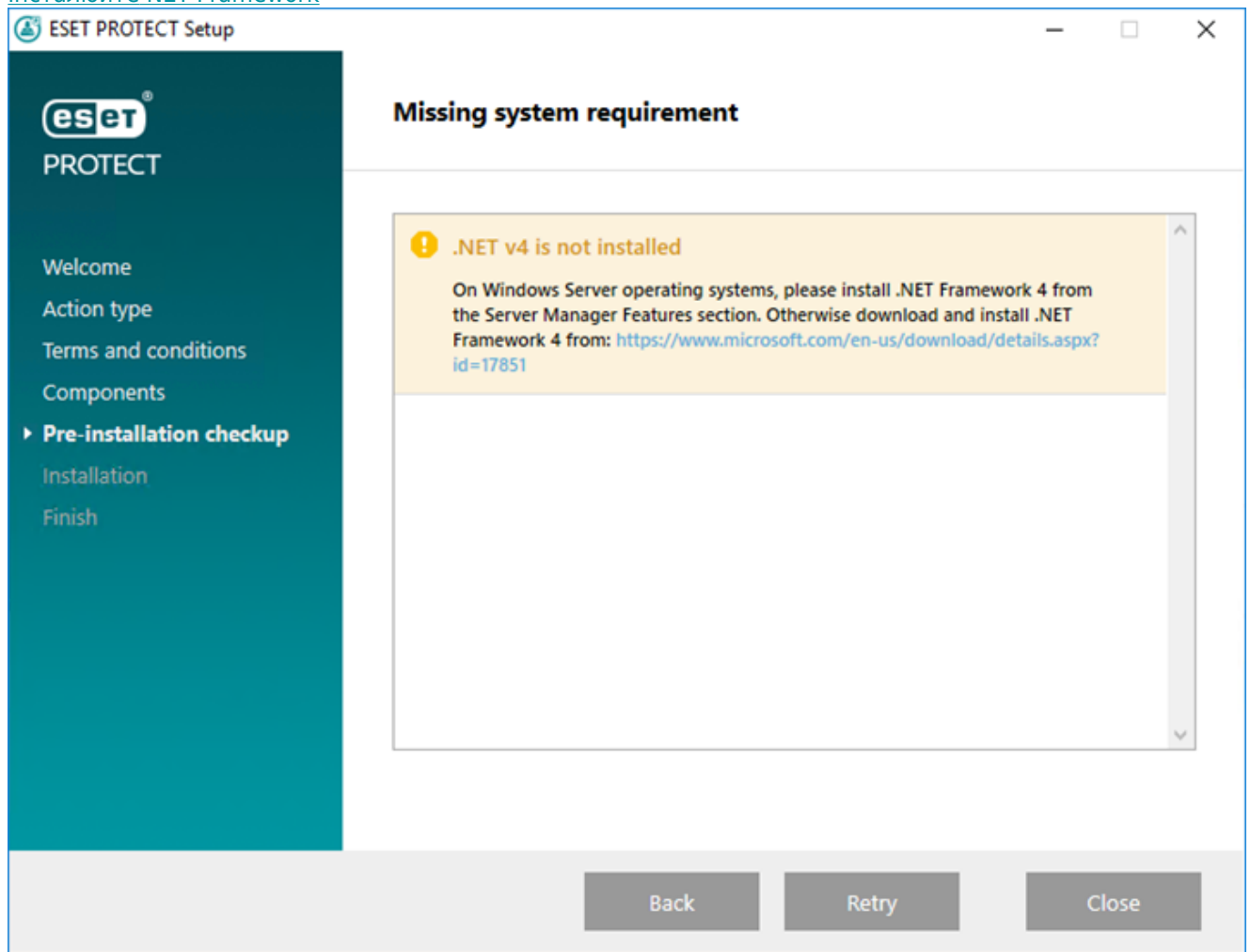


5. Якщо ви вибрали **Додати користувацький сертифікат HTTPS для веб-консолі**, натисніть **Огляд**, виберіть дійсний сертифікат (файл із розширенням .pfx або .p12) і введіть його **парольну фразу** (якщо її немає, залиште це поле порожнім). Сертифікат буде інстальовано на сервері Tomcat і використовуватиметься для доступу до веб-консолі. Щоб продовжити, натисніть **Далі**.

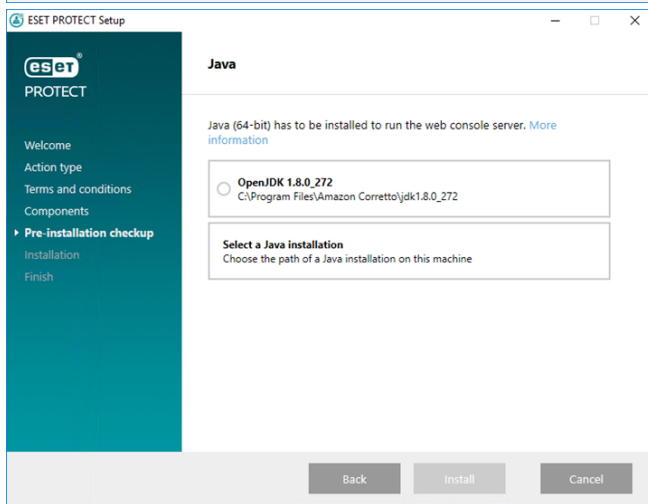
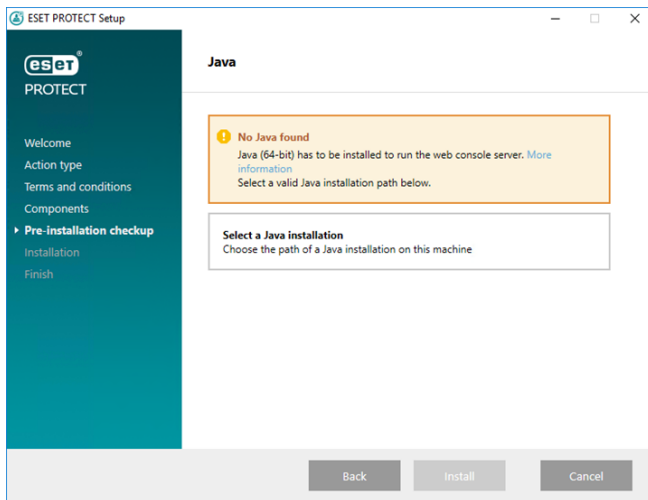


6. Якщо під час перевірки попередніх вимог виявлено помилки, усуньте їх. Переконайтеся, що система відповідає всім [ВИМОГАМ](#).

☒ [.NET версії 4 не інстальовано](#)



- [-] [Не вдалося знайти Java або не вдалося виявити Java \(64-розрядна версія\)](#)



Примітка

Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримувана версія – Java 8)) і залишити лише останню версію Java.



Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інстальувати один із підтримуваних випусків Java.

а) Щоб вибрати вже інстальовану версію Java, натисніть **Вибрати інсталяцію Java**, виберіть папку, у якій інстальовано Java (з підпакою *bin*, наприклад *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) і натисніть **ОК**. З'явиться запит інсталятора про те, чи правильно вибрано шлях.

б) Натисніть **Інстальувати**, щоб продовжити, або **Змінити**, щоб змінити шлях інсталяції Java.

[-] **На системному диску вільно лише 32 МБ**

- Це сповіщення може відобразитися, якщо в на диску недостатньо місця для інсталяції ESET PROTECT.
- Щоб інстальувати ESET PROTECT та всі компоненти продукту, потрібно мати принаймні 4400 МБ вільного місця на диску.

[-] **ESET Remote Administrator 5.x або попередніх версій інстальовано на комп'ютері, який унеможливує подальше виконання інсталятора.**

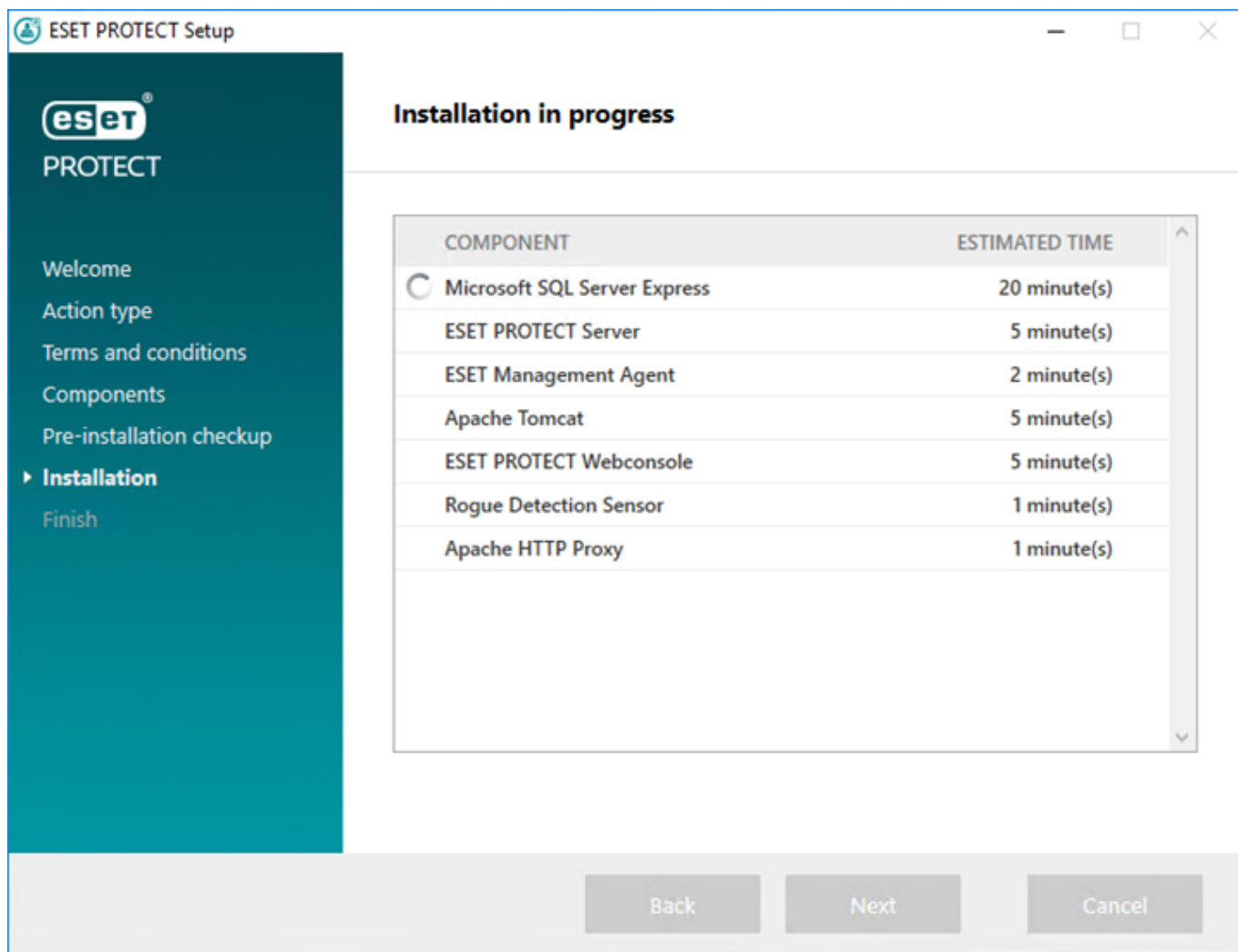
Пряме оновлення не підтримується: див. тему [Перенесення з ERA 5.x](#).

7. Коли завершиться перевірка попередніх вимог і середовище відповідатиме їм, почнеться інсталяція. Зверніть увагу, що інсталяція може тривати понад годину залежно від конфігурації вашої системи та мережі.



Примітка

Поки триває інсталяція, майстер інсталяції ESET PROTECT не відповідає.



8. Якщо в кроці 4 ви інстальювали **Microsoft SQL Server Express**, буде виконано перевірку підключення до бази даних. Перейдіть до розділу [Користувач веб-консолі та підключення до сервера](#). Якщо у вас уже є сервер бази даних, вам буде запропоновано ввести дані для підключення до бази даних під час наступного кроку.

9. Якщо ви використовуєте наявний сервер SQL Server або MySQL, налаштуйте параметри підключення відповідно. Введіть **назву бази даних**, **ім'я хоста**, номер **порту** (ця інформація доступна в диспетчері конфігурацій Microsoft SQL Server) і дані **облікового запису бази даних (ім'я користувача та пароль)** у відповідні поля й натисніть **Далі**. Підключення до бази даних буде перевірено. Якщо на сервері бази даних є наявна база даних ESET PROTECT (яка залишилася після попередньої інсталяції ERA/ESMC), її буде видалено. Ви можете вибрати один із таких варіантів: **Використовувати наявну базу даних і застосувати оновлення** або **Видалити наявну базу даних та інстальювати нову версію**.

Використовувати екземпляр з іменем. Якщо ви використовуєте базу даних MS SQL, можна також поставити прапорець **Використовувати екземпляр з іменем**. Це дасть змогу використовувати налаштовуваний екземпляр бази даних, який можна налаштувати в полі «Ім'я хоста» у формі `HOSTNAME\DB_INSTANCE`, наприклад: `192.168.0.10\ESMC7SQL`. Для кластерної бази даних використовуйте лише ім'я кластера. Якщо вибрати цю опцію, ви не зможете змінити порт, який використовуватиметься. Система використовуватиме порти за замовчуванням, визначені Microsoft.



Примітка

Поставивши прапорець **Використовувати екземпляр з іменем**, сервер ESET PROTECT можна також підключити до бази даних MS SQL, інстальованої у відмовостійкому кластері. У полі **Ім'я хоста** введіть ім'я кластера.

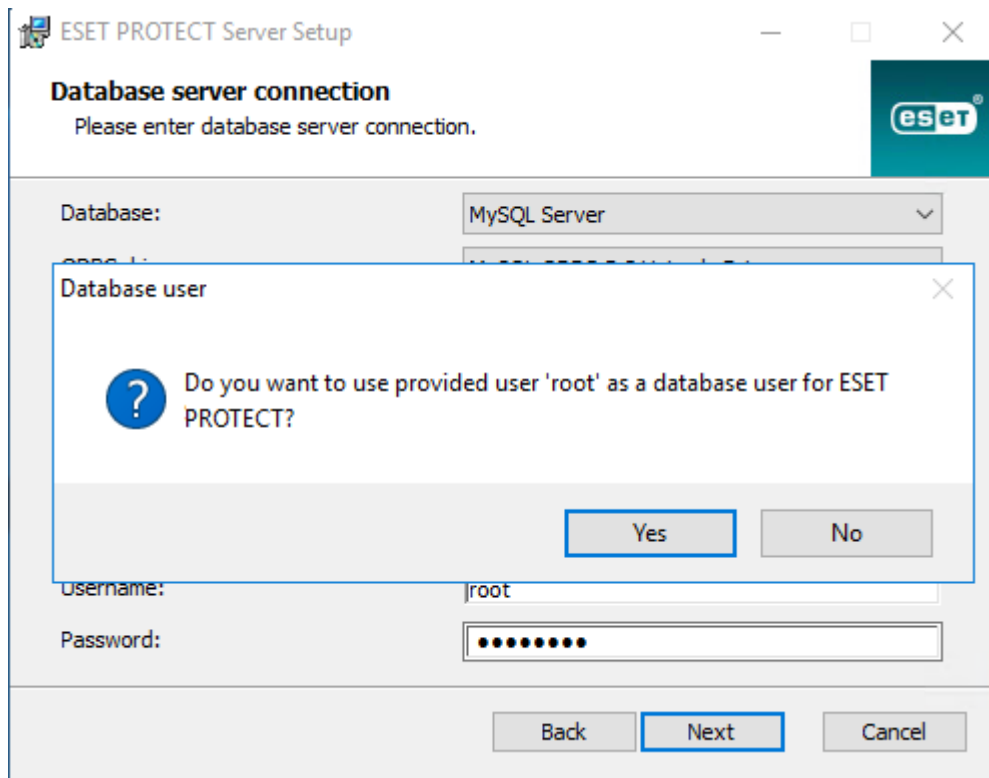


Примітка

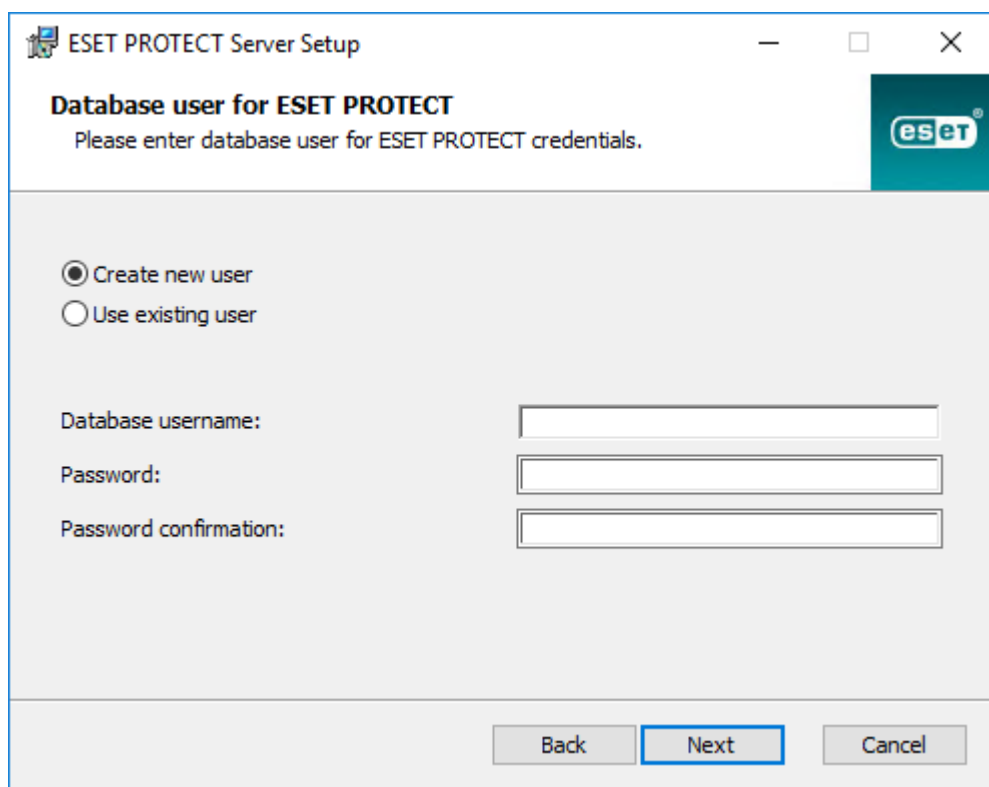
Для введення даних **облікового запису бази даних** є дві опції. Можна використовувати **спеціальний обліковий запис користувача бази даних**, який матиме доступ лише до бази даних ESET PROTECT, **обліковий запис SA** (MS SQL) або **обліковий запис root** (MySQL). Якщо ви виберете спеціальний обліковий запис користувача, потрібно буде створити обліковий запис із конкретними правами. Щоб дізнатися більше, перегляньте розділ [Спеціальний обліковий запис користувача бази даних](#). Якщо ви не збираєтеся використовувати спеціальний обліковий запис користувача, укажіть обліковий запис адміністратора (SA або root).

The screenshot shows the 'Database server connection' dialog box in the ESET PROTECT Server Setup application. The dialog has a title bar with the application name and standard window controls. Below the title bar, the text 'Please enter database server connection.' is displayed. The ESET logo is in the top right corner. The main area contains several fields: 'Database:' is a dropdown menu with 'MS SQL Server' selected; 'ODBC driver:' is a dropdown menu with 'MS SQL Server' selected; 'Database name:' is a text box containing 'era_db'; 'Hostname:' is a text box containing 'localhost'; 'Use Named Instance:' is a checkbox that is unchecked; 'Port:' is a text box containing '1433'; 'Database account' section includes 'Username:' and 'Password:' text boxes. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

Якщо ви вказали обліковий запис **SA** або **root** у попередньому вікні, натисніть **Так**, щоб продовжити використовувати обліковий запис SA чи root як користувач бази даних для ESET PROTECT.



Якщо натиснути **Ні**, потрібно вибрати опцію **Створити нового користувача** (якщо ви ще цього не зробили) або **Використовувати наявного користувача** (якщо у вас є спеціальний обліковий запис користувача бази даних, який згадується [тут](#)).



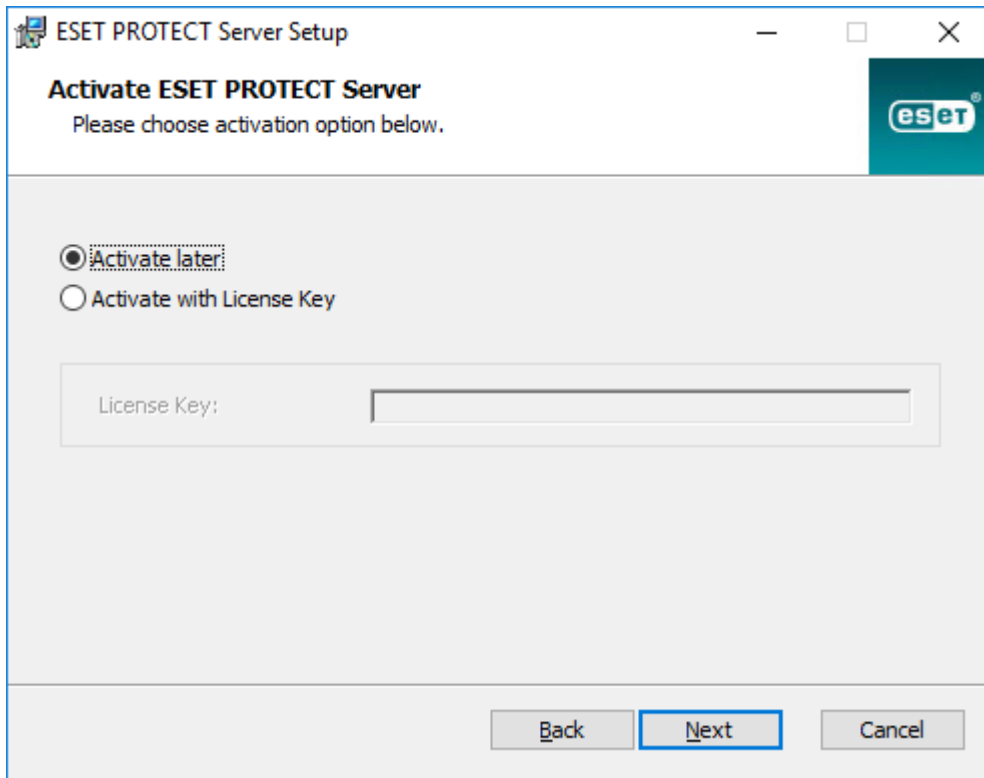
10. З'явиться запит ввести пароль облікового запису адміністратора веб-консолі. Цей пароль є важливим, оскільки він потрібний для доступу до [веб-консолі ESET PROTECT](#). Натисніть кнопку **Далі**.

The screenshot shows the 'Web Console user & server connection' step of the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. The subtitle is 'Web Console user & server connection' with the instruction 'Please enter Web Console user password and server connection.' The ESET logo is in the top right corner. The form contains the following fields: 'Web Console user:' with the value 'Administrator'; 'Password:' and 'Password confirmation:' both with masked characters (dots); 'Agent port:' with the value '2222'; and 'Console port:' with the value '2223'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

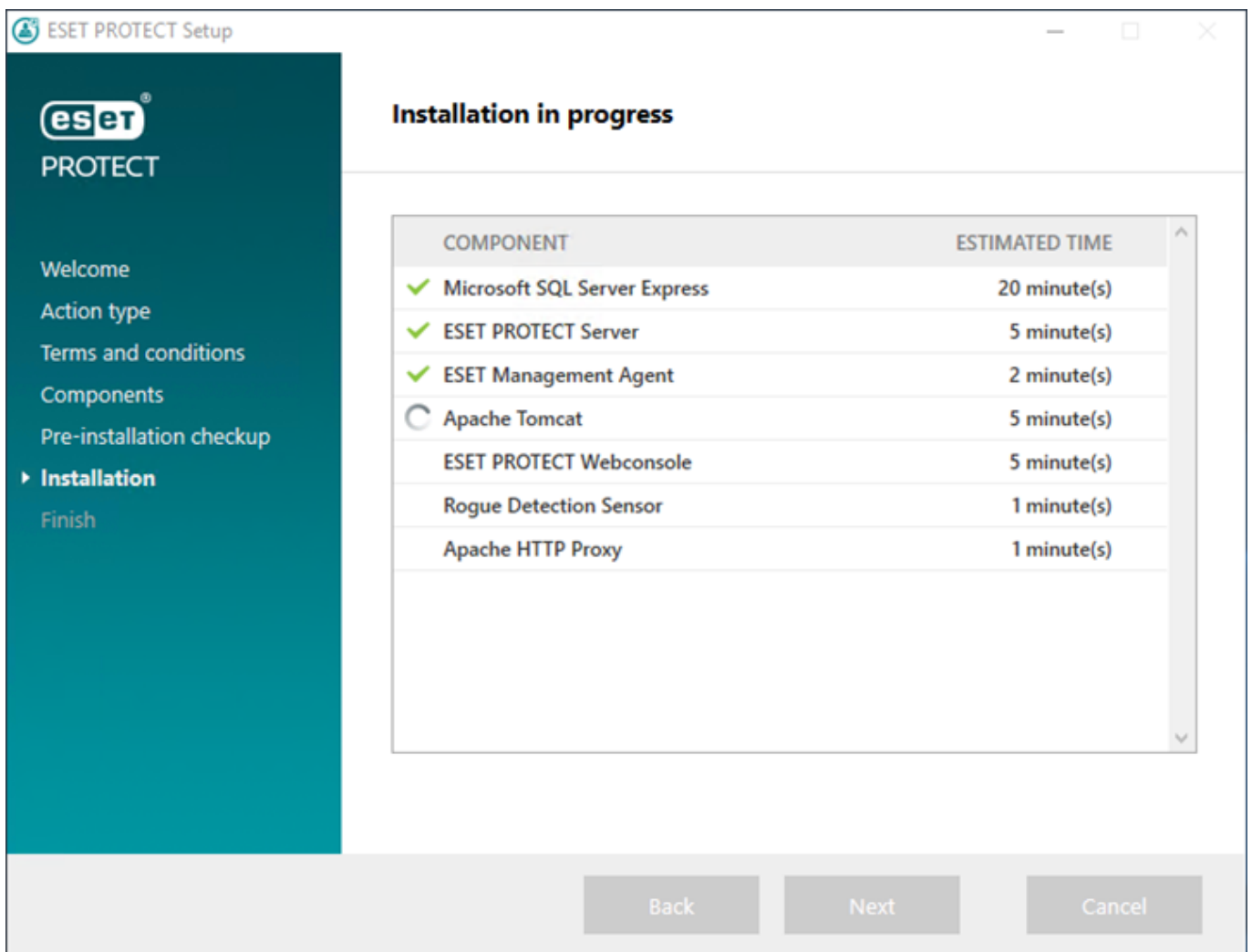
11. Не змінюйте ці поля або введіть у них дані про організацію, що відобразяться в інформації про сертифікати агента ESET Management і сервера ESET PROTECT. Якщо ви введете пароль у полі **Пароль центра**, обов'язково запам'ятайте його. Натисніть кнопку **Далі**.

The screenshot shows the 'Certificate information' step of the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. The subtitle is 'Certificate information' with the instruction 'Please enter common certificate information below.' The ESET logo is in the top right corner. The form contains the following fields: 'Organizational unit:', 'Organization:', 'Locality:', 'State / Country:' (with a dropdown arrow), 'Certificate validity: *' (with the value '10' and a 'Years' dropdown), 'Authority common name: *' (with the value 'Server Certification Authority'), and 'Authority password:'. At the bottom left, there is a note '* required fields'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

12. Введіть дійсний **ліцензійний ключ** (указаний в електронному листі від ESET щодо нової покупки) і натисніть **Далі**. Якщо ви використовуєте облікові дані застарілої ліцензії (ім'я користувача та пароль), [конвертуйте](#) їх у ліцензійний ключ. Ви також можете вибрати опцію **Активувати пізніше**. Якщо ви виберете опцію **Активувати пізніше**, перегляньте додаткові вказівки в розділі [Активація](#).



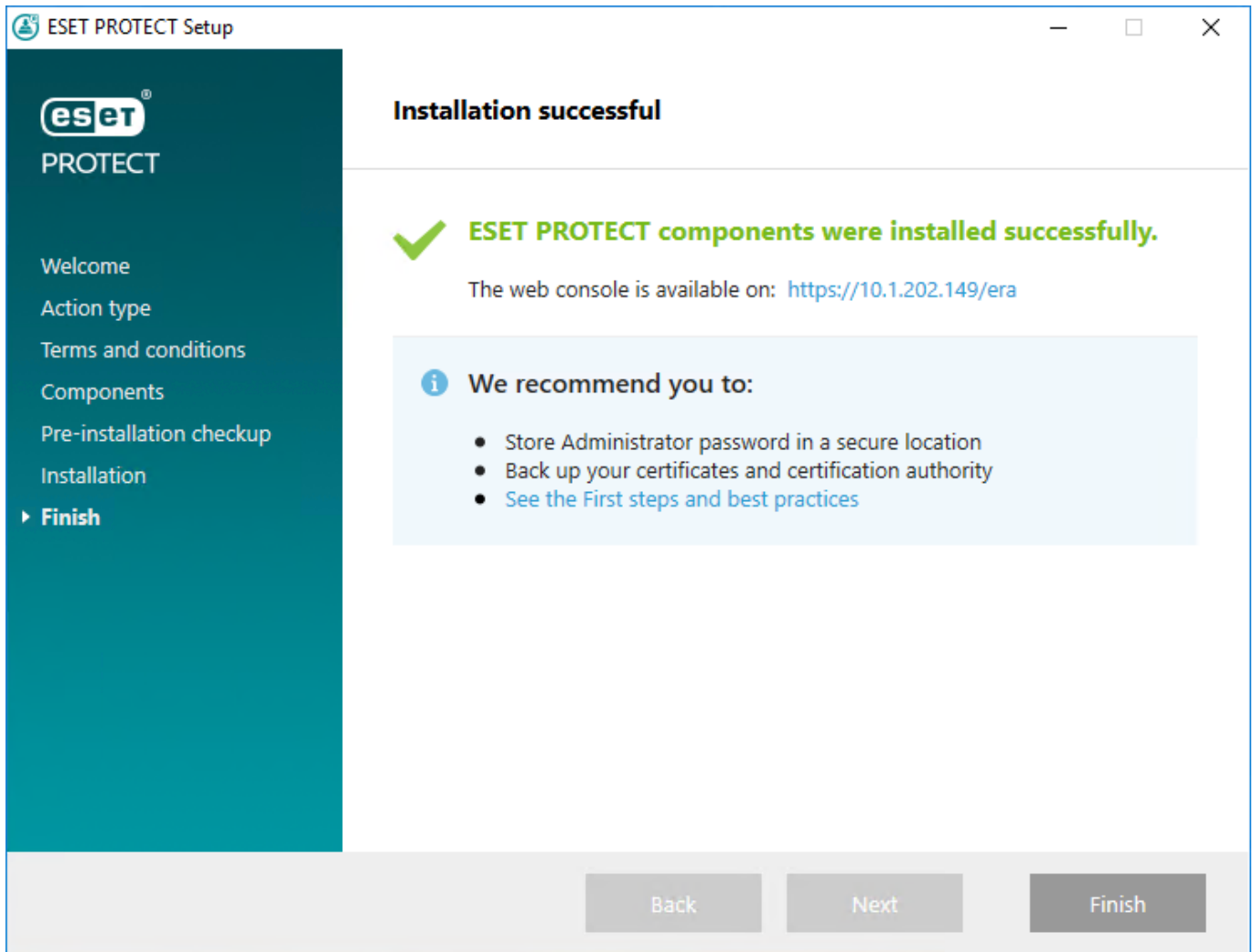
13. Відобразитиметься перебіг інсталяції.



14. Якщо ви вибрали інсталяцію **Rogue Detection Sensor**, з'являться вікна інсталяції драйвера WinPcap.

Поставте прапорець **Автоматично запускати драйвер WinPcap під час завантаження**.

15. Після інсталяції з'явиться повідомлення «Компоненти ESET PROTECT інстальовано успішно» та URL-адреса веб-консолі ESET PROTECT. Натисніть URL-адресу, щоб відкрити [веб-консоль](#), або натисніть **Завершити**.



Якщо не вдалося виконати інсталяцію, виконайте дії нижче.

- Перегляньте файли журналу інсталяції в пакеті універсальної інсталяції. Журнали розташовано в тому самому каталозі, що й універсальний інсталятор, наприклад:
C:\Users\Administrator\Downloads\x64\logs\
- Додаткові дії для вирішення цієї проблеми можна переглянути в розділі [Виправлення неполадок](#).

Інсталяція ESET PROTECT Mobile Device Connector (автономно)

Щоб інстальовати Mobile Device Connector як відокремлений інструмент на комп'ютері без сервера ESET PROTECT, виконайте наступні кроки.



Попередження

Щоб мобільними пристроями можна було керувати будь-коли незалежно від їхнього місцезнаходження, до Mobile Device Connector має бути доступ через Інтернет.

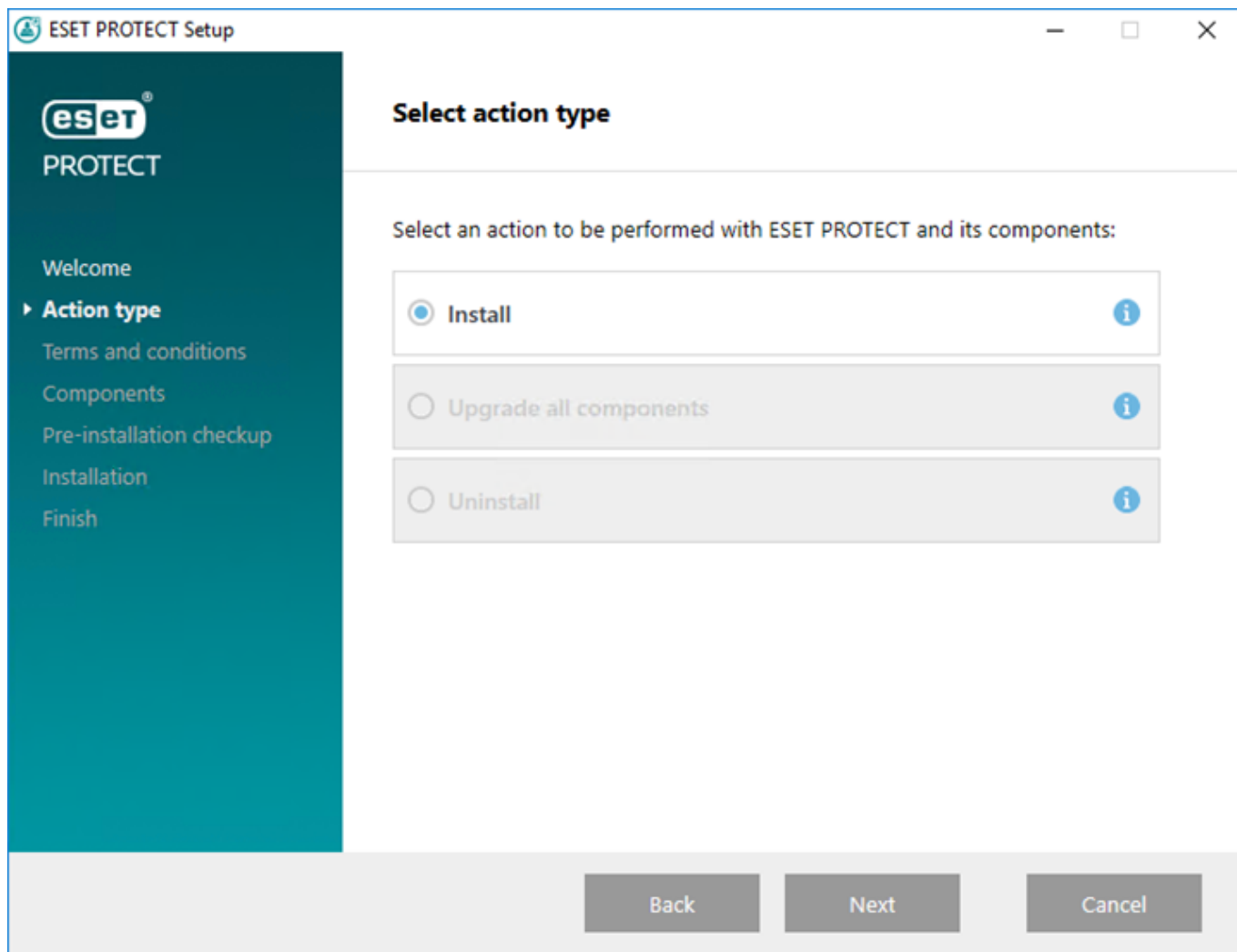


Примітка

Враховуйте, що мобільний пристрій обмінюється даними з Mobile Device Connector, що неминуче підвищує інтенсивність використання мережі мобільних даних. Особливо це стосується мережі в роумінгу.

Виконайте наведені нижче дії, щоб встановити Mobile Device Connector на комп'ютер з ОС Windows:

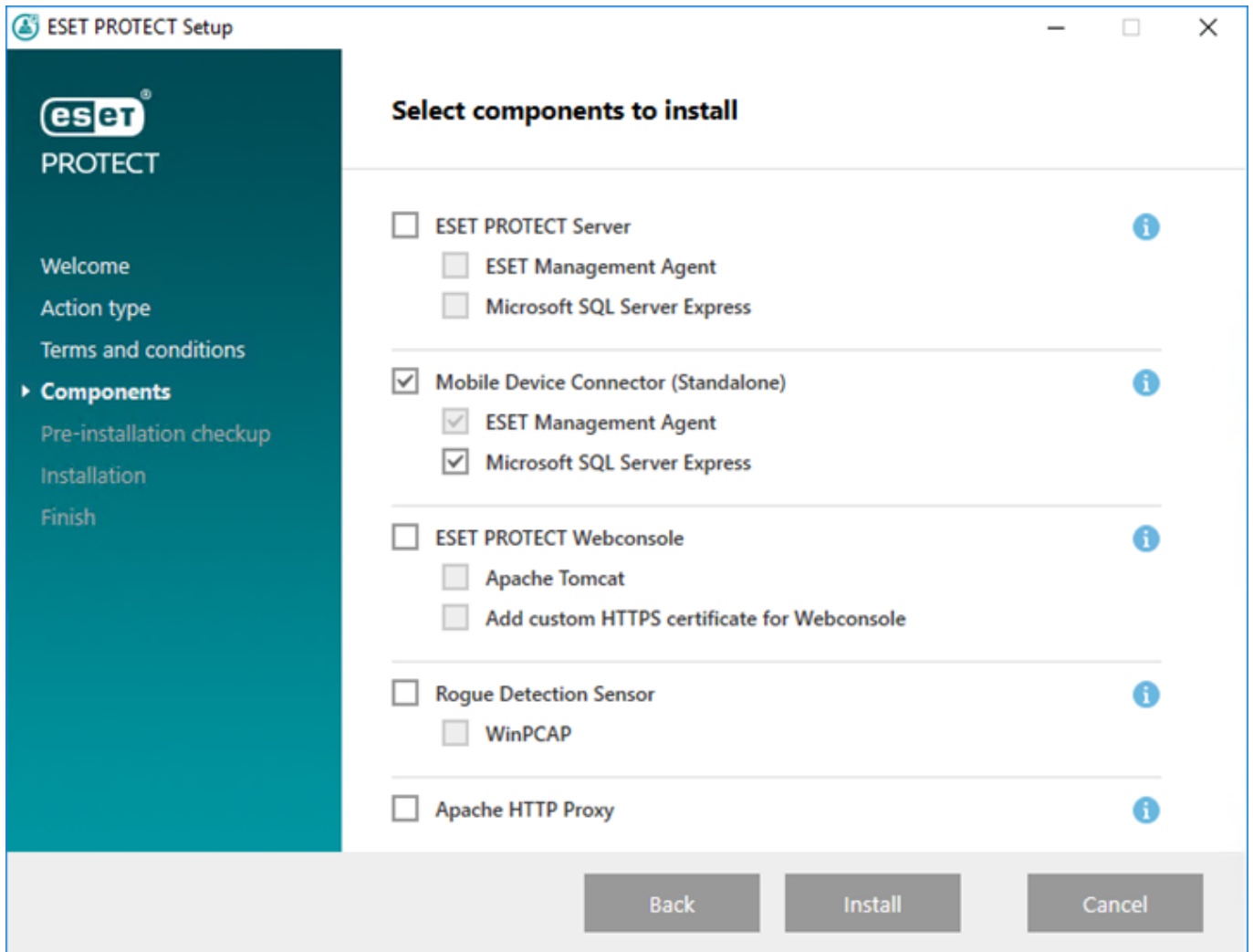
1. Спершу перегляньте [ВИМОГИ](#) та переконайтеся, що виконуєте їх.
2. Двічі натисніть інсталяційний пакет, щоб відкрити його, виберіть **Інсталиювати** та натисніть **Далі**.



3. Якщо ви не хочете надсилати в ESET звіти про аварійне завершення роботи та дані телеметрії, зніміть прапорець **Узяти участь у програмі покращення продукту**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET.

4. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

5. Установіть прапорець лише біля пункту **Mobile Device Connector (Відокремлений)**. Для використання ESET PROTECT Mobile Device Connector необхідна **база даних**. Виберіть **Microsoft SQL Server Express**, якщо ви хочете встановити базу даних, або залиште це поле порожнім. Якщо ви хочете підключитися до наявної бази даних, то зможете це зробити під час інсталяції. Клацніть **Інсталиювати**, щоб розпочати інсталяцію.



6. Якщо ви обрали варіант з інсталяцією бази даних на кроці 5 цієї процедури, базу даних буде встановлено автоматично, а ви можете перейти до кроку 8. Якщо ви вирішили не встановлювати базу даних, вам буде запропоновано підключити компонент MDM до наявної бази даних.



Примітка

Можна використовувати той самий сервер, що й для бази даних ESET PROTECT. Однак рекомендуємо використовувати інший сервер бази даних, якщо ви плануєте зареєструвати понад 80 мобільних пристроїв.

7. Інсталятору потрібно підключитися до наявної бази даних, яку використовуватиме Mobile Device Connector. Укажіть такі дані для підключення:

- **База даних:** MySQL Server / MS SQL Server / MS SQL Server з використанням автентифікації Windows
- **ODBC драйвер:** драйвер MySQL ODBC 5.1 / драйвер MySQL ODBC 5.2 з підтримкою Юнікод / драйвер MySQL ODBC 5.3 з підтримкою Юнікод / драйвер MySQL ODBC 8.0 із підтримкою Юнікод / SQL Server / SQL Server Native Client 10.0 / драйвер ODBC 11 для SQL Server / драйвер ODBC 13 для SQL Server / драйвер ODBC 17 для SQL Server
- **Ім'я бази даних:** рекомендуємо використовувати попередньо встановлене ім'я або змінити його за необхідності.
- **Ім'я хоста:** ім'я хоста або IP-адреса сервера бази даних
- **Порт:** використовується для підключення до сервера бази даних
- **Ім'я користувача / пароль** облікового запису адміністратора бази даних
- **Використовувати екземпляр з іменем.** Якщо ви використовуєте базу даних MS SQL, можна також поставити прапорець **Використовувати екземпляр з іменем**. Це дасть змогу використовувати налаштований екземпляр бази даних, який можна налаштувати в полі «Ім'я хоста» у формі `HOSTNAME\DB_INSTANCE`, наприклад: `192.168.0.10\ESMC7SQL`. Для кластерної бази даних

використовуйте лише ім'я кластера. Якщо вибрати цю опцію, ви не зможете змінити порт, який використовуватиметься. Система використовуватиме порти за замовчуванням, визначені Microsoft.



Примітка

Поставивши прапорець **Використовувати екземпляр з іменем**, сервер ESET PROTECT можна також підключити до бази даних MS SQL, інсталюваної у відмовостійкому кластері. У полі **Ім'я хоста** введіть ім'я кластера.

The screenshot shows the 'Database server connection' dialog box in the ESET PROTECT Mobile Device Connector Setup. The dialog has a title bar with the ESET logo and standard window controls. Below the title bar, it says 'Please enter database server connection.' The form contains several fields: 'Database:' with a dropdown menu showing 'MS SQL Server' selected; 'ODBC driver:' with a dropdown menu showing 'MS SQL Server' selected; 'Database name:' with a text box containing 'era_mdm_db'; 'Hostname:' with a text box containing 'localhost'; 'Use Named Instance:' with an unchecked checkbox; 'Port:' with a text box containing '1433'; 'Database account' section with 'Username:' and 'Password:' text boxes. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

8. Якщо з'єднання було успішним, вам буде запропоновано підтвердити, що ви хочете використовувати вказаного користувача як користувача бази даних для ESET PROTECT MDM.

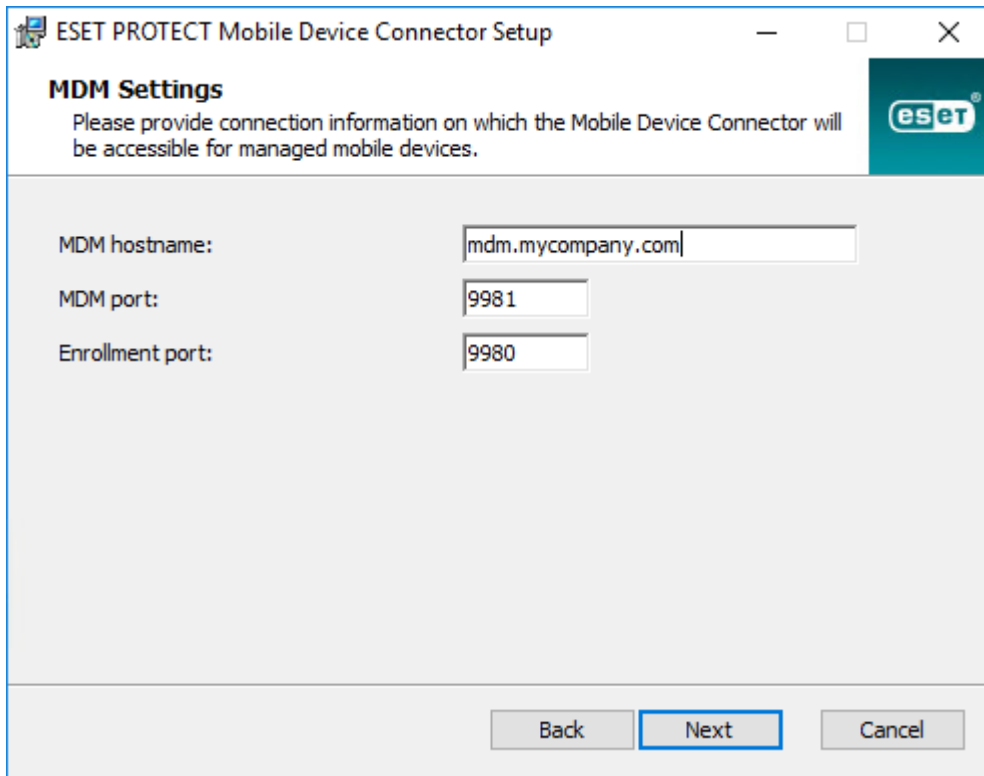
9. Після інсталяції нової або підключення інсталюатора до наявної бази даних ви можете перейти до встановлення MDM. Укажіть **ім'я хоста MDM**: це загальнодоступний домен або загальнодоступна IP-адреса сервера MDM, через які до нього можна отримати доступ із мобільних пристроїв в Інтернеті.

Ім'я хоста MDM потрібно ввести ідентично тому, як його вказано в **сертифікаті сервера HTTPS**. В іншому разі мобільний пристрій iOS відмовиться інсталювати **профіль MDM**. Наприклад, якщо в сертифікаті вказано IP-адресу, введіть її в полі **ім'я хоста MDM**. Якщо в сертифікаті HTTPS вказано повне доменне ім'я (наприклад, `mdm.мусотрану.com`), введіть його в полі **ім'я хоста MDM**. Крім цього, якщо в сертифікаті HTTPS використовується символ узагальнення * (наприклад, `*.мусотрану.com`), ви можете вказати в полі **ім'я хоста MDM** значення `mdm.мусотрану.com`.



Попередження

Будьте дуже уважні, вказуючи **ім'я хоста MDM** на цьому кроці. Якщо ви зазначите невірні дані або дані в неправильному форматі, MDM Connector працюватиме неправильно, а виправити це можна буде лише шляхом повторної інсталяції компонента.



10. На наступному кроці перевірте підключення до бази даних, натиснувши **Далі**.

11. Підключіть MDM Connector до сервера ESET PROTECT. Заповніть поля **Хост сервера** та **Порт сервера**, необхідні для підключення до сервера ESET PROTECT, і виберіть варіант **Інсталяція із сервера** або **Інсталяція в автономному режимі**, щоб продовжити.

Інсталяція із сервера. Укажіть облікові дані адміністратора веб-консолі ESET PROTECT, й інсталятор завантажить необхідні сертифікати автоматично. Також перевірте, чи надано [дозволи](#), необхідні для інсталяції із сервера.

1. Введіть **хост сервера** (назву або IP-адресу сервера ESET PROTECT) і **порт веб-консолі** (якщо ви не використовуєте інший порт, укажіть номер порту за замовчуванням – 2223). Також укажіть облікові дані (**ім'я користувача та пароль**) адміністратора веб-консолі.
2. Коли з'явиться запит прийняти сертифікат, натисніть **Так**. Перейдіть до кроку 11.

Інсталяція в автономному режимі. Укажіть **сертифікат проксі-сервера** та **Центр сертифікації**, який можна [експортувати](#) з ESET PROTECT. Можна також використовувати [налаштовуваний сертифікат](#) і відповідний Центр сертифікації.

1. Натисніть **Огляд** поруч із сертифікатом однорангового вузла та перейдіть до папки, у якій розташовано **цей сертифікат** (це сертифікат проксі-сервера, експортований з ESET PROTECT). Не заповнюйте поле **Пароль сертифіката**, оскільки для цього сертифіката пароль не потрібний.
2. Повторіть процедуру для Центру сертифікації та перейдіть до кроку 11.



Примітка

Якщо в ESET PROTECT використовуються налаштовувані сертифікати (замість сертифікатів за замовчуванням, автоматично згенерованих під час інсталяції ESET PROTECT), їх слід використовувати під час запиту сертифіката проксі-сервера.

12. Укажіть папку призначення для Mobile Device Connector (рекомендується використовувати папку за замовчуванням) і натисніть **Далі** > **Інсталювати**.

Після завершення інсталяції MDM вам буде запропоновано встановити агент. Натисніть кнопку **Далі**, щоб розпочати інсталяцію, прийміть ліцензійну угоду з кінцевим користувачем (якщо погоджуєтесь з її умовами) і виконайте наступні кроки:

1. Введіть **хост сервера** (ім'я хоста або IP-адресу сервера ESET PROTECT) і **порт сервера** (порт за замовчуванням – 2222; якщо ви використовуєте інший порт, укажіть його).



Увага

Переконайтесь, що **Хост сервера** відповідає принаймні одному зі значень (в ідеалі – FQDN), визначених у полі **Хост** пункту **Сертифікат сервера**. В іншому разі відобразиться помилка «Отримано недійсний сертифікат сервера». У полі «Хост» пункту «Сертифікат сервера» може використовуватися символ узагальнення (*). Це означає, що він буде працювати з будь-яким **Хостом сервера**.

2. Якщо ви використовуєте проксі-сервер, встановіть прапорець **Використовувати проксі-сервер**. У цьому разі інсталятор продовжить **інсталяцію в автономному режимі**.



Примітка

Цей параметр проксі-сервера використовується лише для реплікації між агентом ESET Management і сервером ESET PROTECT, а не для кешування оновлень.

- **Ім'я хоста проксі-сервера:** ім'я хоста або IP-адреса комп'ютера, де розміщено проксі-сервер HTTP.
 - **Порт проксі-сервера:** за замовчуванням це 3128.
 - **Ім'я користувача, пароль:** введіть облікові дані проксі-сервера (якщо використовується автентифікація).
- Параметри проксі-сервера можна змінити пізніше в [політиці](#). [Проксі-сервер](#) має бути інстальовано до налаштування підключення «агент – сервер» через проксі-сервер.

3. Виберіть один із наступних варіантів інсталяції та виконайте відповідні кроки:

Інсталяція із сервера. Для цього потрібно вказати облікові дані адміністратора веб-консолі ESET PROTECT (інсталятор завантажить необхідні сертифікати автоматично).

Інсталяція в автономному режимі. Укажіть сертифікат агенту та Центр сертифікації, який можна [експортувати](#) з ESET PROTECT. Замість нього можна використати [налаштовуваний сертифікат](#).

- Щоб завершити **інсталяцію агента з використанням сервера**, виконайте наведені нижче кроки.
 1. Введіть ім'я хоста або IP-адресу веб-консолі ESET PROTECT (такі самі, як у сервера ESET PROTECT) у полі **Хост сервера**. Якщо ви не використовуєте інший порт, залиште в полі **Порт веб-консолі** значення за замовчуванням (порт 2223). Крім того, введіть облікові дані веб-консолі в поля **Ім'я користувача та Пароль**.



Увага

Переконайтесь, що **Хост сервера** відповідає принаймні одному зі значень (в ідеалі – FQDN), визначених у полі **Хост** пункту **Сертифікат сервера**. В іншому разі відобразиться помилка «Отримано недійсний сертифікат сервера». У полі «Хост» пункту «Сертифікат сервера» може використовуватися символ узагальнення (*). Це означає, що він буде працювати з будь-яким **Хостом сервера**.

2. Коли з'явиться запит прийняти сертифікат, натисніть **Так**.
 3. Виберіть **Не створювати комп'ютер** або **Вибрати настроювану статичну групу**. Якщо натиснути **Вибрати настроювану статичну групу**, ви зможете вибрати необхідну статичну групу зі списку наявних у ESET PROTECT. Комп'ютер буде додано до вибраної групи.
 4. Укажіть папку призначення для агента ESET Management (рекомендується використовувати розташування за замовчуванням), натисніть **Далі > Інстальювати**.
- Щоб продовжити **інсталяція агента в автономному режимі**, виконайте наведені нижче кроки.

1. Якщо в попередньому кроці ви вибрали пункт **Проксі-сервер**, укажіть **Ім'я хоста проксі-сервера**, **Порт проксі-сервера** (за замовчуванням: 3128), **Ім'я користувача** та **Пароль** і натисніть кнопку **Далі**.
2. Натисніть **Огляд** і перейдіть до папки, у якій розташовано цей сертифікат (це сертифікат агента, експортований з ESET PROTECT). Не заповнюйте поле **Пароль сертифіката**, оскільки для цього сертифіката пароль не потрібний. Крім того, не потрібно шукати **центр сертифікації**. Залиште це поле порожнім.



Примітка

Якщо ви створили налаштовуваний сертифікат з ESET PROTECT (замість сертифікатів за замовчуванням, автоматично згенерованих під час інсталяції ESET PROTECT), використовуйте саме його.

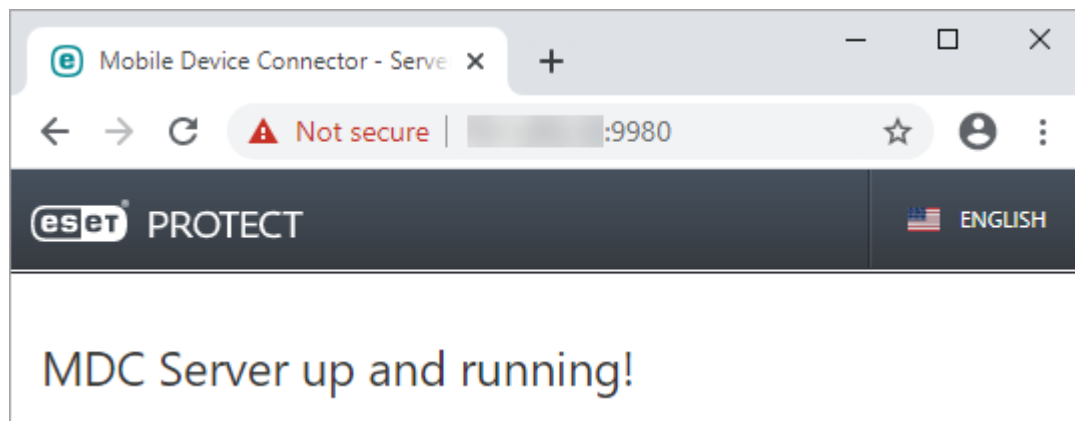


Попередження

Парольна фраза сертифіката не може містити такі символи: " \ Ці символи спричиняють критичну помилку під час ініціалізації агента.

3. Щоб інсталювати програму в папку за замовчуванням, клацніть **Далі**. Щоб вибрати іншу папку (рекомендується використовувати папку за замовчуванням), клацніть **Змінити**.

Коли інсталяція завершиться, перевірте, чи Mobile Device Connector працює належним чином. Для цього відкрийте в браузері або на мобільному пристрої сторінку <https://your-mdm-hostname:enrollment-port> (наприклад, <https://mdm.company.com:9980>) Якщо інсталяцію виконано успішно, з'явиться таке повідомлення:



Тепер ви можете [активувати MDM в ESET PROTECT](#).

Інсталяція в Microsoft Azure

Для користувачів, які надають перевагу керованим рішенням замість локальної підтримки ESET PROTECT, ESET пропонує ESET PROTECT на хмарній платформі [Microsoft Azure](#).

Щоб дізнатися більше, перегляньте нашу базу знань.

- [Початок роботи з ESET PROTECT - Azure](#)
- Віртуальна машина [ESET PROTECT для Microsoft Azure - Запитання й відповіді](#)
- Щоб інсталювати ESET PROTECT 8.0 в Azure, дотримуйтеся інструкції з цієї [статті бази знань](#) і використовуйте [ESET PROTECT 8.0 Універсальний інстальатор](#). Крім того, ви можете інсталювати ERA 6.x в Azure, а потім виконати [оновлення до ESET PROTECT](#).

