ESET PROTECT

Посібник з інсталяції оновлення й міграції

Натисніть тут щоб відкрити версію цього документа

Digital Security
Progress. Protected.

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

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

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

REV. 12.04.2024

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.

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

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

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 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.
Текст курсивом	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.
Гіперпосилання	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 інстальовані програми Windows та інших розробників.

- Онлайн-довідка — основне джерело інформації. Остання версія онлайн-довідки автоматично відображатиметься 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.

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 – 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 Windows (наприклад, ESET Server Security).

ESET PROTECT базується на двох основних принципах:

- **Централізоване керування** – можна здійснювати налаштування, керування та нагляд за системою з одного місця.
- **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 9.0

Детальніша інформація одним натисканням

Швидко переглянути відомості про комп'ютер або виявлені об'єкти ще ніколи не було так просто. Достатньо клацнути ім'я комп'ютера в розділі **Комп'ютери**, і з'явиться бічна панель з інформацією. Докладніше Те саме можна зробити в розділі "**Виявлені об'єкти**" – там достатньо натиснути тип об'єкта. Докладніше

Нова панель інструментів для EDTD

Ми представили нову панель інструментів, де можна знайти корисну інформацію та статистику, пов'язану з ESET Dynamic Threat Defense. Докладніше

Автоматичні оновлення продукту

Задля спрощення роботи з нашими продуктами з безпеки ми додаємо функцію автоматичного оновлення, яка поки що працюватиме в продуктах для робочих станцій Windows. Функцію автоматичного оновлення буде впроваджено в продуктах ESET Endpoint Security/Antivirus v9, які випускатимуться в листопаді. Завдяки автоматичним оновленням ваші продукти ESET завжди будуть в актуальному стані. Докладніше

Керування захистом від атак прямим добором

У продуктах для робочих станцій Windows версії 9 ми впроваджуємо нову функцію безпеки, яка забезпечить захист пристроїв від потенційного підбору облікових даних і несанкціонованого використання віддалених підключень. Ця функція легко налаштовується за допомогою політики безпосередньо на консолі. У розділі **Виявлені об'єкти** можна створити виключення.

Удосконалення ESET Full Disk Encryption

Автоматизація оновлень модулів ESET Full Disk Encryption дає змогу заощадити час. Ми також додали можливість розгорнути інсталятор із попередньо визначеним паролем і екранною клавіатурою для запуску шифрування. І нарешті, що не менш важливо, тепер в інтерфейсі користувача відображаються поточні інстальовані модулі ESET Full Disk Encryption.

Інші покращення й зміни зручності використання

Більш докладні відомості див. в журналі змін.

Архітектура

ESET PROTECT — це система віддаленого управління нового покоління.

Щоб повністю розгорнути продукти з безпеки ESET, мають бути інстальовані вказані нижче компоненти (для платформ Windows і Linux):

- ESET PROTECTСервер
- Веб-консоль ESET PROTECT

- ESET Management Агент

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 Apache HTTP
- 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.

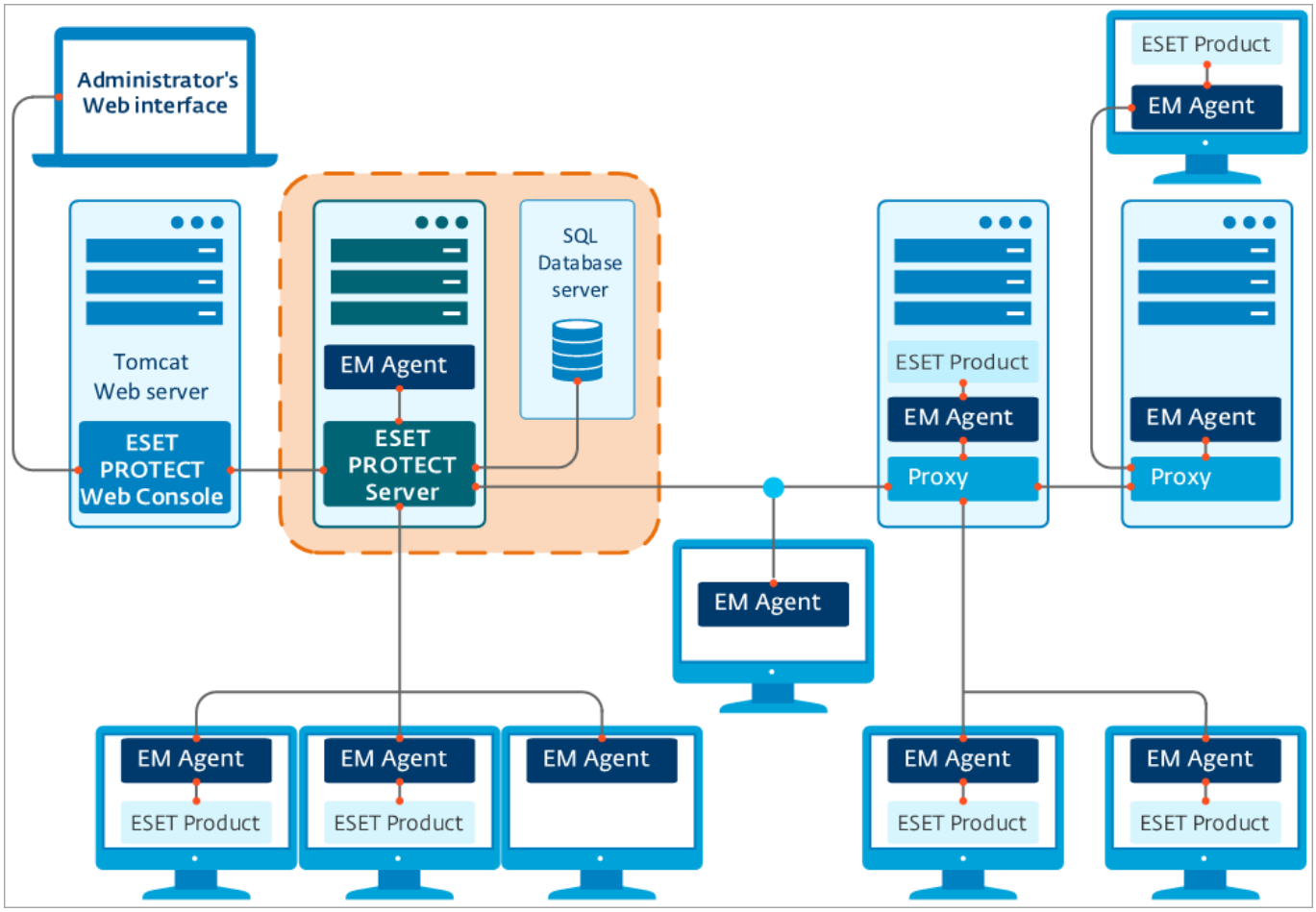
Огляд елементів інфраструктури

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

Функція	ESET PROTECTСервер	ESET Management Агент	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 інсталювати сервер бази даних на іншому комп’ютері.

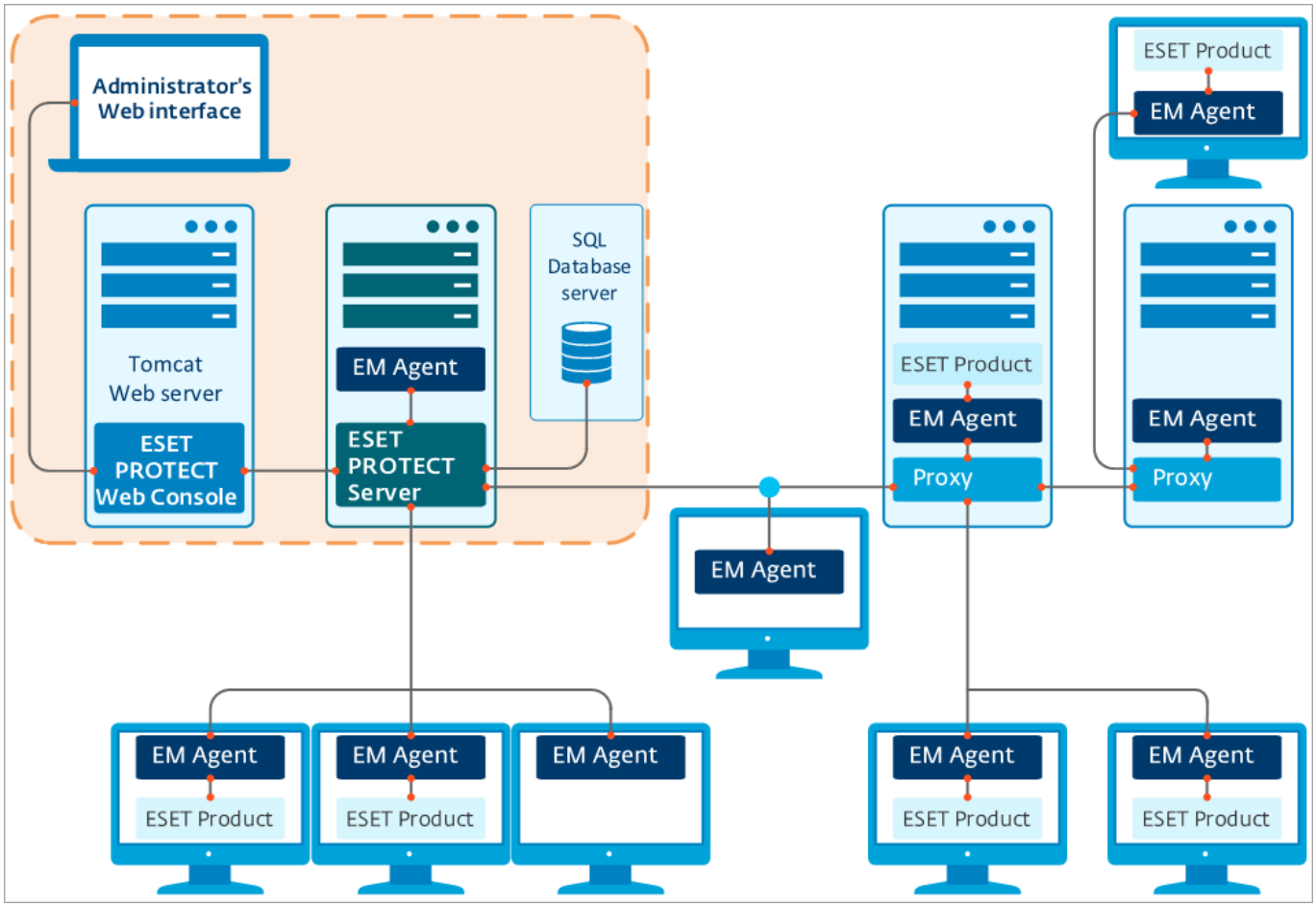


Web Console

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.

Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери.



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.

Як працює проксі-сервер у ESET PROTECT?

ESET PROTECT 9 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 Apache HTTP?

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,

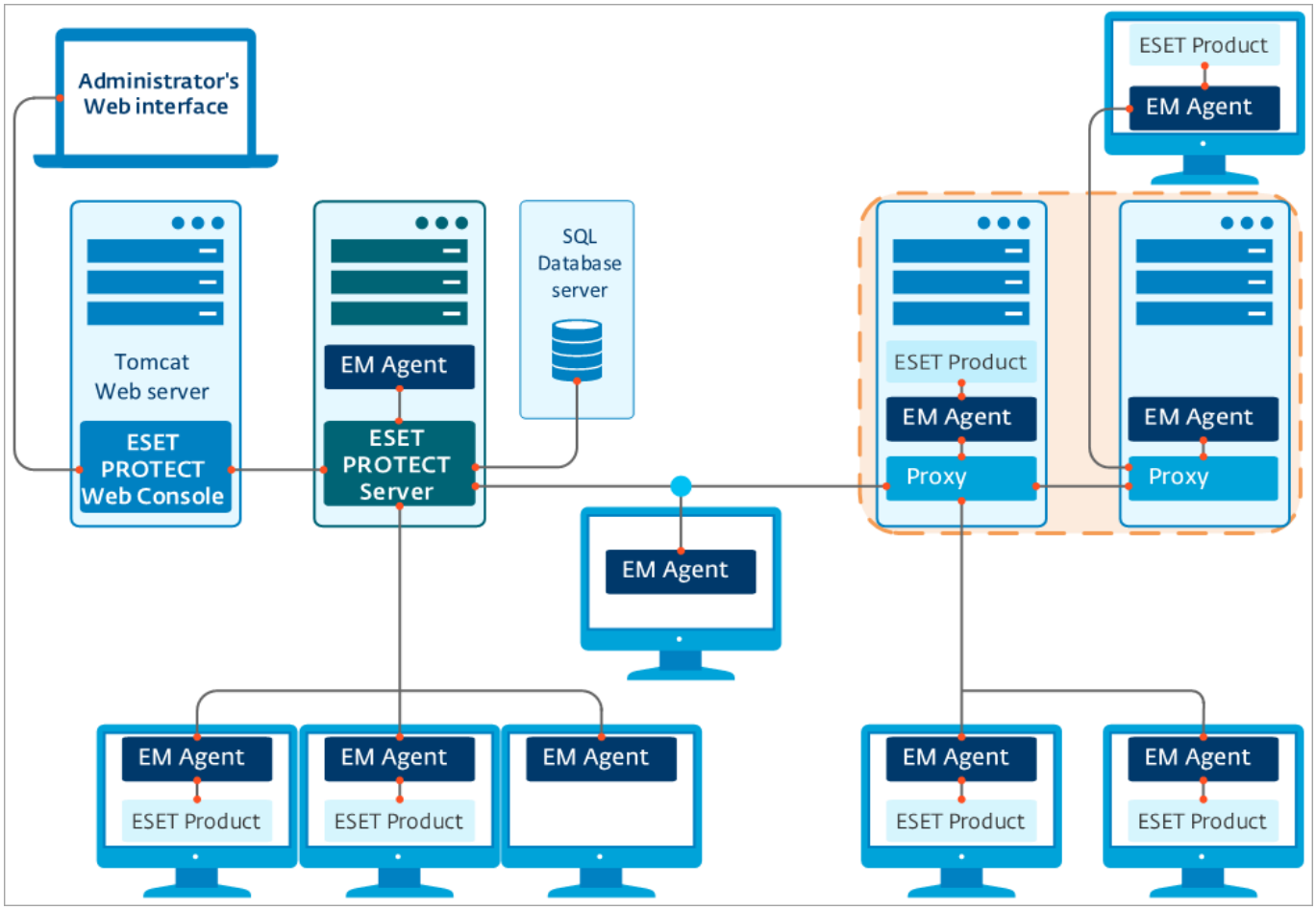
  оміж проксі-серверами та клієнтськими комп’ютерами на віддаленому робочому місці.

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.

> Які ще функції має проксі-сервер Apache HTTP?



Проксі-сервер Apache HTTP

Apache HTTP Proxy – це проксі-сервер, за допомогою якого можна розповсюджувати оновлення на клієнтські комп'ютери.

Щоб інсталювати 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
Реплікація обміну даними між агентами ESET Management і сервером ESET PROTECT	Проксі-сервер Apache HTTP або інший проксі-сервер

Функція кешування

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.

На відміну від інструмента «Дзеркало», який завантажує всі доступні на серверах оновлення ESET дані, Apache HTTP Proxy 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 Proxy 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 Proxy 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 Proxy 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 Proxy можна використовувати для збору та пересилання даних від компонентів ESET PROTECT у віддалене сховище. 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 Proxy 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 Proxy.

Детальніше про Функції проксі-сервера.

Як налаштувати проксі-сервер HTTP

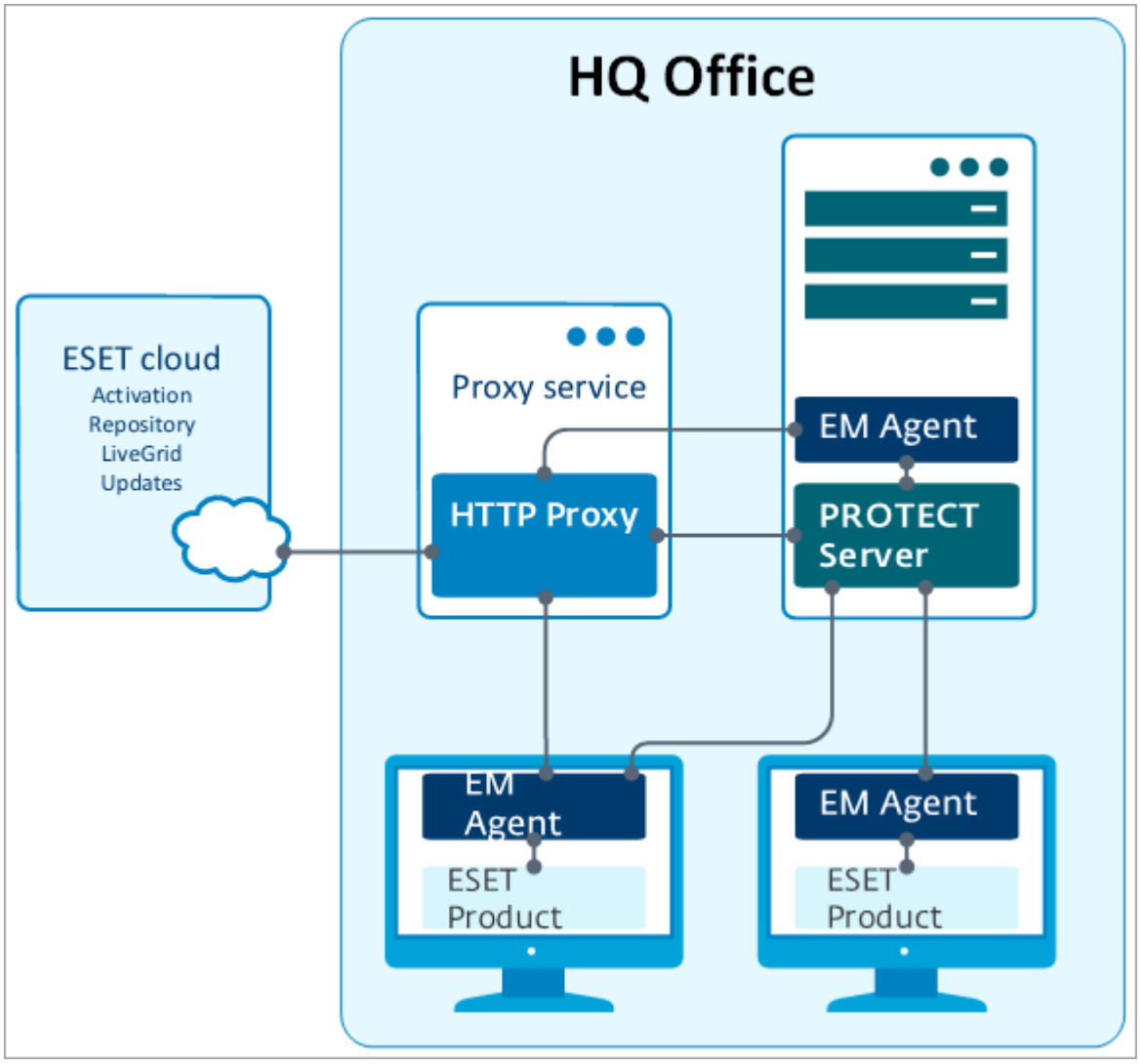
Щоб користуватися проксі-сервером, потрібно налаштувати ім'я хоста проксі-сервера HTTP в політиці агента (**Додаткові параметри** > **Проксі-сервер HTTP**). Для кешування та перенаправлення можна використовувати різні проксі-сервери. Перегляньте параметри політики нижче.

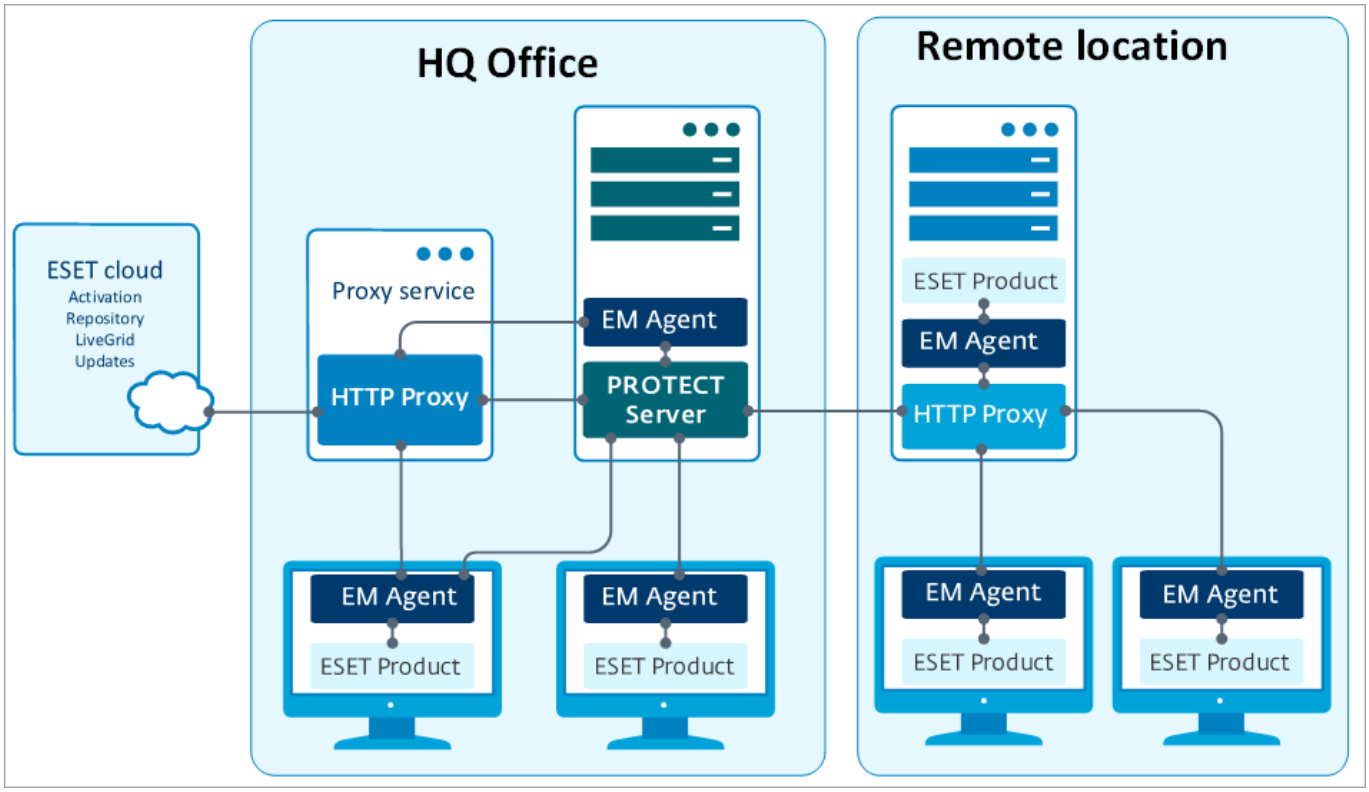
- **Глобальний проксі-сервер**. Один проксі-сервер використовуватиметься для кешування завантажень і перенаправлення даних агента.

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

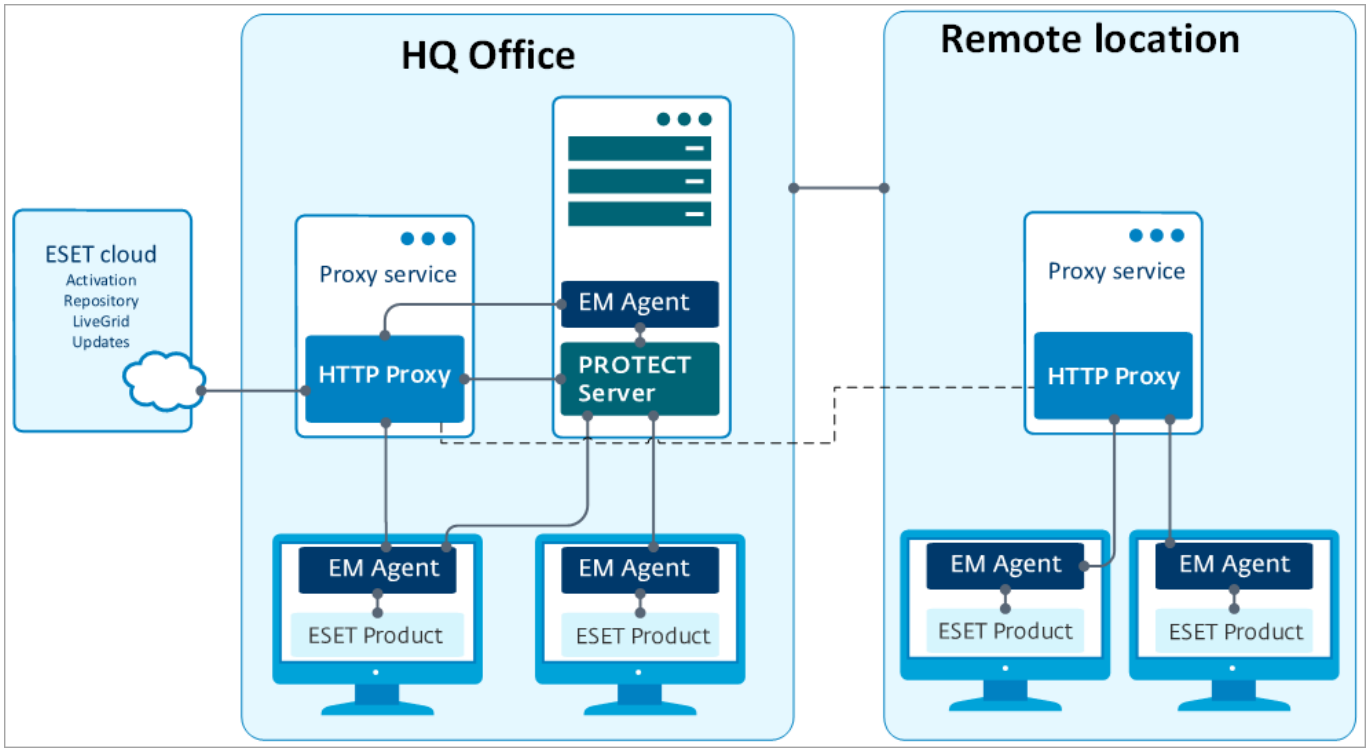
Проксі-сервер Apache HTTP в інфраструктурі

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





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.



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

Агент

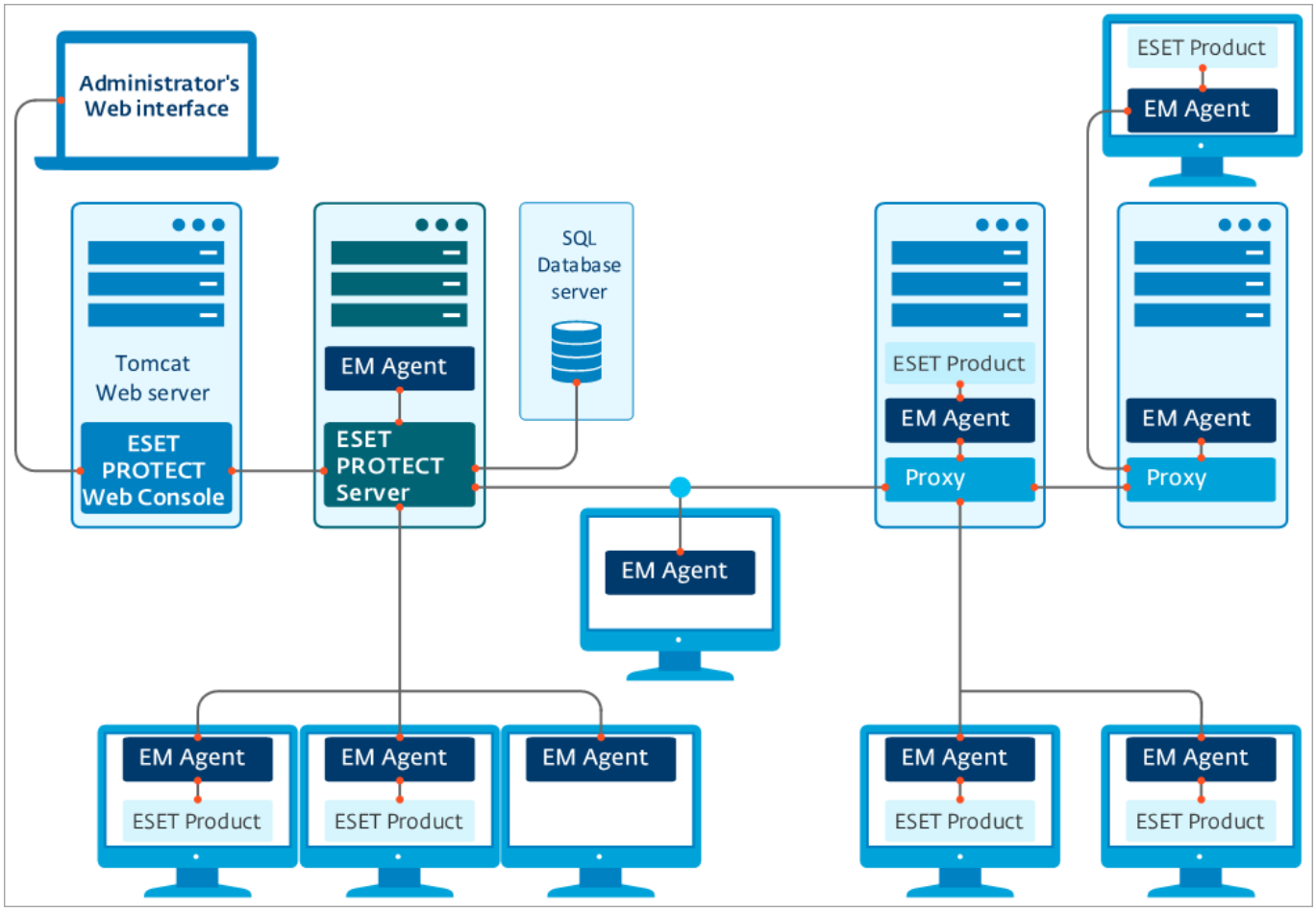
Агент ESET Management є невід'ємною частиною ESET PROTECT. Клієнти передають дані на сервер ESET PROTECT не напряму, а через агента. Агент збирає інформацію від клієнта та надсилає її на сервер ESET PROTECT. Якщо сервер ESET PROTECT надсилає завдання клієнту, воно потрапляє до агента, який пересилає завдання до призначення. Агент ESET Management використовує новий, удосконалений протокол зв'язку.

Для спрощення розгортання захисту робочої станції до пакета ESET ManagementESET PROTECT входить відокремлений агент . 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 інсталювати 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.

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

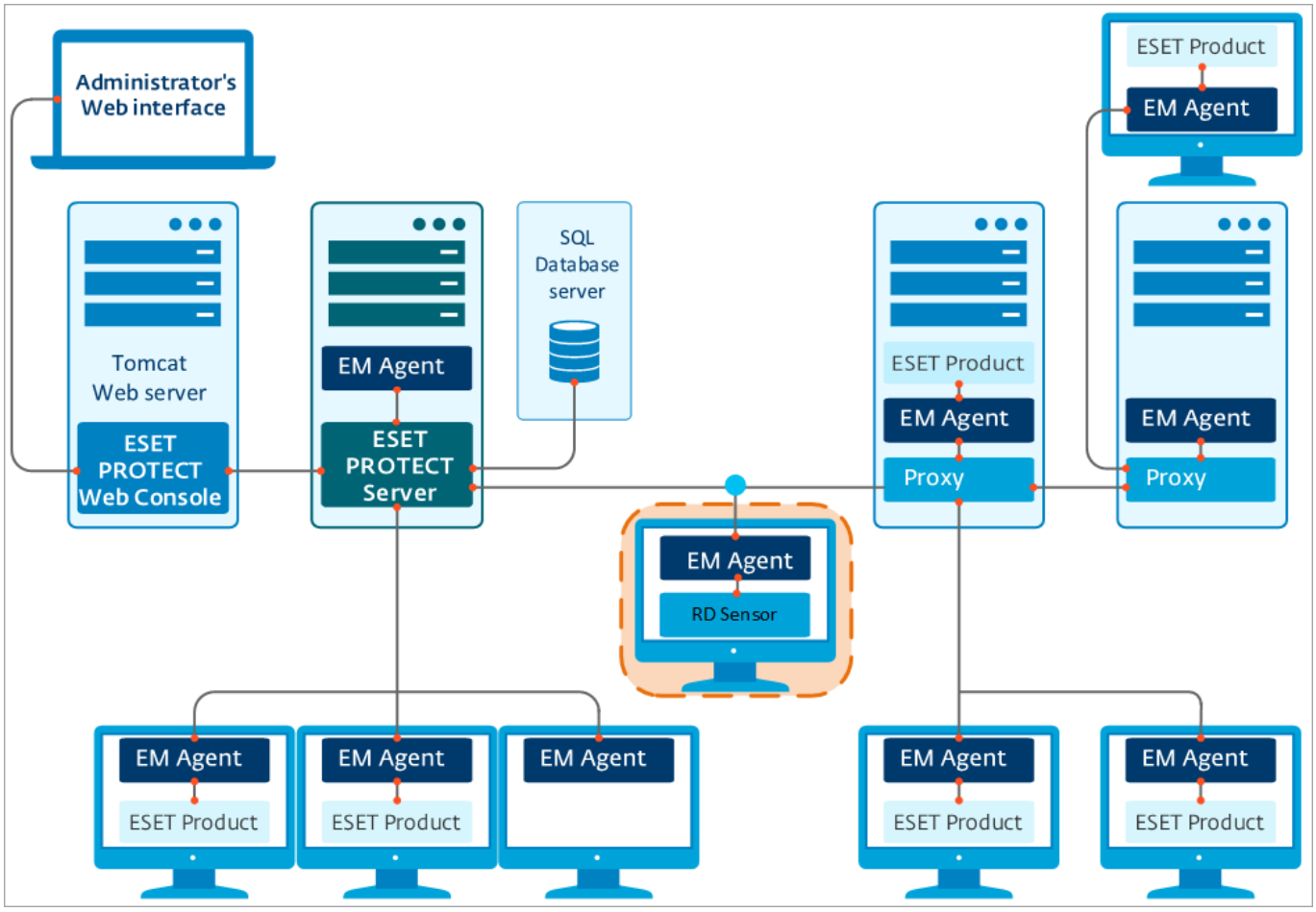
Rogue Detection Sensor (RD Sensor) – це засіб виявлення неавторизованих систем, який здійснює пошук комп'ютерів у вашій мережі. Цей засіб може знаходити нові комп'ютери з ESET PROTECT без ручного пошуку та додавання. Виявлені комп'ютери негайно вносяться до попередньо налаштованого звіту, завдяки чому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

RD Sensor активно прослуховує запити ARP (broadcast). Коли RD Sensor виявить новий активний мережевий компонент, RD Sensor надсилає відповіді ARP (unicast), створює відбитки хоста (з використанням кількох портів) і надсилає інформацію про виявлені комп'ютери на сервер ESET PROTECT. Сервер ESET PROTECT оцінює статус виявлених ПК (невідомі для сервера ESET PROTECT чи під керуванням).

Неможливо вимкнути створення відбитків хоста, оскільки це є основною функцією RD Sensor.

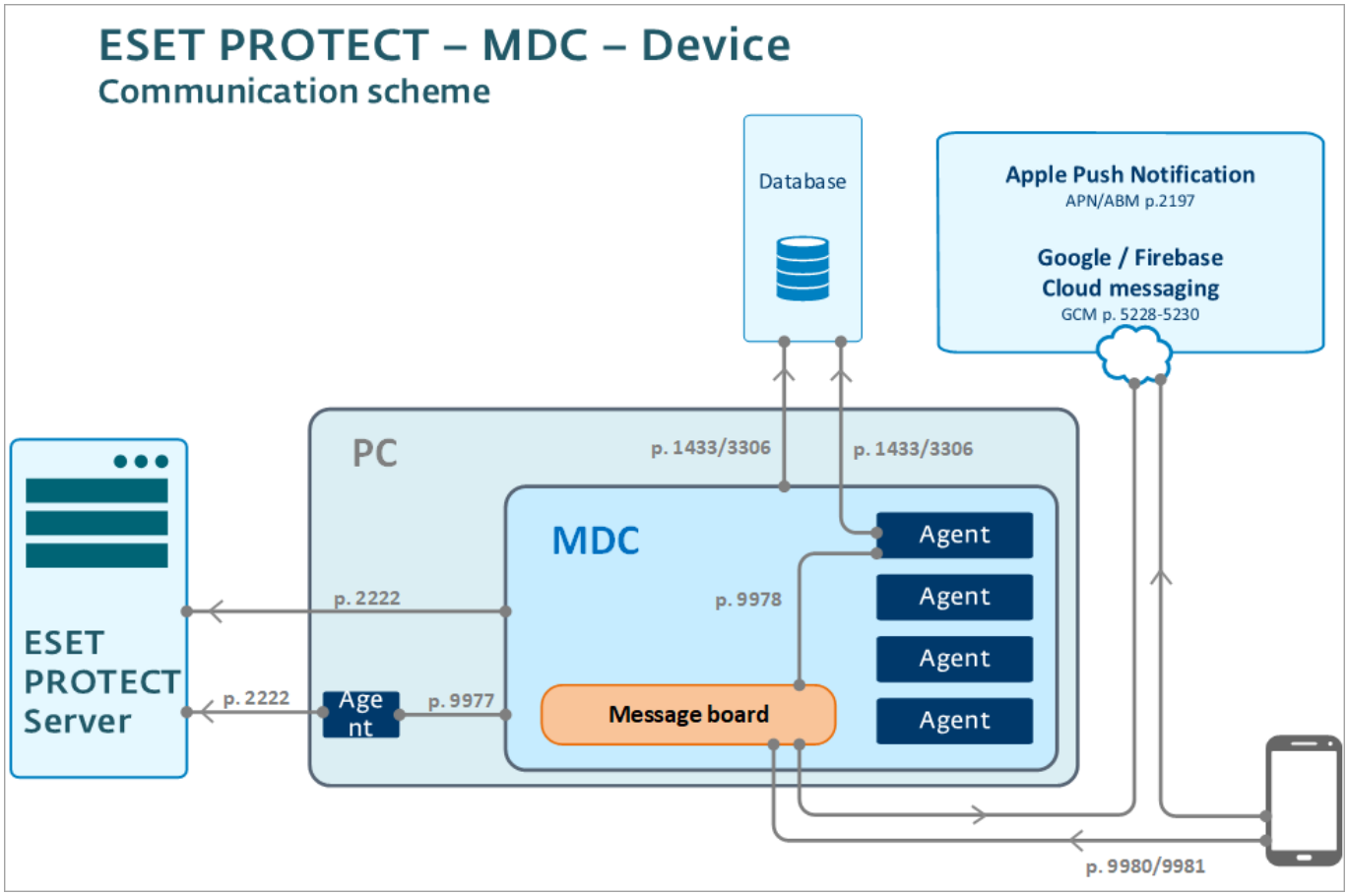
Якщо в мережі є кілька сегментів, Rogue Detection Sensor необхідно інсталювати окремо в кожному сегменті мережі для формування повного списку всіх пристроїв у всій мережі.

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 PROTECTMobile 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.



Збільшити зображення

Рекомендуємо розгортати 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.

Дотримуйтеся інструкцій з інсталяції MDM для Windows (із використанням універсального інсталятора або функції інсталяції компонента) або Linux.

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).

> **i** 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	Варіант 1: кешування за допомогою проксі-сервера	Варіант 2: інструмент «Дзеркало»	Варіант з автономним середовищем
Розгортання агента (з репозиторія за допомогою Push-сповіщень/Live Installer)	Один раз	Приблизно 50 МБ на клієнта	ТАК	ТАК3	НІ	ТАК (GPO / SCCM, змінені Live Installer)4

Тип підключення	Частота підключення	Споживання мережевого трафіка	Передача даних через проксі-сервер	Варіант 1: кешування за допомогою проксі-сервера	Варіант 2: інструмент «Дзеркало»	Варіант з автономним середовищем
Інсталяція на робочій станції (інсталяція програмного забезпечення з репозиторія)	Один раз	Приблизно 100 МБ на клієнта	ТАК	ТАК3	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 місяць5	ТАК	ТАК	ТАК	ТАК (Mirror Tool в автономному режимі та користувацький сервер HTTP)6
Файл з версією для оновленняupdate.ver	Прибл. 8 разів на день	2,6 МБ на місяць7	ТАК	НІ	-	-
Активація/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 ліцензій, використовуйте обліковий запис власника ліцензії або адміністратора безпеки.

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.

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 пропускної 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 наноонovлення після кожного відповідного запиту (якщо оновлення доступне).

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.

> **i** 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

> **i** 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

Для інсталяції й роботи ESET PROTECT ваша систем має відповідати попереднім вимогам до обладнання, бази даних, мережі й програмного забезпечення.

Підтримувані операційні системи

У розділах нижче описано підтримку компонента ESET PROTECT для Windows, Linux, macOS і операційних систем для мобільних пристроїв.

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 і KB4490628		✔	✔	

Операційна система	Сервер	Агент	RD Sensor	MDM
Windows Server 2008 R2 CORE x64 з інстальованим оновленням KB4474419 і KB4490628		✔	✔	
Windows Storage Server 2008 R2 x64 з інстальованим оновленням KB4474419 і KB4490628		✔	✔	
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
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	✔	✔	✔	✔
Windows Server 2022 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)	*	✔	✔	*
Windows 10 для ARM		✔		
Windows 11 x64	*	✔	✔	*

* 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 інсталювати ESET PROTECT для Linux або віртуальний пристрій, де це можливо.

Старіші системи MS Windows:
• У вас завжди має бути інстальовано останню версію пакета оновлень, особливо в старіших системах, таких як Server 2008 та Windows 7.
• ESET PROTECT не підтримує керування комп'ютерами, на яких виконується Windows 7 (без пакета оновлень), Widows Vista і Windows XP.
• 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. Ми не підтримуємо нелегальні чи піратські операційні системи.

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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

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

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 x64	✔	✔	✔	✔
SLED 15 x64	✔	✔	✔	✔

Операційна система	Сервер	Агент	RD Sensor	MDM
SLES 12 x64	✔	✔	✔	✔
SLES 15 x64	✔	✔	✔	✔
OpenSUSE Leap 15.2 x64	✔	✔	✔	✔
Debian 9 x64	✔	✔	✔	✔
Debian 10 x64	✔	✔	✔	✔
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

* Red Hat Entreprise Linux Server 8.x не підтримує створення звітів *.pdf*. Більш докладні відомості див. в розділі щодо відомих проблем ESET PROTECT.

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	✔
macOS 12.0 Monterey	✔

macOS підтримується лише як клієнт. Агент ESET Management і продукти ESET для macOS можна інсталювати в macOS. Однак сервер ESET PROTECT не можна інсталювати в macOS.

Мобільний пристрій

Операційна система	EESA	Власник пристрою EESA	MDM iOS	MDM iOS ABM
Android 5.x+	✔			
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔			

Операційна система	EESA	Власник пристрою EESA	MDM iOS	MDM iOS ABM
iOS 9.x+			✔	?*
iOS 10.x+			✔	?*
iOS 11.x+			✔	?*
iOS 12.0.x			✔	?*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔

* Програма iOS DEP доступна лише у вибраних країнах.

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.

a)Скористайтеся сертифікатом, що надав видавець сертифіката, якому довіряє Apple.

b)Призначте надійність сертифіката вручну перед реєстрацією. Це означає, що перед реєстрацією потрібно інсталювати 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 інсталювали 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 й налаштування розмірів інфраструктури

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

Кількість клієнтів	Сервер ESET PROTECT + сервер бази даних SQL				
	Ядра ЦП	Тактова частота ЦП (ГГц)	ОЗП (ГБ)	Диск[1]	IOPS[2] диска
До 1000	4	2.1	4	Одиночний	500
5.000	8	2.1	8		1.000
10,000 [3]	4	2.1	16	Окремий	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

1 Одиночний/окремий диск: рекомендуємо інсталювати базу даних на окремий диск для систем, які мають більше 10.000 клієнтів.

Мінімальне необхідне значення: 2 IOPS (операцій вводу/виводу на секунду).

• 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`

3 Див. зразок сценарію для середовища з 10 000 клієнтами.

Рекомендації щодо використання диска

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

• 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.

• Продуктивність сервера SQL зросте, якщо розмістити базу даних і файли журналу транзакцій на окремих дисках (бажано використовувати окремі фізичні накопичувачі SSD).

• Якщо у вас один диск, рекомендуємо використовувати накопичувач SSD.

• Рекомендуємо використовувати архітектуру All-Flash. Використовуйте твердотілі накопичувачі (SSD), оскільки вони працюють набагато швидше, ніж звичайні.

• Якщо у вашій конфігурації багато оперативної пам'яті, достатньо налаштувати SAS із R5. Перевірена конфігурація: 10 дисків SAS (1,2 ТБ) у R5: дві групи парності в конфігурації 4+1 без додаткового кешування.

• Продуктивність не покращується, якщо використовуються накопичувачі SSD корпоративного класу з високим значенням IOPS.

• 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.

• Якщо у вас є робоча багаторівнева інфраструктура для зберігання даних, яка дає змогу переносити онлайнові сховища, рекомендуємо починати роботу зі спільними повільнішими рівнями й відстежувати продуктивність роботи ESET PROTECT. Якщо ви помітите, що затримка читання й записування перевищує 20 мс, можна без переривання роботи перемістити сховище на більш продуктивний рівень, щоб використовувати найефективніші серверні ресурси. Ви можете зробити те ж саме в гіпервізорі (якщо ви використовуєте ESET PROTECT як віртуальну машину).

Рекомендації щодо налаштування розмірів для різної кількості клієнтів

Нижче наведено результати роботи для віртуального середовища, в якому протягом року працює задана кількість клієнтів.

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

Ядра ЦП	Тактова частота ЦП (ГГц)	ОЗП (ГБ)	Продуктивність		
			10 000 клієнтів	20 000 клієнтів	40 000 клієнтів
8	2.1	64	Висока	Висока	Звичайний
8	2.1	32	Звичайний	Звичайний	Звичайний
4	2.1	32	Звичайний	Звичайний	Низька
2	2.1	16	Низька	Низька	Недостатньо
2	2.1	8	Дуже низька (не рекомендовано)	Дуже низька (не рекомендовано)	Недостатньо

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

Кількість клієнтів	До 1000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	100.000+
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

* Щоб не заповнювати базу даних ESET PROTECT, ми не рекомендуємо використовувати цей сценарій, якщо ви використовуєте ESET Enterprise Inspector.

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 5.000 клієнтів становить вісім хвилин, відбувається 5.000 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 інсталювати ESET PROTECT для Linux або віртуальний пристрій, де це можливо.

Віддалені офіси з проксі-серверами

Якщо клієнтські комп'ютери 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 інсталювати у 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.

> 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 (ВМ 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)	Продуктивність
8	64	Висока
4	32	Звичайний
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.

ESET PROTECT 9.0 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.
- Інсталятор автоматично генерує випадковий пароль для автентифікації бази даних (зберігається в *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

⚠ 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 або великих мережах;
- якщо ESET PROTECT буде використовуватися з ESET Enterprise Inspector.

Підтримувані сервери баз даних і з’єднувачі з базою даних

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

ESET PROTECT не підтримує MariaDB. 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	• Випуски Express і випуски, відмінні від Express • 2014, 2016, 2017, 2019	• Сервер SQL • SQL Server Native Client 10.0 • Драйвер ODBC для SQL Server 11, 13, 17
MySQL	• 5.6* • 5.7 • 8.0	Версії драйвера ODBC для MySQL: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27 (тільки для Windows)

* Підтримку MySQL 5.6 припинено в лютому 2021 року. Рекомендуємо оновити сервер бази даних MySQL до версії 5.7 або новішої.

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 новіших 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 може обслуговувати значно більшу кількість клієнтів, ніж з MySQL.

Ви можете інсталювати сервер бази даних SQL на:

- Той самий комп’ютер, на якому інстальовано сервер ESET PROTECT.
- На тому ж комп’ютері, проте на окремому диску.
- 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	✔	
MySQL	✔	✔	10.000	✔	✔

Додаткова інформація

Сервер ESET PROTECT не використовує вбудовану функцію резервного копіювання. Настійно рекомендується створити резервну копію сервера бази даних, щоб запобігти втраті даних.

- Не інсталюйте SQL Server у контролері домену (наприклад, 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).

- 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.

- 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 тільки Apache Tomcat 9.x (64-розрядна версія). Рекомендуємо використовувати останню версію Apache Tomcat 9.x.

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

Java

Apache Tomcat потребує 64-розрядної версії Java/OpenJDK.

Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

> ⚠ 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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

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

- 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 9.0

Продукт	Версія продукту
ESET Endpoint Security для Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus для Windows	7.x, 8.x, 9.x
ESET Endpoint Security для macOS	6.8+
ESET Endpoint Antivirus для macOS	6.8+
ESET Endpoint Security для Android	2.x

Продукт	Версія продукту
ESET Server Security для Windows	8.x
ESET File Security для Microsoft Windows Server	7.x
ESET File Security для Microsoft Azure	7.x
ESET Mail Security для Microsoft Exchange Server	7.x, 8.x, 9.x
ESET Security для Microsoft SharePoint Server	7.x, 8.x, 9.x
ESET Mail Security для IBM Domino Server	7.x, 8.x, 9.x
ESET File Security для Linux	7.x, 8.x
ESET Server Security для Linux	8.1+
ESET Endpoint Antivirus для Linux	7.x, 8.x, 9.x
ESET Dynamic Threat Defense	
ESET Enterprise Inspector Agent	1.6
ESET Full Disk Encryption для Windows	
ESET Full Disk Encryption для macOS	

Старіші версії продуктів ESET, якими можна керувати за допомогою ESET PROTECT 9.0

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

* Неможливо керувати цим продуктом за допомогою агента ESET Management версії 9. Для керування продуктом використовуйте агент ESET Management версії 8.1 або попередніх версій.

ESET PROTECT 9 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 Server Security для Windows	8.0
ESET Server Security для Linux	8.1
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

Мова	Код
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 інстальовано 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

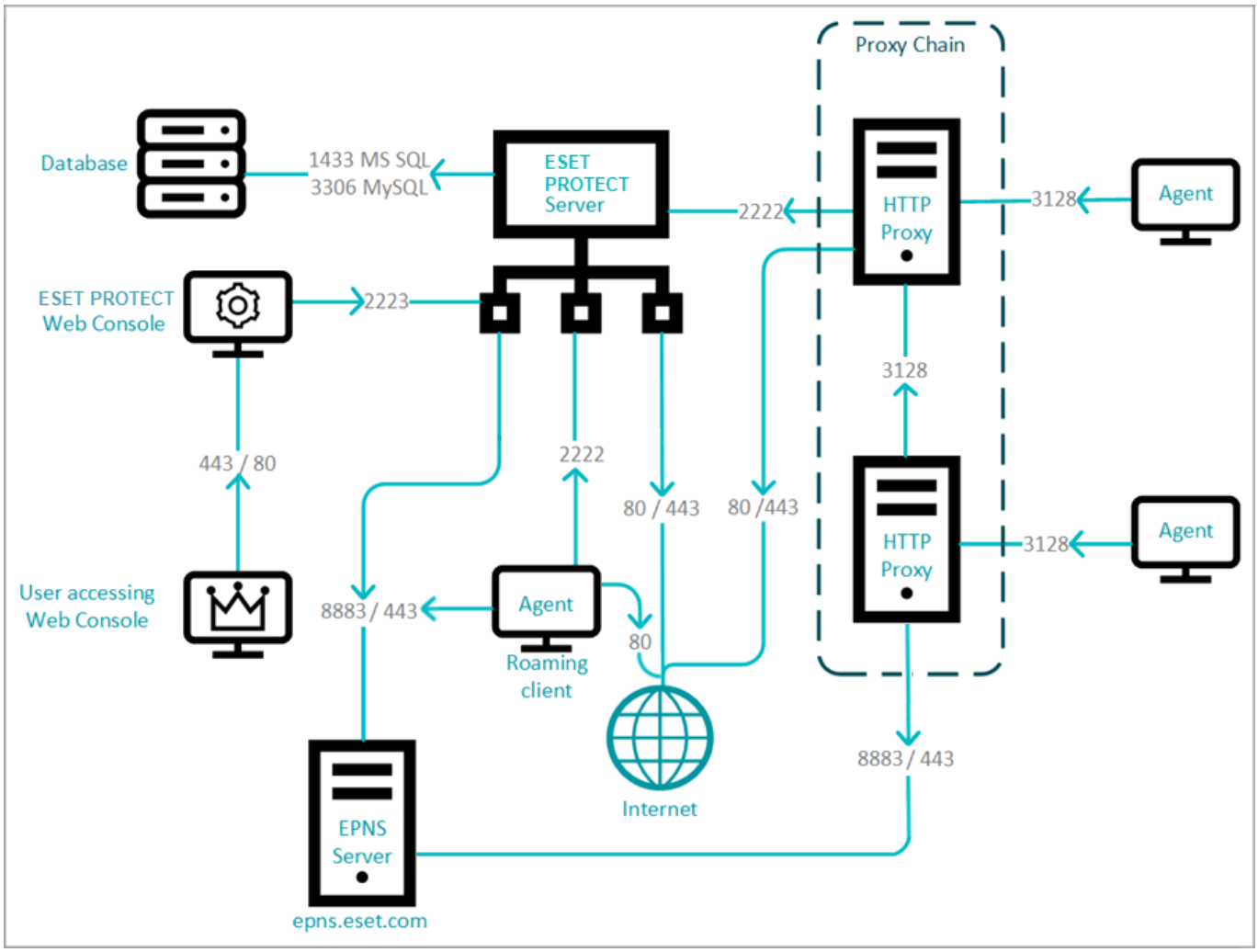
Щоб вирахувати загальний трафік, створений агентами ESET Management, скористайтеся цією формулою:

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

Якщо ви використовуєте ESET Enterprise Inspector, агент ESET Enterprise Inspector генерує 2–5 МБ щоденного трафіку (конкретний обсяг залежить від кількості подій).

Використовувані порти

Сервер ESET PROTECT можна інсталювати 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 інстальовано в інфраструктурі. Інші процеси обміну даними виконуються за допомогою рідних процесів операційної системи (наприклад, NetBIOS over TCP/IP).

> Для належної роботи ESET PROTECT іншим програм не слід використовувати наведені нижче порти.
> Щоб дозволити обмін даними через зазначені нижче порти, обов'язково налаштуйте брандмауер(и) мережі.

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: • 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

Протокол	Порт	Описи
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)

Rogue Detection (RD) Sensor

Протокол	Порт	Описи
TCP	22, 139	Виявлення операційної системи з використанням протоколів SMB (TCP 139) і SSH (TCP 22).
UDP	137	Визначення імені хоста комп'ютера з використанням NetBIOS.

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 (*gateway.push.apple.com*) ESMC версій до 7.2.11.1 (включно)
TCP	2196	Служба Apple Feedback (*feedback.push.apple.com*) ESMC версій до 7.2.11.1 (включно)
HTTPS	2197	• Сповіщення й відповідь Apple Push (*api.push.apple.com*) 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

Протокол	Порт	Описи
TCP	9981	Обмін даними з мобільним пристроєм
TCP	5223	Зовнішній обмін даними зі службою push-сповіщень Apple (iOS)
TCP	443	• 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 інстальовано 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	• 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.

Процес інсталяції

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). Інструкції щодо оновлення наявної інсталяції ESET PROTECT див. у розділі Процедури оновлення.

Інсталятори ESET PROTECT доступні в розділі Завантажити ESET PROTECT на сайті ESET. Для різних способів інсталяції доступні різні формати інсталяторів. За замовчуванням обрано вкладку **Універсальний інсталятор**. Перейдіть на потрібну вкладку, щоб завантажити віртуальний пристрій або окремий інсталятор. Доступні наступні файли:

- Універсальний інсталятор ESET PROTECT для Windows у форматі ZIP.
- Образ у форматі ISO, що містить усі інсталятори 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

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.

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

Див. також розділ Обладнання та налаштування розмірів інфраструктури.

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

Інсталювати програму ESET PROTECT можна кількома способами. Виберіть тип інсталяції, яка найкраще підходить для ваших потреб і середовища. Найпростіший спосіб – скористатись універсальним інсталятором ESET PROTECT. За цим способом можна інсталювати ESET PROTECT і компоненти продукту на одному комп'ютері.

Інсталяція компонентів дає змогу налаштовувати інсталяцію й інсталювати кожен компонент ESET PROTECT на окремому комп'ютері за умови, що він відповідає системним 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

- ESET PROTECTСервер
- Веб-консоль ESET PROTECT — Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери.
- Агент ESET Management (має бути інстальовано на клієнтських комп'ютерах, за бажанням також на сервері ESET PROTECT)

Додаткові компоненти

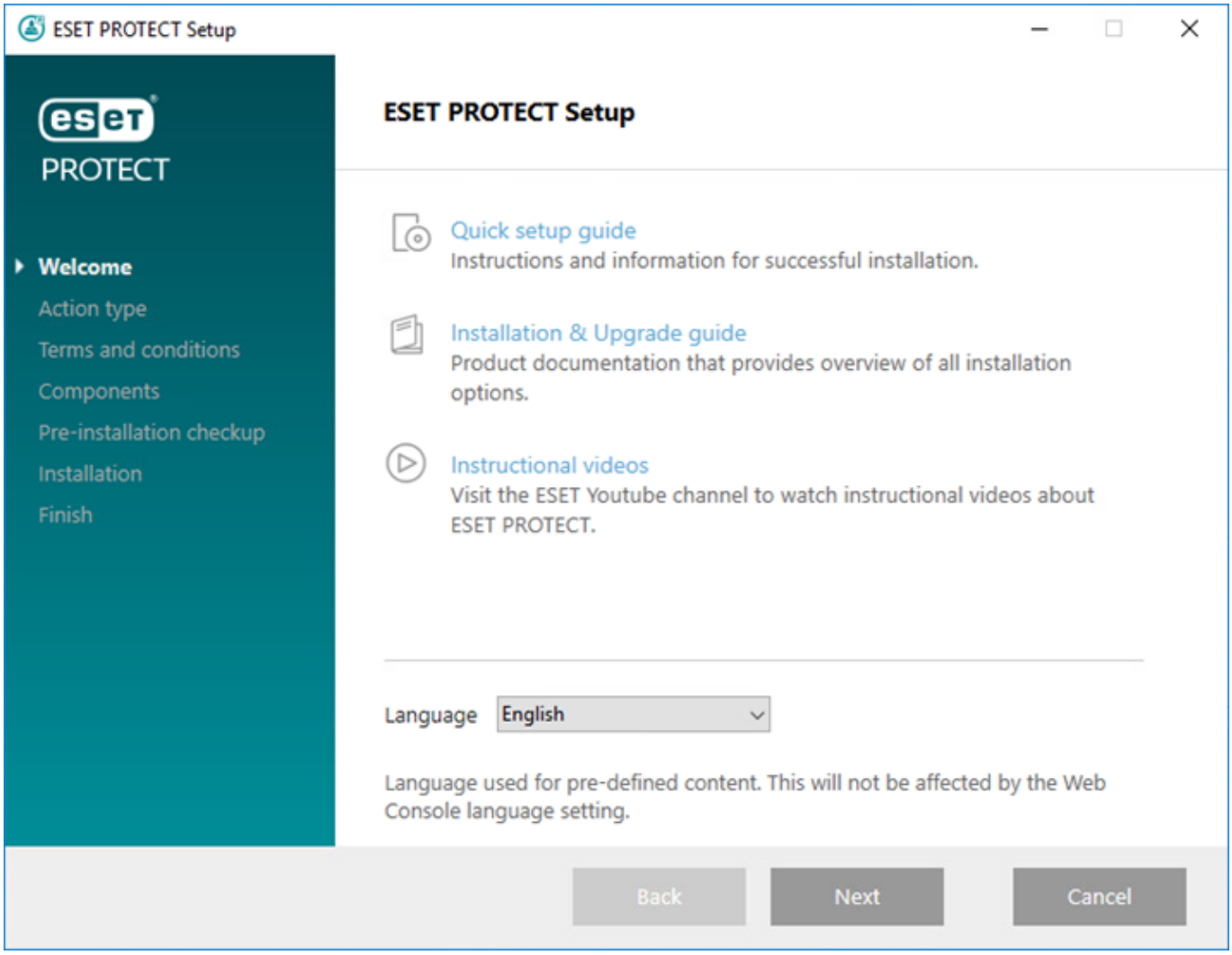
- RD Sensor
- Mobile Device Connector
- Проксі-сервер Apache HTTP
- Інструмент «Дзеркало»

Інструкції з оновлення ESMC до останньої версії ESET PROTECT 9.0 див. за цим посиланням щодо процедур оновлення.

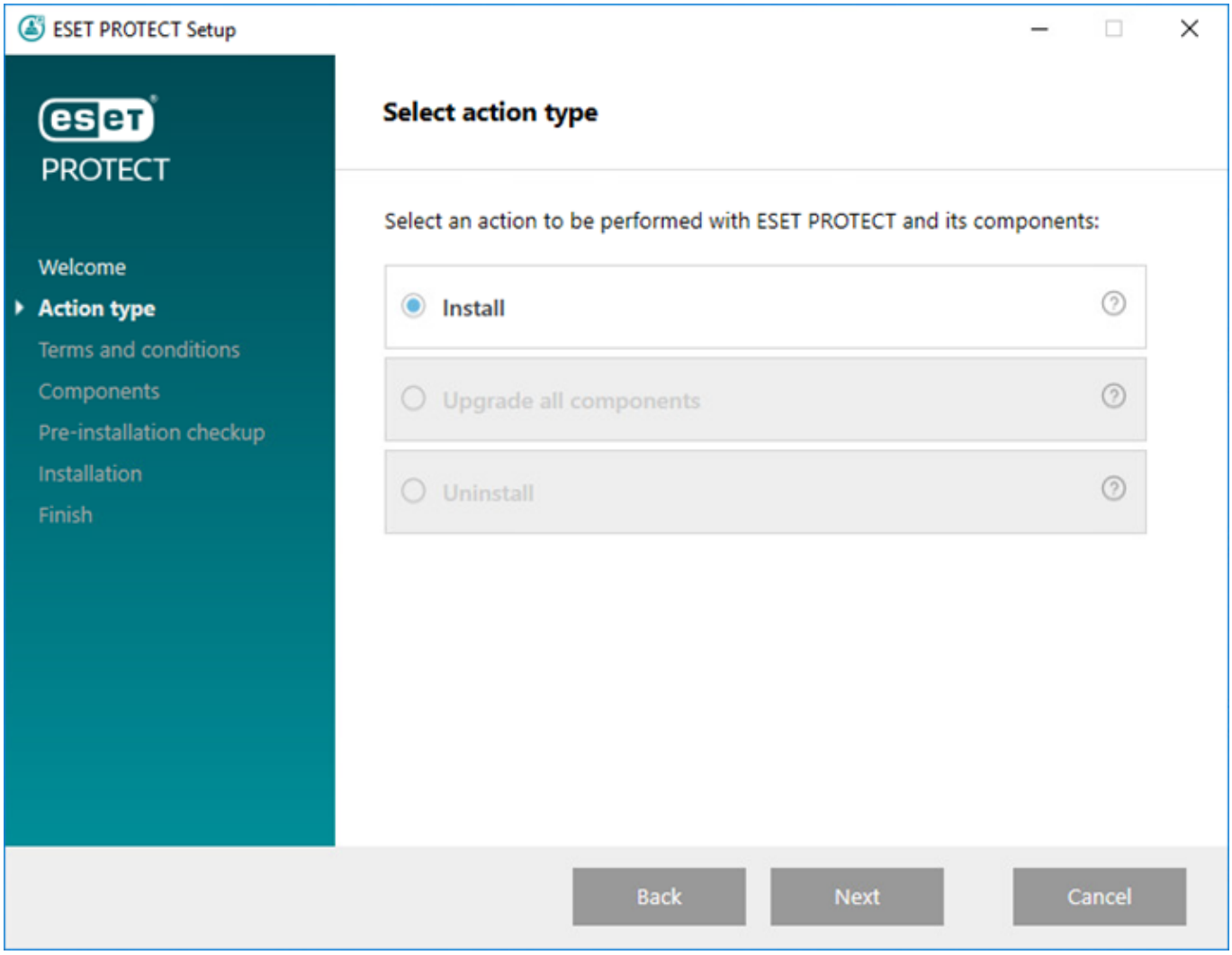
Інсталяція сервера ESET PROTECT

Універсальний інсталятор ESET PROTECT доступний лише для операційних систем Windows. Він дає змогу інсталювати 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 ESET звіти про аварійне завершення роботи та анонімні дані телеметрії (тип і версія ОС, версія продукту ESET та інші дані про продукт), зніміть прапорець **Взяти участь у програмі удосконалення продуктів**. 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 9.0 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.

  - Інсталятор автоматично генерує випадковий пароль для автентифікації бази даних (зберігається в *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

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 або великих мережах;
- якщо ESET PROTECT буде використовуватися з ESET Enterprise Inspector.

- Якщо в системі вже інстальовано іншу підтримувану версію Microsoft SQL Server чи MySQL або ви плануєте підключатися до іншого сервера SQL Server, зніміть прапорець **Microsoft SQL Server Express**.

- Не інсталюйте SQL Server у контролері домену (наприклад, 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 не вибрати цей параметр, інсталятор автоматично згенерує нове сховище ключів для Tomcat (самопідписаний сертифікат HTTPS).

Проксі-сервер Apache HTTP

Опцію **Проксі-сервер Apache HTTP** призначено лише для невеликих або централізованих мереж без переміщуваних клієнтів. Якщо вибрати цей параметр, інсталятор налаштує клієнти на тунельний обмін даними з ESET через проксі-сервер, інстальований на тому самому комп'ютері, що й 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 інсталювати 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 інсталювати проксі-сервер Apache HTTP, а також створити й застосувати політики (під назвою **Використання проксі-сервера HTTP**; застосовуються до групи **Усі**) для таких продуктів:

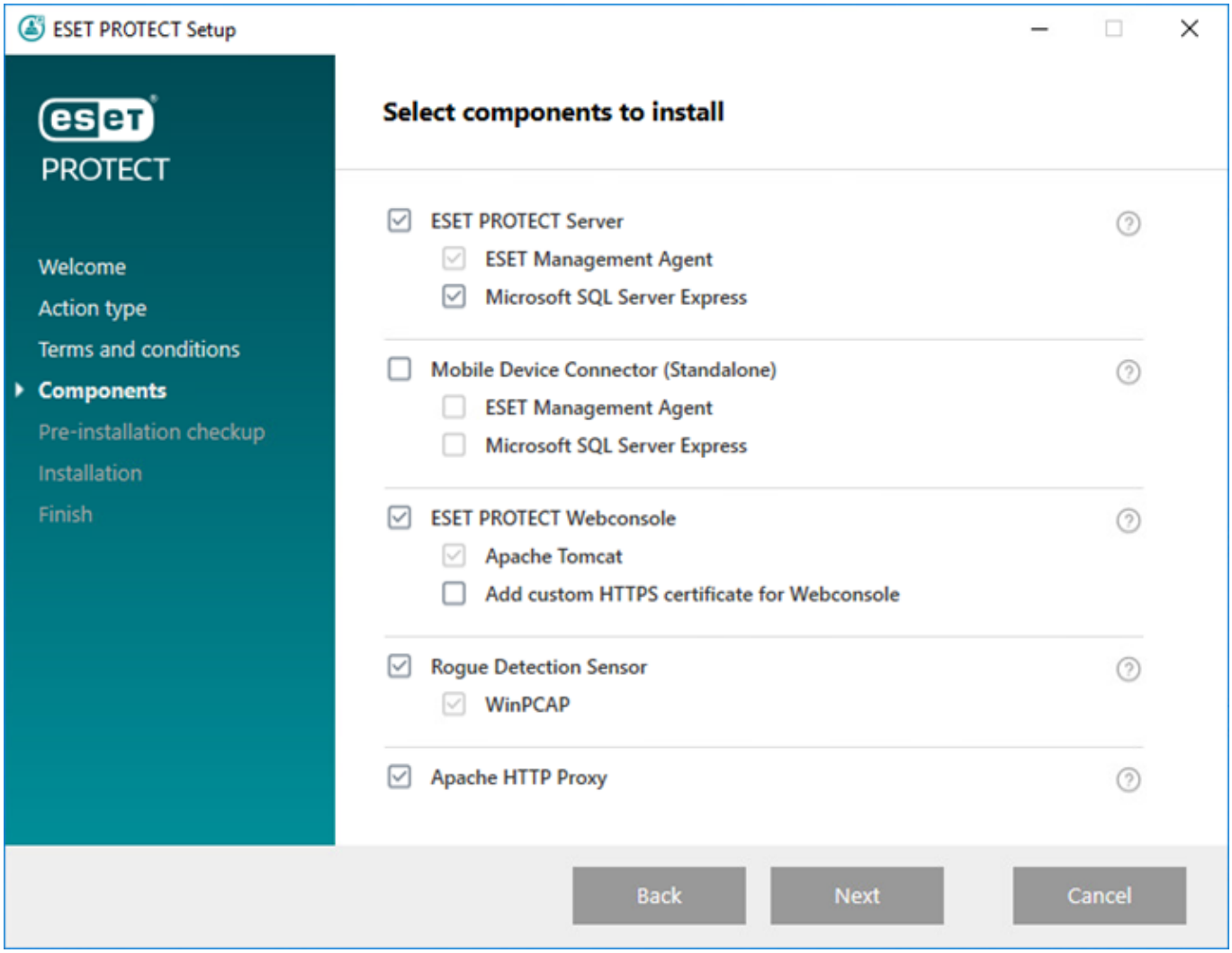
  - ESET Endpoint для Windows

  - ESET Endpoint для macOS (OS X) і Linux

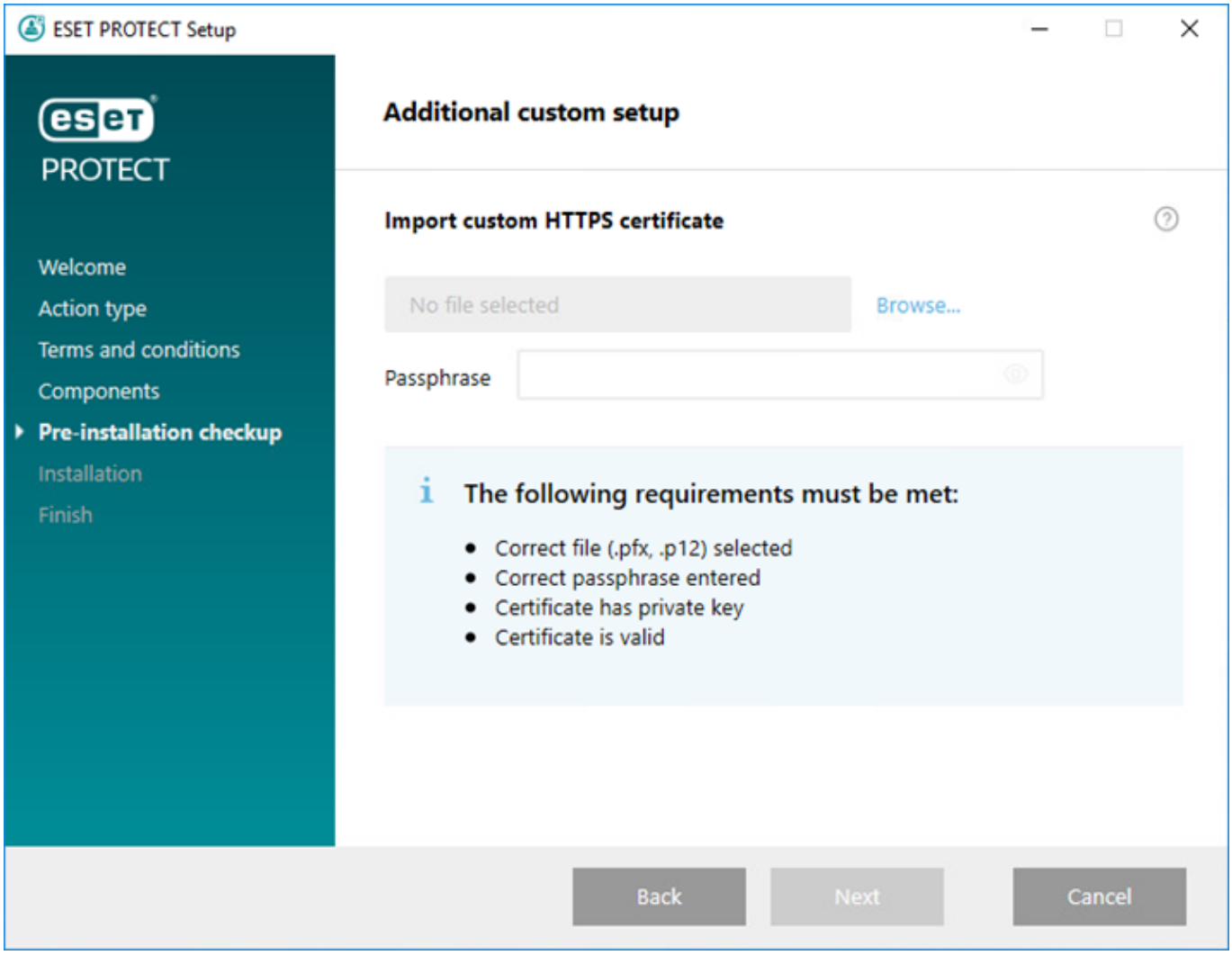
  - ESET Management Agent

- ESET File Security для Windows Server (6+)
- ESET Server Security для Windows (8+)
- ESET 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 вимкнуто. Якщо потрібно налаштувати інші продукти, ви можете скопіювати ці параметри в іншу політику.



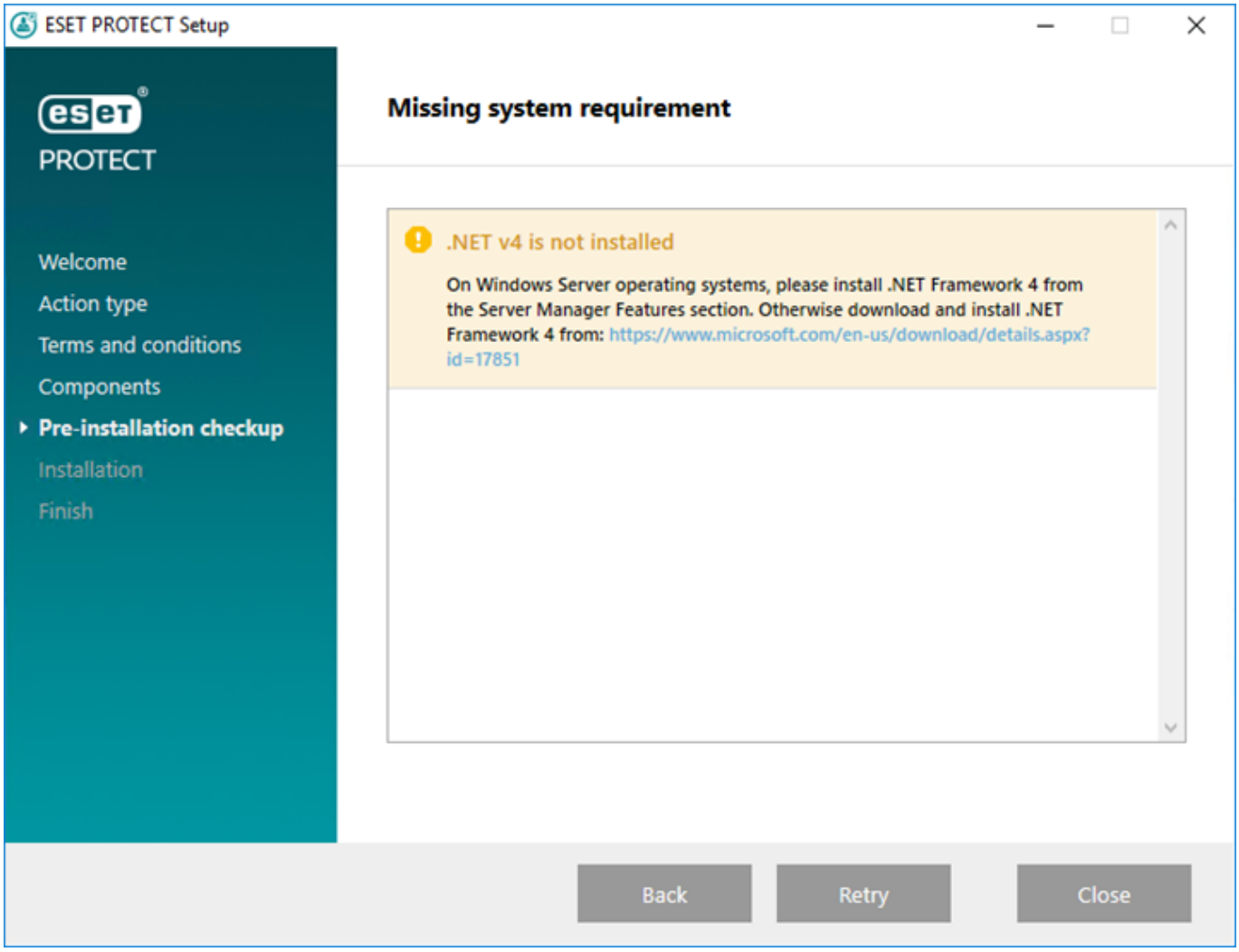
5. Якщо ви вибрали **Додати користувацький сертифікат HTTPS для веб-консолі**, натисніть **Огляд**, виберіть дійсний сертифікат (файл із розширенням *.pfx* або .p12) і введіть його **парольну фразу** (якщо її немає, залиште це поле порожнім). Інсталятор інсталює сертифікат для доступу до веб-консолі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



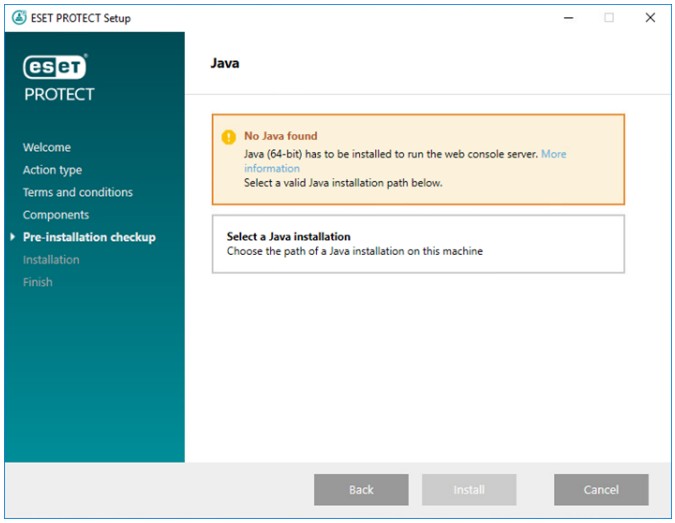
6. Якщо під час перевірки попередніх вимог виявлено помилки, усуньте їх. Переконайтеся, що система відповідає всім вимогам.

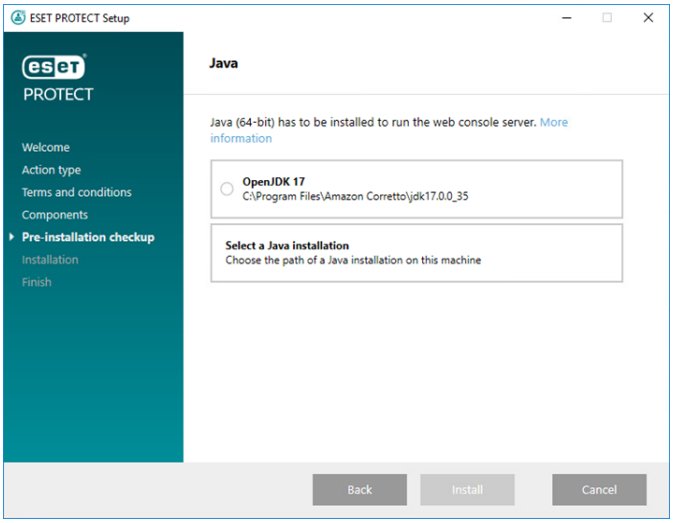
.NET версії 4 не інстальовано

Інсталюйте NET Framework



Не вдалося знайти Java або не вдалося виявити Java (64-розрядна версія)





Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

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

b)Натисніть **Інсталювати**, щоб продовжити, або **Змінити**, щоб змінити шлях інсталяції Java.