Інсталяція компонентів у Windows

У багатьох сценаріях інсталяції передбачено встановлення різних компонентів ESET PROTECT на різних комп'ютерах, щоб пристосувати мережеві архітектури, дотриматися вимог щодо ефективності тощо. Для

окремих компонентів ESET PROTECT доступні вказані нижче пакети інсталяції.

Основні компоненти

- [Сервер ESET PROTECT](#)
- [Веб-консоль ESET PROTECT](#)
- [Агент ESET Management](#) (має бути інстальовано на клієнтських комп'ютерах, за бажанням також на сервері ESET PROTECT)

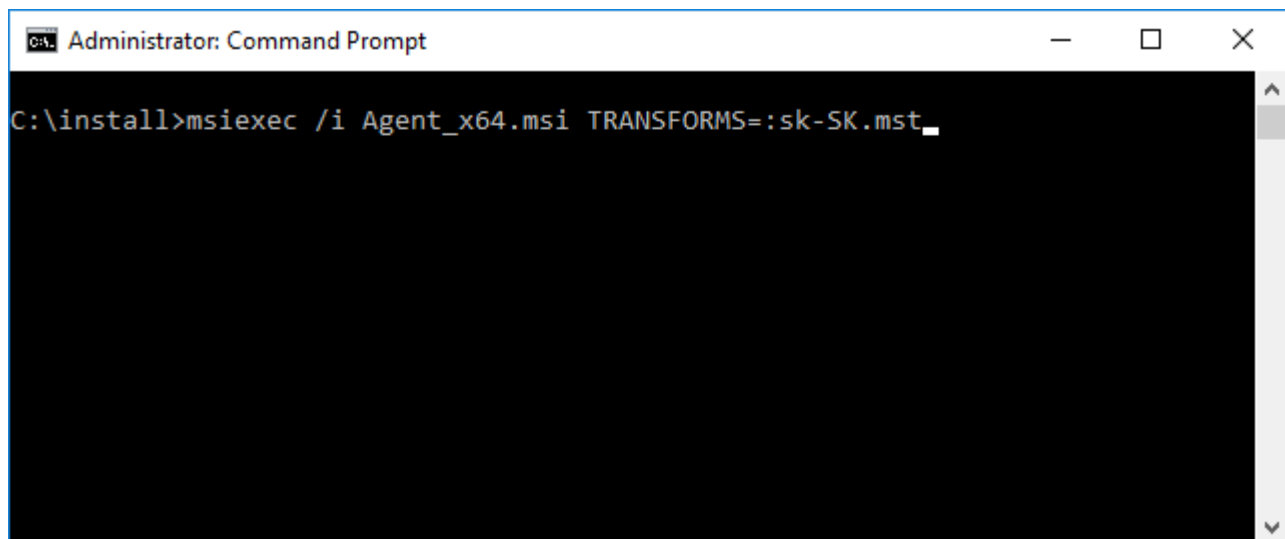
Додаткові компоненти

- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Проксі-сервер HTTP Apache](#)
- [Інструмент «Дзеркало»](#)

Інструкції з оновлення ERA до останньої версії ESET PROTECT 8.0 див. в нашій [статті бази знань](#).

Щоб запустити інсталяцію на власній мові, запустіть інсталятор MSI відповідного компонента ESET PROTECT за допомогою командного рядка.

Нижче наведено приклад запуску інсталяції словацькою:



```
Administrator: Command Prompt
C:\install>msiexec /i Agent_x64.msi TRANSFORMS=:sk-SK.mst_
```

Щоб вибрати мову інсталятора, вкажіть відповідний параметр TRANSFORMS відповідно до цієї таблиці:

Мова	Код
Англійська (США)	en-US
Арабська (Єгипет)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Latin)	hr-HR
Чеська (Чеська Республіка)	cs-CZ
Французька (Франція)	fr-FR
Французька (Канада)	fr-CA
Німецька (Німеччина)	de-DE
Грецька (Греція)	el-GR
Угорська (Угорщина)*	hu-HU
Індонезійська (Індонезія)*	id-ID
Італійська (Італія)	it-IT
Японська (Японія)	ja-JP
Корейська (Корея)	ko-KR
Польська (Польща)	pl-PL

Португальська (Бразилія)	pt-BR
Російська (Росія)	ru-RU
Іспанська (Чилі)	es-CL
Іспанська (Іспанія)	es-ES
Словацька (Словаччина)	sk-SK
Турецька (Туреччина)	tr-TR
Українська (Україна)	uk-UA

* Цією мовою доступний лише продукт; онлайн-довідка недоступна.

Інсталяція сервера

Щоб інстальовати сервер ESET PROTECT у Windows:

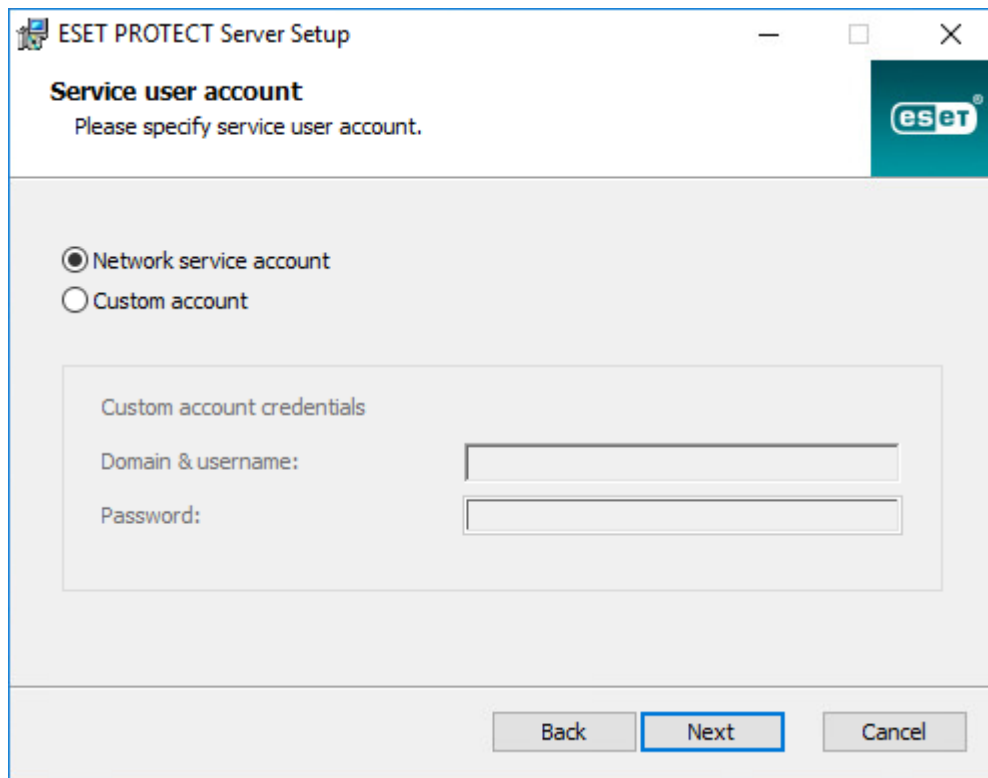
1. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інсталятор для цього компонента ESET PROTECT (server_x64.msi).
2. Переконайтеся, що всі [попередні вимоги](#) виконано.
3. Запустіть інсталятор сервера ESET PROTECT і прийміть ліцензійну угоду з кінцевим користувачем (якщо погоджуєтесь з її умовами).
4. Якщо ви не хочете надсилати в ESET звіти про аварійне завершення роботи та дані телеметрії, зніміть прапорець **Узяти участь у програмі покращення продукту**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET.
5. Не ставте прапорець біля пункту **Це інсталяція в кластері** та натисніть **Далі**. [Ви виконуєте інсталяцію в кластері?](#)



Увага

Якщо ви інстальовуєте сервер ESET PROTECT на відмовостійкий кластер, поставте прапорець біля пункту **Це інсталяція в кластері**. Укажіть **Настроюваний шлях до даних програми**, щоб вибрати спільне сховище для кластера. Дані повинні зберігатися в одному місці, доступ до якого мають всі вузли кластера.

6. Виберіть **Обліковий запис користувача служби**. Цей обліковий запис буде використовуватися для запуску сервера ESET PROTECT. Доступні наведені нижче опції.
 - **Обліковий запис мережевої служби**: виберіть цей параметр, щоб не використовувати домен.
 - **Власний обліковий запис** – укажіть облікові дані користувача домену: ДОМЕН / ІМ'Я КОРИСТУВАЧА та пароль.



7. Підключіться до бази даних. У ній зберігаються всі дані (пароль веб-консолі ESET PROTECT, журнали клієнтських комп'ютерів тощо):

- **База даних:** MySQL Server / MS SQL Server / MS SQL Server з використанням автентифікації Windows
- **ODBC драйвер:** драйвер MySQL ODBC 5.1 / драйвер MySQL ODBC 5.2 з підтримкою Юнікод / драйвер MySQL ODBC 5.3 з підтримкою Юнікод / драйвер MySQL ODBC 8.0 із підтримкою Юнікод / SQL Server / SQL Server Native Client 10.0 / драйвер ODBC 11 для SQL Server / драйвер ODBC 13 для SQL Server / драйвер ODBC 17 для SQL Server
- **Ім'я бази даних:** рекомендуємо використовувати попередньо встановлене ім'я або змінити його за необхідності.
- **Ім'я хоста:** ім'я хоста або IP-адреса сервера бази даних
- **Порт:** використовується для підключення до сервера бази даних
- **Ім'я користувача / пароль** облікового запису адміністратора бази даних
- **Використовувати екземпляр з іменем.** Якщо ви використовуєте базу даних MS SQL, можна також поставити прапорець **Використовувати екземпляр з іменем**. Це дасть змогу використовувати налаштований екземпляр бази даних, який можна налаштувати в полі «Ім'я хоста» у формі *HOSTNAME\INSTANCE*, наприклад: *192.168.0.10\ESMC7SQL*. Для кластерної бази даних використовуйте лише ім'я кластера. Якщо вибрати цю опцію, ви не зможете змінити порт, який використовуватиметься. Система використовуватиме порти за замовчуванням, визначені Microsoft.



Примітка

Поставивши прапорець **Використовувати екземпляр з іменем**, сервер ESET PROTECT можна також підключити до бази даних MS SQL, інсталюваної у відмовостійкому кластері. У полі **Ім'я хоста** введіть ім'я кластера.

The screenshot shows the 'Database server connection' window in the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. Below the title bar, the text reads 'Database server connection' and 'Please enter database server connection.' The ESET logo is in the top right corner. The form contains the following fields and options:

- Database: A dropdown menu with 'MS SQL Server' selected.
- ODBC driver: A dropdown menu with 'MS SQL Server' selected.
- Database name: A text box containing 'era_db'.
- Hostname: A text box containing 'localhost'.
- Use Named Instance: An unchecked checkbox.
- Port: A text box containing '1433'.
- Database account: A section with two empty text boxes for 'Username:' and 'Password:'.

At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.



Примітка

Сервер ESET PROTECT зберігає великі об'єкти даних у базі даних, тому для належної роботи ESET PROTECT потрібно налаштувати [MySQL для приймання пакетів великих розмірів](#).

На цьому кроці перевіряється ваше підключення до бази даних. Якщо підключення працює, перейдіть до наступного кроку.

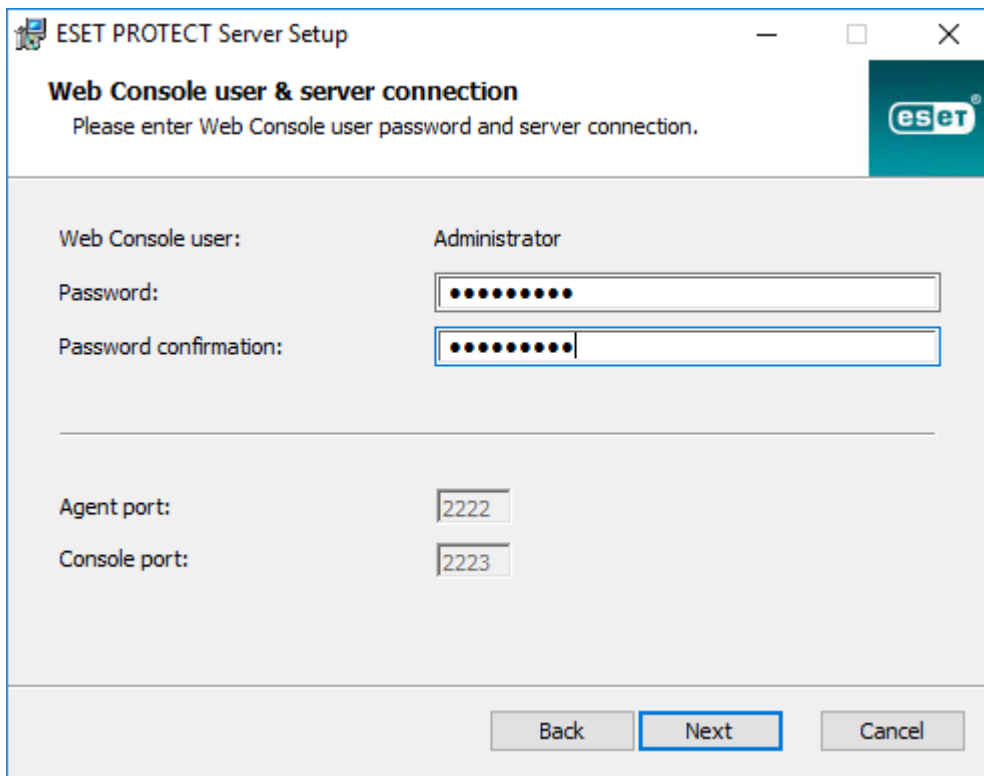
8. Виберіть користувача ESET PROTECT, який має доступ до бази даних. Ви можете використати наявного користувача або створити нового.

The screenshot shows the 'Database user for ESET PROTECT' window in the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. Below the title bar, the text reads 'Database user for ESET PROTECT' and 'Please enter database user for ESET PROTECT credentials.' The ESET logo is in the top right corner. The form contains the following options and fields:

- Radio buttons for 'Create new user' (selected) and 'Use existing user'.
- Database username: An empty text box.
- Password: An empty text box.
- Password confirmation: An empty text box.

At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

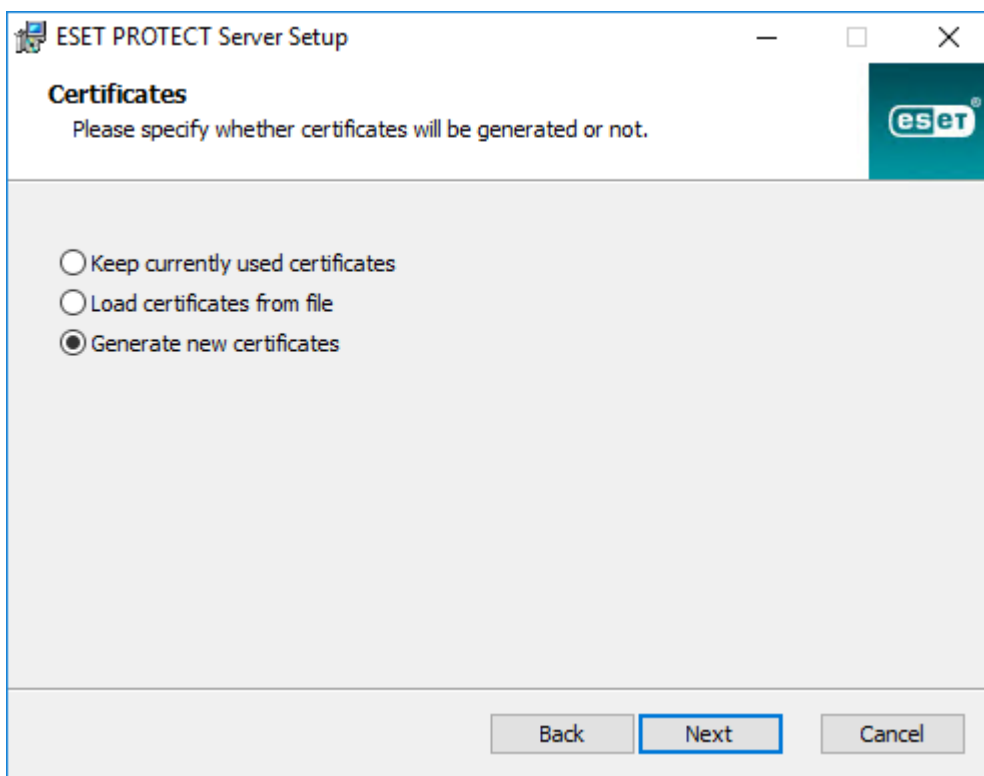
9. Введіть пароль для доступу до **веб-консолі**.



The screenshot shows the 'Web Console user & server connection' dialog box in the ESET PROTECT Server Setup application. The title bar reads 'ESET PROTECT Server Setup'. The main heading is 'Web Console user & server connection' with the instruction 'Please enter Web Console user password and server connection.' The ESET logo is in the top right corner. The dialog contains the following fields: 'Web Console user:' with the value 'Administrator'; 'Password:' and 'Password confirmation:' fields, both containing masked characters (dots); 'Agent port:' with the value '2222'; and 'Console port:' with the value '2223'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

10. ESET PROTECT використовує сертифікати для зв'язку між клієнтом і сервером. Виберіть одну з указаних нижче опцій.

- **Не змінювати поточні сертифікати:** цей параметр доступний, тільки якщо база даних уже використовувалася з іншим ESET PROTECT Server раніше.
- **Завантажувати сертифікати з файлу:** виберіть наявний сертифікат сервера й центр сертифікації.
- **Створювати нові сертифікати:** інсталятор генеруватиме нові сертифікати.

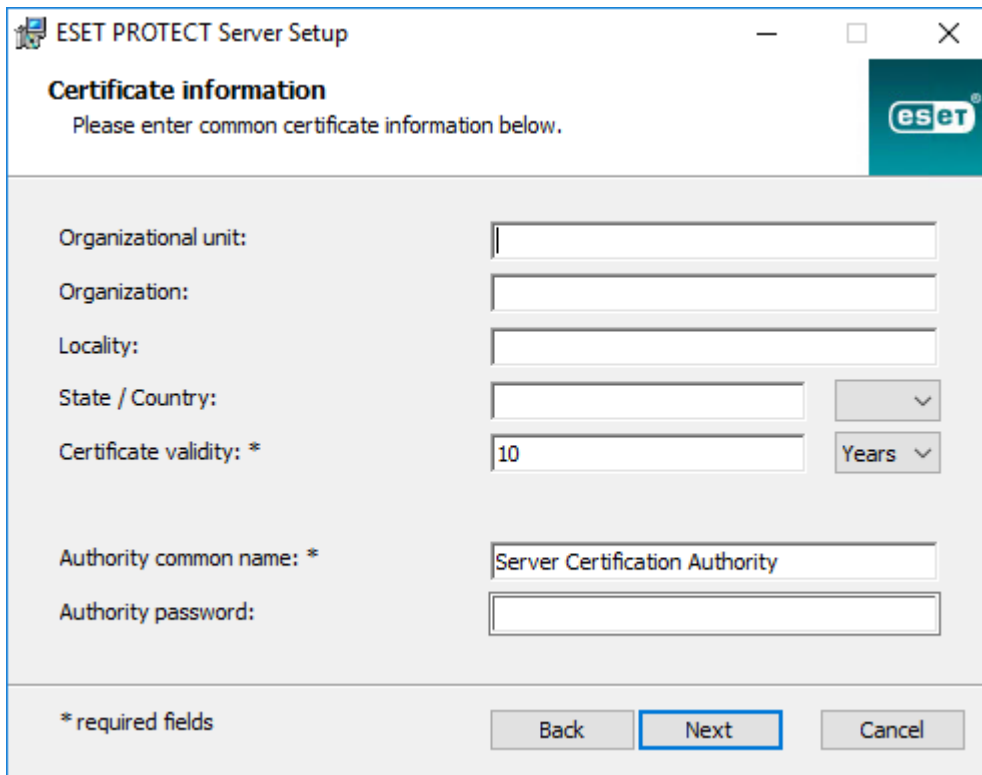


The screenshot shows the 'Certificates' dialog box in the ESET PROTECT Server Setup application. The title bar reads 'ESET PROTECT Server Setup'. The main heading is 'Certificates' with the instruction 'Please specify whether certificates will be generated or not.' The ESET logo is in the top right corner. The dialog contains three radio button options: 'Keep currently used certificates', 'Load certificates from file', and 'Generate new certificates' (which is selected). At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

11. Виконайте інструкцію цього кроку, якщо на попередньому кроці було вибрано **Створювати нові**

сертифікати.

а) Укажіть додаткову інформацію про сертифікати (необов'язково). Якщо ви введете пароль у полі **Пароль центра**, запам'ятайте його.



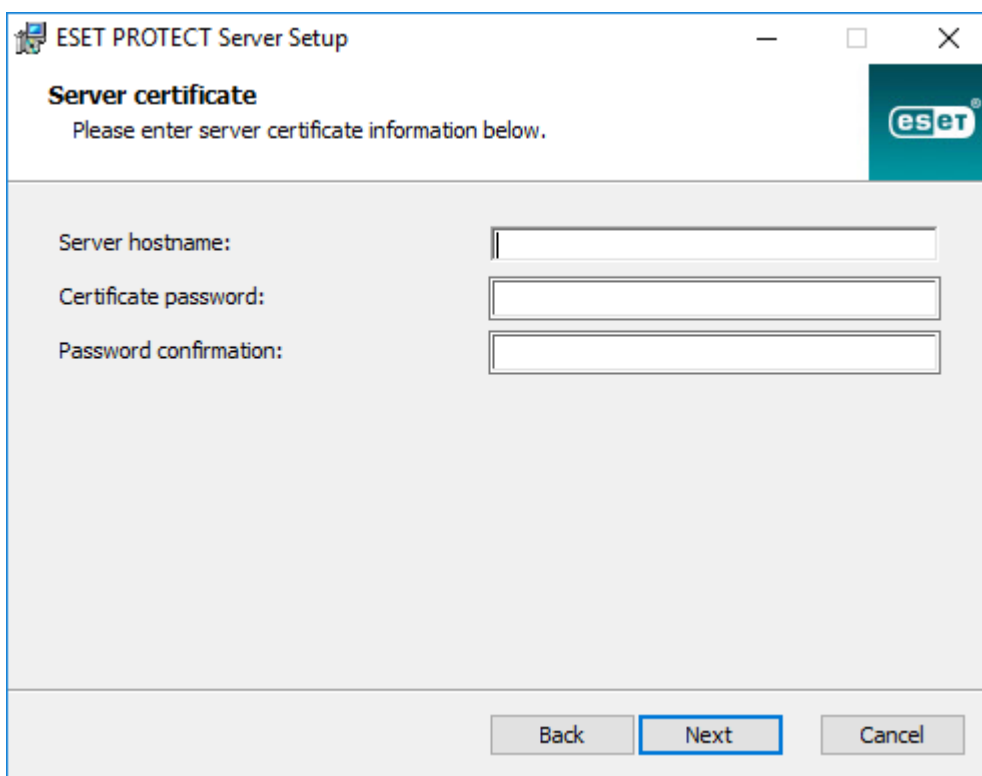
The screenshot shows the 'Certificate information' dialog box in the ESET PROTECT Server Setup application. The title bar reads 'ESET PROTECT Server Setup'. The main heading is 'Certificate information' with the instruction 'Please enter common certificate information below.' and the ESET logo in the top right corner. The dialog contains several input fields: 'Organizational unit:', 'Organization:', 'Locality:', 'State / Country:' (with a dropdown arrow), 'Certificate validity: *' (with a value of '10' and a 'Years' dropdown), 'Authority common name: *' (with the value 'Server Certification Authority'), and 'Authority password:'. At the bottom left, there is a note '* required fields'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

б) У полі **Сертифікат сервера** уведіть **Ім'я хоста сервера** й **Пароль сертифіката** (необов'язково).



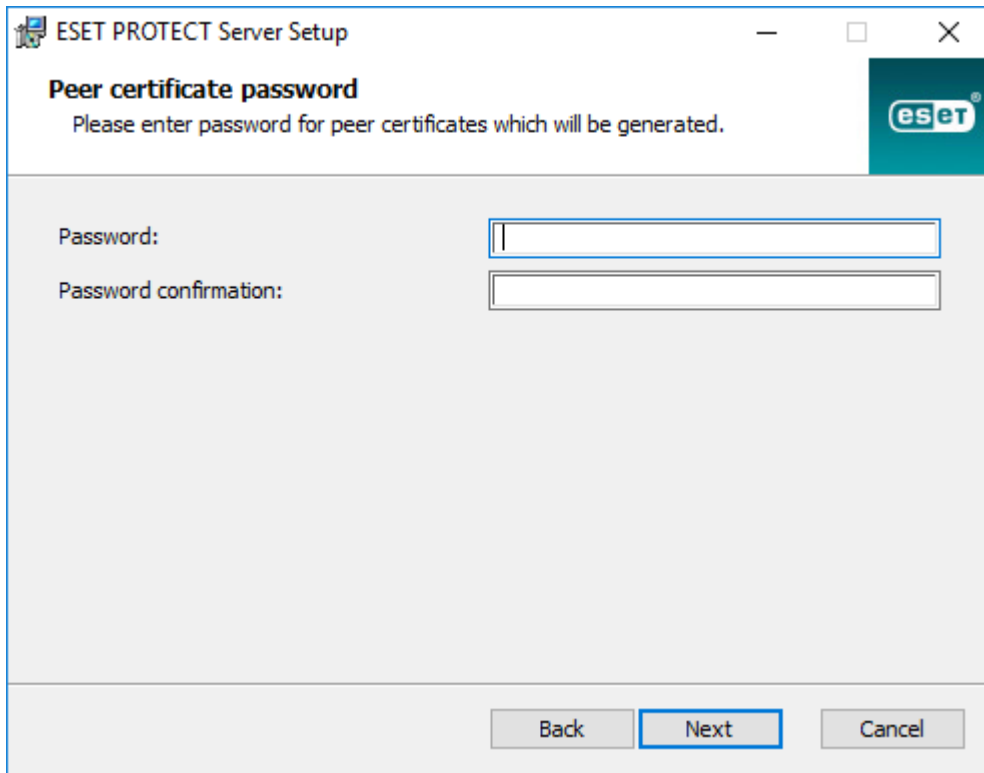
Попередження

У полі **Ім'я хоста сервера** в сертифікаті сервера заборонено використовувати такі ключові слова: server, proxy, agent.



The screenshot shows the 'Server certificate' dialog box in the ESET PROTECT Server Setup application. The title bar reads 'ESET PROTECT Server Setup'. The main heading is 'Server certificate' with the instruction 'Please enter server certificate information below.' and the ESET logo in the top right corner. The dialog contains three input fields: 'Server hostname:', 'Certificate password:', and 'Password confirmation:'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

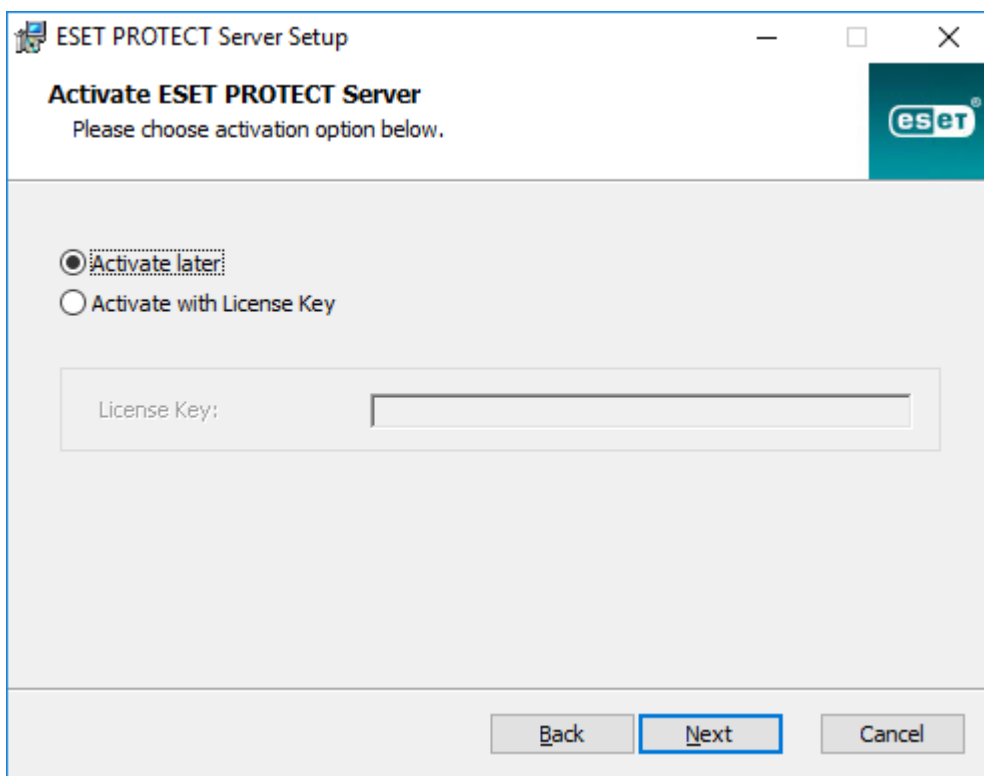
с) У полі **Пароль сертифіката однорангового вузла** введіть пароль для сертифікатів однорангових вузлів агента й проксі-сервера.



The screenshot shows the 'Peer certificate password' step of the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. The main heading is 'Peer certificate password' with the instruction 'Please enter password for peer certificates which will be generated.' Below this, there are two text input fields: 'Password:' and 'Password confirmation:'. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

12. Під час налаштування можна виконати початкове завдання [синхронізації статичної групи](#). Виберіть метод (**Не синхронізувати, Синхронізувати з мережею Windows, Синхронізувати з Active Directory**) і натисніть **Далі**.

13. Введіть дійсний [ліцензійний ключ](#) або виберіть **Активувати пізніше**.



The screenshot shows the 'Activate ESET PROTECT Server' step of the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. The main heading is 'Activate ESET PROTECT Server' with the instruction 'Please choose activation option below.' Below this, there are two radio button options: 'Activate later:' (which is selected) and 'Activate with License Key'. Below the radio buttons, there is a text input field labeled 'License Key:'. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

14. Підтвердьте або змініть папку для інсталяції сервера та натисніть **Далі**.

15. Виберіть **Інсталювати**, щоб інсталювати сервер ESET PROTECT.



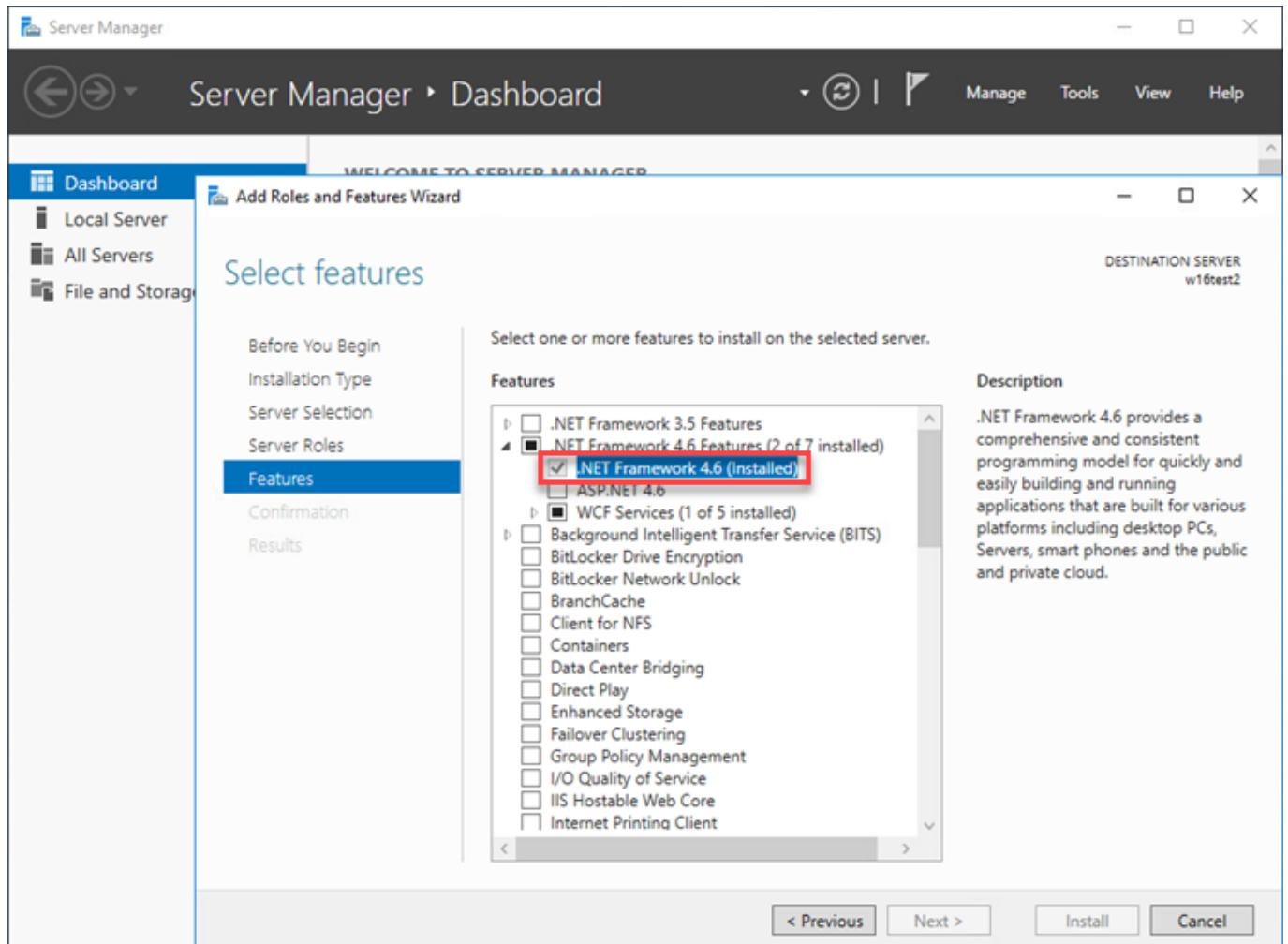
Примітка

Після інсталяції сервера ESET PROTECT на той самий комп'ютер можна інсталювати [агента ESET Management](#) (необов'язково). Завдяки цьому ви зможете керувати сервером, як керуєте клієнтським комп'ютером.

Попередні вимоги до сервера - Windows

Для інсталяції ESET PROTECT Server у Windows мають бути виконані такі попередні вимоги:

- Необхідно мати дійсну [ліцензійний ключ](#).
- Необхідно мати [підтримувану операційну систему Windows](#).
- Необхідні порти мають бути відкриті й доступні (переглянути їх повний перелік можна [тут](#)).
- [Підтримувані сервер бази даних і з'єднувач \(Microsoft SQL Server або MySQL\)](#) мають бути інсталювані та запущені. Рекомендуємо переглянути вказівки з налаштування бази даних ([Microsoft SQL Server](#) або [MySQL](#)), щоб задати належну конфігурацію для використання з ESET PROTECT. Щоб налаштувати базу даних і користувача бази даних для MS SQL та MySQL, перегляньте нашу [статтю бази знань](#).
- [Інсталювано веб-консоль ESET PROTECT](#), щоб керувати сервером ESET PROTECT.
- Має бути інсталювано Microsoft .NET Framework 4. Відповідний пакет можна інсталювати за допомогою **майстра додавання ролей і функцій** (як показано нижче). Фреймворк .NET вимагається лише для інсталяції MS SQL Server Express.



Вимоги до Microsoft SQL Server

Потрібно дотримуватися вказаних нижче вимог до Microsoft SQL Server.

- Інсталюйте [підтримувану версію Microsoft SQL Server](#). Під час інсталяції виберіть **змішаний режим**

автентифікації.

- Якщо у вас уже інстальовано Microsoft SQL Server, виберіть для автентифікації значення **Змішаний режим (автентифікація SQL Server та Windows)**. Для цього виконайте вказівки з цієї [статті бази знань](#). Якщо ви хочете використовувати для входу в Microsoft SQL Server **автентифікацію Windows**, виконайте дії з [цієї статті бази знань](#).
- Дозвольте підключення TCP/IP до сервера SQL Server. Для цього виконайте дії з розділу **II. Дозвіл на підключення TCP/IP до бази даних SQL** [цієї статті бази знань](#).



Примітка

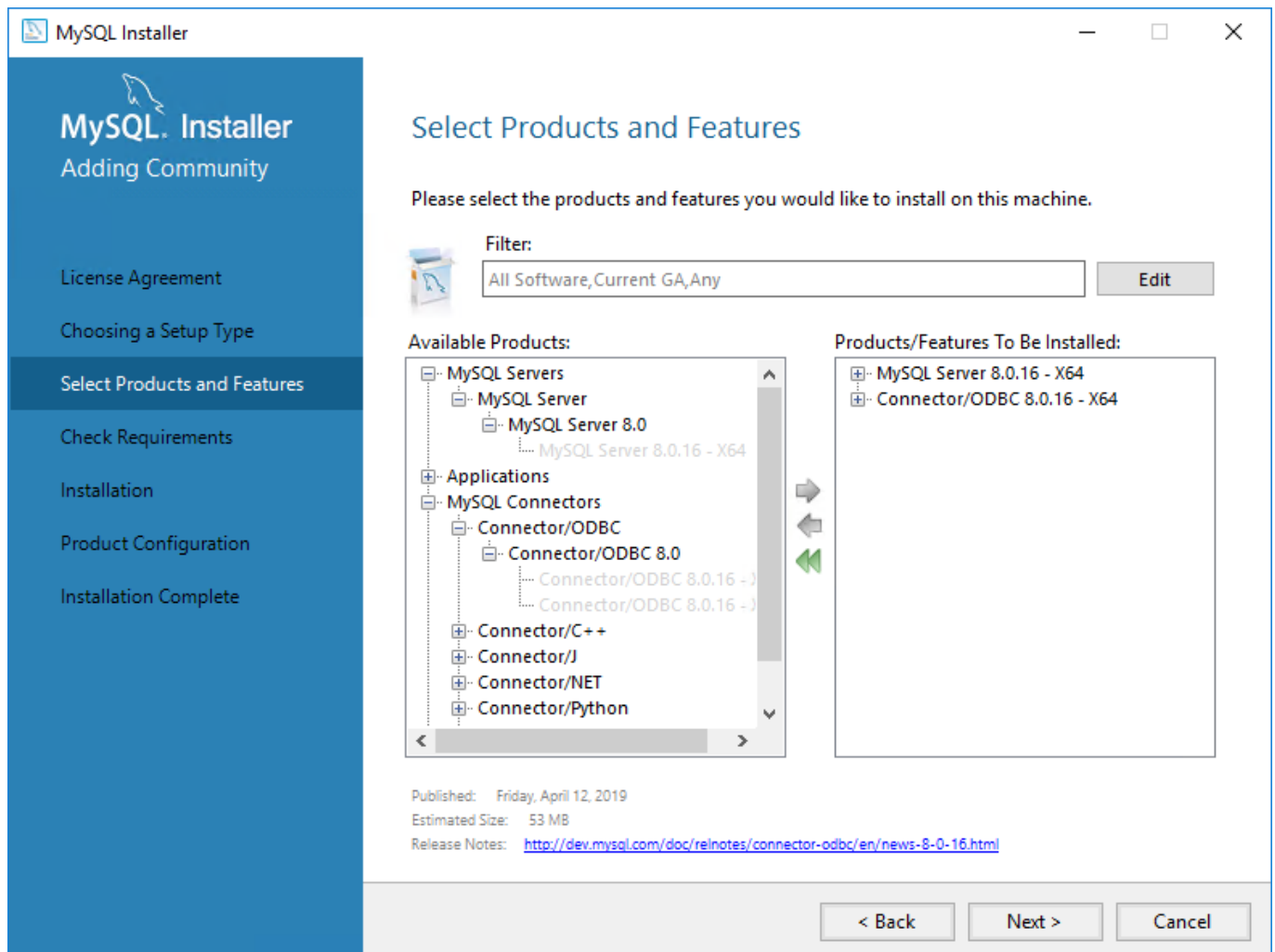
- Щоб налаштувати Microsoft SQL Server та керувати цим сервером (бази даних і користувачі), [завантажте SQL Server Management Studio \(SSMS\)](#).
- Рекомендуємо [не інстальювати SQL Server в контролері домену](#) (наприклад, якщо ви використовуєте Windows SBS / Essentials). Рекомендуємо інстальювати ESET PROTECT на іншому сервері або не вибирати компонент SQL Server Express під час інсталяції (щоб запустити базу даних ESET PROTECT, потрібно скористатися наявним сервером SQL Server або MySQL Server).

Інсталяція та конфігурація сервера MySQL

Інсталяція

Обов'язково інстальюйте [підтримувану версію MySQL Server та з'єднувача ODBC](#).

1. Завантажте інсталятор MySQL 8 для Windows зі сторінки <https://dev.mysql.com/downloads/installer/> та запустіть його.
2. Під час налаштування інсталяції виберіть **Вибіркова**, а потім – **Сервер MySQL і З'єднувач ODBC**. Переконайтеся, що в з'єднувача ODBC та сервера MySQL однакова розрядність (x86 або x64).



3. Виконайте інсталяцію сервера MySQL.

Конфігурація

1. Відкрийте цей файл у текстовому редакторі:

`C:\ProgramData\MySQL\MySQL Server 8.0\my.ini`

2. Знайдіть указану нижче конфігурацію та змініть чи додайте її в розділ `[mysqld]` файлу **my.ini**.

```
max_allowed_packet=33M
```

- Для MySQL 8 потрібно задати таку змінну:

```
o log_bin_trust_function_creators=1
```

Окрім цього, можна вимкнути ведення бінарного журналу: `log_bin=0`

- Для MySQL 5.6.20 і 5.6.21 (щоб визначити версію MySQL, скористайтеся `mysql --version`):

одля параметра `innodb_log_file_size` потрібно вказати значення не менше ніж **200 МБ** (наприклад, `innodb_log_file_size=200M`) і не більше ніж **3000 МБ**

- Для MySQL 5.6.22 й новіших підтримуваних версій (зокрема, версії 8):

одля параметра `innodb_log_file_size*innodb_log_files_in_group` потрібно вказати значення не менше ніж **200 МБ** (символ `*` позначає множення, і результат множення двох параметрів має бути більший ніж 200 МБ. Мінімальне значення для `innodb_log_files_in_group` - 2, а максимальне - 100. Значення має бути цілим числом).

Приклад:

```
innodb_log_file_size=100M
```

```
innodb_log_files_in_group=2
```

3. Збережіть і закрийте файл **my.ini**.

4. Щоб перезавантажити сервер MySQL і застосувати конфігурацію (назва процесу залежить від версії MySQL: 8.0 = `mysql80` тощо), відкрийте командний рядок і введіть у ньому такі команди:

```
net stop mysql80
```

```
net start mysql80
```

5. Щоб перевірити, чи сервер MySQL працює, введіть таку команду в командному рядку:

```
sc query mysql80
```

Спеціальний обліковий запис користувача бази даних

Якщо ви не бажаєте використовувати **обліковий запис SA** (MS SQL) або **обліковий запис root** (MySQL), то можете створити **спеціальний обліковий запис користувача бази даних**. Цей обліковий запис використовуватиметься лише для доступу до бази даних ESET PROTECT. Рекомендується створити спеціальний обліковий запис користувача на сервері баз даних перед початком інсталяції ESET PROTECT. Крім того, вам знадобиться створити порожню базу даних для використання ESET PROTECT з цим обліковим записом.



Примітка

- Існує мінімальний набір прав, які необхідно надати **спеціальному обліковому запису користувача бази даних**.
- Докладну інструкцію з налаштування бази даних і користувача для MS SQL та MySQL див. у [статті бази знань](#).

- Права користувача MySQL:

ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER - для отримання додаткової інформації про привілеї MySQL див.
<http://dev.mysql.com/doc/refman/8.0/en/grant.html>.

- Ролі на рівні бази даних Microsoft SQL Server:
 Користувач бази даних ESET PROTECT має мати роль **db_owner**. Для отримання додаткової інформації про ролі на рівні бази даних Microsoft SQL Server див.
<https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx>

Інсталяція агента

Доступні методи

Існують різні методи інсталяції та розгортання для агента ESET Management на робочих станціях з ОС Windows:

Метод	Документація	Опис
Встановлення за допомогою графічного інтерфейсу інсталятора .msi	<ul style="list-style-type: none"> • Ця глава • КБ 	<ul style="list-style-type: none"> • Стандартний метод інсталяції • Цей метод можна використовувати для інсталяції з використанням сервера або в автономному режимі. • Використовуйте цей метод для інсталяції агента на комп'ютер із сервером ESET PROTECT.
ESET Remote Deployment Tool	<ul style="list-style-type: none"> • Онлайн-довідка 	<ul style="list-style-type: none"> • Рекомендовано для масового розгортання через локальну мережу. • Може використовуватися для розгортання універсального інсталятора (агент + продукт ESET для захисту)
Універсальний інсталятор агента	<ul style="list-style-type: none"> • Створіть універсальний інсталятор агента • КБ 	<ul style="list-style-type: none"> • В інсталятор також можуть входити продукт для захисту та вбудована політика. • Розмір інсталятора складає кілька сотень мегабайт.
Агент Live Installer	<ul style="list-style-type: none"> • Створити Агент Live Installer • КБ 	<ul style="list-style-type: none"> • Інсталятор – це виконуваний скрипт. Він має невеликий розмір, але йому потрібен доступ до місця збереження інсталятора <i>.msi</i>. • Скрипт можна змінити таким чином, щоб він використовував локальний інсталятор і проксі-сервер HTTP.
Розгортання SCCM і GPO	<ul style="list-style-type: none"> • SCCM • GPO • КБ 	<ul style="list-style-type: none"> • Удосконалений метод віддаленого масового розгортання. • За допомогою невеликого файлу <i>.ini</i>.
Завдання сервера – розгортання агента	<ul style="list-style-type: none"> • Онлайн-довідка • КБ 	<ul style="list-style-type: none"> • Альтернатива SCCM та GPO. • Не працює через проксі-сервер HTTP. • Запускається сервером ESET PROTECT з веб-консолі ESET PROTECT.



Увага

Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT, для якого потрібна автентифікація, не працюватиме. Якщо ви не виберете порт для веб-консолі або агента за замовчуванням, можливо, потрібно буде налаштувати брандмауер відповідним чином. В іншому разі інсталяція може закінчитися невдало.

Інсталяція за допомогою графічного інтерфейсу

Для локальної інсталяції агента ESET Management у Windows виконайте вказані нижче дії.

1. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інсталятор для цього компонента ESET PROTECT (agent_x86.msi або agent_x64.msi).
2. Запустіть інсталятор агента ESET Management і прийміть ліцензійну угоду з кінцевим користувачем (якщо погоджуєтеся з її умовами).
3. Якщо ви не хочете надсилати в ESET звіти про аварійне завершення роботи та дані телеметрії, зніміть прапорець **Узяти участь у програмі покращення продукту**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET.
4. Введіть **хост сервера** (ім'я хоста або IP-адресу сервера ESET PROTECT) і **порт сервера** (порт за замовчуванням – 2222; якщо ви використовуєте інший порт, укажіть його).



Увага!

Переконайтесь, що **Хост сервера** відповідає принаймні одному зі значень (в ідеалі – FQDN), визначених у полі **Хост** пункту **Сертифікат сервера**. В іншому разі відобразиться помилка «Отримано недійсний сертифікат сервера». У полі «Хост» пункту «Сертифікат сервера» може використовуватися символ узагальнення (*). Це означає, що сертифікат буде працювати з будь-яким **Хостом сервера**.

5. Якщо ви використовуєте проксі-сервер для підключення між агентом і сервером, установіть прапорець біля пункту **Використовувати проксі-сервер**. У цьому разі інсталятор продовжить [інсталяцію в автономному режимі](#).



Примітка

Цей параметр проксі-сервера використовується лише для реплікації між агентом ESET Management і сервером ESET PROTECT, а не для кешування оновлень.

- **Ім'я хоста проксі-сервера:** ім'я хоста або IP-адреса комп'ютера, де розміщено проксі-сервер HTTP.
- **Порт проксі-сервера:** за замовчуванням це 3128.
- **Ім'я користувача, пароль:** введіть облікові дані проксі-сервера (якщо використовується автентифікація).

Параметри проксі-сервера можна змінити пізніше в [політиці](#). [Проксі-сервер](#) має бути інстальовано до налаштування підключення «агент – сервер» через проксі-сервер.

6. Виберіть один із наступних варіантів інсталяції та виконайте відповідні кроки:

[Інсталяція із сервера](#). Для цього потрібно вказати облікові дані адміністратора веб-консолі ESET PROTECT. Інсталятор автоматично завантажить необхідні сертифікати.

[Інсталяція в автономному режимі](#). Для цього потрібно надати сертифікат агента та вказати Центр сертифікації. Ці дані можна [експортувати](#) з ESET PROTECT. Замість нього можна використати [налаштовуваний сертифікат](#).

Інсталяція через командний рядок

Інсталятор MSI можна запустити локально або віддалено. Завантажте агент ESET Management із [веб-сайту ESET](#).

Параметр	Опис і дозволених значення
P_HOSTNAME=	IP-адреса або ім'я хоста сервера ESET PROTECT.
P_PORT=	Порт сервера для з'єднання з агентом (необов'язково; за замовчуванням використовується порт 2222).
P_CERT_PATH=	Шлях до сертифіката агента у форматі Base64 у файлі .txt (експорт із веб-консолі ESET PROTECT).
P_CERT_AUTH_PATH=	Шлях до Центру сертифікації у форматі Base64 у файлі .txt (експорт із веб-консолі ESET PROTECT).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	YES . Використовуйте цей параметр, коли посилаєтеся на сертифікат агента та Центр сертифікації, що зберігаються у файлах .txt.

P_CERT_PASSWORD=	За допомогою цього параметра можна вказати пароль сертифіката агента.
P_CERT_CONTENT=	Рядок сертифіката агента у форматі Base64 (експорт із веб-консолі ESET PROTECT).
P_CERT_AUTH_CONTENT=	Рядок Центру сертифікації у форматі Base64 (експорт із веб-консолі ESET PROTECT).
P_ENABLE_TELEMETRY=	0 – вимкнено (за замовчуванням); 1 – увімкнено. Надсилання звітів про аварійне завершення роботи та телеметричних даних до ESET (необов'язковий параметр).
P_INSTALL_MODE_EULA_ONLY=	1 . Використовуйте цей параметр для напівавтоматичної інсталяції агента ESET Management. Перед вами відкриється вікно інсталяції агента, у якому вам буде запропоновано прийняти Ліцензійну угоду з Кінцевим Користувачем і ввімкнути/вимкнути телеметрію (P_ENABLE_TELEMETRY ігнорується за відповідного налаштування). Інші параметри інсталяції агента збігаються з параметрами інсталяції через командний рядок. Ви можете переглянути перебіг інсталяції агента.
P_USE_PROXY=	1 . Використовуйте цей параметр, щоб використовувати протокол HTTP (уже інстальований у вашій мережі) для реплікації між агентом ESET Management і сервером ESET PROTECT (а не для кешування оновлень).
P_PROXY_HTTP_HOSTNAME=	IP-адреса або ім'я хоста проксі-сервера HTTP.
P_PROXY_HTTP_PORT=	Порт проксі-сервера HTTP для з'єднання з агентом.

Приклади інсталяції через командний рядок

Замініть виділений оранжевим код необхідними даними.

- Автоматична інсталяція (параметр /q) з підключенням до порту за замовчуванням, увімкненою телеметрією та збереженими у файлах сертифікатом агента й Центром сертифікації:

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- Автоматична інсталяція з рядками сертифіката агента та Центру сертифікації, а також паролем сертифіката агента й параметрами проксі-сервера HTTP:

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=C3Fxtf1kZq12KA19P48HymBha3CkKw P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvkpqayzJJZhSY8qsw00Y3koZ1hvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- Напівавтоматична інсталяція:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

Інсталяція агента з використанням сервера

Щоб завершити **інсталяцію агента з використанням сервера**, виконайте наведені нижче кроки.

1. Введіть ім'я хоста або IP-адресу веб-консолі ESET PROTECT (такі самі, як у сервера ESET PROTECT) у полі **Хост сервера**. Якщо ви не використовуєте інший порт, залиште в полі **Порт веб-консолі** значення за замовчуванням (порт 2223). Крім того, введіть облікові дані веб-консолі в поля **Ім'я користувача та Пароль**.



Увага

Переконайтесь, що **Хост сервера** відповідає принаймні одному зі значень (в ідеалі – FQDN), визначених у полі **Хост** пункту **Сертифікат сервера**. В іншому разі відобразиться помилка «Отримано недійсний сертифікат сервера». У полі «Хост» пункту «Сертифікат сервера» може використовуватися символ узагальнення (*). Це означає, що він буде працювати з будь-яким **Хостом сервера**.

2. Коли з'явиться запит прийняти сертифікат, натисніть **Так**.
3. Виберіть **Не створювати комп'ютер** або **Вибрати настроювану статичну групу**. Якщо натиснути **Вибрати настроювану статичну групу**, ви зможете вибрати необхідну статичну групу зі списку

наявних у ESET PROTECT. Комп'ютер буде додано до вибраної групи.

4. Укажіть папку призначення для агента ESET Management (рекомендується використовувати розташування за замовчуванням), натисніть **Далі** > **Інсталювати**.

Інсталяція агента в автономному режимі

Щоб продовжити **інсталяція агента в автономному режимі**, виконайте наведені нижче кроки.

1. Якщо в попередньому кроці ви вибрали пункт **Проксі-сервер**, укажіть **Ім'я хоста проксі-сервера**, **Порт проксі-сервера** (за замовчуванням: 3128), **Ім'я користувача** та **Пароль** і натисніть кнопку **Далі**.
2. Натисніть **Огляд** і перейдіть до папки, у якій розташовано цей сертифікат (це сертифікат агента, експортований з ESET PROTECT). Не заповнюйте поле **Пароль сертифіката**, оскільки для цього сертифіката пароль не потрібний. Крім того, не потрібно шукати **центр сертифікації**. Залиште це поле порожнім.



Примітка

Якщо ви створили налаштовуваний сертифікат з ESET PROTECT (замість сертифікатів за замовчуванням, автоматично згенерованих під час інсталяції ESET PROTECT), використовуйте саме його.



Попередження

Парольна фраза сертифіката не може містити такі символи: " \ Ці символи спричиняють критичну помилку під час ініціалізації агента.

3. Щоб інсталювати програму в папку за замовчуванням, клацніть **Далі**. Щоб вибрати іншу папку (рекомендується використовувати папку за замовчуванням), клацніть **Змінити**.

Видалення агента й виправлення неполадок

Агент ESET Management можна видалити кількома способами.

Віддалене видалення за допомогою веб-консолі ESET PROTECT

1. [Виконайте вхід у веб-консоль ESET PROTECT](#).
2. У розкривному меню **Комп'ютери** виберіть комп'ютер, з якого необхідно видалити агент ESET Management, і натисніть **Створити завдання**.
Ви також можете вибрати кілька комп'ютерів, встановивши відповідні прапорці, і натиснути **Дії** > **Створити завдання**.
3. Введіть **назву** завдання.
4. У розкривному меню **Категорія завдання** виберіть опцію ESET PROTECT.
5. У розкривному меню **Завдання** виберіть опцію **Припинити керування (Видалити агент ESET Management)**.
6. Перевірте **зведення** завдання й натисніть «Готово».

Після цього буде автоматично створено тригер, який буде виконано якомога швидше. Щоб змінити **Тип тригера**, натисніть завдання клієнта в меню **Завдання** та виберіть **Відомості** > **Тригери**. Після цього натисніть необхідний тригер і виберіть **Редагувати**.



Примітка

Див. [Завдання клієнта](#) в посібнику з адміністрування.

Локальне видалення

1. Підключіться до комп'ютера робочої станції, з якого потрібно видалити агент ESET Management

(наприклад, через RDP).

2. Виберіть **Панель управління > Програми та функції** й двічі натисніть **агента ESET Management**.
3. Виберіть **Далі > Видалити** та дотримуйтесь інструкцій із видалення.



Увага

Якщо ви встановили пароль за допомогою політики агентів ESET Management, введіть його під час видалення. Крім того, перед видаленням агента ESET Management необхідно видалити політику.

Виправлення неполадок під час видалення агента ESET Management

- Див. [файли журналу](#) агента ESET Management.
- Ви можете видалити агент ESET Management за допомогою [Засобу видалення ESET](#) або скористатися нестандартним способом (наприклад, видалити необхідні файли, службу агента ESET Management та записи реєстру). Якщо на цьому самому комп'ютері встановлено продукт ESET для робочих станцій, ви не зможете здійснити видалення через [увімкнену функцію самозахисту](#).

ESET Remote Deployment Tool

ESET Remote Deployment Tool дозволяє в зручний спосіб розповсюдити [пакет інстальатора](#), створений ESET PROTECT для віддаленого розгортання ESET Management Agent і продуктів безпеки ESET на комп'ютерах у мережі.

Інструмент ESET Remote Deployment Tool доступний безкоштовно на [веб-сайті](#) ESET як автономний компонент ESET PROTECT. Інструмент для розгортання призначено в основному для розгортання в малих і середніх мережах та виконується з правами адміністратора.



Примітка

Інструмент ESET Remote Deployment Tool призначено для розгортання агента ESET Management на клієнтських комп'ютерах тільки з [підтримуваними](#) операційними системами Microsoft Windows.

Більш детальну інформацію про попередні вимоги для інсталяції й особливості використання цього інструмента див. у розділі [ESET Remote Deployment Tool](#).