На системному диску вільно лише 32 МБ

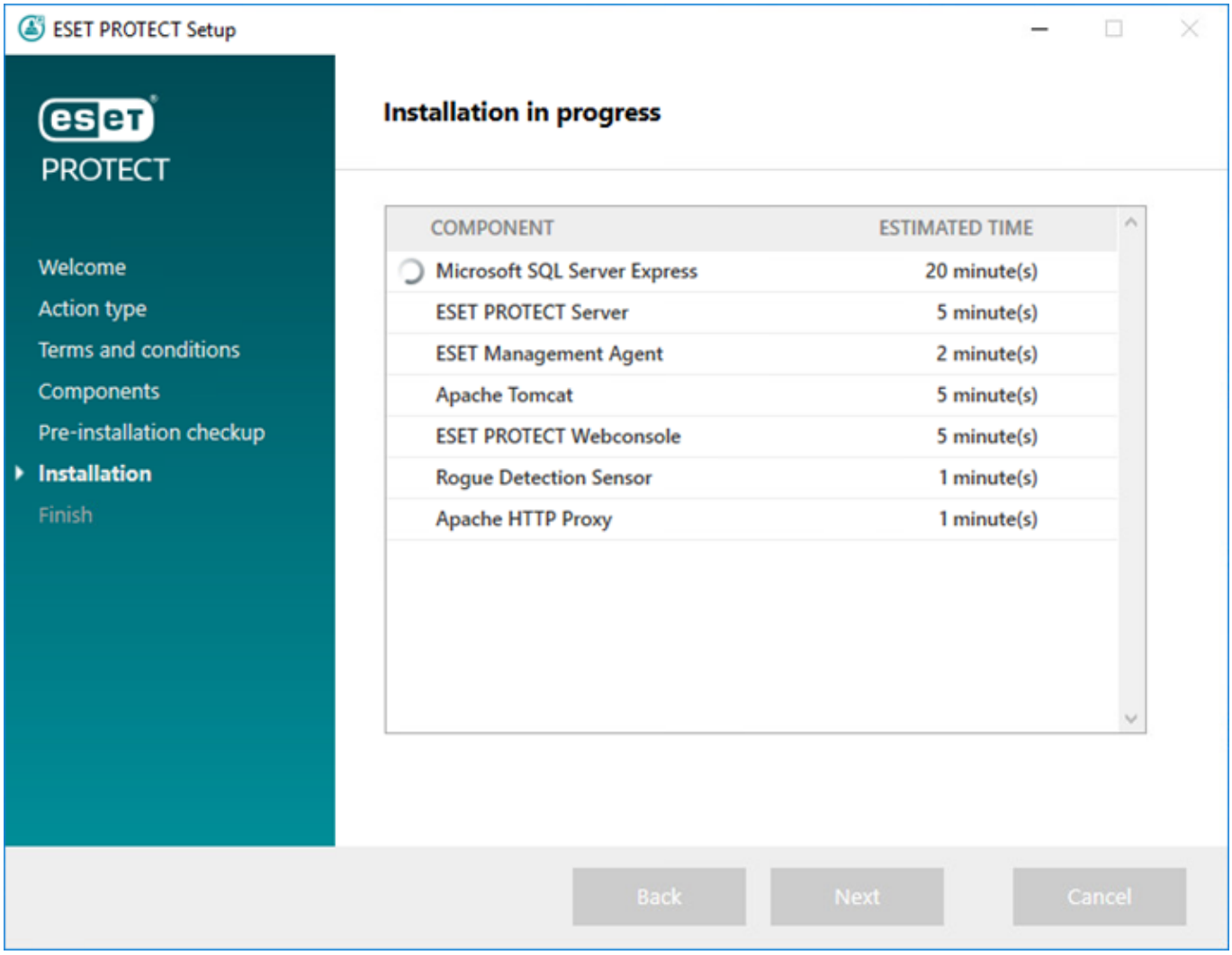
- Інсталятор може повертати це сповіщення, якщо на диску в системі недостатньо місця для інсталяції ESET PROTECT.
- Щоб інсталювати ESET PROTECT та всі компоненти продукту, потрібно мати принаймні 4400 МБ вільного місця на диску.

ESET Remote Administrator 5.x або попередніх версій інстальовано на комп'ютері, який унеможливлює подальше виконання інсталятора.

Пряме оновлення не підтримується: див. тему Перенесення з ERA 5.x або Перенесення з ERA 6.x.

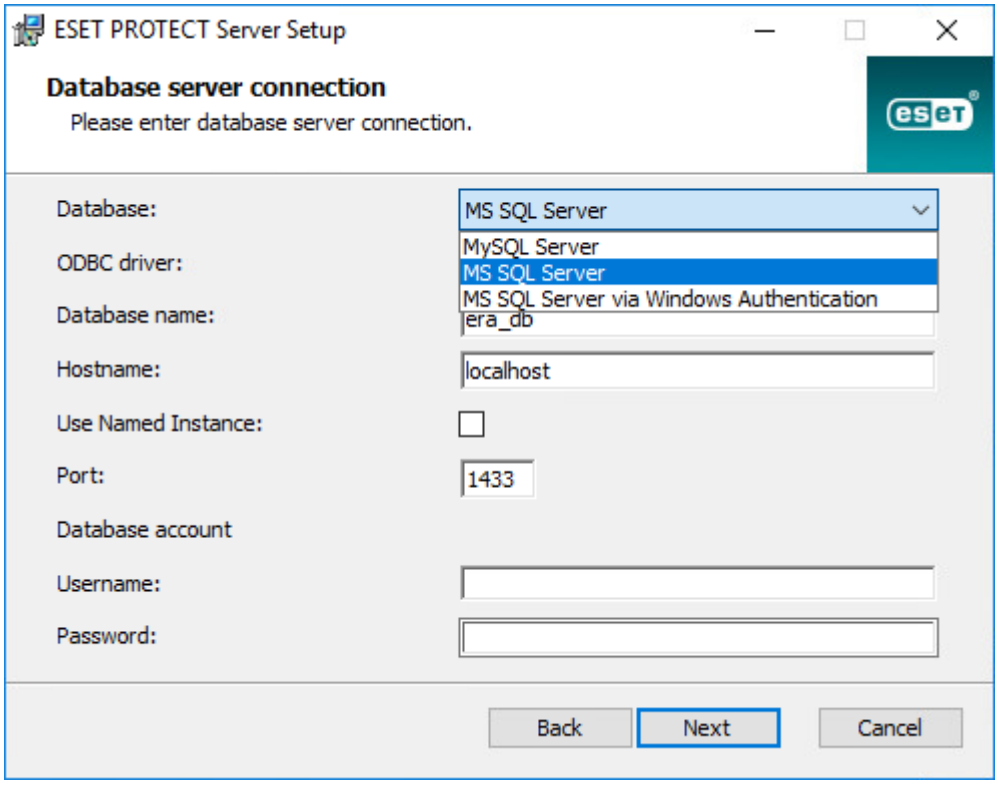
7. Коли завершиться перевірка попередніх вимог і середовище відповідатиме їм, почнеться інсталяція. Зверніть увагу, що інсталяція може тривати понад годину залежно від конфігурації вашої системи та мережі.

Поки триває інсталяція, майстер інсталяції ESET PROTECT не відповідає.



8. Якщо ви інсталюєте **Microsoft SQL Server Express** на кроці 4, інсталятор перевірить підключення до бази даних. Якщо у вас є сервер бази даних, інсталятор запропонує ввести дані для підключення до бази даних:

[Налаштування підключення до сервера SQL/MySQL]

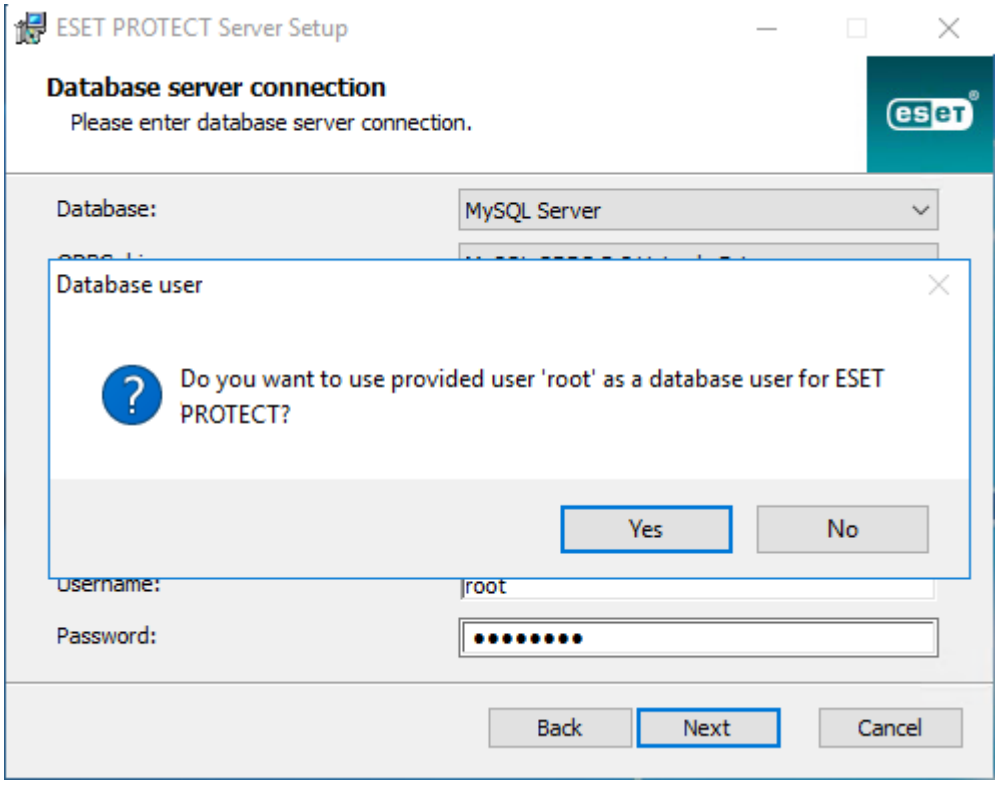


Введіть **назву бази даних**, **ім'я хоста**, **номер порту** (ця інформація доступна в диспетчері конфігурацій Microsoft SQL Server) і дані **облікового запису бази даних** (**ім'я користувача** та **пароль**) у відповідні поля й натисніть **Далі**. Інсталятор підтвердить підключення до бази даних.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

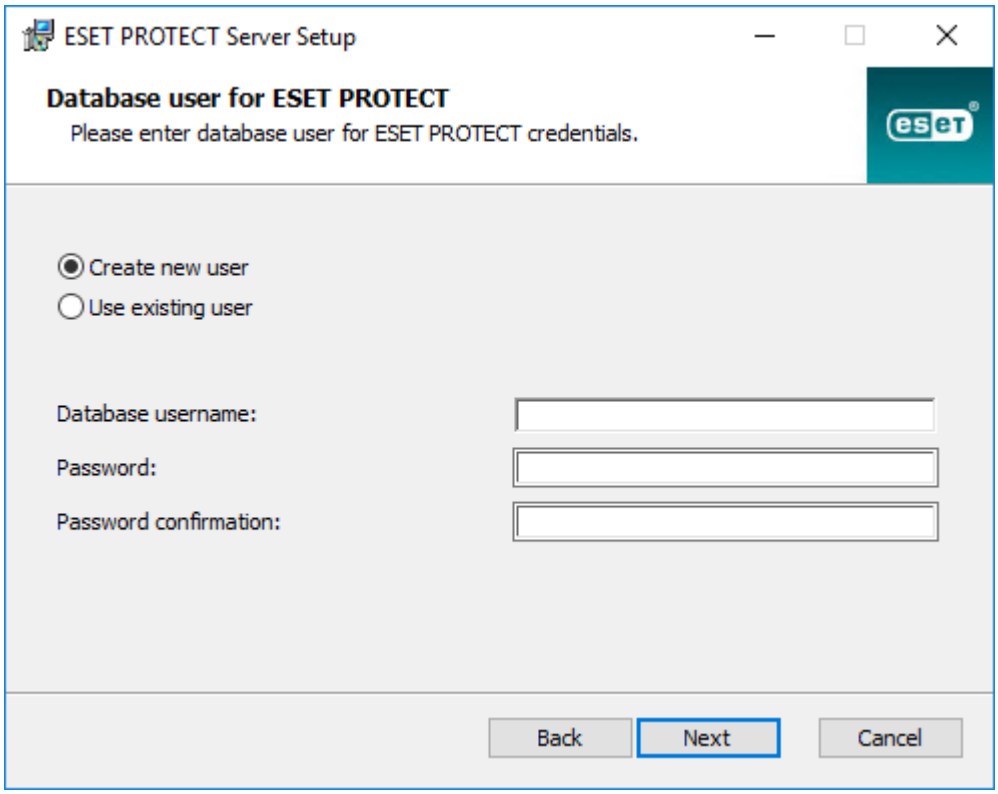
Використовувати екземпляр з іменем: якщо ви використовуєте базу даних MS SQL, можна установити прапорець **Використовувати екземпляр з іменем**, щоб використовувати настроюваний екземпляр бази даних. Його можна задати в полі **Ім'я хоста** у формі *HOSTNAME\DB_INSTANCE* (наприклад, *192.168.0.10\ESMC7SQL*). Для кластерної бази даних використовуйте лише ім'я кластера. Якщо вибрано цей параметр, не можна буде змінити порт підключення до бази даних. Система використовуватиме порти за замовчуванням, визначені Microsoft. Щоб підключити сервер ESET PROTECT до бази даних MS SQL, інстальованій у відмовостійкому кластері, уведіть ім'я кластера в полі **Ім'я хоста**.

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. Більш докладні відомості див. в розділі Спеціальний обліковий запис користувача бази даних. Якщо ви не збираєтеся використовувати спеціальний обліковий запис користувача, укажіть обліковий запис адміністратора (SA або root).

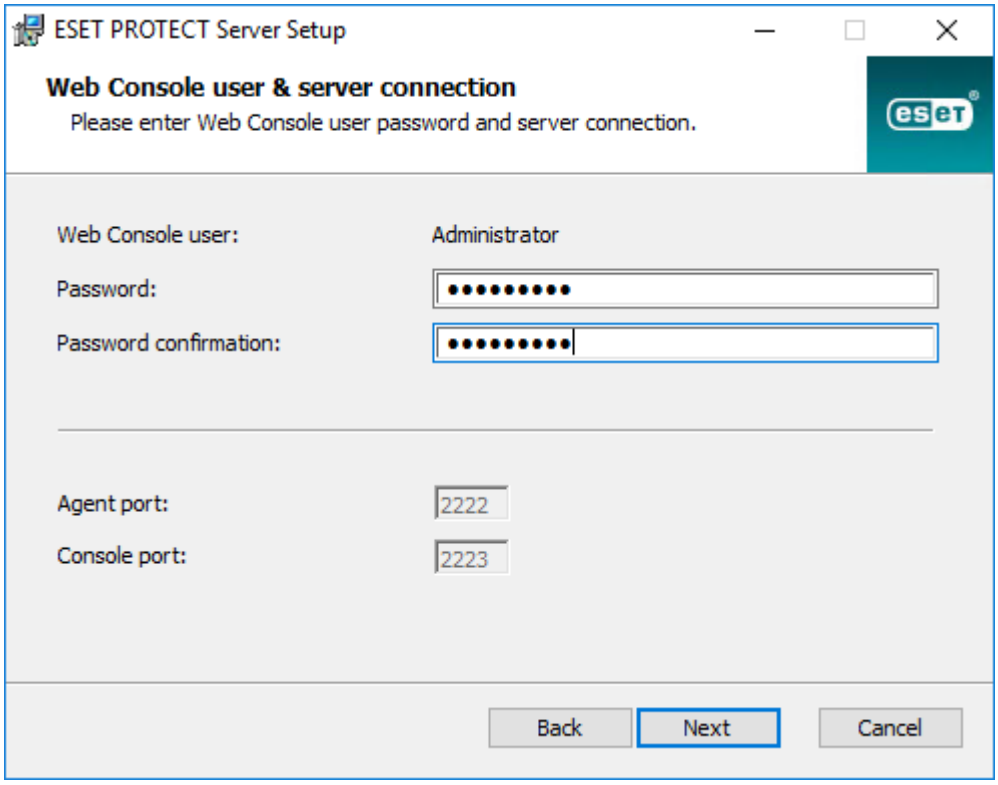
Якщо ви вказали обліковий запис **SA** або **root** у попередньому вікні, натисніть **Так**, щоб продовжити використовувати обліковий запис SA чи root як користувач бази даних для ESET PROTECT.



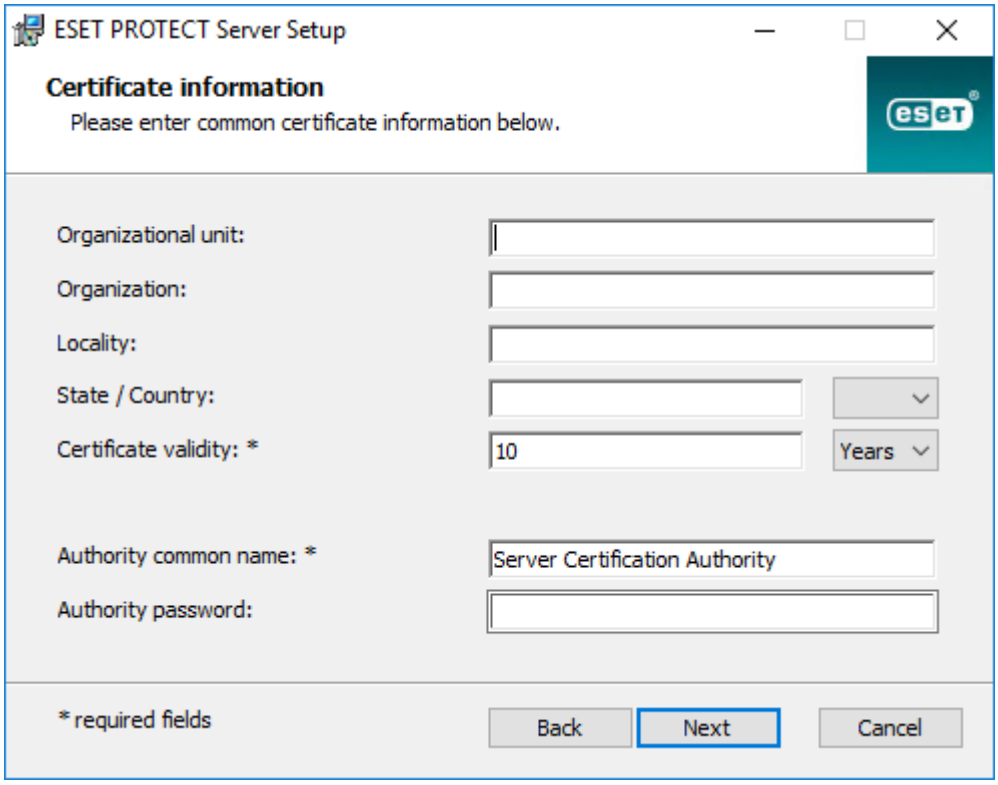
Якщо натиснути **Ні**, потрібно вибрати опцію **Створити нового користувача** (якщо ви ще цього не зробили) або **Використовувати наявного користувача** (якщо у вас є спеціальний обліковий запис користувача бази даних).



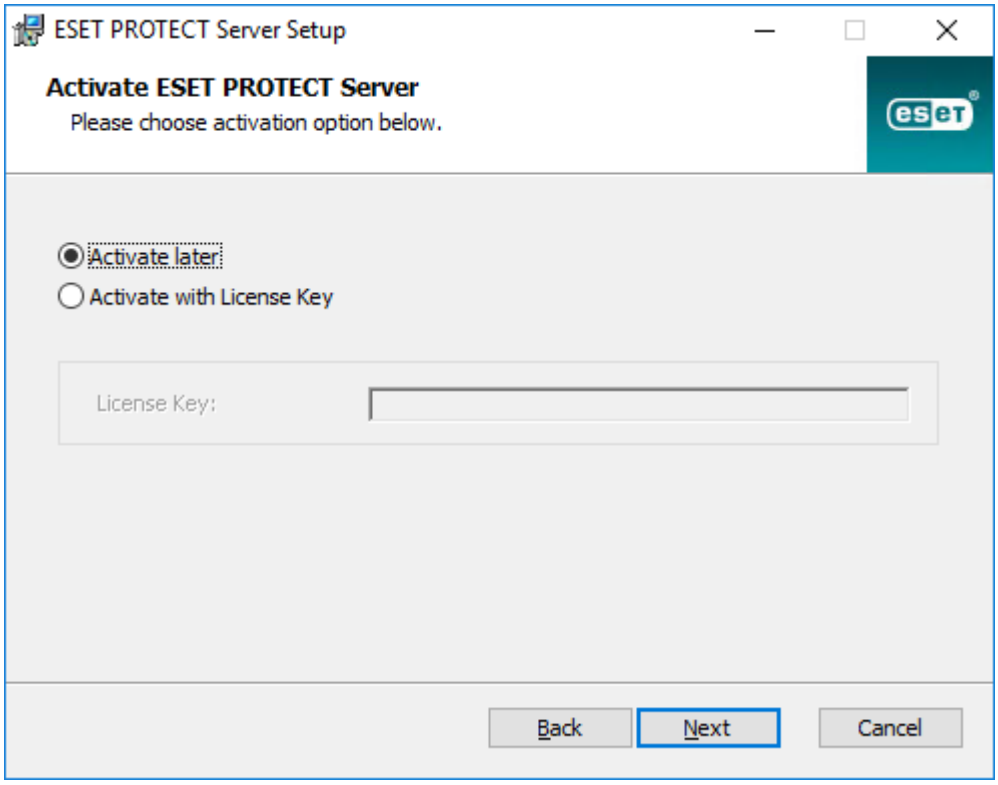
9. Інсталятор запропонує ввести пароль для облікового запису адміністратора веб-консолі. Цей пароль є важливим, оскільки він потрібний для доступу до веб-консолі ESET PROTECT. Натисніть кнопку **Далі**.



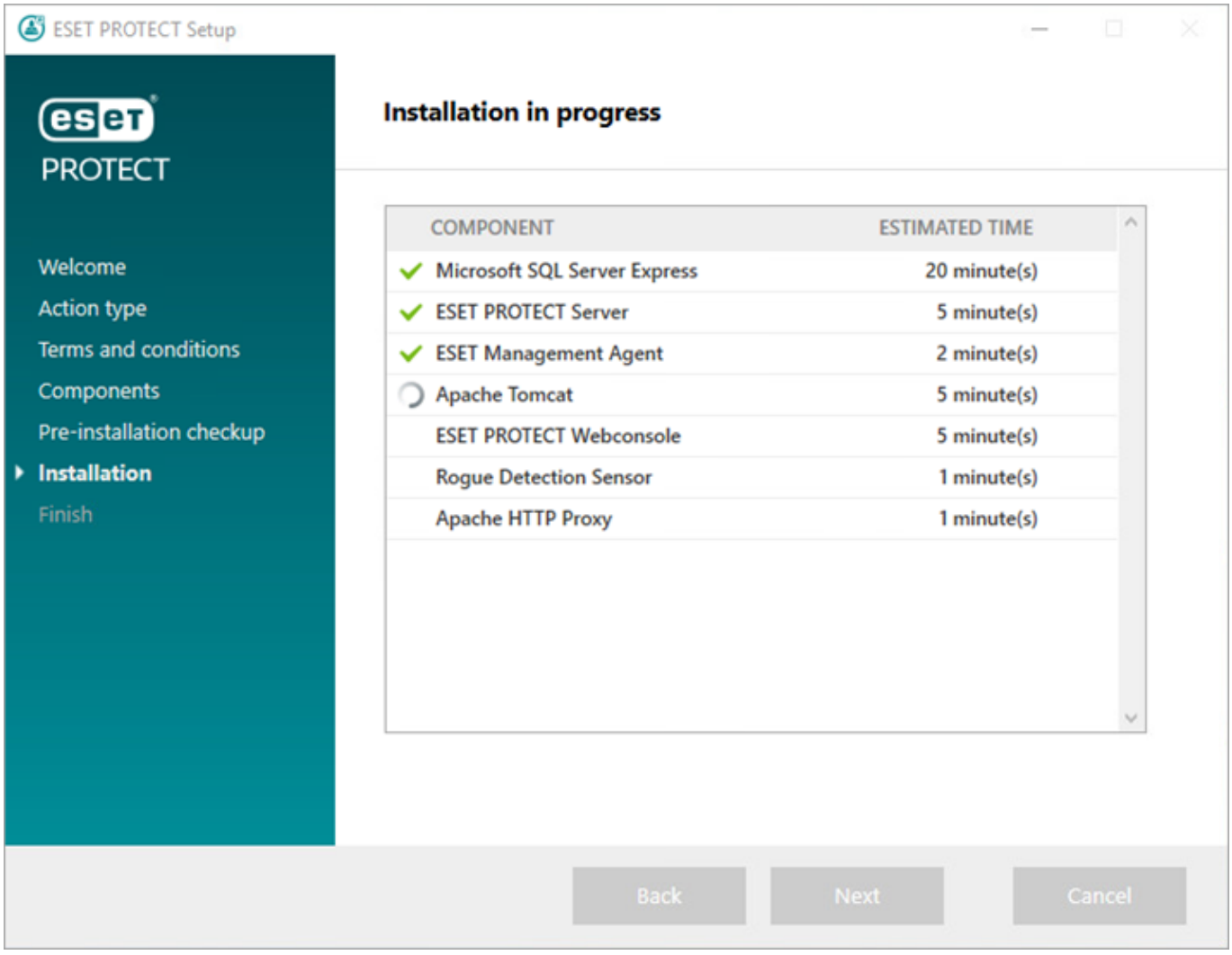
10. Не змінюйте ці поля або введіть у них дані про організацію, що відображатимуться в інформації про сертифікати агента ESET Management і сервера ESET PROTECT. Якщо ви введете пароль у полі **Пароль центра**, обов'язково запам'ятайте його. Натисніть кнопку **Далі**.



11. 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. Крім того, можна вибрати пункт **Активувати пізніше** (додаткові інструкції див. в розділі Активація).



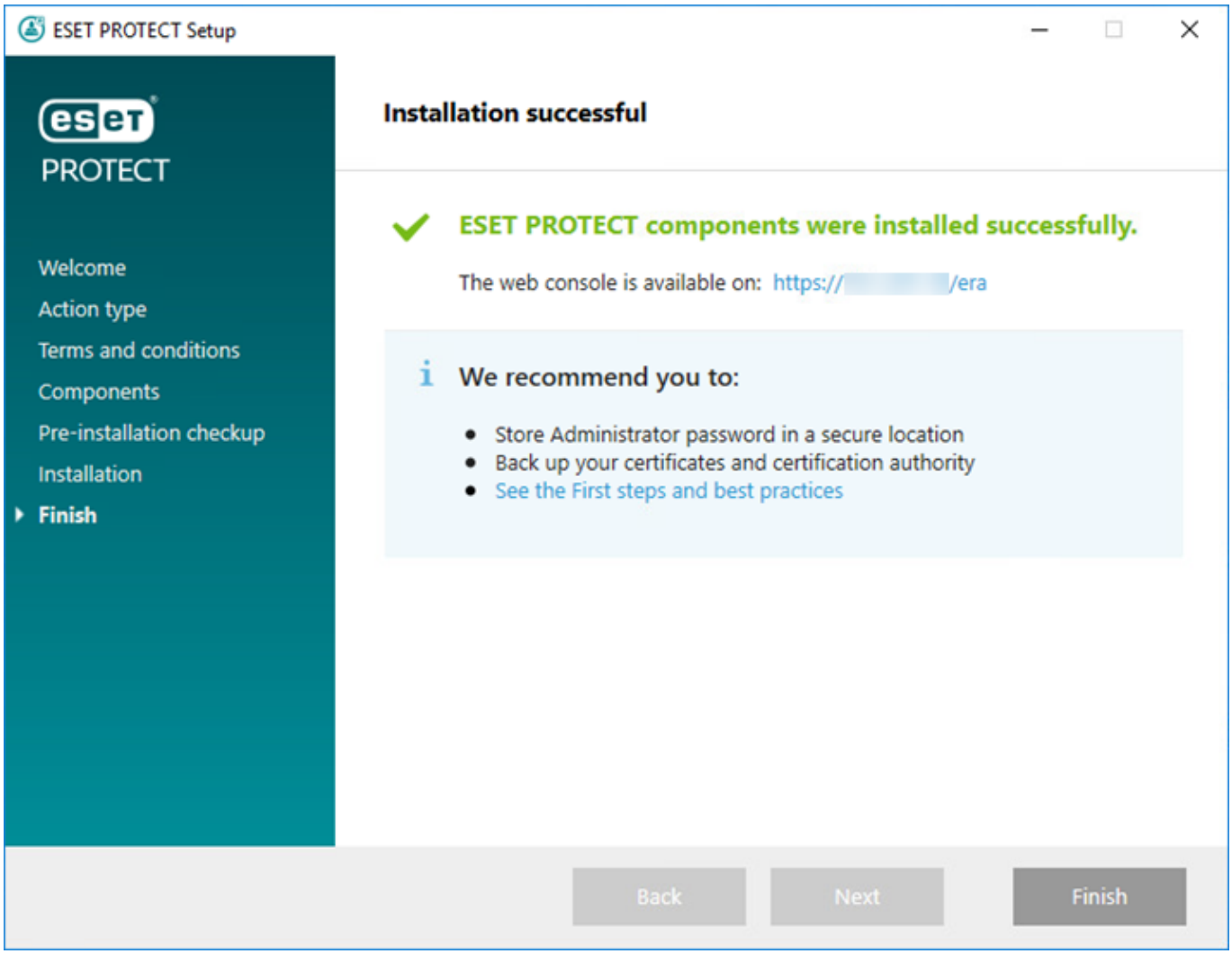
12. Відобразиться хід виконання інсталяції.



13. Якщо ви вибрали інсталяцію **Rogue Detection Sensor**, з’являться вікна інсталяції драйвера

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

14. 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 інсталювати Mobile Device Connector як відокремлений інструмент на комп’ютері без сервера ESET PROTECT, виконайте наступні кроки.

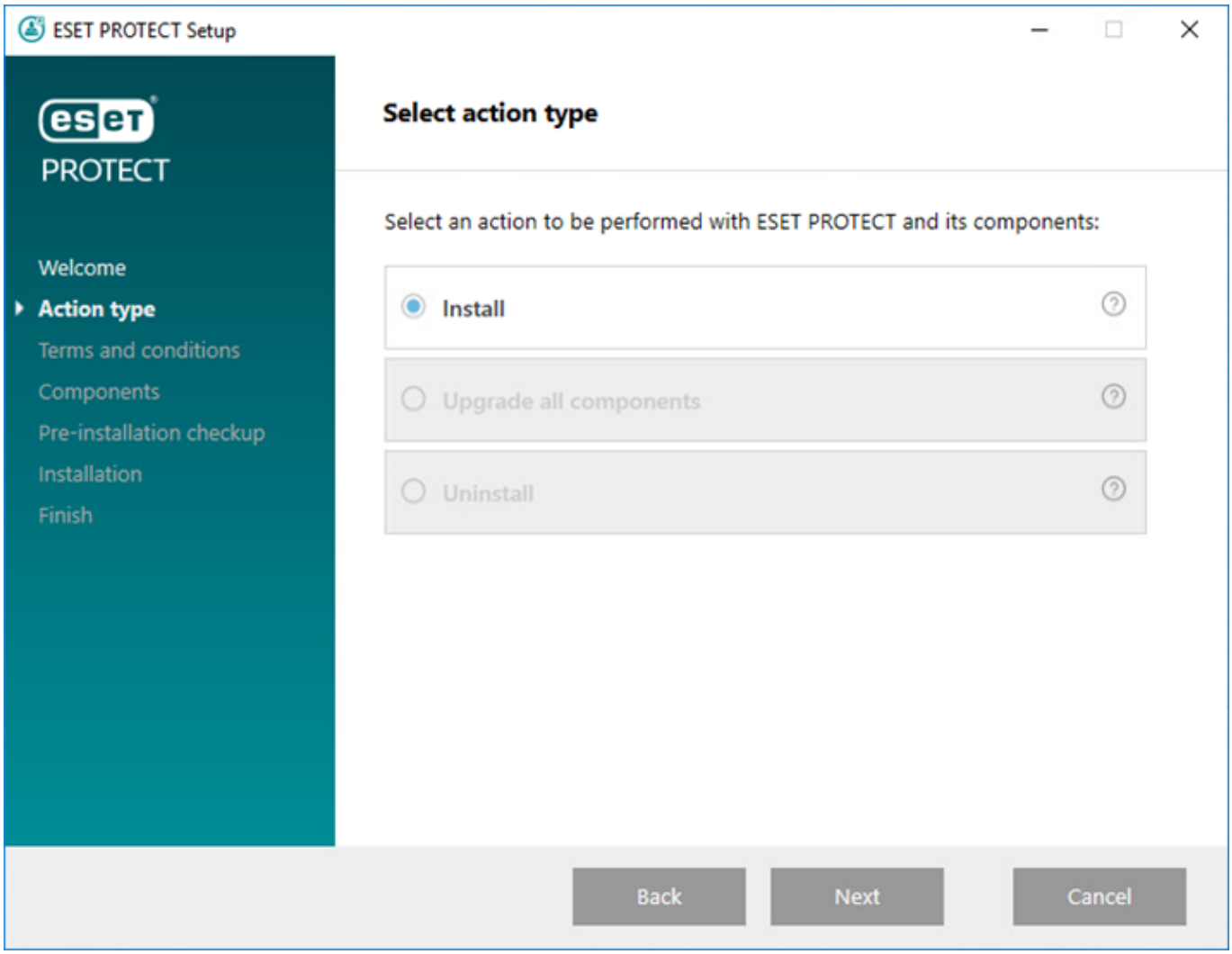
Щоб мобільними пристроями можна було керувати будь-коли незалежно від їхнього місцезнаходження, до Mobile Device Connector має бути доступ через Інтернет.

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 **Інсталювати** та натисніть **Далі**.

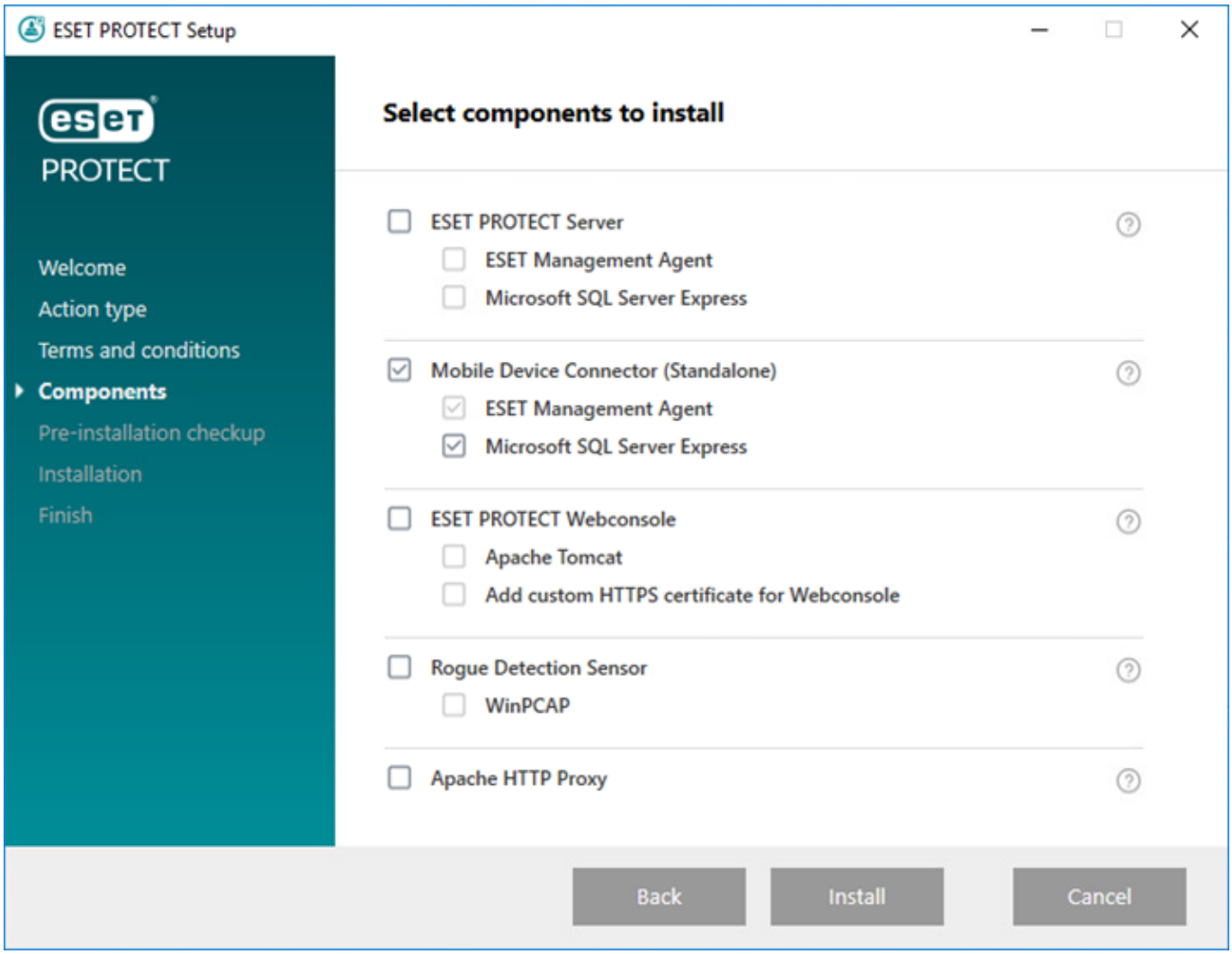


3. Якщо ви не хочете надсилати ESET звіти про аварійне завершення роботи та анонімні дані телеметрії (тип і версія ОС, версія продукту ESET та інші дані про продукт), зніміть прапорець **Взяти участь у програмі удосконалення продуктів**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи 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 **Інсталювати**, щоб розпочати інсталяцію.



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

> 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

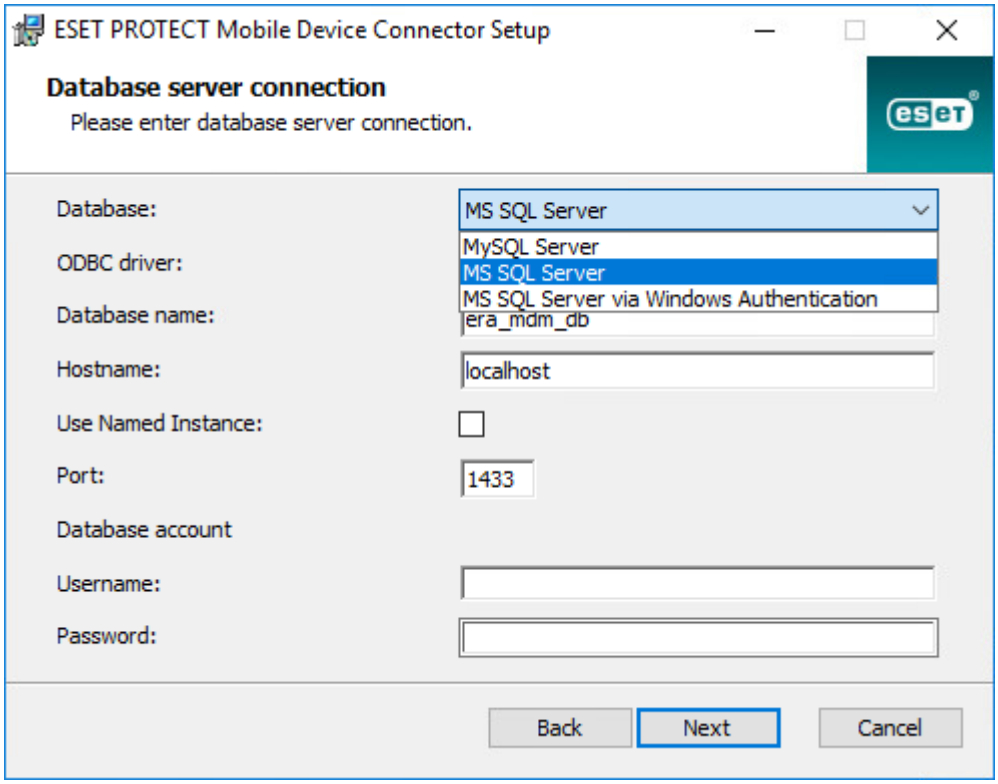
• **Ім’я бази даних**: Рекомендуємо використовувати попередньо встановлене ім’я або змінити його за необхідності.

• **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 установити прапорець **Використовувати екземпляр з іменем**, щоб використовувати настроюваний екземпляр бази даних. Його можна задати 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 вибрано цей параметр, не можна буде змінити порт підключення до бази даних. Система використовуватиме порти за замовчуванням, визначені Microsoft. Щоб підключити сервер ESET PROTECT до бази даних MS SQL, інстальованій у відмовостійкому кластері, уведіть ім’я кластера в полі **Ім’я хоста**.



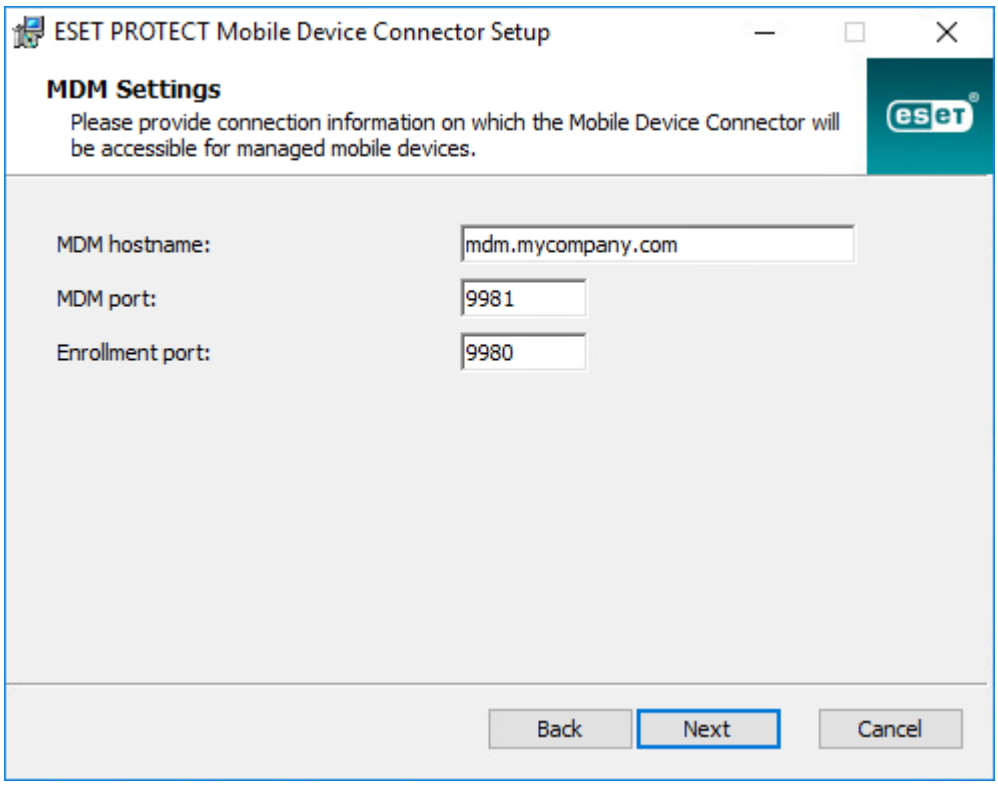
8. Якщо з’єднання було успішним, вам буде запропоновано підтвердити, що ви хочете використовувати вказаного користувача як користувача бази даних для ESET PROTECT MDM.

9. Після інсталяції нової або підключення інсталятора 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 указано повне доменне ім’я (наприклад, `mdm.mycompany.com`), введіть його в полі **Ім’я хоста MDM**. Крім цього, якщо в сертифікаті HTTPS використовується символ

узагальнення * (наприклад, `*.mycompany.com`), ви можете вказати в полі **Ім’я хоста MDM** значення `mdm.mycompany.com`.

> 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 одноранговогo 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.

> 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 погоджуєтеся 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).

> 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, установіть прапорець **Використовувати проксі-сервер**. У цьому разі інсталятор продовжить **інсталяцію в автономному режимі**.

> 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**. Щоб увійти як користувач домену, установіть прапорець поруч із пунктом **Увійти в домен**.

- 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**.
- Для інсталяцій із використанням сервера не можна використовувати користувача з двофакторною автентифікацією.

2. Коли з'явиться запит прийняти сертифікат, натисніть **Так**.

3. Виберіть **Не створювати комп'ютер (він буде створений автоматично під час першого підключення)** або **Виберіть 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**.

- 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.

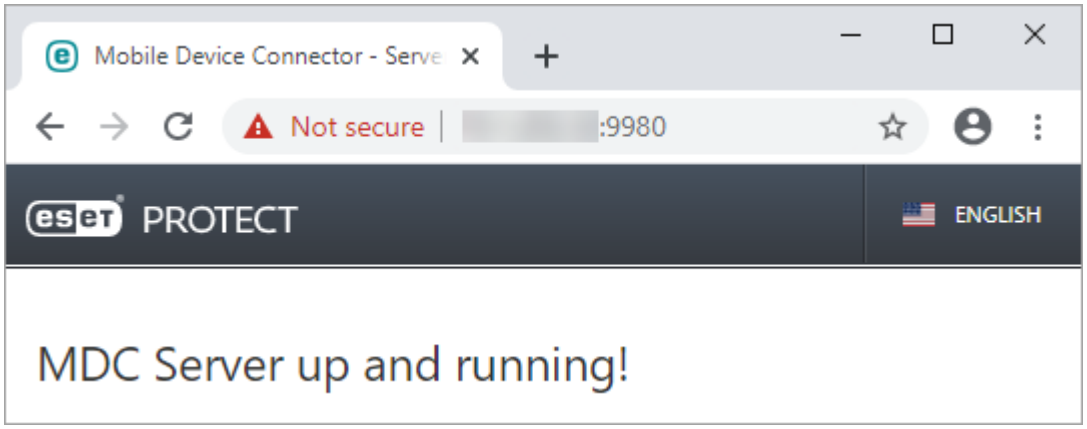
Якщо ви створили налаштовуваний сертифікат з ESET PROTECT (замість сертифікатів за замовчуванням, автоматично згенерованих під час інсталяції ESET PROTECT), використовуйте саме його.

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 9.0. в Azure, дотримуйтесь інструкції з цієї статті бази знань і використовуйте ESET PROTECT 9.0 Універсальний інсталятор. Крім того, ви можете інсталювати ESMC 7.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

- ESET PROTECTСервер
- Веб-консоль ESET PROTECT — Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери.
- Агент ESET Management (має бути інстальовано на клієнтських комп'ютерах, за бажанням також на сервері ESET PROTECT)

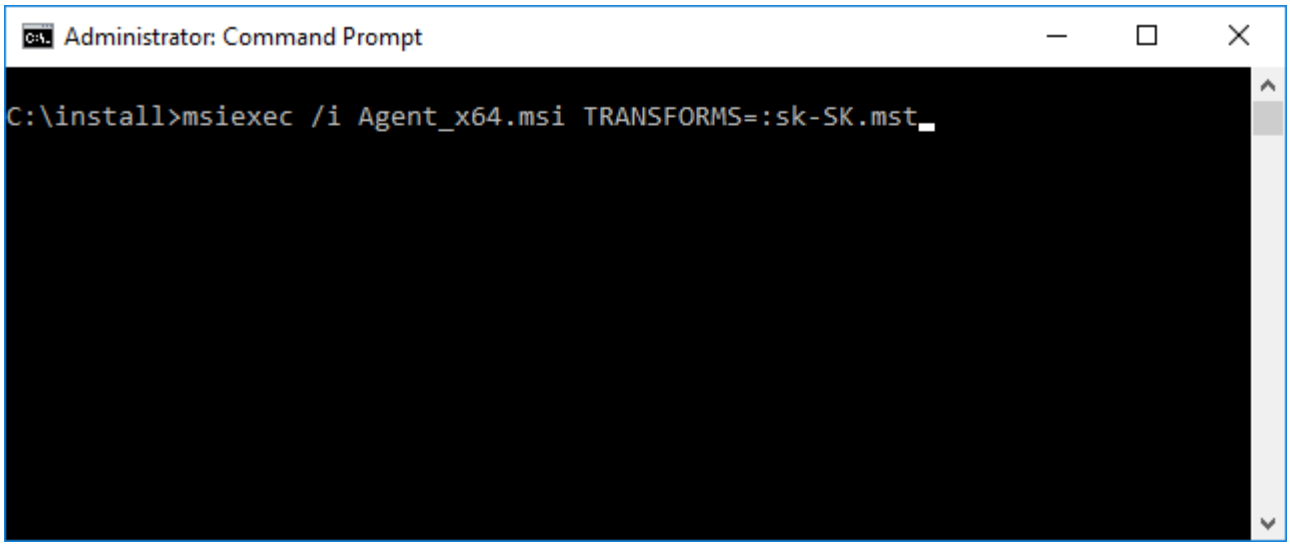
Додаткові компоненти

- RD Sensor
- Mobile Device Connector
- Проксі-сервер Apache HTTP
- Інструмент «Дзеркало»

Інструкції з оновлення ESMC до останньої версії ESET PROTECT 9.0 див. за цим посиланням щодо процедур оновлення.

Щоб інсталяція виконувалася потрібною мовою, запустіть інсталятор MSI відповідного компонента ESET PROTECT за допомогою командного рядка.

Нижче наведено приклад запуску інсталяції словацькою:



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

Мова	Код
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 інсталювати 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 погоджуєтеся з її умовами).

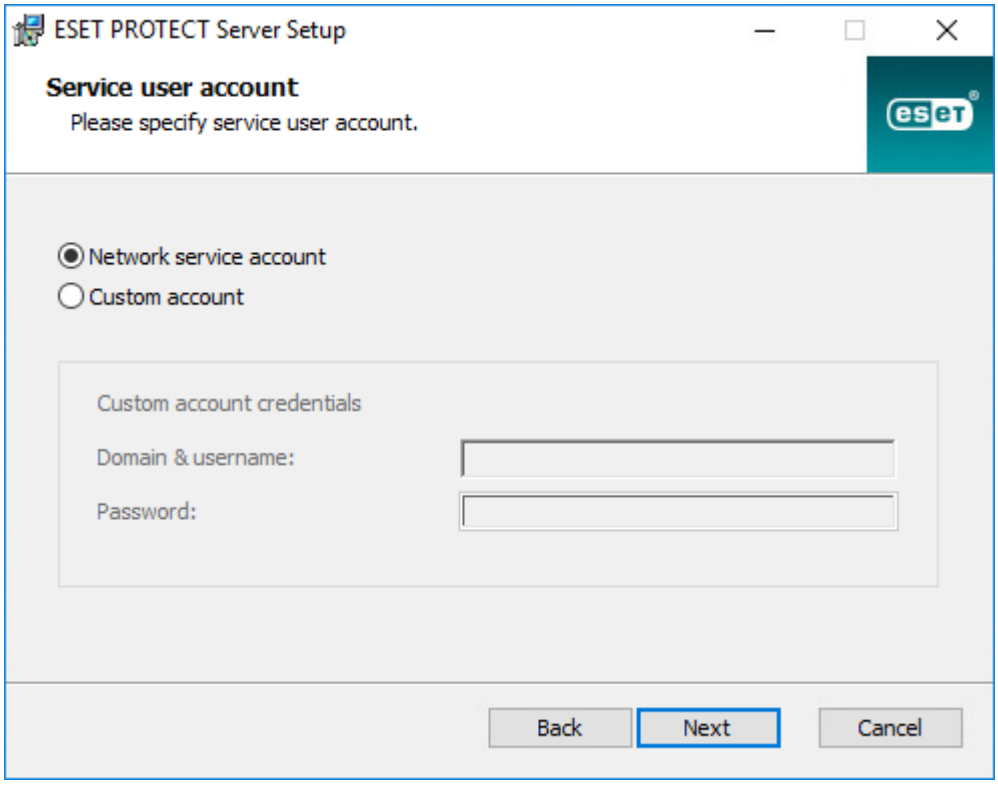
4. Якщо ви не хочете надсилати ESET звіти про аварійне завершення роботи та анонімні дані телеметрії (тип і версія ОС, версія продукту ESET та інші дані про продукт), зніміть прапорець **Взяти участь у програмі удосконалення продуктів**. Якщо не зняти цей прапорець, звіти про аварійне завершення роботи та дані телеметрії надсилатимуться в ESET.

5. Не ставте прапорець біля пункту **Це інсталяція в кластері** та натисніть **Далі**. Ви виконуєте інсталяцію в кластері?

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

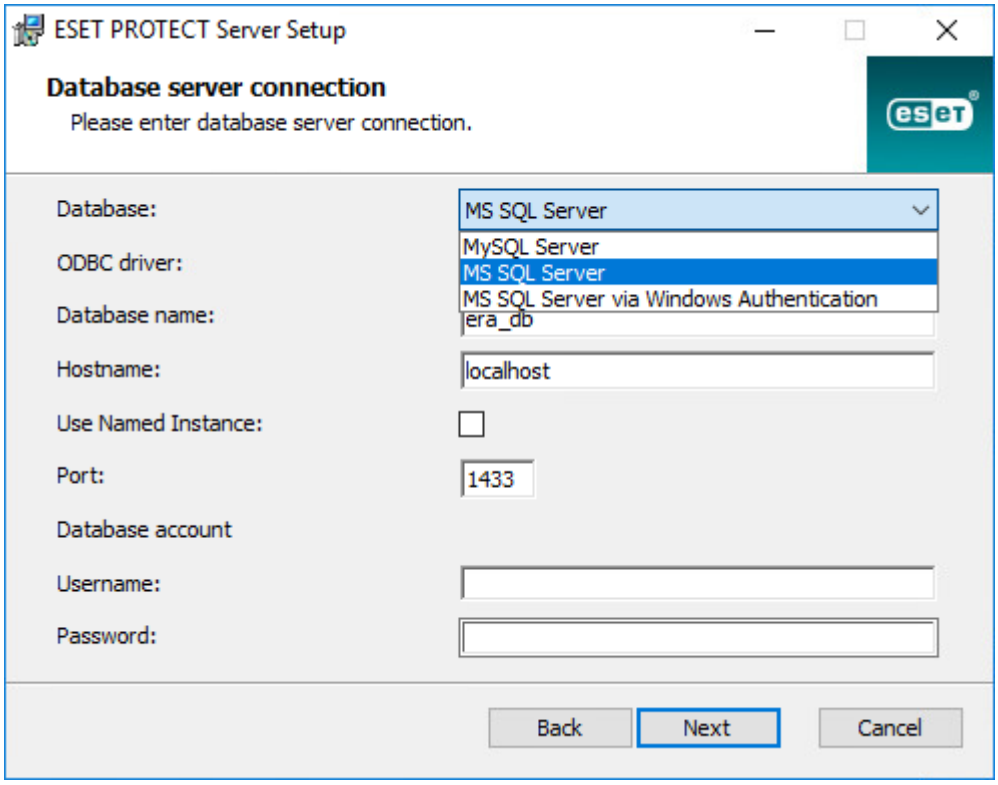
• **Ім'я бази даних**: Рекомендуємо використовувати попередньо встановлене ім'я або змінити його за необхідності.

• **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

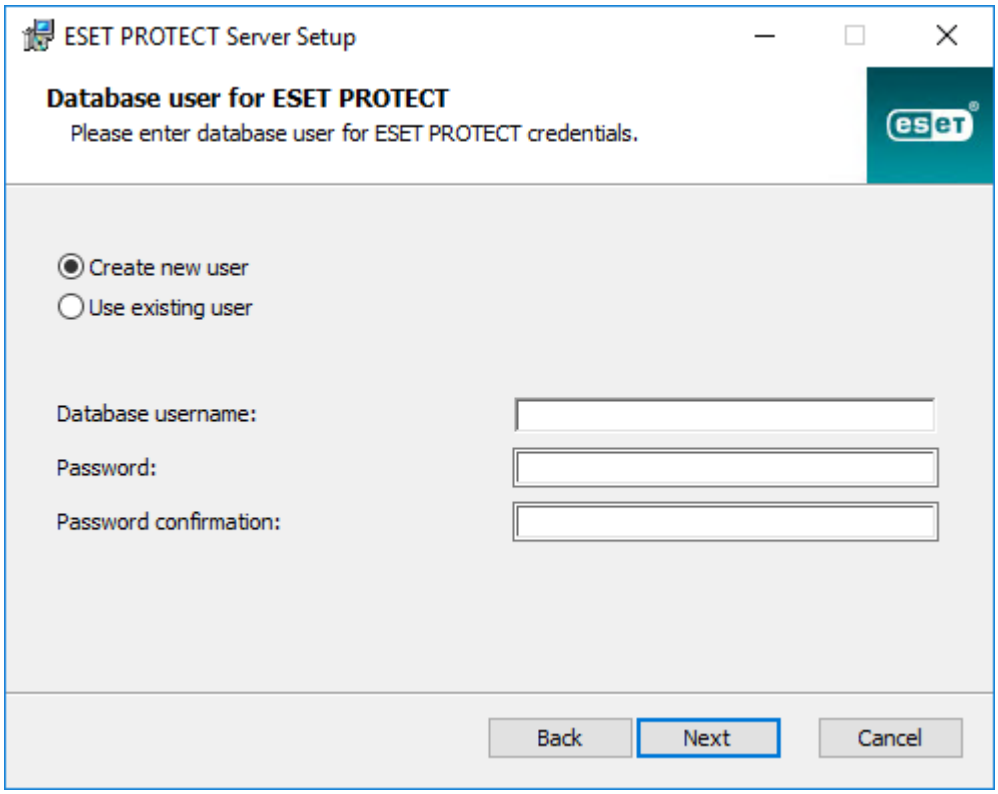
• **Використовувати екземпляр з іменем**: якщо ви використовуєте базу даних MS SQL, можна установити прапорець **Використовувати екземпляр з іменем**, щоб використовувати настроюваний екземпляр бази даних. Його можна задати в полі **Ім'я хоста** у формі *HOSTNAME\DB_INSTANCE* (наприклад, *192.168.0.10\ESMC7SQL*). Для кластерної бази даних використовуйте лише ім'я кластера. Якщо вибрано цей параметр, не можна буде змінити порт підключення до бази даних. Система використовуватиме порти за замовчуванням, визначені Microsoft. Щоб підключити сервер ESET PROTECT до бази даних MS SQL, інстальованій у відмовостійкому кластері, уведіть ім'я кластера в полі **Ім'я хоста**.



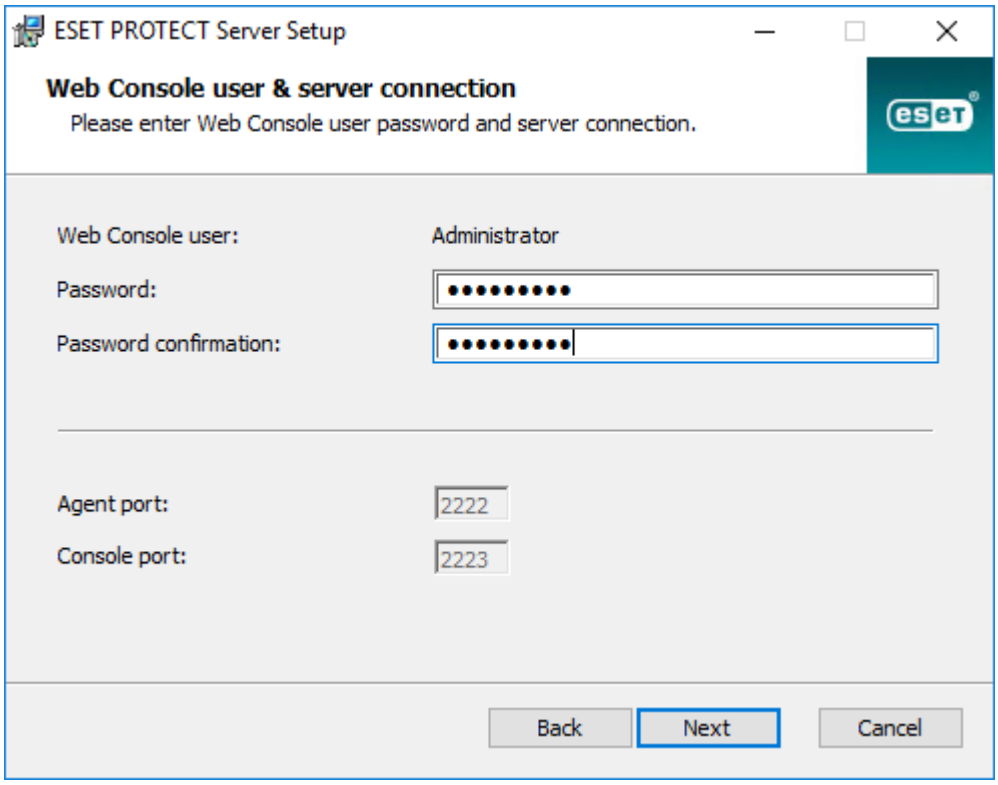
Сервер ESET PROTECT зберігає великі об’єкти даних у базі даних, тому для належної роботи ESET PROTECT потрібно налаштувати MySQL для приймання пакетів великих розмірів.

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.

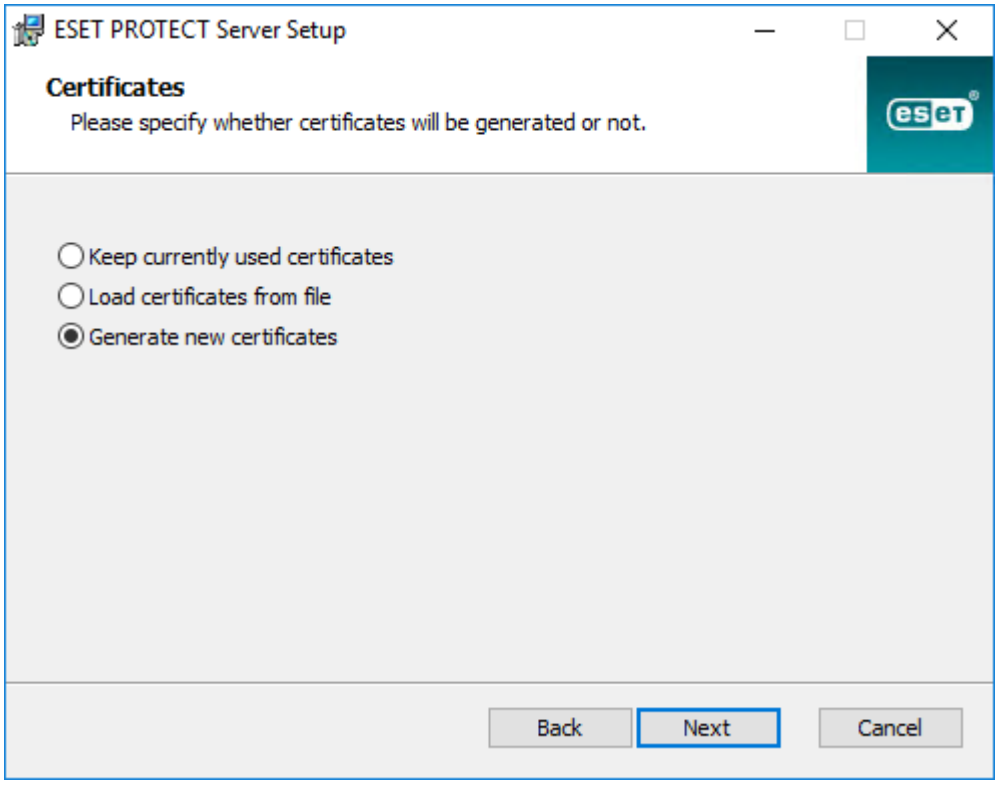


9. Введіть пароль для доступу до **веб-консолі**.



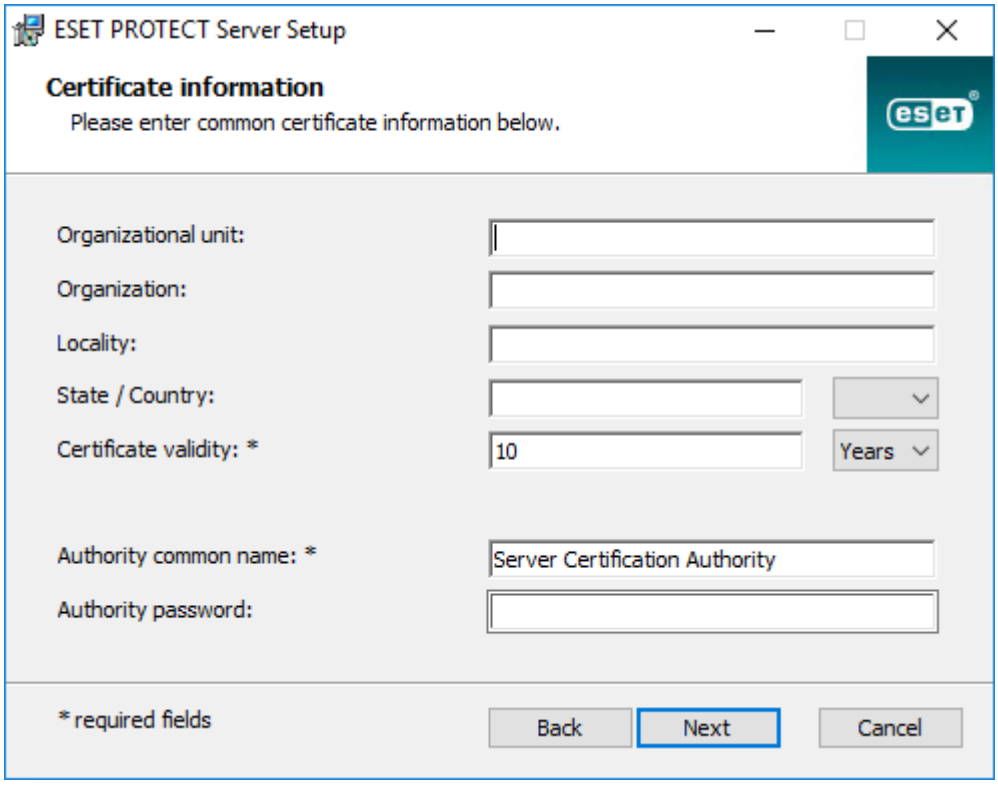
10. ESET PROTECT використовує сертифікати для зв’язку між клієнтом і сервером. Виберіть один із варіантів нижче.

- **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.



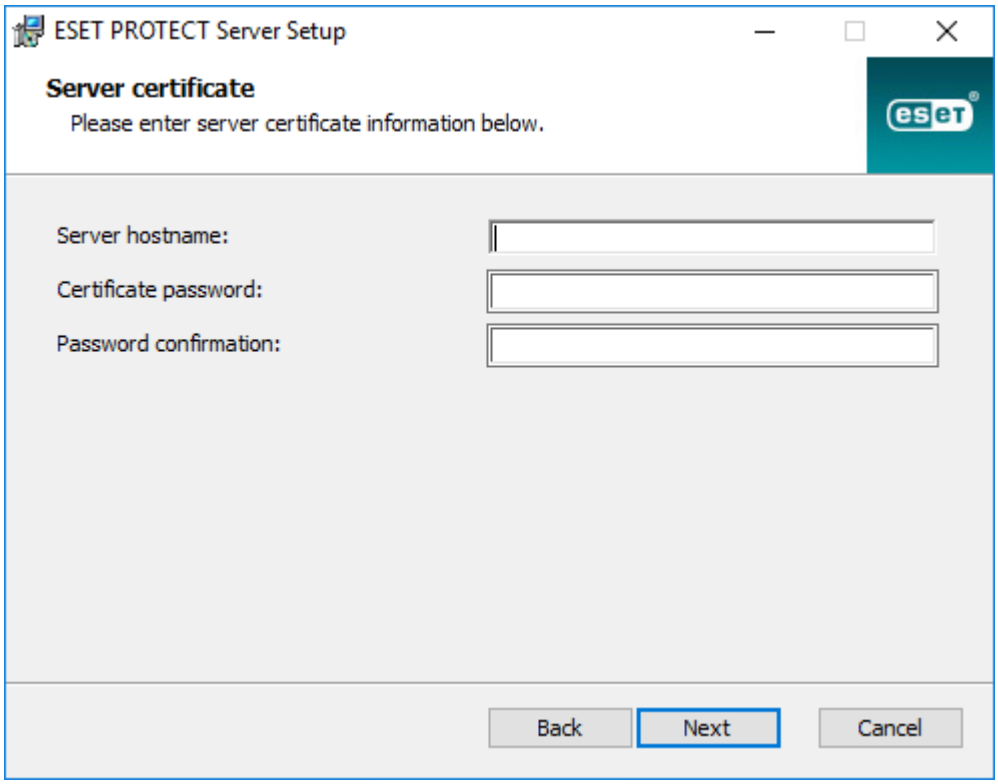
11. Виконайте інструкцію цього кроку, якщо на попередньому кроці було вибрано **Створювати нові сертифікати**.

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

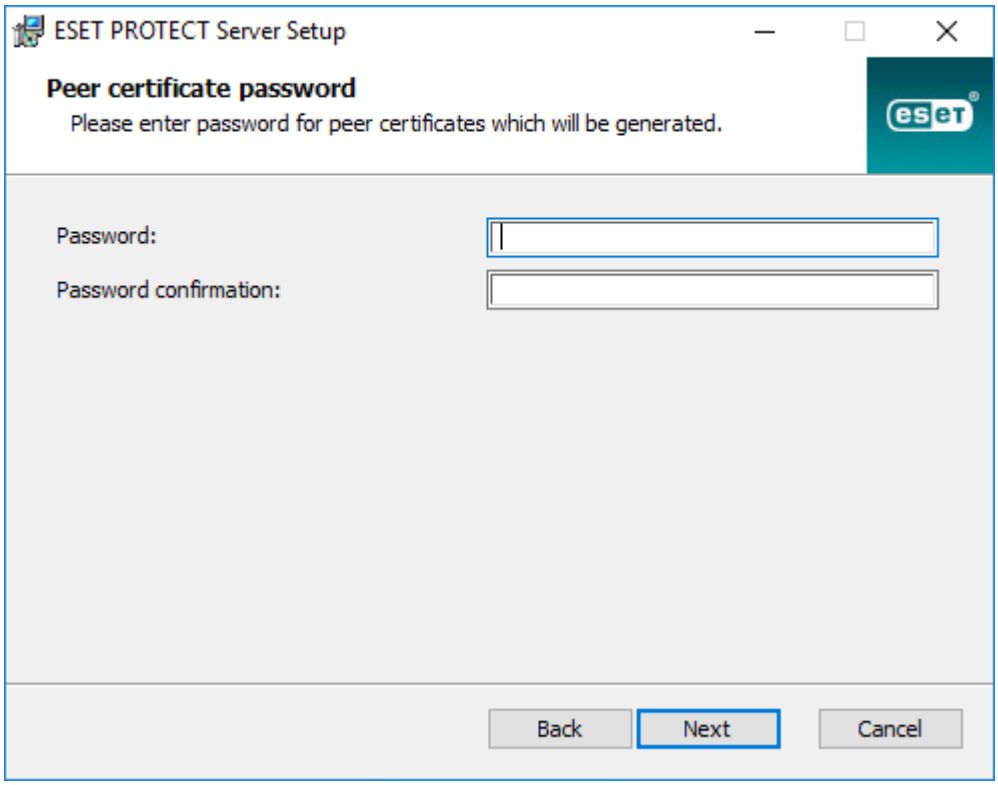


b)У полі **Сертифікат сервера** уведіть **Ім’я хоста сервера** й **Пароль сертифіката** (необов’язково).

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

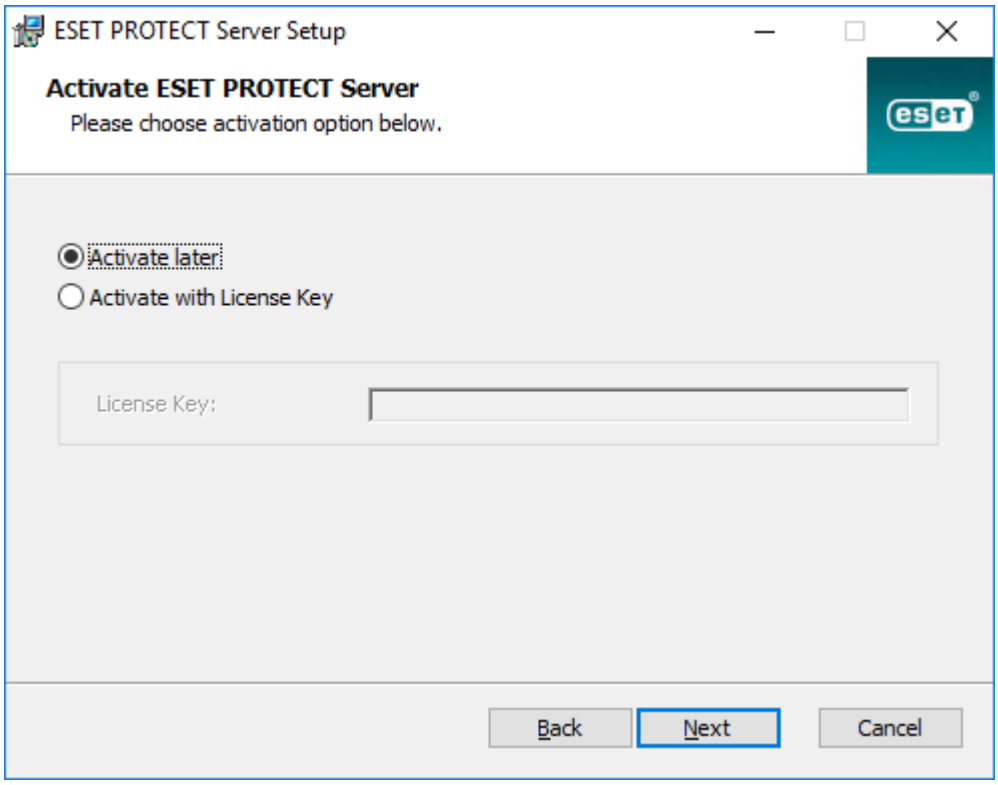


c)У полі **Пароль сертифіката однорангового вузла** введіть пароль для сертифікатів однорангових вузлів агента й проксі-сервера.



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**.



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

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

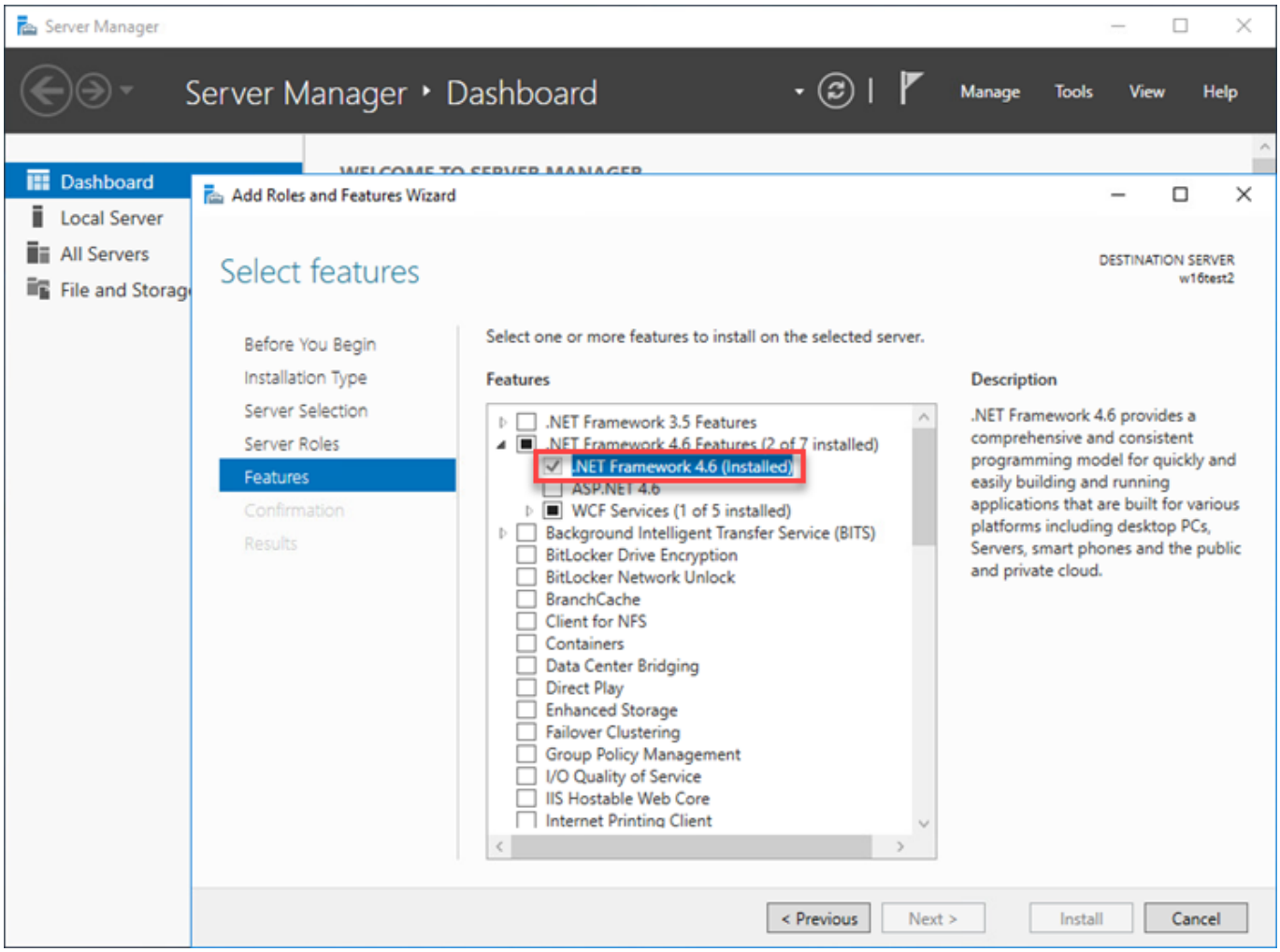
Після інсталяції сервера ESET PROTECT на той самий комп'ютер можна інсталювати агента ESET Management (необов'язково) Завдяки цьому ви зможете керувати сервером, як керуєте клієнтським комп'ютером.

Попередні вимоги до сервера – Windows

Для інсталяції сервера ESET PROTECT 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 інстальовані 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.
- Інстальовано веб-консоль ESET PROTECT, щоб керувати сервером ESET PROTECT.
- Для інсталяції MS SQL Server Express необхідно мати Microsoft .NET Framework 4. Відповідний

пакет можна інсталювати за допомогою **майстра додавання ролей і функцій**:



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.

• Щоб налаштувати Microsoft SQL Server та керувати цим сервером (бази даних і користувачі), завантажте SQL Server Management Studio (SSMS).
• Не інсталюйте SQL Server у контролері домену (наприклад, 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).

Інсталяція та конфігурація сервера MySQL

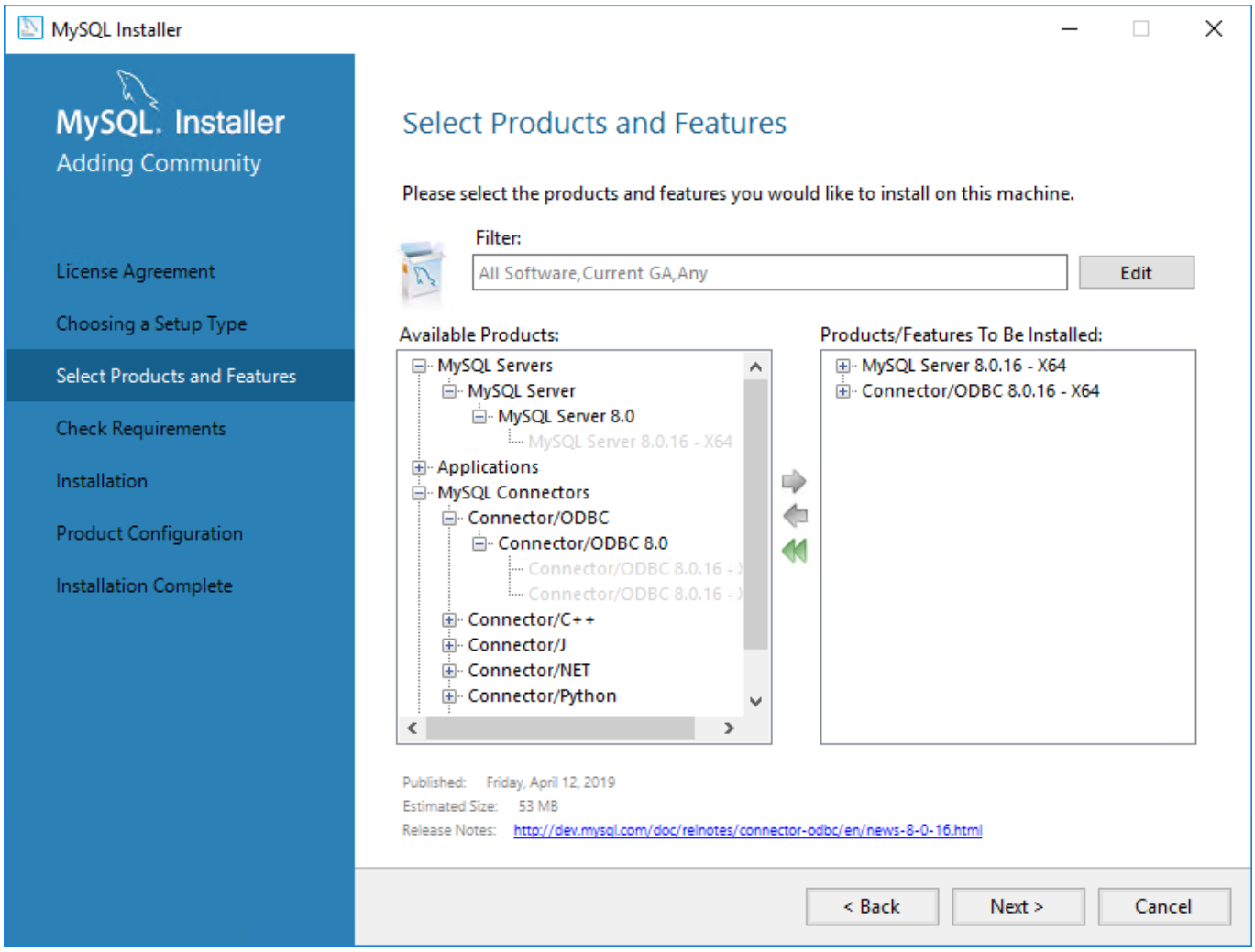
Інсталяція

Обов'язково інсталюйте 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. Установіть прапорець **Я приймаю умови ліцензійної угоди** й клацніть **Далі**.

3. 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).



4. Клацніть **Далі** й виберіть **Виконати**, щоб інсталювати MySQL Server і ODBC Connector.

5. Натисніть кнопку **Далі**. У розділі **Висока доступність** виберіть **Автономний MySQL Server / Класична реплікація MySQL** і клацніть **Далі**.

6. У розділі **Тип і мережа** в розкривному меню **Тип конфігурації** виберіть пункт **Комп'ютер сервера** й клацніть **Далі**.

7. У розділі **Метод автентифікації** виберіть рекомендований параметр **Використовувати надійне шифрування пароля для автентифікації** й клацніть **Далі**.

8. У розділі **Облікові записи й ролі** двічі введіть **кореневий пароль MySQL**. Рекомендується також створити спеціальний обліковий запис користувача бази даних.

9. У розділі **Служба Windows** залиште попередньо вибрані значення незмінними й клацніть **Далі**.

10. Клацніть **Виконати** й дочекайтесь завершення інсталяції MySQL Server. Клацніть **Готово**, **Далі** й **Готово**, щоб закрити вікно інсталяції.