Інсталяція веб-консолі

Є два способи інсталювати веб-консоль ESET PROTECT у Windows:

- [Використання універсального інстальатора](#) (рекомендований метод)
- Досвідчені користувачі можуть виконати [ручну інсталяцію](#)

Інсталяція веб-консолі з використанням універсального інстальатора

Порядок інсталяції компонента ESET PROTECT Web Console з використанням універсального інстальатора

1. Переконайтеся, що перелічені нижче попередні вимоги виконано:

- Інстальовано сервер ESET PROTECT.



Примітка

Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на [різні комп'ютери](#).

- Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.



Примітка

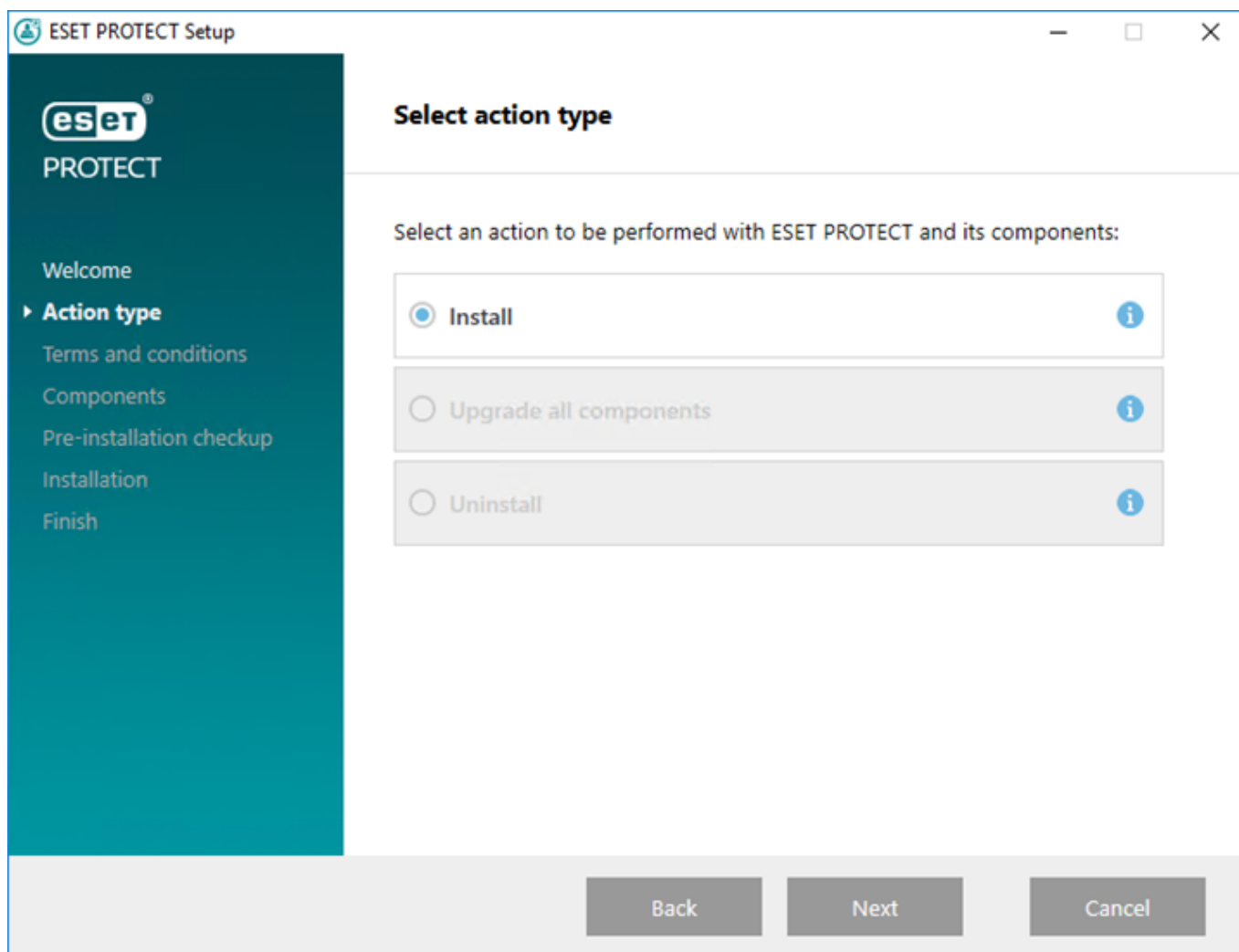
Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримування версія – Java 8)) і залишити лише останню версію Java.



Попередження

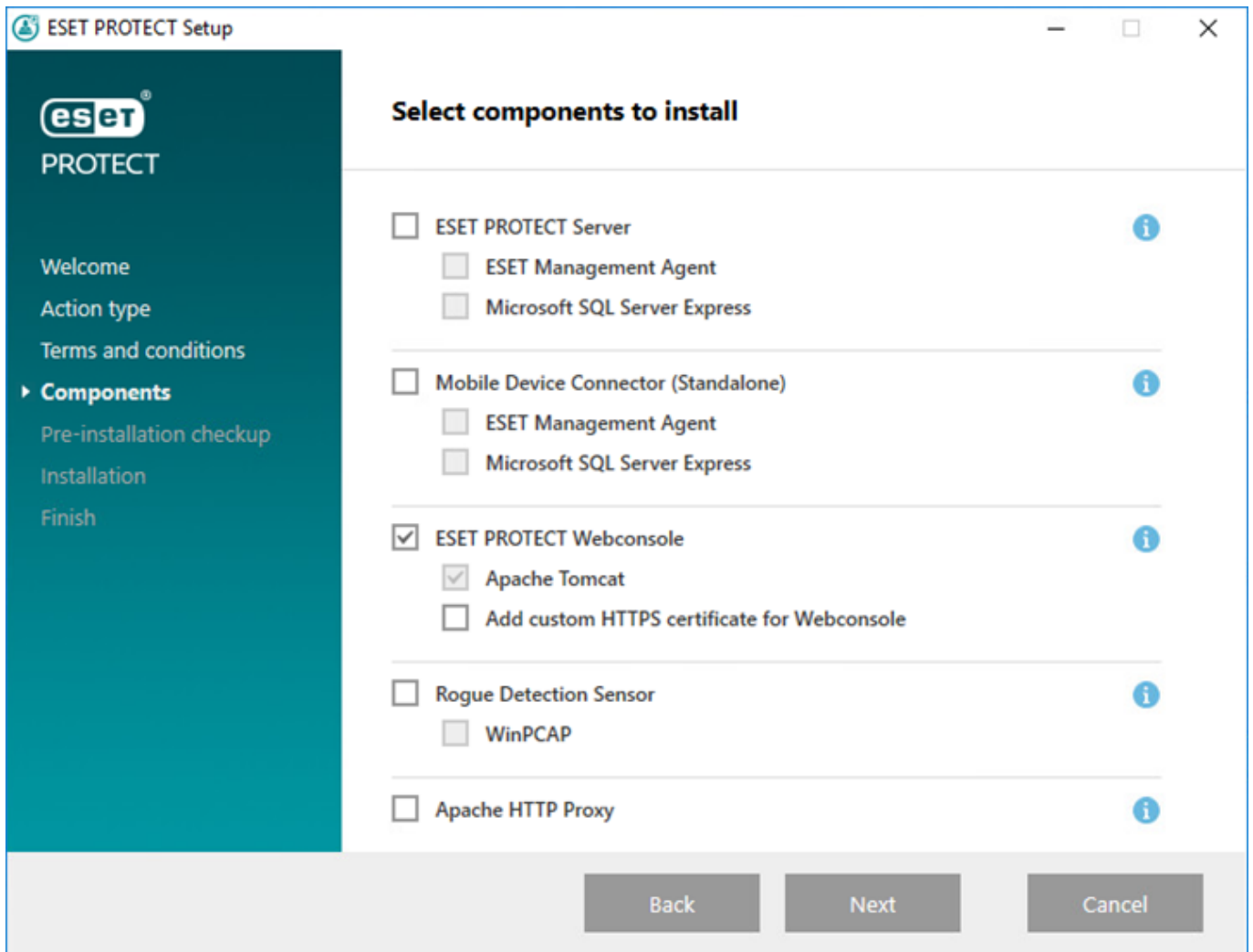
Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інстальувати один із підтримуваних випусків Java.

2. Завантажте [універсальний інстальатор ESET PROTECT](#) з веб-сайту ESET і розархівуйте завантажений файл.
3. Щоб інстальувати останню версію Apache Tomcat за умови, коли універсальний інстальатор містить старішу версію Apache Tomcat (цей крок не є обов'язковим; перейдіть до кроку 4, якщо вам не потрібна остання версія Apache Tomcat):
 - a. Відкрийте папку x64 і перейдіть у папку *installers*.
 - b. Видаліть файл `apache-tomcat-9.0.x-windows-x64.zip`, розташований у папці *installers*.
 - c. Завантажте ZIP-пакет 64-розрядної версії Apache Tomcat 9 [для Windows](#).
 - d. Перемістіть завантажений ZIP-пакет у папку *installers*.
4. Щоб запустити універсальний інстальатор, двічі клацніть файл **Setup.exe** й натисніть клавішу **Далі** на екрані **привітання**.
5. Виберіть **Інстальувати** й натисніть **Далі**.



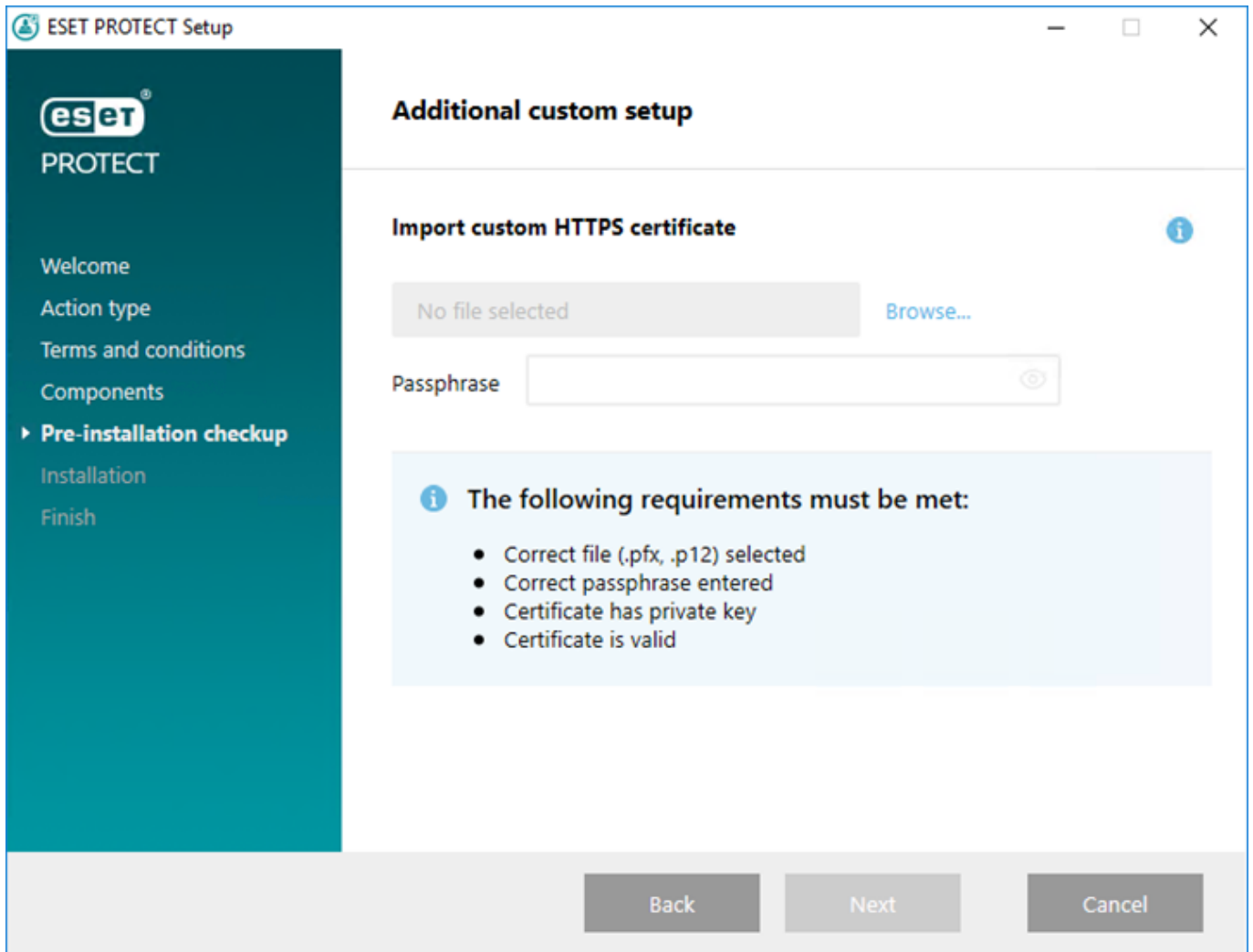
6. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

7. У розділі **Виберіть компоненти для інсталяції** установіть прапорець **ESET PROTECT Webconsole** і клацніть **Далі**.



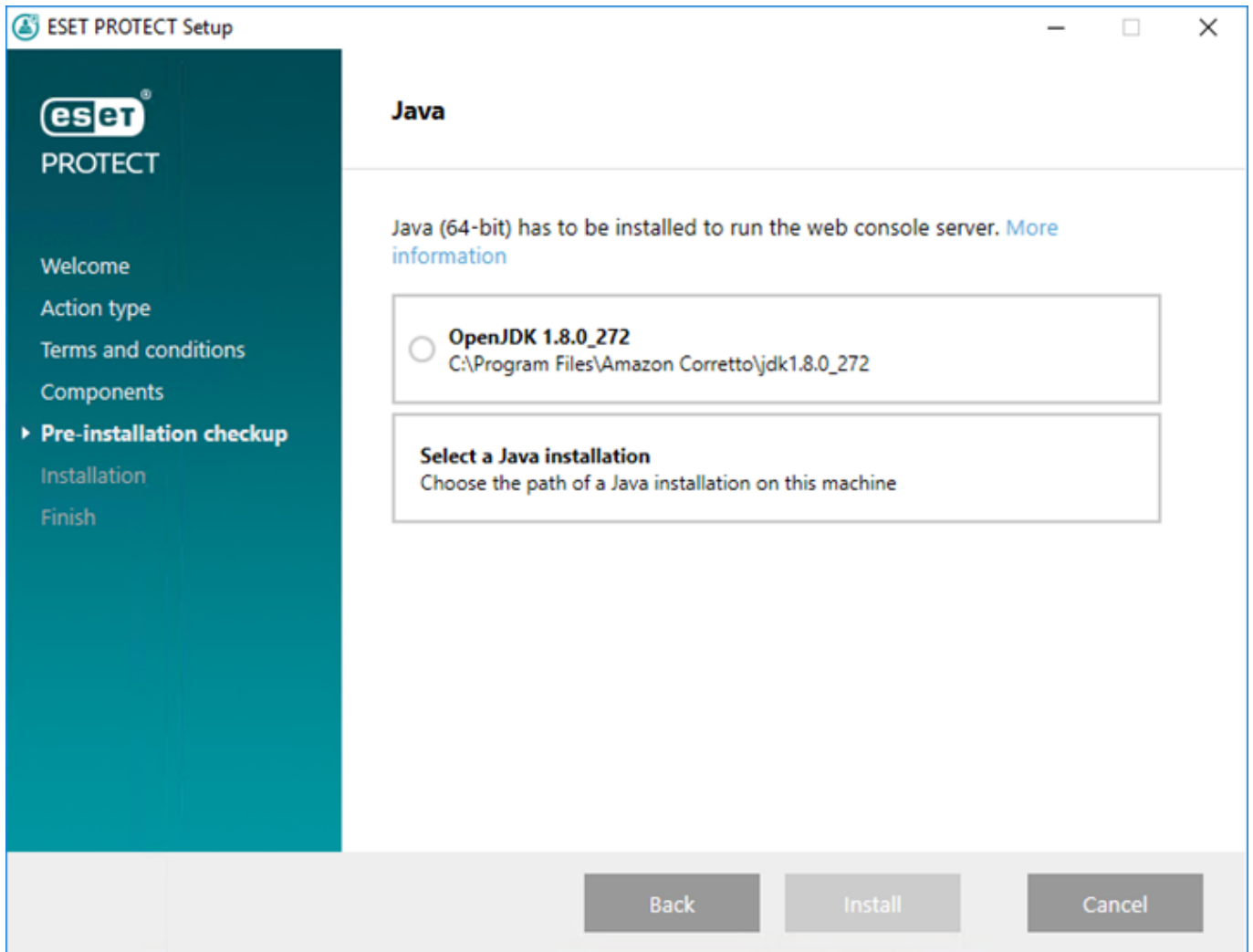
За бажанням установіть прапорець **Додати користувацький HTTPS сертифікат для Webconsole**.

- Виберіть цю опцію, якщо хочете використовувати користувацький сертифікат HTTPS для веб-консолі ESET PROTECT.
- Якщо ви не виберете цю опцію, для Tomcat буде автоматично створено сховище ключів.
- Якщо ви вибрали **Додати користувацький сертифікат HTTPS для веб-консолі**, натисніть **Огляд**, виберіть дійсний сертифікат (файл із розширенням .pfx або .p12) і введіть його **парольну фразу** (якщо її немає, залиште це поле порожнім). Сертифікат буде інстальовано на сервері Tomcat і використовуватиметься для доступу до веб-консолі. Щоб продовжити, натисніть **Далі**.



8. Виберіть інсталяцію Java на комп'ютері. Переконайтеся, що використовуєте останню версію Java/OpenJDK.

- a) Щоб вибрати вже інсталювану версію Java, натисніть **Вибрати інсталяцію Java**, виберіть папку, у якій інсталювано Java (з підпакою *bin*, наприклад *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) і натисніть **ОК**. З'явиться запит інсталювача про те, чи правильно вибрано шлях.
- b) Натисніть **Інсталювати**, щоб продовжити, або **Змінити**, щоб змінити шлях інсталяції Java.



9. Коли завершиться інсталяція, клацніть **Готово**.



Увага

Якщо веб-консоль ESET PROTECT і сервер ESET PROTECT інстальовано на різних комп'ютерах, виконайте дії нижче, щоб забезпечити обмін даними між веб-консоллю ESET PROTECT та сервером ESET PROTECT.

- Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.
- Запустіть Блокнот від імені адміністратора та відредагуйте файл `C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.
- Знайдіть рядок `server_address=localhost`.
- Замініть `localhost` на IP-адресу вашого сервера ESET PROTECT та збережіть файл.
- Запустіть службу Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Запустити**.

10. Відкрийте веб-консоль ESET PROTECT у підтримуваному браузері: <https://Server-IP/era/> (замініть Server-IP на IP-адресу вашого сервера ESET PROTECT). Відобразиться екран входу в систему.



Примітка

Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).

Інсталяція веб-консолі вручну



Увага

Ручна інсталяція компонента ESET PROTECT Web Console — складна процедура. Рекомендуємо інсталювати ESET PROTECT Web Console за допомогою [універсального інсталятора](#).

Порядок інсталяції компонента ESET PROTECT Web Console у Windows уручну

1. Переконайтеся, що перелічені далі попередні вимоги виконано.

- Інсталювано сервер ESET PROTECT.



Примітка

Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на [різні комп'ютери](#).

- Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT. Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.



Примітка

Якщо в системі інсталювано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримування версія – Java 8) і залишити лише останню версію Java.



Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інсталювати один із підтримуваних випусків Java.

- а) Завантажте останню [підтримувану версію](#) файлу інсталятора Apache Tomcat (32-рядна або 64-розрядна версія інсталятора для Windows) apache-tomcat-[версія].exe із сайту <https://tomcat.apache.org>.
- б) Запустіть інсталятор.
- в) Під час інсталяції вкажіть шлях до компоненту Java (батьківська папка для папок Java bin і lib).
- г) Після інсталяції переконайтеся, що вибрано **Автоматичний** тип запуску служби Apache Tomcat (у файлі **services.msc**).

2. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інсталятор для цього компонента ESET PROTECT (Web Console era.war).

3. Скопіюйте era.war у папку веб-програм Apache Tomcat:

C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps

4. Зачекайте кілька хвилин, поки буде виконано видобування файлів та інсталяцію веб-консолі ESET PROTECT.

5. Перейдіть до кроків, що відповідають вашим умовам.

- Якщо веб-консоль ESET PROTECT і сервер ESET PROTECT інсталювано на один комп'ютер, виконайте дії нижче.

а) Перезавантаження служби Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**. Зачекайте 30 секунд, а потім натисніть **Пуск**.

б) Відкрийте веб-консоль ESET PROTECT у [підтримуваному браузері](#): <http://localhost:8080/era/>. Відобразиться екран входу в систему.



Примітка

Під час інсталяції Apache Tomcat порт 8080 буде встановлено як порт HTTP за замовчуванням. Ви також можете налаштувати [підключення HTTPS для Apache Tomcat](#).

• Якщо веб-консоль ESET PROTECT і сервер ESET PROTECT інстальовано на різних комп'ютерах, виконайте дії нижче, щоб забезпечити обмін даними між веб-консоллю ESET PROTECT та сервером ESET PROTECT.

а) Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.

б) Запустіть Блокнот від імені адміністратора та відредагуйте файл `C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.

в) Знайдіть рядок `server_address=localhost`.

г) Замініть `localhost` на IP-адресу вашого сервера ESET PROTECT та збережіть файл.

е) Запустіть службу Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Запустити**.

ф) Відкрийте веб-консоль ESET PROTECT у [підтримуваному браузері](#): <https://Server-IP/era/> (замініть Server-IP на IP-адресу вашого сервера ESET PROTECT). Відобразиться екран входу в систему.



Примітка

Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).

Інсталяція проксі-сервера HTTP

Про проксі-сервер HTTP

Проксі-сервер HTTP призначений замінити проксі-сервер ERA б.х. Його функція полягає в передачі зашифрованих даних між агентом ESET Management та сервером ESET PROTECT. За замовчуванням ESET PROTECT використовує сервер Apache як проксі-сервер HTTP.

Використовуйте проксі-сервер HTTP, лише якщо агенти ESET Management не можуть підключитися до сервера ESET PROTECT напряму. Проксі-сервер HTTP не збирає дані та не обмежує мережевий трафік.

Рекомендується інсталювати агент ESET Management на той самий комп'ютер, на якому інстальовано проксі-сервер HTTP, але це не обов'язково. Агент ESET Management не може керувати проксі-сервером HTTP та налаштувати його.

- [Архітектура проксі-сервера HTTP](#)
- [Архітектура проксі-сервера Apache HTTP](#)
- [Додаткові сценарії для проксі-сервера HTTP](#)

Перед інсталяцією

Якщо ви оновлюєте наявне середовище, дотримуйтеся [процедури оновлення](#).



Увага

Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT, для якого потрібна автентифікація, не працюватиме.

Якщо ви не виберете порт для веб-консолі або агента за замовчуванням, можливо, потрібно буде налаштувати брандмауер відповідним чином. В іншому разі інсталяція може закінчитися невдало.

Інсталяція та конфігурація

Ви можете інсталювати проксі-сервер Apache HTTP за допомогою окремого або універсального інсталятора

ESET PROTECT.

- Для використання універсального інстальатора необхідно [завантажити](#) весь пакет програм, але ця процедура є простішою. Запустіть завантажений інстальатор і виберіть у ньому лише **проксі-сервер Apache HTTP**. Після інсталяції сервера Apache його потрібно [налаштувати](#).
- Інсталювати програмне забезпечення з [окремого](#) інстальатора складніше, проте в цьому разі необхідно завантажити лише кілька МБ даних. Див. інструкції з [інсталяції](#) та [налаштування](#).

Конфігурація проксі-сервера HTTP для великої кількості клієнтів

Якщо ви використовуєте 64-розрядний проксі-сервер Apache HTTP, то можете збільшити ліміт потоків для Apache HTTP Proxy. Змініть файл конфігурації `httpd.conf` у папці Apache HTTP Proxy. Знайдіть у файлі вказані нижче параметри та змініть їхнє значення на кількість клієнтів.

Замініть значення 5000, наведене як приклад, на своє число. Максимальне значення дорівнює 32000.

```
ThreadLimit 5000
```

```
ThreadsPerChild 5000
```

Не змінюйте інший текст файлу.

Інсталяція RD Sensor

Щоб інсталювати компонент RD Sensor у Windows, виконайте вказані нижче дії.

1. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інстальатор для цього компонента ESET PROTECT (`rdsensor_x86.msi` або `rdsensor_x64.msi`).
2. Переконайтеся, що всі [попередні вимоги](#) виконано.
3. Для запуску інсталяції двічі натисніть на інстальатор RD Sensor.
4. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.
5. Якщо ви не хочете надсилати в ESET звіти про аварійне завершення роботи та дані телеметрії, зніміть прапорець **Узяти участь у програмі покращення продукту**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET.
6. Виберіть місце для інсталяції RD Sensor та натисніть **Далі > Інсталювати**.

Попередні вимоги до RD Sensor

Щоб інсталювати компонент RD Sensor у Windows, потрібно виконати вказані нижче вимоги.

- [WinPCAP](#): використовуйте останню версію WinPCAP (принаймні 4.1.0).
- Мережу потрібно налаштувати належним чином (відповідні [порти](#) мають бути відкриті, вхідний обмін даними не має блокуватися брандмауером тощо).
- Сервер ESET PROTECT має бути доступний.
- [Агент ESET Management](#) має бути інсталювано на локальному комп'ютері, щоб повністю підтримувати всі програмні функції.
- Файл журналу Rogue Detection Sensor має бути розташовано за цим шляхом:
`C:\ProgramData\ESET\Rogue Detection Sensor\Logs\`.

Інструмент «Дзеркало» - Windows

[Користуєтесь Linux?](#)

Для автономного оновлення ядра виявлення необхідний інструмент «Дзеркало». Якщо на клієнтських комп'ютерах відсутнє підключення до Інтернету, але потрібно оновити ядро виявлення, за допомогою інструмента «Дзеркало» можна завантажити файли оновлення із серверів оновлення ESET і зберегти їх локально.



Примітка

Інструмент «Дзеркало» завантажує лише оновлення ядра виявлення й інші модулі програми та не завантажує оновлення компонентів програми й дані ESET LiveGrid®. Він також може створити [автономний репозиторій](#). Крім цього, можна оновлювати кожен продукт окремо.

Необхідні компоненти



Увага

Інструмент «Дзеркало» не підтримується у Windows XP та Windows Server 2003.

- Цільова папка має бути доступна для спільного використання, Samba/Windows або служби HTTP/FTP залежно від вибраного способу отримання доступу до оновлень.
- Необхідно мати дійсний файл [автономної ліцензії](#), що містить ім'я користувача та пароль. Під час створення файлу ліцензії поставте прапорець **Включити ім'я користувача та пароль**. Також можна вказати **назву** ліцензії. Файл автономної ліцензії потрібний для активації інструмента «Дзеркало» та створення дзеркала оновлення.

Create offline license file

Product
ESET Endpoint Security for Windows

Name
Test license

Units count
1 /3

Username and password

Include Username and Password
When included it is possible to update from ESET servers

ESET PROTECT

Allow management with ESET PROTECT

GENERATE CANCEL

- Перш ніж запускати інструмент «Дзеркало», інсталюйте ці пакети:

- [Visual C++ Redistributable for Visual Studio 2010](#)
- [Visual C++ 2015 Redistributable x86](#)

Як користуватись інструментом «Дзеркало»

1. Завантажте інструмент «Дзеркало» з [цієї сторінки ESET](#) (розділ **Автономні інсталятори**).
2. Розархівуйте завантажений архів.
3. Відкрийте командний рядок і перейдіть у папку, що містить файл *MirrorTool.exe*.
4. Щоб переглянути всі доступні параметри інструмента «Дзеркало», виконайте вказану нижче команду.

```
MirrorTool.exe --help
```


```

C:\[redacted]\MirrorTool_Win32\Win32>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2020. All rights reserved.
Allowed options:
  --mirrorType arg                [required for module update]
                                  Type of mirror. Possible values (case
                                  insensitive): regular, pre-release,
                                  delayed.
  --intermediateUpdateDirectory arg [required for module update]
                                  Files will be downloaded to this
                                  directory to create mirror in output
                                  directory.
  --offlineLicenseFilename arg    [required for module update]
                                  Offline license file.
  --updateServer arg              [optional]
                                  Update server. (e.g.:
                                  http://update.eset.com/eset_upd/ep6/)
                                  Mirror will be created in output
                                  directory, only specified path in
                                  server will be mirrored.
  --outputDirectory arg           [required for module update]
                                  Directory where mirror will be created.
  --proxyHost arg                 [optional]
                                  Http proxy address (fqdn or IP).
  --proxyPort arg                 [optional]
                                  Http proxy port.
  --proxyUsername arg             [optional]
                                  Http proxy username.
  --proxyPassword arg             [optional]
                                  Http proxy password.
  --networkDriveUsername arg      [optional]
                                  Username used, when output directory is
                                  accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg      [optional]
                                  Password used, when output directory is
                                  accessed using smb(e.g:\\hostname).
  --excludedProducts arg          [optional]
                                  Disable creating mirror for specified
                                  products. Possible values: ep4 ep5 ep6
                                  ep7 era6.
  --repositoryServer arg          [required for repository update]
                                  Repository server for repository
                                  creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                  Files will be downloaded to this
                                  directory to create offline mirror in
                                  output directory.
  --outputRepositoryDirectory arg  [required for repository update]
                                  Directory where offline repository will
                                  be created.
  --languageFilterForRepository arg [optional]
                                  Download only packages with provided
                                  languages.
  --productFilterForRepository arg [optional]
                                  Download only packages with provided
                                  product.
  --downloadLegacyForRepository    [optional]
                                  If set, download also legacy packages.
  --trustDownloadedFilesInRepositoryTemp [optional]
                                  If set, hash on allready downloaded
                                  files are not checked.
  --mirrorOnlyLevelUpdates         [optional]
                                  If set, only level upgrades will be
                                  downloaded (nano/continuous updates
                                  will not be downloaded)
  --mirrorFileFormat arg           [optional]
                                  Specifies which type of update files
                                  will be downloaded. Possible values
                                  (case insensitive): dll, dat. Parameter
                                  is ignored when creating mirror for
                                  legacy products (ep4, ep5)
  --help                           [optional]
                                  Display this help and exit

```

Параметр	Опис
--updateServer	Під час використання потрібно вказати повну URL-адресу сервера оновлення.
--offlineLicenseFilename	Необхідно вказати шлях до файлу автономної ліцензії (як згадувалося вище).
--languageFilterForRepository	Можна вказати коди мов, наприклад для французької мови введіть fr_FR. Коди інших мов наведено в таблиці нижче. Щоб вибрати кілька мов, розділіть їх пробілом, наприклад: en_US zh_TW de_DE
--productFilterForRepository	Можна вказати рядок, який інструмент «Дзеркало» використовує як фільтр завантаження. Інструмент «Дзеркало» завантажує лише файли, які містять цей рядок у своїх звичних іменах. Можна вибрати кілька продуктів, додавши інші аргументи, наприклад: --productFilterForRepository Antivirus Security Інструмент «Дзеркало» завантажує всі мови для кожного вибраного продукту.
--downloadLegacyForRepository	Указувати аргументи непотрібно. Використовуйте цей параметр, щоб також завантажити застарілі пакети. Якщо його не використовувати, застарілі пакети не завантажуватимуться. Щоб дізнатися, які продукти є застарілими, перейдіть у меню Інсталяція програмного забезпечення > Завдання клієнта > Налаштування > Пакет для інсталяції > Вибрати пакет > Застарілі .

Нові параметри в інструменті «Дзеркало» розповсюджені на ESMC 7.2 і ESET PROTECT

--mirrorOnlyLevelUpdates	Указувати аргументи непотрібно. Якщо його задано, завантажуватимуться лише оновлення рівнів (нанооновлення не буде завантажено). Докладніше про типи оновлень можна дізнатися в нашій статті бази знань .
--mirrorFileFormat	<div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;">  <p>Попередження Цей параметр призначено лише для досвідчених користувачів. Перш ніж використовувати параметр --mirrorFileFormat, переконайтеся, що середовище не містить одночасно стару (6.5 і ранішні версії) та нову (6.6 і пізніші версії) версії продукту захисту ESET. Неправильне використання цього параметра може призвести до неправильних оновлень продуктів захисту ESET.</p> </div> <p>Ви можете вказати, які типи файлів оновлення завантажувати. Можливі значення (з урахуванням реєстру):</p> <ul style="list-style-type: none"> • dat – використовуйте це значення, якщо середовище містить лише продукт захисту ESET 6.5 або старіших версій; • dll – використовуйте це значення, якщо середовище містить лише продукт захисту ESET 6.6 або новіших версій. <p>Параметр ігнорується, коли дзеркало створюється для застарілих продуктів (er4, er5).</p>



Примітка

Усі фільтри чутливі до реєстру.



Увага

Інструмент «Дзеркало» створює структуру папок, що відрізняється від тої, яку створює дзеркало робочої станції. Кожна папка містить файли оновлень для групи продуктів. Необхідно вказати повний шлях до правильної папки в параметрах оновлення продукту за допомогою дзеркала.
Наприклад, щоб оновити ESET PROTECT8.0 із дзеркала, для параметра [Сервер оновлень](#) встановіть указане нижче значення (відповідно до основного розташування сервера HTTP):
`http://your_server_address/mirror/eset_upd/era6`

Щоб створити дзеркало, запустіть інструмент «Дзеркало» з принаймні мінімальною кількістю необхідних параметрів. Нижче наведено приклад.

```
MirrorTool.exe --mirrorType regular ^  
--intermediateUpdateDirectory c:\temp\mirrorTemp ^  
--offlineLicenseFilename c:\temp\offline.lf ^  
--outputDirectory c:\temp\mirror
```

Нижче наведено приклад розширеної конфігурації автономного репозиторію з вибраними продуктами, мовами та ввімкненим завантаженням застарілих файлів.

```
MirrorTool.exe --repositoryServer AUTOSELECT ^  
--intermediateRepositoryDirectory c:\temp\repoTemp ^  
--outputRepositoryDirectory c:\temp\repository ^  
--languageFilterForRepository sk_SK fr_FR de_DE ^  
--productFilterForRepository Antivirus Security ^  
--downloadLegacyForRepository
```

Інструмент «Дзеркало» та параметри оновлення

- Щоб автоматично завантажувати оновлення модулів, створіть розклад запуску інструмента «Дзеркало». Для цього відкрийте веб-консоль і натисніть **Клієнтські завдання > Операційна система > Виконати команду. Виберіть Командний рядок для виконання** (зокрема, шлях до файлу MirrorTool.exe) і належний тригер (наприклад, CRON на кожен годину 0 0 * * * ? *). Крім цього, можна скористатися планувальником завдань Windows або Cron у Linux.
- Щоб налаштувати оновлення на клієнтських комп'ютерах, створіть політику й налаштуйте **сервер оновлення** для вказування на адресу дзеркала або спільну папку.



Увага

Якщо ви використовуєте сервер-дзеркало HTTPS, імпортуйте його сертифікат у надійне кореневе сховище на клієнтському комп'ютері. Перегляньте розділ [Інсталяція надійного кореневого сертифіката](#) у Windows.



Примітка

Щоб налаштувати ланцюг інструмента «Дзеркало», прочитайте [цю статтю бази знань](#) (налаштування інструмента «Дзеркало» для завантаження оновлень з іншого інструмента «Дзеркало»).

Інсталяція Mobile Device Connector

Щоб інсталювати компонент Mobile Device Connector для сервера ESET PROTECT, виконайте вказані нижче дії.



Попередження

Щоб мобільними пристроями можна було керувати будь-коли незалежно від їхнього місцезнаходження, до Mobile Device Connector має бути доступ через Інтернет.



Примітка

Рекомендуємо розгорнути компонент MDM на хост-пристрої, на якому не розміщено сервер ESET PROTECT.

1. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інсталятор для цього компонента ESET PROTECT (mdmcore_x64.msi).
2. Спершу перегляньте [вимоги](#) та переконайтеся, що виконуєте їх.
3. Запустіть інсталятор Mobile Device Connector та прийміть ліцензійну угоду з кінцевим користувачем (якщо погоджуєтеся з її умовами).
4. Натисніть **Огляд**, перейдіть у папку, у якій розташовано [сертифікат SSL](#), що використовуватиметься для обміну даними через протокол HTTPS, і введіть пароль цього сертифіката.
5. Укажіть **ім'я хоста MDM**: це загальнодоступний домен або загальнодоступна IP-адреса сервера MDM, через які до нього можна отримати доступ із мобільних пристроїв в Інтернеті.



Увага

Ім'я хоста MDM потрібно ввести ідентично тому, як його вказано в **сертифікаті сервера HTTPS**. В іншому разі мобільний пристрій iOS відмовиться інстальювати [профіль MDM](#). Наприклад, якщо в сертифікаті вказано IP-адресу, введіть її в полі **Ім'я хоста MDM**. Якщо в сертифікаті HTTPS вказано повне доменне ім'я (наприклад, mdm.мускомпану.com), введіть його в полі **Ім'я хоста MDM**. Крім цього, якщо в сертифікаті HTTPS використовується символ узагальнення * (наприклад, *.мускомпану.com), ви можете вказати в полі **Ім'я хоста MDM** значення mdm.мускомпану.com.

6. Тепер інсталятору потрібно підключитися до наявної бази даних, яку використовуватиме Mobile Device Connector. Укажіть такі дані для підключення:

- **База даних:** MySQL Server / MS SQL Server / MS SQL Server з використанням автентифікації Windows
- **ODBC драйвер:** драйвер MySQL ODBC 5.1 / драйвер MySQL ODBC 5.2 з підтримкою Юнікод / драйвер MySQL ODBC 5.3 з підтримкою Юнікод / драйвер MySQL ODBC 8.0 із підтримкою Юнікод / SQL Server / SQL Server Native Client 10.0 / драйвер ODBC 11 для SQL Server / драйвер ODBC 13 для SQL Server / драйвер ODBC 17 для SQL Server
- **Ім'я бази даних:** рекомендуємо використовувати попередньо встановлене ім'я або змінити його за необхідності.
- **Ім'я хоста:** ім'я хоста або IP-адреса сервера бази даних
- **Порт:** використовується для підключення до сервера бази даних
- **Ім'я користувача / пароль** облікового запису адміністратора бази даних
- **Використовувати екземпляр з іменем.** Якщо ви використовуєте базу даних MS SQL, можна також поставити прапорець **Використовувати екземпляр з іменем**. Це дасть змогу використовувати налаштовуваний екземпляр бази даних, який можна налаштувати в полі «Ім'я хоста» у формі `HOSTNAME\DB_INSTANCE`, наприклад: `192.168.0.10\ESMCTSQL`. Для кластерної бази даних використовуйте лише ім'я кластера. Якщо вибрати цю опцію, ви не зможете змінити порт, який використовуватиметься. Система використовуватиме порти за замовчуванням, визначені Microsoft.



Примітка

Поставивши прапорець **Використовувати екземпляр з іменем**, сервер ESET PROTECT можна також підключити до бази даних MS SQL, інстальованої у відмовостійкому кластері. У полі **Ім'я хоста** введіть ім'я кластера.



Примітка

Можна використовувати той самий сервер, що й для бази даних ESET PROTECT. Однак рекомендуємо використовувати інший сервер бази даних, якщо ви плануєте зареєструвати понад 80 мобільних пристроїв.

7. Укажіть користувача створеної бази даних Mobile Device Connector. Можна **створити нового**

користувача або **використовувати наявного**. Введіть пароль користувача бази даних.

8. Введіть **хост сервера** (назву або IP-адресу сервера ESET PROTECT) і **порт сервера** (порт за замовчуванням – 2222; якщо ви використовуєте інший порт, укажіть його).

9. Підключіть MDM Connector до сервера ESET PROTECT. Заповніть поля **Хост сервера** та **Порт сервера**, необхідні для підключення до сервера ESET PROTECT, і виберіть варіант **Інсталяція із сервера** або **Інсталяція в автономному режимі**, щоб продовжити.

Інсталяція із сервера. Укажіть облікові дані адміністратора веб-консолі ESET PROTECT, й інсталятор завантажить необхідні сертифікати автоматично. Також перевірте, чи надано [дозволи](#), необхідні для інсталяції із сервера.

1. Введіть **хост сервера** (назву або IP-адресу сервера ESET PROTECT) і **порт веб-консолі** (якщо ви не використовуєте інший порт, укажіть номер порту за замовчуванням – 2223). Також укажіть облікові дані (**ім'я користувача та пароль**) адміністратора веб-консолі.
2. Коли з'явиться запит прийняти сертифікат, натисніть **Так**. Перейдіть до кроку 11.

Інсталяція в автономному режимі. Укажіть **сертифікат проксі-сервера** та **Центр сертифікації**, який можна [експортувати](#) з ESET PROTECT. Можна також використовувати [налаштовуваний сертифікат](#) і відповідний Центр сертифікації.

1. Натисніть **Огляд** поруч із сертифікатом однорангового вузла та перейдіть до папки, у якій розташовано **цей сертифікат** (це сертифікат проксі-сервера, експортований з ESET PROTECT). Не заповнюйте поле **Пароль сертифіката**, оскільки для цього сертифіката пароль не потрібний.
2. Повторіть процедуру для Центру сертифікації та перейдіть до кроку 11.



Примітка

Якщо в ESET PROTECT використовуються налаштовувані сертифікати (замість сертифікатів за замовчуванням, автоматично згенерованих під час інсталяції ESET PROTECT), їх слід використовувати під час запити сертифіката проксі-сервера.

10. Укажіть цільову папку для Mobile Device Connector (рекомендуємо використовувати папку за замовчуванням), натисніть **Далі**, а потім – **Інсталювати**.

11. Коли інсталяція завершиться, перевірте, чи Mobile Device Connector працює належним чином. Для цього відкрийте в браузері або на мобільному пристрої сторінку <https://your-mdm-hostname:enrollment-port> (наприклад, <https://mdm.company.com:9980>). Якщо інсталяцію виконано успішно, з'явиться таке повідомлення: Сервер MDM працює!

12. Тепер ви можете [активувати MDM в ESET PROTECT](#).

Попередні вимоги до Mobile Device Connector



Попередження

Якщо порт або ім'я хоста сервера MDM змінено, усі мобільні пристрої потрібно зареєструвати знову.

Тому рекомендуємо налаштувати окреме ім'я хоста для сервера MDM, щоб, якщо потрібно буде змінити хост-пристрій сервера MDM, можна було перепризначити імені хоста MDM IP-адресу нового хост-пристрою в параметрах DNS.

Щоб інсталювати Mobile Device Connector у Windows, потрібно виконати вказані нижче вимоги.

- Загальнодоступну IP-адресу чи ім'я хоста або загальнодоступний домен, доступний в Інтернеті.



Примітка

Якщо потрібно змінити ім'я хоста сервера MDM, виконайте відновлювальну інсталяцію компонента MDC. Якщо ви зміните ім'я хоста сервера MDM, імпортуйте новий **сертифікат сервера HTTPS**, який містить нове ім'я хоста, щоб сервер MDM працював належним чином.

- Порти мають бути відкриті й доступні (переглянути їх повний перелік можна [тут](#)). Рекомендуємо використовувати номери портів 9981 і 9980 за замовчуванням. За потреби їх можна змінити у файлі конфігурації сервера MDM. Переконайтеся, що мобільні пристрої можуть підключатися через указані порти. Для цього змініть параметри брандмауера та/або мережі (якщо застосовно). Докладнішу інформацію про архітектуру MDM можна переглянути [тут](#).
- Параметри брандмауера: коли Mobile Device Connector інсталюється на несерверну ОС, наприклад Windows 7 (лише з метою ознайомлення), дозвольте обмін даними через порти, створивши [правила брандмауера](#) для:

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9981

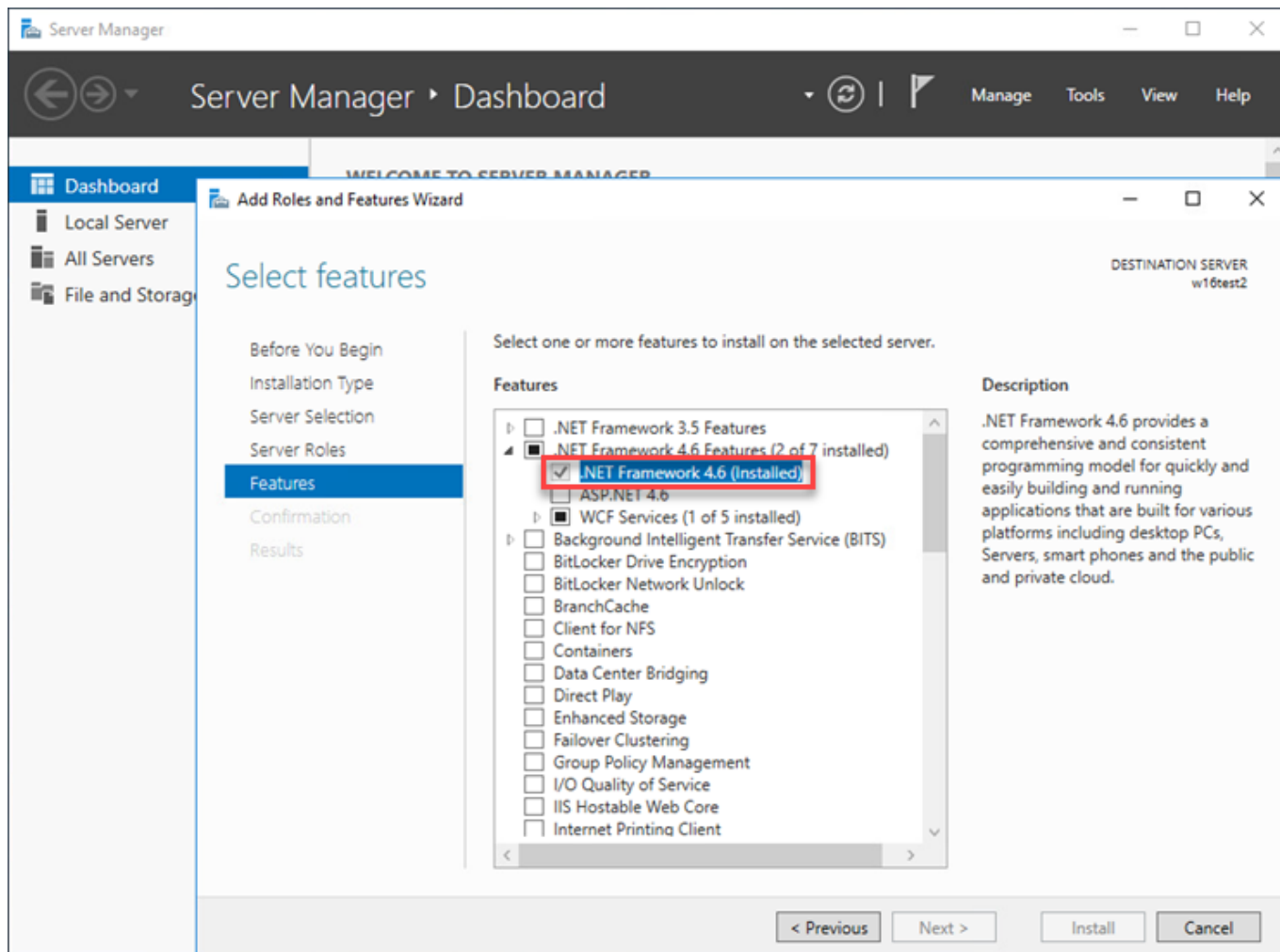
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP port 2222



Примітка

Фактичні шляхи до файлів .exe можуть відрізнитися залежно від того, де інстальовано кожен компонент ESET PROTECT в ОС клієнта.

- Сервер бази даних уже інстальовано та налаштовано. Переконайтеся, що виконано вимоги [Microsoft SQL](#) або [MySQL](#).
- Використання оперативної пам'яті з'єднувача MDM оптимізовано, тому одночасно може виконуватися щонайбільше 48 процесів модуля ESET PROTECT MDMCore. Якщо користувач підключить більше пристроїв, процеси періодично переходитимуть на пристрої, яким зараз потрібні ресурси.
- Має бути інстальовано Microsoft .NET Framework 4. Відповідний пакет можна інсталювати за допомогою **майстра додавання ролей і функцій** (як показано нижче). Фреймворк .NET вимагається лише для інсталяції MS SQL Server Express.



Вимоги до сертифіката

- Для безпечного обміну даними через протокол HTTPS потрібен **сертифікат SSL** у форматі .pfx. Рекомендуємо використовувати сертифікат, наданий Центром сертифікації (ЦС ESET PROTECT або сторонній ЦС). Не радимо використовувати самопідписані сертифікати, оскільки не всі мобільні пристрої дозволяють користувачам приймати такі сертифікати. Натомість сертифікати, підписані ЦС, є довіреними й не вимагають дій зі сторони користувача.
- Щоб об'єднати їх в один файл .pfx, потрібно мати сертифікат, підписаний ЦС (ESET PROTECT або стороннім ЦС), відповідний закритий ключ і виконати стандартні процедури (зазвичай за допомогою OpenSSL):

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx
```

 Це стандартна процедура для більшості серверів, які використовують сертифікати SSL.
- Щоб виконати [інсталяцію в автономному режимі](#), потрібно надати сертифікат однорангового вузла (**сертифікат агента**, [експортований](#) з ESET PROTECT). Замість нього в ESET PROTECT можна використовувати [налаштовуваний сертифікат](#).

Активация Mobile Device Connector

Після інсталяції компонента Mobile Device Connector його потрібно активувати за допомогою ліцензії ESET Endpoint, Business or Office.

1. Додайте ліцензію **ESET Endpoint, Business or Office** у програму керування ліцензіями ESET PROTECT, виконавши [ці дії](#).
2. Активуйте Mobile Device Connector за допомогою клієнтських завдань [Активация продукту](#). Ця процедура аналогічна для активації будь-яких продуктів ESET на клієнтському комп'ютері: у цьому випадку Mobile Device Connector є клієнтським комп'ютером.

Ліцензування iOS в MDM

Оскільки ESET не продає програму в Apple App Store, ESET Mobile Device Connector зберігає всю інформацію про ліцензування для пристроїв iOS.

Ліцензії призначено для окремих пристроїв, і їх можна активувати за допомогою [завдання активації продукту](#) (так само, як в Android).

Є кілька способів дезактивувати ліцензії iOS:

- видалити пристрій зі списку керованих за допомогою завдання «Припинити керування»;
- видалити Mobile Device Connector за допомогою опції **Видалити базу даних**;
- дезактивувати іншим способом (через ESET PROTECT або [дезактивацію EBA](#)).

Оскільки MDC обмінюється даними із серверами ліцензування ESET від імені пристроїв iOS, портал EBA відображає стан MDC, а не стан окремих пристроїв. Поточна інформація про пристрій завжди доступна у веб-консолі ESET PROTECT.

Неактивовані пристрої та пристрої, термін дії ліцензії яких минув, матимуть червоний статус захисту й відображатимуть повідомлення «Продукт не активовано». Ці пристрої відхилятимуть завдання, не встановлюватимуть політики та не доставлятимуть журнали некритичних помилок.

Якщо вибрано опцію **Не видаляти базу даних**, під час деінсталяції MDM ліцензії, які використовуються, не буде дезактивовано. Ці ліцензії можна використати повторно, якщо їх було видалено через ESET PROTECT або [дезактивацію EBA](#) (для цього потрібно знову інсталювати MDM у цій базі даних). У разі перенесення на інший сервер MDM потрібно [ще раз виконати завдання активації продукту](#).

Вимоги до сертифіката HTTPS

Щоб зареєструвати мобільний пристрій в ESET Mobile Device Connector, сервер HTTPS має повертати повний ланцюжок сертифікатів.

Щоб сертифікат працював належним чином, слід дотримуватися наведених нижче вимог.

- Сертифікат HTTPS (контейнер pkcs#12/pfx) повинен містити повний ланцюжок сертифікатів, зокрема кореневий центр сертифікації.
- Сертифікат повинен бути дійсним протягом необхідного періоду часу (дійсний з/до).
- Параметри **CommonName** чи **subjectAltName** мають збігатися з іменем хоста MDM.



Примітка

Якщо параметр **Ім'я хоста MDM** має значення hostname.mdm.domain.com, ваш сертифікат може містити наступні імена:

- hostname.mdm.domain.com
- *.mdm.domain.com

При цьому він не може містити такі імена:

- *
- *.com
- *.domain.com

Це значить, що символ «*» не можна використовувати замість «крапки». Процедура підтвердження сертифікатів для MDM в iOS підтверджує це правило.



Примітка

Зауважте, що під час перевірки дійсності сертифіката деякі пристрої враховують поточний часовий пояс. Щоб уникнути можливих проблем, установіть термін дії сертифікату за день або два до поточної дати.

Інсталяція проксі-сервера Apache HTTP та кеш

Про проксі-сервер Apache HTTP

Проксі-сервер Apache HTTP може виконувати різні функції:

Функція	Проксі-сервер, на якому доступна ця функція
Кешування завантажень і оновлень	Проксі-сервер Apache HTTP або інший проксі-сервер
Кешування результатів ESET Dynamic Threat Defense	Лише налаштований проксі-сервер Apache HTTP
Реплікація обміну даними між агентами ESET Management і сервером ESET PROTECT	Проксі-сервер Apache HTTP або інший проксі-сервер



Увага

Якщо ви вже інсталиювали проксі-сервер Apache HTTP в середовище Windows і хочете оновити його до останньої версії, перейдіть до пункту [Оновлення проксі-сервера Apache HTTP](#).

Функція кешування проксі-сервера Apache HTTP

Apache HTTP Proxy завантажує й кешує:

- оновлення модулів ESET;
- пакети інсталяцій із серверів репозиторію;
- оновлення компонентів продуктів.

Кешовані дані розповсюджуються клієнтам робочих станцій у вашій мережі. Кешування може значно зменшити інтернет-трафік у вашій мережі.



Примітка

Як альтернативу проксі-серверу Apache HTTP можна інсталиювати [Squid](#).

Інсталиювати проксі-сервер Apache HTTP у Windows можна в два таких способи:

- [Інсталяція за допомогою універсального інсталятора](#)
- [Інсталяція за допомогою автономного інсталятора](#)

Інсталяція за допомогою автономного інсталятора

1. Перейдіть у [розділ завантажень](#) ESET PROTECT і завантажте окремий інсталятор для цього компонента ESET PROTECT (apachehttp.zip).
2. Відкрийте архів ApacheHttp.zip і видобудьте файли в папку *C:\Program Files\Apache HTTP Proxy*.



Примітка

Щоб інсталиювати проксі-сервер Apache HTTP на інший жорсткий диск, *C:\Program Files* потрібно замінити на відповідний шлях у наведених нижче інструкціях і у файлі httpd.conf, розташованому в каталозі *Apache HTTP Proxy\conf*. Наприклад, щоб видобути архів ApacheHttp.zip в папку *D:\Apache Http Proxy*, замість *C:\Program Files* укажіть *D:\Apache Http Proxy*.

3. Відкрийте командний рядок адміністратора та змініть папку на *C:\Program Files\Apache HTTP Proxy\bin*
4. Виконайте цю команду:

```
httpd.exe -k install -n ApacheHttpProxy
```

5. Запустіть службу **ApacheHttpProxy** за допомогою цієї команди:

```
sc start ApacheHttpProxy
```

6. Ви можете перевірити, чи працює служба проксі-сервера Apache HTTP, в оснастці `services.msc` (знайдіть **ApacheHttpProxy**). За замовчуванням налаштовано автоматичний запуск служби.

Після інсталяції [налаштуйте](#) на проксі-сервері Apache HTTP необхідні функції.

Конфігурація проксі-сервера Apache HTTP

Інсталятор проксі-сервера Apache HTTP, що надається ESET, налаштовано попередньо. Однак для коректної роботи служби потрібне додаткове налаштування.

Конфігурація проксі-сервера Apache HTTP для реплікації (агент - сервер)

1. Змініть файл конфігурації *Apache HTTP Proxy* `httpd.conf`, розташований у каталозі `C:\Program Files\Apache HTTP Proxy\conf`.

а. За замовчуванням для обміну даними з агентом ESET Management використовується порт 2222. Якщо ви змінили порт під час інсталяції, вкажіть новий номер порту. Змініть значення «2222» в рядку `AllowCONNECT 443 563 2222 8883` на номер вашого порту.

б. Додайте окремий сегмент `ProxyMatch`.

I. Адреса, яку агенти використовують для підключення до сервера ESET PROTECT.

II. Усі інші адреси сервера ESET PROTECT (IP-адреса, повне доменне ім'я).

(Додайте весь указаний нижче код; IP-адреса `10.1.1.10` та ім'я хоста `hostname.example` є лише прикладами, їх потрібно замінити своїми адресами. Ви також можете створити вираз `ProxyMatch` в [цій статті бази знань](#).)

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>
Allow from all
</ProxyMatch>
```

с. Перезавантаження служби *Apache HTTP Proxy*.

2. Створіть відповідну [політику агента](#), щоб ваші агенти використовували для реплікації проксі-сервер.

Конфігурація проксі-сервера Apache HTTP для кешування

1. Зупиніть роботу служби **ApacheHttpProxy** за допомогою цієї команди:

```
sc stop ApacheHttpProxy
```

2. Відкрийте файл `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf` у текстовому редакторі. Додайте у файл такі рядки:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

3. Збережіть файл і запустіть службу Apache.

```
sc start ApacheHttpProxy
```



Примітка

Якщо ви бажаєте, щоб папка для кешування знаходилася в іншому місці, наприклад, на іншому диску (D:\Apache HTTP Proxy\cache), то в останньому рядку наведеного вище коду змініть значення "C:\Program Files\Apache HTTP Proxy\cache" на "D:\Apache HTTP Proxy\cache".

Конфігурація проксі-сервера Apache HTTP для використання ім'я користувача та пароля

Ім'я користувача та пароль можна використовувати лише для кешування. [Протокол реплікації](#), який використовується під час обміну даними між агентом і сервером, не підтримує автентифікацію.