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
```

Щоб визначити версію MySQL, виконайте команду: `mysql --version`

- Для підтримуваних версій MySQL 8.x необхідно вказати таку змінну:

  o`log_bin_trust_function_creators=1`

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

- Для підтримуваних версій MySQL 8.x, 5.7 і 5.6.22 (і новіших версій 5.6.x):

  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
  ```

- Для MySQL 5.6.20 і 5.6.21:

  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**.

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

4. Щоб перезавантажити сервер MySQL і застосувати конфігурацію (назва процесу залежить від версії MySQ: 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.

Існує мінімальний набір прав, які необхідно надати спеціальному обліковому запису користувача бази даних:

• 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

Докладну інструкцію з налаштування бази даних і користувача для MS SQL та MySQL див. у статті бази знань.

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*	• Ця глава • КБ	• **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.

Метод	Документація	Опис
ESET Remote Deployment Tool	• Онлайн-довідка	• Рекомендовано для масового розгортання через локальну мережу. • Може використовуватися для розгортання універсального інсталятора (агент + продукт ESET для захисту)
Універсальний інсталятор агента	• Створіть універсальний інсталятор агента • КБ	• В інсталятор також можуть входити продукт для захисту та вбудована політика. • Розмір інсталятора складає кілька сотень мегабайт.
Агент Live Installer	• Створити Агент Live Installer • КБ	• Інсталятор – це виконуваний скрипт. Він має невеликий розмір, але йому потрібен доступ до місця збереження інсталятора *.msi*. • Скрипт можна змінити таким чином, щоб він використовував локальний інсталятор і проксі-сервер HTTP.
Розгортання SCCM і GPO	• SCCM • GPO • КБ	• Удосконалений метод віддаленого масового розгортання. • За допомогою невеликого файлу *.ini*.
Завдання сервера – розгортання агента	• Онлайн-довідка • КБ	• Альтернатива SCCM та GPO. • Не працює через проксі-сервер HTTP. • Запускається сервером ESET PROTECT з веб-консолі ESET PROTECT.

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* або *agent_arm64.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 ESET звіти про аварійне завершення роботи та анонімні дані телеметрії (тип і версія ОС, версія продукту ESET та інші дані про продукт), зніміть прапорець **Взяти участь у програмі удосконалення продуктів**. 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).

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.

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.

Для інсталяцій із використанням сервера не можна використовувати користувача з двофакторною автентифікацією.

• 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 дозволені 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).

Параметр	Опис і дозволені значення
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** – вимкнуто (за замовчуванням); **1** – увімкнуто. 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\Ad
ministrator\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=
CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvk
pqayzjJZhSY8qswDQYJKoZIhvc 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\Deskt
op\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**. Щоб увійти як користувач домену, установіть прапорець поруч із пунктом **Увійти в домен**.

> • 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**.
> • Для інсталяцій із використанням сервера не можна використовувати користувача з двофакторною автентифікацією.

2. Коли з’явиться запит прийняти сертифікат, натисніть **Так**.

3. Виберіть **Не створювати комп’ютер (він буде створений автоматично під час першого підключення)** або **Виберіть 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.

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

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**.

ESET Remote Deployment Tool

ESET Remote Deployment Tool дозволяє в зручний спосіб розповсюдити пакет інсталятора, 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.

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 інсталятора (рекомендований метод)
- Досвідчені користувачі можуть виконати ручну інсталяцію

Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери.

Інсталяція веб-консолі з використанням універсального інсталятора

Порядок інсталяції компонента ESET PROTECT Web Console з використанням універсального інсталятора

1. Переконайтеся, що перелічені нижче попередні вимоги виконано:

- Інстальовано сервер ESET PROTECT.

> Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери. Для цього потрібні додаткові кроки.

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

- Apache Tomcat потребує 64-розрядної версії Java/OpenJDK. Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

> 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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

2. Завантажте універсальний інсталятор ESET PROTECT з веб-сайту ESET і розархівуйте завантажений файл.

3. Щоб інсталювати останню версію Apache Tomcat за умови, коли універсальний інсталятор 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*.

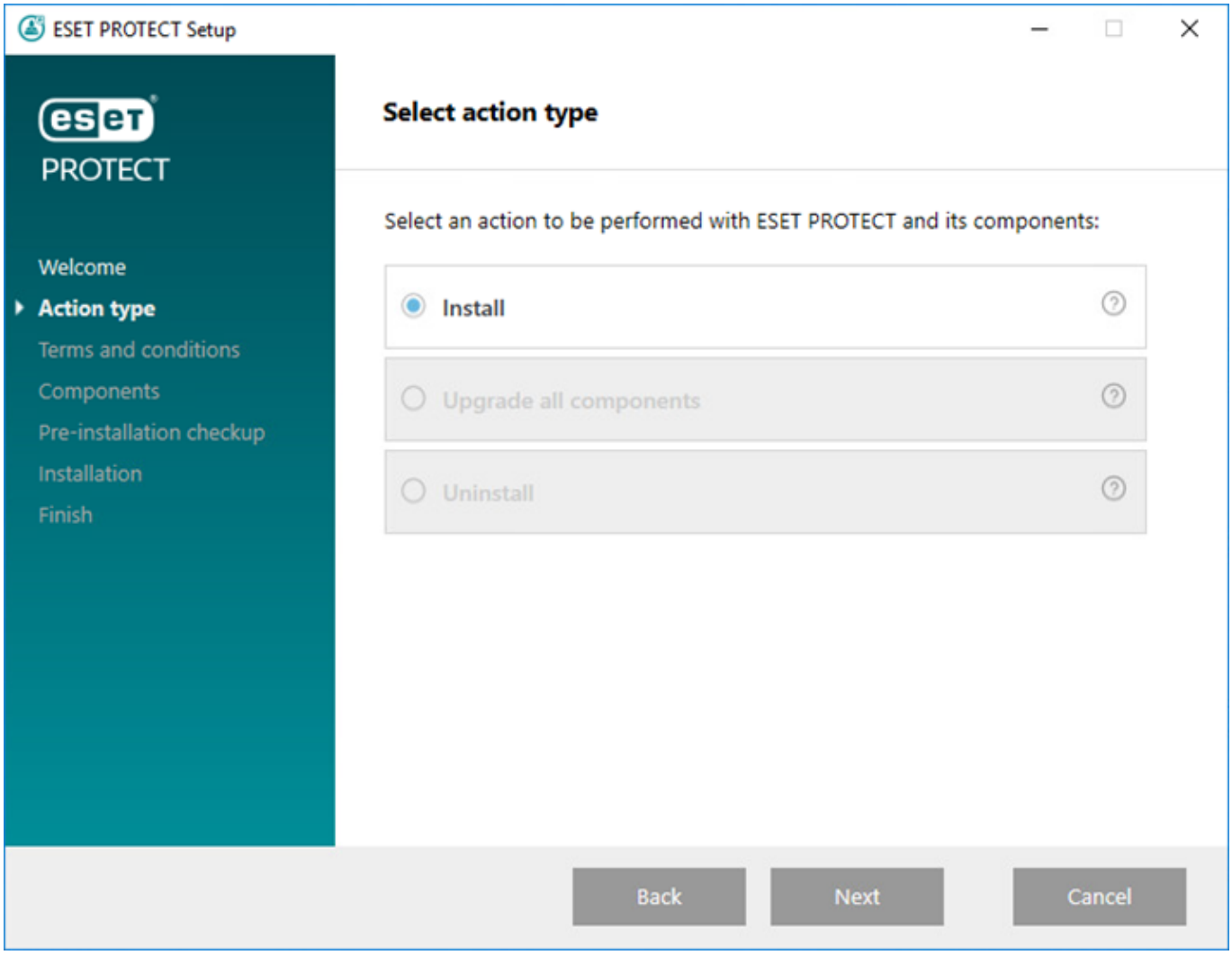
b. Видаліть файл *apache-tomcat-9.0.x-windows-x64.zip*, розташований у папці *installers*.

c. Завантажте ZIP-пакет 64-розрядної версії Apache Tomcat 9 для Windows.

d. Перемістить завантажений ZIP-пакет у папку *installers*.

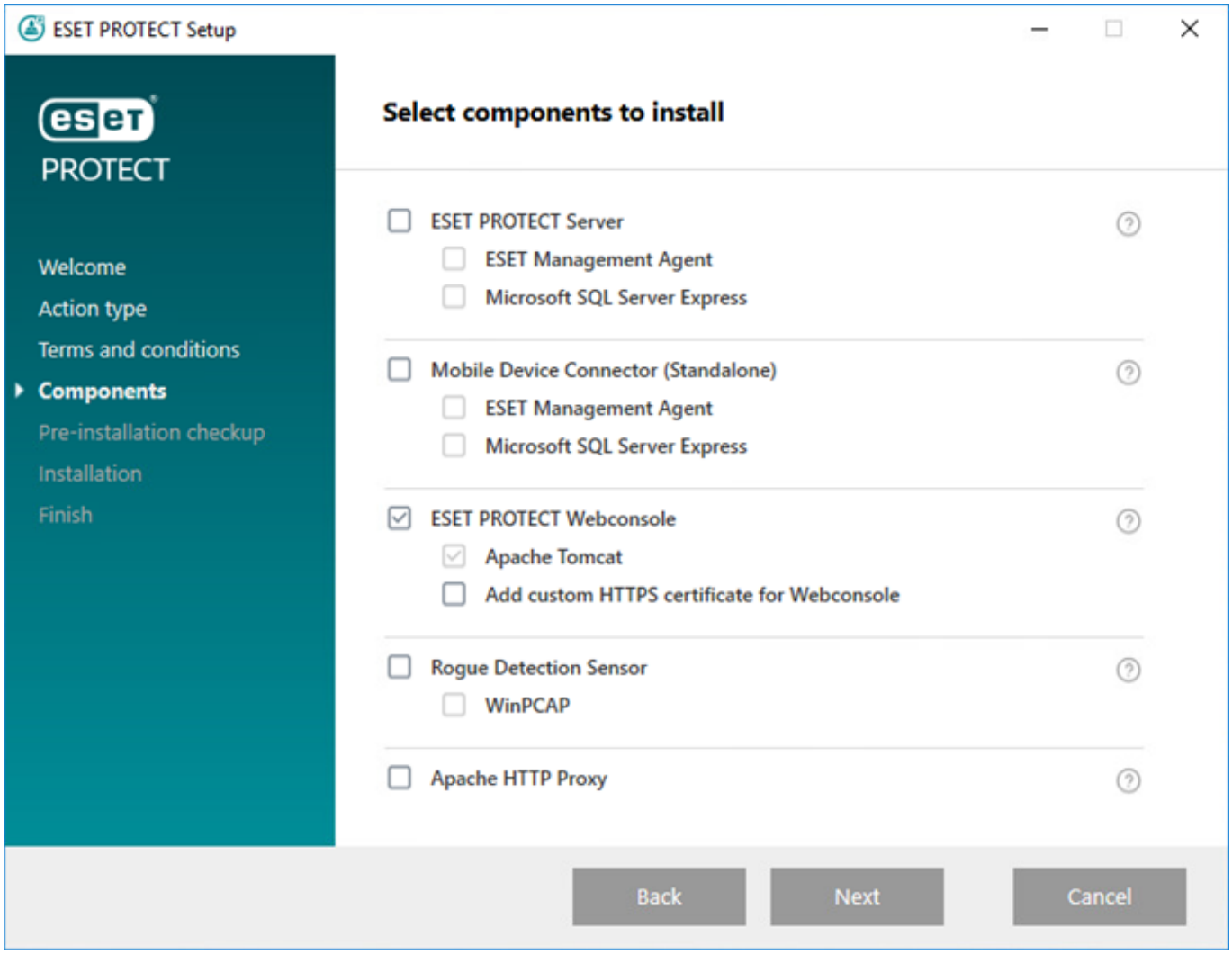
4. Щоб запустити універсальний інсталятор, двічі клацніть файл *Setup.exe* й натисніть клавішу **Далі** на екрані **привітання**.

5. Виберіть **Інсталювати** й натисніть **Далі**.



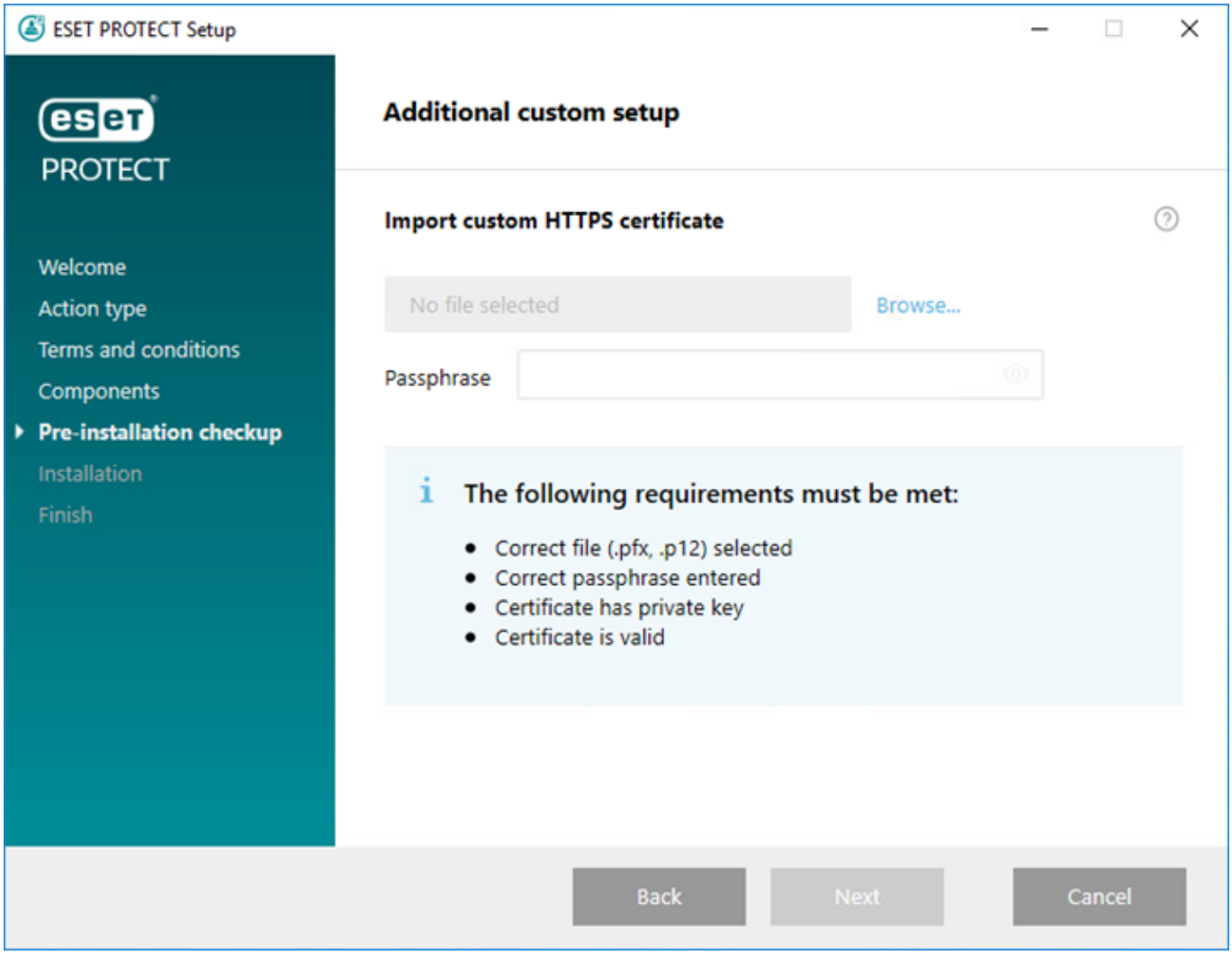
6. Прийміть умови Ліцензійної угоди з кінцевим користувачем і натисніть **Далі**.

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**.

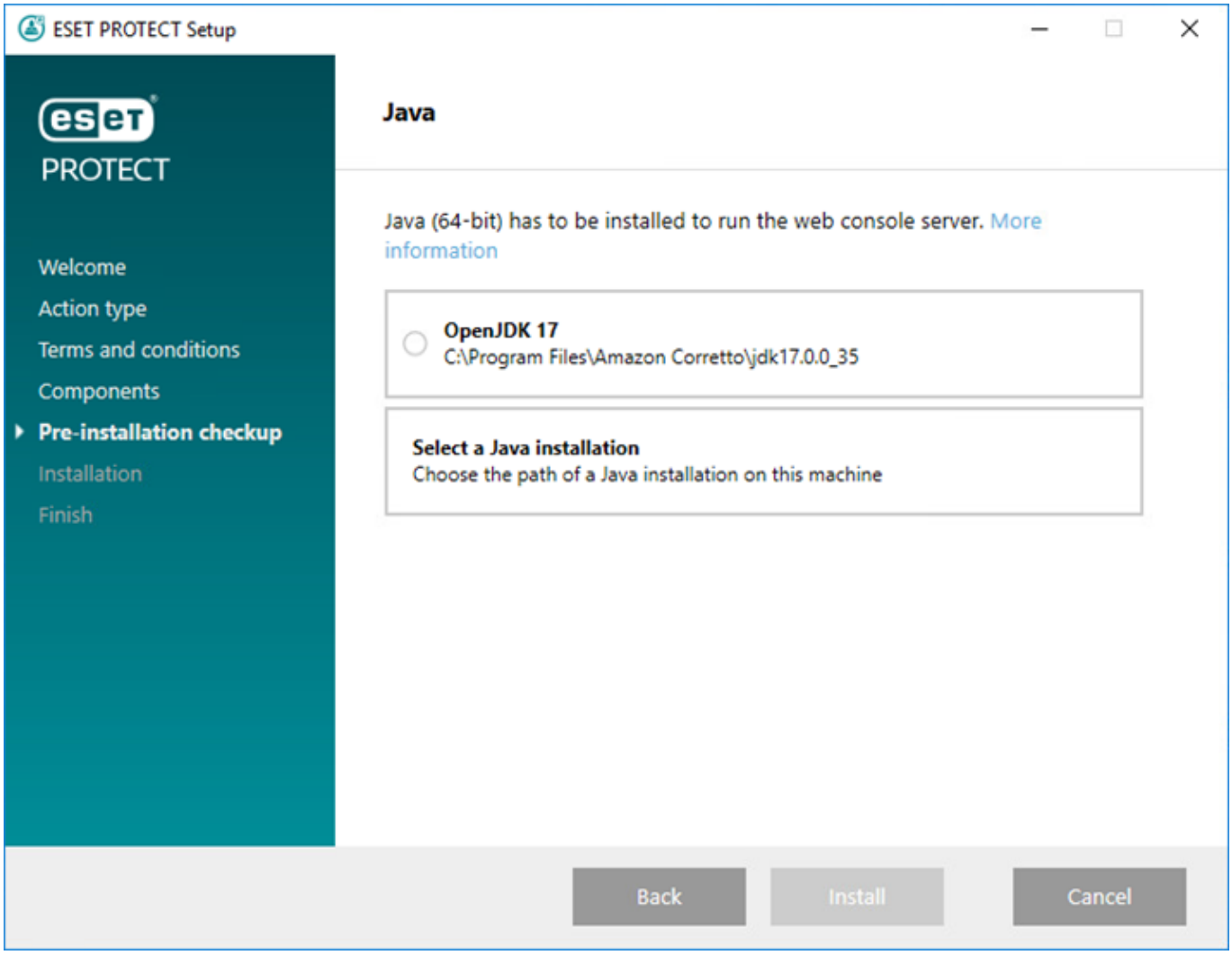
- Виберіть цю опцію, якщо хочете використовувати користувацький сертифікат HTTPS для веб-консолі ESET PROTECT.
- Якщо не вибрати цей параметр, інсталятор автоматично згенерує нове сховище ключів для Tomcat (самопідписаний сертифікат HTTPS).
- Якщо ви вибрали **Додати користувацький сертифікат HTTPS для 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). Інсталятор інсталює сертифікат для доступу до веб-консолі на сервері Tomcat. Щоб продовжити, натисніть **Далі**.



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

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

b)Натисніть **Інсталювати**, щоб продовжити, або **Змінити**, щоб змінити шлях інсталяції Java.



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

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.
a)Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск** > **Служби** > правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.
b)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*.
c)Знайдіть рядок `server_address=localhost`.
d)Замініть `localhost` на IP-адресу вашого сервера ESET PROTECT та збережіть файл.
e) 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. Відобразиться екран входу в систему.

- З комп'ютера, на якому розміщено веб-консоль ESET PROTECT: *https://localhost/era*

- З будь-якого комп'ютера з інтернет-доступом до веб-консолі ESET PROTECT (замініть *IP_ADDRESS_OR_HOSTNAME* IP-адресою або ім'ям хоста веб-консолі ESET PROTECT): *https://IP_ADDRESS_OR_HOSTNAME/era*

Див. також тему Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи.

Інсталяція веб-консолі вручну

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.

- Інстальовано сервер ESET PROTECT.

Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери. Для цього потрібні додаткові кроки.

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

- Apache Tomcat потребує 64-розрядної версії Java/OpenJDK. Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

a)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.

a)Запустіть інсталятор.

b)Під час інсталяції виберіть шлях до Java (батьківської папки Java *bin* і папок *lib*) і встановіть прапорець **Run Apache Tomcat**.

c)Після інсталяції переконайтеся, що службу Apache Tomcat запущено, а для типу її запуску задано параметр **Автоматичний** (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. Apache Tomcat автоматично видобуде файл *era.war* у папку *era* і інсталює веб-консоль ESET PROTECT. Зачекайте кілька хвилин, поки видобування завершиться. Якщо видобування не запускається, виконайте дії з виправлення неполадок.

5. Якщо веб-консоль ESET PROTECT і сервер ESET PROTECT інстальовано на одному комп'ютері, перезапустіть службу 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**.

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.
a)Зупиніть роботу служби Apache Tomcat. Для цього перейдіть у меню **Пуск** > **Служби** > правою клавішею миші натисніть службу Apache Tomcat і виберіть **Зупинити**.
b)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*.
c)Знайдіть рядок `server_address=localhost`.
d)Замініть `localhost` на IP-адресу вашого сервера ESET PROTECT та збережіть файл.
e) Запустіть службу Apache Tomcat. Для цього перейдіть у меню **Пуск** > **Служби** > правою клавішею миші натисніть службу Apache Tomcat і виберіть **Запустити**.

6. Відкрийте веб-консоль ESET PROTECT у підтримуваному веб-браузері. Відобразиться екран входу в систему:

- З комп'ютера, на якому розміщено веб-консоль ESET PROTECT: *http://localhost:8080/era*
- З будь-якого комп'ютера з інтернет-доступом до веб-консолі ESET PROTECT (замініть *IP_ADDRESS_OR_HOSTNAME* IP-адресою або ім'ям хоста веб-консолі ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

7. Налаштуйте веб-консоль після інсталяції:

- Під час інсталяції Apache Tomcat уручну для порту HTTP за замовчуванням задається номер 8080. Рекомендуємо налаштувати підключення HTTPS для Apache Tomcat.
- 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 переспрямовує трафік зашифрованого обміну даними між агентом ESET Management і 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 або налаштовувати його.

- Архітектура проксі-сервера HTTP

- Архітектура проксі-сервера Apache HTTP
- Додаткові сценарії для проксі-сервера HTTP

Перед інсталяцією

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 інсталятора необхідно завантажити весь пакет програм, але ця процедура є простішою. Запустіть завантажений інсталятор і виберіть у ньому лише **проксі-сервер Apache HTTP**. Після інсталяції сервера Apache його потрібно налаштувати.

- Інсталювати програмне забезпечення з окремого інсталятора 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

Якщо в мережі є кілька сегментів, Rogue Detection Sensor необхідно інсталювати окремо в кожному сегменті мережі для формування повного списку всіх пристроїв у всій мережі.

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

1. Перейдіть у розділ завантажень ESET PROTECT і завантажте окремий інсталятор 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 інсталятор RD Sensor.

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

5. Якщо ви не хочете надсилати ESET звіти про аварійне завершення роботи та анонімні дані телеметрії (тип і версія ОС, версія продукту ESET та інші дані про продукт), зніміть прапорець **Взяти участь у програмі удосконалення продуктів**. 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 інстальовано 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

Користуєтеся 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 зберігати їх локально.

> **i** 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.

Попередні вимоги відсутні

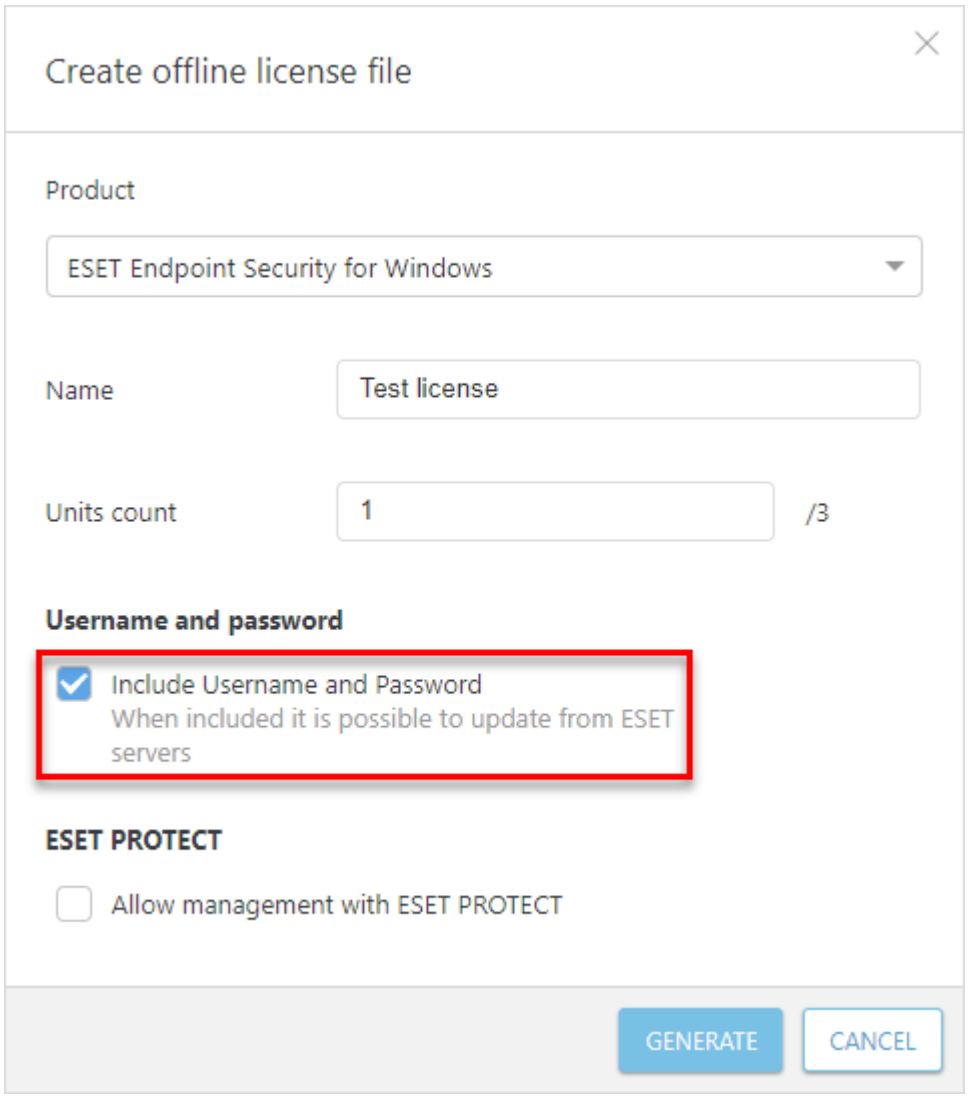
Інструмент «Дзеркало» не підтримується у Windows XP та Windows Server 2003.

• Цільова папка має бути доступна для спільного використання, Samba/Windows або служби HTTP/FTP залежно від вибраного способу отримання доступу до оновлень.

oПродукти з безпеки ESET для Windows: їх можна оновлювати віддалено через HTTP або з використанням спільної папки.

oПродукти з безпеки ESET для Linux/macOS: їх можна оновлювати віддалено лише через HTTP. Якщо ви використовуєте спільну папку, вона має бути на тому самому комп'ютері, що й продукт із безпеки ESET.

• 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.



• 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» та його версію, виконайте вказану нижче команду:

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

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. 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. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --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.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already 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.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Усі фільтри чутливі до регістру.

Параметр	Опис
`--updateServer`	Під час використання потрібно вказати повну URL-адресу сервера оновлення.
`--offlineLicenseFilename`	Необхідно вказати шлях до файлу автономної ліцензії (як згадувалося вище).
`--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`	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. Ви можете вказати, які типи файлів оновлення завантажувати. Можливі значення (з урахуванням регістру): • `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. Параметр ігнорується, коли дзеркало створюється для застарілих продуктів (`ep4`, `ep5`).
`--compatibilityVersion`	Цей необов'язковий параметр застосовується до інструмента «Дзеркало», який розповсюджується з продуктом ESET PROTECT 8.1 і пізніших версій. Інструмент «Дзеркало» завантажить файли оновлень, сумісні з версією репозиторію ESET PROTECT, указаною в аргументі параметра у форматі `x.x` або `x.x.x.x`. Наприклад, `--compatibilityVersion 9.0` або `--compatibilityVersion 8.1.13.0`.

Щоб зменшити обсяг даних, що завантажуються з репозиторію ESET, рекомендуємо використовувати нові параметри в інструменті "Дзеркало", що розповсюджується у складі ESET PROTECT 9: `--filterFilePath` і `--dryRun`. Дотримуйтеся таких інструкцій:
1.Створіть фільтр у форматі *JSON* (див. `--filterFilePath` нижче).
2.Запустіть тестовий інструмент "Дзеркало" з параметром `--dryRun` (див. нижче) і налаштуйте фільтр на свій розсуд.
3.Запустіть інструмент "Дзеркало" з параметром `--filterFilePath` і визначеним фільтром завантаження разом із параметрами `--intermediateRepositoryDirectory` і `--outputRepositoryDirectory`.
4.Регулярно запускайте інструмент "Дзеркало" для того, аби завжди використовувати найновіші інсталятори.

Параметр	Опис

`--filterFilePath`	Цей необов'язковий параметр дає змогу фільтрувати продукти з безпеки ESET на основі текстового файлу (у форматі *JSON*), розміщеного в папці інструмента «Дзеркало», наприклад, `--filterFilePath filter.txt`).
	Опис конфігурації фільтра
	Файл конфігурації для фільтрації продуктів має формат *JSON* із такою структурою:
	• кореневий об'єкт *JSON*:
	o`use_legacy` (логічне значення, необов'язково): якщо має значення true, буде включено застарілі продукти;
	o`defaults` (об'єкт *JSON*, необов'язково): визначає властивості фільтра, які будуть застосовані до всіх продуктів;
	■`languages` (рядок): укажіть коди ISO для мов, які потрібно включити. Наприклад, для французької мови введіть `"fr_FR"`. Коди інших мов наведено в таблиці нижче. Якщо потрібно вказати кілька мов, розділіть їх комами з пробілом. Приклад: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (рядок): платформи, які потрібно включити (`["x64", "x86", "arm64"]`).
	Використовуйте фільтр `platforms` обачливо. Наприклад, якщо інструмент "Дзеркало" завантажує лише 64-розрядні інсталятори, а у вашій інфраструктурі є 32-розрядні комп'ютери, 64-розрядні продукти з безпеки ESET не вдасться інсталювати на 32-розрядних комп'ютерах.
	
	■`os_types` (рядок): типи ОС, які потрібно включити (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (список об'єктів JSON, необов'язково): фільтри для застосування до певних продуктів; перевизначте `defaults` для вказаних продуктів. Об'єкти мають такі властивості:
	■`app_id` (рядок): обов'язково, якщо не вказано `name`.
	■`name` (рядок): обов'язково, якщо не вказано `app_id`.
	■`version` (рядок): визначає версію або діапазон версій, які потрібно включити.
	■`languages` (рядок): коди ISO для мов, які потрібно включити (див. таблицю нижче).
	■`platforms` (рядок): платформи, які потрібно включити (`["x64", "x86", "arm64"]`).
	■`os_types` (рядок): типи ОС, які потрібно включити (`["windows"]`, `["linux"]`, `["mac"]`).
	Щоб визначити відповідні значення для полів, запустіть інструмент "Дзеркало" в режимі тестового виконання й знайдіть відповідний продукт у створеному файлі CSV.
	Описи формату рядка версії
	Усі номери версій складаються з чотирьох цифр, розділених крапками (наприклад, `7.1.0.0`). Під час створення фільтрів версій можна вказати меншу кількість номерів (наприклад, `7.1`), тоді решта номерів будуть нульовими (версія `7.1` ідентична версії `7.1.0.0`).
	Рядок версії може бути в одному з таких форматів:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oВибирає версії, які порівняно зі вказаною версією будуть мати такі відношення: більше/менше, дорівнює/менше або дорівнює/дорівнює.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oВибирає версії, які є не меншими за нижню межу або не більшими за верхню межу.
	Кожна частина номеру версії порівнюється арифметично зліва направо.
	Приклад JSON
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Параметр `--filterFilePath` тепер використовується замість параметрів `--languageFilterForRepository`, `--productFilterForRepository` і `--downloadLegacyForRepository`, які використовувалися в старіших версіях інструмента "Дзеркало" (який випускався з ESET PROTECT 8.x).

Параметр	Опис
`--dryRun`	Якщо використовується цей необов'язковий параметр, інструмент «Дзеркало» не завантажуватиме жодних файлів, проте згенерує файл *.csv* з усіма пакетами для завантаження. Цей параметр можна використовувати без обов'язкових параметрів `--intermediateRepositoryDirectory` й `--outputRepositoryDirectory`. Наприклад, `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. ℹ Деякі інсталятори ESET є універсальними з точки зору мови (з кодом мови `multilang`), тому інструмент "Дзеркало" помістить їх у файл *.csv*, навіть якщо ви вкажете конкретні `мови` в параметрі `--filterFilePath`. Якщо ви використовуєте параметр `--dryRun` разом із параметрами `--intermediateRepositoryDirectory` й `--outputRepositoryDirectory`, інструмент «Дзеркало» не очищує значення *outputRepositoryDirectory*.
`--listUpdatableProducts`	Список усіх продуктів ESET, для яких Mirror Tool може завантажити оновлення модуля (якщо не використовується параметр `--excludedProducts`). Цей параметр доступний у таких версіях Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

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 PROTECT 9 із дзеркала, для параметра Сервер оновлень встановіть указане нижче значення (відповідно до основного розташування сервера HTTP): `http://your_server_address/mirror/eset_upd/era6`
Примітка: Папка дзеркала `era6` є спільною для цих рішень віддаленого управління ESET: ERA 6, ESMC 7, ESET PROTECT.

Таблиця кодів мов

```
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, визначених у файлі *filter.txt* (див. приклад вмісту файлу в описі параметра `--filterFilePath` вище):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

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 кожну 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.

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.

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.

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

Рекомендуємо розгортати 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.

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 указано повне доменне ім'я (наприклад, `mdm.mycompany.com`), введіть його в полі **Ім'я хоста MDM**. Крім цього, якщо в сертифікаті HTTPS використовується символ узагальнення * (наприклад, `*.mycompany.com`), ви можете вказати в полі **Ім'я хоста MDM** значення `mdm.mycompany.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 установити прапорець **Використовувати екземпляр з іменем**, щоб використовувати настроюваний екземпляр бази даних. Його можна задати 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 вибрано цей параметр, не можна буде змінити порт підключення до бази даних. Система використовуватиме порти за замовчуванням, визначені Microsoft. Щоб підключити сервер ESET PROTECT до бази даних MS SQL, інстальованій у відмовостійкому кластері, уведіть ім'я кластера в полі **Ім'я хоста**.

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.

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.

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

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.

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). Докладніше про архітектуру MDM.

• 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

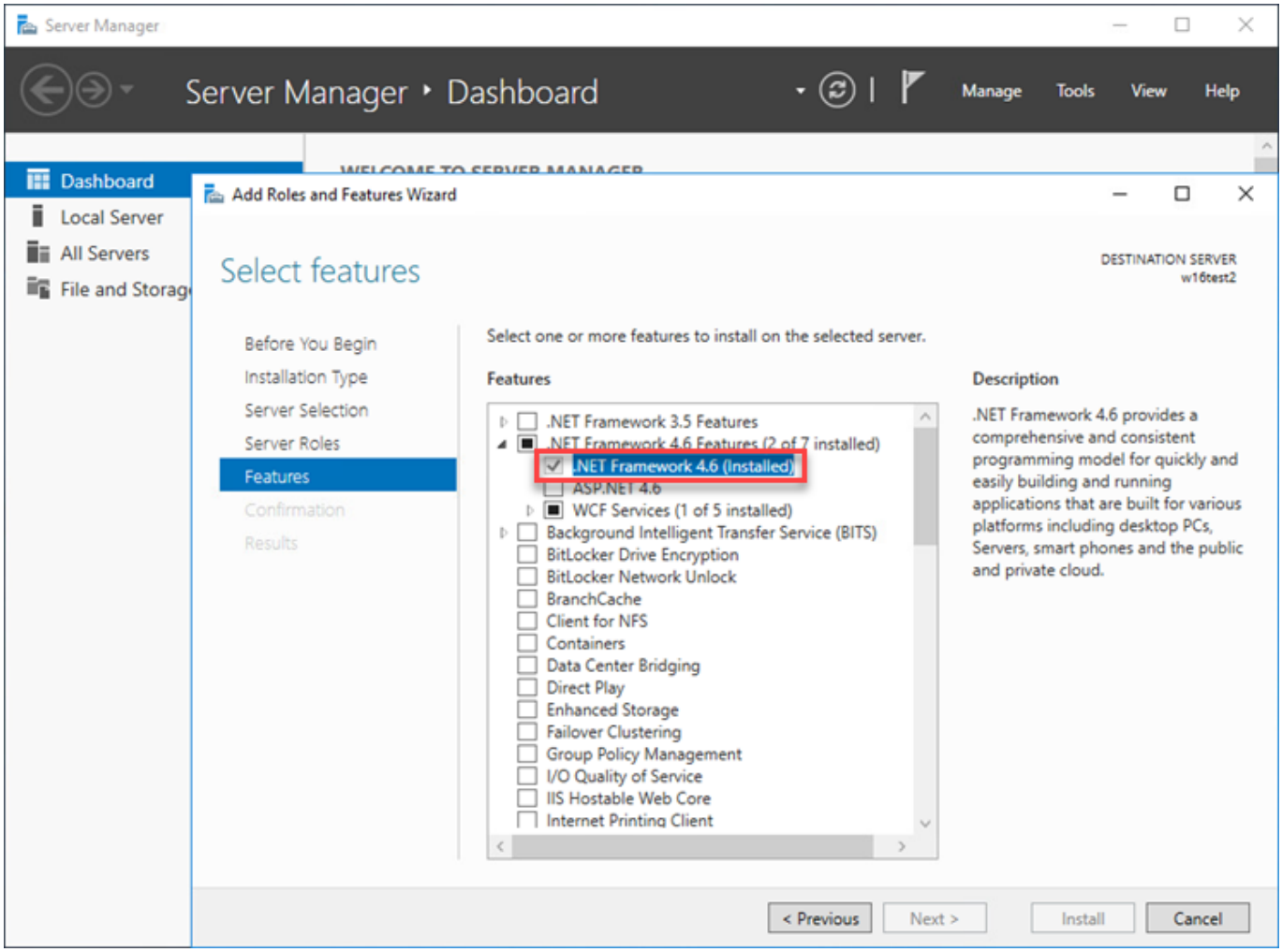
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP port 2222

Фактичні шляхи до файлів *.exe* можуть відрізнятися 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.

• Для інсталяції MS SQL Server Express необхідно мати Microsoft .NET Framework 4. Відповідний пакет можна інсталювати за допомогою **майстра додавання ролей і функцій**:



Вимоги до сертифіката

• Для безпечного обміну даними через протокол HTTPS потрібен **сертифікат SSL** у форматі *.pfx*. Рекомендуємо використовувати сертифікат, наданий стороннім центром сертифікації. Не рекомендуємо використовувати самопідписані сертифікати (зокрема, сертифікати, підписані ЦС ESET PROTECT), оскільки не всі мобільні пристрої дозволяють користувачам приймати такі сертифікати.

• Щоб об'єднати їх в один файл *.pfx*, потрібно мати сертифікат, підписаний 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.

Активація Mobile Device Connector

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

1.У розділі ESET PROTECT "Керування ліцензією" додайте ліцензію ESET Endpoint, Business або Office.

2.Активуйте Mobile Device Connector за допомогою клієнтських завдань Активація 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.

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.

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

Якщо ви вже інсталювали 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.

Як альтернативу проксі-серверу Apache HTTP можна інсталювати Squid.

Інсталювати 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 2.[x.xx]*

Щоб інсталювати 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, якщо ви видобуваєте вміст архіву *ApacheHttp.zip* у папку *D:\Apache Http Proxy*, тоді *C:\Program Files* потрібно замінити на *D:\Apache Http Proxy*.

3. Відкрийте командний рядок адміністратора та змініть папку на *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]\conf*.

a.За замовчуванням для обміну даними з агентом ESET Management використовується порт 2222. Якщо ви змінили порт під час інсталяції, вказуйте новий номер порту. Змініть значення «2222» в рядку `AllowCONNECT 443 563 2222 8883 53535` 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 службу *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 2.[x.xx]\conf\httpd.conf* у текстовому редакторі. Додайте у файл такі рядки:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"

DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"

<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">

Options Indexes FollowSymLinks

AllowOverride None

Require all granted

</Directory>

CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

3. Збережіть файл і запустіть службу Apache.