1. Зупиніть роботу служби **ApacheHttpProxy**. Для цього відкритте [командний рядок адміністратора](#) та виконайте таку команду:

```
sc stop ApacheHttpProxy
```

2. Перевірте наявність наступних модулів у папці *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

3. Додайте в розділ `<Proxy *>` такі рядки *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

4. Створіть файл із назвою `password.file` в папці `Apache HTTP Proxy\bin\` за допомогою команди `htpasswd` (вам знадобиться ввести пароль):

```
htpasswd.exe -c ..\password.file username
```

5. Вручну створіть файл `group.file` в папці `Apache HTTP Proxy\` з таким вмістом:

```
usergroup:username
```

6. Запустіть службу **ApacheHttpProxy**. Для цього відкрийте командний рядок адміністратора та виконайте таку команду:

```
sc start ApacheHttpProxy
```

7. Перевірте підключення до проксі-сервера HTTP. Для цього в браузері перейдіть за цією URL-адресою:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)



Примітка

Після інсталяції проксі-сервера Apache HTTP ви зможете дозволити передавати лише дані ESET (блокуючи весь інший трафік, встановлено за замовчуванням) або будь-які дані. Змініть конфігурацію згідно з наведеними нижче інструкціями:

- [Перенаправлення лише даних ESET](#)
- [Ланцюжок проксі-серверів \(усі дані\)](#)

Відкрийте список вмісту кеша

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -a -p "C:\ProgramData\Apache HTTP Proxy\cache"
```

Використайте інструмент [htcacheclean](#) для очищення кеша диска. Див. рекомендовану команду нижче (установлює розмір кешу 20 ГБ і обмежує кількість кешованих файлів до приблизно 128 000):

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -n -t ^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M -L128000
```

Щоб виконувати очищення кеша щогодини, запустіть таку команду:

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask ^  
/TR "\"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe\" ^  
-n -t -p "\"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M -L128000"
```

Якщо ви вирішите дозволити весь трафік, використайте рекомендовані команди:

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -n -t ^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M
```

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask ^  
/TR "\"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe\" ^  
-n -t -p "\"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M"
```



Примітка

У наведених вище командах обов'язково вказуйте символ `^` після рядка. В іншому разі команда буде виконуватися неправильно.

Щоб отримати додаткову інформацію, див. [статтю бази знань](#) або [Інструкції з автентифікації й авторизації Apache](#).

Squid інсталяція у Windows і кешування проксі-сервера HTTP

Squid – це альтернатива [проксі-серверу Apache HTTP](#). Щоб інсталювати Squid у Windows, виконайте вказані нижче дії.

1. [Завантажте](#) інсталятор Squid MSI та інсталюйте Squid.
2. Натисніть піктограму **Squid for Windows** в області сповіщень і виберіть **Stop Squid Service**.
3. Перейдіть у папку інсталяції Squid (наприклад, C:\Squid\bin) і виконайте в рядку таку команду:

```
squid.exe -z -F
```

У результаті буде створено своп-каталоги для кешу.

4. Натисніть піктограму **Squid for Windows** в області сповіщень і виберіть **Open Squid Configuration**.
5. Замініти `http_access deny all` на `http_access allow all`.
6. Увімкніть кешування диска. Для цього додайте такий рядок:

```
cache_dir aufs /cygdrive/c/Squid/var/cache 3000 16 256
```



Примітка

- Ви можете змінити розташування каталогу кешу відповідно до своїх потреб. У прикладі каталог кешу розташовано в C:\Squid\var\cache (зверніть увагу на формат шляху в команді).
- У каталозі кешу можна змінити загальний розмір кешу (наприклад, 3000 МБ) і кількість підкаталогів першого рівня (наприклад, 16) та другого рівня (наприклад, 256).

7. Збережіть і закрийте файл конфігурації Squidsquid.cofn.
8. Натисніть піктограму **Squid for Windows** в області сповіщень і виберіть **Start Squid Service**.
9. Ви можете перевірити, чи служба Squid працює, в оснастці `services.msc` (знайдіть **Squid for Windows**).

Автономний репозиторій

Після виходу ERA версії 6.5 інструмент «Дзеркало» можна використовувати для створення автономного репозиторію (у Windows). Зазвичай це потрібно для закритих комп'ютерних мереж або мереж з обмеженим доступом до Інтернету. За допомогою інструмента «Дзеркало» можна створити клон репозиторію ESET у локальній папці. Цей клонований репозиторій можна потім перемістити (наприклад, на зовнішній диск) у розташування в закритій мережі. Його можна скопіювати в безпечне місце в локальній мережі та надати доступ до нього через сервер HTTP.

Щоб оновити автономний репозиторій, виконайте ту саму команду з тими самими параметрами, що використовувалися для його створення. Буде використано попередні дані в проміжній папці, а завантажуватимуться лише застарілі файли.



Увага

Зауважте, що розмір репозиторію збільшується й у проміжного каталогу буде такий самий розмір. Перш ніж починати цей процес, переконайтеся, що у вас є принаймні **600 ГБ** вільного місця.

Приклад сценарію для Windows

Частина 1. Клонування репозиторію

1. [Завантажте](#) інструмент «Дзеркало».
2. Видобудьте інструмент «Дзеркало» із завантаженого файлу *.zip*.
3. Підготуйте (створіть) папки для:
 - проміжних файлів;
 - кінцевої версії репозиторію.
4. Відкрийте командний рядок і змініть каталог на папку, яка містить видобутий інструмент «Дзеркало» (команда `cd`).
5. Виконайте цю команду (змініть проміжний каталог і каталог виводу репозиторію на папки з кроку 3):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^  
--intermediateRepositoryDirectory C:\Intermediary ^  
--outputRepositoryDirectory C:\Repository
```

6. Коли репозиторій буде скопійовано в папку `outputRepositoryDirectory`, перемістіть папку та її вміст на інший комп'ютер, який має доступ до закритої мережі.

Частина 2. Налаштування сервера HTTP

7. Потрібно, щоб сервер HTTP працював на комп'ютері, підключеному до закритої мережі. Для цього можна використати:

- Apache HTTP Proxy із [сайту завантаження](#) ESET (цей сценарій);
- інший сервер HTTP.

8. Відкрийте архів `apachehttp.zip` і видобудьте файли в папку `C:\Program Files\Apache HTTP Proxy`.
9. Відкрийте командний рядок адміністратора та змініть каталог на `C:\Program Files\Apache HTTP Proxy\bin` (команда `cd`).
10. Виконайте цю команду:

```
httpd.exe -k install -n ApacheHttpProxy
```

11. За допомогою простого текстового редактора відкрийте файл `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf` і внизу файлу додайте ці рядки:

```
Listen 80  
ServerRoot "C:\Program Files\Apache HTTP Proxy"  
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"  
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">  
Options Indexes FollowSymLinks  
AllowOverride None  
Require all granted  
</Directory>  
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

12. Запустіть службу **ApacheHttpProxy** за допомогою цієї команди:

```
sc start ApacheHttpProxy
```

13. Перевірте, чи служба працює. Для цього в браузері відкрийте сторінку <http://YourIPAddress:80/index.html> (замініть *YourIPAddress* на IP-адресу комп'ютера).

Частина 3. Запуск автономного репозиторію

14. Створіть папку для автономного репозиторію, наприклад *C:\Repository*..

15. У файлі *httpd.conf* замініть ці рядки

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"  
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
```

на адресу папки репозиторію, як показано нижче:

```
DocumentRoot "C:\Repository"  
<Directory "C:\Repository">
```

16. Скопіюйте завантажений репозиторій у розташування *C:\Repository* ..

17. Перезавантажте службу **ApacheHttpProxy** за допомогою цієї команди:

```
sc restart ApacheHttpProxy
```

18. Тепер автономний репозиторій працює за адресою <http://vashaIP-adresa> (наприклад, <http://10.1.1.10>).

19. Задайте нову адресу репозиторію:

- a. На [сервері ESET PROTECT](#) відкрийте веб-консоль ESET PROTECT і натисніть **Додатково > Параметри сервера**.
- b. Для всіх [агентів ESET Management](#) натисніть **Політики**.

Відмовостійкий кластер

Нижче наведено високорівневі кроки, необхідні для інсталяції ESET PROTECT у середовищі з відмовостійким кластером.



Примітка

Перегляньте також цю [статтю бази знань](#) про інсталяцію сервера ESET PROTECT в кластері.

1. Створіть відмовостійкий кластер зі спільним диском:

- [Інструкція зі створення відмовостійкого кластера на Windows Server 2016 і 2019 R2](#)
- [Інструкція зі створення відмовостійкого кластера на Windows Server 2012 і 2012 R2](#)
- [Інструкція зі створення відмовостійкого кластера на Windows Server 2008 R2](#)

2. У **майстрі створення кластера** введіть необхідні ім'я хоста (нове) і IP-адресу.

3. Запустіть спільний диск кластера на вузлі node1 та [інсталюйте сервер ESET PROTECT за допомогою відокремленого інсталятора](#) на цьому вузлі. Виберіть параметр **Це інсталяція в кластері** та встановіть спільний диск як сховище даних програм. Введіть нове ім'я хоста в сертифікат сервера ESET PROTECT поруч із попередньо вказаними іменами хостів. Запам'ятайте це ім'я хоста та використайте його на кроці 6 під час створення ролі сервера ESET PROTECT в Диспетчері кластера.

4. Вимкніть сервер ESET PROTECT на вузлі node1, запустіть спільний диск кластера на вузлі node2 та [інсталюйте сервер ESET PROTECT за допомогою відокремленого інсталятора](#) на цьому вузлі. Під час інсталяції виберіть параметр **Це інсталяція в кластері**. Установіть спільний диск як сховище даних

програм. Не змінюйте дані підключення до бази даних і відомості сертифікатів, оскільки їх вже було налаштовано під час інсталяції сервера ESET PROTECT на вузлі node1.

5. Відкрийте брандмауер і дозвольте вхідні з'єднання на всіх [портах](#), які використовує сервер ESET PROTECT.

6. У диспетчері кластера створіть і запустіть роль (*Налаштувати роль > Вибрати роль > Загальна служба...*) для служби сервера ESET PROTECT. Виберіть службу **сервера** ESET PROTECT зі списку доступних служб. Дуже важливо вказати для ролі те саме ім'я хоста, що на кроці 3 було вказано в сертифікаті сервера.



Примітка

Термін **Роль** доступний у Windows Server 2012 і новіших версій. У Windows Server 2008 R2 натомість використовується термін **Служби та програми**.

7. Інсталюйте агент ESET Management на всі вузли кластера за допомогою відокремленого інсталятора. На екранах **Конфігурація агента** та **Підключення до сервера ESET PROTECT** використовуйте те саме ім'я хоста, що й на кроці 6. Збережіть дані агента на локальному вузлі (, а не на кластерному диску).

8. Веб-сервер (Apache Tomcat) не підтримує використання кластера, тому його потрібно встановити на окремий диск або інший комп'ютер:

а. [Інсталюйте Web Console](#) на окремому комп'ютері й налаштуйте її для підключення до ролі кластера ESET PROTECT Server.

б. Після інсталяції веб-консолі перейдіть до її файлу конфігурації: `C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`

с. Відкрийте цей файл у Блокноті чи будь-якому іншому текстовому редакторі. У рядку `server_address=localhost` замініть значення «localhost» на IP-адресу або ім'я хоста для ролі кластера серверів ESET PROTECT.

Інсталяція компонентів у Linux

У багатьох сценаріях інсталяції передбачено встановлення різних компонентів ESET PROTECT на різних комп'ютерах, щоб пристосувати різні мережеві архітектури, дотриматися вимог щодо ефективності тощо.

Покрокові інструкції з інсталяції сервера ESET PROTECT див. [у цьому розділі](#).

Щоб оновити ESET PROTECT для Linux до останньої версії, див. розділ [Завдання з оновлення компонентів](#) або [статтю бази знань](#).



Примітка

Щоб інсталювати програмні пакети в Fedora, скористайтеся командою `dnf` замість `yum`.

Основні компоненти

- [Сервер ESET PROTECT](#)
- [Веб-консоль ESET PROTECT](#)
- [Агент ESET Management](#)
- Сервер [бази даних](#)

Додаткові компоненти

- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Проксі-сервер HTTP Apache](#)
- [Проксі-сервер Apache HTTP для агента – Підключення до сервера](#)

- [Інструмент «Дзеркало»](#)

Інсталяція та конфігурація MySQL

Інсталяція



Попередження

Обов'язково інстальуйте [підтримувану версію MySQL Server](#) та з'єднувача ODBC.

Якщо ви вже інстальували й налаштували MySQL, перейдіть до розділу [Конфігурація](#).

1. Перш ніж інстальувати базу даних у Linux, додайте репозиторій MySQL:

Debian, Ubuntu	Виконайте такі команди в Terminal: a) <code>wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb</code> b) <code>sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb</code> Див. також: Додавання репозиторію MySQL APT
CentOS, Red Hat, Fedora	Додавання репозиторію MySQL Yum
OpenSuse, SUSE Linux Enterprise Server	Додавання репозиторію MySQL SLES

2. Коли додасте репозиторій MySQL, оновіть локальний кеш репозиторію (наприклад, у Debian запустіть `sudo apt-get update`). Після цього ви зможете продовжити інсталяцію MySQL.

3. Процес інсталяції MySQL може відрізнятись залежно від розподілу та версії Linux:

Linux розподіл:	MySQL Команда інсталяції сервера:	MySQL Розширена інсталяція сервера:
Debian, Ubuntu	<code>sudo apt-get install mysql-server</code>	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-apt-repo.html
CentOS, Red Hat, Fedora	<code>sudo yum install mysql-server</code>	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-yum-repo.html
OpenSuse, SUSE Linux Enterprise Server	<code>sudo zypper install mysql-community-server</code>	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-sles-repo.html

- Інсталяція вручну. Завантажте й інстальуйте випуск MySQL Community Server зі сторінки <https://dev.mysql.com/downloads/mysql/>

Конфігурація

1. Щоб відкрити файл `my.cnf` (`my.ini` для Windows) у текстовому редакторі, виконайте цю команду:

```
sudo nano /etc/mysql/my.cnf
```

Якщо файлу немає, спробуйте команду `/etc/my.cnf` або `/etc/my.cnf.d/community-mysql-server.cnf`

2. Знайдіть конфігурацію в розділі `[mysqld]` файлу `my.cnf` і змініть значення. Якщо параметрів немає у файлі, додайте їх у розділ `[mysqld]`.

```
max_allowed_packet=33M
```

- Для MySQL 8 потрібно задати таку змінну:
`olog_bin_trust_function_creators=1`
Окрім цього, можна вимкнути ведення бінарного журналу: `log_bin=0`

- Для MySQL 5.6.20 і 5.6.21 (щоб визначити версію MySQL, скористайтеся `mysql --version`):
одля параметра `innodb_log_file_size` потрібно вказати значення не менше ніж **200 МБ** (наприклад, `innodb_log_file_size=200M`) і не більше ніж **3000 МБ**
- Для MySQL 5.6.22 й новіших підтримуваних версій (зокрема, версії 8):
одля параметра `innodb_log_file_size*innodb_log_files_in_group` потрібно вказати значення не менше ніж **200 МБ** (символ * позначає множення, і результат множення двох параметрів має бути більший ніж 200 МБ. Мінімальне значення для `innodb_log_files_in_group` - 2, а максимальне - 100. Значення має бути цілим числом).
Приклад:
`innodb_log_file_size=100M`
`innodb_log_files_in_group=2`

3. Збережіть і закрийте файл та введіть вказану нижче команду, щоб перезавантажити сервер MySQL і застосувати конфігурацію (у деяких випадках служба називається `mysqld`).

```
sudo service mysql restart
```

4. Щоб налаштувати MySQL, зокрема права та пароль, виконайте цю команду (цей крок необов'язковий; для деяких розподілів Linux це не можна зробити):

```
/usr/bin/mysql_secure_installation
```

5. Щоб перевірити, чи сервер MySQL працює, введіть таку команду:

```
sudo service mysql status
```

Інсталяція та конфігурація ODBC



Попередження

Обов'язково інстальуйте [підтримувану версію MySQL Server та з'єднувача ODBC](#).



Примітка

Ви можете інстальувати драйвер MS ODBC 13 або новішої версії, щоб підключити сервер ESET PROTECT у Linux до MS SQL Server у Windows. Щоб дізнатися більше, перегляньте [цю статтю бази знань](#).

Debian, Ubuntu

Виконайте такі команди в Terminal:

1. `sudo apt-get install unixodbc`
2. Завантажте з'єднувач ODBC:
 - Ubuntu 16: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
 - Ubuntu 18: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
 - Ubuntu 19 і 20: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
3. `gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz` (пакет може мати іншу назву залежно від використовуваного посилання).
4. `tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar` (пакет може мати іншу назву залежно від використовуваного посилання).

5. `cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit` (пакет може мати іншу назву залежно від використовуваного посилання).

6. `sudo cp bin/* /usr/local/bin`

7. `sudo cp lib/* /usr/local/lib`

8. Зареєструйте драйвер для ODBC. Для нових версій Linux (наприклад, Ubuntu 20.x) рекомендуємо використовувати драйвер Unicode; виберіть крок «а»). Для інших систем, або в тих випадках, коли драйвер Unicode не працює, виберіть крок «б»).

a. `sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t "Driver=/usr/local/lib/libmyodbc8w.so"`

b. `sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t "Driver=/usr/local/lib/libmyodbc8a.so"`

9. `myodbc-installer -d -l`

Додаткову інформацію див. за посиланням

<https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html>.

Інші підтримувані дистрибутиви Linux

1. Завантажте з'єднувач ODBC для MySQL з [офіційного сайту MySQL](#). Виберіть і завантажте версію, сумісну з вашим розподілом і версією Linux.

2. Щоб інсталювати драйвер ODBC, дотримуйтеся вказаних нижче інструкцій:

- **CentOS, Red Hat, Fedora:**

<https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-yum.html>

- **OpenSuse, SUSE Linux Enterprise Server:**

<https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html>

3. Щоб відкрити файл **odbcinst.ini** в текстовому редакторі, виконайте цю команду:

```
sudo nano /etc/odbcinst.ini
```

4. Скопіюйте вказану нижче конфігурацію у файл **odbcinst.ini** (переконайтеся, що шляхи до ключів **Драйвер** і **Налаштування** вказано правильно), а потім збережіть та закрийте його:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

У деяких дистрибутивах ключ «Драйвер» може мати інше розташування. Знайти файл можна за допомогою цієї команди:

```
sudo find /usr -iname "*libmyodbc*"
```

5. Оновіть файли конфігурації, які керують доступом ODBC до серверів бази даних на поточному хості. Для цього виконайте таку команду:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

Інсталяція сервера - Linux

Інсталяція сервера ESET PROTECT на Linux виконується за допомогою команди в терміналі. Ви можете підготувати скрипт інсталяції, а потім виконати його через `sudo`. Перед початком інсталяції переконайтеся, що всі [попередні вимоги](#) виконано.



Примітка

Щоб інстальювати сервер ESET PROTECT на SUSE Linux Enterprise Server (SLES), дотримуйтеся інструкцій зі [Статті бази знань](#)

1. Завантажте компонент ESET PROTECT Server:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server-linux-x86_64.sh
```

2. Зробіть завантажений файл виконуваним:

```
chmod +x server-linux-x86_64.sh
```

3. Запустіть сценарій інсталяції на основі наведеного нижче прикладу (Нові рядки розділяються символом "\", що дає змогу скопіювати всю команду в Terminal):

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

Ви можете змінити наступні атрибути:

Атрибут	Опис	Потрібно
--uninstall	Видаляє продукт.	-
--keep-database	Під час видалення бази даних видалено не буде.	-
--locale	Локальний ідентифікатор (LCID) інстальованого сервера (значення за замовчуванням – en_US). Див. доступні мови в пункті підтримувані мови . Примітка: Ви можете вибрати мову для кожної сесії веб-консолі ESET PROTECT.	Так
--skip-license	Інсталятор не просить користувача підтвердити ліцензійну угоду.	-
--skip-cert	Пропустити генерацію сертифікатів (використовувати з параметром --server-cert-path).	-
--license-key	Ліцензійний ключ ESET. Можна налаштувати пізніше.	-
--server-port	порт сервера ESET PROTECT (за замовчуванням: 2222).	-
--console-port	Порт консолі ESET PROTECT (за замовчуванням: 2223)	-
--server-root-password	Пароль для входу в обліковий запис адміністратора веб-консолі має містити не менше 8 символів.	Так
--db-type	Тип бази даних, яка буде використовуватися (можливі значення: "MySQL Server", "MS SQL Server"). MS SQL Server в Linux не підтримується. Однак ви можете підключити сервер ESET PROTECT у Linux до MS SQL Server у Windows .	-
--db-driver	Драйвер ODBC, який використовується для підключення до бази даних (команда <code>odbcinst -q -d</code> відображає список доступних драйверів. Використовуйте один із наступних драйверів: --db-driver=MySQL.	Так
--db-hostname	Ім'я комп'ютера або IP-адреса сервера бази даних. Екземпляр бази даних з іменем не підтримується.	Так

Атрибут	Опис	Потрібно
--db-port	Порт сервера бази даних (за замовчуванням: 3306).	Так
--db-name	Ім'я бази даних сервера ESET PROTECT (за замовчуванням: era_db).	-
--db-admin-username	Ім'я адміністратора бази даних (використовується інсталятором для створення та налаштування бази даних). Можна пропустити цей параметр, якщо в параметрах --db-user-username і --db-user-password визначено раніше створеного користувача бази даних	Так
--db-admin-password	Пароль адміністратора бази даних. Можна пропустити цей параметр, якщо в параметрах --db-user-username і --db-user-password визначено раніше створеного користувача бази даних	Так
--db-user-username	Ім'я користувача сервера ESET PROTECT бази даних (використовується для підключення сервера ESET PROTECT до бази даних); макс. довжина – 16 символів.	Так
--db-user-password	Пароль користувача сервера ESET PROTECT бази даних	Так
--cert-hostname	Містить усі можливі імена та/або IP-адреси комп'ютера, на якому буде встановлено сервер ESET PROTECT. Цей параметр має збігатися з іменем сервера, зазначеним у сертифікаті агента, що намагається підключитися до сервера.	Так
--server-cert-path	Шлях до сертифікату однорангового вузла сервера (використовуйте цей параметр, якщо ви також вибрали --skip-cert)	-
--server-cert-password	Пароль сертифікату однорангового вузла сервера	-
--agent-cert-password	Пароль сертифікату однорангового вузла агента	-
--cert-auth-password	Пароль Центру сертифікації	-
--cert-auth-path	Шлях до файлу Центру сертифікації сервера	-
--cert-auth-common-name	Загальне ім'я Центру сертифікації (використовуйте «»)»	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	Термін дії сертифікату в днях або роках (вказіть в аргументі --cert-validity-unit)	-
--cert-validity-unit	Одиниця виміру терміну дії сертифікату, можливі значення: «Years» (роки) або «Days» (дні) (за замовчуванням: Years)	-
--ad-server	Сервер Active Directory	-
--ad-user-name	Ім'я користувача, який має права на виконання пошуку мережі AD	-
--ad-user-password	Пароль користувача Active Directory	-
--ad-cdn-include	Шлях до дерева Active Directory, що буде використано для синхронізації; щоб синхронізувати все дерево, використовуйте порожні лапки	-
--enable-imp-program	Увімкнути програму удосконалення продуктів.	-
--disable-imp-program	Вимкнути програму удосконалення продуктів.	-

4. Спочатку вам знадобиться відповісти, чи погоджуєтеся ви взяти участь у програмі покращення продукту. Натисніть **Y**, якщо ви згодні надсилати звіти про аварійне завершення роботи та телеметричні дані до ESET, або **N**, щоб не надсилати жодних даних.

5. Сервер ESET PROTECT та службу eraserver буде інстальовано за наступним шляхом:

```
/opt/eset/RemoteAdministrator/Server
```

6. Після інсталяції переконайтеся, що службу сервера ESET PROTECT можна запустити за допомогою наведеної нижче команди:

service eraserver status

```
root@protect:~  
[root@protect ~]# service eraserver status  
Redirecting to /bin/systemctl status eraserver.service  
● eraserver.service - ESET PROTECT Server  
   Loaded: loaded (/etc/systemd/system/eraserver.service; enabled; vendor preset: disabled)  
   Active: active (running) since Thu 2020-11-26 11:58:09 CET; 4h 22min ago  
 Main PID: 2670 (ERAServer)  
   CGroup: /system.slice/eraserver.service  
           └─2670 /opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid  
  
Nov 26 11:58:09 protect.local systemd[1]: Starting ESET PROTECT Server...  
Nov 26 11:58:09 protect.local systemd[1]: Started ESET PROTECT Server.  
[root@protect ~]#
```

Журнал інстальатора

Журнал інстальатора може знадобитися для виправлення неполадок. Знайти його можна в папці [Файли журналу](#).

Попередні вимоги до сервера - Linux

Щоб інсталювати сервер ESET PROTECT у Linux, потрібно виконати вказані нижче вимоги.

- Необхідно мати дійсну [ліцензію](#).
- [Сервер бази даних має бути інстальовано й налаштовано](#) за допомогою облікового запису root. Обліковий запис користувача не обов'язково створювати до інсталяції, це може зробити інстальатор. [MS SQL Server в Linux](#) не підтримується. Однак ви можете [підключити сервер ESET PROTECT у Linux до MS SQL Server у Windows](#).



Примітка

Сервер ESET PROTECT зберігає в базі даних великі бінарні об'єкти. Для належної роботи ESET PROTECT потрібно налаштувати MySQL [для приймання пакетів великих розмірів](#).

- **Драйвер ODBC** використовується, щоб установлювати підключення із [сервером бази даних](#) (MySQL).
- Файл інсталяції сервера потрібно вказати як виконуваний. Для цього виконайте таку команду терміналу:

```
chmod +x server-linux-x86_64.sh
```
- **Рекомендуємо використовувати останню версію OpenSSL(1.1.1)**. Мінімальна підтримувана версія OpenSSL – openssl-1.0.1e-30. В одній системі одночасно може бути інстальовано кілька версій OpenSSL. Принаймні одна з них має бути підтримуваною.

ОЩоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
ОВи можете переглянути перелік усіх версій OpenSSL, інстальованих у системі. Щоб переглянути список розширень файлів, скористайтеся командою `sudo find / -iname *libcrypto.so*`.
ОКористувачі *Fedora Linux* мають використовувати пакет `compat-openssl10`.

- **Xvfb** – вимагається для належного друку звітів у серверних системах Linux без графічного інтерфейсу ([створення звіту](#)).
- **cifs-utils** – вимагається для належного розгортання агента в ОС Windows.
- **Бібліотеки Qt4 WebKit** – використовуються для друку звітів у форматах PDF і PS (потрібно використовувати версію 4.8, а не 5). Усі інші залежності Qt4 буде інстальовано автоматично. Якщо використовується CentOS, пакет може бути відсутній в офіційних репозиторіях. Ви можете [інстальувати його з репозиторію третьої сторони](#) (наприклад, EPEL) або самостійно створити його на цільовому комп'ютері.
- **kinit + klist** – Kerberos використовується для автентифікації користувача домену під час входу та виконання завдання синхронізації Active Directory. Переконайтеся, що Kerberos налаштовано належним чином (*/etc/krb5.conf*). ESET PROTECT 8.0 підтримує синхронізацію з кількома доменами.
- **ldapsearch** – використовується для авторизації та завдання синхронізації AD.
- **snmptrap** – використовується для надсилання пасток SNMP. Якщо функція не використовуватиметься, цей параметр необов'язковий. SNMP також потрібно налаштувати.
- **Пакет розробника SELinux** – використовується під час інсталяції продукту для створення модулів політики SELinux. Це потрібно лише в системах, у яких увімкнено SELinux (CentOS, Fedora, RHEL). SELinux може спричиняти проблеми з іншими програмами. Для сервера ESET PROTECT цей параметр необов'язковий.

Таблиця нижче містить відповідні команди терміналу для кожного описаного вище пакета для різних розподілів Linux.

Пакет	Дистрибутиви Debian і Ubuntu	Дистрибутиви CentOS, Red Hat і Fedora	Дистрибутив OpenSUSE
ODBC драйвер	Перегляньте розділ Інсталяція та конфігурація ODBC .		
xvfb	<code>apt-get install xvfb</code>	<code>yum install xorg-x11-server-Xvfb</code>	<code>zypper install xorg-x11-server-extra</code>
cifs-utils	<code>apt-get install cifs-utils</code>	<code>yum install cifs-utils</code>	<code>zypper install cifs-utils</code>
Бібліотеки Qt4 WebKit	<code>apt-get install libqtwebkit4</code>	Перегляньте статтю бази знань .	<code>zypper install libqtwebkit4</code>
kinit + klist – необов'язково (потрібно для служби Active Directory)	<code>apt-get install krb5-user</code>	<code>yum install krb5-workstation</code>	<code>zypper install krb5</code>
ldapsearch	<code>apt-get install ldap-utils libsasl2-modules-gssapi-mit</code>	<code>yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap</code>	<code>zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop</code>
snmptrap	<code>apt-get install snmp</code>	<code>yum install net-snmp-utils net-snmp</code>	<code>zypper install net-snmp</code>
Пакет розробника SELinux (необов'язково для сервера ESET PROTECT; SELinux може спричиняти проблеми з іншими програмами)	<code>apt-get install selinux-policy-dev</code>	<code>yum install policycoreutils-devel</code>	<code>zypper install selinux-policy-devel</code>

Пакет	Дистрибутиви Debian і Ubuntu	Дистрибутиви CentOS, Red Hat і Fedora	Дистрибутив OpenSUSE
samba (необов'язково, потрібно лише для віддаленого розгортання)	apt-get install samba	yum install samba samba-winbind-clients	zypper install samba samba-client

Інсталяція агента - Linux

Інсталяція агента ESET Management на Linux виконується за допомогою команди в терміналі. Переконайтеся, що всі [попередні вимоги](#) виконано.

1. Завантажте сценарій інсталяції агента:

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Зробіть файл виконуваним:

```
chmod +x agent-linux-x86_64.sh
```

3. Запустіть сценарій інсталяції на основі наведеного нижче прикладу (Нові рядки розділяються символом "\", що дає змогу скопіювати всю команду в Terminal):

Інсталяція з використанням сервера

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.179.36 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Інсталяція в автономному режимі

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

Параметри:

Підключення до сервера ESET PROTECT налаштовується за допомогою параметрів --hostname та --port (за наявності запису SRV порт не використовується). [Можливі формати підключення.](#)

- **Ім'я хоста та порт**
- **Адреса IPv4 та порт**
- **Адреса IPv6 і порт**
- Запис служби (запис SRV) – щоб налаштувати запис ресурсів DNS у Linux, комп'ютер повинен знаходитися в одному домені з працюючим сервером DNS. Див. [Запис ресурсів DNS](#). Запис SRV повинен починатися з префікса «_NAME._tcp», де «NAME» – це власне ім'я (наприклад, «era»).

Атрибут	Опис	Потрібно
--hostname	IP-адреса або ім'я хоста сервера ESET PROTECT для підключення.	Так
--port	Порт сервера ESET PROTECT (за замовчуванням: 2222).	Так

Атрибут	Опис	Потрібно
--cert-path	Локальний шлях до файлу сертифіката агента (див. докладніше про сертифікат).	Так (в автономному режимі)
--cert-auth-path	Шлях до файлу Центру сертифікації сервера (див. докладніше про центр).	Так (в автономному режимі)
--cert-password	Пароль сертифіката агента.	Так (в автономному режимі)
--cert-auth-password	Пароль Центру сертифікації.	Так (якщо використовується)
--skip-license	Інсталятор не просить користувача підтвердити ліцензійну угоду.	Ні
--cert-content	Для налаштування захищених каналів зв'язку із сервером і агентами використовується зашифрований вміст у форматі Base64 зашифрованого сертифіката відкритого ключа у форматі PKCS12 та приватний ключ. Використовуйте лише один із параметрів: --cert-path або --cert-content.	Ні
--cert-auth-content	Для перевірки віддалених вузлів (проксі-сервера або звичайного сервера) використовується зашифрований вміст у форматі Base64 зашифрованого сертифіката приватного ключа у форматі DER. Використовуйте лише один із параметрів: --cert-auth-path або --cert-auth-content.	Ні
--webconsole-hostname	Ім'я хоста або IP-адреса, які використовує веб-консоль для підключення до сервера (якщо залишити це поле порожнім, його значення буде скопійовано з поля «Ім'я хоста»).	Ні
--webconsole-port	Порт, який використовує веб-консоль для підключення до сервера (значення за замовчуванням – 2223).	Ні
--webconsole-user	Ім'я користувача, яке використовує веб-консоль для підключення до сервера (значення за замовчуванням – Administrator).	Ні
--webconsole-password	Пароль, який використовує веб-консоль для підключення до сервера.	Так (S-a)
--proxy-hostname	Ім'я хоста проксі-сервера HTTP для підключення до сервера.	Якщо використовується проксі-сервер
--proxy-port	Порт проксі-сервера HTTP для підключення до сервера.	Якщо використовується проксі-сервер
--proxy-user	Ім'я користувача проксі-сервера HTTP.	Якщо використовується проксі-сервер
--proxy-password	Пароль проксі-сервера HTTP.	Якщо використовується проксі-сервер
--enable-imp-program	Взяти участь у програмі удосконалення продуктів.	Ні
--disable-imp-program	Відмовитися від участі в програмі вдосконалення продуктів.	Ні

Підключення та сертифікати

- **Необхідно встановити з'єднання із сервером ESET PROTECT:** --hostname, --port (за наявності запису служби вказувати порт не потрібно, порт за замовчуванням: 2222)
- Для **інсталяції з використанням сервера** надайте наступні дані для підключення: --webconsole-port, --webconsole-user, --webconsole-password
- Для **інсталяції в автономному режимі** надайте дані про сертифікат: --cert-path, --cert-password

Для використання параметрів інсталяції --cert-path і --cert-auth-path потрібні файли сертифікатів (.pfx та .der), які можна експортувати з веб-консолі ESET PROTECT. (Ознайомтеся з інструкціями щодо [експорту файлів .pfx і .der.](#))

Параметри типу пароля

Параметри типу пароля можна задати за допомогою змінних середовища чи файлів, зчитати stdin або надати у вигляді тексту. Перелік параметрів:

- password=env:SECRET_PASSWORD, де SECRET_PASSWORD – це змінна середовища з паролем;
- password=file:/opt/secret, де перший рядок звичайного файлу /opt/secret містить ваш пароль;
- password=stdin вказує інстальатору зчитати пароль зі стандартного вводу;
- password="pass:PASSWORD" є аналогом --password="PASSWORD". Цей параметр необхідно використовувати, якщо як пароль використовується значення "stdin"(standard input) або рядок, що починається з "env:", "file:" чи "pass:"



Попередження

Парольна фраза сертифіката не може містити такі символи: " \ Ці символи спричиняють критичну помилку під час ініціалізації агента.

Підключення до проксі-сервера HTTP

Якщо ви використовуєте проксі-сервер HTTP, то можете вказати параметри підключення в --proxy-hostname, --proxy-port, --proxy-user і --proxy-password.

ПРИКЛАД - інсталяція агента в автономному режимі за допомогою проксі-сервера HTTP

```
./agent-linux-x86_64.sh \  
--skip-license \  
--cert-path=/home/admin/Desktop/agent.pfx \  
--cert-auth-path=/home/admin/Desktop/CA.der \  
--cert-password=N3llluI4#2aCC \  
--hostname=10.1.179.36 \  
--port=2222 \  
--proxy-hostname=10.1.180.3 \  
--proxy-port=3333 \  
--proxy-user=Administrator \  
--proxy-password=AdMiN_p1$$w0r4
```



Увага

Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT, для якого потрібна автентифікація, не працюватиме.

Якщо ви не виберете порт для веб-консолі або агента за замовчуванням, можливо, потрібно буде налаштувати брандмауер відповідним чином. В іншому разі інсталяція може закінчитися невдало.

Журнал інстальатора

Журнал інстальатора може знадобитися для виправлення неполадок. Знайти його можна в папці [Файли журналу](#).

Щоб дізнатися, чи інсталяція пройшла успішно, перевірте, чи служба працює. Для цього виконайте таку команду:

```
sudo service eraagent status
```

Оновлення та виправлення агента в Linux

Якщо вручну запустити інсталяцію агента в системі, де вже встановлено агента, можливі такі сценарії:

- **Оновлення** – запускається більш актуальна версія інсталлятора.
Оінсталяція з використанням сервера – програма оновлюється, але зберігає попередні сертифікати.
Оінсталяція в автономному режимі – програма оновлюється, після чого використовуються нові сертифікати.
- **Виправлення** – запускається та сама версія інсталлятора. Цю функцію можна використовувати для міграції агента на інший сервер ESET PROTECT.
Оінсталяція з використанням сервера – програма інсталюється повторно й отримує поточні сертифікати із сервера ESET PROTECT (згідно з параметром `hostname`).
Оінсталяція в автономному режимі – програма інсталюється повторно, після чого використовуються нові сертифікати.

Якщо ви виконуєте міграцію агента на більшу нову версію сервера ESET PROTECT та використовуєте інсталяцію з використанням сервера, команду інсталяції необхідно запускати двічі. Перша команда оновить агент, а друга – отримає нові сертифікати для підключення агента до сервера ESET PROTECT.

Попередні вимоги до агента - Linux

Щоб інсталювати компонент агента ESET Management у Linux, потрібно виконати вказані нижче вимоги.

Попередні умови для інсталяції агента з використанням сервера

- Необхідно забезпечити можливість підключення до комп'ютера до сервера з мережі. Крім того, на ньому має бути інсталювано [сервер ESET PROTECT](#) і [веб-консоль ESET PROTECT](#).
- **Рекомендуємо використовувати останню версію OpenSSL(1.1.1)**. Мінімальна підтримувана версія OpenSSL – openssl-1.0.1e-30. В одній системі одночасно може бути інсталювано кілька версій OpenSSL. Принаймні одна з них має бути підтримуваною.
ОЩоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
ОВи можете переглянути перелік усіх версій OpenSSL, інсталюваних у системі. Щоб переглянути список розширень файлів, скористайтеся командою `sudo find / -iname *libcrypto.so*`.
ОКористувачі *Fedora Linux* мають використовувати пакет `compat-openssl10`.

Попередні умови для інсталяції агента в автономному режимі

- Необхідно забезпечити можливість підключення до комп'ютера до сервера з мережі. Крім того, на ньому має бути інсталювано [сервер ESET PROTECT](#).
- Також слід підготувати [сертифікат](#) агента
- Крім того, потрібен файл відкритого ключа [центру сертифікації](#) сервера
- **Рекомендуємо використовувати останню версію OpenSSL(1.1.1)**. Мінімальна підтримувана версія OpenSSL – openssl-1.0.1e-30. В одній системі одночасно може бути інсталювано кілька версій OpenSSL. Принаймні одна з них має бути підтримуваною.
ОЩоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
ОВи можете переглянути перелік усіх версій OpenSSL, інсталюваних у системі. Щоб переглянути список розширень файлів, скористайтеся командою `sudo find / -iname *libcrypto.so*`.
ОКористувачі *Fedora Linux* мають використовувати пакет `compat-openssl10`.



Примітка

Для Linux CentOS рекомендовано інстальювати пакет `policycoreutils-devel`. Для цього виконайте таку команду:
`yum install policycoreutils-devel`

Інсталяція веб-консолі - Linux

Дотримуйтеся цих інструкцій, щоб інстальювати ESET PROTECT Web Console:

1. Інсталюйте пакети Apache Tomcat і Java. Використовуйте команди терміналу залежно від дистрибутивів Linux. Наведені нижче приклади назв пакетів можуть відрізнятися від пакетів, доступних у репозиторії дистрибутива Linux.

Дистрибутиви Debian і Ubuntu	<code>sudo apt-get update</code> <code>sudo apt-get install openjdk-11-jdk tomcat9</code>
Дистрибутиви CentOS, Red Hat і Fedora	<code>yum update</code> <code>yum install java-1.8.0-openjdk tomcat</code>
OpenSUSE	<code>zypper refresh</code> <code>zypper install java-1_8_0-openjdk tomcat</code>

2. Завантажте файл Web Console (`era.war`):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. Скопіюйте файл `era.war` у папку Tomcat:

Дистрибутиви Debian і Ubuntu	<code>sudo cp era.war /var/lib/tomcat9/webapps/</code>
Дистрибутиви CentOS, Red Hat і Fedora	<code>sudo cp era.war /var/lib/tomcat/webapps/</code>
Дистрибутив OpenSUSE	<code>sudo cp era.war /usr/share/tomcat/webapps/</code>

Крім того, ви можете видобути вміст файлу `era.war` до `/var/lib/tomcat/webapps/era/`

4. Перезапустіть службу Tomcat і розгорніть файл `.war`:

Дистрибутиви Debian і Ubuntu	<code>sudo service tomcat9 restart</code>
Дистрибутиви CentOS, Red Hat і Fedora	<code>sudo service tomcat restart</code>
Дистрибутив OpenSUSE	<code>sudo service tomcat restart</code>

5. Якщо веб-консоль ESET PROTECT і сервер ESET PROTECT інстальовано на різних комп'ютерах, виконайте дії нижче, щоб забезпечити обмін даними між веб-консоллю ESET PROTECT та сервером ESET PROTECT.

I.Зупиніть роботу служби Tomcat: `sudo service tomcat9 stop`.

II.Відредагуйте файл **EraWebServerConfig.properties**:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties
```

Якщо файл **EraWebServerConfig.properties** не розташовано за вказаним вище шляхом, ви можете скористатися наступною командою, щоб знайти його:

```
find / -iname "EraWebServerConfig.properties"
```

III.Знайдіть рядок `server_address=localhost`.

IV.Замініть `localhost` на IP-адресу вашого сервера ESET PROTECT та збережіть файл.

V.Перезавантаження служби Tomcat: `sudo service tomcat9 restart`

Перевірте підключення до веб-консолі ESET PROTECT після інсталяції. Перейдіть за наступним посиланням у [підтримуваному браузері](#) на локальному хості (відобразиться екран входу):

<http://localhost:8080/era> або, якщо працює віддалене підключення до сервера, `http://IP_ADDRES_OR_HOSTNAME:8080/era`



Примітка

- Під час ручної інсталяції Apache Tomcat порт 8080 буде встановлено як порт HTTP за замовчуванням. Ви також можете налаштувати [підключення HTTPS для Apache Tomcat](#).
- Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).

Інсталяція проксі-сервера - Linux

У ESMC 7 функцію проксі-сервера ERA замінено на Apache HTTP Proху, що зазвичай розповсюджується в пакеті `apache2` або `httpd`. Агенти ESET Management Agent можуть підключатися до ESET PROTECT Server через Apache HTTP Proху. Дізнайтеся більше про те, [як проксі-сервер працює для агентів ESET Management](#).

Виберіть потрібний сценарій:

- [Нова інсталяція в Linux](#)
- [Оновлення з попередньої версії інстальованого в Linux проксі-сервера ERA](#)
- [Оновлення проксі-сервера ERA Proху в Linux або на віртуальному пристрої](#)

Нова інсталяція в Linux

1. [Інсталюйте та налаштуйте проксі-сервер Apache HTTP](#).

2. Налаштуйте в проксі-сервері Apache HTTP переадресацію підключень агентів.

а. На проксі-сервері відкрийте файл

і. Дистрибутиви Debian

`/etc/apache2/mods-available/proxy.conf`

ii. Дистрибутиви Red Hat

`/etc/httpd/conf/httpd.conf`

б. Додайте в кінці файлу рядок із портом, за допомогою якого агент підключається до сервера ESET PROTECT. За замовчуванням це порт 2222.

`AllowCONNECT 443 563 2222 8883`

с. На проксі-сервері відкрийте файл

і. Дистрибутиви Debian

`/etc/apache2/apache2.conf`

ii. Дистрибутиви Red Hat

`/etc/httpd/conf/httpd.conf`

d. Знайдіть цей рядок

```
Listen 80
```

і змініть його на

```
Listen 3128
```

e. Якщо ви додали обмеження для IP-адрес у конфігурації проксі-сервера (крок 1), потрібно надати доступ до сервера ESET PROTECT.

Додайте окремий сегмент ProxyMatch.

I. Адреса, яку агенти використовують для підключення до сервера ESET PROTECT.

II. Усі інші адреси сервера ESET PROTECT (IP-адреса, повне доменне ім'я).

(Додайте весь указаний нижче код; IP-адреса 10.1.1.10 та ім'я хоста hostname.example є лише прикладами, їх потрібно замінити своїми адресами. Ви також можете створити вираз ProxyMatch в [цій статті бази знань](#).)

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\.)*?|10\.1\.1\.10(:[0-9]+)?(\.)*?)$>
Allow from all
</ProxyMatch>
```

f. Перезавантаження служби *Apache HTTP Proxy*.

Оновлення з попередньої версії інстальованого в Linux проксі-сервера ERA

Оновлення середовища з проксі-сервером ERA 6.x у Linux дуже схоже на [оновлення Windows](#), за винятком налаштування шляхів до файлів. Виконайте вказівки зі [статті про оновлення інфраструктури](#) та скористайтеся відповідним пакетом і шляхами до файлів для вашого дистрибутива Linux.

Переглянути практичні поради для оновлення інфраструктури, у якій використовується проксі-сервер ERA, можна в [вказаних нижче посібниках](#).

- [Оновлення проксі-сервера ERA Proxy в Linux або на віртуальному пристрої](#)
- [Оновлення проксі-сервера ERA на хості Windows](#)

Налаштування SELinux

Якщо проксі-сервер використовується на віртуальному пристрої ESET PROTECT, політику SELinux потрібно змінити (інші дистрибутиви Linux можуть мати такі самі вимоги). Відкрийте термінал на віртуальному пристрої ESET PROTECT і виконайте вказані нижче команди.

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

```
sudo semanage port -a -t http_port_t -p tcp 2222
```

Попередні вимоги й інсталяція Rogue Detection Sensor - Linux

Щоб інсталювати компонент RD Sensor в Linux, потрібно виконати вказані нижче дії.

1. Переконайтеся, що перелічені далі попередні вимоги виконано.
 - Мережа доступна для виявлення (порти відкрито, брандмауер не блокує вхідний обмін даними тощо).

- Комп'ютер, на якому встановлено сервер, доступний.
- [Агент ESET Management](#) має бути встановлено на локальному комп'ютері, щоб повністю підтримувати всі програмні функції.
- Термінал відкрито.
- Файл інсталяції RD Sensor потрібно вказати як виконуваний.

```
chmod +x rdsensor-linux-x86_64.sh
```

2. Щоб запустити файл інсталяції як sudo, скористайтеся цією командою:

```
sudo ./rdsensor-linux-x86_64.sh
```

3. Прочитайте ліцензійну угоду з кінцевим користувачем. Щоб перейти на наступну сторінку угоди, натисніть **клавiшу пробiлу**.

У вікні запиту потрібно буде вказати, чи приймаєте ви умови угоди. Якщо приймаєте, натисніть клавiшу **Y** на клавіатурі, якщо ні – **N**.

4. Якщо ви погоджуєтесь взяти участь у програмі покращення продукту, натисніть клавiшу **Y**, якщо ні – **N**.

5. ESET Rogue Detection Sensor запуститься після завершення інсталяції.

6. Щоб дізнатися, чи інсталяція пройшла успішно, перевірте, чи служба працює. Для цього виконайте таку команду:

```
sudo service rdsensor status
```

7. Файл журналу Rogue Detection Sensor розташовано в папці [Файли журналу](#):

```
/var/log/eset/RogueDetectionSensor/trace.log
```

Інсталяція Mobile Device Connector - Linux

Ви можете інстальювати Mobile Device Connector та сервер ESET PROTECT на різних серверах. Це може бути корисно, якщо, наприклад, потрібно мати доступ до Mobile Device Connector через Інтернет, щоб мобільними пристроями користувача можна було керувати коли завгодно.

Інсталяція компонента MDC на Linux виконується за допомогою команди в терміналі. Переконайтеся, що всі [попередні вимоги](#) виконано. Ви можете підготувати сценарій інсталяції, а потім виконати його через sudo.

Існує багато додаткових параметрів інсталяції, однак деякі є обов'язковими.

Для інсталяції потрібен [сертифікат однорангового вузла](#) ESET PROTECT. Сертифікат однорангового вузла ESET PROTECT можна отримати двома способами.

- **Інсталяція із сервера.** Для цього потрібно вказати облікові дані адміністратора веб-консолі ESET PROTECT (інсталятор завантажить необхідні сертифікати автоматично).
- **Інсталяція в автономному режимі.** Для цього потрібно надати сертифікат однорангового вузла (сертифікат проксі-сервера, [експортований](#) з ESET PROTECT). Замість нього можна використати [налаштовуваний сертифікат](#).

Нижче вказано параметри інсталяції, які обов'язково потрібно вказати.

Сертифікат HTTPS (проксі-сервер):

```
--https-cert-path=  
--https-cert-password=
```


Сертифікат однорангового вузла:

Для способу **Інсталяція із сервера** потрібно вказати принаймні цей параметр:

```
--webconsole-password=
```

Для способу **Інсталяція в автономному режимі** потрібно вказати ці параметри:

```
--cert-path=  
--cert-password= (пароль для сертифіката агента за замовчуванням, створеного під час початкової  
інсталяції сервера ESET PROTECT, не потрібний)
```

Підключення до сервера ESET PROTECT (ім'я або IP-адреса сервера):

```
--hostname=
```

Для бази даних MySQL потрібно вказати ці параметри:

```
--db-type="MySQL Server"  
--db-driver=  
--db-admin-username=  
--db-admin-password=  
--db-user-password=
```

Для бази даних MSSQL потрібно вказати ці параметри:

```
--db-type="Microsoft SQL Server"  
--db-driver=  
--db-admin-username=  
--db-admin-password=  
--db-user-password=
```

Приклад сценарію інсталяції

Запустіть сценарій інсталяції на основі наведеного нижче прикладу (Нові рядки розділяються символом "\", що дає змогу скопіювати всю команду в Terminal):

```
sudo ./mdmcore-linux-x86_64-0.0.0.0.sh \  
--https-cert-path="full_path/proxycert.pfx" \  
--https-cert-password="123456789" \  
--port=2222 \  
--db-type="MySQL Server" \  
--db-driver="MySQL ODBC 8.0 Driver" \  
--db-admin-username="root" \  
--db-admin-password=123456789 \  
--db-user-password=123456789 \  
--db-hostname="127.0.0.1" \  
--webconsole-password=123456789 \  
--hostname=username.LOCAL \  
--mdm-hostname=username.LOCAL
```

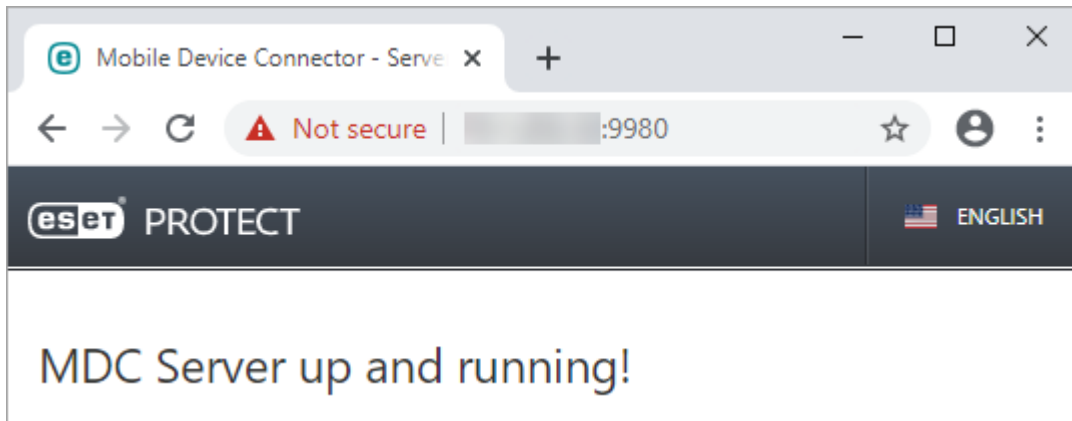
Щоб переглянути повний перелік доступних параметрів (друк повідомлення довідки), введіть таку команду:

--help

Журнал інстальатора

Журнал інстальатора може знадобитися для виправлення неполадок. Знайти його можна в папці [Файли журналу](#).

Коли інсталяція завершиться, перевірте, чи Mobile Device Connector працює належним чином. Для цього відкрийте в браузері сторінку <https://ім'я-хоста-mdm:порт-реєстрації> (наприклад, <https://eramdm:9980>). Якщо інсталяцію виконано успішно, з'явиться таке повідомлення:



За допомогою цієї URL-адреси можна також перевіряти доступність сервера, на якому інстальовано Mobile Device Connector, в Інтернеті (якщо виконано відповідні налаштування). Для цього перейдіть за цим посиланням на мобільному пристрої. Якщо сторінка недоступна, перевірте брандмауер і конфігурацію інфраструктури мережі.

Попередні вимоги до Mobile Device Connector - Linux

Щоб інстальувати Mobile Device Connector в Linux, потрібно виконати вказані нижче вимоги.

- Сервер бази даних уже інстальовано й налаштовано за допомогою облікового запису root (обліковий запис користувача не обов'язково створювати до інсталяції, це може зробити інстальатор).
- Для підключення до [сервера бази даних](#) (MySQL / MS SQL) на комп'ютері потрібно інстальувати драйвер ODBC. Перегляньте розділ [Інсталяція та конфігурація ODBC](#).



Примітка

Щоб під час підключення MDC до бази даних MySQL не виникало проблем, потрібно використовувати пакет unixODBC_23 (а не пакет unixODBC за замовчуванням). Особливо це стосується SUSE Linux.



Примітка

Рекомендуємо розгортати компонент MDM на хост-пристрої, на якому не розміщено сервер ESET PROTECT.

- Файл інсталяції MDMCore потрібно вказати як виконуваний.

```
chmod +x mdmcore-linux-x86_64.sh
```

- Після інсталяції переконайтеся, що служба MDMCore працює.

```
service eramdmcore status
```

- **Рекомендуємо використовувати останню версію OpenSSL(1.1.1)**. Мінімальна підтримувана

версія OpenSSL – openssl-1.0.1e-30. В одній системі одночасно може бути інстальовано кілька версій OpenSSL. Принаймні одна з них має бути підтримуваною.

ОЩоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
ОВи можете переглянути перелік усіх версій OpenSSL, інстальованих у системі. Щоб переглянути список розширень файлів, скористайтеся командою `sudo find / -iname *libcrypto.so*`.
ОКористувачі *Fedora Linux* мають використовувати пакет `compat-openssl10`.



Примітка

Якщо база даних MDM у MySQL завелика (тисячі пристроїв), значення за замовчуванням `innodb_buffer_pool_size` буде замалим. Щоб дізнатися більше про оптимізацію бази даних, перегляньте сторінку <https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html>.

Вимоги до сертифіката

- Для безпечного обміну даними через протокол HTTPS потрібен **сертифікат SSL** у форматі `.pfx`. Рекомендуємо використовувати сертифікат, наданий Центром сертифікації (ЦС ESET PROTECT або сторонній ЦС). Не радимо використовувати самопідписані сертифікати, оскільки не всі мобільні пристрої дозволяють користувачам приймати такі сертифікати. Натомість сертифікати, підписані ЦС, є довіреними й не вимагають дій зі сторони користувача.
- Щоб об'єднати їх в один файл `.pfx`, потрібно мати сертифікат, підписаний ЦС (ESET PROTECT або стороннім ЦС), відповідний закритий ключ і виконати стандартні процедури (зазвичай за допомогою OpenSSL):
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
Це стандартна процедура для більшості серверів, які використовують сертифікати SSL.
- Щоб виконати [інсталяцію в автономному режимі](#), потрібно надати сертифікат однорангового вузла (**сертифікат агента**, [експортований](#) з ESET PROTECT). Замість нього в ESET PROTECT можна використовувати [налаштовуваний сертифікат](#).

Інсталяція проксі-сервера Apache HTTP - Linux

Виберіть спосіб інсталяції [проксі-сервера Apache HTTP](#) відповідно до дистрибутива Linux на сервері. Якщо ви також хочете використовувати Apache для кешування результатів від ESET Dynamic Threat Defense, див. відповідну [документацію](#).

Інсталяція проксі-сервера Apache HTTP на Linux (загальне розповсюдження)

1. Інсталюйте проксі-сервера Apache HTTP (версії 2.4.10 або вище).
2. Перевірте, чи завантажено наступні модулі:

```
access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile,  
authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
```

3. Додайте конфігурацію кешування:

```
CacheEnable disk http://  
CacheDirLevels 4  
CacheDirLength 2  
CacheDefaultExpire 3600  
CacheMaxFileSize 200000000  
CacheMaxExpire 604800  
CacheQuickHandler Off  
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Якщо каталог `/var/cache/apache2/mod_cache_disk` не існує, створіть його та надайте йому права Apache (r,w,x).
5. Add Proxy configuration:

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Увімкніть доданий проксі-сервер кешування та конфігурацію (якщо конфігурація перебуває в основному файлі конфігурації Apache, цей крок можна пропустити).

7. Якщо потрібно, вкажіть інший порт прослуховування (за замовчуванням це порт 3128).

8. Необов'язкова базова автентифікація.

Ододайте конфігурацію автентифікації в директиву проксі-сервера:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

ОСтворіть файл пароля за допомогою `/etc/httpd/.htpasswd -c`.

ОВручну створіть файл `group.file` із `usergroup:username`

9. Перезавантажте проксі-сервер Apache HTTP.

Інсталяція проксі-сервера Apache HTTP на сервер Ubuntu та інших дистрибутивах Linux на базі Debian

1. Інсталюйте останню версію проксі-сервера Apache HTTP з репозиторія APT:

```
sudo apt-get install apache2
```

2. Щоб завантажити необхідні модулі Apache, виконайте цю команду:

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core\
authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Відредагуйте файл конфігурації кешування Apache:

```
sudo vim /etc/apache2/conf-available/cache_disk.conf
```

і скопіюйте та вставте таку конфігурацію:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 2000000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Цей крок не є обов'язковим, але якщо каталог кешування відсутній, виконайте такі команди:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Відредагуйте файл конфігурації проксі-сервера Apache:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

і вставте таку конфігурацію:

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Увімкніть файли конфігурації, які було відредаговано на попередніх етапах:

```
sudo a2enconf cache_disk.conf proxy.conf
```

7. Установіть порт 3128 як порт прослуховування проксі-сервера Apache HTTP. Відредагуйте файл `/etc/apache2/ports.conf` і замініть `Listen 80` на `Listen 3128`.

8. Необов'язкова базова автентифікація.

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

ОСкопіюйте та вставте конфігурацію автентифікації перед `</Proxy>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

ОІнсталюйте `apache2-utils` і створіть новий файл пароля (наприклад, ім'я користувача `user`, група `usergroup`):

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
```

ОСтворіть файл `group`:

```
sudo vim /etc/apache2/group.file
```

і скопіюйте та вставте в нього такий рядок:

```
usergroup:user
```

9. Перезавантажте проксі-сервер Apache HTTP за допомогою цієї команди:

```
sudo service apache2 restart
```

Перенаправлення лише для підключення ESET

Щоб дозволити перенаправлення лише для підключення ESET, видаліть такі параметри:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

і додайте наступне:

```
<Proxy *>
Deny from all
</Proxy>

##.eset.com:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]*)?([a-zA-Z0-9-]{0,63}\.)*[a-zA-Z0-9-]{0,63}\.([e,E][s,S][e,E][t,T]\.([c,C][o,O][m,M])?(:[0-9]+)?(/.)*)?$>
Allow from all
</ProxyMatch>

##.eset.eu:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]*)?([a-zA-Z0-9-]{0,63}\.)*[a-zA-Z0-9-]{0,63}\.([e,E][s,S][e,E][t,T]\.([e,E][u,U])?(:[0-9]+)?(/.)*)?$>
Allow from all
</ProxyMatch>

#Antispam module (ESET Mail Security only):
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]*)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.)*?$>
Allow from all
</ProxyMatch>

#Services (activation)
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]*)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.)*?$>
Allow from all
</ProxyMatch>

#ESET servers accessed directly via IP address:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]*)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)(:[0-9]+)(:[0-9]+)?(/.)*?$>
Allow from all
</ProxyMatch>
```

Перенаправлення для всіх підключень

Щоб дозволити перенаправлення для всіх підключень, додайте такі параметри:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

і видаліть наступні:

```

<Proxy *>
Deny from all
</Proxy>

#*.eset.com:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]?)?([a-zA-Z0-9-]{0,63}\.){0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.)*?>
Allow from all
</ProxyMatch>

#*.eset.eu:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]?)?([a-zA-Z0-9-]{0,63}\.){0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.)*?>
Allow from all
</ProxyMatch>

#Antispam module (ESET Mail Security only):
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]?)?([ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net])(:[0-9]+)?(/.)*?>
Allow from all
</ProxyMatch>

#Services (activation)
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]?)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.)*?>
Allow from all
</ProxyMatch>

#ESET servers accessed directly via IP address:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\/*]?)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)(:[0-9]+)?(/.)*?>
Allow from all
</ProxyMatch>

```

Ланцюжок проксі-серверів (увесь трафік)

ESET PROTECT не може використовувати такі ланцюжки, якщо проксі-сервери вимагають автентифікації. Ви можете використовувати власний прозорий проксі-сервер, однак він може потребувати додаткового налаштування. Додайте в конфігурацію проксі-сервера такий текст (пароль працює лише на дочірньому проксі-сервері):

```
ProxyRemote * http://IP_ADDRESS:3128
```

Якщо ланцюжок проксі-серверів використовується на віртуальному пристрої ESET PROTECT, політику SELinux потрібно змінити. Відкрите термінал на віртуальному пристрої ESET PROTECT і запустіть вказану нижче команду:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

Конфігурація проксі-сервера HTTP для великої кількості клієнтів

Якщо ви використовуєте 64-розрядний проксі-сервер Apache HTTP, то можете збільшити ліміт потоків для Apache HTTP Proxy. Змініть файл конфігурації `httpd.conf` у папці Apache HTTP Proxy. Знайдіть у файлі вказані нижче параметри та змініть їхнє значення на кількість клієнтів.

Замініть значення 5000, наведене як приклад, на своє число. Максимальне значення дорівнює 32000.

```
ThreadLimit 5000
```

```
ThreadsPerChild 5000
```

Не змінюйте інший текст файлу.

Інсталяція проксі-сервера Squid HTTP на сервері Ubuntu

У сервері Ubuntu замість проксі-сервера Apache можна використовувати Squid. Щоб інсталювати й налаштувати Squid на сервері Ubuntu (і схожих дистрибутивах Linux на базі Debian), виконайте вказані нижче дії.

1. Інсталюйте пакет Squid3:

```
sudo apt-get install squid3
```

2. Внесіть зміни у файл конфігурації `/etc/squid3/squid.conf` і замініть

```
#cache_dir ufs /var/spool/squid3 100 16 256
```

на таке:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=200000000
```



Примітка

- У каталозі кешу можна змінити загальний розмір кешу (наприклад, 3000 МБ) і кількість підкаталогів першого рівня (наприклад, 16) та другого рівня (наприклад, 256).
- Параметр `max-size` визначає максимальний розмір кешованого файлу в байтах.

3. Зупиніть роботу служби `squid3`.

```
sudo service squid3 stop  
sudo squid3 -z
```

4. Знову внесіть зміни у файл конфігурації `Squid` і додайте `http_access allow all` перед `http_access deny all`, щоб усі клієнти отримали доступ до проксі-сервера.

5. Перезавантажте службу `squid3`:

```
sudo service squid3 restart
```

Інструмент «Дзеркало» - Linux

[Користуєтесь Windows?](#)

Для автономного оновлення ядра виявлення необхідний інструмент «Дзеркало». Якщо на клієнтських комп'ютерах відсутнє підключення до Інтернету, але потрібно оновити ядро виявлення, за допомогою інструмента «Дзеркало» можна завантажити файли оновлення із серверів оновлення ESET і зберегти їх локально.



Примітка

Інструмент «Дзеркало» завантажує лише оновлення ядра виявлення й інші модулі програми та не завантажує оновлення компонентів програми й дані ESET LiveGrid®. Він також може створити [автономний репозиторій](#). Крім цього, можна оновлювати кожен продукт окремо.

Необхідні компоненти

- Цільова папка має бути доступна для спільного використання, Samba/Windows або служби HTTP/FTP залежно від вибраного способу отримання доступу до оновлень.
- Необхідно мати дійсний файл [автономної ліцензії](#), що містить ім'я користувача та пароль. Під час створення файлу ліцензії поставте прапорець **Включити ім'я користувача та пароль**. Також можна вказати **назву** ліцензії. Файл автономної ліцензії потрібний для активації інструмента «Дзеркало» та створення дзеркала оновлення.

Create offline license file ✕

Product
ESET Endpoint Security for Windows

Name
Test license

Units count
1 /3

Username and password

Include Username and Password
When included it is possible to update from ESET servers

ESET PROTECT

Allow management with ESET PROTECT

GENERATE CANCEL

Як користуватись інструментом «Дзеркало»

1. Завантажте інструмент «Дзеркало» з [цієї сторінки ESET](#) (розділ **Автономні інстлятори**).
 2. Розархівуйте завантажений архів.
 3. Відкрийте термінал у папці, що містить файл *MirrorTool*.
 4. Щоб переглянути всі доступні параметри інструмента «Дзеркало», виконайте вказану нижче команду.
- ```
./MirrorTool --help
```

```


user@mint-linux1 ~/Desktop/MirrorTool_x86_64/x86_64 $./MirrorTool --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2020. All rights reserved.
Allowed options:
--mirrorType arg [required for module update]
 Type of mirror. Possible values (case
 insensitive): regular, pre-release,
 delayed.
--intermediateUpdateDirectory arg [required for module update]
 Files will be downloaded to this
 directory to create mirror in output
 directory.
--offlineLicenseFilename arg [required for module update]
 Offline license file.
--updateServer arg [optional]
 Update server. (e.g.:
 http://update.eset.com/eset_upd/ep6/)
 Mirror will be created in output
 directory, only specified path in
 server will be mirrored.
--outputDirectory arg [required for module update]
 Directory where mirror will be created.
--proxyHost arg [optional]
 Http proxy address (fqdn or IP).
--proxyPort arg [optional]
 Http proxy port.
--proxyUsername arg [optional]
 Http proxy username.
--proxyPassword arg [optional]
 Http proxy password.
--networkDriveUsername arg [optional]
 Username used, when output directory is
 accessed using smb(e.g:\\hostname).
--networkDrivePassword arg [optional]
 Password used, when output directory is
 accessed using smb(e.g:\\hostname).
--excludedProducts arg [optional]
 Disable creating mirror for specified
 products. Possible values: ep4 ep5 ep6
 ep7 era6.
--repositoryServer arg [required for repository update]
 Repository server for repository
 creation.
--intermediateRepositoryDirectory arg [required for repository update]
 Files will be downloaded to this
 directory to create offline mirror in
 output directory.
--outputRepositoryDirectory arg [required for repository update]
 Directory where offline repository will
 be created.
--languageFilterForRepository arg [optional]
 Download only packages with provided
 languages.
--productFilterForRepository arg [optional]
 Download only packages with provided
 product.
--downloadLegacyForRepository [optional]
 If set, download also legacy packages.
--trustDownloadedFilesInRepositoryTemp [optional]
 If set, hash on allready downloaded
 files are not checked.
--mirrorOnlyLevelUpdates [optional]
 If set, only level upgrades will be
 downloaded (nano/continuous updates
 will not be downloaded)
--mirrorFileFormat arg [optional]
 Specifies which type of update files
 will be downloaded. Possible values
 (case insensitive): dll, dat. Parameter
 is ignored when creating mirror for
 legacy products (ep4, ep5)
--help [optional]
 Display this help and exit

```

| Параметр | Опис |
|----------|------|
|----------|------|

|                               |                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --updateServer                | Під час використання потрібно вказати повну URL-адресу сервера оновлення.                                                                                                                                                                                                                                                                                                                         |
| --offlineLicenseFilename      | Необхідно вказати шлях до файлу автономної ліцензії (як згадувалося вище).                                                                                                                                                                                                                                                                                                                        |
| --languageFilterForRepository | Можна вказати коди мов, наприклад для французької мови введіть fr_FR. Коди інших мов наведено в таблиці нижче. Щоб вибрати кілька мов, розділіть їх пробілом, наприклад: en_US zh_TW de_DE                                                                                                                                                                                                        |
| --productFilterForRepository  | Можна вказати рядок, який інструмент «Дзеркало» використовує як фільтр завантаження. Інструмент «Дзеркало» завантажує лише файли, які містять цей рядок у своїх звичних іменах. Можна вибрати кілька продуктів, додавши інші аргументи, наприклад: --productFilterForRepository Antivirus Security<br>Інструмент «Дзеркало» завантажує всі мови для кожного вибраного продукту.                   |
| --downloadLegacyForRepository | Указувати аргументи непотрібно. Використовуйте цей параметр, щоб також завантажити застарілі пакети. Якщо його не використовувати, застарілі пакети не завантажуватимуться. Щоб дізнатися, які продукти є застарілими, перейдіть у меню <a href="#">Інсталяція програмного забезпечення &gt; Завдання клієнта &gt; Налаштування &gt; Пакет для інсталяції &gt; Вибрати пакет &gt; Застарілі</a> . |

#### Нові параметри в інструменті «Дзеркало» розповсюджені на ESMC 7.2 і ESET PROTECT

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --mirrorOnlyLevelUpdates | Указувати аргументи непотрібно. Якщо його задано, завантажуватимуться лише оновлення рівнів (нанооновлення не буде завантажено). Докладніше про типи оновлень можна дізнатися в нашій <a href="#">статті бази знань</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --mirrorFileFormat       | <div style="border: 1px solid red; padding: 10px; background-color: #f8d7da;">  <p><b>Попередження</b><br/>Цей параметр призначено лише для досвідчених користувачів. Перш ніж використовувати параметр --mirrorFileFormat, переконайтеся, що середовище не містить одночасно стару (6.5 і ранішні версії) та нову (6.6 і пізніші версії) версії продукту захисту ESET. Неправильне використання цього параметра може призвести до неправильних оновлень продуктів захисту ESET.</p> </div> <p>Ви можете вказати, які типи файлів оновлення завантажувати. Можливі значення (з урахуванням реєстру):</p> <ul style="list-style-type: none"> <li>• <b>dat</b> – використовуйте це значення, якщо середовище містить лише продукт захисту ESET 6.5 або старіших версій;</li> <li>• <b>dll</b> – використовуйте це значення, якщо середовище містить лише продукт захисту ESET 6.6 або новіших версій.</li> </ul> <p>Параметр ігнорується, коли дзеркало створюється для застарілих продуктів (er4, er5).</p> |



#### Примітка

Усі фільтри чутливі до реєстру.



#### Увага

Інструмент «Дзеркало» створює структуру папок, що відрізняється від тої, яку створює дзеркало робочої станції. Кожна папка містить файли оновлень для групи продуктів. Необхідно вказати повний шлях до правильної папки в параметрах оновлення продукту за допомогою дзеркала.  
Наприклад, щоб оновити ESET PROTECT8.0 із дзеркала, для параметра [Сервер оновлень](#) встановіть указане нижче значення (відповідно до основного розташування сервера HTTP):  
`http://your_server_address/mirror/eset_upd/era6`

Щоб створити дзеркало, запустіть інструмент «Дзеркало» з принаймні мінімальною кількістю необхідних параметрів. Нижче наведено приклад.

```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

Нижче наведено приклад розширеної конфігурації автономного репозиторію з вибраними продуктами, мовами та ввімкненим завантаженням застарілих файлів.

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--languageFilterForRepository sk_SK fr_FR de_DE \
--productFilterForRepository Antivirus Security \
--downloadLegacyForRepository
```

### Інструмент «Дзеркало» та параметри оновлення

- Щоб автоматично завантажувати оновлення модулів, створіть розклад запуску інструмента «Дзеркало». Для цього відкрийте веб-консоль і натисніть **Клієнтські завдання > Операційна система > Виконати команду. Виберіть Командний рядок для виконання** (зокрема, шлях до файлу `MirrorTool.exe`) і належний тригер (наприклад, CRON на кожен годину `0 0 * * * ? *`). Крім цього, можна скористатися планувальником завдань Windows або Cron у Linux.
- Щоб налаштувати оновлення на клієнтських комп'ютерах, створіть політику й налаштуйте **сервер оновлення** для вказування на адресу дзеркала або спільну папку.

### Відмовостійкий кластер - Linux

Нижче описано процедуру інсталяції та налаштування ESET PROTECT на кластері високої доступності Red Hat.

#### Підтримка кластерів Linux

Компоненти сервера ESET PROTECT можна інсталювати на кластері **Red Hat Linux 6** і вище. Відмовостійкий кластер працює лише в активному/пасивному режимі за допомогою диспетчера кластера `rgmanager`.

#### Необхідні компоненти

- Необхідно інсталювати та налаштувати активний/пасивний кластер. Одночасно може бути активним лише один вузол, інші вузли повинні бути в режимі очікування. Функція розподілення навантаження не підтримується.
- Підтримується спільне сховище, iSCSI SAN, NFS та інші рішення (усі технології й протоколи, що забезпечують доступ до спільного сховища за блоками або файлами та видають спільні пристрої за локально підключені до операційної системи). Необхідно забезпечити можливість доступу до спільного сховища з кожного активного вузла кластера, а також належним чином ініціалізувати спільну файлову систему (наприклад, використати файлову систему EXT3 або EXT4).
- Для керування системою потрібні такі додатки високої доступності:
  - `rgmanager`
  - `Conga`
- `rgmanager` – це традиційний стек кластерів високої доступності Red Hat. Це обов'язковий

компонент.

- Графічний інтерфейс **Conga** є необов'язковий. Ви можете керувати відмовостійким кластером без нього, проте ми радимо встановити цей інтерфейс для підвищення продуктивності. У цьому посібнику припускається, що графічний інтерфейс було встановлено.
- Для запобігання пошкодження даних необхідно налаштувати **ізоляцію окремих вузлів кластера**. Це повинен зробити адміністратор кластера.

Якщо кластер ще не запущено, скористайтеся наступним посібником, щоб налаштувати відмовостійкий кластер високої доступності (активний/пасивний) на Red Hat: [Адміністрування кластерів на Red Hat Enterprise Linux 6](#).

## Область

Компоненти ESET PROTECT, які можна встановити на кластері високої доступності **Red Hat Linux**:

- Сервер ESET PROTECT з агентом ESET Management



### Примітка

- Без інсталюваного агента ESET Management служба кластеру ESET PROTECT не запуститься.
- Інсталювати базу даних ESET PROTECT на кластері можна лише якщо кластер використовує службу SQL, а ESET PROTECT підключається до однієї адреси хоста бази даних.

Нижче наведено приклад інсталяції на кластер із 2 вузлами. А втім, ви можете інсталювати ESET PROTECT на багатовузловий кластер, використовуючи цей приклад як довідку. Вузли кластера в цьому прикладі мають назви **node1** і **node2**.

## Етапи інсталяції

1. Інсталюйте [сервер ESET PROTECT](#) на вузол node1.  
Озверніть увагу, що ім'я хоста в сертифікаті сервера повинно містити зовнішню IP-адресу (або ім'я хоста) інтерфейсу кластера (а не локальну IP-адресу та не ім'я хоста вузла).

2. Зупиніть і вимкніть службу сервера ESET PROTECT на Linux за допомогою наступних команд:

```
service eraserver stop
chkconfig eraserver off
```

3. Підключіть спільне сховище до вузла node1. У цьому прикладі спільне сховище підключається за шляхом `/usr/share/erag2cluster`.

4. У папці **/usr/share/erag2cluster** створіть наступні папки:

```
/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server
```

5. Рекурсивно перемістіть ці папки за вказаними нижче шляхами (джерело > пункт призначення):

| Перемістити папку:                                    | Перемістити до групи:                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------|
| <code>/etc/opt/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator</code> |
| <code>/opt/eset/RemoteAdministrator/Server</code>     | <code>/usr/share/erag2cluster/opt/eset/RemoteAdministrator</code>     |
| <code>/var/log/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/var/log/eset/RemoteAdministrator</code> |
| <code>/var/opt/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator</code> |

6. Створіть символічні посилання (вони можуть знадобитися для створення нових папок вручну):

```
ln -s /usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server
/etc/opt/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server
/opt/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server
/var/log/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server
/var/opt/eset/RemoteAdministrator/Server
```

7. Скопіюйте скрипт `eracluster_server` з папки налаштувань сервера ESET PROTECT до `/usr/share/cluster`. Скрипти не використовують розширення `.sh` у папці налаштувань.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/
eracluster_server.sh
```

8. Відключіть спільне сховище від `node1`.

9. Підключіть спільне сховище до тієї самої папки на вузлі `node2`, що й на `node1` (`/usr/share/erag2cluster`).

10. Створіть на вузлі `node2` наступні символічні посилання:

```
ln -s /usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server
/etc/opt/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server
/opt/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server
/var/log/eset/RemoteAdministrator/Server ln -s
/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server
/var/opt/eset/RemoteAdministrator/Server
```

11. Скопіюйте скрипт `eracluster_server` з папки налаштувань сервера ESET PROTECT до `/usr/share/cluster`. Скрипти не використовують розширення `.sh` у папці налаштувань.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/
eracluster_server.sh
```

Наступні кроки виконуються в графічному інтерфейсі адміністрування кластера Conga:

12. Створіть **Групу служб**, наприклад `ESMCSservice`.

Для служби кластерів ESET PROTECT необхідно надати три ресурси: IP-адресу, файлову систему та скрипт.

13. Створіть необхідні ресурси.

Додайте IP-адресу (зовнішню адресу кластера, до якої підключатимуться агенти), файлову систему та скрипт.

Файлова системи повинна вказувати на спільне сховище.

Необхідна точка підключення файлової системи: `/usr/share/erag2cluster`.

Установіть для параметра скрипта «Повний шлях до файлу скрипта» значення `/usr/share/cluster/eracluster_server`.

14. Додайте вищевказані ресурси до групи `ESMCSservice`.

Після успішного налаштування кластера серверів [інстальуйте агента ESET Management](#) на обох вузлах

локального диска (а не на спільному диску кластера). Укажіть зовнішню IP-адресу або ім'я хоста інтерфейсу кластера (не localhost!) за допомогою команди --hostname=.

## Покрокова інсталяція сервера ESET PROTECT в Linux

У цьому сценарії описано покрокову інсталяцію сервера ESET PROTECT та веб-консолі ESET PROTECT. Інсталяцію буде виконано за допомогою MySQL.

### Перед інсталяцією

1. Переконайтеся, що у вашій мережі є [сервер бази даних](#), а ви можете отримати доступ до нього з локального/віддаленого сервера. Якщо сервер бази даних не інстальовано, інстальуйте й налаштуйте новий сервер.
2. Завантажте автономні компоненти ESET PROTECT для Linux (Agent, Server, Web Console). Ці файли інсталяції розміщено в категорії [Відокремлені інсталятори ESET PROTECT](#) на веб-сайті ESET.

### Процес інсталяції



#### Примітка

- У вас має бути можливість виконувати команду sudo або інстальувати файли від імені користувача root.
- Щоб інстальувати сервер ESET PROTECT на SUSE Linux Enterprise Server (SLES), дотримуйтесь інструкцій зі [Статті бази знань](#)

1. Інстальуйте [необхідні пакети](#) для сервера ESET PROTECT.
2. Налаштуйте зв'язок із сервером MySQL згідно з розділом [Конфігурація MySQL](#).
3. Перевірте конфігурацію драйвера MySQL ODBC. Більш докладну інформацію див. в темі [Інсталяція та конфігурація ODBC](#).
4. Налаштуйте параметри та запустіть інсталяцію сервера ESET PROTECT. Для отримання додаткової інформації див. [Інсталяція сервера – Linux](#).
5. Інстальуйте потрібні пакети Java й Tomcat, потім інстальуйте ESET PROTECT Web Console, як описано в темі [Інсталяція ESET PROTECT Web Console](#). Якщо у вас виникли проблеми з підключенням HTTPS до ESET PROTECT Web Console, див. додаткову інформацію в розділі [Налаштування підключення HTTPS/SSL](#).
6. [Інстальуйте агент ESET Management](#) на комп'ютер із сервером.

## Інсталяція компонентів у macOS

У багатьох сценаріях інсталяції передбачено встановлення різних компонентів ESET PROTECT на різних комп'ютерах, щоб пристосувати різні мережеві архітектури, дотриматися вимог щодо ефективності тощо.



#### Примітка

macOS підтримується лише як клієнт. [Агент ESET Management](#) і [продукти ESET для macOS](#) можна інстальувати в macOS, однак не можна інстальувати сервер ESET PROTECT.

## Інсталяція агента - macOS

Нижче описано локальну інсталяцію агента.

1. Переконайтеся, що всі **попередні вимоги** виконано:
  - На комп'ютері із сервером інстальовано **сервер ESET PROTECT** і **веб-консоль ESET PROTECT**.
  - Створено [сертифікат агента](#), збережений на локальному диску.
  - На локальному диску підготовлено [центр сертифікації](#) (лише для непідписаних сертифікатів).



### Примітка

У разі виникнення проблем під час віддаленого розгортання агента ESET Management (не вдається завершити завдання сервера з **розгортання агента**) див. розділ довідки [Усунення неполадок під час розгортання агента](#).

2. Завантажте інсталятор (відокремлений інсталятор агента *.dmg*) на сайті [ESET](#) або отримайте його від адміністратора системи.

3. Двічі натисніть файл Agent-MacOSX-x86\_64.dmg і файл *.pkg*, щоб розпочати інсталяцію.

4. Виконайте необхідні для інсталяції дії. Коли відкриється відповідний запит, введіть дані для **підключення до сервера**:

- **Ім'я хоста сервера**: ім'я хоста або IP-адреса сервера ESET PROTECT.
- **Порт сервера**: порт для обміну даними між агентом і сервером, за замовчуванням: 2222.
- **Проксі-сервер**: виберіть, щоб використовувати проксі-сервер HTTP для обміну даними між агентом і сервером.



### Примітка

Цей параметр проксі-сервера використовується лише для реплікації між агентом ESET Management і сервером ESET PROTECT, а не для кешування оновлень.

- **Ім'я хоста проксі-сервера**: ім'я хоста або IP-адреса комп'ютера, де розміщено проксі-сервер HTTP.
- **Порт проксі-сервера**: за замовчуванням це 3128.
- **Ім'я користувача, пароль**: введіть облікові дані проксі-сервера (якщо використовується автентифікація).

Параметри проксі-сервера можна змінити пізніше в [політиці](#). [Проксі-сервер](#) має бути інстальовано до налаштування підключення «агент – сервер» через проксі-сервер.

5. Виберіть [сертифікат](#) однорангового вузла та пароль для нього. Ви також можете додати [центр сертифікації](#).



### Попередження

Парольна фраза сертифіката не може містити такі символи: " \ Ці символи спричиняють критичну помилку під час ініціалізації агента.

6. Перегляньте місце встановлення та натисніть **Інстальювати**. Агента буде інстальовано на ваш комп'ютер.

7. Файл журналу агента ESET Management має бути розташовано за цим шляхом:

```
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log
```



### Увага

Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT, для якого потрібна автентифікація, не працюватиме.

Якщо ви не виберете порт для веб-консолі або агента за замовчуванням, можливо, потрібно буде налаштувати брандмауер відповідним чином. В іншому разі інсталяція може закінчитися невдало.

## Образ ISO

Файл образу ISO – це один із форматів, у якому можна [завантажити](#) (у категорії універсальних інсталяторів) інсталятори ESET PROTECT. Образ ISO містить такі компоненти:

- пакет інсталятора ESET PROTECT;



- окремі інсталятори для кожного компонента.

Образ ISO корисний, коли потрібно зібрати всі інсталятори ESET PROTECT в єдиному місці. Також він усуває потребу завантажувати інсталятори з веб-сайту ESET перед кожною інсталяцією. Крім цього, образ ISO знадобиться, коли потрібно інсталювати ESET PROTECT на віртуальній машині.

### Запис служби DNS

#### Щоб налаштувати Запис ресурсів DNS:

1. На своєму DNS-сервері (контролера домену) перейдіть до пункту **Панель управління > Адміністративні інструменти**.
2. Виберіть значення DNS.
3. У диспетчері DNS виберіть пункт `_tcp` із дерева та створіть новий запис **Розташування служби (SRV)**.
4. Введіть ім'я служби в поле **Служба** згідно зі стандартними правилами DNS і додайте перед ним символ підкреслення `_` (використовуйте власне ім'я служби, наприклад `_era`).
5. Введіть протокол TCP в поле **Протокол** у такому форматі: `_tcp`.
6. Введіть порт 2222 в поле **Номер порту**.
7. Введіть повне доменне ім'я сервера ESET PROTECT у полі **Хост, на якому працює ця служба**.
8. Виберіть **ОК > Готово**, щоб зберегти запис. Запис відобразиться в списку.

#### Щоб перевірити запис DNS, виконайте наведені нижче дії.

1. Увійдіть у систему будь-якого комп'ютера у своєму домені та відкрийте командний рядок (cmd.exe).
2. Введіть команду `nslookup` в командний рядок і натисніть **Enter**.
3. Введіть `set querytype=svr` і натисніть **Enter**.
4. Введіть `_era._tcp.domain.name` і натисніть **Enter**. Відобразиться розташування служби.



#### Примітка

У разі інсталяції сервера ESET PROTECT на новий комп'ютер обов'язково змініть значення параметра «Хост, на якому працює ця служба» на FQDN вашого нового сервера.

### Сценарій інсталяції ESET PROTECT в автономному режимі

Іноді потрібно інсталювати програму ESET PROTECT та її компоненти в середовищах без доступу до Інтернету. Для цього виконайте наведені нижче вказівки з інсталяції.



#### Увага

Вказівки з оновлення ESET PROTECT доступні в розділі [Оновлення компонентів ESET PROTECT в автономному середовищі](#).

Інсталяція з використанням GPO/SCCM: перегляньте [статтю бази знань](#)

### Інсталяція з локального репозиторію

1. [Інсталювати ESET PROTECT](#). Під час інсталяції виберіть **Активувати пізніше** й [активуйте ESET PROTECT](#) потім за допомогою [автономної ліцензії](#).
2. Створіть локальний репозиторій для пакетів інсталяції. Це можна зробити трьома способами (див. нижче).
  - а) Створіть локальний репозиторій за допомогою компонента Apache Tomcat, уже інсталюваного разом із ESET PROTECT.
    - I. Перейдіть у папку `C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps\`
    - II. Створіть папку для локального репозиторію, наприклад `protect_repository`.
    - III. Скопіюйте пакети інсталяції в репозиторій.
    - IV. Пакети інсталяції будуть доступні за цією адресою:  
`https://tomcat_server:tomcat_port/protect_repository/Agent_MacOSX-x86_64.dmg`

б) Створіть локальний репозиторій за допомогою проксі-сервера Apache HTTP.

I. [Інсталюйте проксі-сервер Apache HTTP](#).

II. Перейдіть у папку *C:\Program Files\Apache HTTP Proxy\htdocs\* (розташування можна змінити у файлі конфігурації).

III. Скопіюйте пакети інсталяції в цю папку.

IV. Пакети інсталяції будуть доступні за цією адресою:

[http://proxy\\_server:proxy\\_port/Agent\\_MacOSX-x86\\_64.dmg](http://proxy_server:proxy_port/Agent_MacOSX-x86_64.dmg)

с) Скористайтеся спільною мережевою папкою або диском.

3. Інсталюйте агент ESET Management за допомогою [інтерактивної інсталяції агента](#). Для цього скористайтеся URL-адресою пакета інсталяції агента з локального репозиторію в сценарії інсталяції. Щоб дізнатися більше, перегляньте [статтю бази знань](#).

4. Розгорніть продукти ESET Endpoint на робочих станціях за допомогою [завдання інсталяції програмного забезпечення](#). Виберіть спеціальну URL-адресу пакета інсталяції в локальному репозиторії. Щоб завантажити пакети інсталяції, перейдіть на [сторінку завантажень](#) ESET.com.

5. Активуйте робочі станції за допомогою автономної ліцензії.

- [Як активувати продукти ESET для бізнесу в автономному режимі?](#)
- [Як активувати продукти ESET для бізнесу в ESET PROTECT?](#)

6. [Вимкнути ESET LiveGrid®](#).

7. Дзеркало оновлення – існує два сценарії (а, б).



#### Увага

Apache HTTP Proxy працює як дзеркало, але компонент Apache Tomcat потрібно налаштувати так, щоб він працював без протоколу SSL, оскільки підключення до веб-консолі ESET PROTECT не буде захищено через дзеркало оновлення.

а) У закритій мережі без доступу до Інтернету адміністратор має створити налаштовуваний сервер оновлення (папку «дзеркала», у якій зберігаються файли оновлень для клієнтів).

I. Якщо Apache HTTP Proxy/Apache Tomcat використовується як сервер оновлення, [у клієнтах потрібно налаштувати використання налаштовуваного сервера оновлення](#) (не проксі-сервера).

II. Якщо рішення Endpoint Security для Windows використовується як сервер дзеркала, у клієнтах потрібно [налаштувати завантаження з дзеркала клієнта](#).

б) Якщо хоча б один комп'ютер має доступ до Інтернету:

I. Ви можете за допомогою Apache HTTP Proxy [налаштувати в клієнті використання проксі-сервера](#).

II. Ви можете використовувати Tomcat як сервер оновлення й інструмент «Дзеркало» та налаштувати в клієнті [використання налаштовуваного сервера оновлення](#).

III. Ви можете налаштувати дзеркало за допомогою Endpoint Security для Windows і сконфігурувати в клієнтах [завантаження з дзеркала клієнта](#).

8. Рекомендуємо регулярно оновлювати модулі. Якщо вони не будуть оновлені, комп'ютери буде позначено у веб-консолі міткою **Не оновлено**. Це попередження можна вимкнути у веб-консолі ESET PROTECT, натиснувши комп'ютер у списку та вибравши опцію **Вимкнути сповіщення** в розкритому меню.

## Процедури оновлення, міграції та повторної інсталяції

Існує кілька способів оновити, перенести чи повторно інсталювати сервер ESET PROTECT та інші компоненти ESET PROTECT.



### Попередження

- Переконайтеся, що маєте [підтримувану операційну систему](#) перед оновленням до ESET PROTECT 8.0.
- Компонент сервера ESET PROTECT версії 8.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 6.5–7.0 до 8.0.
- Якщо ви вже запустили оновлення й система не працює, потрібно вручну повторно інсталювати всі компоненти ESET PROTECT в оригінальній версії.
- Щоб оновити їх, потрібно перенести поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустити завдання оновлення.
- ESET PROTECT 8.0 використовує [LDAPS як протокол за замовчуванням для синхронізації Active Directory](#). Якщо використовується синхронізація Active Directory, оновлення версій 6.5–7.1 на машині Windows до ESET PROTECT 8.0 призведе до помилки завдання синхронізації в ESET PROTECT 8.0.

## 1. Оновлення з покоління ERA 5

Пряме оновлення не підтримується: див. тему [Перенесення з ERA 5.x](#).

## 2. Оновлення з ERA 6.5 до ESMC 7.x або до ESET PROTECT версії 8.0

Виконайте оновлення до останньої версії:

- за допомогою завдання [Оновити компоненти](#);
- за допомогою [ESET PROTECT 8.Рекомендуємо використовувати універсальний інстальатор 0](#), якщо наявну інсталяцію ERA/ESMC виконано за допомогою універсального інстальатора;
- [вручну](#) (для досвідчених користувачів).

Якщо в інфраструктурі використовується компонент проксі-сервера ERA, перед оновленням перегляньте [документацію](#) з перенесення проксі-сервера.



### Примітка

Щоб дізнатися версію кожного використовуваного компонента ESET PROTECT, перевірте, яку версію сервера ESET PROTECT у вас інстальовано. Перейдіть на сторінку [Про програму](#) у веб-консолі ESET PROTECT та перегляньте в [цій статті база знань](#) список усіх версій компонентів ESET PROTECT для версії сервера ESET PROTECT.

## 3. Перенесіть ESET PROTECT 8 з одного сервера на інший або заново інсталюйте його

[Перенесіть дані з одного сервера на інший](#) або [повторно інсталюйте сервер ESET PROTECT](#).



### Увага

Якщо ви плануєте перенести дані з одного сервера ESET PROTECT на новий сервер, експортуйте всі Центри сертифікації та сертифікат сервера ESET PROTECT або створіть їхні резервні копії. В іншому разі компоненти ESET PROTECT не зможуть обмінюватися даними з новим сервером ESET PROTECT.

## 4. Інші процедури

[Змінення IP-адреси чи імені хосту](#) на сервері ESET PROTECT.



### Увага

[Після оновлення з ERA 6.5](#) до ESET PROTECT версії 8.0 будуть помітні істотні зміни.

Завдання з оновлення компонентів ESET PROTECT

## Рекомендації перед оновленням

Для оновлення інфраструктури ESET PROTECT рекомендується використовувати завдання з [ESET PROTECT оновлення компонентів](#) у веб-консолі ESET PROTECT. Перед оновленням уважно ознайомтеся з наведеними тут інструкціями.



### Примітка

- ESET PROTECT 8 відображає автоматичне сповіщення [за наявності більш нової версії сервера ESET PROTECT](#).
- Додаткові інструкції з оновлення ESET PROTECT до останньої версії можна переглянути в нашій [статті бази знань](#).

[Виконуєте оновлення з віртуального пристрою ERA/ESMC?](#)

[Оновлюєте середовище за допомогою проксі-сервера ERA?](#)

[-] [Екземпляр сервера ESET PROTECT встановлено на відмовостійкому кластері?](#)

Якщо екземпляр сервера ESET PROTECT встановлено на відмовостійкому кластері, необхідно оновити сервер ESET PROTECT на кожному вузлі кластера вручну. Після оновлення сервера ESET PROTECT запустіть завдання з [оновлення компонентів](#), щоб оновити решту вашої інфраструктури (наприклад, агент ESET Management на клієнтських комп'ютерах).

[-] [Важливі вказівки перед оновленням проксі-сервера Apache HTTP на Microsoft Windows](#)

Якщо ви використовуєте проксі-сервер Apache HTTP й задали налаштовувані параметри у файлі `httpd.conf` (наприклад, ім'я користувача та пароль), створіть резервну копію оригінального файлу `httpd.conf` (розташованого в папці `C:\Program Files\Apache HTTP Proxy\conf`). Якщо ви не задавали налаштовувані параметри, створювати резервну копію файлу `httpd.conf` не потрібно. Оновіть проксі-сервер Apache HTTP до останньої версії у будь-який спосіб, описаний у [цій статті](#).



### Попередження

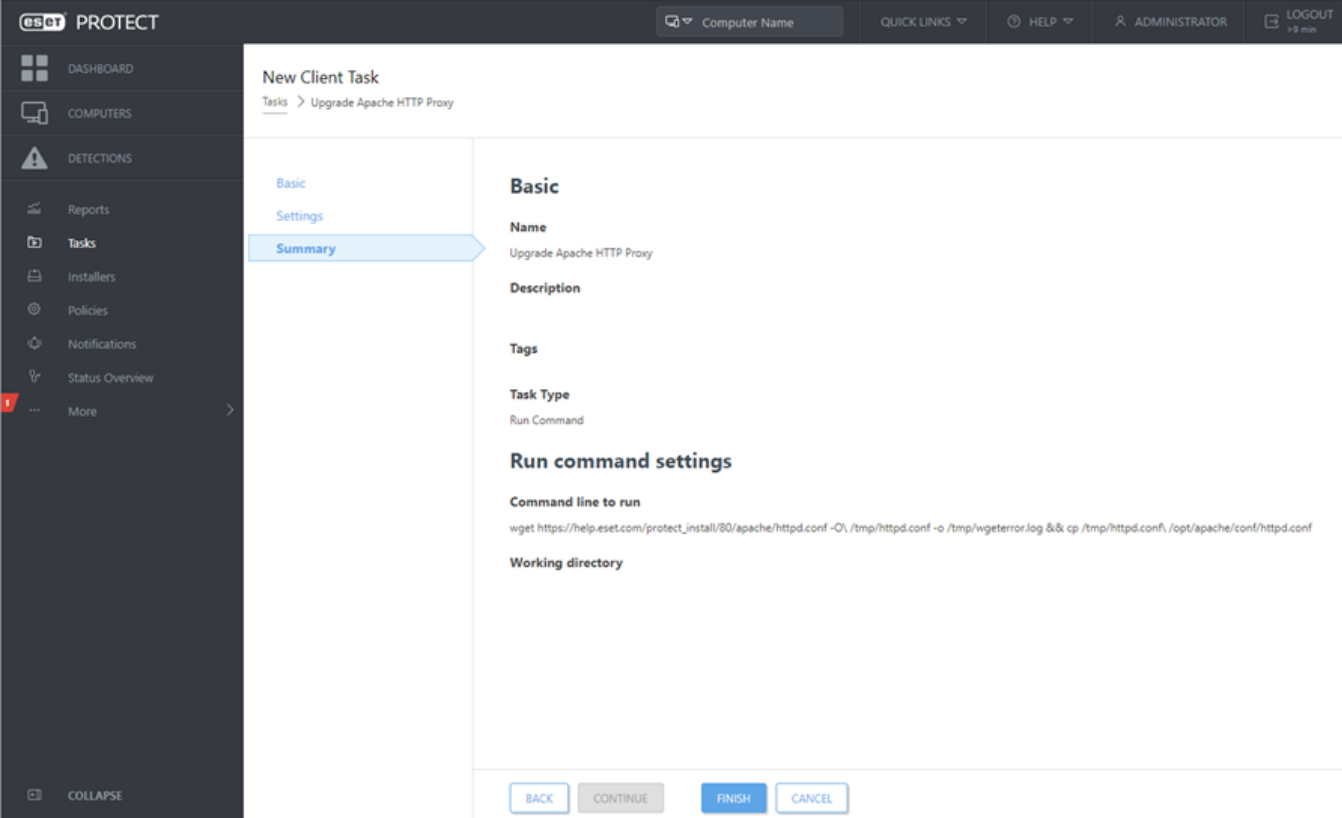
Коли ви оновите Apache HTTP Proxy у Windows і задасте налаштовувані параметри в оригінальному файлі `httpd.conf` (наприклад, ім'я користувача та пароль), скопіюйте параметри з резервної копії файлу `httpd.conf` і застосуйте налаштовувані параметри лише в новому файлі `httpd.conf`. Не використовуйте оригінальний файл `httpd.conf` з оновленою версією проксі-сервера Apache HTTP Proxy, оскільки він працюватиме неналежним чином. Скопіюйте з нього лише налаштовувані параметри та використовуйте новий файл `httpd.conf`. Також ви можете налаштувати новий файл `httpd.conf` вручну (див. статтю [Інсталяція проксі-сервера Apache HTTP - Windows](#)).

[-] [Важливі вказівки перед оновленням проксі-сервера Apache HTTP на віртуальному пристрої](#)

Якщо ви використовуєте **проксі-сервер Apache HTTP** та задали власні параметри у файлі `httpd.conf` (наприклад, ім'я користувача й пароль), створіть резервну копію оригінального файлу `httpd.conf` (розташованого в папці `/opt/apache/conf/`), а потім запустіть завдання з **Оновлення компонентів ESET PROTECT**, щоб оновити **проксі-сервер Apache HTTP**. Якщо ви не використовуєте власні параметри, створювати резервну копію `httpd.conf` не потрібно.

Після завершення завдання з оновлення компонентів запустіть наступну команду. Призначте її до комп'ютера, на якому інстальовано проксі-сервер Apache HTTP. Використайте завдання клієнта [Виконати команду](#), щоб оновити файл `httpd.conf` (це потрібно для забезпечення нормальної роботи оновленої версії проксі-сервера Apache HTTP):

```
wget https://help.eset.com/protect_install/80/apache/httpd.conf -O\
/tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
/opt/apache/conf/httpd.conf
```



The screenshot displays the ESET PROTECT web interface. The top navigation bar includes the ESET PROTECT logo, a search bar for 'Computer Name', and links for 'QUICK LINKS', 'HELP', 'ADMINISTRATOR', and 'LOGOUT'. The left sidebar contains a menu with options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies, Notifications, Status Overview, and More. The main content area is titled 'New Client Task' and shows the configuration for a task named 'Upgrade Apache HTTP Proxy'. The task type is 'Run Command'. The 'Run command settings' section shows the command line to run: `wget https://help.eset.com/protect_install/80/apache/httpd.conf -O\ /tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\ /opt/apache/conf/httpd.conf`. At the bottom of the configuration area, there are buttons for 'BACK', 'CONTINUE', 'FINISH', and 'CANCEL'.

Якщо проксі-сервер Apache HTTP інстальовано на комп'ютері з віртуальним пристроєм, ви можете запустити ту саму команду безпосередньо з консолі віртуального пристрою ESET PROTECT. Ви також можете замінити файл конфігурації проксі-сервера Apache HTTP [httpd.conf](#) вручну.



### Попередження

Якщо ви внесли власні параметри у файл `httpd.conf` (наприклад, ім'я користувача та пароль), скопіюйте параметри з резервної копії файлу `httpd.conf` і додайте до нового файлу `httpd.conf` лише власні налаштування. Не використовуйте оригінальний файл `httpd.conf` з оновленою версією проксі-сервера Apache HTTP, оскільки він працюватиме неправильно. Скопіюйте лише власні параметри та використайте новий файл `httpd.conf`. Також ви можете налаштувати новий файл `httpd.conf` вручну (див. статтю [Інсталяція проксі-сервера Apache HTTP - Linux](#)).



### Увага

Виконати оновлення до ESET PROTECT 8.0 можна тільки з ERA версії 6.5 і новіших.

Перед початком оновлення створіть резервну копію наступних даних:

- усіх сертифікатів (центр сертифікації, сертифікат сервера та сертифікат агента).
- Екпортуйте свої [сертифікати від Центру сертифікації](#) зі старого сервера ESET PROTECT у файл .der і збережіть його в зовнішньому сховищі.
- Екпортуйте свої [сертифікати однорангового вузла](#) (для агента ESET Management, сервера ESET PROTECT) і файл .pfx з приватним ключем із сервера ESET PROTECT та збережіть їх у зовнішньому сховищі.
- Ваша база даних [ERA/ESMC](#). Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MSSQL 2008), [оновіть базу даних](#) до [сумісної версії](#), перш ніж оновлювати сервер ESET PROTECT.

Переконайтеся, що маєте [підтримувану операційну систему](#) перед оновленням до ESET PROTECT 8.0.

Компонент сервера ESET PROTECT версії 8.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 6.5–7.0 до 8.0.

- Якщо ви вже запустили оновлення й система не працює, потрібно вручну повторно інстальювати всі компоненти ESET PROTECT в оригінальній версії.
- Щоб оновити їх, потрібно перенести поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустити завдання оновлення.

ESET PROTECT 8.0 використовує [LDAPs як протокол за замовчуванням для синхронізації Active Directory](#). Якщо використовується синхронізація Active Directory, оновлення версій 6.5–7.1 на машині Windows до ESET PROTECT 8.0 призведе до помилки завдання синхронізації в ESET PROTECT 8.0.

Щоб оновити продукти ESET для захисту, використайте [завдання](#) з [інсталяції програмного забезпечення](#). Запустіть завдання з пакетом інсталятора останньої версії, щоб встановити останню версію наявного продукту.

### Рекомендована процедура оновлення

1. Оновіть ESET PROTECT Server: для завдання **Оновити компоненти ESET PROTECT** укажіть цільовою тільки ту машину, яка має ESET PROTECT Server.



### Попередження

Якщо виконується оновлення з ERA 6.x, то перед оновленням агентів необхідно виконати оновлення до ESET PROTECT Server. В агентах ESET Management Agent використовується новий протокол зв'язку, тому вони не можуть підключитися до ERA Server 6.x.

2. Виберіть кілька клієнтських комп'ютерів (для тестового оновлення виберіть принаймні один клієнт із кожної системи/розрядності) й запустіть на них завдання **Оновити компоненти ESET PROTECT**.
  - Для обмеження навантаження на мережу рекомендується використовувати [Проксі-сервер Apache HTTP](#) (або інший прозорий проксі-сервер з увімкненим кешуванням). На тестових клієнтських комп'ютерах розпочнеться завантаження/кешування інсталяторів. Після наступного виконання завдання інсталятори буде перенесено на клієнтські комп'ютери безпосередньо з кешу.
3. Після підключення комп'ютерів із оновленим ESET Management Agent до ESET PROTECT Server продовжте оновлювати решту клієнтів.



### Примітка

Щоб оновити агенти ESET Management Agent на всіх керованих комп'ютерах у мережі, укажіть статичну групу **Всі** цільовою для завдання **Оновити компоненти ESET PROTECT**. Оновлені раніше комп'ютери не буде оновлено знову.

## Список компонентів, що оновлюються:

- Сервер ESET PROTECT
- Агент ESET Management
- Веб-консоль ESET PROTECT використовується лише якщо Apache Tomcat, зокрема ESET PROTECT Virtual Appliance, було інстальовано в ОС Windows або Linux у папку за замовчуванням (наприклад: /var/lib/tomcat8/webapps/, /var/lib/tomcat7/webapps/, /var/lib/tomcat/webapps/).



### Попередження

ОApache Tomcat не оновлюється під час оновлення веб-консолі ESET PROTECT за допомогою завдання з оновлення компонентів.

ООновлення веб-консолі ESET PROTECT не виконується, якщо Apache Tomcat встановлено в інше місце.

ОЯкщо інстальовано налаштовувану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інстальатора або завдання «Оновлення компонентів» не підтримується.

- ESET PROTECT Mobile Device Connector Перед оновленням середовища до версії 8.0 рекомендується оновити MDM до версії 6.5.

## Компоненти, які необхідно оновити вручну:

- Apache Tomcat (настійно рекомендується регулярно оновлювати Apache Tomcat, див. [Оновлення Apache Tomcat](#))
- [Сервер бази даних](#)
- Проксі-сервер Apache HTTP (його можна оновити за допомогою універсального інстальатора, див. [Оновлення Проксі-сервер Apache HTTP](#))
- [ESET Rogue Detection Sensor](#): для оновлення інстальуйте новішу версію поверх наявної (дотримуйтеся інструкцій з інсталяції для [Windows](#) або [Linux](#)). Якщо ви встановили RD Sensor з ESMC версії 7.x, виконувати оновлення не потрібно, оскільки це остання версія RD Sensor.

## Виправлення неполадок



### Попередження

Якщо на комп'ютері з веб-консоллю або сервером ESET PROTECT не вдалось оновити компоненти, під час віддаленого входу у веб-консоль можуть виникнути проблеми. Рекомендується забезпечити можливість фізичного доступу до сервера перед виконанням оновлення. Якщо фізичний доступ до сервера відсутній, переконайтеся, що ви можете ввійти на нього з віддаленого робочого столу за допомогою облікового запису адміністратора. Перед оновленням рекомендується [створити резервну копію](#) баз даних сервера ESET PROTECT та Mobile Device Connector. Щоб створити резервну копію віртуального пристрою, створіть його знімок або точну копію віртуальної машини.

- Перевірте, чи можете ви [отримати доступ до репозиторія ESET PROTECT](#) з оновленого комп'ютера.
- Повторно запустити завдання з оновлення компонентів ESET PROTECT неможливо, якщо принаймні один компонент вже було оновлено.
- Якщо чіткої причини проблем із запуском завдання немає, можна оновити компоненти вручну. Див. керівництво для [Windows](#) або [Linux](#).
- Щоб переглянути додаткові шляхи вирішення проблем із оновленням, див. [загальну інформацію щодо усунення несправностей](#).

Оновлення за допомогою ESET PROTECT8.0 Універсальний інстальатор

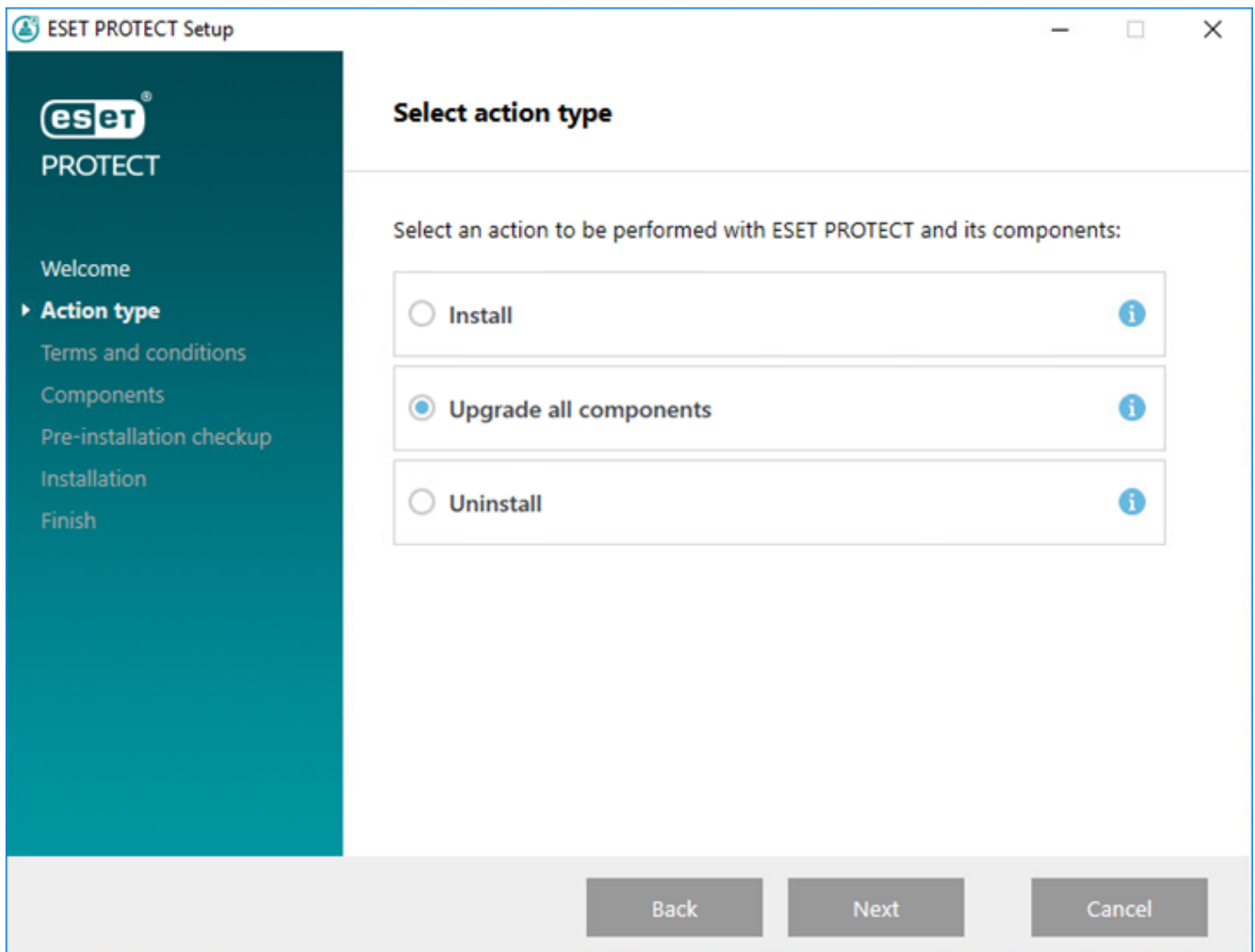
Оновіть ERA 6.5 або ESMC 7.x до останньої версії ESET PROTECT 8.0 за допомогою ESET PROTECT 8.0 Універсальний інстальатор.



### Увага

- Рекомендуємо використовувати цю опцію, якщо наявну інсталяцію виконано за допомогою універсального інстлятора.
- Виконати оновлення до ESET PROTECT 8.0 можна тільки з ERA версії 6.5 і новіших.
- Переконайтеся, що маєте [підтримувану операційну систему](#) перед оновленням до ESET PROTECT 8.0.
- Компонент сервера ESET PROTECT версії 8.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 6.5–7.0 до 8.0.
- Якщо ви вже запустили оновлення й система не працює, потрібно вручну повторно інсталювати всі компоненти ESET PROTECT в оригінальній версії.
- Щоб оновити їх, потрібно перенести поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустити завдання оновлення.
- Якщо у вас інсталювано старішу непідтримувану базу даних (MySQL 5.5 або MSSQL 2008), [оновіть базу даних](#) до [сумісної версії](#), перш ніж оновлювати сервер ESET PROTECT.
- ESET PROTECT 8.0 [Універсальний інстлятор](#) за замовчуванням інсталює Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інсталюватиметься за замовчуванням.
- ESET PROTECT 8.0 використовує [LDAPS як протокол за замовчуванням для синхронізації Active Directory](#). Якщо використовується синхронізація Active Directory, оновлення версій 6.5–7.1 на машині Windows до ESET PROTECT 8.0 призведе до помилки завдання синхронізації в ESET PROTECT 8.0.

1. Запустити Setup.exe.
2. Виберіть мову й натисніть **Далі**.
3. Виберіть **Оновити всі компоненти** й натисніть **Далі**.



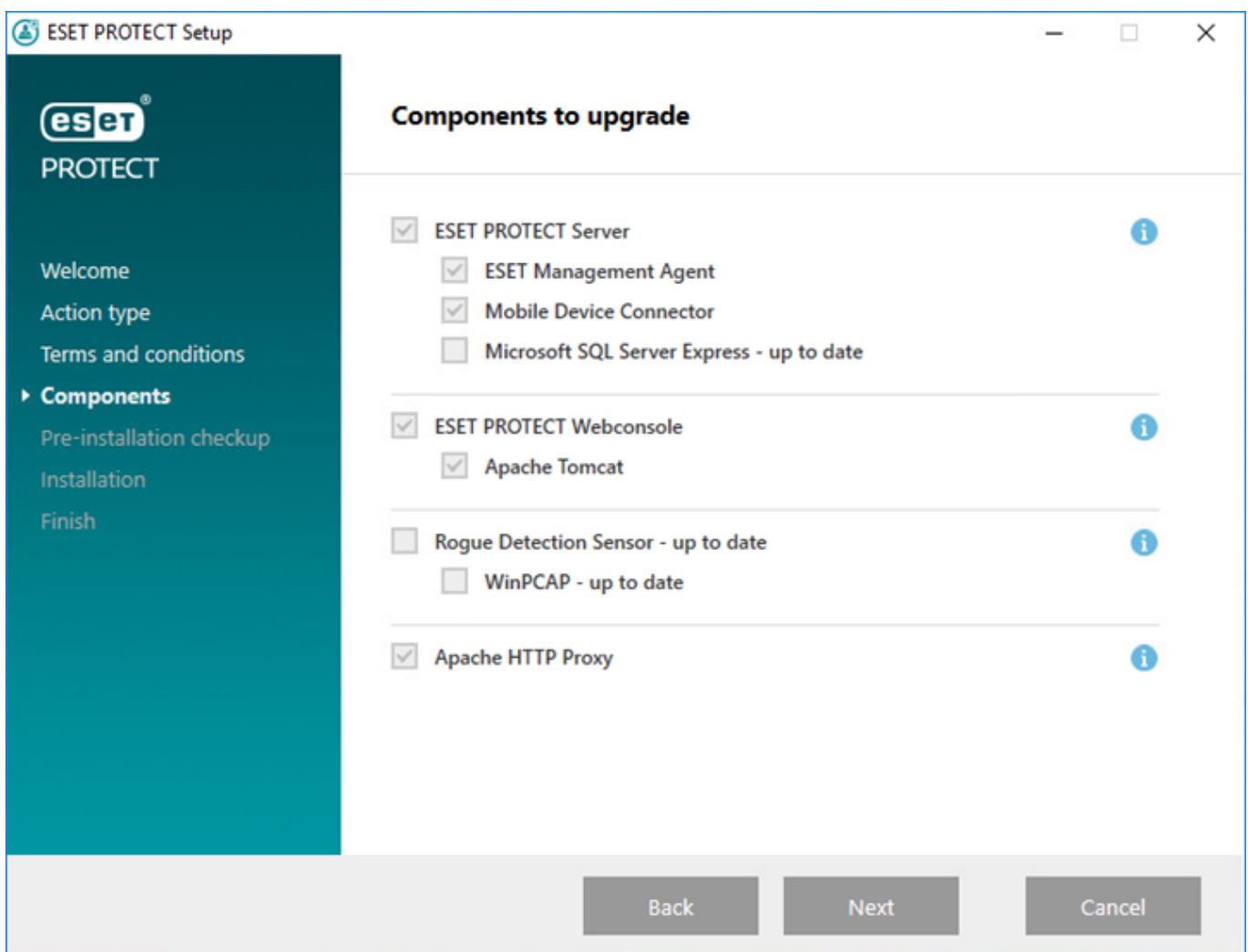


- Прочитайте **ліцензійну угоду з кінцевим користувачем**, прийміть її й натисніть **Далі**.
- Перегляньте, які компоненти ESET PROTECT можна оновити, і натисніть **Далі**.