```
sc start ApacheHttpProxy
```

> 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 2.[x.xx]\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 відкрийте командний рядок адміністратора та виконайте таку команду:

```
sc stop ApacheHttpProxy
```

2. Перевірте наявність наступних модулів у папці *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]\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

> Після інсталяції проксі-сервера Apache HTTP ви зможете дозволити передавати лише дані ESET (блокуючи весь інший трафік, установлено за замовчуванням) або будь-які дані. Змініть конфігурацію згідно з наведеними нижче інструкціями:
> • Перенаправлення лише для підключення ESET
> • Ланцюжок проксі-серверів (увесь трафік)

Відкрийте список вмісту кеша

"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]\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 2.[x.xx]\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 2.[x.xx]\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 2.[x.xx]\bin\htcacheclean.exe\"^
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M"
```

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

Щоб дізнатися більше, перегляньте статтю бази знань або документацію 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. Замінити `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
```

> • 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 Squid *squid.conf*.

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

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.

> Зауважте, що розмір репозиторію збільшується й у проміжного каталогу буде такий самий розмір. Перш ніж починати цей процес, переконайтеся, що у вас є принаймні **1.2 ТБ** вільного місця.

Рекомендації

Перегляньте також статтю бази знань ESET Практичні поради з використання в ESET PROTECT автономному середовищі.

Приклад сценарію для Windows

I. Клонування репозиторію

1. Завантажте інструмент «Дзеркало».

2. Видобудьте інструмент «Дзеркало» із завантажено 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.

II. 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*

2.[x.xx]

9. Відкрийте командний рядок адміністратора та змініть каталог на *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]\conf\httpd.conf* і внизу файлу додайте ці рядки:

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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).

III. 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 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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://YourIPaddress* (наприклад, *http://10.1.1.10*).

19. Задайте нову адресу репозиторію за допомогою веб-консолі ESET PROTECT:

a.Сервер ESET PROTECT: клацніть **Докладніше** > **Параметри сервера** > **Додаткові параметри** > **Репозиторій** і введіть адресу автономного репозиторію в полі **Сервер**.

b.Агенти ESET Management: клацніть **Політики**, виберіть політику агента й клацніть > **Змінити** > **Параметри** > **Додаткові параметри** > **Репозиторій** і введіть адресу автономного репозиторію в полі **Сервер**.

c.Продукти ESET Endpoint (для Windows): клацніть **Політики**, виберіть політику **ESET Endpoint для Windows** і клацніть **Змінити** > **Параметри** >**Оновити** > **Профілі** > **Оновлення** > **Оновлення модулів**, зніміть прапорець **Автоматичний вибір** і введіть адресу автономного репозиторію в поле **Спеціальний сервер**.

Відмовостійкий кластер

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

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

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 ESET PROTECT Server 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 ESET PROTECT Server 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 ESET PROTECT Server на вузлі node1.

5. Відкрийте брандмауер і дозвольте вхідні з’єднання на всіх портах, які використовує ESET PROTECT Server.

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

було вказано в сертифікаті сервера.

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:

a. Інсталюйте Web Console на окремому комп'ютері й налаштуйте її для підключення до ролі кластера ESET PROTECT Server.

b. 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*

c. 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.

Основні компоненти

- ESET PROTECTСервер
- Веб-консоль ESET PROTECT — Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери.
- ESET Management Агент
- Сервер бази даних

Додаткові компоненти

- RD Sensor
- Mobile Device Connector
- Проксі-сервер Apache HTTP

- Інструмент «Дзеркало»

Інсталяція та конфігурація MySQL

Інсталяція

⚠ Обов'язково інсталюйте підтримувану версію MySQL Server та з'єднувача ODBC.

Якщо ви вже інсталювали й налаштували MySQL, перейдіть до розділу Конфігурація.

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

Debian, Ubuntu	Виконайте такі команди в Terminal:
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	Див. також: Додавання репозиторію MySQL APT

CentOS, Red Hat	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 відрізнятися залежно від розподілу та версії Linux:

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

- Інсталяція вручну. Завантажте й інсталюйте 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
```

Щоб визначити версію MySQL, виконайте команду: `mysql --version`

- Для підтримуваних версій MySQL 8.x необхідно вказати таку змінну:
  - o`log_bin_trust_function_creators=1`
  - oКрім цього, можна вимкнути ведення бінарного журналу: `log_bin=0`
- Для підтримуваних версій MySQL 8.x, 5.7 і 5.6.22 (і новіших версій 5.6.x):
  - oдля 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`
- Для MySQL 5.6.20 і 5.6.21:
  - oдля 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**.

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

⚠ Обов'язково інсталюйте підтримувану версію MySQL Server та з'єднувача ODBC.

ℹ Ви можете інсталювати 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 «a)». 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**:
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.

> **Інструкції з інсталяції для вибраних дистрибутивів Linux**
> Інструкції для конкретного дистрибутива ви можете дізнатися у таких статтях нашої бази знань:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

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 базу даних видалено не буде.	-
`--locale`	Локальний ідентифікатор (LCID) інстальованого сервера (значення за замовчуванням – `en_US`). Див. доступні мови в пункті підтримувані мови. **i** Якщо не вказати параметр `--locale`, сервер ESET PROTECT буде інстальовано в локалізації англійською мовою. Після інсталяції ESET PROTECT ви можете вибирати мову для кожного сеансу веб-консолі ESET PROTECT. Пам'ятайте, що не всі елементи веб-консолі зміняться після змінення мови. Деякі елементи (панелі інструментів за замовчуванням, політики, завдання тощо) створюються під час інсталяції ESET PROTECT, тому їхню мову неможливо змінити.	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.	-

Атрибут	Опис	Потрібно
`--db-driver`	Драйвер ODBC, який використовується для підключення до бази даних у файлі *odbcinst.ini* (список доступних драйверів виводиться командою `odbcinst -q -d`. Використовуйте один із указаних нижче драйверів: `--db-driver="MySQL ODBC 8.0 Driver"`).	Так
`--db-hostname`	Ім’я комп’ютера або IP-адреса сервера бази даних. Екземпляр бази даних з іменем не підтримується.	Так
`--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 сертифіката в днях або роках (вкажіть в аргументі `--cert-validity-unit`)	-

Атрибут	Опис	Потрібно
`--cert-validity-unit`	Одиниця виміру терміну дії сертифіката, 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.	-

ESET рекомендує видалити з історії командного рядка команди, що містять важливі дані (наприклад, пароль):
1.Запустіть `history`, щоб переглянути список усіх команд в історії.
2.Запустіть `history -d line_number` (укажіть номер рядка команди). Окрім того, можна запустити `history -c`, щоб видалити всю історію командного рядка.

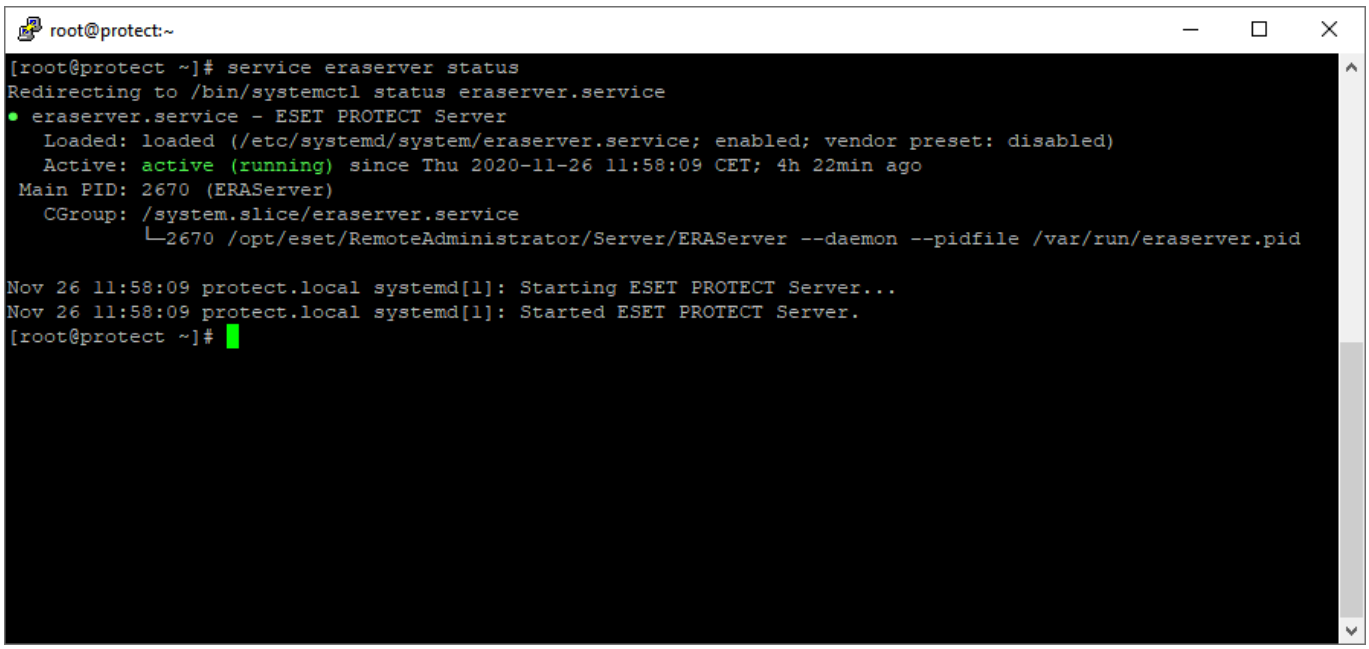
4. Спочатку вам знадобиться відповісти, чи погоджуєтеся ви взяти участь у програмі покращення продукту. Натисніть **Y**, якщо ви згодні надсилати звіти про аварійне завершення роботи та телеметричні дані до ESET, або **N**, щоб не надсилати жодних даних.

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
```



Журнал інсталятора

Журнал інсталятора 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.
- Необхідно мати підтримувану операційну систему Linux.
- Необхідні порти мають бути відкриті й доступні (переглянути їх повний перелік можна тут).
- 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 інсталятор. MS SQL Server в Linux не підтримується. Однак ви можете підключити сервер ESET PROTECT у Linux до MS SQL Server у Windows.

> 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 термінала:

```
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.

    - Щоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
    - Ви можете переглянути перелік усіх версій OpenSSL, інстальованих у системі. Щоб вивести список закінчень імен файлів, виконайте команду `sudo find / -iname *libcrypto.so*`

- **Xvfb** – вимагається для належного друку звітів у серверних системах Linux без графічного інтерфейсу (створення звіту).
- **Xauth**: пакет інсталюється разом із **xvfb**. Якщо ви не інсталюєте **xvfb**, потрібно інсталювати **xauth**.
- **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 пакет недоступний у репозиторії операційної системи, його можна створити на цільовому комп'ютері або інсталювати зі стороннього репозиторію (наприклад, із репозиторію EPEL). Інструкції для CentOS 7, інструкції для Ubuntu 20.04.

- **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 9.0 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, RHEL). SELinux може спричиняти проблеми з іншими програмами. Для сервера ESET PROTECT цей параметр необов'язковий.

- **lshw** - : інсталюйте пакет `lshw` на комп'ютері клієнта/сервера з Linux, щоб агент ESET Management правильно надіслав повідомлення про інвентар обладнання.

Таблиця нижче містить відповідні команди термінала для кожного описаного вище пакета для різних дистрибутивів Linux (виконайте команди як `sudo` або `root`):

Пакет	Дистрибутиви Debian і Ubuntu	Дистрибутиви CentOS і Red Hat	Дистрибутив OpenSUSE
ODBC драйвер	Перегляньте розділ Інсталяція та конфігурація ODBC.		
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb`	`zypper install xorg-x11-server-extra`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`	`zypper install cifs-utils`
Бібліотеки Qt4 WebKit	`apt-get install libqtwebkit4` Див. інструкції для Ubuntu 20.04.	Перегляньте статтю бази знань.	`zypper install libqtwebkit4`
kinit + klist – необов'язково (потрібно для служби Active Directory)	`apt-get install krb5-user`	`yum install krb5-workstation`	`zypper install krb5`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap`	`zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`	`zypper install net-snmp`

Пакет	Дистрибутиви Debian і Ubuntu	Дистрибутиви CentOS і Red Hat	Дистрибутив OpenSUSE
Пакет розробника SELinux (необов'язково для сервера ESET PROTECT; SELinux може спричиняти проблеми з іншими програмами)	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`	`zypper install selinux-policy-devel`
samba (необов'язково, потрібно лише для віддаленого розгортання)	`apt-get install samba`	`yum install samba samba-winbind-clients`	`zypper install samba samba-client`
lshw	`apt-get install -y lshw`	`yum install -y lshw`	`zypper install lshw`

Інсталяція агента – Linux

Інсталяція агента ESET Management в 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
```

ESET рекомендує видалити з історії командного рядка команди, що містять важливі дані (наприклад, пароль):
1.Запустіть `history`, щоб переглянути список усіх команд в історії.
2.Запустіть `history -d line_number` (укажіть номер рядка команди). Окрім того, можна запустити `history -c`, щоб видалити всю історію командного рядка.

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, «ера»).

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
`--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

Атрибут	Опис	Потрібно
`--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`). Для інсталяцій із використанням сервера не можна використовувати користувача з двофакторною автентифікацією.	Ні
`--webconsole-password`	Пароль, який використовує веб-консоль для підключення до сервера.	Так (із використанням сервера)
`--proxy-hostname`	Ім'я хоста проксі-сервера HTTP. 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).	Якщо використовується проксі-сервер
`--proxy-port`	Порт проксі-сервера HTTP для підключення до сервера.	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 інсталятору зчитати пароль зі стандартного вводу;

`--password="pass:PASSWORD"` є аналогом `--password="PASSWORD"`. Цей параметр необхідно використовувати, якщо для пароля використовується значення `"stdin"` (стандартне введення) або рядок, що починається з `"env:"` `"file:"` чи `"pass:"`

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

Підключення до проксі-сервера HTTP

Якщо проксі-сервер HTTP використовується для реплікації між агентом ESET Management і сервером ESET PROTECT (а не для кешування оновлень), можна вказати параметри підключення `--proxy-hostname` і `--proxy-port`.

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=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

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 інсталятора

Журнал інсталятора 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 інсталятора.

  oІнсталяція з використанням сервера – програма оновлюється, але зберігає попередні сертифікати.

  oІнсталяція в автономному режимі – програма оновлюється, після чого використовуються нові сертифікати.

- **Виправлення** – запускається та сама версія інсталятора. Цю функцію можна використовувати для міграції агента на інший сервер ESET PROTECT.

  oІнсталяція з використанням сервера – програма інсталюється повторно й отримує поточні сертифікати із сервера ESET PROTECT (згідно з параметром `hostname`).

  oІнсталяція 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.

- **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.

oЩоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.

oВи можете переглянути перелік усіх версій OpenSSL, інстальованих у системі. Щоб вивести список закінчень імен файлів, виконайте команду `sudo find / -iname *libcrypto.so*`

• : інсталюйте пакет `lshw` на комп'ютері клієнта/сервера з Linux, щоб агент ESET Management правильно надіслав повідомлення про інвентар обладнання.

Дистрибутив Linux	Команда термінала
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

• Для Linux CentOS рекомендовано інсталювати пакет `policycoreutils-devel`. Для цього виконайте таку команду:

```
yum install policycoreutils-devel
```

Інсталяція агента з використанням сервера:

• Необхідно забезпечити можливість підключення до комп'ютера до сервера з мережі. Крім того, на ньому має бути інстальовано сервер ESET PROTECT і веб-консоль ESET PROTECT.

Інсталяція агента в автономному режимі:

• Необхідно забезпечити можливість підключення до комп'ютера до сервера з мережі. Крім того, на ньому має бути інстальовано сервер ESET PROTECT.

• Також слід підготувати сертифікат агента

• Крім того, потрібен файл відкритого ключа центру сертифікації сервера

Інсталяція веб-консолі – Linux

Дотримуйтеся цих інструкцій, щоб інсталювати ESET PROTECT Web Console:

> **i** Крім того, можна інсталювати веб-консоль ESET PROTECT і сервер ESET PROTECT на різні комп'ютери. Для цього потрібні додаткові кроки.

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

Дистрибутив Linux	Команди термінала
Дистрибутиви Debian і Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-11-jdk tomcat9`
Дистрибутиви CentOS і Red Hat	`yum update` `yum install java-1.8.0-openjdk tomcat`
OpenSUSE	`zypper refresh` `zypper install java-1_8_0-openjdk tomcat`

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	`sudo cp era.war /var/lib/tomcat9/webapps/`
Дистрибутиви CentOS і Red Hat	`sudo cp era.war /var/lib/tomcat/webapps/`
Дистрибутив OpenSUSE	`sudo cp era.war /usr/share/tomcat/webapps/`

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

4. Перезапустіть службу Tomcat, щоб розгорнути файл *.war*:

Дистрибутиви Debian і Ubuntu	`sudo service tomcat9 restart`
Дистрибутиви CentOS і Red Hat	`sudo service tomcat restart`
Дистрибутив OpenSUSE	`sudo service tomcat restart`

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.

a)Зупиніть роботу служби Tomcat: `sudo service tomcat stop`

b)Відредагуйте файл *EraWebServerConfig.properties*:

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

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

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

c)Знайдіть рядок `server_address=localhost`

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

e)Перезавантаження службу Tomcat: `sudo service tomcat restart`

6. Відкрийте веб-консоль ESET PROTECT у підтримуваному веб-браузері. Відобразиться екран входу в систему:

• З комп'ютера, на якому розміщено веб-консоль ESET PROTECT: *http://localhost:8080/era*

• З будь-якого комп'ютера з інтернет-доступом до веб-консолі ESET PROTECT (замініть *IP_ADDRESS_OR_HOSTNAME* IP-адресою або ім'ям хоста веб-консолі ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

7. Налаштуйте веб-консоль після інсталяції:

• Під час інсталяції Apache Tomcat уручну для порту HTTP за замовчуванням задається номер 8080. Рекомендуємо налаштувати підключення HTTPS для Apache Tomcat.

• Див. також тему Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи.

Попередні вимоги й інсталяція Rogue Detection Sensor – Linux

Якщо в мережі є кілька сегментів, Rogue Detection Sensor необхідно інсталювати окремо в кожному сегменті мережі для формування повного списку всіх пристроїв у всій мережі.

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 інстальовано 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 **клавішу пробілу**.
У вікні запиту потрібно буде вказати, чи приймаєте ви умови угоди. Якщо приймаєте, натисніть клавішу **Y** на клавіатурі, якщо ні – **N**.

4. Якщо ви погоджуєтеся взяти участь у програмі покращення продукту, натисніть клавішу **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 інсталювати Mobile Device Connector та сервер ESET PROTECT на різних серверах. Наприклад, за допомогою цього сценарію інсталяції можна в будь-який час зробити Mobile Device Connector доступним з Інтернету для керування мобільними пристроями користувача.

Виконайте інсталяцію компонента MDC в Linux за допомогою команди в терміналі. Переконайтеся у відповідності всім попереднім вимогам. Ви можете підготувати скрипт інсталяції, а потім виконати його через `sudo`.

Необхідні параметри команди інсталяції

Існує багато додаткових параметрів інсталяції, однак деякі є обов'язковими:

- Сертифікат однорангового вузла: отримати сертифікат однорангового вузла ESET PROTECT можна двома способами, які наведено нижче:

  • **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.

  оДля способу **Інсталяція із сервера** потрібно вказати принаймні цей параметр:

  ```
  --webconsole-password=
  ```

  оДля способу **Інсталяція в автономному режимі** потрібно вказати ці параметри:

  ```
  --cert-path=
  --cert-password=
  ```

(Для сертифіката агента за замовчуванням, створеного під час інсталяції сервера ESET PROTECT, пароль не потрібен).

- Сертифікат HTTPS (проксі-сервер):

  - Якщо у вас уже є сертифікат HTTPS:

```
--https-cert-path=
--https-cert-password=
```

  - Порядок створення нового сертифіката HTTPS

```
--https-cert-generate
--mdm-hostname=
```

- Підключення до сервера ESET PROTECT (ім’я або IP-адреса сервера):

```
--hostname=
```

- Підключення до бази даних:

  - 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 MS SQL потрібно вказати такі відомості:

```
--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:

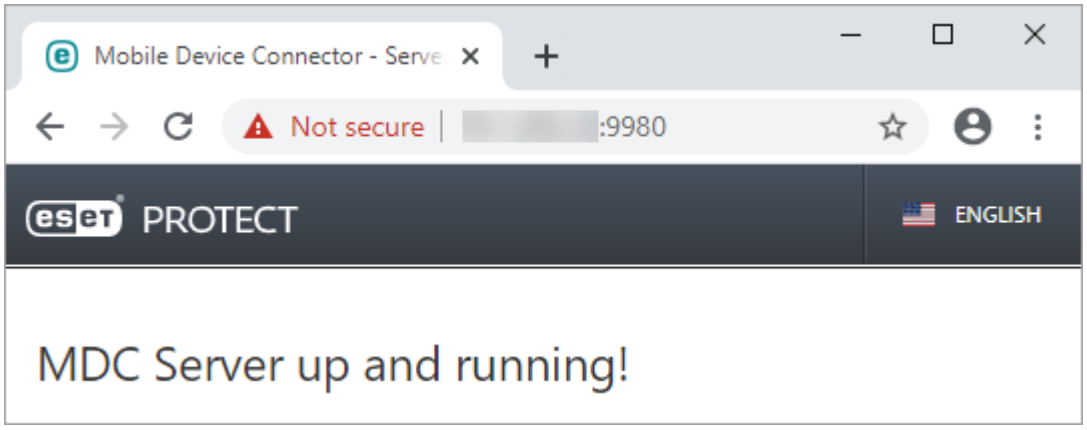
```
--help
```

ESET рекомендує видалити з історії командного рядка команди, що містять важливі дані (наприклад, пароль):
1.Запустіть `history`, щоб переглянути список усіх команд в історії.
2.Запустіть `history -d line_number` (укажіть номер рядка команди). Окрім того, можна запустити `history -c`, щоб видалити всю історію командного рядка.

Журнал інсталятора

Журнал інсталятора може знадобитися для виправлення неполадок. Його можна знайти у файлах 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 інсталювати 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 інсталятор).
- Для підключення до сервера бази даних (MySQL / MS SQL) на комп'ютері потрібно інсталювати драйвер ODBC. Перегляньте розділ Інсталяція та конфігурація ODBC.

> 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.

> 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.

  - Щоб перевірити поточну версію за замовчуванням, скористайтеся командою `openssl version`.
  - Ви можете переглянути перелік усіх версій OpenSSL, інстальованих у системі. Щоб вивести список закінчень імен файлів, виконайте команду `sudo find / -iname *libcrypto.so*`

> 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 стороннім центром сертифікації. Не рекомендуємо використовувати самопідписані сертифікати (зокрема, сертифікати, підписані ЦС ESET PROTECT), оскільки не всі мобільні пристрої дозволяють користувачам приймати такі сертифікати.
- Щоб об'єднати їх в один файл *.pfx*, потрібно мати сертифікат, підписаний 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

Агенти ESET Management Agent можуть підключатися до ESET PROTECT Server через Apache HTTP Proxy. Дізнайтеся більше про те, як проксі-сервер працює для агентів ESET Management.

Зазвичай Apache HTTP Proxy розповсюджується як пакет `apache2` або `httpd`.

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 500000000
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. Додайте конфігурацію проксі-сервера:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on
```

```
CacheLockMaxAge 10
ProxyTimeOut 900

SetEnv proxy-initial-not-pooled 1

<VirtualHost *:3128>
ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
ServerName r.edtd.eset.com

<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>

ProxyRequests Off
CacheEnable disk /
SSLProxyEngine On

RequestHeader set Front-End-Https "On"
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. За замовчуванням для обміну даними з агентом ESET Management використовується порт 2222. Якщо ви змінили порт під час інсталяції, вказуйте новий номер порту. Змініть значення «2222» в рядку `AllowCONNECT 443 563 2222 8883 53535` на номер вашого порту.

7. Увімкніть доданий проксі-сервер кешування та конфігурацію (якщо конфігурація перебуває в основному файлі конфігурації Apache, цей крок можна пропустити).

8. Якщо потрібно, укажіть інший порт прослуховування (за замовчуванням це порт 3128).

9. Необов’язкова базова автентифікація.

- oДодайте конфігурацію автентифікації в директиву проксі-сервера:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

- oСтворіть файл пароля за допомогою `/etc/httpd/.htpasswd -c`.
- oВручну створіть файл group.file із `usergroup:username`.

10. 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 500000000
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 скопіюйте та вставте таку конфігурацію:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900


SetEnv proxy-initial-not-pooled 1


<VirtualHost *:3128>

ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

        ServerName r.edtd.eset.com


<If "%{REQUEST_METHOD} == 'CONNECT'">

Require all denied

</If>


ProxyRequests Off

CacheEnable disk /

SSLProxyEngine On


RequestHeader set Front-End-Https "On"

ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0

ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>


<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. За замовчуванням для обміну даними з агентом ESET Management використовується порт 2222. Якщо ви змінили порт під час інсталяції, вказуйте новий номер порту. Змініть значення «2222» в рядку `AllowCONNECT 443 563 2222 8883 53535` на номер вашого порту.

7. Увімкніть файли конфігурації, які було відредаговано на попередніх етапах:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Установіть порт 3128 як порт прослуховування проксі-сервера Apache HTTP. Відредагуйте файл */etc/apache2/ports.conf* і замініть `Listen 80` на `Listen 3128`.

9. Необов'язкова базова автентифікація.

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

oСкопіюйте та вставте конфігурацію автентифікації перед `</Proxy>`:

```
  AuthType Basic
  AuthName "Password Required"
  AuthUserFile /etc/apache2/password.file
  AuthGroupFile /etc/apache2/group.file
  Require group usergroup
```

oІнсталюйте `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
```

oСтворіть файл `group`:

```
sudo vim /etc/apache2/group.file
```

і скопіюйте та вставте в нього такий рядок:

```
usergroup:user
```

10. Перезавантажте проксі-сервер Apache HTTP за допомогою цієї команди:

```
sudo service apache2 restart
```

Перенаправлення лише для підключення ESETЩоб 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>


#*.eset.systems:

<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]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[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>


#AV Cloud over port 53535

<ProxyMatch ^.*e5.sk.*$>

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}\.)?[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>


#*.eset.systems:

<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]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[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.|91.2
28.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#AV Cloud over port 53535

<ProxyMatch ^.*e5.sk.*$>

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):

```
<VirtualHost *:3128>

ProxyRequests On

ProxyRemote * http://IP_ADDRESS:3128

</VirtualHost>
```

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.

Налаштування переадресації підключень «агент-сервер» у проксі-сервері Apache HTTP

1. На проксі-сервері відкрийте файл

    i. Дистрибутиви Debian
    `/etc/apache2/mods-available/proxy.conf`

    ii. Дистрибутиви Red Hat
    `/etc/httpd/conf/httpd.conf`

2. У кінці файлу додайте ці рядки:
`AllowCONNECT 443 563 2222 8883 53535`

3. На проксі-сервері відкрийте файл

    i. Дистрибутиви Debian
    `/etc/apache2/apache2.conf`

    ii. Дистрибутиви Red Hat
    `/etc/httpd/conf/httpd.conf`

4. Знайдіть цей рядок
`Listen 80`
і змініть його на
`Listen 3128`

5. 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>
```

6.Перезавантаження службу *Apache HTTP Proxy*.

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
```

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
```

- 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

Користуєтеся 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 зберігати їх локально.

> **i** 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.

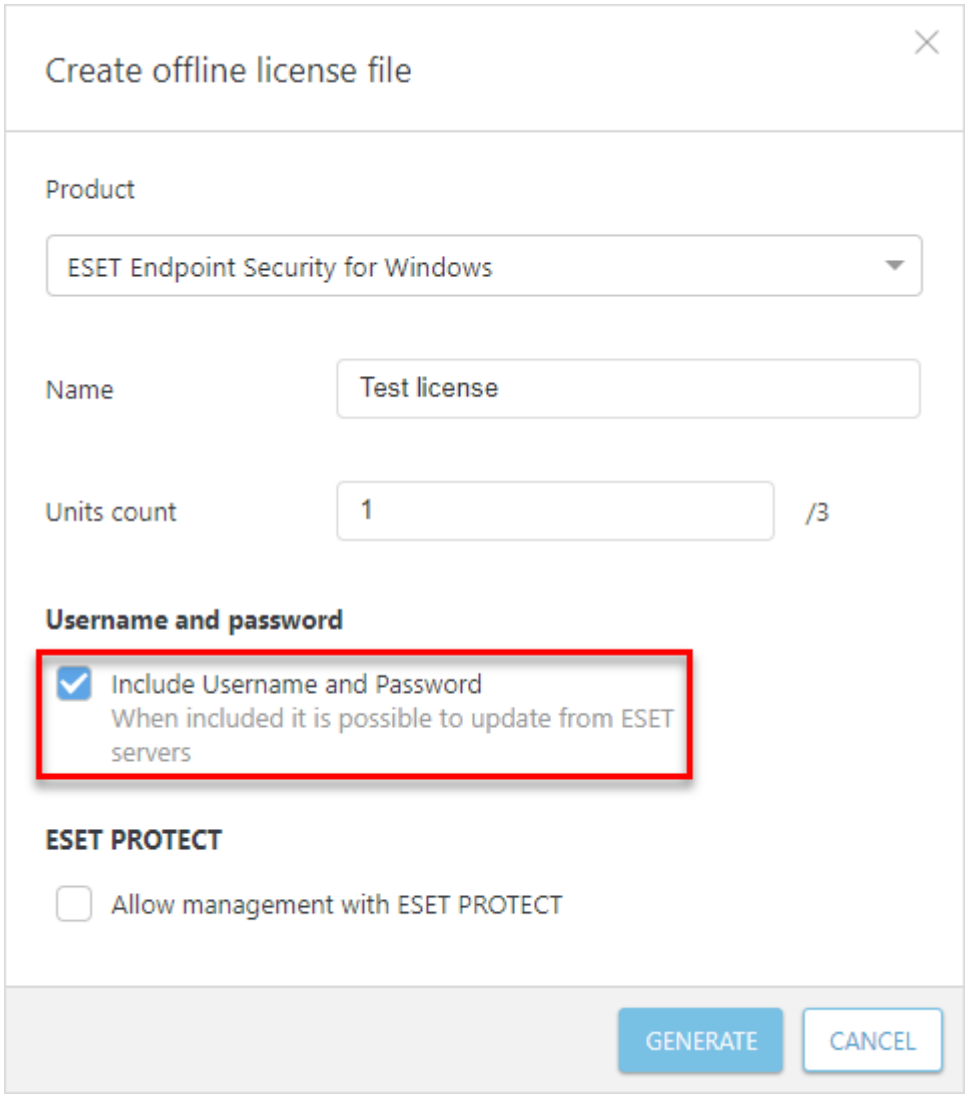
Попередні вимоги відсутні

• Цільова папка має бути доступна для спільного використання, Samba/Windows або служби HTTP/FTP залежно від вибраного способу отримання доступу до оновлень.

  o Продукти з безпеки ESET для Windows: їх можна оновлювати віддалено через HTTP або з використанням спільної папки.

  o Продукти з безпеки ESET для Linux/macOS: їх можна оновлювати віддалено лише через HTTP. Якщо ви використовуєте спільну папку, вона має бути на тому самому комп'ютері, що й продукт із безпеки ESET.

• 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.



Як користуватись інструментом «Дзеркало»

1.Завантажте інструмент «Дзеркало» з цієї сторінки ESET (розділ **Автономні інсталятори**).

2.Розархівуйте завантажений архів.

3.Відкрийте термінал у папці, що містить файл *MirrorTool* і зробіть цей файл виконуваним:

```
chmod +x MirrorTool
```

4.Щоб переглянути всі доступні параметри інструмента «Дзеркало» та його версію, виконайте вказану нижче команду:

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. 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. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --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.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already 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.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Усі фільтри чутливі до регістру.

Параметр	Опис
`--updateServer`	Під час використання потрібно вказати повну URL-адресу сервера оновлення.
`--offlineLicenseFilename`	Необхідно вказати шлях до файлу автономної ліцензії (як згадувалося вище).
`--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`	⚠ 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. Ви можете вказати, які типи файлів оновлення завантажувати. Можливі значення (з урахуванням регістру): • `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. Параметр ігнорується, коли дзеркало створюється для застарілих продуктів (`ep4`, `ep5`).
`--compatibilityVersion`	Цей необов'язковий параметр застосовується до інструмента «Дзеркало», який розповсюджується з продуктом ESET PROTECT 8.1 і пізніших версій. Інструмент «Дзеркало» завантажить файли оновлень, сумісні з версією репозиторію ESET PROTECT, указаною в аргументі параметра у форматі `x.x` або `x.x.x.x`. Наприклад, `--compatibilityVersion 9.0` або `--compatibilityVersion 8.1.13.0`.

ℹ Щоб зменшити обсяг даних, що завантажуються з репозиторію ESET, рекомендуємо використовувати нові параметри в інструменті "Дзеркало", що розповсюджується у складі ESET PROTECT 9: `--filterFilePath` і `--dryRun`. Дотримуйтеся таких інструкцій:
1.Створіть фільтр у форматі *JSON* (див. `--filterFilePath` нижче).
2.Запустіть тестовий інструмент "Дзеркало" з параметром `--dryRun` (див. нижче) і налаштуйте фільтр на свій розсуд.
3.Запустіть інструмент "Дзеркало" з параметром `--filterFilePath` і визначеним фільтром завантаження разом із параметрами `--intermediateRepositoryDirectory` і `--outputRepositoryDirectory`.
4.Регулярно запускайте інструмент "Дзеркало" для того, аби завжди використовувати найновіші інсталятори.

Параметр	Опис

`--filterFilePath`	Цей необов'язковий параметр дає змогу фільтрувати продукти з безпеки ESET на основі текстового файлу (у форматі *JSON*), розміщеного в папці інструмента «Дзеркало», наприклад, `--filterFilePath filter.txt`).
	Опис конфігурації фільтра
	Файл конфігурації для фільтрації продуктів має формат *JSON* із такою структурою:
	• кореневий об'єкт *JSON*:
	o`use_legacy` (логічне значення, необов'язково): якщо має значення true, буде включено застарілі продукти;
	o`defaults` (об'єкт *JSON*, необов'язково): визначає властивості фільтра, які будуть застосовані до всіх продуктів;
	■`languages` (рядок): укажіть коди ISO для мов, які потрібно включити. Наприклад, для французької мови введіть `"fr_FR"`. Коди інших мов наведено в таблиці нижче. Якщо потрібно вказати кілька мов, розділіть їх комами з пробілом. Приклад: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (рядок): платформи, які потрібно включити (`["x64", "x86", "arm64"]`).
	Використовуйте фільтр `platforms` обачливо. Наприклад, якщо інструмент "Дзеркало" завантажує лише 64-розрядні інсталятори, а у вашій інфраструктурі є 32-розрядні комп'ютери, 64-розрядні продукти з безпеки ESET не вдасться інсталювати на 32-розрядних комп'ютерах.
	
	■`os_types` (рядок): типи ОС, які потрібно включити (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (список об'єктів JSON, необов'язково): фільтри для застосування до певних продуктів; перевизначте `defaults` для вказаних продуктів. Об'єкти мають такі властивості:
	■`app_id` (рядок): обов'язково, якщо не вказано `name`.
	■`name` (рядок): обов'язково, якщо не вказано `app_id`.
	■`version` (рядок): визначає версію або діапазон версій, які потрібно включити.
	■`languages` (рядок): коди ISO для мов, які потрібно включити (див. таблицю нижче).
	■`platforms` (рядок): платформи, які потрібно включити (`["x64", "x86", "arm64"]`).
	■`os_types` (рядок): типи ОС, які потрібно включити (`["windows"]`, `["linux"]`, `["mac"]`).
	Щоб визначити відповідні значення для полів, запустіть інструмент "Дзеркало" в режимі тестового виконання й знайдіть відповідний продукт у створеному файлі CSV.
	Описи формату рядка версії
	Усі номери версій складаються з чотирьох цифр, розділених крапками (наприклад, `7.1.0.0`). Під час створення фільтрів версій можна вказати меншу кількість номерів (наприклад, `7.1`), тоді решта номерів будуть нульовими (версія `7.1` ідентична версії `7.1.0.0`).
	Рядок версії може бути в одному з таких форматів:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oВибирає версії, які порівняно зі вказаною версією будуть мати такі відношення: більше/менше, дорівнює/менше або дорівнює/дорівнює.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oВибирає версії, які є не меншими за нижню межу або не більшими за верхню межу.
	Кожна частина номеру версії порівнюється арифметично зліва направо.
	Приклад JSON
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Параметр `--filterFilePath` тепер використовується замість параметрів `--languageFilterForRepository`, `--productFilterForRepository` і `--downloadLegacyForRepository`, які використовувалися в старіших версіях інструмента "Дзеркало" (який випускався з ESET PROTECT 8.x).

Параметр	Опис
`--dryRun`	Якщо використовується цей необов'язковий параметр, інструмент «Дзеркало» не завантажуватиме жодних файлів, проте згенерує файл *.csv* з усіма пакетами для завантаження. Цей параметр можна використовувати без обов'язкових параметрів `--intermediateRepositoryDirectory` й `--outputRepositoryDirectory`. Наприклад, `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. ℹ Деякі інсталятори ESET є універсальними з точки зору мови (з кодом мови `multilang`), тому інструмент "Дзеркало" помістить їх у файл *.csv*, навіть якщо ви вкажете конкретні `мови` в параметрі `--filterFilePath`. Якщо ви використовуєте параметр `--dryRun` разом із параметрами `--intermediateRepositoryDirectory` й `--outputRepositoryDirectory`, інструмент «Дзеркало» не очищує значення *outputRepositoryDirectory*.
`--listUpdatableProducts`	Список усіх продуктів ESET, для яких Mirror Tool може завантажити оновлення модуля (якщо не використовується параметр `--excludedProducts`). Цей параметр доступний у таких версіях Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

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 PROTECT 9 із дзеркала, для параметра Сервер оновлень встановіть указане нижче значення (відповідно до основного розташування сервера HTTP): `http://your_server_address/mirror/eset_upd/era6`
Примітка: Папка дзеркала `era6` є спільною для цих рішень віддаленого управління ESET: ERA 6, ESMC 7, ESET PROTECT.

Таблиця кодів мов

```
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, визначених у файлі *filter.txt* (див. приклад вмісту файлу в описі параметра `--filterFilePath` вище):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

ESET рекомендує видалити з історії командного рядка команди, що містять важливі дані (наприклад, пароль):
1.Запустіть `history`, щоб переглянути список усіх команд в історії.
2.Запустіть `history -d line_number` (укажіть номер рядка команди). Окрім того, можна запустити `history -c`, щоб видалити всю історію командного рядка.

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 кожну 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 кластери Red Hat Linux 7 і вище. Відмовостійкий кластер працює лише в активному/пасивному режимі за допомогою диспетчера кластера `rgmanager`.

Попередні вимоги відсутні

• 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 7.

Область

Компоненти ESET PROTECT, які можна встановити на кластері високої доступності **Red Hat Linux**:

• Сервер ESET PROTECT з агентом ESET Management: без інстальованого агента ESET Management служба кластера 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.

• Зверніть 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 каталозі */usr/share/erag2cluster* створіть такі каталоги:

/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:
/etc/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator*
/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/opt/eset/RemoteAdministrator*
/var/log/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/var/log/eset/RemoteAdministrator*
/var/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator*

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/Remo
teAdministrator/Server

ln -
s /usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server /opt/eset/RemoteAdmini
strator/Server

ln -
s /usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server /var/log/eset/Remo
teAdministrator/Server

ln -
s /usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server /var/opt/eset/Remo
teAdministrator/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/e
racluster_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/Remo
teAdministrator/Server

ln -
```

```
s /usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server /opt/eset/RemoteAdmini
strator/Server

ln -
s /usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server /var/log/eset/Remo
teAdministrator/Server

ln -
s /usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server /var/opt/eset/Remo
teAdministrator/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/e
racluster_server.sh
```

Наступні кроки виконуються в графічному інтерфейсі адміністрування кластера Conga:

12. Створіть **Групу служб**, наприклад PROTECTService.

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 в групу PROTECTService.

Після успішного налаштування кластера серверів інсталюйте 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.

Інструкції з інсталяції для вибраних дистрибутивів Linux

Інструкції для конкретного дистрибутива ви можете дізнатися у таких статтях нашої бази знань:

- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

Перед інсталяцією

1. Перевірте наявність у вашій мережі сервера бази даних та доступу до нього на локальному/віддаленому сервері. Якщо сервер бази даних не інстальовано, інсталюйте 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

У вас має бути можливість виконувати команду `sudo` або інсталювати файли від імені користувача `root`.

1. Інсталюйте 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. Інсталюйте потрібні пакети Java й Tomcat, потім інсталюйте 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. Інсталюйте агент ESET Management на комп'ютер із сервером.