### Попередження

- Якщо інстальовано налаштовану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інстальатора або завдання «Оновлення компонентів» не підтримується.
- Під час оновлення Apache Tomcat буде видалено папку *era*, розташовану в каталозі `C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps`. Якщо ви зберігаєте додаткові дані в папці *era*, перед оновленням створіть їх резервну копію.
- Якщо `C:\Program Files\Apache Software Foundation\[Tomcat папка]\каталог webapps` містить додаткові дані (крім даних у папках *era* і *ROOT*), оновиться лише веб-консоль, а Apache Tomcat – ні.
- Після оновлення Web Console і Apache Tomcat файли [автономної довідки](#) видаляються. Якщо ви використовували автономну довідку з ERA/ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 8.0. Це дозволить мати найновішу автономну довідку, що відповідає вашій версії ESET PROTECT.



- Щоб завершити оновлення ESET PROTECT, виконуйте вказівки майстра.

### Оновлення інфраструктури за допомогою проксі-сервера ERA 6.5

Компонент ERA Proxy не підтримується в ESMC 7 і новіших версій. Доступне рішення для заміни [проксі-сервера](#). Під час оновлення інфраструктури (сервера й агентів) потрібно перенести проксі-сервер.

Перед оновленням прочитайте вказану нижче інформацію.



## Попередження

- Зверніть увагу на сумісність підключення.  
o ERA Agent версії 6.x може підключатися до ESET PROTECT Server.  
o Агент ESET Management (починаючи з версії 7) не може підключатися до сервера ESET PROTECT через проксі-сервер ERA.  
o ESET Management Agent (версії 7 або новіших) не може підключатися до ERA.
- Протокол обміну даними між агентом і сервером ESET PROTECT не підтримує автентифікацію. Проксі-сервер, який використовується для перенаправлення даних агента на сервер ESET PROTECT і потребує автентифікації, не працюватиме.
- **Не оновлюйте агенти ERA (які підключаються через проксі-сервер), поки не налаштуєте належний проксі-сервер.**

## Сценарії оновлення

Якщо у вас працює середовище, яке використовує компонент проксі-сервера ERA, скористайтесь одним із вказаних нижче сценаріїв оновлення інфраструктури до ESET PROTECT 8.

- [Проксі-сервер ERA, інстальований у Windows](#) (ця сторінка)
- [Проксі-сервер ERA, інстальований у Windows](#) (стаття бази знань із детальнішими вказівками)
- [ERA Proxy, розгорнутий у Linux або як віртуальний пристрій](#) (стаття бази знань)

## Оновлення інфраструктури за допомогою ERA Проксі-сервер, інстальований у Windows

1. Створіть резервну копію сервера ERA.
2. Оновіть сервер ERA до версії ESET PROTECT 8 за допомогою завдання **Оновлення компонентів Remote Administrator**. (Оновлюються сервер, агент і веб-консоль)
3. Зачекайте приблизно 24 години та переконайтеся, що оновлене середовище працює без перешкод.
4. Оновіть ERA Agent на комп'ютері ERA за допомогою завдання **Оновити компоненти ESET PROTECT**.
5. Інстальуйте *Apache HTTP Proxy* на комп'ютері, на якому інстальовано проксі-сервер ERA. Використовуйте попередньо налаштовану версію ESET *Apache*. ([посилання для завантаження](#))
6. Змініть файл конфігурації *Apache HTTP Proxy* `httpd.conf`, розташований у каталозі `C:\Program Files\Apache HTTP Proxy\conf`.
  - a. За замовчуванням для обміну даними з агентом ESET Management використовується порт 2222. Якщо ви змінили порт під час інсталяції, вкажіть його номер. Змініть значення «2222» в рядку `AllowCONNECT 443 563 2222 8883` на номер вашого порту.
  - b. Додайте окремий сегмент `ProxyMatch`.
    - I. Адреса, яку агенти використовують для підключення до сервера ESET PROTECT.
    - II. Усі інші адреси сервера ESET PROTECT (IP-адреса, повне доменне ім'я).  
(Додайте весь указаний нижче код; IP-адреса 10.1.1.10 та ім'я хоста `hostname.example` є лише прикладами, їх потрібно замінити своїми адресами. Ви також можете створити вираз `ProxyMatch` в [цій статті бази знань](#).)

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>
Allow from all
</ProxyMatch>
```

- c. Перезавантаження служби *Apache HTTP Proxy*.
7. Створіть політику на сервері ESET PROTECT.
    - a. У веб-консолі ESET PROTECT натисніть **Політики > Створити нову**.
    - b. У розділі **Основне** введіть **назву** політики.
    - c. У розділі **Параметри** виберіть агент ESET Management.

- d. Перейдіть у меню **Підключення > Сервер підключається до > Змінити список серверів**.
- e. Натисніть **Додати** та введіть адресу комп'ютера проксі-сервера (комп'ютер, на якому встановлено проксі-сервер ERA) у полі **Хост**. Клацніть **ОК**.
- f. Повторіть крок вище та додайте адресу сервера ESET PROTECT (адреса має збігатися з тою, що використовувалася для конфігурації агента).
- g. Натисніть **Зберегти**.
- h. Перейдіть у меню **Додаткові параметри > Проксі-сервер HTTP** та виберіть для параметра **Конфігурація проксі-сервера** значення **Інший проксі-сервер для кожної служби**.
- i. Натисніть **Реплікація > Змінити** та ввімкніть опцію **Використовувати проксі-сервер**.
- j. Введіть IP-адресу комп'ютера проксі-сервера в полі **Хост**. (IP-адреса 10.1.1.10 є лише прикладом, замініть її на свою адресу)
- k. Залиште значення за замовчуванням **3128** для **порту**.
- l. Щоб зберегти політику, натисніть **Зберегти** та **Готово**. Наразі не призначайте її жодному комп'ютеру.



#### Увага

- Обов'язково необхідно внести обидві IP-адреси в один список, що застосовується до клієнта. Якщо агент не має цієї інформації в одній політиці, після оновлення він не зможе підключитися до проксі-сервера та сервера. У такий агент потрібно внести зміни вручну. Для цього виконайте відновлювальну інсталяцію та вкажіть правильну адресу сервера ESET PROTECT.
- Якщо параметр проксі-сервера HTTP не застосовується в політиці, агент не зможе підключитися до сервера ESET PROTECT.

8. Виберіть один комп'ютер, підключений через проксі-сервер ERA, і призначте йому нову політику.
9. Зачекайте кілька хвилин, поки політика застосовується, і перевірте підключення комп'ютера до сервера ESET PROTECT.
10. Щоб оновити клієнт, виконайте завдання **Оновити компоненти ESET PROTECT**.
11. Коли клієнт оновиться до версії 8, перевірте його підключення до сервера ESET PROTECT. Якщо після оновлення комп'ютеру вдається підключитися, оновіть інші комп'ютери.



#### Увага

Якщо у вас велика мережа, почніть оновлення з відділів, у яких користувачі мають досвід роботи з IT-технологіями або фізично знаходяться ближче до комп'ютерів. Це спростить процес виправлення неполадок.

12. Застосуйте політику (з кроку 7) до інших комп'ютерів, підключених через проксі-сервер ERA.
13. Зачекайте кілька хвилин, поки політика застосовується, і перевірте підключення клієнтів до сервера ESET PROTECT.
14. Запустіть завдання **Оновити компоненти ESET PROTECT** на цих клієнтах.
15. Якщо після оновлення всі клієнти підключаються до сервера ESET PROTECT, перейдіть до наступних кроків.
16. Змініть політику (з кроку 5). Перейдіть у меню **Політики**, натисніть піктограму шестирні біля політики, яку потрібно змінити, і виберіть **Редагувати**.
- a. У меню **Параметри > Підключення** натисніть **Редагувати список серверів** і видаліть адресу комп'ютера проксі-сервера ERA.
- b. Натисніть **Зберегти**.
- c. Щоб зберегти та застосувати політику, натисніть **Готово**.
17. Видаліть проксі-сервер ERA в меню **Завдання > Видалення програмного забезпечення**.

#### Перенесення з ERA 5.x

Неможливо напряму оновити або виконати перехід із ERA 5.x до ESET PROTECT 8.0.

Якщо ви інсталиювали ERA 5.x, виконайте такі дії:

1. [Перейдіть із ERA 5.x до ESMC 7.2](#)
2. [Оновіть ESMC 7.2 до ESET PROTECT 8.0](#)

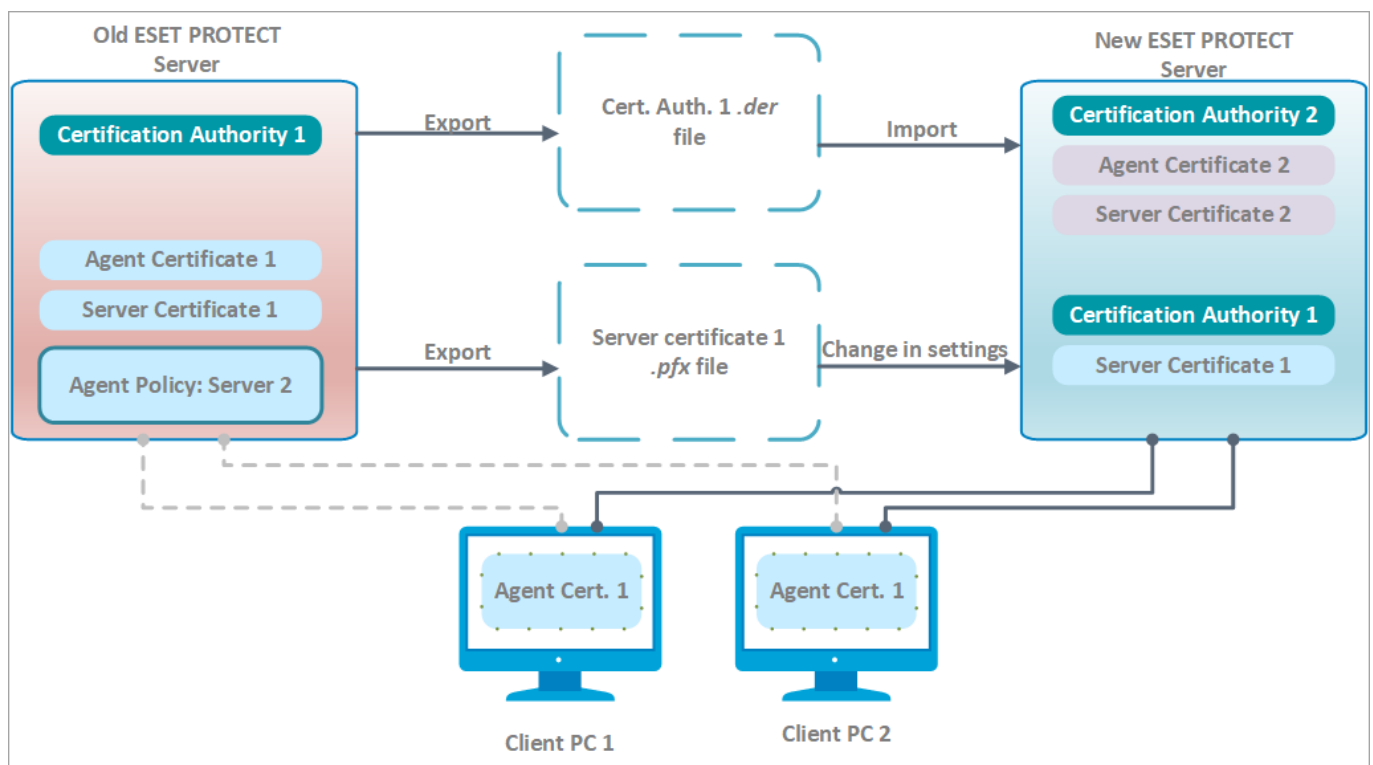
## Перенесення з одного сервера на інший

Існує кілька способів перенести ESET PROTECT з одного сервера на інший (ці сценарії можна використовувати під час повторної інсталяції ESET PROTECT Server).

- [Чиста інсталяція – така сама IP-адреса](#): під час нової інсталяції не використовується попередня база даних зі старого сервера ESET PROTECT і зберігається оригінальна IP-адреса.
- [Чиста інсталяція – інша IP-адреса](#) (стаття бази знань): під час нової інсталяції не використовується попередня база даних зі старого сервера ESET PROTECT і змінюється IP-адреса.
- [Перенесена база даних: інша/така сама IP-адреса](#): переносити базу даних можна, лише якщо обидві бази даних належать до двох однакових типів (з MySQL у MySQL або з MSSQL у MSSQL) і мають схожі версії ESET PROTECT.

## Чиста інсталяція - така сама IP-адреса

Мета цієї процедури – інсталювати повністю новий екземпляр сервера ESET PROTECT, який не використовуватиме попередню базу даних, але зберігатиме записи клієнтських комп'ютерів. Новий сервер ESET PROTECT матиме **таку саму IP-адресу**, що й попередній, але не буде використовувати базу даних зі старого сервера ESET PROTECT.



[Клацніть тут, щоб збільшити зображення](#)

- На поточному (старому) сервері ESET PROTECT виконайте вказані нижче дії:**



### Попередження

Якщо клієнтські комп'ютери зашифровані за допомогою [ESET Full Disk Encryption](#), [дешифруйте](#) їх перед переносом на інший сервер ESET PROTECT Server, щоб уникнути втрати [даних для відновлення](#). Після міграції можна знову [зашифрувати](#) клієнтські комп'ютери з використанням нового ESET PROTECT Server.

1. Експортуйте сертифікат сервера з поточного сервера ESET PROTECT і збережіть його в зовнішньому сховищі.

- Експортуйте всі [сертифікати Центру сертифікації](#) із сервера ESET PROTECT і збережіть кожен із них

як файл .der.

- Екпоруйте [сертифікат сервера](#) із сервера ESET PROTECT у файл .pfx. Експортований файл .pfx міститиме також закритий ключ.

2. Зупиніть службу сервера ESET PROTECT.

3. Вимкніть комп'ютер, на якому запущено сервер ESET PROTECT.



#### Увага!

Поки не видаляйте й не виводьте з роботи свій старий ESET PROTECT Server.

**На новому сервері ESET PROTECT виконайте вказані нижче дії.**



#### Увага

Щоб використовувати новий ESET PROTECT Server із тією ж самою IP-адресою, переконайтеся, що конфігурація мережі на новому ESET PROTECT Server (**IP-адреса, FQDN, ім'я комп'ютера, запис SRV DNS**) збігається з вашим старим ESET PROTECT Server.

1. Інсталюйте сервер ESET PROTECT або MDM за допомогою [універсального інсталятора](#) (Windows) або виберіть [інший спосіб інсталяції](#) (ручна інсталяція у Windows, Linux або на віртуальному пристрої).

2. [Підключіться](#) до веб-консолі ESET PROTECT.

3. Імпоруйте всі центри сертифікації, експортовані зі старого сервера ESET PROTECT. Для цього виконайте вказівки з [імпорту відкритого ключа](#).

4. Змініть сертифікат сервера ESET PROTECT у розділі [Параметри сервера](#), щоб використовувати сертифікат старого сервера ESET PROTECT.

5. [Імпоруйте всі відповідні ліцензії ESET](#) до ESET PROTECT.

6. Перезавантажте службу сервера ESET PROTECT. Докладніше див. у [статті бази знань](#).

Тепер клієнтські комп'ютери мають підключатися до нового сервера ESET PROTECT за допомогою оригінального сертифіката агента ESET Management, автентифікованого ЦС, імпортованим зі старого сервера ESET PROTECT. Якщо клієнти не підключаються, перегляньте розділ [Проблеми після оновлення/перенесення сервера ESET PROTECT](#).



#### Примітка

Коли додаєте нові клієнтські комп'ютери, використовуйте нові Центри сертифікації для підпису сертифікатів агента. За допомогою імпортованих ЦС не можна підписувати нові сертифікати однорангових вузлів, а можна лише автентифікувати перенесені агенти ESET Management клієнтських комп'ютерів.

**Видалення старого сервера ESET PROTECT або MDM:**

Перевіривши, що на новому сервері ESET PROTECT все працює належним чином, виконайте [покрокові інструкції](#) й обережно виведіть із роботи старий сервер ESET PROTECT або MDM.

### Перенесена база даних: інша/така сама IP-адреса

Мета цієї процедури – інсталювати повністю новий екземпляр сервера ESET PROTECT і **зберегти наявну базу даних** ESET PROTECT, зокрема наявні клієнтські комп'ютери. Новий ESET PROTECT Server матиме **таку саму або іншу IP-адресу**, а базу даних старого ESET PROTECT Server буде імпортовано на новий сервер перед інсталяцією.



### Увага

- [Перенесення баз даних](#) підтримується лише для ідентичних типів баз даних (з MySQL у MySQL і з MSSQL у MSSQL).
- Перенесення бази даних потрібно виконувати між екземплярами однакової версії ESET PROTECT. Перегляньте вказівки з визначення версій компонентів ESET PROTECT у нашій [статті бази знань](#). Після перенесення бази даних можна виконати оновлення (за необхідності), щоб отримати останню версію ESET PROTECT.

### На поточному (старому) сервері ESET PROTECT виконайте вказані нижче дії:



### Увага

- Якщо новий ESET PROTECT Server має **іншу IP-адресу**, виконайте вказані додаткові дії по відношенню до поточного (старого) ESET PROTECT Server:
- а) Створіть [новий сертифікат сервера ESET PROTECT](#) з інформацією про підключення для нового сервера ESET PROTECT. Залиште значення за замовчуванням (зірочку) у полі **Хост**, щоб дозволити розповсюдження цього сертифіката без прив'язки до конкретного імені DNS чи IP-адреси.
  - б) Створіть політику, щоб задати [нову IP-адресу сервера ESET PROTECT](#) і призначити її всім комп'ютерам. Зачекайте, поки політика розповсюдиться на всі клієнтські комп'ютери (комп'ютери переставатимуть звітувати, щойно отримають інформацію про новий сервер).

1. Зупиніть службу сервера ESET PROTECT.
2. [Експортуйте базу даних ESET PROTECT або створіть її резервну копію](#).
3. Вимкніть поточний ESET PROTECT Server (необов'язково, якщо новий сервер має іншу IP-адресу).



### Увага!

Поки не видаляйте й не виводьте з роботи свій старий ESET PROTECT Server.

### На новому сервері ESET PROTECT виконайте вказані нижче дії.



### Увага

Щоб використовувати новий ESET PROTECT Server із тією ж самою IP-адресою, переконайтеся, що конфігурація мережі на новому ESET PROTECT Server (**IP-адреса, FQDN, ім'я комп'ютера, запис SRV DNS**) збігається з вашим старим ESET PROTECT Server.

1. Інсталюйте або запустіть [підтримувану](#) базу даних ESET PROTECT.
2. Імпортуйте або відновіть [базу даних ESET PROTECT](#) зі старого сервера ESET PROTECT.
3. Інсталюйте сервер ESET PROTECT або MDM за допомогою [універсального інсталюатора](#) (Windows) або виберіть [інший спосіб інсталяції](#) (ручна інсталяція у Windows, Linux або на віртуальному пристрої). Під час інсталяції сервера ESET PROTECT задайте налаштування підключення бази даних.
4. [Підключіться](#) до веб-консолі ESET PROTECT.

Тепер клієнтські комп'ютери мають підключатися до нового ESET PROTECT Server за допомогою оригінального сертифіката ESET Management Agent. Якщо клієнти не підключаються, перегляньте розділ [Проблеми після оновлення/перенесення сервера ESET PROTECT](#).

### Видалення старого сервера ESET PROTECT або MDM:

Перевіривши, що на новому сервері ESET PROTECT все працює належним чином, виконайте [покрокові інструкції](#) й обережно виведіть із роботи старий сервер ESET PROTECT або MDM.

Створення резервної копії, оновлення сервера бази даних і перенесення бази даних ESET PROTECT

ESET PROTECT використовує базу даних для зберігання даних клієнта. Нижче докладно описано процедури [резервного копіювання](#), [оновлення](#) й [перенесення](#) бази даних ESET PROTECT Server (ESMC Server, ERA Server або ERA 6.x Proxy) або бази даних MDM:

- Якщо у вас немає бази даних, яку можна використовувати сервером ESET PROTECT, до інсталятора також буде додано **Microsoft SQL Server Express**. ESET PROTECT 8.0 [Універсальний інсталятор](#) за замовчуванням інсталує Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інстальватиметься за замовчуванням.
- Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MSSQL 2008), [оновіть базу даних](#) до [сумісної версії](#), перш ніж оновлювати сервер ESET PROTECT.



#### Примітка

Компонет проксі-сервера ERA версії 6 замінено сторонньою службою [проксі-сервера](#) через змінення протоколу реплікації агента. Не переносьте базу даних проксі-сервера версії 6. [Оновлюєте середовище за допомогою проксі-сервера ERA?](#)

Потрібно дотримуватися вказаних нижче вимог до Microsoft SQL Server.

- Інстальуйте [підтримувану версію Microsoft SQL Server](#). Під час інсталяції виберіть **змішаний режим** автентифікації.
- Якщо у вас уже інстальовано Microsoft SQL Server, виберіть для автентифікації значення **Змішаний режим (автентифікація SQL Server та Windows)**. Для цього виконайте вказівки з цієї [статті бази знань](#). Якщо ви хочете використовувати для входу в Microsoft SQL Server **автентифікацію Windows**, виконайте дії з [цієї статті бази знань](#).
- Дозвольте підключення TCP/IP до сервера SQL Server. Для цього виконайте дії з розділу **II. Дозвіл на підключення TCP/IP до бази даних SQL** [цієї статті бази знань](#).



#### Примітка

- Щоб налаштувати Microsoft SQL Server та керувати цим сервером (бази даних і користувачі), [завантажте SQL Server Management Studio \(SSMS\)](#).
- Рекомендуємо [не інстальювати SQL Server в контролері домену](#) (наприклад, якщо ви використовуєте Windows SBS / Essentials). Рекомендуємо інстальювати ESET PROTECT на іншому сервері або не вибирати компонент SQL Server Express під час інсталяції (щоб запустити базу даних ESET PROTECT, потрібно скористатися наявним сервером SQL Server або MySQL Server).

## Перенесення бази даних ESET PROTECT

Наведені нижче інструкції описують процедуру перенесення бази даних ESET PROTECT між різними екземплярами SQL Server (а також перенесення на іншу версію SQL Server або SQL Server, розміщений на іншому комп'ютері).

- [Процедура міграції для MS SQL Server](#)
- [Процедура міграції для MySQL Server](#)

## Створення резервної копії та відновлення сервера бази даних

Всі дані та налаштування ESET PROTECT зберігаються в базі даних. Рекомендується регулярно створювати резервні копії бази даних, щоб запобігти втраті даних. Див. розділ, що відповідає базі даних, яку ви використовуєте:



### Примітка

- Резервну копію також можна використовувати в разі міграції ESET PROTECT на новий сервер.
- Назви баз даних і файлів журналів не змінилися навіть після перейменування продукту з ESET Remote Administrator на ESET Security Management Center або ESET PROTECT.

## Інструкції з резервного копіювання MS SQL

Для резервного копіювання бази даних MS SQL у файл виконайте наведені нижче інструкції:



### Увага

- Ці інструкції призначено для налаштувань за замовчуванням (наприклад, для баз даних, ім'я та параметри підключення яких не було змінено). Налаштуйте свій скрипт резервного копіювання відповідно до всіх змін, які ви внесли до налаштувань за замовчуванням.
- Для виконання команд нижче обліковий запис має мати певні права. Якщо ви не використовуєте локальний обліковий запис адміністратора, змініть шлях для збереження резервної копії, наприклад на 'C:\USERS\PUBLIC\BACKUPFILE'.

## Одноразове резервне копіювання бази даних

Виконайте цю команду в командному рядку Windows, щоб створити резервну копію у файлі **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```



### Примітка

У цьому прикладі **HOST** містить IP-адресу або ім'я хоста, а **ERASQL** – ім'я екземпляра сервера MS SQL. Починаючи з версії ESET PROTECT 7, ви можете (при використанні бази даних MS SQL) інсталювати сервер ESET PROTECT на екземпляр SQL із власною назвою. Змініть скрипти резервного копіювання відповідно до цього сценарію використання.

## Регулярне резервне копіювання бази даних за допомогою скрипта SQL

Виберіть одну з таких команд SQL:

а) Регулярно створюйте резервні копії та зберігайте їх за датою створення:

```
1. @ECHO OFF
2. SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'
WITH NOFORMAT, INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
3. REN BACKUPFILE BACKUPFILE-[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

б) Зберіть свої резервні копії в один файл:

```
1. @ECHO OFF
2. SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'
WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
```

## Відновлення MS SQL

Щоб відновити базу даних MS SQL із файлу, скористайтеся наведеною нижче командою:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

## Резервне копіювання MySQL

Щоб зберегти резервну копію бази даних MySQL у файл, скористайтеся наведеною нижче командою:



```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -p ERADBNNAME > BACKUPFILE
```



#### Примітка

У цьому прикладі **HOST** містить IP-адресу або ім'я хоста сервера MySQL, **ROOTLOGIN** – кореневий обліковий запис MySQL Server, а **ERADBNNAME** – ім'я бази даних ESET PROTECT.

## Відновлення MySQL

Щоб відновити базу даних MySQL із файлу, скористайтеся наведеною нижче командою:

```
mysql --host HOST -u ROOTLOGIN -p ERADBNNAME < BACKUPFILE
```



#### Примітка

Для отримання додаткової інформації про резервне копіювання Microsoft SQL Server відвідайте [сайт TechNet від Microsoft](#). Для отримання додаткової інформації про резервне копіювання MySQL Server відвідайте [сайт із документацією щодо MySQL](#).

## Оновлення сервера бази даних

Дотримуйтеся наведених нижче інструкцій, щоб оновити наявний екземпляр Microsoft SQL Server для використання з базою даних сервера ESET PROTECT.

1. Зупиніть роботу всіх запущених служб сервера ERA/ESMC/ESET PROTECT або проксі-сервера ERA, що підключаються до сервера бази даних, який необхідно оновити. Також зупиніть роботу всіх інших програм, що можуть підключатися до вашого екземпляра Microsoft SQL Server.
2. Перш ніж продовжувати, [створіть резервну копію](#) всіх відповідних баз даних.
3. Виконайте оновлення сервера бази даних.

## Оновлення SQL Server:

Інструкції з оновлення бази даних MS SQL Express 2008 до останньої версії див. у [статті бази знань](#). Крім того, ви можете скористатись інструкціями виробника бази даних: <https://msdn.microsoft.com/en-us/library/bb677622.aspx>.

## Оновлення MySQL Server:

- [Оновлення з MySQL 5.5 до версії 5.6](#)
- [Оновлення з MySQL 5.6 до версії 5.7](#)
- [Оновлення з MySQL 5.7 до версії 8](#)

4. Запустіть службу сервера ESET PROTECT та перегляньте журнали трасування, щоб переконатися, що підключення до бази даних здійснено правильно.

## Процедура міграції для MS SQL Server

Ця процедура міграції підходить для **Microsoft SQL Server** та **Microsoft SQL Server Express**.

Додаткову інформацію див. у наступній статті бази знань Microsoft: <https://msdn.microsoft.com/en-us/library/ms189624.aspx>.



### Примітка

Компонет проксі-сервера ERA версії 6 замінено сторонньою службою [проксі-сервера](#) через змінення протоколу реплікації агента. Не переносьте базу даних проксі-сервера версії 6. [Оновлюєте середовище за допомогою проксі-сервера ERA?](#)

### Необхідні компоненти

- Необхідно інстальювати вихідний і цільовий екземпляри SQL Server. Їх можна розмістити на різних комп'ютерах.
- Версія цільового екземпляра SQL Server повинна бути не менше версії вихідного екземпляра.

### Пониження версії не підтримується!

- Має бути інстальовано **SQL Server Management Studio**. Якщо екземпляри SQL Server розміщено на різних комп'ютерах, SQL Server Management Studio також слід інстальювати на обидва комп'ютери.

### Міграцію за допомогою SQL Server Management Studio.

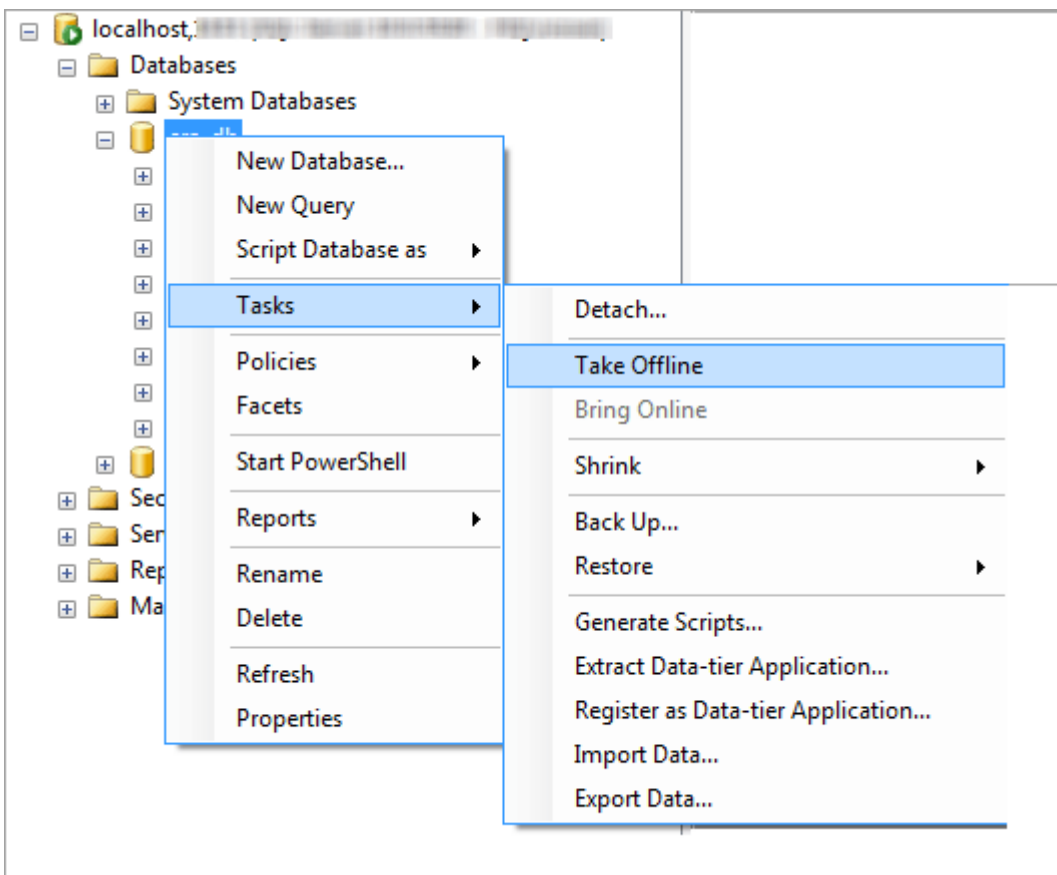
1. Вимкніть службу ESET PROTECT Server (ESMC Server або ERA Server або службу ERA 6.x Proxy) або службу ESET PROTECT MDM.



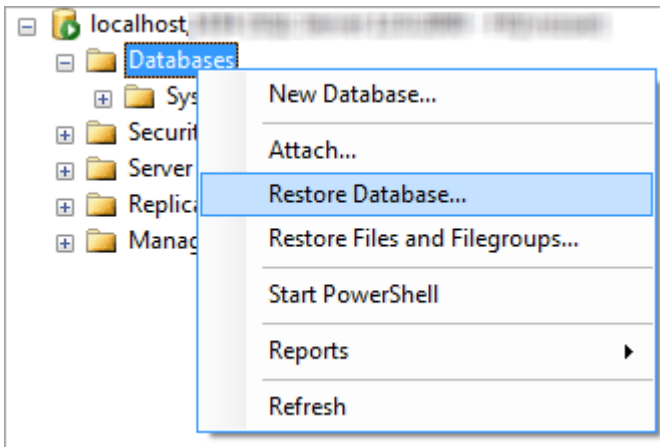
### Попередження

Не запускайте сервер ESET PROTECT та ESET PROTECT MDM, поки не виконаєте всі описані нижче кроки.

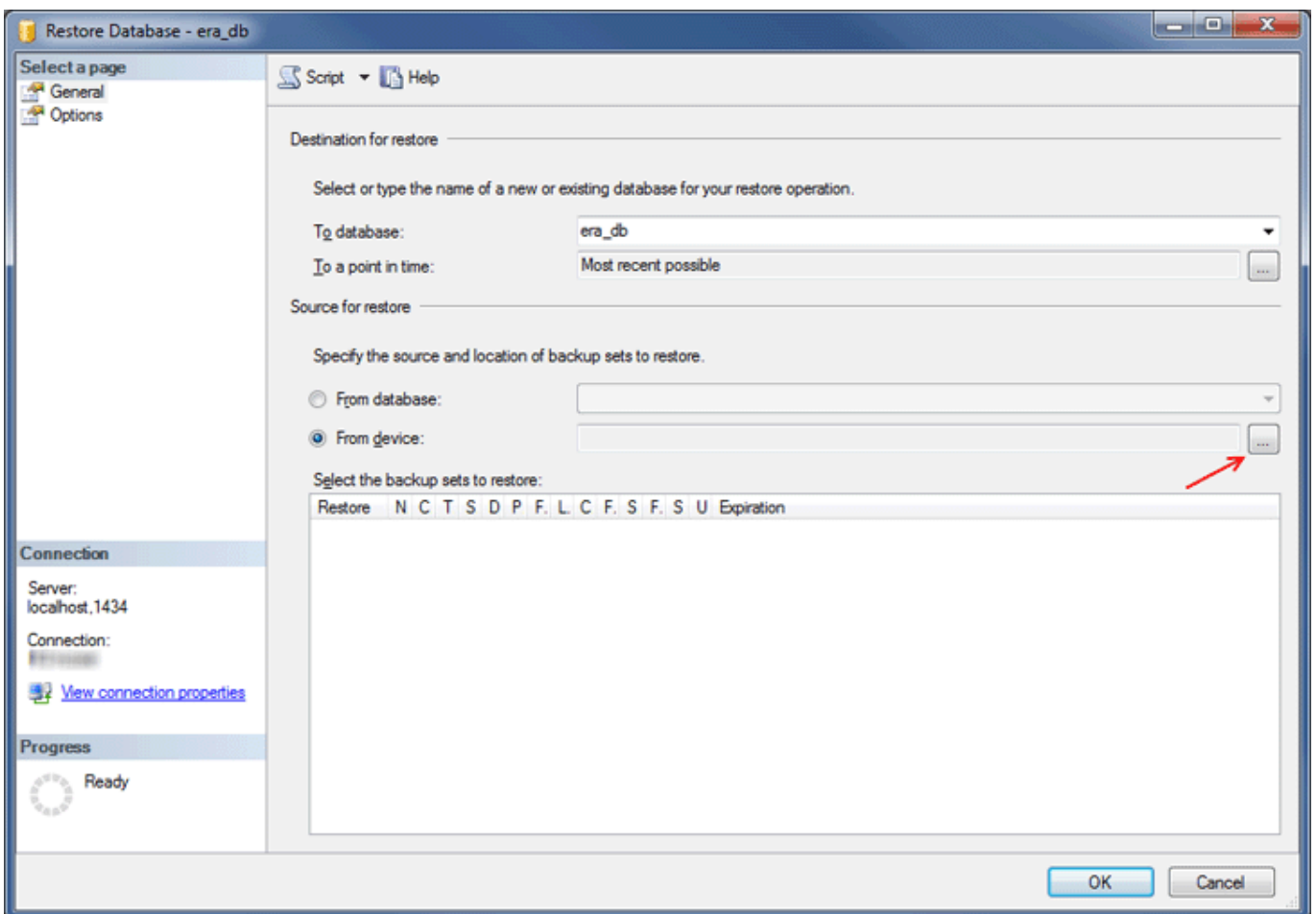
2. Увійдіть у вихідний екземпляр SQL Server за допомогою SQL Server Management Studio.
3. Створіть [повну резервну копію бази даних](#), міграція якої виконується. Рекомендується вказати нове ім'я для набору резервних копій. Якщо набір резервних копій вже існує, нову резервну копію буде додано до нього. Це призведе до створення занадто великої резервної копії.
4. Виберіть **Завдання > Відключити**, щоб відключити вихідну базу даних від мережі.



5. Скопіюйте створену на кроці 3 резервну копію (.bak) у папку, доступну з цільового екземпляра SQL Server. Вам може знадобитися змінити права доступу до резервної копії бази даних.
6. Увійдіть у цільовий екземпляр SQL Server за допомогою SQL Server Management Studio.
7. [Відновіть свою базу даних](#) на цільовому екземплярі SQL Server.



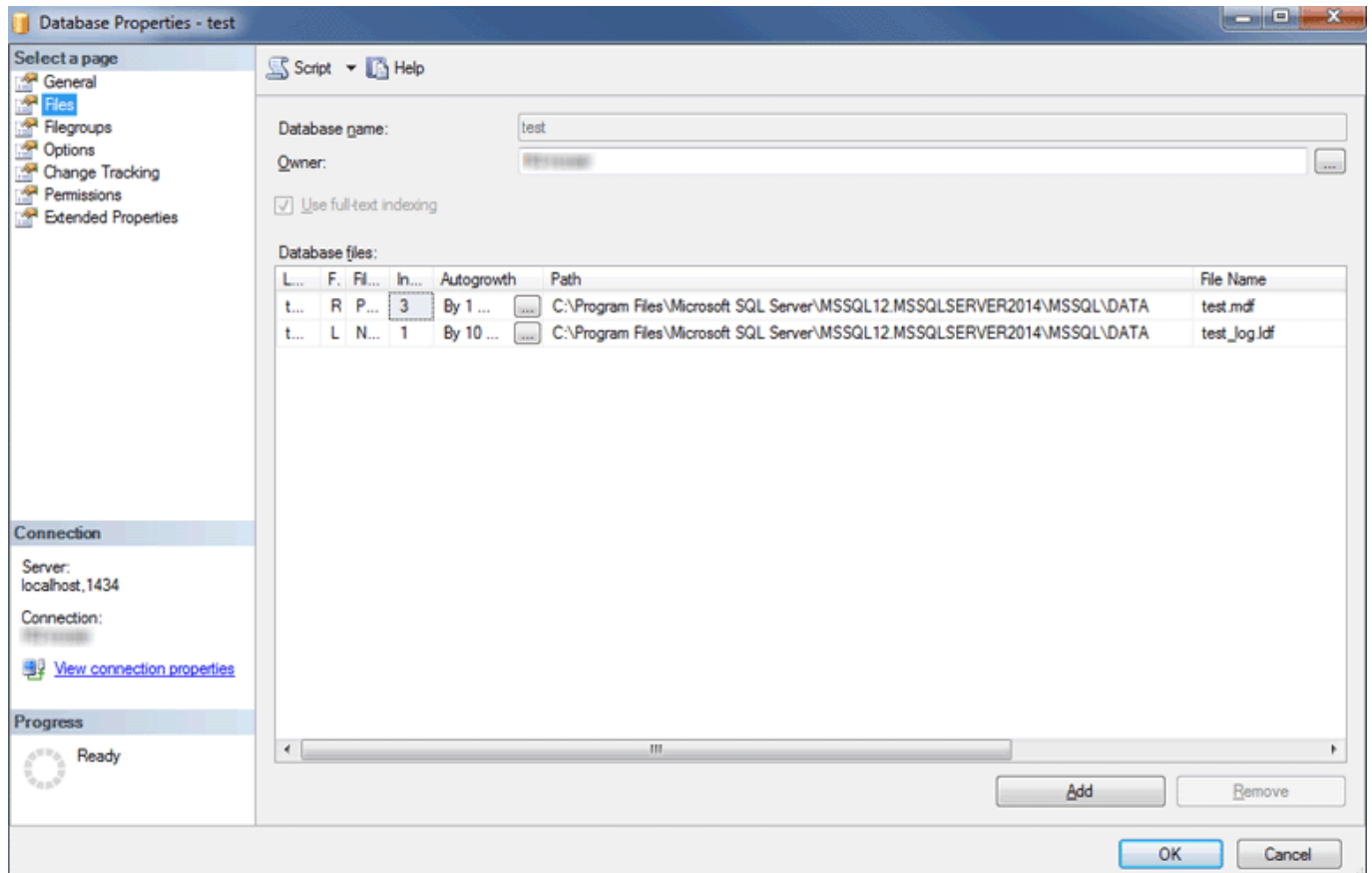
8. Введіть ім'я нової бази даних у поле **До бази даних**. Ви можете використати попереднє ім'я бази даних.
9. Виберіть пункт «З пристрою» в меню **Вкажіть джерело та місце розташування набору резервних копій для відновлення** й натисніть «...».



10. Клацніть **Додати**, перейдіть до резервної копії та відкрийте її.
11. Виберіть найновішу резервну копію для відновлення (у наборі може міститися кілька резервних копій).

12. Перейдіть на сторінку **Параметри** майстра відновлення. Ви також можете вибрати **Перезаписати наявну базу даних**. У цьому разі ще раз перевірте місця для відновлення бази даних (.mdf) і журналу (.ldf). Якщо ви не змінюєте значення за замовчуванням, використовуються шляхи з вихідного SQL-сервера, які необхідно перевірити.

- Якщо ви не знаєте, де зберігаються файли БД на цільовому екземплярі SQL Server, клацніть правою кнопкою миші наявну базу даних, виберіть **Властивості** та перейдіть на вкладку **Файли**. Папка, у якій зберігається база даних, відображається в стовпці **Шлях** наведеної нижче таблиці.

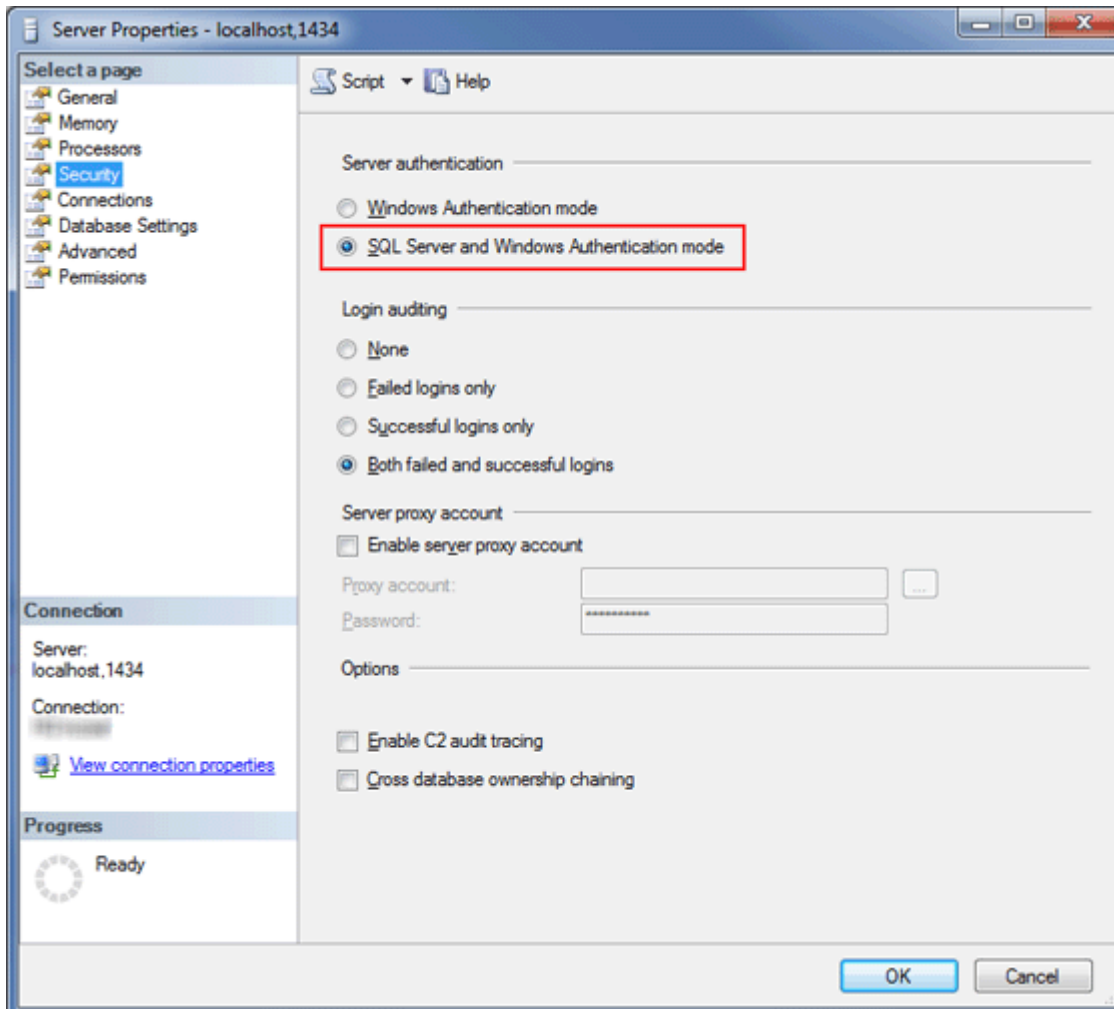


13. Натисніть **OK** у вікні майстра відновлення.

14. Клацніть правою кнопкою миші базу даних **era\_db**, виберіть **Новий запит** і запустіть наведений нижче запит, щоб видалити вміст таблиці **tbl\_authentication\_certificate** (в іншому разі агенти не зможуть підключитися до нового сервера):

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Переконайтесь, що на новому сервері баз даних увімкнено **автентифікацію SQL Server**. Клацніть правою кнопкою миші сервер і натисніть **Властивості**. Перейдіть на вкладку **Безпека** й переконайтесь, що пункт **Режим автентифікації SQL Server та Windows** вибрано.



16. Створіть нове ім'я користувача для SQL Server (для сервера ESET PROTECT/ESET PROTECT MDM) на цільовому SQL Server в пункті **Автентифікація SQL Server** та призначте це ім'я для користувача з відновленої бази даних.

○ Не встановлюйте термін дії пароля!

○ Рекомендовані символи для використання в імені користувача:

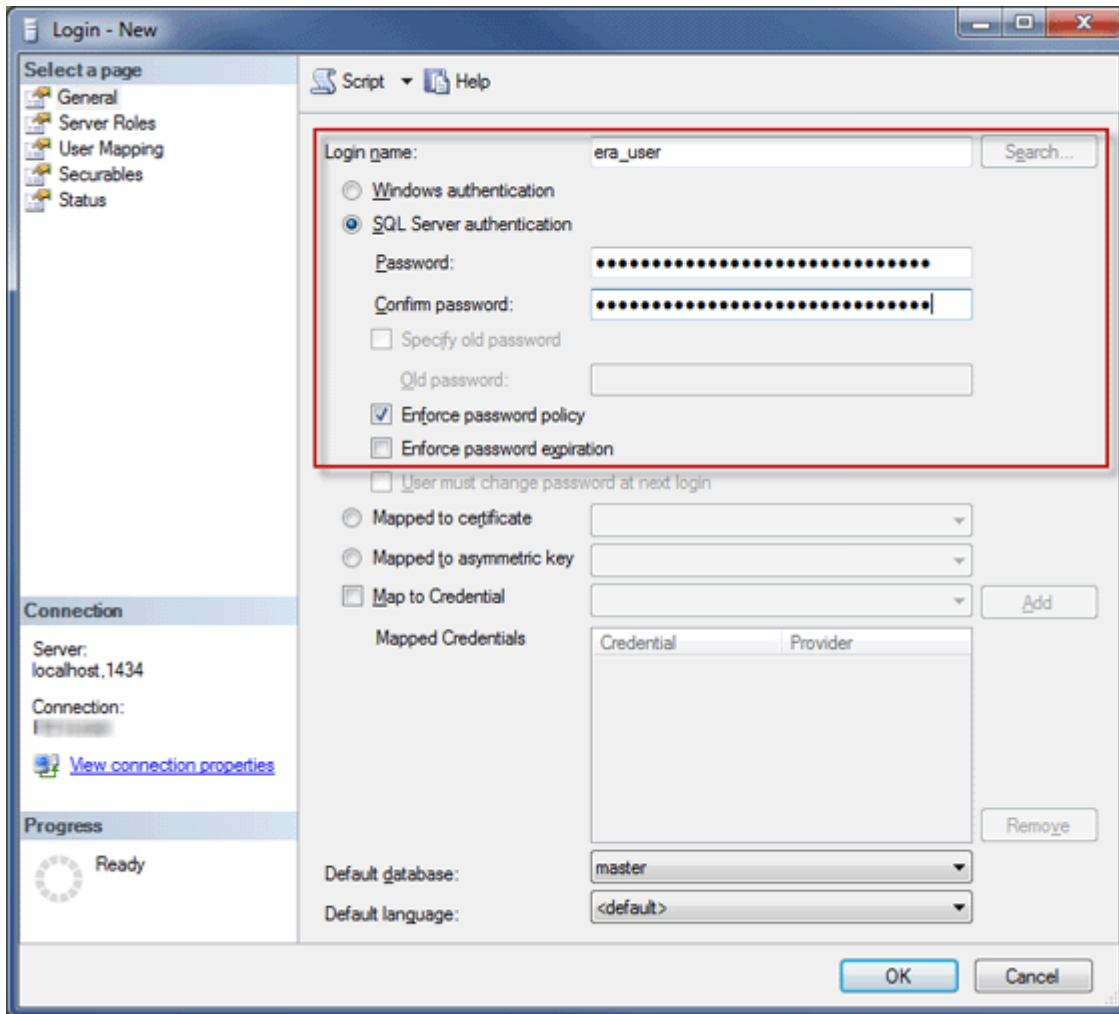
- Букви ASCII у нижньому регістрі, цифри та символи підкреслення «\_»

○ Рекомендовані символи для використання в паролі:

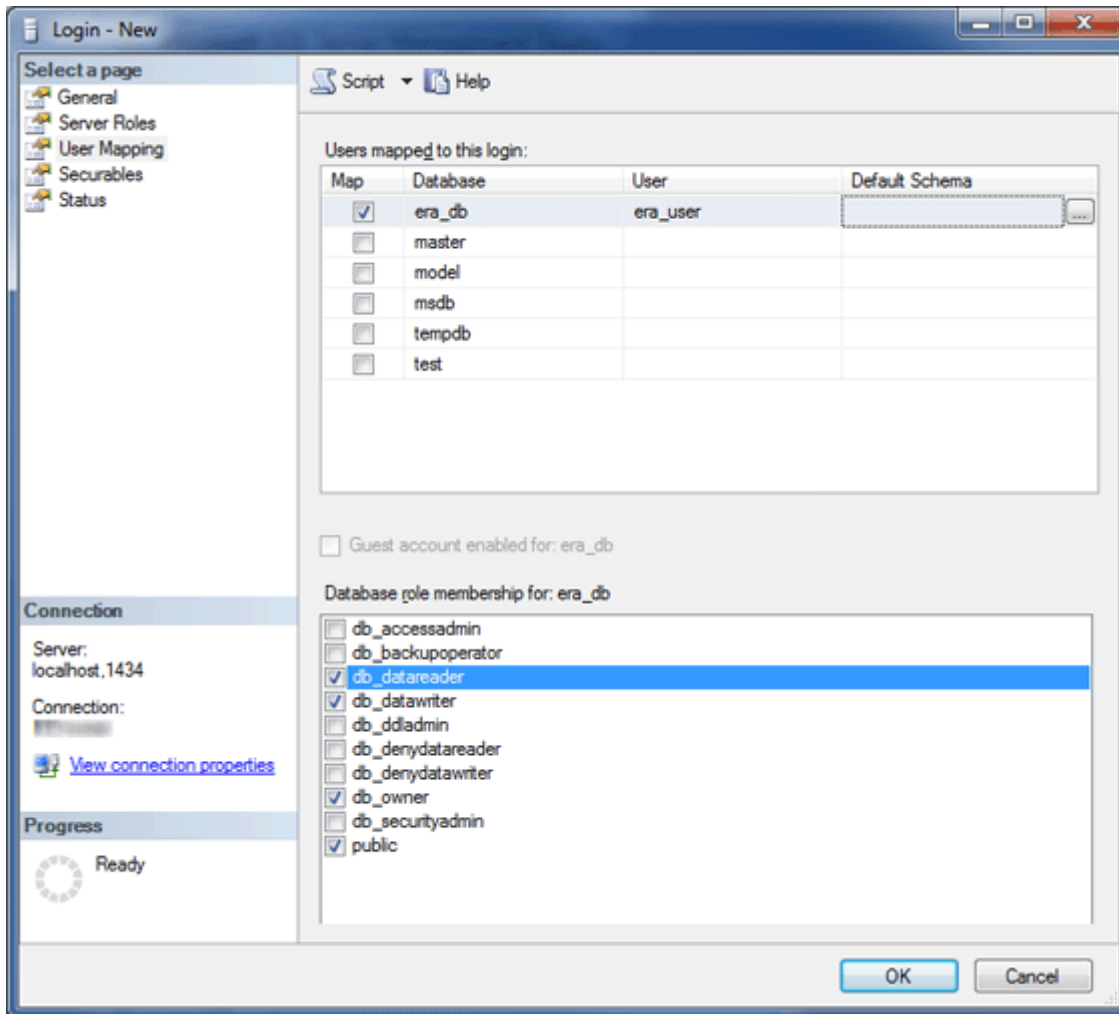
- ТІЛЬКИ символи ASCII, зокрема букви ASCII у верхньому та нижньому регістрах, цифри, пробіли, спеціальні символи

○ Не використовуйте інші символи, окрім ASCII, фігурні дужки «{}» і знак «@»

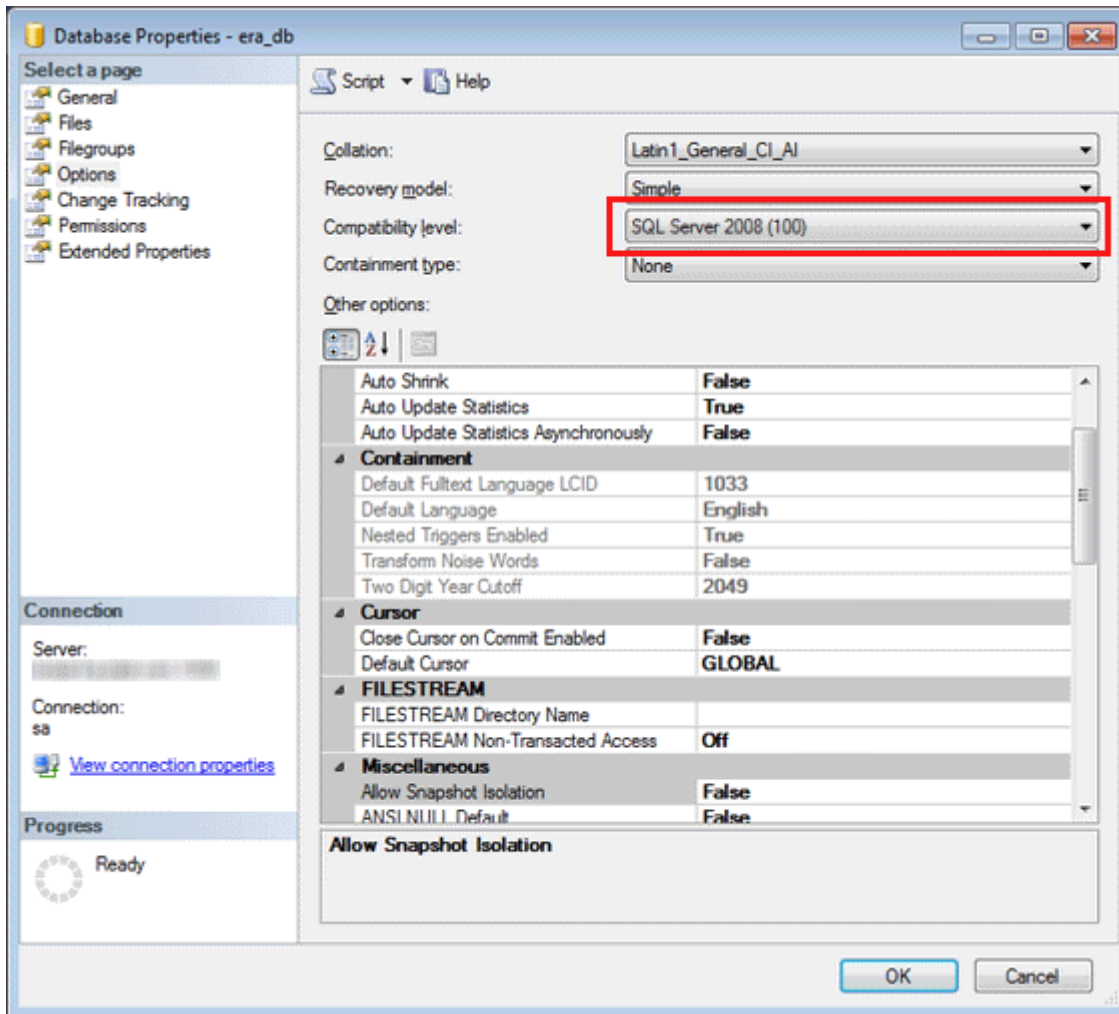
○ Зауважте, що в разі недотримання наведених вище рекомендацій у вас можуть виникнути проблеми з підключенням до бази даних, а під час подальшої зміни рядка підключення до бази даних ви не зможете використовувати спеціальні символи. Правила екранування символів не наведено в цьому документі.



17. Назначте ім'я для користувача з цільової бази даних. Переконайтеся, що на вкладці **зiставлення користувачiв** користувач має наступнi ролi: **db\_datareader**, **db\_datawriter**, **db\_owner**.



18. Щоб використовувати нові функції сервера баз даних, установіть для відновленої бази даних **Рівень сумісності** з останньою інстальованою версією. Клацніть правою кнопкою миші нову базу даних і відкрийте **Властивості**.

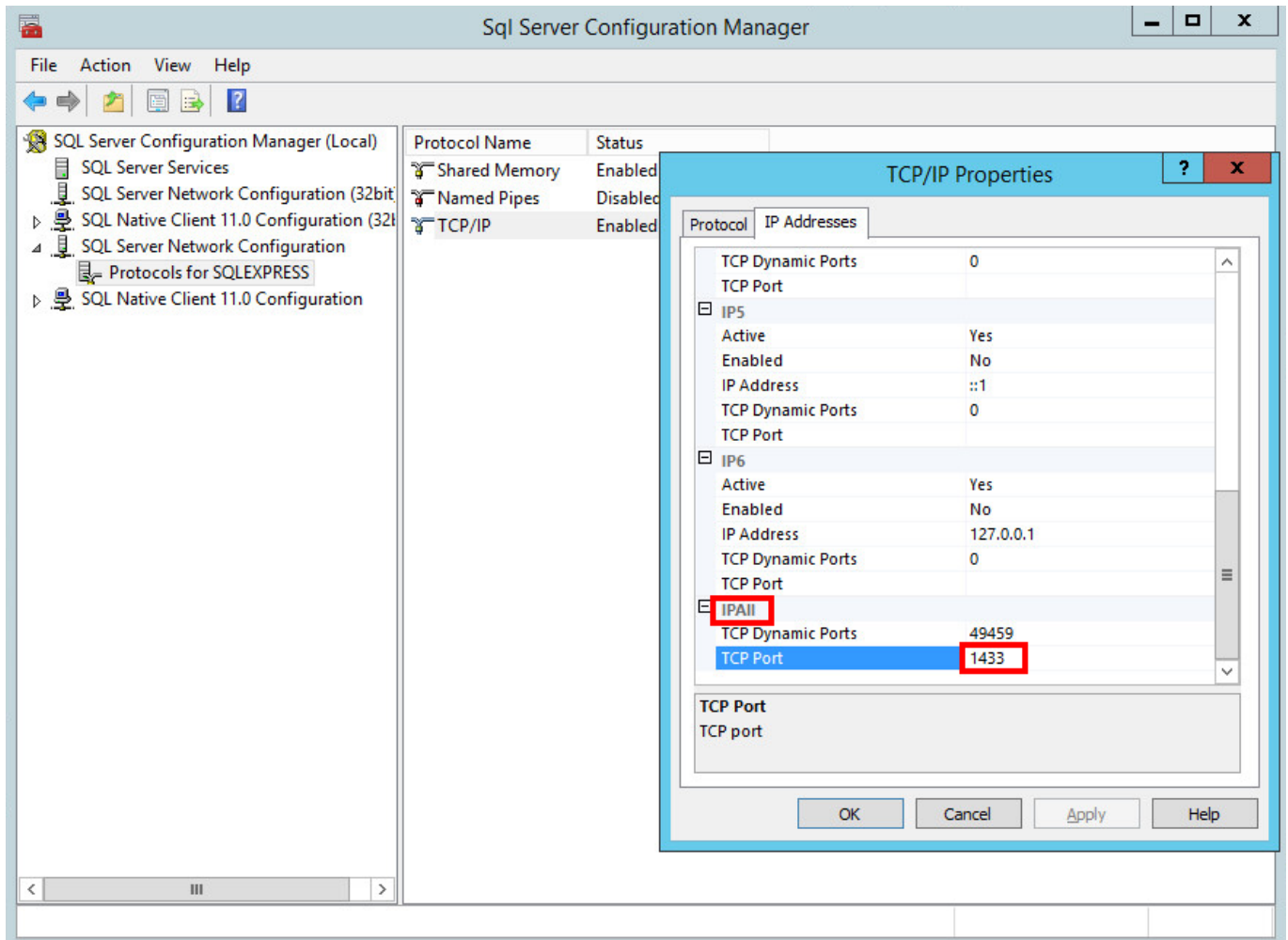


### Примітка

QL Server Management Studio не може визначити рівні сумісності з версіями, випущеними після використовуваної. Наприклад, SQL Server Management Studio 2014 не може бути сумісною з SQL Server 2019.

19. Переконайтеся, що протокол підключення **TCP/IP** для «db\_instance\_name» (наприклад, SQLEXPRESS або MSSQLSERVER) **увімкнено**, а також встановлено **порт TCP/IP 1433**. Для цього відкрийте **диспетчер конфігурацій Sql Server**, перейдіть до пункту *Конфігурація мережі SQL Server > Протоколи для db\_instance\_name*, клацніть правою кнопкою пункт **TCP/IP** та виберіть **Увімкнено**. Двічі клацніть пункт **TCP/IP**, перейдіть на вкладку **Протоколи**, прокрутіть екран до пункту **IPAll** і вкажіть для поля **Порт TCP** значення «1433». Натисніть **OK** і перезавантажте службу **SQL Server**.





20. Підключіть сервер ESET PROTECT або MDM до бази даних.

## Процедура міграції для MySQL Server

### Необхідні компоненти

- Необхідно інсталиювати вихідний і цільовий екземпляри SQL Server. Їх можна розмістити на різних комп'ютерах.
- Інструменти MySQL повинні бути інстальовані принаймні на одному з комп'ютерів (клієнти mysqldump і mysql).

### Корисні посилання

- <https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysql.html>

### Процедура перенесення



### Примітка

У наведених нижче командах, файлах конфігурації й операторах SQL замінійте:

- **SRCHOST** на адресу вихідного сервера баз даних;
- **SRCROOTLOGIN** на ім'я кореневого користувача вихідного сервера MySQL;
- **SRCERADBDNAME** на ім'я джерела бази даних ESET PROTECT для резервного копіювання;
- **BACKUPFILE** на шлях до файлу резервної копії;
- **TARGETROOTLOGIN** на ім'я кореневого користувача цільового сервера MySQL;
- **TARGETHOST** на адресу цільового сервера баз даних;
- **TARGETERADBDNAME** на назву цільової бази даних ESET PROTECT (після перенесення);
- **TARGETERALOGIN** на ім'я нового користувача бази даних ESET PROTECT на цільовому сервері бази даних;
- **TARGETERAPASSWD** на пароль нового користувача бази даних ESET PROTECT на цільовому сервері бази даних.

Запускати наведені нижче оператори SQL за допомогою командного рядка не потрібно. Якщо інстальовано графічний інтерфейс, ви можете використовувати вже відому програму.

1. **Зупиніть** службу сервера ESET PROTECT/MDM.

2. **Створіть** повну резервну копію вихідної бази даних ESET PROTECT (перенесення якої виконується):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -u SRCROOTLOGIN -p SRCERADBDNAME > BACKUPFILE
```

3. **Підготуйте** порожню базу даних на цільовому сервері MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE DATABASE TARGETERADBDNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```



### Примітка

У системах Linux використовуйте символ апострофа (') замість лапок (").

4. **Відновіть** базу даних на цільовому сервері MySQL до попередньо підготовленої порожньої бази даних:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETERADBDNAME < BACKUPFILE
```

5. **Створіть** користувача бази даних ESET PROTECT на цільовому сервері MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE USER TARGETERALOGIN@%' IDENTIFIED BY 'TARGETERAPASSWD';"
```

Рекомендовані символи для використання в полі **TARGETERALOGIN**:

- Букви ASCII у нижньому регістрі, цифри та символи підкреслення «\_»

Рекомендовані символи для використання в полі **TARGETERAPASSWD**:

- Тільки символи ASCII, зокрема букви ASCII у верхньому та нижньому регістрах, цифри, пробіли, спеціальні символи
- Не використовуйте інші символи, окрім ASCII, фігурні дужки «{}» і знак «@»

Зауважте, що в разі недотримання наведених вище рекомендацій у вас можуть виникнути проблеми з підключенням до бази даних, а під час подальшої зміни рядка підключення до бази даних ви не зможете використовувати спеціальні символи. Правила екранування символів не наведено в цьому документі.

6. **Надайте** відповідні права доступу для користувача бази даних ESET PROTECT на цільовому сервері MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=GRANT ALL ON TARGETERADBDNAME.* TO TARGETERALOGIN;"
```



### Примітка

У системах Linux використовуйте символ апострофа (') замість лапок (").

7. Видаліть вміст таблиці **tbl\_authentication\_certificate** (в іншому разі агенти не зможуть підключитися до нового сервера):

```
mysql --host TARGETHOST -u root -p "--execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Підключіть сервер ESET PROTECT або MDM до бази даних.

## Підключення сервера ESET PROTECT або MDM до бази даних

Виконайте наведені нижче дії на комп'ютері, де інстальовано сервер ESET PROTECT або MDM ESET PROTECT, щоб підключити його до бази даних.

1. Зупиніть службу сервера ESET PROTECT/MDM.

2. Знайдіть файл *startupconfiguration.ini*

ОУ Windows Vista та новіших версіях:

Сервер:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini
```

ОУ попередніх версіях Windows:

Сервер:

```
%ALLUSERSPROFILE%\Application
```

```
Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
```

MDMCore:

```
%ALLUSERSPROFILE%\Application
```

```
Data\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini
```

ОУ Linux:

Сервер:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. Змініть рядок підключення до бази даних у файлі *startupconfiguration.ini* сервера ESET PROTECT/MDM.

ОУстановіть адресу та порт нового сервера баз даних.

ОУстановіть нове ім'я користувача та пароль ESET PROTECT у рядку підключення.

Остаточний результат має виглядати так, як показано нижче.

#### • MS SQL:

```
DatabaseType=MSSQL0dbc
```

```
DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETERALOGIN;Pwd={TARGETERAPASSWD};CharSet=utf8;Database=TARGETERADBNAM;
```

#### • MySQL:

```
DatabaseType=MySQL0dbc
```

```
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETERALOGIN;Password={TARGETERAPASSWD};CharSet=utf8;Database=TARGETERADBNAM;
```



### Примітка

У наведеній вище конфігурації необхідно виконати такі заміщення:

- **TARGETHOST** на адресу цільового сервера баз даних;
- **TARGETERADBDNAME** на назву цільової бази даних ESET PROTECT (після перенесення);
- **TARGETERALOGIN** на ім'я нового користувача бази даних ESET PROTECT на цільовому сервері бази даних;
- **TARGETERAPASSWD** на пароль нового користувача бази даних ESET PROTECT на цільовому сервері бази даних.

4. Запустіть сервер ESET PROTECT або MDM ESET PROTECT і переконайтеся, що служба працює належним чином.

### Перенесення MDM

Мета цієї процедури – перенести наявний екземпляр ESET PROTECT MDM і **зберегти наявну базу даних ESET PROTECT MDM**, зокрема зареєстровані мобільні пристрої. Перенесений екземпляр ESET PROTECT MDM матиме **таку саму IP-адресу або ім'я хоста**, як і старий екземпляр ESET PROTECT MDM, а базу даних старого екземпляра ESET PROTECT MDM буде імпортовано в новий екземпляр MDM перед інсталяцією.



### Увага

- [Перенесення баз даних](#) підтримується лише для ідентичних типів баз даних (з MySQL у MySQL і з MSSQL у MSSQL).
- Перенесення бази даних потрібно виконувати між екземплярами однакової версії ESET PROTECT. Перегляньте вказівки з визначення версій компонентів ESET PROTECT у нашій [статті бази знань](#). Після перенесення бази даних можна виконати оновлення (за необхідності), щоб отримати останню версію ESET PROTECT.

### На поточному (старому) сервері ESET PROTECT MDM виконайте вказані нижче дії.

1. Перейдіть у меню **Інформація про комп'ютер** поточного сервера MDM і **експортуйте конфігурацію** з поточного (старого) сервера MDM. Відкрийте конфігурацію й екпортуйте вказані нижче елементи в зовнішнє сховище.

- Точне ім'я хоста сервера MDM.
- Екпортуйте сертифікати вузлів, які зараз є частиною політики MDM, із сервера ESET PROTECT у файл .rfx. Експортований файл .rfx міститиме закритий ключ. Екпортуйте також вказані нижче сертифікати та маркери (якщо є).

oСертифікат HTTPS

oСертифікат підпису профілю реєстрації

oСертифікат APNS (екпортуйте сертифікат і закритий ключ APNS).

oМаркер авторизації програми реєстрації пристроїв (DEP) Apple.

2. **Зупиніть** службу ESET PROTECT MDM.

3. [Екпортуйте базу даних ESET PROTECT MDM або створіть її резервну копію.](#)

4. **Вимкніть** поточний комп'ютер, на якому запущено ESET PROTECT MDM (необов'язково).



### Увага

Поки що не деінсталюйте та не виводьте з роботи старий сервер ESET PROTECT MDM.

### На новому сервері ESET PROTECT MDM виконайте вказані нижче дії.



### Увага

Переконайтеся, що конфігурація мережі на новому сервері ESET PROTECT MDM (**ім'я хоста, експортоване з конфігурації старого сервера MDM**) збігається з конфігурацією старого сервера ESET PROTECT MDM.

1. Інсталюйте або запустіть [підтримувану базу даних ESET PROTECT MDM](#).
2. Імпортуйте або відновіть [базу даних ESET PROTECT MDM](#) зі старого сервера ESET PROTECT MDM.
3. Інсталюйте сервер ESET PROTECT або MDM за допомогою [універсального інстальатора](#) (Windows) або виберіть [інший спосіб інсталяції](#) (ручна інсталяція у Windows, Linux або на віртуальному пристрої). Під час інсталяції ESET PROTECT MDM задайте налаштування підключення бази даних.
4. [Підключіться](#) до веб-консолі ESET PROTECT.
5. Створіть політику MDM та імпортуйте всі сертифікати у відповідні розташування в політиці.
6. **Перезавантажте** службу ESET PROTECT MDM. Докладніше див. у [статті бази знань](#).

Тепер керовані мобільні пристрої мають підключатися до нового сервера ESET PROTECT MDM за вихідними сертифікатами.

### Видалення старого сервера ESET PROTECT або MDM:

Перевіривши, що на новому сервері ESET PROTECT все працює належним чином, виконайте [покрокові інструкції](#) й обережно виведіть із роботи старий сервер ESET PROTECT або MDM.

Оновлення рішення ERA/ESMC, інсталюваного у відмовостійкому кластері у Windows

Якщо сервер ERA/ESMC [інсталювано в середовищі відмовостійкого кластера](#) у Windows і ви оновлюєте інсталяцію, виконайте дії нижче.



### Примітка

Термін **Роль** доступний у Windows Server 2012 і новіших версій. У Windows Server 2008 R2 натомість використовується термін **Служби та програми**.

### Оновлення з ERA 6.5 (або новішої версії) до останньої версії

1. Зупиніть роль кластера сервера ERA в диспетчері кластера. Переконайтеся, що службу **ESET Remote Administrator Server** зупинено на всіх вузлах кластера.
2. Підключіть спільний диск кластера на вузлі node1 до Інтернету й оновіть сервер ERA вручну. Для цього запустіть найновіший інстальатор *.msi*, так само як в процесі [інсталяції компонента](#). Після інсталяції (оновлення) переконайтеся, що службу **ESET Remote Administrator Server** зупинено.
3. Підключіть спільний диск кластера на вузлі node2 до Інтернету й оновіть сервер ERA, так само як у кроці 2.
4. Коли сервер ESET PROTECT буде оновлено на всіх вузлах кластера, запустіть роль сервера ESET PROTECT в диспетчері кластера.
5. Оновіть агент ESET Management вручну, запустивши найновіший інстальатор *.msi* на всіх вузлах кластера.
6. У веб-консолі ESET PROTECT перевірте, чи для всіх вузлів відображаються останні версії агента й сервера, до яких виконувалось оновлення.

### Оновлення проксі-сервера Apache HTTP

[Проксі-сервер HTTP Apache](#) – це служба, яку можна використовувати в комбінації з ESET PROTECT для розповсюдження оновлень на клієнтські комп'ютери й інсталяції пакетів на агентах ESET Management.

Якщо ви вже інсталювали проксі-сервер Apache HTTP у Windows раніше, а тепер хочете оновити його, то можете зробити це двома способами: [вручну](#) або за допомогою [універсального інстальатора](#).

## Оновлення проксі-сервера Apache HTTP за допомогою універсального інсталлятора (Windows)

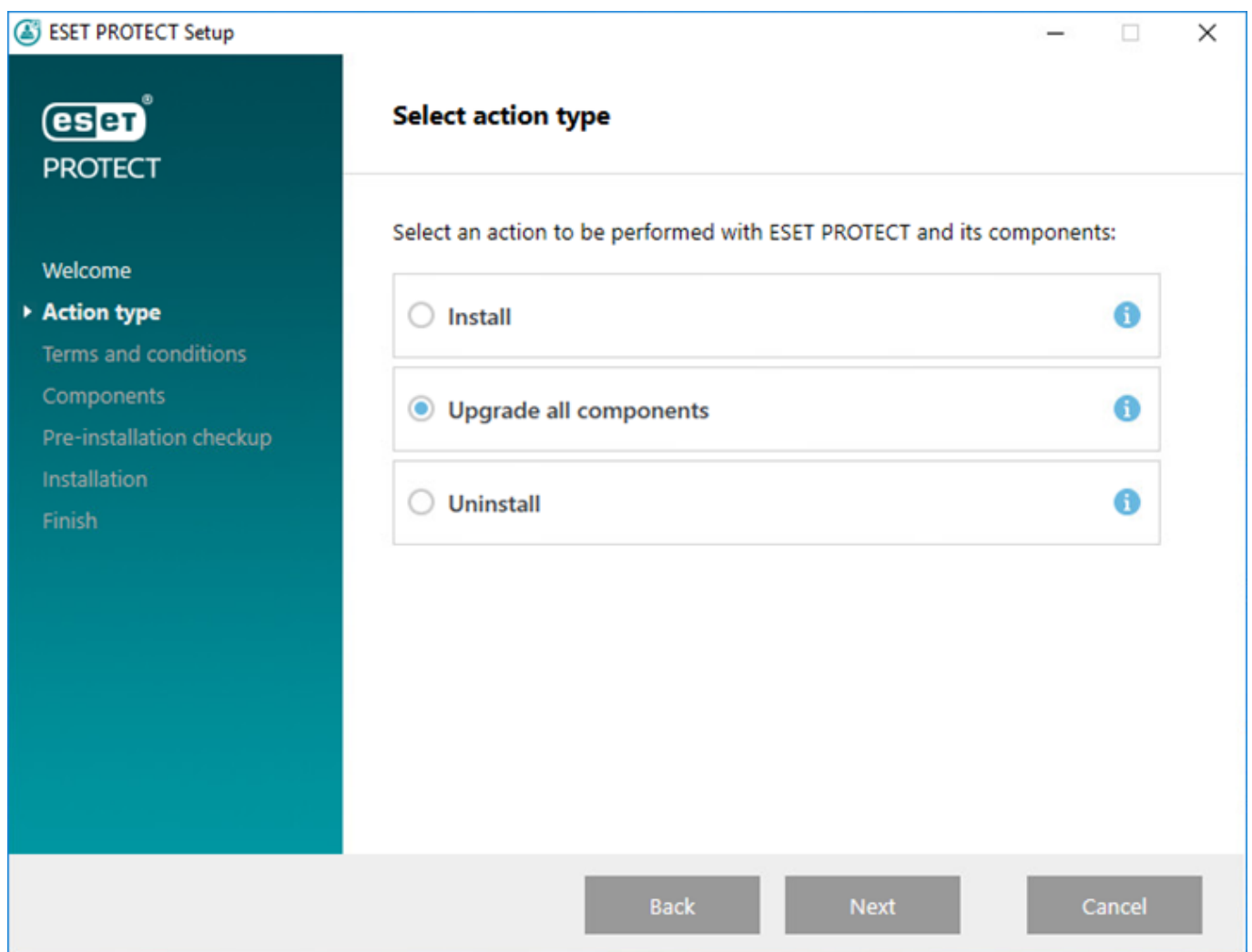
Якщо [універсальний інсталлятор ESET PROTECT](#) розташовано на локальному диску, можна скористатися цим способом, щоб швидко оновити проксі-сервер Apache HTTP до останньої версії. Якщо у вас немає інсталлятора, буде швидше [оновити проксі-сервер Apache HTTP вручну](#).

1. Створіть резервні копії цих файлів:

- *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
- *C:\Program Files\Apache HTTP Proxy\bin\password.file*
- *C:\Program Files\Apache HTTP Proxy\bin\group.file*

2. Запустіть універсальний інсталлятор, двічі натиснувши файл **setup.exe**, і виберіть **Далі** на екрані привітання.

3. Виберіть **Оновити всі компоненти** й натисніть **Далі**.



4. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

5. Натисніть **Оновити**, щоб виконати оновлення, а потім – **Готово**.

6. Перевірте підключення до проксі-сервера Apache HTTP. Для цього в браузері перейдіть за цією URL-адресою:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)

## Виправлення неполадок

### Щоб виправити неполадку, перегляньте [файли журналу проксі-сервера Apache HTTP](#).

Якщо користувацька конфігурація не збереглася після оновлення, виконайте вказівки нижче.

1. Зупиніть роботу служби **ApacheHttpProxy**. Для цього відкрийте [командний рядок адміністратора](#) та виконайте таку команду:  
`sc stop ApacheHttpProxy`
2. Якщо для доступу до проксі-сервера Apache HTTP використовується ім'я користувача або пароль (розділ [Інсталяція проксі-сервера Apache HTTP](#)), замініть цей блок коду:

```
<Proxy *>
Deny from all
</Proxy>
```

на такий (з резервної копії httpd.conf):

```
<Proxy *>
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

3. Якщо під час попередньої інсталяції проксі-сервера Apache HTTP ви вносили інші зміни у файл `httpd.conf`, скопіюйте ці зміни з файлу резервної копії `httpd.conf` у новий (оновлений) файл `httpd.conf`.
4. Збережіть зміни та запустіть службу **ApacheHttpProxy**. Для цього відкрийте [командний рядок у режимі адміністратора](#) та виконайте таку команду:  
`sc start ApacheHttpProxy`

## Оновлення проксі-сервера Apache HTTP вручну (Windows)

Щоб оновити Apache HTTP Proxy до останньої версії, виконайте дії нижче.

1. Створіть резервні копії цих файлів:
  - `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf`
  - `C:\Program Files\Apache HTTP Proxy\bin\password.file`
  - `C:\Program Files\Apache HTTP Proxy\bin\group.file`
2. Зупиніть роботу служби **ApacheHttpProxy**. Для цього відкрийте [командний рядок адміністратора](#) та виконайте таку команду:  
`sc stop ApacheHttpProxy`
3. Завантажте файл інсталятора Apache HTTP Proxy із [сайту завантаження](#) ESET і видобудьте його вміст у каталог `C:\Program Files\Apache HTTP Proxy\`. Під час видобування перезапишіть наявні файли.
4. Перейдіть у каталог `C:\Program Files\Apache HTTP Proxy\conf`, двічі натисніть **httpd.conf** і в контекстному меню виберіть **Відкрити за допомогою > Блокнот**.

5. Додайте внизу файлу `httpd.conf` цей код:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
 Options Indexes FollowSymLinks
 AllowOverride None
 Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

6. Якщо для доступу до проксі-сервера Apache HTTP використовується ім'я користувача або пароль (розділ [Інсталяція проксі-сервера Apache HTTP](#)), замініть цей блок коду:

```
<Proxy *>
 Deny from all
</Proxy>
```

на цей (з файлу `httpd.conf`, резервну копію якого ви створили на кроці 1):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

- Якщо під час попередньої інсталяції проксі-сервера Apache HTTP ви вносили інші зміни у файл `httpd.conf`, скопіюйте ці зміни з файлу резервної копії `httpd.conf` у новий (оновлений) файл `httpd.conf`.

7. Збережіть зміни та запустіть службу **ApacheHttpProxy**. Для цього відкрийте [командний рядок адміністратора](#) та виконайте таку команду:

```
sc start ApacheHttpProxy
```

8. Оновіть версію в описі служби.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Перевірте підключення до проксі-сервера Apache HTTP. Для цього в браузері перейдіть за цією URL-адресою:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)

Якщо потрібно виправити неполадку, перегляньте розділ [Файли журналу проксі-сервера Apache HTTP](#).

## Оновлення Apache Tomcat

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT.

Якщо оновлюєте ESET PROTECT до останньої версії або якщо ви не оновлювали Apache Tomcat протягом довгого періоду, рекомендуємо оновити Apache Tomcat до останньої версії. Якщо загальнодоступні служби,



зокрема Apache Tomcat і залежності цього компонента, своєчасно оновлюються, це підвищує захист системи безпеки середовища.

Щоб оновити Apache Tomcat, виконайте вказівки для своєї ОС.

- [Вказівки для Windows \(ручне оновлення\)](#) або [вказівки для Windows \(універсальне оновлення\)](#).
- [Вказівки для Linux](#).

## Оновлення Apache Tomcat за допомогою універсального інстальатора (Windows)

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT. Використовуйте цей спосіб, щоб швидко оновити Apache Tomcat за допомогою останньої версії [ESET PROTECT 8.0 Універсальний інстальатор](#). Крім цього, ви можете [оновити Apache Tomcat вручну](#).

1. Створіть резервні копії цих файлів:

```
C:\Program Files\Apache Software Foundation\[Tomcat папка]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat папка]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat папка]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

Якщо ви використовуєте налаштовуваний сертифікат SSL, що зберігається в папці *Tomcat*, створіть його резервну копію теж.



### Попередження

- Якщо встановлено налаштовану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інстальатора або завдання «Оновлення компонентів» не підтримується.
- Під час оновлення Apache Tomcat буде видалено папку *era*, розташовану в каталозі *C:\Program Files\Apache Software Foundation\[ Tomcat папка ]\webapps\*. Якщо ви зберігаєте додаткові дані в папці *era*, перед оновленням створіть їх резервну копію.
- Якщо *C:\Program Files\Apache Software Foundation\[ Tomcat папка ]\каталог webapps\* містить додаткові дані (крім даних у папках *era* і *ROOT*), оновиться лише веб-консоль, а Apache Tomcat – ні.
- Після оновлення Web Console і Apache Tomcat файли [автономної довідки](#) видаляються. Якщо ви використовували автономну довідку з ERA/ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 8.0. Це дозволить мати найновішу автономну довідку, що відповідає вашій версії ESET PROTECT.

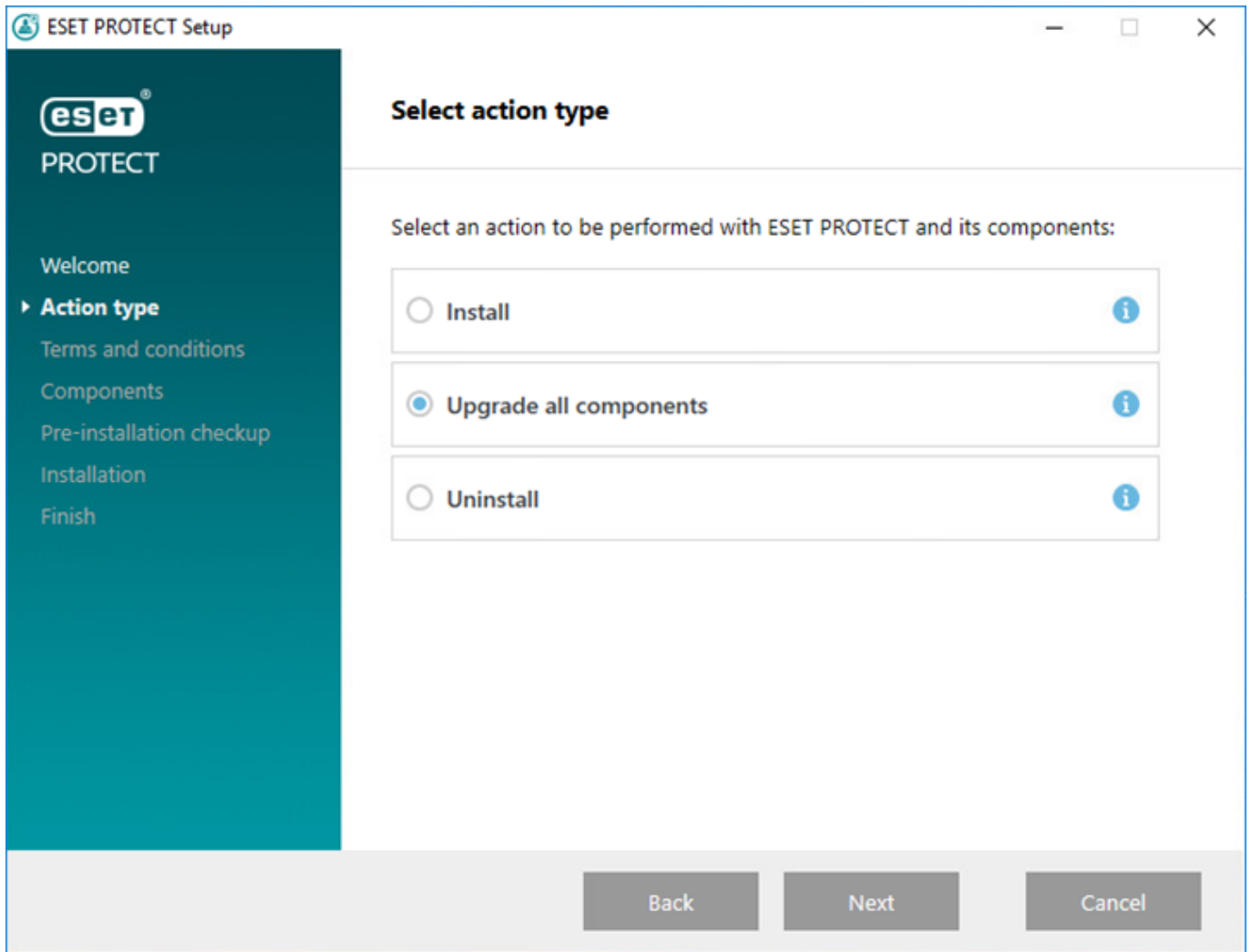
2. Завантажте [універсальний інстальатор ESET PROTECT](#) з веб-сайту ESET і розархівуйте завантажений файл.

3. Щоб встановити останню версію Apache Tomcat за умови, коли універсальний інстальатор містить старішу версію Apache Tomcat (цей крок не є обов'язковим; перейдіть до кроку 4, якщо вам не потрібна остання версія Apache Tomcat):

- Відкрийте папку *x64* і перейдіть у папку *installers*.
- Видаліть файл *apache-tomcat-9.0.x-windows-x64.zip*, розташований у папці *installers*.
- Завантажте ZIP-паquet 64-розрядної версії Apache Tomcat 9 [для Windows](#).
- Перемістіть завантажений ZIP-паquet у папку *installers*.

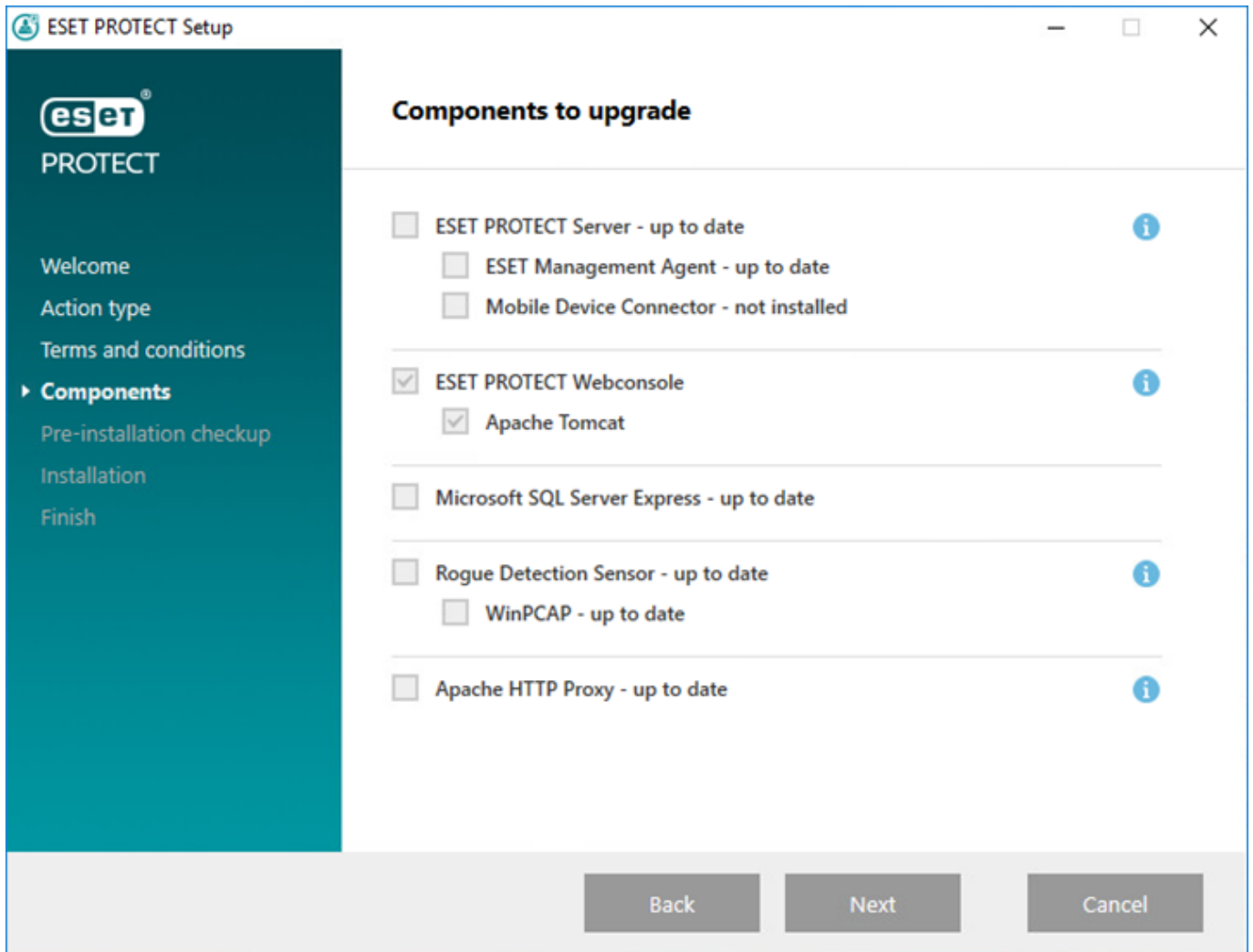
4. Щоб запустити універсальний інстальатор, двічі клацніть файл **Setup.exe** й натисніть клавішу **Далі** на екрані **привітання**.

5. Виберіть **Оновити всі компоненти** й натисніть **Далі**.



6. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

7. Універсальний інсталятор автоматично виявить, чи доступне оновлення: біля компонентів ESET PROTECT, які можна оновити, стоятиме прапорець. Натисніть кнопку **Далі**.



8. Виберіть інсталяцію Java на комп'ютері. Переконайтеся, що використовуєте останню версію Java/OpenJDK. Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.



#### Примітка

Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримування версія – Java 8) і залишити лише останню версію Java.



#### Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інсталювати один із підтримуваних випусків Java.

9. Натисніть **Оновити**, щоб виконати оновлення, а потім – **Готово**.

10. Якщо веб-консоль і сервер ESET PROTECT інстальовано на різних комп'ютерах, виконайте дії нижче.

а) Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.

б) Відновіть файл `EraWebServerConfig.properties` (з кроку 1) в оригінальному розташуванні.

в) Запустіть службу Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Запустити**.

11. [Підключіться до веб-консолі ESET PROTECT](#) і переконайтеся, що програма працює належним чином.



### Примітка

Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).

## Виправлення неполадок

Якщо Apache Tomcat не вдасться оновити, інстальуйте попередню версію та застосуйте конфігурацію з кроку 1.

## Оновлення Apache Tomcat вручну (Windows)

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT.



### Увага

Якщо інстальовано налаштовану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інстальатора або завдання «Оновлення компонентів» не підтримується.

Щоб оновити Apache Tomcat вручну (якщо у вас немає останньої версії універсального інстальатора ESET PROTECT), виконайте вказівки нижче.

### Перед оновленням

1. Переконайтеся, що використовуєте останню версію Java/OpenJDK. Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.



### Примітка

Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java (найстаріша підтримуванна версія – Java 8) і залишити лише останню версію Java.



### Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інсталювати один із підтримуваних випусків Java.

2. Перевірте, яка версія Apache Tomcat наразі доступна.

а. Перейдіть у папку інсталяції Apache Tomcat:

*C:\Program Files\Apache Software Foundation\[Tomcat папка ]\*

б. Відкрийте файл RELEASE-NOTES у текстовому редакторі та перевірте номер версії (наприклад, 7.0.90).

с. Якщо доступна новіша [підтримувана версія](#), виконайте оновлення.

### Інструкції з оновлення

1. Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск > Служби >** правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.

Закрийте файл Tomcat7w.exe, якщо його запущено в системному треї.

2. Створіть резервні копії цих файлів:

*C:\Program Files\Apache Software Foundation\[Tomcat папка ]\keystore*

*C:\Program Files\Apache Software Foundation\[Tomcat папка ]\conf\server.xml*

*C:\Program Files\Apache Software Foundation\[Tomcat папка ]\webapps\era\WEB-*

*INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

Якщо ви використовуєте налаштований сертифікат SSL, що зберігається в папці Tomcat, створіть його

резервну копію теж.

3. Видаліть поточну версію Apache Tomcat.
4. Видаліть указану нижче папку, якщо вона все ще є у вашій системі:

`C:\Program Files\Apache Software Foundation\[ Tomcat папка ]\`

5. Завантажте останню підтримувану версію файлу інстальатора Apache Tomcat (32-рядна або 64-розрядна версія інстальатора для Windows) `apache-tomcat-[версія].exe` із сайту <https://tomcat.apache.org>.

6. Інсталюйте нову завантажену версію Apache Tomcat.

- Якщо інсталювано кілька версій Java, під час інсталяції виберіть шлях до найновішої версії Java.
- Після завершення зніміть прапорець **Запустити Apache Tomcat**.

7. Відновіть `.keystore`, `server.xml` і налаштовувані сертифікати в оригінальному розташуванні.

8. Відкрийте файл `server.xml` і переконайтеся, що шлях `keystoreFile` указано правильно (оновіть шлях, якщо ви виконали оновлення до новішої основної версії Apache Tomcat):

```
keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat папка]\keystore"
```

9. Переконайтеся, що [підключення HTTPS для Apache Tomcat](#) для веб-консолі ESET PROTECT налаштовано належним чином.

10. Розгорніть веб-консоль ESET PROTECT (див. розділ [Інсталяція веб-консоли – Windows](#)).

11. Відновіть `EraWebServerConfig.properties` в оригінальному розташуванні.

12. Запустіть Apache Tomcat і задайте правильну віртуальну машину Java.

а) Перейдіть у папку `C:\Program Files\Apache Software Foundation\[ Tomcat папка ]\bin` і запустіть **Tomcat9w.exe**.

б) На вкладці **Загальне** виберіть для параметра **Тип запуску** значення **Автоматично** й натисніть **Запустити**.

в) Натисніть вкладку **Java**, переконайтеся, що прапорець **Використовувати значення за замовчуванням** не встановлено, а **віртуальна машина Java** містить шлях до файлу `jvm.dll` ([перегляньте ілюстровані вказівки в базі знань](#)), і натисніть **ОК**.

13. [Підключіться до веб-консоли ESET PROTECT](#) і переконайтеся, що програма працює належним чином.



#### Примітка

Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).

#### Виправлення неполадок

- Якщо вам не вдалося встановити підключення HTTPS для Apache Tomcat, пропустіть цей крок і тимчасово використовуйте підключення HTTP.
- Якщо Apache Tomcat не вдасться оновити, інсталюйте оригінальну версію та застосуйте конфігурацію з кроку 2.
- Після оновлення Web Console і Apache Tomcat файли [автономної довідки](#) видаляються. Якщо ви використовували автономну довідку з ERA/ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 8.0. Це дозволить мати найновішу автономну довідку, що відповідає вашій версії ESET PROTECT.

## Оновлення Apache Tomcat (Linux)

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT.

### Дії, які потрібно виконати перед оновленням Apache Tomcat

1. Переконайтеся, що Java у вашій системі оновлюється належним чином.
  - Переконайтеся, що пакет *openjdk* оновлено (див. нижче).
2. Перевірте, яка версія Apache Tomcat зараз використовується. Якщо доступна новіша версія, виконайте оновлення.
  - Виконайте цю команду: `cd /usr/share/tomcat/bin && ./version.sh` (у деяких випадках папка називається *tomcat7* або *tomcat8*).
3. Перегляньте перелік [підтримуваних версій Apache Tomcat](#), щоб переконатися, що нова версія сумісна з продуктами ESET.
4. Створіть резервну копію файлу конфігурації Tomcat */etc/tomcat7/server.xml*.

### Інструкції з оновлення

1. Зупинити роботу служби Apache Tomcat.
  - Виконайте цю команду: `service tomcat stop` (у деяких випадках служба називається *tomcat7*).
2. Оновіть Apache Tomcat і Java. Використовуйте команди терміналу залежно від дистрибутивів Linux. Наведені нижче приклади назв пакетів можуть відрізнятися від пакетів, доступних у репозиторії дистрибутива Linux.

|                                       |                                                                            |
|---------------------------------------|----------------------------------------------------------------------------|
| Дистрибутиви Debian і Ubuntu          | <pre>sudo apt-get update sudo apt-get install openjdk-11-jdk tomcat9</pre> |
| Дистрибутиви CentOS, Red Hat і Fedora | <pre>yum update yum install java-1.8.0-openjdk tomcat</pre>                |
| OpenSUSE                              | <pre>zypper refresh zypper install java-1_8_0-openjdk tomcat</pre>         |

3. Замініть файл */etc/tomcat9/server.xml* на файл *server.xml* з резервної копії.
4. Відкрийте файл *server.xml* і переконайтеся, що шлях *keystoreFile* вказано правильно.
5. Переконайтеся, що [підключення HTTPS для Apache Tomcat](#) налаштовано належним чином.



#### Примітка

Див. також тему [Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи](#).



#### Увага

Після оновлення Apache Tomcat до останньої основної версії (наприклад, з версії 7.x до 9.x):

- розгорніть веб-консоль ESET PROTECT ще раз (див. розділ [Інсталяція веб-консолі ESET PROTECT – Linux](#));
- повторно використайте `%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`, щоб зберегти налаштовані параметри у веб-консолі ESET PROTECT.
- Після оновлення Web Console і Apache Tomcat файли [автономної довідки](#) видаляються. Якщо ви використовували автономну довідку з ERA/ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 8.0. Це дозволить мати найновішу автономну довідку, що відповідає вашій версії ESET PROTECT.

## Змінення IP-адреси чи імені хоста сервера ESET PROTECT після перенесення

Щоб змінити IP-адресу чи ім'я хоста сервера ESET PROTECT, виконайте наступні кроки.

1. Якщо ваш сертифікат сервера ESET PROTECT вже містить певну IP-адресу й/або ім'я хоста, [створіть новий сертифікат сервера](#) та вкажіть у ньому нову IP-адресу або ім'я хоста. Однак, якщо в полі «Хост» сертифіката сервера використовується символ узагальнення (\*), **перейдіть до кроку 2**. Якщо такого символу немає ні, створіть новий сертифікат сервера, додайте до нього нову IP-адресу й ім'я хоста через кому, а також укажіть попередню IP-адресу та ім'я хоста.
2. Підпишіть новий сертифікат сервера за допомогою Центру сертифікації сервера ESET PROTECT.
3. Створіть політику для змінення параметрів підключення клієнта на нову IP-адресу або ім'я хоста (бажано використовувати IP-адресу) і додайте до неї стару IP-адресу чи ім'я хоста, щоб агент ESET Management міг підключатися до обох серверів. Детальніше див. у розділі [Створення політики для агентів ESET Management для підключення до нового сервера ESET PROTECT](#).
4. Застосуйте цю політику на клієнтських комп'ютерах і дозвольте агентам ESET Management виконати реплікацію. Хоча політика перенаправляє клієнтів на новий сервер (який ще не працює), агенти ESET Management використовуватимуть альтернативні дані сервера для підключення до вихідної IP-адреси.
5. Перегляньте [новий сертифікат сервера в його налаштуваннях](#).
6. Перезапустіть службу сервера ESET PROTECT та змініть IP-адресу або ім'я хоста.

Див. графічні вказівки щодо змінення адреси сервера ESET PROTECT в статті [бази знань](#).

## Оновлення рішення ERA/ESMC, інстальованого у відмовостійкому кластері в Linux

Якщо сервер ESET PROTECT інстальовано в [середовищі відмовостійкого кластера в Linux](#) і потрібно оновити інсталяцію, виконайте дії нижче.

### [Оновлюєте середовище за допомогою проксі-сервера ERA?](#)

#### **Оновлення з ERA 6.5 (або новішої версії) до останньої версії ESET PROTECT вручну**

1. Вимкніть службу *EraService* у Conga (графічний інтерфейс адміністрування кластера) у розділі **Групи служб** і зупиніть роботу агента ERA та сервера ERA на обох вузлах.
2. Оновіть сервер ERA на вузлі node1, виконавши дії нижче.
  - a. Підключіть спільне сховище до цього вузла.
  - b. Оновіть сервер ERA вручну до останньої версії. Для цього виконайте сценарій інсталяції сервера `server-linux-x86_64.sh` з правами `root` або `sudo`.
  - c. Замініть старий кластер, розташований у каталозі `/usr/share/cluster/eracluster_server.sh`, на новий із каталогу `/opt/eset/RemoteAdministrator/Server/setup/eracluster_server`. Не змінюйте ім'я файлу `eracluster_server.sh`.
  - d. Після оновлення зупиніть службу сервера ESET PROTECT (`stop eraserver`).
  - e. Вимкніть автозапуск сервера ESET PROTECT, змінивши імена цих двох файлів:

```
i.mv /etc/init/eraserver.conf /etc/init/eraserver.conf.disabled
ii.mv /etc/init/eraserver-xvfb.conf /etc/init/eraserver-xvfb.conf.disabled
```
  - f. Відключіть спільне сховище від цього вузла.
3. Повторіть ці дії, щоб оновити сервера ERA на вузлі node2.
4. Запустіть службу *EraService* у Conga (графічний інтерфейс адміністрування кластера) у розділі «Групи служб».
5. Оновіть **агент ERA** на всіх вузлах кластера.
6. Перевірте у веб-консолі ESET PROTECT, чи всі вузли підключаються й відображаються як остання версія.

# Видалення сервера ESET PROTECT і його компонентів

Щоб видалити сервер ESET PROTECT, виберіть один із вказаних нижче розділів.

- [Windows - Видалення сервера ESET PROTECT і його компонентів](#)
- [Linux – Оновлення, повторна інсталяція або видалення компонентів ESET PROTECT](#)
- [macOS: видалення ESET Management Agent і продукту ESET Endpoint](#)
- [Видалення старого сервера ERA/ESMC/ESET PROTECT/MDM після перенесення на новий сервер](#)

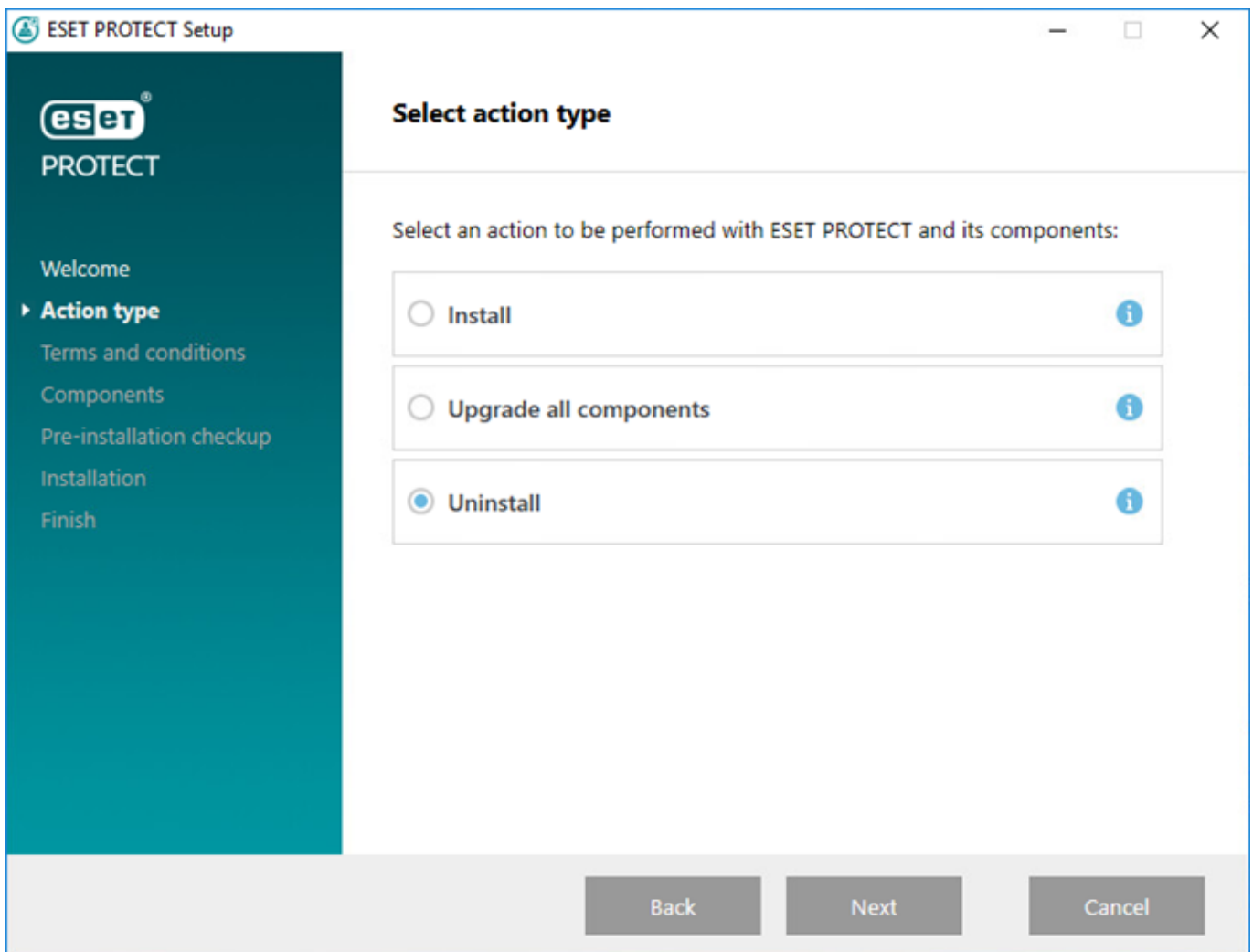
Windows - Видалення сервера ESET PROTECT і його компонентів

Щоб видалити компоненти ESET PROTECT, запустіть [універсальний інсталятор ESET PROTECT](#) і виберіть **Видалити**. Перш ніж продовжити, ви також можете вибрати **мову** в розкритому меню.



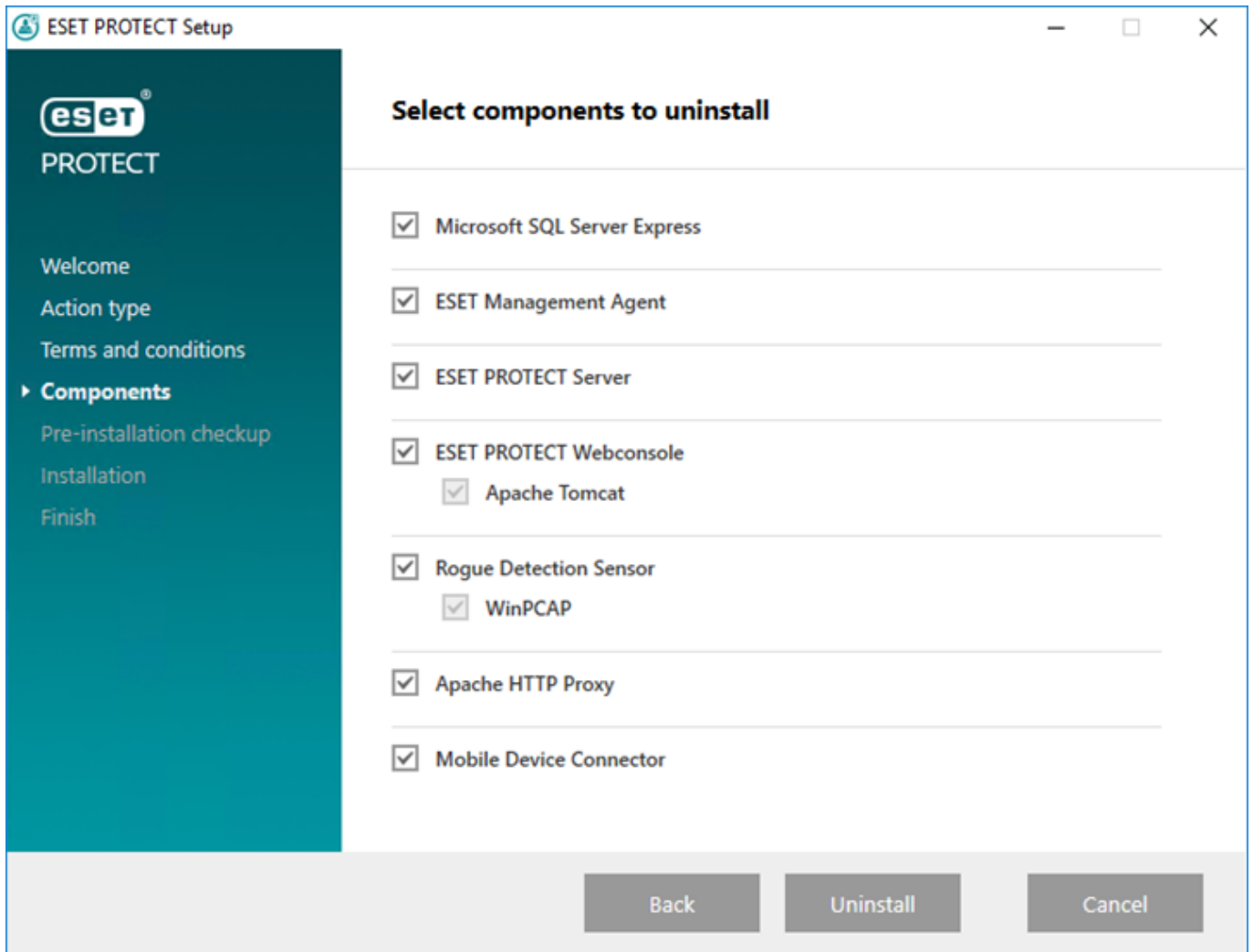
## Примітка

Перед видаленням Mobile Device Connector перегляньте розділ [Ліцензування iOS в MDM](#).



Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**. Виберіть компоненти, які потрібно видалити, і натисніть **Далі**.





### Примітка

- Щоб завершити видалення певних компонентів, можливо, знадобиться перезавантажити комп'ютер.
- Перегляньте також розділ [Видалення старого сервера ERA/ESMC/ESET PROTECT/MDM після перенесення на новий сервер](#).

## Linux – Оновлення, повторна інсталяція або видалення компонентів ESET PROTECT

Якщо потрібно повторно інсталювати або оновити компонент до останньої версії, виконайте сценарій інсталяції ще раз.

Щоб видалити компонент (у цьому випадку сервер ESET PROTECT), запустіть інсталятор із параметром `--uninstall`, як показано нижче.

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Щоб видалити інший компонент, укажіть у команді назву відповідного пакета. Наприклад, для агента ESET Management:

```
sudo ./agent-linux-x86_64.sh --uninstall
```



### Увага

Під час видалення буде видалено файли конфігурації та бази даних. Щоб зберегти файли бази даних, створіть дамп SQL бази даних або скористайтеся параметром `--keep-database`.

Після видалення перевірте, чи:

- видалена служба `eraserver`;
- видалена папка `/etc/opt/eset/RemoteAdministrator/Server/`.



### Примітка

Перш виконувати видалення, рекомендуємо створити резервну копію дампу бази даних на випадок, якщо потрібно відновити дані.

Щоб дізнатися більше про видалення агента, перегляньте відповідний [розділ](#).

macOS: видалення ESET Management Agent і продукту ESET Endpoint

Видаліть ESET Management Agent і продукт ESET Endpoint локально або віддалено за допомогою ESET PROTECT.



### Примітка

- Якщо потрібно видалити продукт ESET Endpoint віддалено, зробіть це до видалення ESET Management Agent.
- Більш докладні інструкції щодо локального видалення ESET Management Agent і продукту ESET Endpoint див. в [цій статті нашої бази знань](#).

## Локальне видалення ESET Management Agent

1. Клацніть **Finder**, щоб відкрити нове вікно **Finder**.
2. Клацніть **Програми** > утримуйте клавішу **CTRL** > клацніть **ESET Management Agent** > у контекстному меню виберіть пункт **Show Package Contents** (Показати вміст пакета).
3. Виберіть **Зміст** > **Сценарії** й двічі клацніть **Uninstaller.command**, щоб запустити інсталятор.
4. Після появи запиту на введення пароля введіть пароль адміністратора й натисніть клавішу **Enter**.
5. Після видалення ESET Management Agent з'явиться повідомлення **Process completed** (Процес завершено).

## Локальне видалення ESET Management Agent у Terminal

1. Відкрийте **Finder** > **Програми** > **Утиліти** > **Terminal**.
2. Уведіть указану нижче команду й натисніть клавішу **Enter**:  

```
sudo /Applications/ESET\ Administrator\ Agent.app/Contents/Scripts/Uninstall.command ; exit;
```
3. Після появи запиту на введення пароля введіть пароль адміністратора й натисніть клавішу **Enter**.
4. Після видалення ESET Management Agent з'явиться повідомлення **Process completed** (Процес завершено).