ESET рекомендує видалити з історії командного рядка команди, що містять важливі дані (наприклад, пароль):
1.Запустіть `history`, щоб переглянути список усіх команд в історії.
2.Запустіть `history -d line_number` (укажіть номер рядка команди). Окрім того, можна запустити `history -c`, щоб видалити всю історію командного рядка.

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.

macOS підтримується лише як клієнт. Агент ESET Management і продукти ESET для macOS можна інсталювати в macOS. Однак сервер ESET PROTECT не можна інсталювати в macOS.

Інсталяція агента – macOS

Нижче описано локальну інсталяцію агента.

1. Переконайтеся, що всі **попередні вимоги** виконано:

   • На комп'ютері із сервером інстальовано ESET PROTECTсервер і ESET PROTECTвеб-консоль .

   • Створено сертифікат агента, збережений на локальному диску.

   • На локальному диску підготовлено центр сертифікації (лише для непідписаних сертифікатів).

Якщо під час віддаленого розгортання агента ESET Management виникають проблеми (серверне завдання **Розгортання агента** завершується помилкою), див. розділ Виправлення неполадок із розгортанням 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.

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.

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

6. Перегляньте місце встановлення та натисніть **Інсталювати**. 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

> 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 **OK** > **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=srv` і натисніть **Enter**.

4.Введіть `_era._tcp.domain.name` і натисніть **Enter**. Відобразиться розташування служби.

> **i** 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

Щоб інсталювати ESET PROTECT і його компоненти в середовищах без доступу до Інтернету, дотримуйтеся інструкцій із високорівневої інсталяції (за наявності ESET PROTECT, інстальованого в ОС Windows).

На комп'ютері з доступом до Інтернету

1. Створіть спільну мережеву папку.
2. Завантажте в спільну папку такі інсталятори:
   - ESET PROTECT Універсальний інсталятор
   - Підтримуваний пакет JDK (потрібен для веб-консолі).
   - Інсталятор агента ESET Management
   - Інсталятори продукту з безпеки ESET (наприклад, ESET Endpoint Security)

На автономному комп'ютері Windows у тій самій локальній мережі

1. Скопіюйте інсталятори з мережевої спільної папки на автономний комп'ютер Windows, на який потрібно інсталювати ESET PROTECT.
2. Інсталюйте пакет JDK.
3. Інсталюйте ESET PROTECT у Windows за допомогою універсального інсталятора. Під час інсталяції виберіть **Активувати пізніше**.
4. Активація ESET PROTECT за допомогою автономної ліцензії.

5. Розгорніть агент ESET Management на комп'ютерах в автономному середовищі за допомогою Live installer агента. Змініть сценарій інсталяції, щоб використовувати нову URL-адресу для пакета інсталяції агента зі спільної мережевої папки.

6. Розгорніть продукти з безпеки ESET на робочих станціях за допомогою завдання інсталяції програмного забезпечення. Клацніть **<Choose package>** і вкажіть спеціальну URL-адресу пакета інсталяції в локальному репозиторії.

7. Активуйте керовані робочі станції за допомогою автономної ліцензії.

8. Вимкнути ESET LiveGrid®.

Наполегливо рекомендуємо регулярно оновлювати автономну інфраструктуру ESET через локальний репозиторій оновлень. Регулярно оновлюйте модулі продукту з безпеки ESET. Якщо модулі не оновлюються, веб-консоль ESET PROTECT позначає комп'ютери надписом **Не оновлено**. Щоб вимкнути це попередження веб-консолі, клацніть комп'ютер у списку і в контекстному меню виберіть пункт **Увімкнути режим без звуку**.

Вказівки з оновлення ESET PROTECT доступні в розділі Оновлення компонентів ESET PROTECT в автономному середовищі.

Процедури оновлення, міграції та повторної інсталяції

Існує кілька способів оновити, перенести чи повторно інсталювати сервер ESET PROTECT та інші компоненти ESET PROTECT.

Переконайтеся, що маєте підтримувану операційну систему перед оновленням до ESET PROTECT 9.0. Компонент сервера ESET PROTECT версії 9.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 7.0 до 9.0.
• Якщо ви вже запустили оновлення й система не працює, уручну повторно інсталюйте всі компоненти ESET PROTECT в оригінальній версії.
• Перед оновлення перенесіть поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустіть завдання оновлення.
Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MS SQL 2008/2012), оновіть базу даних до сумісної версії, перш ніж оновлювати сервер ESET PROTECT.
ESET PROTECT 9.0 використовує LDAPS як протокол за замовчуванням для синхронізації Active Directory. Якщо використовується синхронізація Active Directory, оновлення версій 7.0–7.1 на машині Windows до ESET PROTECT 9.0. призведе до помилки завдання синхронізації в ESET PROTECT 9.0.

Оновлення з ERA 5 або 6.5

Пряме оновлення не підтримується: див. тему Перенесення з ERA 5.x або Перенесення з ERA 6.x.

Оновлення з ESMC 7.x до ESET PROTECT версії 9.0

Виберіть одну з процедур оновлення:

Процедури оновлення	Операційна система	Коментар
Завдання Оновлення компонентів на веб-консолі	Windows/Linux	
ESET PROTECT 9.0 Універсальний інсталятор	Windows	Універсальний інсталятор рекомендується використовувати, якщо наявну інсталяцію виконано за допомогою універсального інсталятора (інсталяції бази даних MS SQL і Apache Tomcat за замовчуванням).
Оновлення компонентів уручну	Linux	Інструкції для Linux для досвідчених користувачів.

Щоб дізнатися версію кожного використовуваного компонента ESET PROTECT, перевірте, яку версію сервера ESET PROTECT у вас інстальовано. Відкрийте сторінку Про програму на веб-консолі ESET PROTECT. На цій сторінці відображається список всіх версій компонентів ESET PROTECT.

Перенесіть ESET PROTECT 9 з одного сервера на інший або заново інсталюйте його

Перенесіть дані з одного сервера на інший або повторно інсталюйте сервер ESET PROTECT.

Щоб 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.

Інші процедури

Змінення IP-адреси чи імені хосту на сервері ESET PROTECT.

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.

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.

Виконуєте оновлення з віртуального пристрою ESMC?

Екземпляр сервера ESET PROTECT інстальовано на відмовостійкому кластері?

Якщо екземпляр сервера ESET PROTECT інстальовано 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 2.[x.xx]\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.

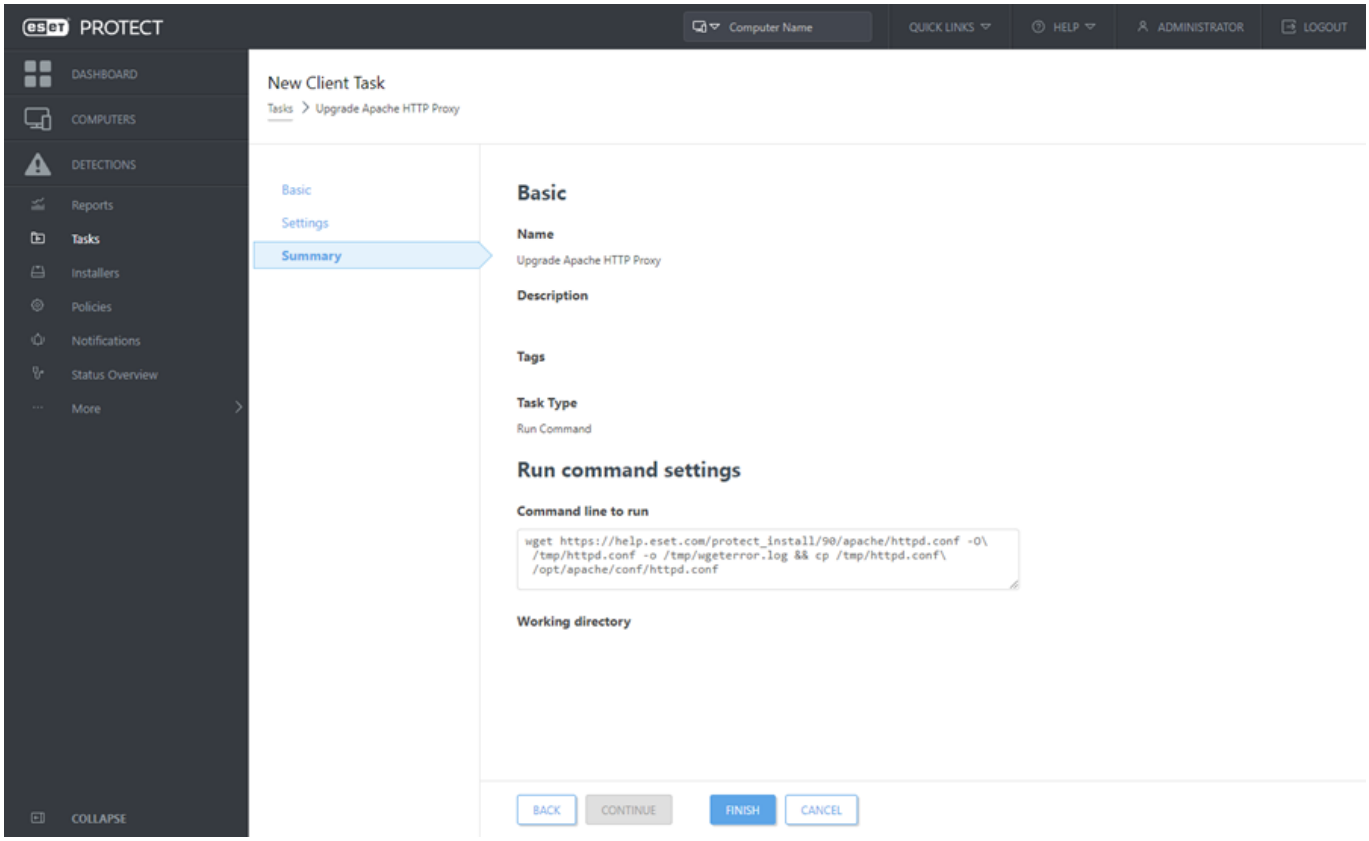
Коли ви оновите Apache HTTP Proxy у Windows і задасте налаштовувані параметри в оригінальному файлі *httpd.conf* (наприклад, ім'я користувача та пароль), скопіюйте параметри з резервної копії файлу *httpd.conf* і застосуйте налаштовувані параметри лише в новому файлі *httpd.conf*. Не використовуйте оригінальний 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/90/apache/httpd.conf -O\
 /tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
 /opt/apache/conf/httpd.conf
```



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.

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* уручну. Перегляньте додаткові параметри в розділі Інсталяція проксі-сервера Apache HTTP – Linux.

Виконати оновлення до ESET PROTECT 9.0 можна тільки з ESMC версії 7.0 і новіших.
ESET PROTECT 9 відображає автоматичне сповіщення за наявності більш нової версії сервера ESET PROTECT.
Перед запуском оновлення створіть резервну копію таких даних:
• усіх сертифікатів (центр сертифікації, сертифікат сервера та сертифікат агента).
• Експортуйте свої сертифікати від Центру сертифікації зі старого сервера ESET PROTECT у файл *.der* і збережіть його в зовнішньому сховищі.
• Експортуйте 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 ESMC/ESET PROTECT. Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MS SQL 2008/2012), оновіть базу даних до сумісної версії, перш ніж оновлювати сервер ESET PROTECT.

Переконайтеся, що маєте підтримувану операційну систему перед оновленням до ESET PROTECT 9.0.
Компонент сервера ESET PROTECT версії 9.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 7.0 до 9.0.
• Якщо ви вже запустили оновлення й система не працює, уручну повторно інсталюйте всі компоненти ESET PROTECT в оригінальній версії.
• Перед оновлення перенесіть поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустіть завдання оновлення.
ESET PROTECT 9.0 використовує LDAPS як протокол за замовчуванням для синхронізації Active Directory. Якщо використовується синхронізація Active Directory, оновлення версій 7.0–7.1 на машині Windows до ESET PROTECT 9.0. призведе до помилки завдання синхронізації в ESET PROTECT 9.0.
Щоб оновити продукти з безпеки ESET, запустіть завдання інсталяції програми за допомогою пакета інсталятора останньої версії для інсталяції найновішої версії 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.

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.

Щоб оновити агенти ESET Management Agent на всіх керованих комп'ютерах у мережі, укажіть статичну групу **Всі** цільовою для завдання **Оновити компоненти ESET PROTECT**. Завдання пропускає комп'ютери, на яких уже виконується найновіший агент ESET Management.
ESET PROTECT 9.0 підтримує автоматичне оновлення агента ESET Management на керованих комп'ютерах.

Компоненти, які оновлюються автоматично:

- ESET PROTECTСервер
- ESET Management Агент
- 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/*).

Обмеження для оновлення веб-консолі
- Apache Tomcat не оновлюється під час оновлення веб-консолі ESET PROTECT за допомогою завдання з оновлення компонентів.
- Оновлення веб-консолі ESET PROTECT не виконується, якщо Apache Tomcat встановлено в інше місце.
- Якщо інстальовано налаштовувану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інсталятора або завдання «Оновлення компонентів» не підтримується.

- ESET PROTECT Mobile Device Connector

Компоненти, для яких потрібне оновлення 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 інсталятора, див. Оновлення Проксі-сервер Apache HTTP)
- ESET Rogue Detection Sensor: для оновлення використовуйте завдання інсталяції програми. Окрім цього, можна інсталювати новішу версію поверх наявної (дотримуйтеся інструкцій з інсталяції для Windows або Linux). Якщо ви встановили RD Sensor з ESMC версії 7.2 і новіших версій, виконувати оновлення не потрібно, оскільки це остання версія RD Sensor.

Виправлення неполадок

- 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.

Використання універсального інсталятора ESET PROTECT 9.0 для оновлення

Використовуйте універсальний інсталятор ESET PROTECT 9.0 для оновлення ESMC 7.x або старішої версії ESET PROTECT до останньої версії ESET PROTECT 9.0.

Універсальний інсталятор рекомендується використовувати, якщо наявну інсталяцію виконано за допомогою універсального інсталятора (інсталяції бази даних MS SQL і Apache Tomcat за замовчуванням).

ESET PROTECT 9.0 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.

- Інсталятор автоматично генерує випадковий пароль для автентифікації бази даних (зберігається в *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

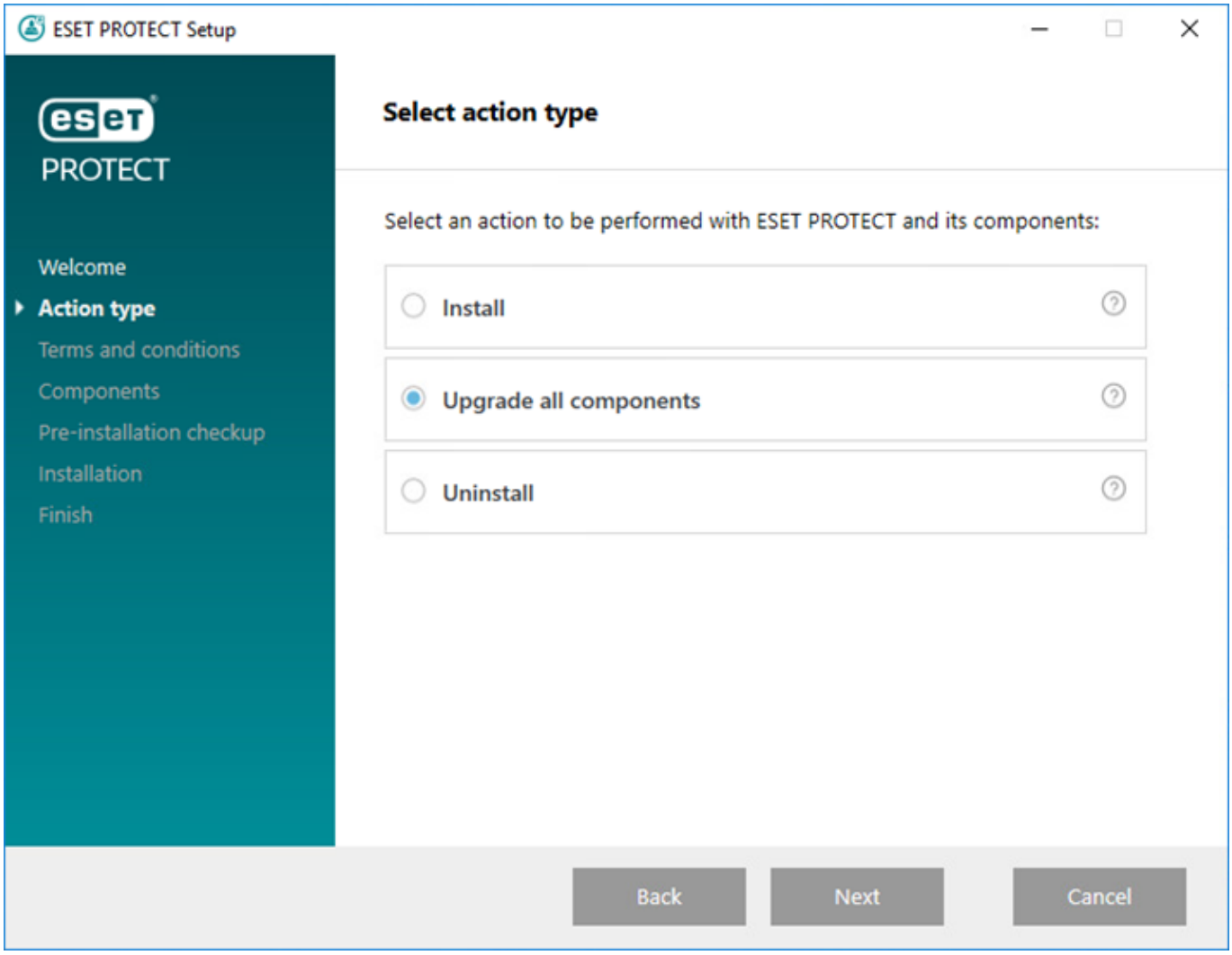
Розмір однієї реляційної бази даних у Microsoft SQL Server Express не може перевищувати 10 ГБ. Не рекомендується використовувати Microsoft SQL Server Express:
- у корпоративних середовищах або великих мережах;
- якщо ESET PROTECT буде використовуватися з ESET Enterprise Inspector.

Виконати оновлення до ESET PROTECT 9.0 можна тільки з ESMC версії 7.0 і новіших.
Перед запуском оновлення створіть резервну копію таких даних:
• усіх сертифікатів (центр сертифікації, сертифікат сервера та сертифікат агента).
• Експортуйте свої сертифікати від Центру сертифікації зі старого сервера ESET PROTECT у файл *.der* і збережіть його в зовнішньому сховищі.
• Експортуйте 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 ESMC/ESET PROTECT. Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MS SQL 2008/2012), оновіть базу даних до сумісної версії, перш ніж оновлювати сервер ESET PROTECT.
Переконайтеся, що маєте підтримувану операційну систему перед оновленням до ESET PROTECT 9.0.
Компонент сервера ESET PROTECT версії 9.0 не сумісний із 32-розрядними комп'ютерами (архітектура x86). 32-розрядний комп'ютер із сервером не вдасться оновити з версій 7.0 до 9.0.
• Якщо ви вже запустили оновлення й система не працює, уручну повторно інсталюйте всі компоненти ESET PROTECT в оригінальній версії.
• Перед оновлення перенесіть поточний компонент ESET PROTECT на 64-розрядний комп'ютер і після цього запустіть завдання оновлення.
ESET PROTECT 9.0 використовує LDAPS як протокол за замовчуванням для синхронізації Active Directory. Якщо використовується синхронізація Active Directory, оновлення версій 7.0–7.1 на машині Windows до ESET PROTECT 9.0. призведе до помилки завдання синхронізації в ESET PROTECT 9.0.

1.Запустити *Setup.exe*.

2.Виберіть мову й натисніть **Далі**.

3.Виберіть **Оновити всі компоненти** й натисніть **Далі**.



4.Прочитайте **ліцензійну угоду з кінцевим користувачем**, прийміть її й натисніть **Далі**.

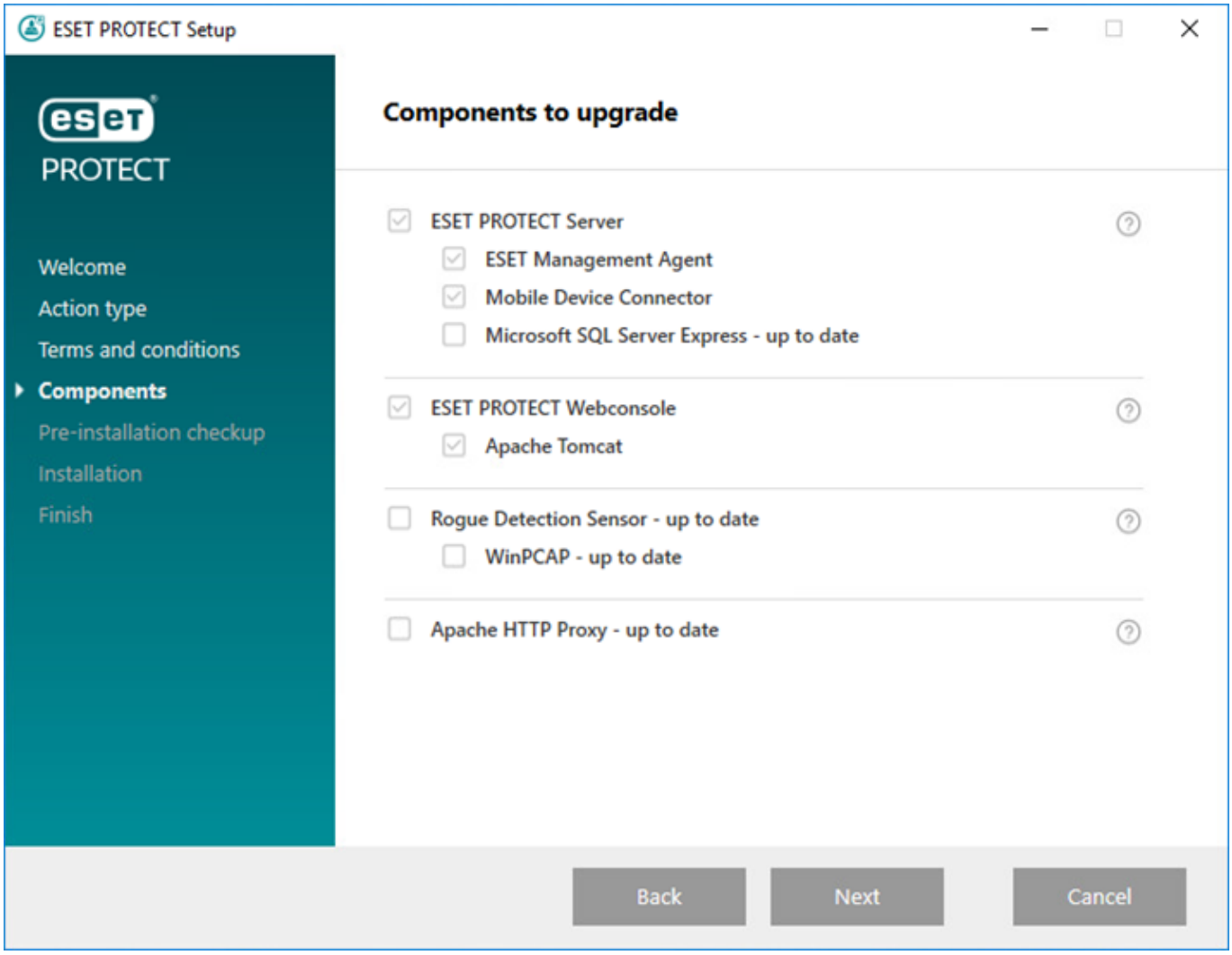
5.У розділі **Компоненти** перегляньте компоненти ESET PROTECT, які можна оновити, і клацніть **Далі**.

Обмеження для оновлення Apache Tomcat і веб-консолі

- Якщо інстальовано налаштовувану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інсталятора 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 ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 9.0. Це необхідно для того, що ви мали найновішу автономну довідку, яка відповідає вашій версії ESET PROTECT.

Обмеження оновлення проксі-сервера Apache HTTP

Універсальний інсталятор замінює файл *httpd.conf*, а для оригінальної конфігурації створює файл *httpd.conf.old*. Щоб зберегти настроювану конфігурацію проксі-сервера Apache HTTP, створіть її резервну копію для подальшого використання.



6.Дотримуйтеся інструкцій у розділі **Перевірка перед інсталяцією**, щоб переконатися, що система відповідає всім вимогам.

7.Клацніть **Оновити**, щоб запустити оновлення ESET PROTECT. Оновлення може тривати певний час залежно від конфігурації системи й мережі.

8.Коли оновлення завершиться, клацніть **Готово**.

9.Після оновлення ESET PROTECT оновіть агент ESET Management на керованих комп'ютерах за допомогою завдання оновлення компонентів. ESET PROTECT 9.0 підтримує автоматичне оновлення агента ESET Management на керованих комп'ютерах.

Перенесення з ERA 5.x

Неможливо напряму оновити або виконати перехід із ERA 5.x до ESET PROTECT 9.0.

Якщо ви інсталювали ERA 5.x, виконайте такі дії:

1.Перейдіть із ERA 5.x до ESMC 7.2

2.Оновіть ESMC 7.2 до ESET PROTECT 9.0

Оновлення з ERA 6.5

Неможливо напряму виконати оновлення до ESET PROTECT 9.0.

Якщо ви інсталювали ERA 6.5, виконайте такі дії:

1. Оновіть ERA 6.5 до ESET PROTECT 8.1.
2. Оновіть ESET PROTECT 8.1 до ESET PROTECT 9.0.

Перенесення з одного сервера на інший

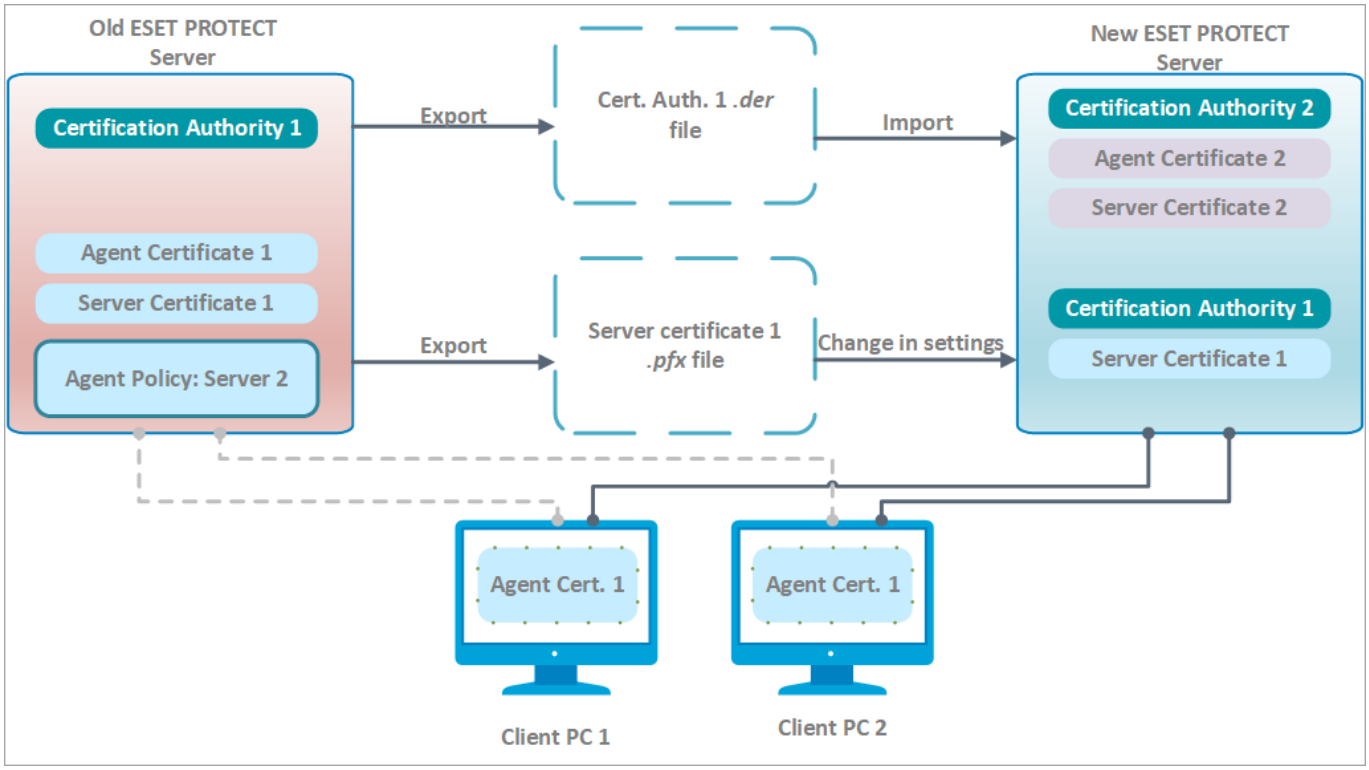
Існує кілька способів перенести ESET PROTECT з одного сервера на інший (ці сценарії можна використовувати під час повторної інсталяції ESET PROTECT Server).

- 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 MS SQL у MS SQL) 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. Новий сервер ESET PROTECT матиме **таку саму IP-адресу**, що й попередній, але не буде використовувати базу даних зі старого сервера ESET PROTECT.

Згідно з наведеними нижче інструкціями потрібно, щоб на старому сервері ESET PROTECT була доступна веб-консоль. Якщо старий сервер ESET PROTECT недоступний, дотримуйтеся таких інструкцій:
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. Додайте клієнтські комп'ютери в інфраструктуру ESET PROTECT і розгорніть агент ESET Management локально або віддалено.



Збільшити зображення

❑На поточному (старому) сервері ESET PROTECT виконайте вказані нижче дії.

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*.

   • Експортуйте 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.

Поки не видаляйте й не виводьте з роботи свій старий ESET PROTECT Server.

❑ На новому сервері ESET PROTECT виконайте вказані нижче дії.

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 компютера, 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. Імпортуйте 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. Імпортуйте всі відповідні ліцензії ESET до ESET PROTECT.

6. Перезавантажте службу сервера ESET PROTECT. Докладніше див. у статті бази знань.

Коли спливе час, еквівалентний одному або двом інтервалам підключення агента, клієнтські комп'ютери мають підключатися до нового сервера ESET PROTECT за допомогою оригінального сертифіката агента ESET Management, який автентифікується ЦС, імпортованим зі старого сервера ESET PROTECT. Якщо клієнти не підключаються, перегляньте розділ Проблеми після оновлення/перенесення сервера ESET PROTECT.

Коли додаєте нові клієнтські комп'ютери, використовуйте нові Центри сертифікації для підпису сертифікатів агента. За допомогою імпортованих ЦС не можна підписувати нові сертифікати одноранговых 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.

- Перенесення баз даних підтримується лише для ідентичних типів баз даних (з MySQL у MySQL і з MS SQL у MS SQL).
- 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:**

Перенесення бази даних на іншу IP-адресу рекомендується виконувати лише досвідченим користувачам. Якщо новий ESET PROTECT Server має **іншу IP-адресу**, виконайте вказані додаткові дії по відношенню до поточного (старого) ESET PROTECT Server:
a)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.
b)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).

Поки не видаляйте й не виводьте з роботи свій старий ESET PROTECT Server.

❑ **На новому сервері ESET PROTECT виконайте вказані нижче дії.**

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 інсталятора (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.

5. Виберіть пункти **Докладніше** > **Параметри сервера** > **Підключення**. Клацніть **Змінити сертифікат** > **Відкрити список сертифікатів** і виберіть **Сертифікат сервера** для старого сервера ESET PROTECT, потім двічі клацніть **OK**.

6. Перезавантажте службу ESET PROTECT Server.

7. Увійдіть на веб-консоль ESET PROTECT і клацніть **Комп'ютери**.

Коли спливе час, еквівалентний одному або двом інтервалам підключення агента, клієнтські комп'ютери мають підключатися до нового сервера ESET PROTECT за допомогою оригінального сертифіката агента ESET Management. 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 (або ESMC Server) 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 9.0 Універсальний інсталятор за замовчуванням інсталює Microsoft SQL Server Express 2019.

oЯкщо ви використовуєте старіші випуски Windows (Server 2012 або SBS 2011), Microsoft SQL Server Express 2014 не інсталюватиметься за замовчуванням.

oІнсталятор автоматично генерує випадковий пароль для автентифікації бази даних (зберігається в *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

⚠ 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 або великих мережах;
• якщо ESET PROTECT буде використовуватися з ESET Enterprise Inspector.

• Якщо у вас інстальовано старішу непідтримувану базу даних (MySQL 5.5 або MS SQL 2008/2012), оновіть базу даних до сумісної версії, перш ніж оновлювати сервер ESET PROTECT.

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.

- Щоб налаштувати Microsoft SQL Server та керувати цим сервером (бази даних і користувачі), завантажте SQL Server Management Studio (SSMS).
- Не інсталюйте SQL Server у контролері домену (наприклад, 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).

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. Резервну копію можна використати пізніше під час перенесення ESET PROTECT на новий сервер. Див. розділ, що відповідає базі даних, яку ви використовуєте:

- Назви баз даних і файлів журналів не змінилися навіть після перейменування продукту з ESET Security Management Center на ESET PROTECT.
- Якщо використовується віртуальний пристрій ESET PROTECT, дотримуйтеся інструкцій із резервного копіювання бази даних віртуального пристрою.

Інструкції з резервного копіювання MS SQL

Для резервного копіювання бази даних MS SQL у файл виконайте наведені нижче інструкції:

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'"
```

> У цьому прикладі **HOST** містить IP-адресу або ім'я хоста, а **ERASQL** – ім'я екземпляра сервера MS SQL. Можна інсталювати сервер ESET PROTECT в екземплярі SQL із власною назвою (під час використання бази даних MS SQL). Змініть скрипти резервного копіювання відповідно до цього сценарію використання.

Регулярне резервне копіювання бази даних за допомогою скрипта SQL

Виберіть одну з таких команд SQL:

a)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, CHE
CKSUM, STATS=10"

3.REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)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 DBNAME -r BACKUPFILE
```

У цьому прикладі **HOST** містить IP-адресу або ім'я хоста сервера MySQL, **ROOTLOGIN** – кореневий обліковий запис MySQL Server, а **DBNAME** – 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 DBNAME < BACKUPFILE
```

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 ESMC/ESET PROTECT або проксі-сервера , 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 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 **Microsof 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.

Попередні вимоги відсутні

• Необхідно інсталювати 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 інсталювати на обидва комп'ютери.

Міграцію за допомогою SQL Server Management Studio.

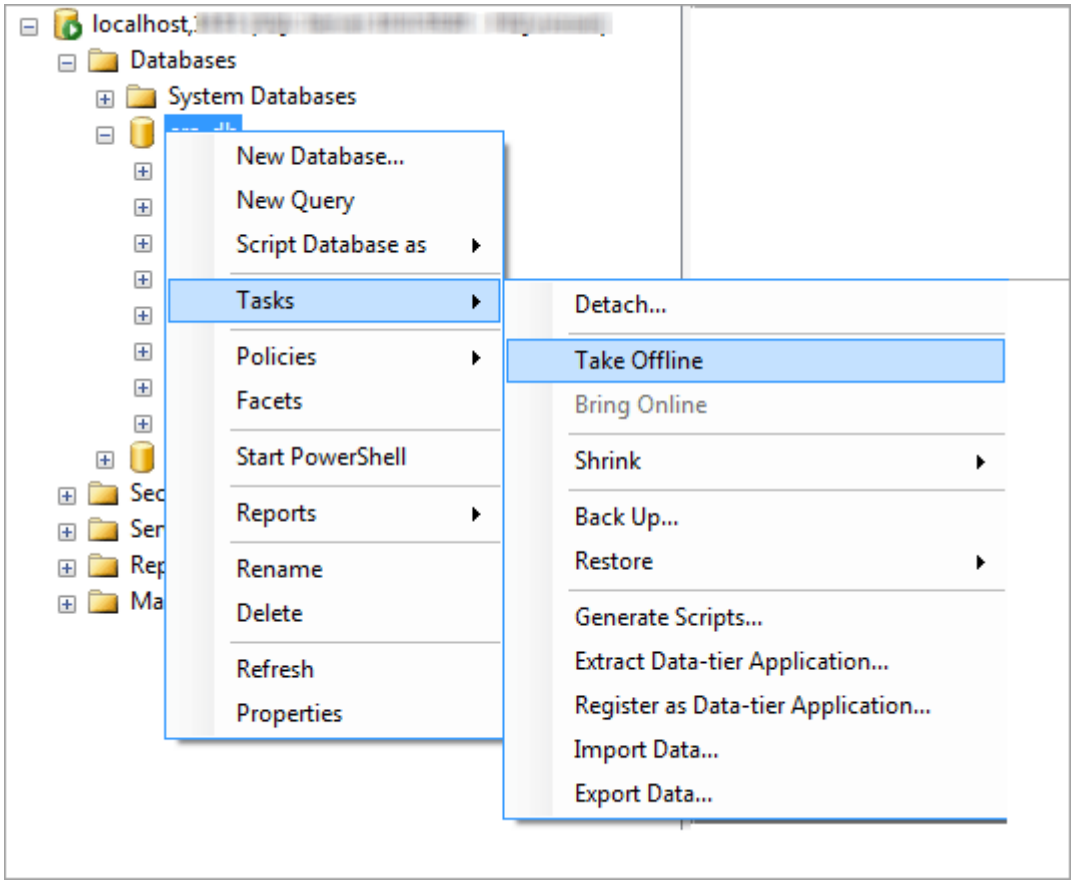
1. Зупиніть роботу служби ESET PROTECT Server (служби ESMC Server) або служби ESET PROTECT MDM.

⚠ 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.

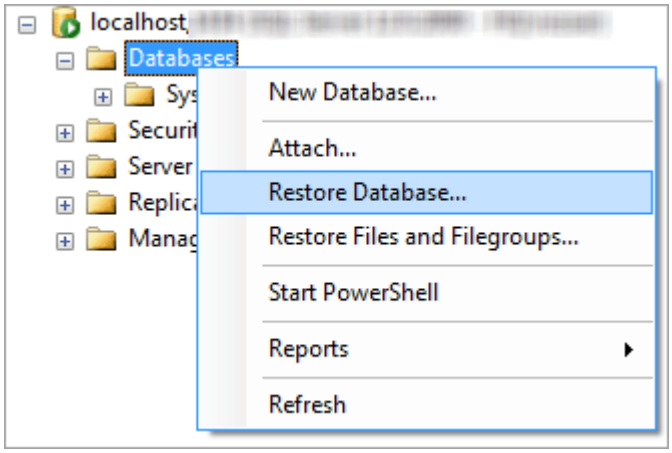
4. Виберіть **Завдання** > **Відключити**, щоб відключити вихідну базу даних від мережі.



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.

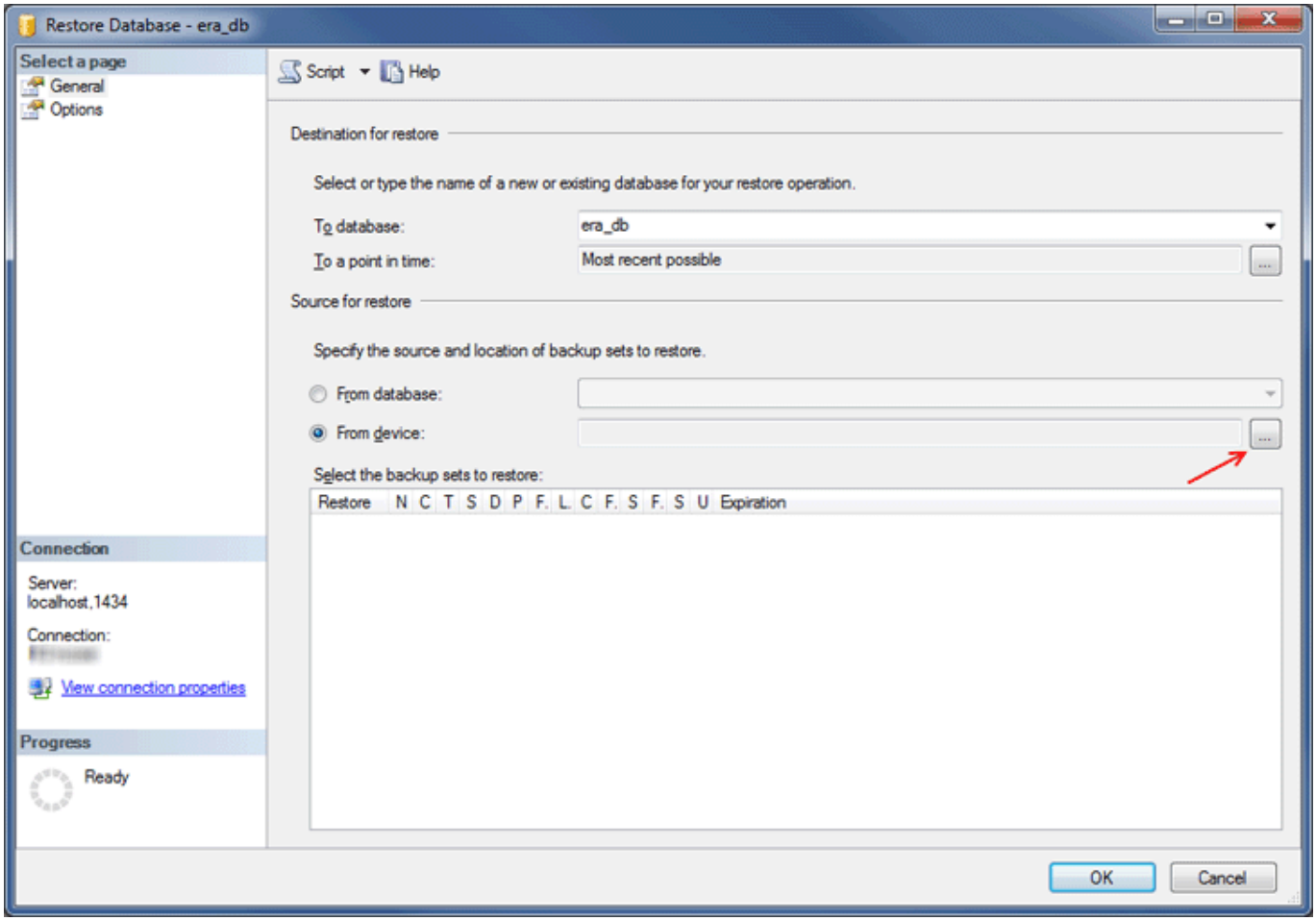
6. Увійдіть у цільовий екземпляр SQL Server за допомогою SQL Server Management Studio.