## Віддалене видалення ESET Management Agent за допомогою ESET PROTECT

У розділі **Комп'ютери** клацніть клієнтський комп'ютер macOS і виберіть [Видалити](#), щоб видалити ESET Management Agent і скасувати керування комп'ютером.

## Локальне видалення продукту ESET Endpoint

1. Клацніть **Finder**, щоб відкрити нове вікно **Finder**.
2. Клацніть **Програми** > утримуйте клавішу **CTRL** > клацніть **ESET Endpoint Security** або **ESET Endpoint Antivirus** > у контекстному меню виберіть пункт **Show Package Contents** (Показати вміст

пакета).

3. Виберіть **Зміст > Helpers** (Помічники) й двічі клацніть **Uninstaller.app**, щоб запустити програму видалення.
4. Клацніть **Видалити**.
5. Після появи запиту на введення пароля введіть пароль адміністратора й клацніть **OK**.
6. Після видалення ESET Endpoint Security або ESET Endpoint Antivirus з'явиться повідомлення **Uninstall Succeeded** (Успішно видалено). Клацніть **Закрити**.

### Локальне видалення продукту ESET Endpoint у Terminal

1. Відкрийте **Finder > Програми > Утиліти > Terminal**.
2. Уведіть указану нижче команду й натисніть клавішу **Enter**:  

```
sudo /Applications/ESET\ Endpoint\
Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
sudo /Applications/ESET\ Endpoint\
Security.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```
3. Після появи запиту на введення пароля введіть пароль адміністратора й натисніть клавішу **Enter**.
4. Після видалення продукту ESET Endpoint з'явиться повідомлення **Process completed** (Процес завершено).

### Віддалене видалення продукту ESET Endpoint за допомогою ESET PROTECT

Для віддаленого видалення ESET Management Agent за допомогою ESET PROTECT можна використовувати один із таких параметрів:

- У розділі **Комп'ютери** клацніть клієнтський комп'ютер macOS, виберіть **Показати подробиці > Інсталювані програми** > виберіть **ESET Endpoint Security** або **ESET Endpoint Antivirus** і натисніть кнопку **Видалити**.
- За допомогою завдання [Видалення програми](#) .

Видалення старого сервера ERA/ESMC/ESET PROTECT/MDM після перенесення на новий сервер



#### Попередження

Переконайтеся, що новий сервер ESET PROTECT/MDM працює, а клієнтські комп'ютери та мобільні пристрої підключено до нового сервера ESET PROTECT належним чином.

Є кілька варіантів видалення старого сервера ERA/ESMC/ESET PROTECT/MDM після перенесення на новий.

### I.Зберегти ОС серверного комп'ютера й повторно використати її

1. [Зупиніть службу сервера ERA/ESMC](#).
2. Видаліть (DROP DATABASE) старий екземпляр бази даних ERA/ESMC/ESET PROTECT Server (MS SQL або MySQL).



#### Попередження

Якщо ви перенесли базу даних на новий ESET PROTECT, перед її видаленням переконайтеся, що видалили її зі старого ERA/ESMC/ESET PROTECT Server. Це потрібно, щоб ліцензії не було від'єднано від (видалено з) нової бази даних ESET PROTECT Server.

3. Видаліть старий сервер ERA/ESMC/ESET PROTECT/MDM і всі його компоненти (зокрема, агент ESET Management, Rogue Detection Sensor, MDM тощо).

[ОВидалити ERA 6.5 - Windows](#)

[ОВидалити ESMC 7.x - Windows](#)

[ОВидалити ESET PROTECT 8.x - Windows](#)

[ОВидалити ESET PROTECT - Linux](#)



### Увага

Не видаляйте базу даних, якщо є програмне забезпечення, яке залежить від неї.

4. Після видалення перезавантажте операційну систему сервера.

## II.Зберегти ОС серверного комп'ютера

Найпростіший спосіб видалити ERA/ESMC/ESET PROTECT/MDM — відформатувати диск, на якому встановлено цей продукт.



### Попередження

Ця процедура видалить увесь вміст диску, зокрема ОС.

## Виправлення неполадок

Оскільки ESET PROTECT є складним продуктом, який використовує кілька сторонніх інструментів і підтримує багато платформ ОС, є імовірність, що під час його використання виникатимуть неполадки, які потребуватимуть виправлення.

У документації ESET наведено кілька способів виправлення неполадок в ESET PROTECT. Перегляньте розділ [Рішення поширених проблем під час інсталяції](#), щоб вирішити поширені проблеми ESET PROTECT.

### Не вдалося виправити неполадку?

- У кожного компонента ESET PROTECT є [файл журналу](#), який залежно від налаштувань може бути більш або менш детальним. Переглядайте журнали, щоб визначити, які помилки є причиною неполадки.

Одетальність журналу кожного компонента задається в його [політиці](#). Щоб політика набрала чинності, її потрібно застосувати на пристрої.

- [Політика агента ESET Management](#)
- [RD Sensor](#)
- [Сервер ESET PROTECT](#)
- MDM Core



### Примітка

Щоб увімкнути повне ведення журналу, створіть порожній файл із назвою *traceAll* без розширення в тій самій папці, у якій розташовано файл *trace.log*, і перезавантажте службу агента ESET Management. Після цього увімкнеться повне ведення журналу у файлі *trace.log*.

- Якщо вам не вдається виправити неполадку, відвідайте [форум безпеки ESET](#) і зверніться до спільноти ESET, щоб отримати інформацію про можливі проблеми.
- Коли ви звертаєтесь у [службу технічної підтримки ESET](#), спеціалісти служби можуть попросити вас зібрати необхідні файли журналів. Для цього скористайтесь [ESET Log Collector](#) або нашим [інструментом діагностики](#). Рекомендуємо додавати журнали, коли звертаєтесь у службу технічної підтримки. Так ви пришвидшите виконання свого запиту.

### Оновлення компонентів ESET PROTECT в автономному середовищі

Щоб оновити компоненти ESET PROTECT і продукти ESET Endpoint без доступу до Інтернету, виконайте вказівки нижче.



### Увага

[Завдання оновлення компонентів](#) можна використовувати для автономного середовища, якщо:

- доступний [автономний репозиторій](#);
- розташування репозиторію для агента ESET Management в доступному місці налаштовано за допомогою [політики](#).

1. Спершу оновіть сервер і веб-консоль ESET PROTECT.

- а. [Перевірте, яка версія ESET PROTECT](#) працює на сервері.
- б. Перевірте наявність [останніх версій компонентів](#).
- в. Завантажте найновіші автономні інсталятори із [сайту завантаження ESET](#).
- г. [Виконайте оновлення по компонентам](#) сервера ESET PROTECT і веб-консолі ESET PROTECT вручну.



### Примітка

Після оновлення Web Console і Apache Tomcat файли [автономної довідки](#) видаляються. Якщо ви використовували автономну довідку з ERA/ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 8.0. Це дозволить мати найновішу автономну довідку, що відповідає вашій версії ESET PROTECT.

2. Продовжуйте автономне оновлення продуктів ESET Endpoint.

- а. Перегляньте, які продукти ESET інстальовано на клієнтах. Відкрийте веб-консоль ESET PROTECT і перейдіть у меню **Панель інструментів > Програми ESET**.
- б. Перевірте наявність [останніх версій продуктів ESET Endpoint](#).
- в. Завантажте інсталятори із [сайту завантаження ESET](#) у локальний репозиторій, налаштований під час [інсталяції в автономному режимі](#).
- г. Запустіть [завдання інсталяції програми](#) з веб-консолі ESET PROTECT.

Рішення поширених проблем під час інсталяції

Розгорніть повідомлення про помилку, яке ви хочете вирішити:

 [Сервер ESET PROTECT](#)

Служба сервера ESET PROTECT не запускається:

#### **Пошкоджений інстальатор**

- Можливі причини: відсутні ключі реєстру або файли, недійсні дозволи на доступ до файлів.
- Універсальний інстальатор ESET веде власний [журнал](#). У разі ручної інсталяції компонентів використовуйте спосіб [Ведення журналів MSI](#).

#### **Порт прослуховування вже використовується (найчастіше 2222 або 2223)**

Використовуйте відповідні до своєї ОС команди:

- Windows:

```
netstat -an | find "2222"
```

```
netstat -an | find "2223"
```

• Linux:

```
netstat | grep 2222
```

```
netstat | grep 2223
```

**База даних не працює/неможливо отримати доступ до бази даних**

- MS SQL Server: Переконайтеся, що порт 1433 на сервері бази даних приймає та передає дані або увійдіть у систему за допомогою SQL Server Management Studio.
- MySQL: Переконайтеся, що порт 3306 на сервері бази даних приймає та передає дані або увійдіть в інтерфейс бази даних (наприклад, за допомогою інтерфейсу командного рядка MySQL чи phpmyadmin).

#### **Пошкоджена база даних**

У файлі журналу сервера ESET PROTECT відобразатимуться кілька помилок SQL. Рекомендується відновити базу даних із резервної копії. Якщо резервної копії немає, інсталюйте ESET PROTECT повторно.

#### **Недостатньо системних ресурсів (оперативної пам'яті, місця на диску)**

Перегляньте запущені процеси та продуктивність системи:

- Користувачі Windows: Запустіть диспетчер завдань або засіб перегляду подій і перегляньте інформацію в ньому

- Користувачі Linux: Виконайте одну з таких команд:

```
df -h (для перегляду інформації про місце на диску)
```

```
cat /proc/meminfo (для перегляду інформації про місце в пам'яті)
```

```
dmesg (для перегляду стану системи Linux)
```

#### **Помилка з'єднувача ODBC під час інсталяції сервера ESET PROTECT**

```
Error: (Error 65533) ODBC connector compatibility check failed.
```

```
Please install ODBC driver with support for multi-threading.
```

Інсталюйте версію драйвера ODBC, що підтримує багатопотоковість, або переналаштуйте `odbcinst.ini` згідно з розділом [Налаштування ODBC](#).

#### **Помилка підключення до бази даних під час інсталяції сервера ESET PROTECT**

Інсталяція сервера ESET PROTECT переривається, після чого відображається повідомлення про помилку:

```
The database server is not configured correctly.
```

```
Please check the documentation and reconfigure the database server as needed.
```

Повідомлення про помилку з журналу інсталяції:

```
Error: Execution test of long statement failed with exception:
```

```
CMysqlCodeTokenExecutor: CheckVariableInnoDBLogFileSize:
```

```
Server variables innodb_log_file_size*innodb_log_files_in_group
```

```
value 100663296 is too low.
```

Переконайтеся, що конфігурація драйвера бази даних відповідає вказаній у розділі [Налаштування ODBC](#).

☐ [Агент ESET Management](#)

**Під час видалення агента відображається повідомлення «Не вдається оновити базу даних. Спочатку видаліть продукт».**

Виправлення агента ESET Management:

1. Виберіть **Панель управління > Програми та функції** та двічі натисніть **агент ESET Management**.
2. Виберіть **Далі > Виправлення** та дотримуйтесь інструкцій, що відобразяться.

**Чи існують інші способи видалення агента ESET Management?**

Усі можливі способи видалення агента ESET Management описано в розділі [Видалення](#).

**Під час інсталяції агента відображається код помилки 1603**

Ця помилка може статися, якщо файли інсталятора не знаходяться на локальному диску. Щоб виправити її, скопіюйте файли інсталятора в локальну папку та запустіть інсталяцію ще раз. Якщо файли вже перенесено в локальну папку або помилка виникає знову, див. [Інструкції з бази знань](#).

**Під час інсталяції агента в ОС Linux відображається повідомлення про помилку**

Повідомлення про помилку:

```
Checking certificate ... failed
```

```
Error checking peer certificate: NOT_REGULAR_FILE
```

Можлива причина цієї помилки – неправильне ім'я файлу в команді інсталяції. Консоль працює з урахуванням реєстру. Наприклад, `Agent.pfx` відрізняється від `agent.pfx`.

**Збій віддаленого розгортання з Linux на Windows 8.1 (32bit)**

Це помилка автентифікації, викликана оновленням KB3161949 від Microsoft. Щоб її вирішити, потрібно видалити це оновлення з хостів, на яких неможливо виконати розгортання.

## **Агент ESET Management не може підключитися до ESET PROTECT Сервер**

Перегляньте [статтю бази знань](#).

**Агент Live Installer припинив роботу та відобразив код 30**

Ви використовуєте сценарій Live Installer зі спеціальним місцем інсталяції та неправильно відредагували сценарій. Перегляньте [довідку](#) та спробуйте ще раз.

### [Web Console](#)

#### [Проксі-сервер Apache HTTP](#)

**Розмір кешу проксі-сервера Apache HTTP становить кілька гігабайт і продовжує зростати**

Якщо ви інсталиювали проксі-сервер Apache HTTP за допомогою універсального інсталятора, очищення вмикається автоматично. Якщо воно не працює належним чином, [виконайте очищення вручну або заплануйте відповідне завдання](#).

**Оновлення ядра виявлення не працюють після інсталяції проксі-сервера Apache HTTP**

Якщо робочі станції клієнта не оновлюються, перегляньте інструкції з бази знань щодо тимчасового [вимкнення проксі-сервера Apache HTTP на робочих станціях](#). Після усунення проблем із підключенням можна знову ввімкнути проксі-сервер Apache HTTP.

**Збій віддаленого оновлення Агента ESET Management, код помилки 20008**

У разі збою віддаленого оновлення Агента ESET Management відображається наступне повідомлення:  
*GetFile: Failed to process the HTTP request (error code 20008, url: 'http://repository.eset.com/v1//info.meta')*

[Виконайте кроки 1-3 з цієї статті](#) для усунення проблеми з підключенням. Якщо комп'ютер, на якому оновлюється Агент ESET Management, не входить до вашої корпоративної мережі, налаштуйте політику, що забороняє Агенту ESET Management використовувати проксі-сервер для підключення до репозиторію за межами корпоративної мережі.

#### [ESET Rogue Detection Sensor](#)

### Чому таке повідомлення про помилку постійно вноситься до файлу trace.log ESET Rogue Detector?

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} threw error:
Device open failed with error:Error opening adapter:

The system cannot find the device specified. (20)
```

Це проблема з WinPcap. Вимкніть службу ESET Rogue Detector Sensor, повторно інсталюйте останню версію WinPcap (принаймні 4.1.0) і знову ввімкніть службу ESET Rogue Detector Sensor.

#### Linux

### Відсутня залежність libQtWebKit у CentOS Linux

```
Якщо відображається така помилка:
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

Дотримуйтесь інструкцій зі [статті бази знань](#).

### Збій інсталяції сервера ESET PROTECT на CentOS 7

```
Якщо відображається така помилка:
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

Можливо, ця проблема викликана налаштуваннями середовища/локальної мережі. Запустіть наступну команду перед виконанням скрипта інсталюатора сервера:  
export LC\_ALL="en\_US.UTF-8"

#### Microsoft SQL Server

### Під час інсталяції Microsoft SQL Server відображається код помилки 2068052081.

Перезавантажте комп'ютер і запустіть інсталяцію ще раз. Якщо проблема не зникне, видаліть Native Client SQL Server та запустіть інсталяцію ще раз. Якщо проблема все одно залишилася, видаліть усі продукти Microsoft SQL Server, перезавантажте комп'ютер і запустіть інсталяцію ще раз.

### Під час інсталяції Microsoft SQL Server відображається код помилки 2067922943.

Переконайтеся, що ваша система відповідає [вимогам до бази даних](#) ESET PROTECT.

### Під час інсталяції Microsoft SQL Server відображається код помилки 2067922934.

Переконайтеся, що у вас є відповідні [права користувача](#).

### На веб-консолі відображається повідомлення «Не вдалося завантажити дані».

MS SQL Server намагається використовувати весь дисковий простір для збереження журналів транзакцій.

Щоб виправити цю проблему, [відвідайте офіційний веб-сайт Microsoft](#).

### Під час інсталяції Microsoft SQL Server відображається код помилки 2067919934.

Переконайтеся, що всі попередні кроки виконано успішно. Ця помилка викликана неправильним налаштуванням системних файлів. Перезавантажте комп'ютер і запустіть інсталяцію ще раз.

#### Файли журналу

Кожен компонент ESET PROTECT виконує реєстрацію в журналах. Компоненти ESET PROTECT записують інформацію про певні події у файли журналів. Розташування файлів журналу різне для кожного компонента. Нижче наведено перелік розташувань файлів журналів.

#### Windows

|                                          |                                                                                                                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Сервер ESET PROTECT                      | C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\                                                                                                                         |
| Агент ESET Management                    | C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\<br>Див. також <a href="#">Виправлення неполадок із підключенням агента</a> .                                              |
| ESET PROTECT Web Console і Apache Tomcat | C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\<br>Див. також сторінку <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a> |
| Mobile Device Connector                  | C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs\                                                                                                                                                 |



|                                         |                                                                                              |
|-----------------------------------------|----------------------------------------------------------------------------------------------|
| Rogue Detection Sensor                  | C:\ProgramData\ESET\Rogue Detection Sensor\Logs\                                             |
| Проксі-сервер Apache HTTP               | C:\Program Files\Apache HTTP Proxy\logs\<br>C:\Program Files\Apache HTTP Proxy\logs\errorlog |
| У старіших операційних системах Windows | C:\Documents and Settings\All Users\Application Data\ESET\...                                |



### Примітка

Папку C:\ProgramData приховано за замовчуванням.  Щоб відобразити її, виконайте [вказані нижче дії](#).

1. Перейдіть у меню **Пуск > Панель управління > Параметри папки > Вигляд**.
2. Виберіть параметр **Відображати приховані файли, папки й диски** та натисніть **ОК**.

## Linux

|                                          |                                                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Сервер ESET PROTECT                      | /var/log/eset/RemoteAdministrator/Server/<br>/var/log/eset/RemoteAdministrator/EraServerInstaller.log                                                             |
| Агент ESET Management                    | /var/log/eset/RemoteAdministrator/Agent/<br>/var/log/eset/RemoteAdministrator/EraAgentInstaller.log                                                               |
| Mobile Device Connector                  | /var/log/eset/RemoteAdministrator/MDMCore/<br>/var/log/eset/RemoteAdministrator/MDMCore/Proxy/                                                                    |
| Проксі-сервер Apache HTTP                | /var/log/httpd/                                                                                                                                                   |
| ESET PROTECT Web Console і Apache Tomcat | /var/log/tomcat/<br>Див. також сторінку <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a> |
| ESET RD Sensor                           | /var/log/eset/RogueDetectionSensor/                                                                                                                               |

### ESET PROTECT Віртуальний пристрій

|                                                 |                                                          |
|-------------------------------------------------|----------------------------------------------------------|
| Конфігурація віртуального пристрою ESET PROTECT | /root/appliance-configuration-log.txt                    |
| Сервер ESET PROTECT                             | /var/log/eset/RemoteAdministrator/EraServerInstaller.log |
| Проксі-сервер Apache HTTP                       | /var/log/httpd                                           |

## macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

### Інструмент діагностики

Інструмент діагностики входить до складу всіх компонентів ESET PROTECT. Він використовується для збору й пакування журналів, які співробітники служби технічної підтримки та розробники можуть використовувати для вирішення проблем із компонентами продуктів.

### Місце знаходження інструменту діагностики

#### Windows

Папка C:\Program Files\ESET\RemoteAdministrator\*<product>*\Diagnostic.exe.

#### Linux

У наступній папці на сервері: /opt/eset/RemoteAdministrator/*<product>*/ міститься виконуваний файл **Diagnostics<product>** (наприклад, **DiagnosticsServer** або **DiagnosticsAgent**)

### Використання (Linux)

Запустіть виконуваний файл інструменту діагностики в терміналі від імені кореневого користувача та дотримуйтесь інструкцій, що відобразяться на екрані.

### Використання (Windows)

1. Запустіть інструмент за допомогою командного рядка.

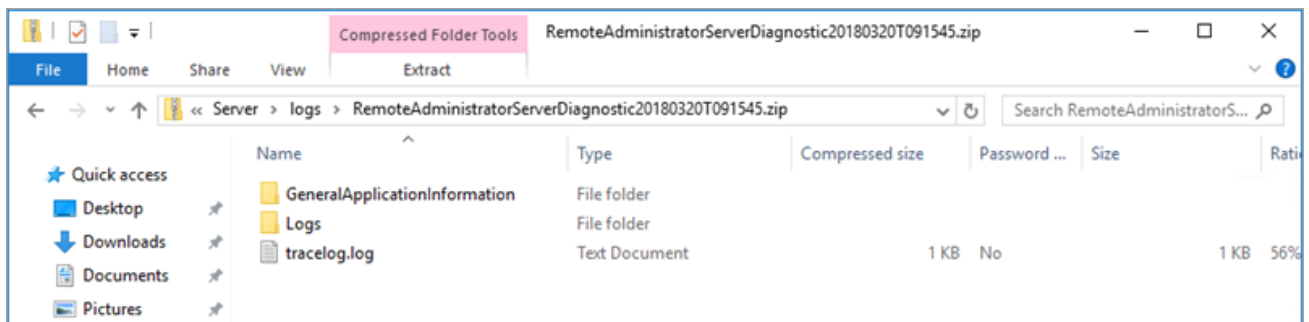
2. Введіть шлях, за яким слід зберегти файли журналу (наприклад, «logs») і натисніть **Enter**.
3. Введіть інформацію, яку необхідно зібрати (наприклад, 1 trace status 3). Більш докладну інформацію див. у розділі **Дії**.

```

Administrator: Command Prompt
C:\Program Files\ESET\RemoteAdministrator\Server>Diagnostic.exe
Starting diagnostics for product type: Server
Provide path to folder, where ZIP file will be stored: logs
Actions:
1. ActionEraLogs. Get product logs. Specific log can be selected with options: trace,status,last-error,avremo
ver,software-install,software-uninstall,ra-upgrade-agent,ra-upgrade-infrastructure,ra-agent-uninstall.
2. ActionGetDumps. Dump process and get already created dumps.
3. ActionGeneralApplicationInformation. Get general application information.
4. ActionConfiguration. Get configuration.
Provide actions (numbers) and options (specified in actions) separated by spaces (example: 1 trace status 3):
1 trace status 3
Executing all actions.
Action: ActionEraLogs started.
Action: ActionEraLogs successfully finished.
Action: ActionGeneralApplicationInformation started.
Action: ActionGeneralApplicationInformation successfully finished.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation started.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation finished.
C:\Program Files\ESET\RemoteAdministrator\Server>_

```

4. Після закінчення файли журналу буде збережено у файлі формату *zip* у папці «**logs**» каталогу з інструментом діагностики.



## Дії

- **ActionEraLogs** – створюється папка, у яку зберігаються всі журнали. Щоб вибрати лише певні журнали, використовуйте пробіл для розділення.
- **ActionGetDumps** – створюється нова папка. Файл дампа процесу, як правило, створюється в разі виявлення проблеми. За наявності серйозної проблеми система генерує файл дампа. Щоб вручну переглянути його, перейдіть до папки %temp% (у Windows) або /tmp/ (у Linux) і вставте файл формату dmp.

**Примітка**  
Необхідно запуснути службу компонента (Agent, Server, RD Sensor).

- **ActionGeneralApplicationInformation** – Створюється папка GeneralApplicationInformation із файлом GeneralApplicationInformation.txt. У цьому файлі міститься певна текстова інформація, зокрема назва та версія інсталюваного продукту.
- **ActionConfiguration** – створюється папка конфігурації, у якій зберігається файл storage.lua.

## Проблеми після оновлення або перенесення сервера ESET PROTECT

Якщо вам не вдається запустити службу ESET PROTECT через пошкодження інстальованого продукту або невідомі помилки, зареєстровані у файлі журналу, виконайте операцію відновлення за допомогою вказаних нижче дій.



### Попередження

Перш ніж почати відновлення, рекомендуємо [створити резервну копію сервера бази даних](#).

1. Перейдіть у меню **Пуск > Панель управління > Програми та функції** й двічі натисніть **сервер ESET PROTECT**.
2. Виберіть **Відновити** й натисніть **Далі**.
3. Повторно скористайтеся наявними параметрами підключення до бази даних і натисніть **Далі**. Натисніть **Так**, якщо з'явиться запит на підтвердження.
4. Виберіть **Використовувати пароль адміністратора, який уже зберігається в базі даних** і натисніть **Далі**.
5. Виберіть **Зберегти наявні сертифікати** та натисніть **Далі**.
6. Натисніть **Відновити**.
7. [Підключіться до веб-консолі](#) ще раз і перевірте, чи все працює.

Інші сценарії виправлення неполадок

### Сервер ESET PROTECT не працює, але є резервна копія бази даних:

1. Відновіть [резервну копію бази даних](#).
2. Щоб агенти підключилися, переконайтеся, що новий комп'ютер використовує таку саму IP-адресу й ім'я хоста, що й раніше інстальований продукт.
3. Відновіть ESET Security Management Server та скористайтеся відновленою базою даних.

### Сервер ESET PROTECT не працює, але у вас є експортований із нього сертифікат сервера та Центр сертифікації:

1. Щоб агенти підключилися, переконайтеся, що новий комп'ютер використовує таку саму IP-адресу й ім'я хоста, що й раніше інстальований продукт.
2. Відновіть ESET Security Management Server за допомогою резервних копій сертифікатів (під час відновлення виберіть **Завантажити сертифікати з файлу** та дотримуйтеся вказівок).

### Сервер ESET PROTECT не працює й у вас немає резервної копії бази даних чи експортованого з нього сертифіката або Центру сертифікації сервера ESET PROTECT:

1. Відновіть ESET Security Management Server.
2. Відновіть агенти ESET Management за допомогою одного з указаних нижче способів.

- Агент Live Installer
- Віддалене розгортання (потрібно буде вимкнути брандмауер на цільових комп'ютерах)
- Інсталятор компонентів агента для ручної інсталяції

### Ведення журналів MSI

Це корисно, якщо вам не вдається належним чином інсталювати компонент ESET PROTECT у Windows (наприклад, агент ESET Management):

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

# API ESET PROTECT

ServerApi ESET PROTECT (ServerApi.dll) – це прикладний програмний інтерфейс, що складається з набору функцій та інструментів для створення необхідних спеціальних програм. Завдяки ServerApi ви можете додати у свою програму користувальницький інтерфейс, а також використовувати такі функції та виконувати такі операції, для яких зазвичай потрібна веб-консоль ESET PROTECT. Наприклад, ви можете керувати ESET PROTECT, генерувати й отримувати звіти тощо.

Щоб отримати додаткову інформацію й переглянути приклади коду мовою програмування C та список доступних повідомлень JSON, скористайтесь онлайн-довідкою:

[API ESET PROTECT8](#)

## Питання й відповіді

**Чому ми встановлюємо Java на сервер? Чи не створює це ризики? Більшість усіх компаній, що надають послуги захисту, і систем безпеки рекомендують видаляти Java з комп'ютерів, особливо із серверів.**

Для роботи веб-консолі ESET PROTECT потрібний Java/OpenJDK. Java – це галузевий стандарт для веб-консолей, тому всі популярні веб-консолі використовують Java та веб-сервери (Apache Tomcat). Java забезпечує підтримку багатоплатформних веб-серверів. Для підвищення рівня безпеки ви можете встановити веб-сервер на окремий комп'ютер.



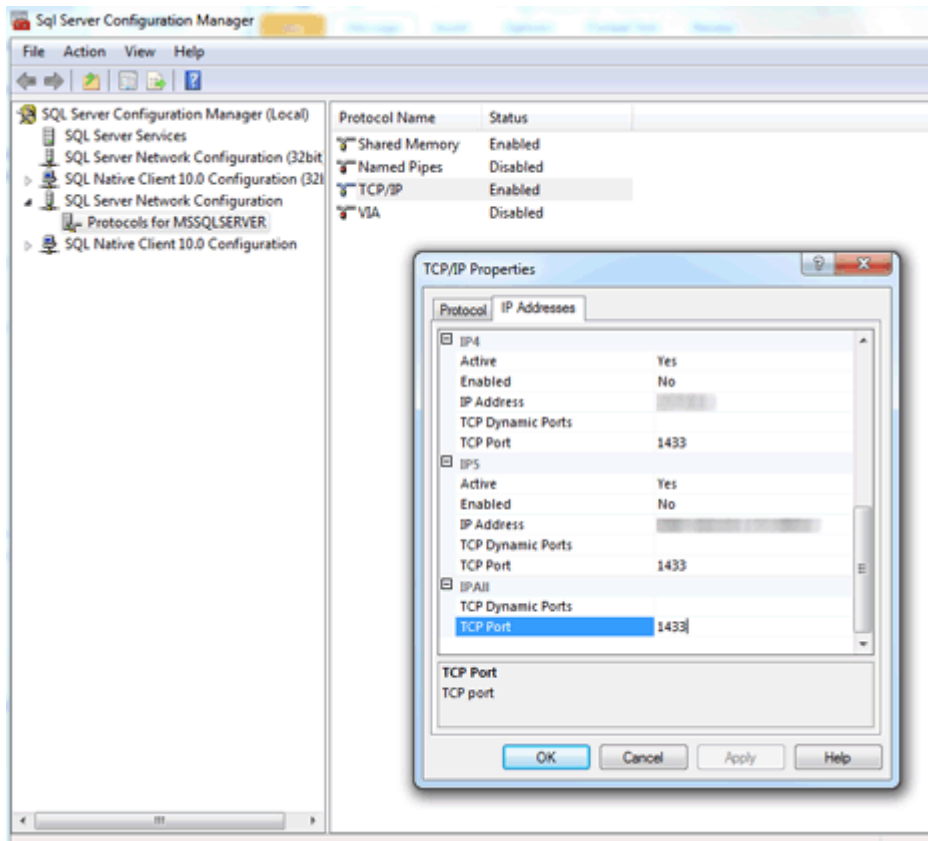
### Попередження

Із січня 2019 року загальнодоступні оновлення Oracle JAVA SE 8 для бізнесу, комерційного або промислового використання будуть доступні лише за наявності комерційної ліцензії. Якщо ви не придбали підписку JAVA SE, можете скористатися [цим посібником](#), щоб перейти на безкоштовну версію й інсталювати один із підтримуваних випусків Java.

---

### Як визначити, який порт використовує SQL Server?

Це можна зробити кількома способами. Для отримання найточнішого результату скористайтеся Диспетчером конфігурації SQL Server. Нижче наведено приклад того, як знайти цю інформацію в Диспетчері конфігурації SQL:



Після встановлення SQL Server Express (що входить до пакету ПЗ ESET PROTECT) на сервер Windows Server 2012 здається, що він не прослуховує стандартний порт SQL. Швидше за все, при цьому прослуховується не встановлений за замовчуванням порт 1433, а інший порт.

---

## Як налаштувати MySQL на прийняття пакетів великого розміру?

Див. «Керівництво з інсталяції та конфігурації MySQL» для [Windows](#) або [Linux](#).

---

## Якщо я встановлюю SQL самостійно, як мені створити базу даних для ESET PROTECT?

Вам не потрібно створювати базу даних. Це робить інсталятор **Server.msi**, а не інсталятор ESET PROTECT. Інсталятор ESET PROTECT спрощує загальну процедуру налаштування, він встановлює SQL Server, після чого інсталятор `server.msi` створює базу даних.

---

## Чи може інсталятор ESET PROTECT створити нову базу даних у

## **наявному екземплярі MS SQL Server, якщо я вкажу належну інформацію й облікові дані для підключення до MS SQL Server? Було б зручно, якби інсталятор підтримував різні версії SQL Server (2012, 2014 тощо).**

База даних створює Server.msi. Отже, інсталятор також може створити базу даних ESET PROTECT для окремих екземплярів SQL Server. Він підтримує версію MS SQL Server 2012 і новіші версії. ESET PROTECT 8.0 [Універсальний інсталятор](#) за замовчуванням інсталує Microsoft SQL Server Express 2019. Якщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інсталуватиметься за замовчуванням.

---

### **Чи повинен SQL Server використовувати вбудований режим автентифікації Windows за замовчуванням у разі встановлення на наявний SQL Server?**

Ні, тому що режим автентифікації Windows можна вимкнути на SQL Server, після чого можна буде виконати вхід лише за допомогою автентифікації SQL Server (вказавши ім'я користувача та пароль). Під час встановлення сервера ESET PROTECT необхідно використовувати змішаний режим автентифікації (автентифікація SQL Server й автентифікація Windows). У разі встановлення SQL Server вручну рекомендується створити кореневий пароль (ім'я кореневого користувача – sa, тобто security admin, адміністратор безпеки) і зберегти його для подальшого використання. Кореневий пароль може знадобитися під час оновлення сервера ESET PROTECT. Ви можете налаштувати [автентифікацію Windows](#) після встановлення сервера ESET PROTECT.

---

### **Чи можна використовувати MariaDB замість MySQL?**

Ні, MariaDB не підтримується. Обов'язково інстальуйте [підтримувану версію MySQL Server та з'єднувача ODBC](#). Див. керівництво з [інсталяції та конфігурації MySQL](#).

---

## **Мені довелося встановити Microsoft .NET Framework 4, оскільки інсталятор ESET PROTECT спрямував мене до <http://www.microsoft.com/en-us/download/details.aspx?id=17851>), але продукт не працює на новому екземплярі Windows Server 2012 R2 з SP1.**

Цей інсталятор не можна використовувати з Windows Server 2012 через політику безпеки Windows Server 2012. Має бути інстальовано Microsoft .NET Framework 4 за допомогою **майстра додавання ролей і функцій**.

---

### **Визначити, чи працює інсталятор SQL Server, дуже важко. Як дізнатися, що відбувається, якщо інсталяція займає більше 10 хвилин?**

У рідкісних випадках інсталяція SQL Server може тривати до 1 години. Швидкість інсталяції залежать від продуктивності системи.

---

## Як скинути пароль адміністратора веб-консолі (вказаний під час налаштування)?

Щоб скинути пароль, запустіть інсталятор сервера та виберіть пункт **Виправлення**. Пам'ятайте, що якщо ви не використовували автентифікацію Windows під час створення бази даних, для отримання доступу до бази даних ESET PROTECT вам може знадобитися пароль.



### Увага

- Будьте уважні, оскільки в разі використання певних параметрів виправлення може бути видалено збережені дані.
- У разі скидання пароля вимикається функція [двофакторної автентифікації](#).

---

## Який формат необхідно використовувати для імпорту файлу, що містить перелік комп'ютерів, які потрібно додати до ESET PROTECT?

Формат складається з наступних рядків:

```
All\Group1\GroupN\Computer1
```

```
All\Group1\GroupM\ComputerX
```

**All** – це обов'язкова назва кореневої групи.

---

## Чи можна використовувати IIS замість Apache? Чи можна додати інший сервер HTTP?

IIS – це сервер HTTP. Для запуску веб-консолі потрібен контейнер сервлетів Java (наприклад, Tomcat), сервера HTTP недостатньо. Існують рішення, що дають змогу зробити з IIS контейнер сервлетів Java, але в цілому ця можливість не підтримується.



### Примітка

Ми використовуємо не Apache HTTP Server, а інший продукт – Apache Tomcat.

---

## Чи підтримує ESET PROTECT інтерфейс командного рядка?

Так, ми використовуємо ESET PROTECT [ServerApi](#).

---

## Чи можна інсталиювати ESET PROTECT на контролер домену?

Рекомендуємо [не інсталиювати SQL Server в контролері домену](#) (наприклад, якщо ви використовуєте Windows SBS / Essentials). Рекомендуємо інсталиювати ESET PROTECT на іншому сервері або не вибирати компонент SQL Server Express під час інсталяції (щоб запустити базу даних ESET PROTECT, потрібно скористатися наявним сервером SQL Server або MySQL Server).

---

### Чи може інсталятор сервера ESET PROTECT виявити, що в системі вже встановлено SQL? Що станеться, якщо може? Що буде з MySQL?

ESET PROTECT перевірить наявність SQL у системі, якщо ви інсталиюєте SQL express за допомогою майстра інсталяції. Якщо в системі вже працює SQL, майстер відобразить сповіщення про видалення наявної версії SQL, а потім запустить інсталяцію або встановить ESET PROTECT без SQL Express. Див. [системні вимоги](#) для ESET PROTECT.

---

### Де можна знайти компонент ESET PROTECT, зіставлений за версією випуску?

Перегляньте [статтю бази знань](#).

---

### Як оновити ESET PROTECT до останньої версії?

ОС Windows:

- Оновіть веб-консоль ESET PROTECT (виконавши завдання для оновлення компонентів клієнта): <https://support.eset.com/kb7701/>
- Ручне оновлення: <https://support.eset.com/kb7702/>

ОС Linux: <https://support.eset.com/kb7733/>

---

### Як оновити систему без підключення до Інтернету?

Для цього необхідно інсталиювати проксі-сервер HTTP на комп'ютер, що може підключатися до серверів оновлення ESET (де зберігаються кешовані файли оновлення), а також налаштувати Endpoint на оновлення з цього проксі-сервера HTTP в локальній мережі. Якщо ваш сервер не підключено до Інтернету, ви можете ввімкнути функцію дзеркала Endpoint на одному комп'ютері, перенести файли оновлення на цей комп'ютер за допомогою USB-накопичувача, а потім установити його як сервер оновлення для інших не підключених до Інтернету комп'ютерів.

Для отримання детальної інформації про інсталяцію без підключення до Інтернету [дотримуйтеся цих інструкцій](#).

---



## Як переустановити сервер ESET PROTECT і підключити його до наявного SQL Server, якщо SQL Server було автоматично налаштовано під час ESET PROTECT інсталяція?

Якщо ви інсталуєте новий екземпляр сервера ESET PROTECT, використовуючи той самий обліковий запис користувача (наприклад, обліковий запис адміністратора домену), під яким інсталиували вихідну версію ESET PROTECT Server, то можете використовувати **MS SQL Server з автентифікацією Windows**.

---

### Як виправити проблеми із синхронізацією Active Directory в Linux?

Доменне ім'я має бути введено великими літерами (administrator@TEST.LOCAL, а не administrator@test.local).

---

### Чи можна використовувати власний мережевий ресурс (наприклад, папку SMB) замість сховища?

Ви можете вказати пряму URL-адресу пакету. Якщо ви використовуєте спільну папку, вкажіть шлях до неї в такому форматі: file:// + повний мережевий шлях до файлу, наприклад:

[file://\leraserver\install\ees\\_nt64\\_ENU.msi](file://\leraserver\install\ees_nt64_ENU.msi)

---

### Як скинути або змінити пароль?

Обліковий запис адміністратора рекомендується використовувати лише для створення облікових записів для окремих адміністраторів. Після створення [облікових записів адміністраторів](#) необхідно зберегти пароль адміністратора та не використовувати обліковий запис адміністратора. Таким чином обліковий запис адміністратора використовуватиметься лише для скидання пароля/відомостей облікового запису.

Як скинути пароль вбудованого облікового запису адміністратора ESET PROTECT:

1. Відкрийте пункт **Програми та засоби** (запустіть appwiz.cpl), знайдіть сервер ESET PROTECT і натисніть кнопку правою кнопкою миші.
2. Виберіть параметр **Змінити** в контекстному меню.
3. Виберіть **Виправлення**.
4. Укажіть дані для підключення до бази даних.
5. Виберіть **Використовувати наявну базу даних і застосувати оновлення**.
6. Скасуйте вибір **Використовувати пароль, який уже зберігається в базі даних** і введіть новий пароль.
7. Увійдіть до веб-консолі ESET PROTECT за допомогою нового пароля.



#### Примітка

Настійно рекомендується створити додаткові облікові записи з конкретними правами доступу на основі наявних обов'язків користувачів.

---

### Як змінити порти сервера ESET PROTECT і веб-консолі ESET PROTECT?

Щоб забезпечити можливість підключення веб-сервера до нового порту, необхідно змінити порт у конфігурації веб-сервера. Виконайте наведені нижче дії.

1. Вимкніть веб-сервер.
2. Змініть порт у конфігурації веб-сервера.
  - a) Відкрийте файл `webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`
  - b) Установіть новий номер порту (наприклад, `server_port=44591`).
3. Запустіть веб-сервер повторно.

---

### Чи можна оновити ERA v.5 до ESET PROTECT8 через універсальний інсталятор?

Пряме оновлення не підтримується: див. тему [Перенесення з ERA 5.x](#).

---

## Я отримую повідомлення про помилку або стикаюся з проблемами під час використання ESET PROTECT Як це зробити?

Див. [Запитання й відповіді щодо виправлення неполадок](#).

## 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: 31 333 535) (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 погоджуєтесь 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 погоджуєтесь з положеннями цієї Угоди й дотримуєтесь усіх наведених тут умов і положень, Постачальник надає Вам указані права ("Ліцензію").

**а) Інсталяція та використання.** Вам надається невиняткове та непередаване право 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.

г) **ОЕМ-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) **НДП та ПРОБНА ВЕРСІЯ Програмного забезпечення.** Програмне забезпечення, що визначається як «не для продажу» (НДП), або його ПРОБНА ВЕРСІЯ не підлягає оплаті та має використовуватися лише в демонстраційних цілях чи для тестування функцій Програмного забезпечення.

е) **Припинення дії ліцензії.** Дія ліцензії припиняється автоматично після закінчення періоду, на який вона надається. Якщо Ви не дотримуетесь 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 дозволу на збір даних:

а) **Оновлення Програмного забезпечення.** Постачальник може час від часу випускати оновлення Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення інстальюються автоматично, якщо Користувач не вимкнув відповідну функцію. Для надання оновлень нам необхідно перевірити автентичність Ліцензії, включаючи інформацію про комп'ютер та (або) платформу, на якій інстальовано Програмне забезпечення у відповідності до Політики конфіденційності.

б) **Надсилання Даних Постачальнику.** Програмне забезпечення оснащено функціями, які збирають дані про процес інсталяції, комп'ютер і (або) платформу, на яких інстальовано Програмне забезпечення, операції й роботу Програмного забезпечення, а також інформацію про керовані пристрої. Ці відомості (далі "Дані") надсилаються Постачальнику. Інформація може містити дані (зокрема персональні дані, які отримано випадково або в довільному порядку), які відносяться до керованих пристроїв. Активуючи описану вище функцію Програмного забезпечення, Ви підтверджуєте свою згоду надсилати Інформацію Постачальнику, а також надаєте Постачальнику право на обробку отриманої Інформації відповідно до чинних правових норм.

Для Програмного забезпечення потрібен компонент, інстальований на керованому комп'ютері, який дозволяє передавати інформацію між керованим комп'ютером і програмою віддаленого керування. Передавані дані містять такі відомості про керування, як інформація про апаратне та програмне забезпечення керованого комп'ютера, а також інструкції від інструментів віддаленого керування. Інший вміст даних, які передаються від керованого комп'ютера, має визначатися параметрами програми, інстальованої на керованому комп'ютері. Вміст інструкцій від інструментів віддаленого керування визначатиметься параметрами цих інструментів.

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'язуєтесь реалізувати права Користувача особисто або через своїх співробітників. Ви маєте право використовувати Програмне забезпечення лише для захисту безпеки своєї роботи та тих комп'ютерів і комп'ютерних систем, для яких надано Ліцензію.

**6. Обмеження прав.** Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Програмного забезпечення. Використовуючи Програмне забезпечення, Ви зобов'язуєтесь дотримуватися наведених нижче обмежень.

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

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.

г) Ви погоджуєтесь використовувати Програмне забезпечення лише таким способом, що відповідає всім застосовним юридичним нормам законодавства, яке регулює його застосування, включно з відповідними обмеженнями згідно із законом про авторське право й інші права на інтелектуальну власність, але не обмежуючись цим.

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 погоджуєтесь не вчиняти будь-які дії щодо використання Ліцензійного ключа, які суперечать положенням цієї Угоди або можуть призвести до передачі Ліцензійного ключа будь-якій особі, яка не має права використовувати Програмне забезпечення. Зокрема, Ви погоджуєтесь не передавати використовуваний або невикористовуваний Ліцензійний ключ у будь-якій формі, а також утриматися від несанкціонованого відтворення або розповсюдження дублікатів Ліцензійних ключів або створених Ліцензійних ключів або від використання Програмного забезпечення з Ліцензійним ключем, отриманим із будь-якого іншого джерела, окрім Постачальника.

**7. Авторське право.** Програмне забезпечення та всі права, включно із правами власності та відповідними правами на інтелектуальну власність без обмежень, належать компанії ESET та/або її ліцензіарам. Ці права захищено положеннями міжнародного договірної права та всіма іншими застосовними законами країни, у

якій використовується Програмне забезпечення. Структура, організація та код Програмного забезпечення є комерційною таємницею та конфіденційною інформацією компанії ESET і/або її ліцензіарів. Ви не маєте права копіювати Програмне забезпечення, за винятком визначених у розділі 6 (а) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то погоджуєтесь, що будь-яка отримана таким чином інформація буде автоматично й безповоротно вважатися належною для передавання Постачальнику та цілком належатиме йому з моменту її отримання, незалежно від права Постачальника на розірвання цієї Угоди.

**8. Захист прав.** Постачальник залишає за собою всі права на Програмне забезпечення, за винятком тих, що чітко надані Вам як Користувачу Програмного забезпечення відповідно до умов цієї Угоди.

**9. Багатомовні версії, програмне забезпечення, що постачається на носіях двох типів, кілька копій.**

Якщо Програмне забезпечення підтримує кілька платформ чи мов, або Ви одержали кілька копій Програмного забезпечення, Ви не маєте права інсталювати Програмне забезпечення на більшій кількості комп'ютерних систем або інші версії ніж ті, на які розповсюджується Ліцензія. Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, укладати договір лізингу, надавати право на користування чи передавати версії або копії Програмного забезпечення, які Ви не використовуєте.

**10. Набуття Угодою чинності та припинення дії Угоди.** Ця Угода набуває чинності з дати погодження з її умовами. Ви можете припинити дію цієї Угоди, остаточно видаливши, знищивши або повернувши за власний кошт Програмне забезпечення, усі резервні копії та всі пов'язані матеріали, отримані від Постачальника або його ділових партнерів. Незалежно від способу припинення дії цієї Угоди, умови розділів 7, 8, 11, 13, 19 і 21 є чинними без обмежень у часі.

**11. ЗАЯВА КОРИСТУВАЧА.** ЯК КОРИСТУВАЧ, ВИ ВИЗНАЄТЕ, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАДАЄТЬСЯ «ЯК Є» БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОПУСКАЄТЬСЯ ЧИННИМ ЗАКОНОДАВСТВОМ. НІ ПОСТАЧАЛЬНИК РАЗОМ ІЗ ЙОГО ЛІЦЕНЗІАРАМИ Й ДОЧІРНІМИ КОМПАНІЯМИ, НІ ВЛАСНИКИ АВТОРСЬКОГО ПРАВА НЕ НАДАЮТЬ БУДЬ-ЯКИХ ТВЕРДЖЕНЬ АБО СПЕЦІАЛЬНИХ ЧИ НЕПРЯМИХ ГАРАНТІЙ, ЗОКРЕМА ГАРАНТІЙ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ ЧИ КОНКРЕТНОГО ЗАСТОСУВАННЯ АБО ГАРАНТІЙ ТОГО, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НЕ ПОРУШУЄ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЄ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ АБО ВОНО ФУНКЦІОНУВАТИМЕ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ'ЯЗАНІ З ВИБОРОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ, А ТАКОЖ ЗА ІНСТАЛЯЦІЮ, ВИКОРИСТАННЯ ТА НАСЛІДКИ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

**12. Відсутність інших зобов'язань.** Ця Угода не створює жодних зобов'язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

**13. ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ.** У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ЛІЦЕНЗІАРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ВТРАЧЕНІ ПРИБУТКИ, ДОХОДИ, ЗНИЖЕННЯ ОБСЯГІВ ПРОДАЖІВ АБО ВТРАТУ ДАНИХ, А ТАКОЖ ДОДАТКОВІ ВИТРАТИ, ПОВ'ЯЗАНІ З ПРИДБАННЯМ ЗАПАСНИХ ТОВАРІВ АБО ПОСЛУГ, ЗАПОДІЯНУ МАЙНУ ШКОДУ, ОСОБИСТУ ШКОДУ, ПРИПИНЕННЯ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, ВТРАТУ ДІЛОВОЇ ІНФОРМАЦІЇ ЧИ БУДЬ-ЯКІ СПЕЦІАЛЬНІ, ПРЯМІ, НЕПРЯМІ, ВИПАДКОВІ, КОМЕРЦІЙНІ, ШТРАФНІ ЧИ ОПОСЕРЕДКОВАНІ ЗБИТКИ, БУДЬ-ЯКИМ ЧИНОМ ОБУМОВЛЕНІ ДІЄЮ УГОДИ, ЦИВІЛЬНЕ ПРАВОПОРУШЕННЯ, НЕДБАЛИСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНИМ КОМПАНІЯМ ВІДОМО ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ. В ОКРЕМИХ КРАЇНАХ І ЮРИСДИКЦІЯХ НЕ ПЕРЕДБАЧЕНО ВИНЯТКИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ, АЛЕ ЇЇ МОЖЕ БУТИ ОБМЕЖЕНО. ТОБТО ВІДПОВІДАЛЬНІСТЬ ПОСТАЧАЛЬНИКА, ЙОГО СПІВРОБІТНИКІВ, ЛІЦЕНЗІАРІВ АБО ДОЧІРНИХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ЛІЦЕНЗІЮ.

**14.** Жодна умова цієї Угоди не має порушувати законні права будь-якої сторони, що виступає як клієнт, у тих випадках, коли вони їм суперечать.

**15. Технічна підтримка.** Компанія ESET або вповноважені нею треті сторони надають технічну підтримку на власний розсуд без жодних гарантій або заяв. Перед наданням технічної підтримки Користувач повинен створити резервні копії всіх поточних даних, програмного забезпечення та програмних засобів. Компанія ESET або вповноважені нею треті сторони не несуть відповідальності за пошкодження або втрату даних, майна, програмного чи апаратного забезпечення, а також комерційні збитки, що виникають унаслідок надання технічної підтримки. Компанія ESET і/або вповноважені нею треті сторони залишають за собою право приймати рішення щодо того, чи належить проблема до обсягу послуг, які надаються в рамках технічної підтримки. Компанія ESET залишає за собою право на власний розсуд приймати рішення щодо відмови в наданні технічної підтримки, її призупинення чи скасування. Для забезпечення технічного обслуговування може знадобитися інформація про Ліцензію та інші дані у відповідності до Політики конфіденційності.

**16. Передача Ліцензії.** Програмне забезпечення може передаватися з однієї комп'ютерної системи на іншу, якщо такі дії не суперечать умовам Угоди. За умови дотримання положень Угоди Користувач має право остаточної передачі Ліцензії та всіх прав, що виникають унаслідок укладання цієї Угоди, іншому Користувачеві за згоди Постачальника, якщо (i) вихідний Користувач не зберігає жодних копій Програмного забезпечення; (ii) виконується пряма передача прав, наприклад, від вихідного Користувача до нового; (iii) новий Користувач приймає від вихідного всі права, що надаються відповідно до умов цієї Угоди; (iv) вихідний Користувач надає новому документацію, що дозволяє підтвердити автентичність Програмного забезпечення відповідно до розділу 17.

**17. Підтвердження автентичності Програмного забезпечення.** Кінцевий користувач може підтвердити своє право застосовувати Програмне забезпечення одним із таких способів: (i) за допомогою ліцензійного сертифіката, наданого Постачальником або вповноваженою ним третьою особою; (ii) за допомогою ліцензійної угоди в письмовій формі (якщо така укладалася); (iii) надавши надісланий Постачальником електронний лист із ліцензійними даними (ім'я користувача та пароль). Для підтвердження автентичності Програмного забезпечення може знадобитися інформація про Ліцензію та ідентифікаційні дані Кінцевого споживача у відповідності до Політики конфіденційності.

**18. Надання ліцензії органам державної влади й уряду США.** Програмне забезпечення надається органам державної влади, включно з урядом США, з урахуванням ліцензійних прав і обмежень, наведених у цій Угоді.

**19. Дотримання процедур із контролю за торгівлею.**

а) Забороняється в прямий чи непрямий спосіб експортувати, реекспортувати, передавати або іншим чином надавати програмне забезпечення будь-яким іншим особам. Ви зобов'язуєтеся утриматися від будь-яких способів використання цього програмного забезпечення й (або) не брати участь у жодних діях, які можуть призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET, її холдингових і дочірніх компаній або дочірніх компаній будь-яких холдингових компаній ESET, відповідно до законів із контролю за торгівлею, зокрема тих, що наведені нижче:

i. Усі закони, які регулюють, обмежують або накладають ліцензійні вимоги для експорту, реекспорту або передачі товарів, програмного забезпечення, технологій або послуг, що видані або прийняті будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії (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.а 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.

v) 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 погоджуєтесь, що розгляд будь-яких заяв до Постачальника чи суперечок із ним, які викликані 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-ESMC-20-01

## Політика конфіденційності

Компанія ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic), внесена до комерційного реєстру окружного суду м. Братислави I, Розділ Sro, запис № 3586/B, реєстраційний номер: 31 333 535) як Контролер Даних (далі "ESET" або "Ми") прагне прозорості в справах, що стосуються обробки персональних даних і збереження конфіденційності наших клієнтів. З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів ("Кінцевий користувач" або "Ви") про такі теми:

- Обробка персональних даних
- Конфіденційність даних
- Права суб'єкта захисту даних

### Обробка персональних даних

Служби, які надаються ESET, реалізовані в нашому продукті й надаються згідно з Ліцензійною угодою з кінцевим користувачем (далі "Ліцензійна угода"). Однак деякі аспекти потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов'язаний із наданням наших послуг. Ми



надаємо різні служби, наведені в Ліцензійній угоді й документації для відповідного продукту. Ідеться, зокрема, про службу оновлення/модернізації, ESET LiveGrid®, захист від несанкціонованого використання даних, служби підтримки тощо. Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

- Для керування продуктами безпеки ESET потрібні такі дані, які зберігатимуться локально: ідентифікатор та ім'я робочого місця, ім'я продукту, інформація про ліцензію, інформація про активацію й завершення терміну дії, інформація про обладнання й програми на керованому комп'ютері з інстальованим продуктом безпеки ESET. Усі операції керованих продуктів безпеки ESET і пристроїв записуються в журнали, що дозволяє спростити керування функціями й службами та контроль за їхньою роботою без автоматичного надсилання в ESET.
- Інформація, пов'язана з процесом інсталяції, зокрема платформою, на якій інстальовано продукт, а також інформація про операції й функціональність наших продуктів, зокрема унікальний код обладнання, ідентифікатори інсталяції, аварійні дампи пам'яті, ідентифікатори ліцензії, IP-адреси, MAC-адреси, параметри конфігурації продукту (це може відноситися й до керованих пристроїв).
- Інформація про ліцензію, зокрема ідентифікатор ліцензії й персональні дані (ім'я, прізвище, адреса, адреса електронної пошти), потрібна для виставлення рахунків, перевірки автентичності ліцензії й надання наших служб.
- Контактна інформація і дані, які містяться в запитах до служби підтримки, можуть знадобитися для надання послуг підтримки. У залежності від обраного каналу зв'язку ми можемо збирати такі дані: адреса електронної пошти, номер телефону, дані ліцензії, дані продукту й опис Вашого звернення до служби підтримки. До Вас може надійти запит щодо надання іншої інформації для прискорення обслуговування службою підтримки. Наприклад, це може бути запит на сформовані файли журналу.
- Дані про використання нашої служби є абсолютно анонімними до завершення сеансу. Після завершення сеансу не зберігається жодних даних, за якими можна ідентифікувати особу.

### **Конфіденційність даних**

ESET — це компанія, яка працює в усьому світі через афілійовані компанії або партнерів, які входять до нашої мережі розповсюдження, обслуговування та підтримки. Інформація, яка оброблюється ESET, може передаватися афілійованим компаніям або партнерам або отримуватися від них. Це необхідно для виконання вимог Ліцензійної угоди, таких як надання послуг або підтримки або виставлення рахунків. В залежності від розташування і використовуваних Вами служб ми можемо бути змушені передавати Ваші дані державним установам без належного рішення Європейської Комісії. Навіть у такому випадку кожна передача інформації є предметом регулювання з боку законодавства про захист даних і відбувається тільки в тих випадках, коли це необхідно. Стандартні договірні умови й обов'язкові правила організації або інші належні заходи щодо захисту інформації мають застосовуватися без будь-яких обмежень.

Ми робимо все, що від нас залежить, щоб не зберігати довше, ніж це потрібно, дані, зібрані нами в зв'язку з наданням послуг відповідно до Ліцензійної угоди. Дані можуть зберігатися й після закінчення строку дії Вашої ліцензії, що дозволить Вам швидко й зручно поновити дію ліцензії. Статистична інформація в стисnutій і анонімній формі, а також інші дані від ESET LiveGrid® можуть оброблятися для статистичних цілей.

ESET впроваджує відповідні технічні та організаційні заходи, щоб забезпечити безпеку на тому рівні, якій відповідає потенційним ризикам. Ми докладємо всіх зусиль, щоб постійно забезпечувати конфіденційність, цілісність, доступність і стійкість систем обробки й сервісів. Однак у випадку витоку конфіденційної інформації, що загрожує Вашим правам та свободам, ми готові сповістити про це відповідний наглядовий орган, а також суб'єктів захисту персональних даних. Як суб'єкт захисту персональних даних Ви маєте право подавати скарги до вищестоящих органів влади.

### **Права суб'єкта захисту персональних даних**

ESET є суб'єктом регулювання відповідно до законів Словацької Республіки. Для Вас є чинними всі умови, визначені застосовними законами щодо захисту даних. Як суб'єкт захисту персональних даних Ви маєте такі права:

- право запитувати доступ до персональних даних від ESET;
- право на уточнення персональних даних у разі їх неточності (також у Вас є право доповнити неповні персональні дані);
- право надіслати запит на видалення персональних даних;
- право надіслати запит на обмеження обробки персональних даних;
- право не погоджуватися з обробкою даних;
- право подати скаргу, а також
- право забезпечити можливість переносу даних.

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