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 «...».

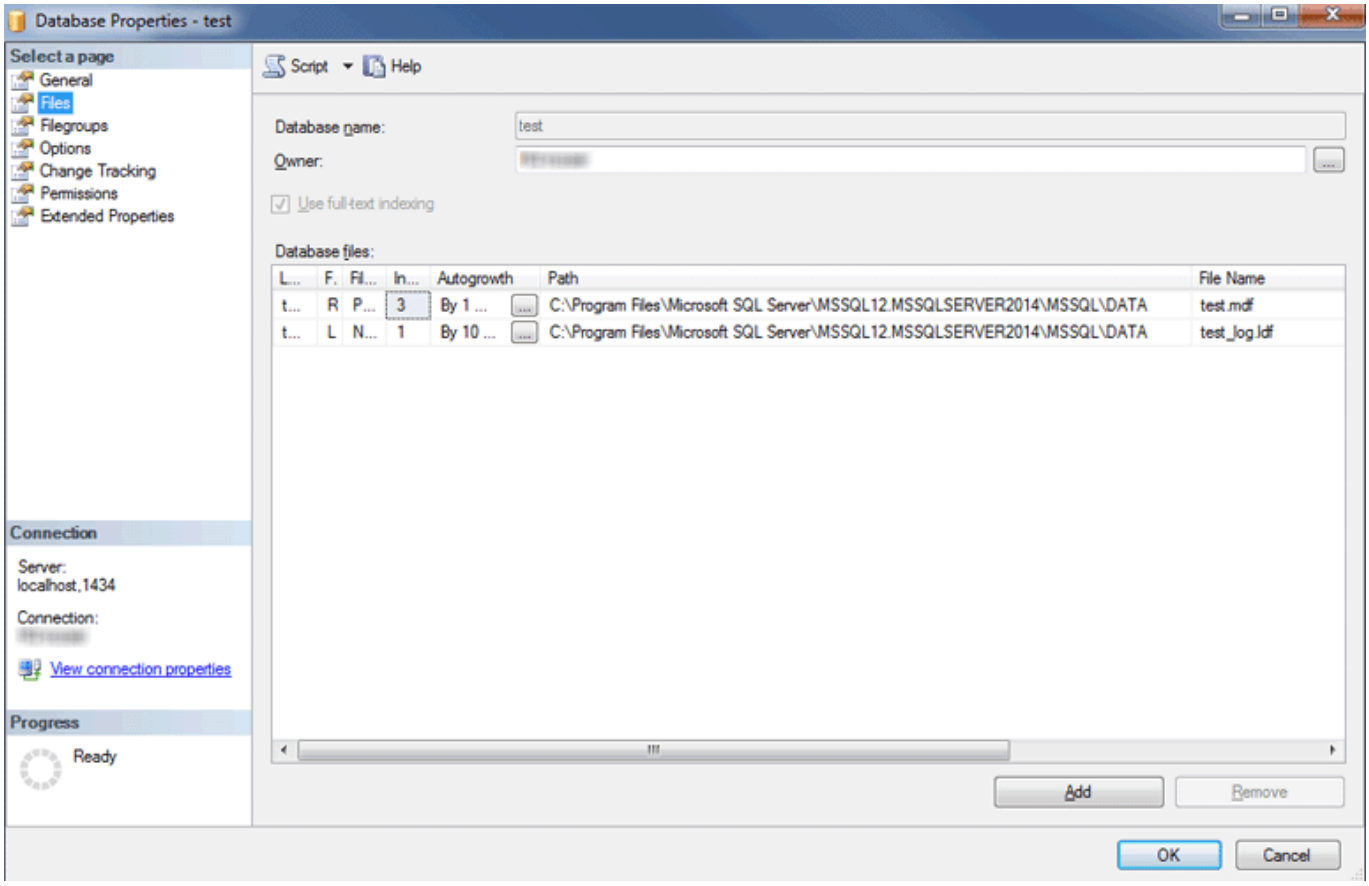


10. Клацніть **Додати**, перейдіть до резервної копії та відкрийте її.

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.

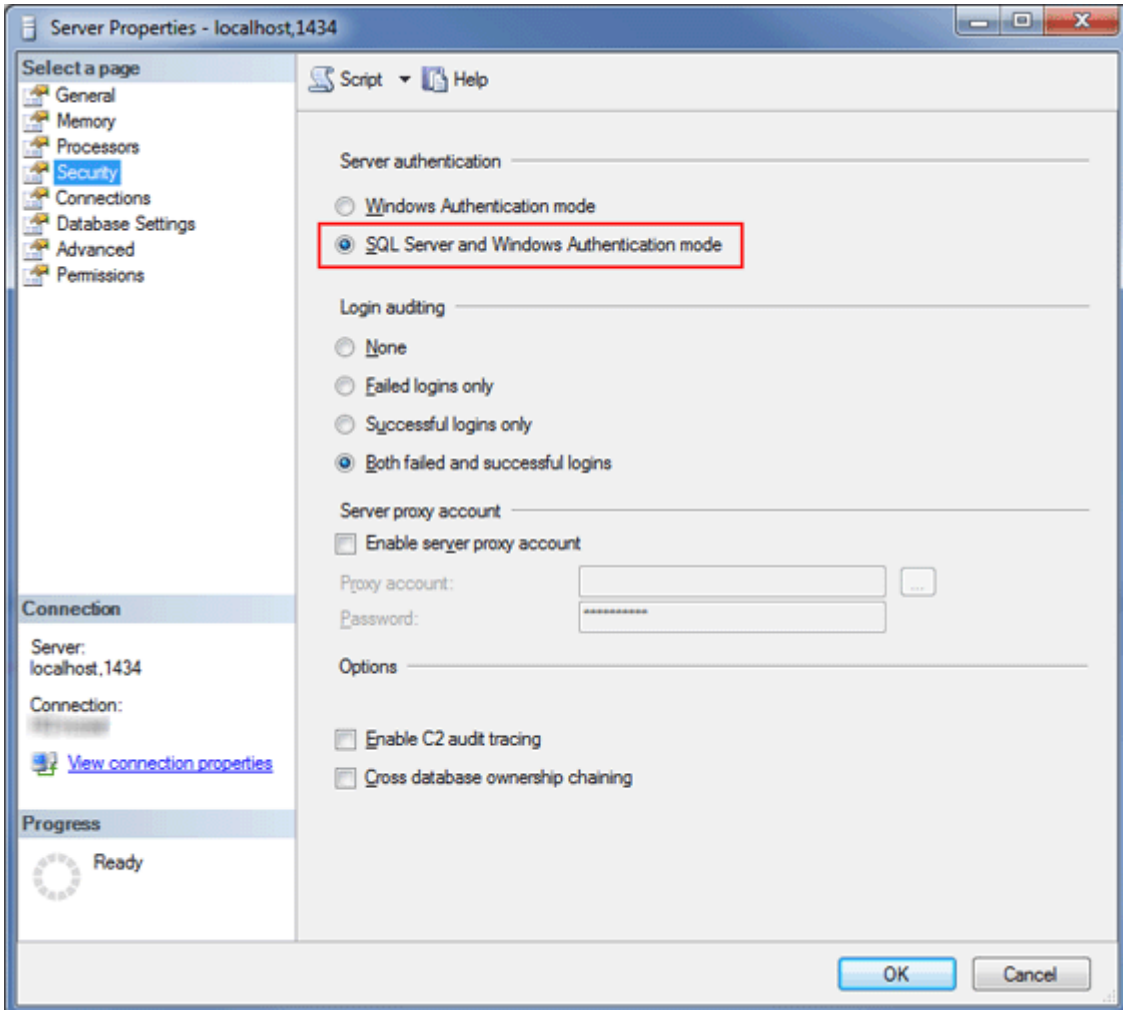


13. Натисніть **OK** у вікні майстра відновлення.

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):

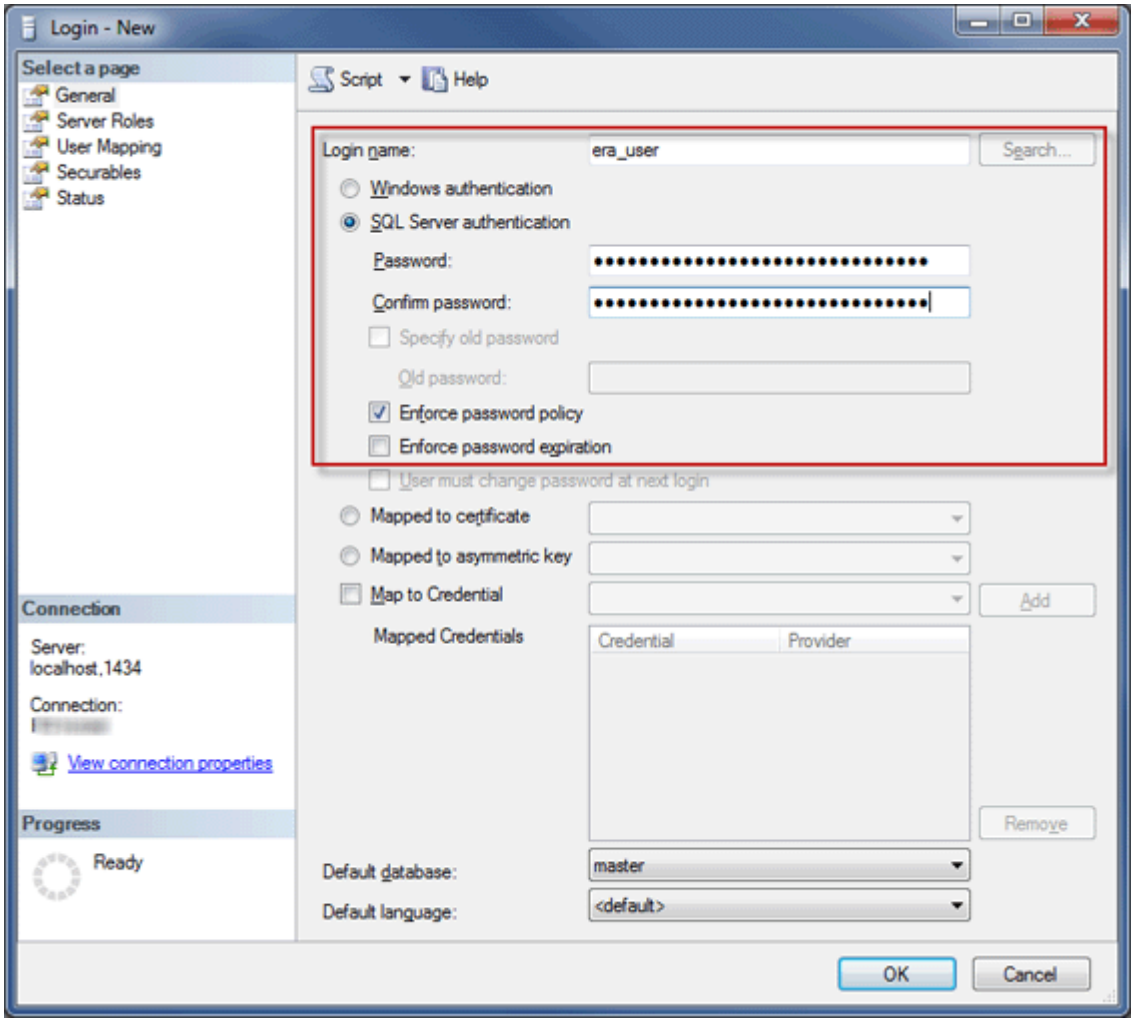
```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

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 переконайтеся, що пункт **Режим автентифікації SQL Server та Windows** вибрано.

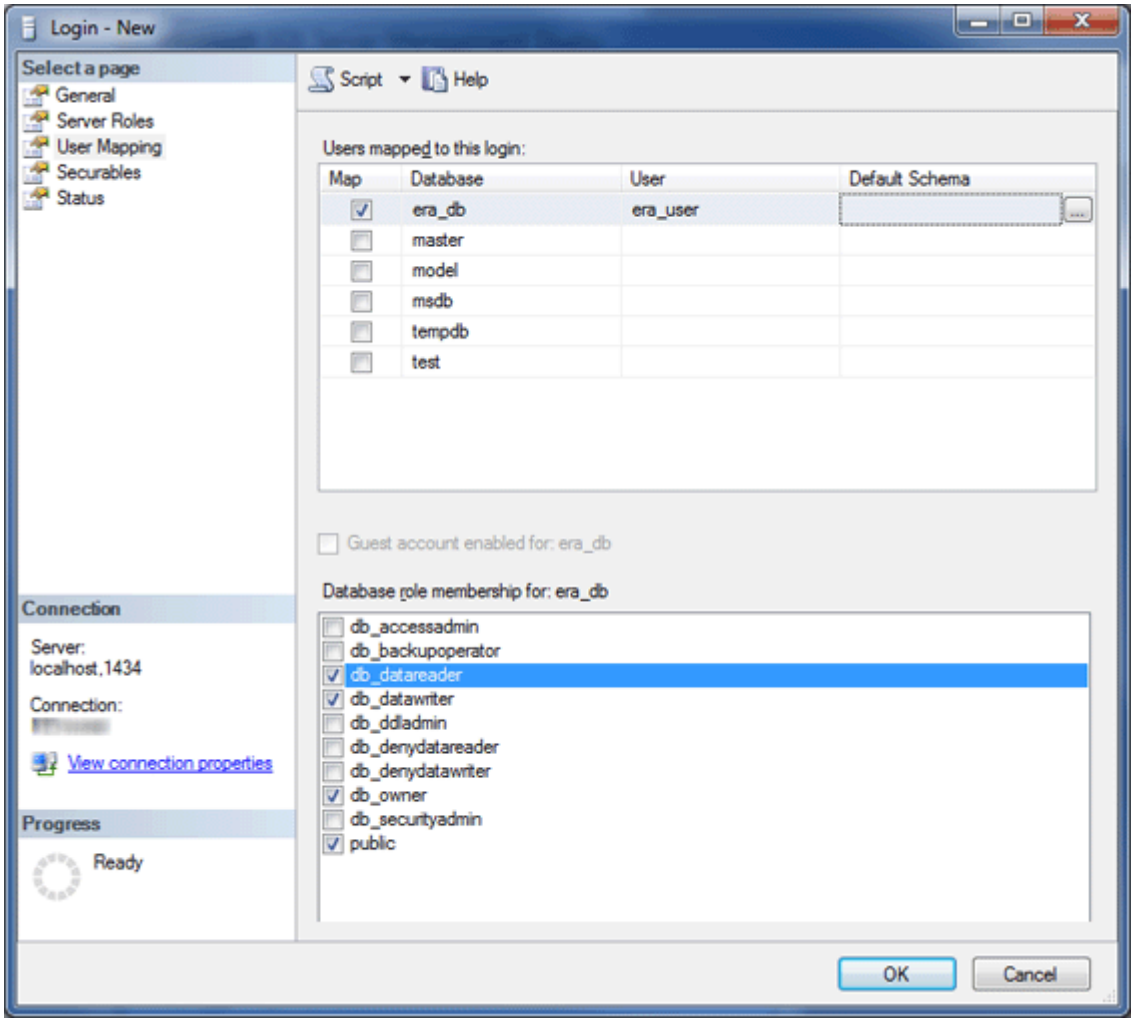


16. Створіть нове ім’я користувача для SQL Server (для сервера ESET PROTECT/ESET PROTECT MDM) на цільовому SQL Server в пункті **Автентифікація SQL Server** та призначте це ім’я для користувача з відновленої бази даних.

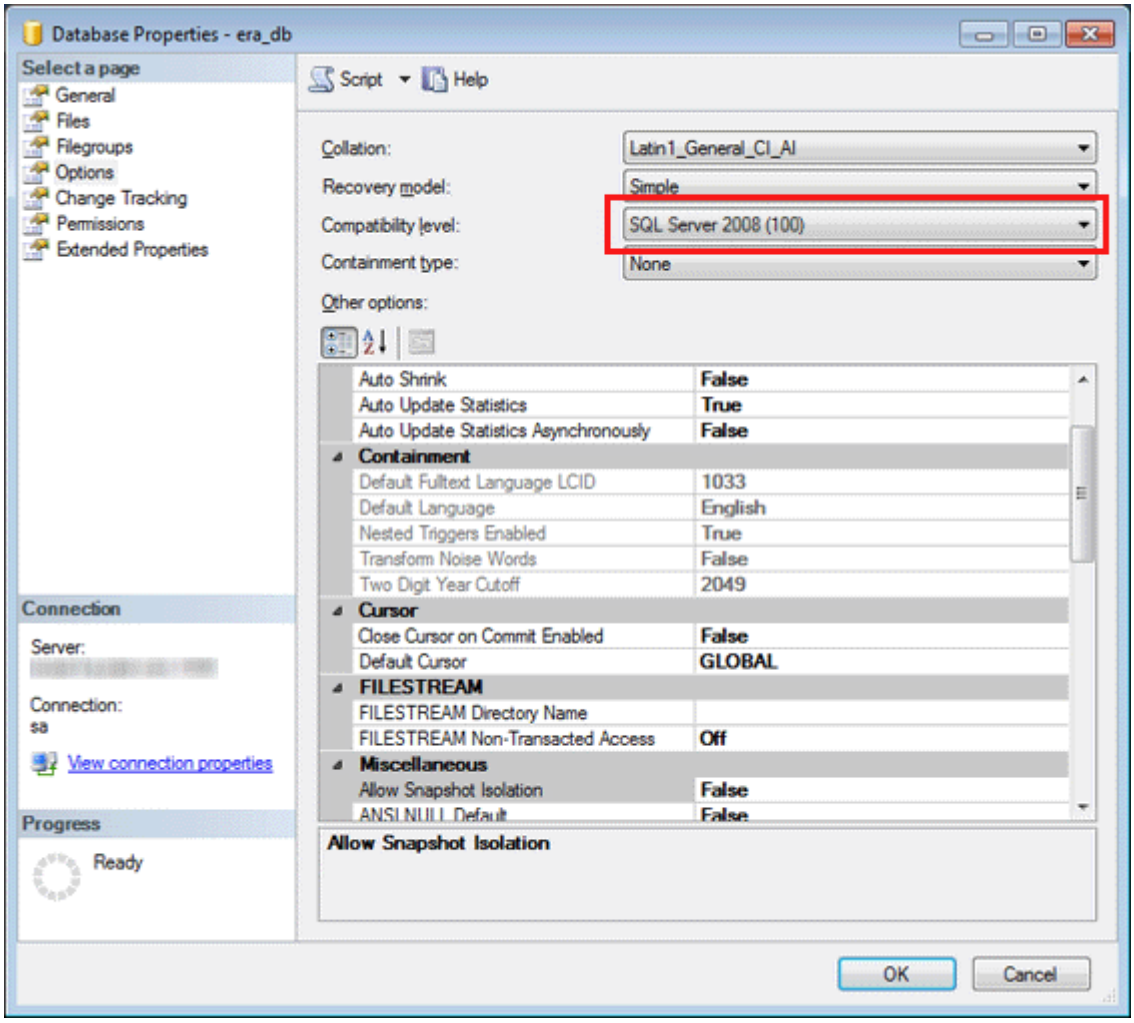
- Не встановлюйте термін дії пароля!
- Рекомендовані символи для використання в імені користувача:
  - Букви ASCII у нижньому регістрі, цифри та символи підкреслення «_»
- Рекомендовані символи для використання в паролі:
  - ТІЛЬКИ символи ASCII, зокрема букви ASCII у верхньому та нижньому регістрах, 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 **зіставлення користувачів** користувач має наступні ролі: **db_datareader**, **db_datawriter**, **db_owner**.

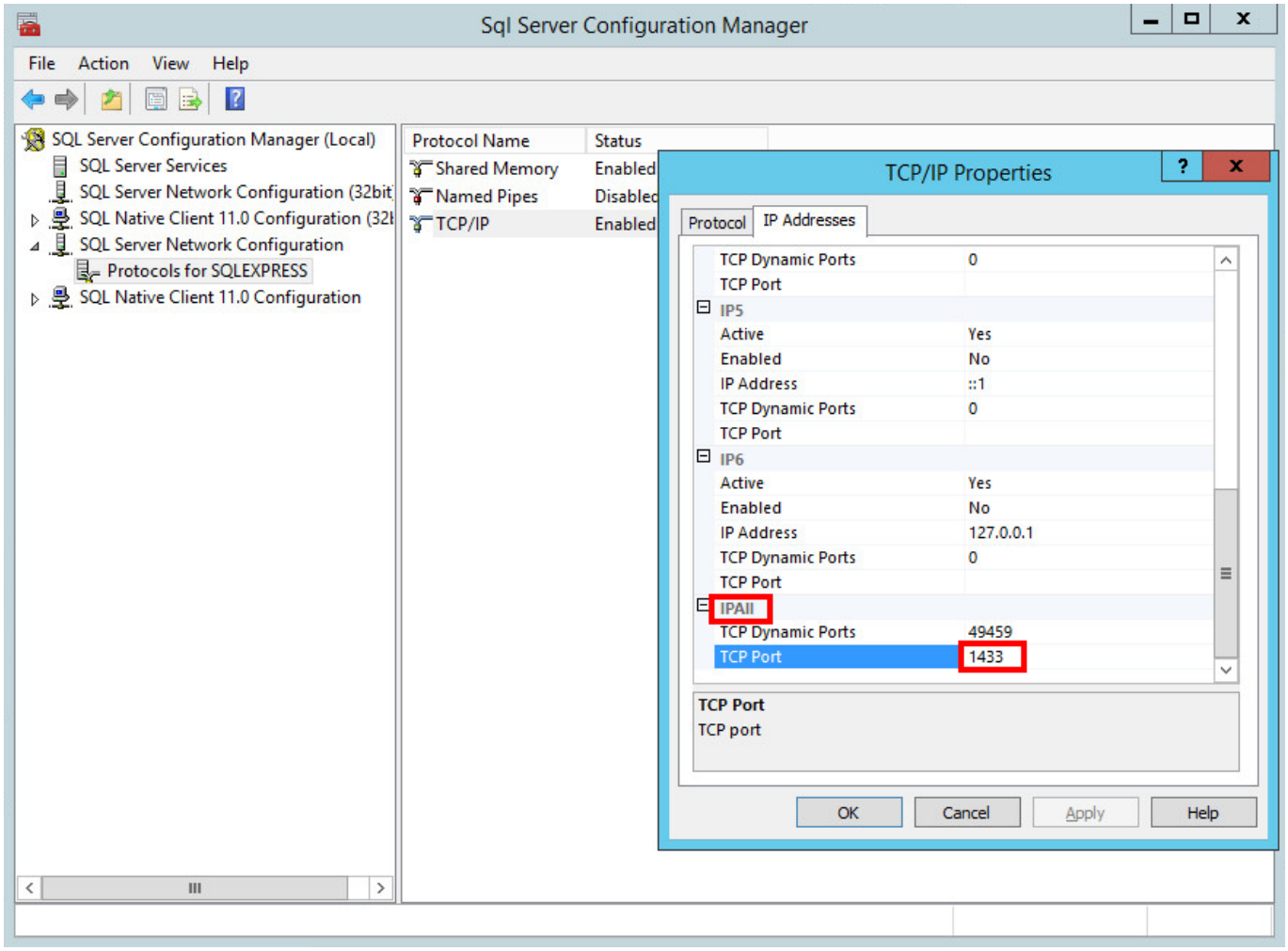


18. Щоб використовувати нові функції сервера баз даних, установіть для відновленої бази даних **Рівень сумісності** з останньою інстальованою версією. Клацніть правою кнопкою миші нову базу даних і відкрийте **Властивості**.



> 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

Попередні вимоги відсутні

• Необхідно інсталювати вихідний і цільовий екземпляри SQL Server. Їх можна розмістити на різних комп'ютерах.

• Інструменти MySQL повинні бути інстальовані принаймні на одному з комп'ютерів (клієнті `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

У наведених нижче командах, файлах конфігурації й операторах SQL замінюйте:
- **SRCHOST** на адресу вихідного сервера баз даних;
- **SRCROOTLOGIN** на ім'я кореневого користувача вихідного сервера MySQL;
- **SRCDBNAME** 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;
- **TARGETDBNAME** на назву цільової бази даних ESET PROTECT (після перенесення);
- **TARGETLOGIN** на ім'я нового користувача бази даних ESET PROTECT на цільовому сервері бази даних;
- **TARGETPASSWD** 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 SRCDBNAME > BACKUPFILE
```

3. Підготуйте порожню базу даних на цільовому сервері MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

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 TARGETDBNAME < BACKUPFILE
```

5. Створіть користувача бази даних ESET PROTECT на цільовому сервері MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Рекомендовані символи для використання в полі **TARGETLOGIN**:

- Букви ASCII у нижньому регістрі, цифри та символи підкреслення «_»

Рекомендовані символи для використання в полі **TARGETPASSWD**:

- 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 TARGETDBNAME.* TO TARGETLOGIN;"
```

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*
   - Windows:

Сервер:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

- 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.

oУстановіть адресу та порт нового сервера баз даних.

oУстановіть нове ім'я користувача та пароль ESET PROTECT у рядку підключення.

Остаточний результат має виглядати так, як показано нижче.

- MS SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

У наведеній вище конфігурації необхідно виконати такі заміщення:
• **TARGETHOST** на адресу цільового сервера баз даних;
• **TARGETDBNAME** на назву цільової бази даних ESET PROTECT (після перенесення);
• **TARGETLOGIN** на ім'я нового користувача бази даних ESET PROTECT на цільовому сервері бази даних;
• **TARGETPASSWD** 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.

- Перенесення баз даних підтримується лише для ідентичних типів баз даних (з MySQL у MySQL і з MS SQL у MS SQL).
- 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. Створіть резервну копію конфігурації MDM.

a)У меню **Комп'ютери** клацніть сервер MDM і виберіть пункт **Показати подробиці**.

b)Клацніть **Конфігурація** > **Надіслати запит на отримання конфігурації**. Можливо, для створення запитаної конфігурації знадобиться певний час (залежно від інтервалу підключення агента).

c)Клацніть **ESET PROTECT Mobile Device Connector** і виберіть пункт **Відкрити конфігурацію**.

d)Експортуйте такі елементи з конфігурації в зовнішнє сховище:

- Точне ім'я хоста сервера MDM.
- Сертифікати однорангового вузла: експортований файл *.pfx* міститиме закритий ключ.

Якщо ви використовуєте сервер ESET PROTECT MDM в Linux, експортуйте сертифікат HTTPS із політики конфігурації MDM:
I.Клацніть **Переглянути** поруч із пунктом **Сертифікат HTTPS**.
II.Клацніть **Завантажити** й завантажте сертифікат HTTPS у форматі PFX.

e)Експортуйте також указані нижче сертифікати та маркери (якщо є).

- Сертифікат підпису профілю реєстрації.
- Сертифікат APNS (експортуйте сертифікат і закритий ключ APNS).
- Маркер авторизації програми реєстрації пристроїв (DEP) Apple.

2. Зупиніть службу ESET PROTECT MDM.

3. Експортуйте базу даних ESET PROTECT MDM або створіть її резервну копію.

4. Вимкніть поточний комп'ютер, на якому запущено ESET PROTECT MDM.

Поки що не деінсталюйте та не виводьте з роботи старий сервер ESET PROTECT MDM.

❑ **На новому сервері ESET PROTECT MDM виконайте вказані нижче дії.**

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 інсталятора (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.

Під час інсталяції ESET PROTECT MDM в Linux використовуйте сертифікат HTTPS із вашої резервної копії.

4. Підключіться до веб-консолі ESET PROTECT.

5. Перезапустіть службу ESET PROTECT MDM.

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 ESMC/ESET PROTECT, інстальованого у відмовостійкому кластері у Windows

Якщо сервер ESMC/ESET PROTECT інстальовано в середовищі відмовостійкого кластеру у Windows, дотримуйтеся вказаних нижче інструкцій, щоб оновити його до ESET PROTECT:

Переконайтеся, що маєте підтримувану операційну систему.

1. Зупиніть роль кластера сервера ESET PROTECT/ESMC в диспетчері кластера. Переконайтеся, що службу (**ESET Security Management Center Server** або **ESET PROTECT Server**) зупинено на всіх вузлах кластера.

2. Підключіть спільний диск кластера на вузлі node1 до Інтернету й оновіть серверний компонент уручну. Для цього запустіть найновіший інсталятор *.msi*, так само як у процесі інсталяції компонента.

3. Після інсталяції (оновлення) переконайтеся, що службу **ESET PROTECT Server** зупинено.

4. Підключіть спільний диск кластера на вузлі node2 до Інтернету й оновіть серверний компонент, так само як у кроці 2.

5. Коли сервер ESET PROTECT буде оновлено на всіх вузлах кластера, запустіть **роль сервера ESET PROTECT** в диспетчері кластера.

6. Оновіть агент ESET Management вручну, запустивши найновіший інсталятор *.msi* на всіх вузлах кластера.

7. 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 інсталятора.

Оновлення проксі-сервера Apache HTTP за допомогою універсального інсталятора (Windows)

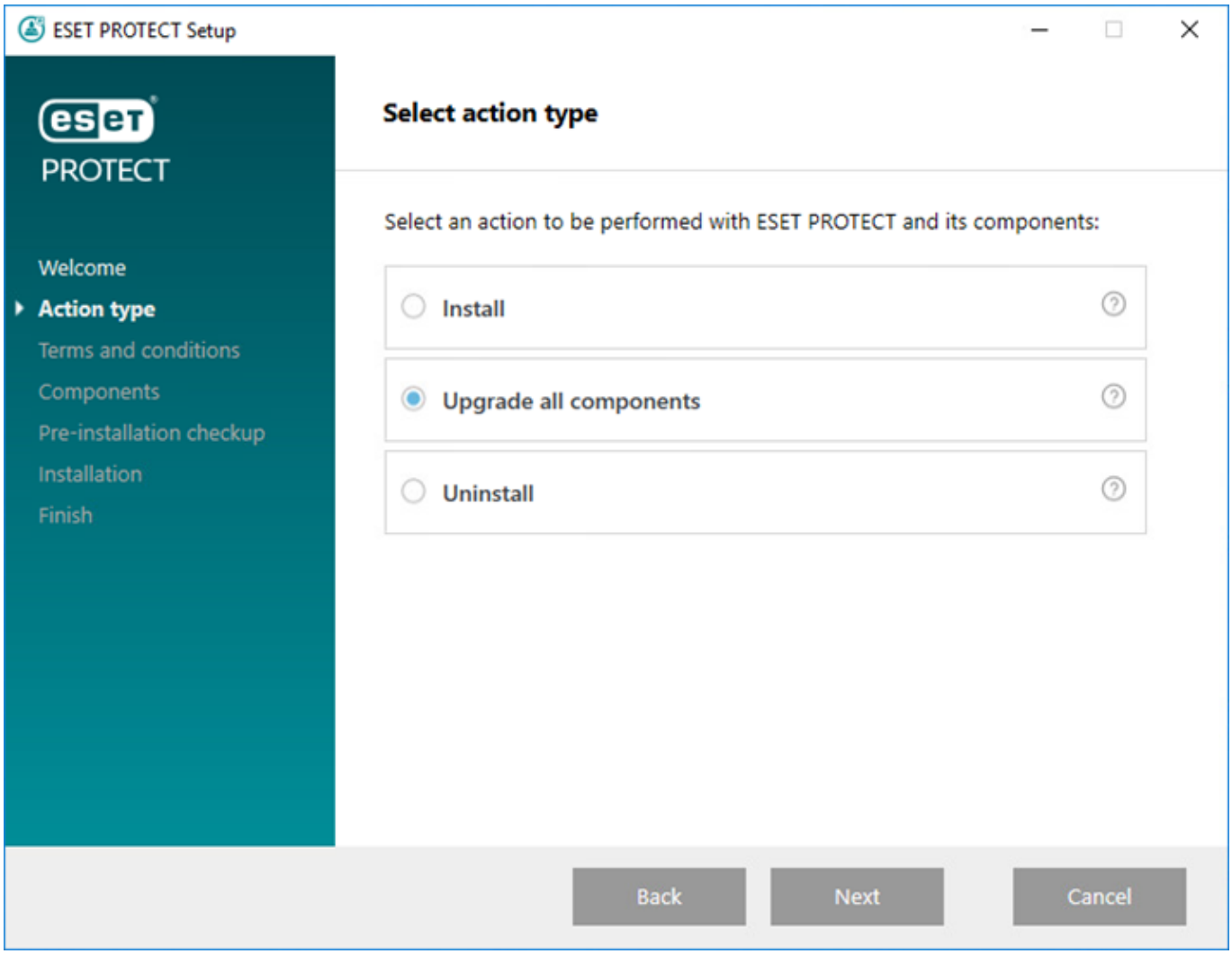
Якщо ви завантажили останню версію універсального інсталятора ESET PROTECT, можна скористатися цим методом для швидкого оновлення проксі-сервера Apache HTTP до останньої версії. Якщо інсталятор має одну з попередніх версій, скористайтеся методом ручного оновлення проксі-сервера Apache HTTP.

1. Створіть резервні копії цих файлів:

   - *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*
   - *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*
   - *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\group.file*

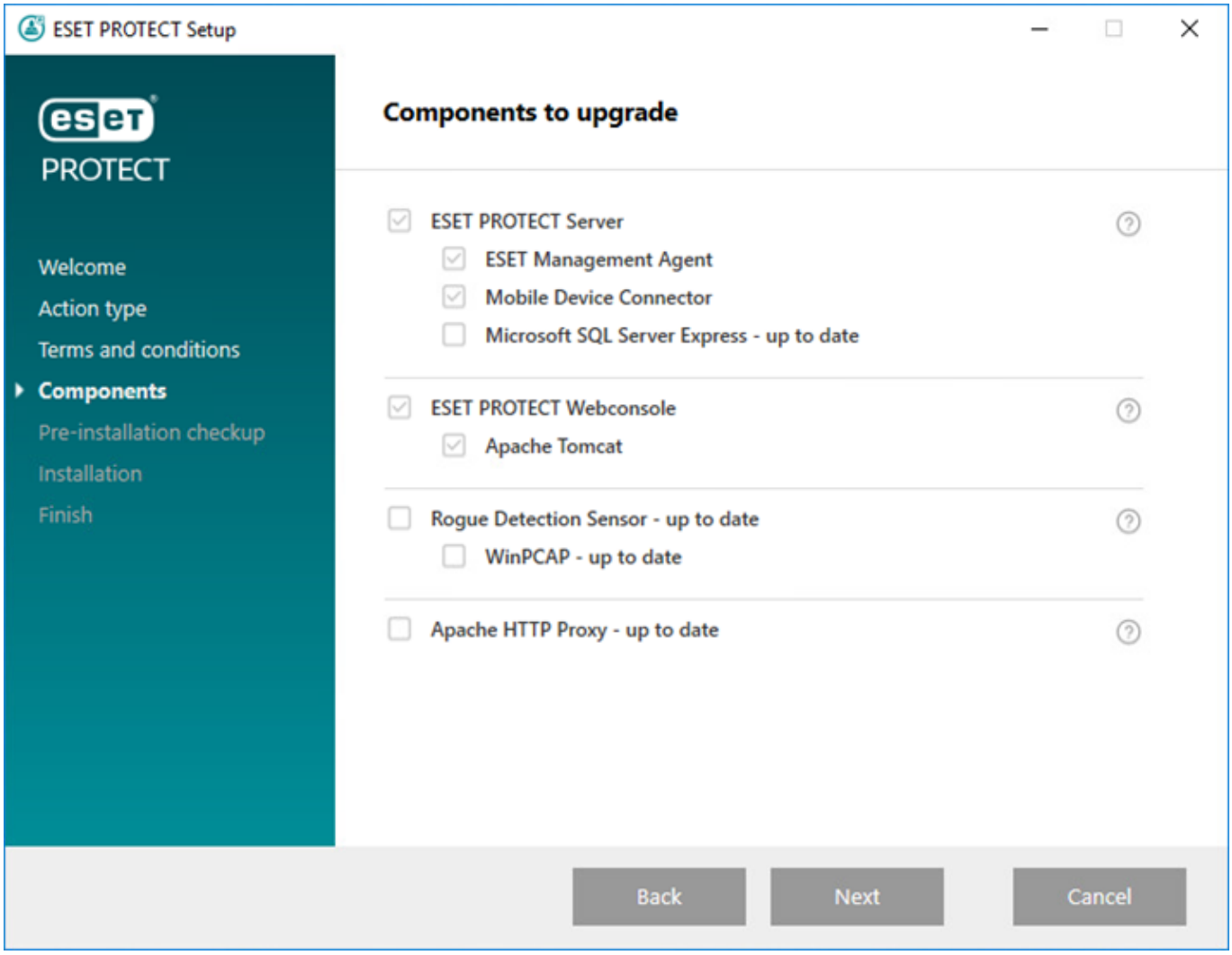
2. Запустіть універсальний інсталятор, двічі натиснувши файл *setup.exe*, і виберіть **Далі** на екрані привітання.

3. Виберіть **Оновити всі компоненти** й натисніть **Далі**.



4. Прочитайте **ліцензійну угоду з кінцевим користувачем**, прийміть її й натисніть **Далі**.

5. У розділі **Компоненти** перегляньте компоненти ESET PROTECT, які можна оновити, і клацніть **Далі**.



6. Дотримуйтеся інструкцій у розділі **Перевірка перед інсталяцією**, щоб переконатися, що система відповідає всім вимогам.

7. Клацніть **Оновити**, щоб запустити оновлення ESET PROTECT. Оновлення може тривати певний час залежно від конфігурації системи й мережі.

8. Коли оновлення завершиться, клацніть **Готово**.

Універсальний інсталятор замінює файл *httpd.conf*, а для оригінальної конфігурації створює файл *httpd.conf.old*. Щоб зберегти настроювану конфігурацію проксі-сервера Apache HTTP, створіть її резервну копію для подальшого використання.

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

http://[IP address]:3128/index.html

Виправлення неполадок

Щоб виправити неполадку, перегляньте файли журналу проксі-сервера Apache HTTP.

Якщо під час попередньої інсталяції проксі-сервера Apache HTTP у файл *httpd.conf* було внесено інші налаштування, дотримуйтеся таких інструкцій:

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*, уручну скопіюйте ці зміни з файлу *httpd.conf.old* (або з резервної копії файлу *httpd.conf*, яку створено на кроці 1) 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 2.[x.xx]\conf\httpd.conf*
   - *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*
   - *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]*. Під час видобування перезапишіть наявні файли.

4. Перейдіть у каталог *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
 Options Indexes FollowSymLinks
 AllowOverride None
 Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\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 у файл *httpd.conf* було внесено інші налаштування, скопіюйте зміни конфігурації з резервної копії файлу *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

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:

- Інструкції для Windows (найновіша версія універсального інсталятора ESET PROTECT) - Рекомендуємо використовувати цей варіант оновлення, якщо наявну інсталяцію Apache Tomcat виконано за допомогою універсального інсталятора.

- Інструкції для Windows (інсталяція вручну) - Оновіть Apache Tomcat уручну, якщо наявну інсталяцію Apache Tomcat виконано вручну або у вас немає найновішої версії універсального інсталятора ESET PROTECT.

- Вказівки для Linux.

Оновлення Apache Tomcat за допомогою універсального інсталятора (Windows)

Apache Tomcat – обов'язковий компонент, необхідний для роботи веб-консолі ESET PROTECT. Використовуйте цей спосіб, щоб оновити Apache Tomcat з використанням останньої версії автономного інсталятора ESET PROTECT 9.0. Рекомендуємо використовувати цей варіант оновлення, якщо наявну інсталяцію Apache Tomcat виконано за допомогою універсального інсталятора. 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.

Обмеження для оновлення Apache Tomcat і веб-консолі

- Якщо інстальовано налаштовувану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інсталятора 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 ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 9.0. Це необхідно для того, що ви мали найновішу автономну довідку, яка відповідає вашій версії ESET PROTECT.

2. Завантажте універсальний інсталятор ESET PROTECT з веб-сайту ESET і розархівуйте завантажений файл.

3. Щоб інсталювати останню версію Apache Tomcat за умови, коли універсальний інсталятор 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*.

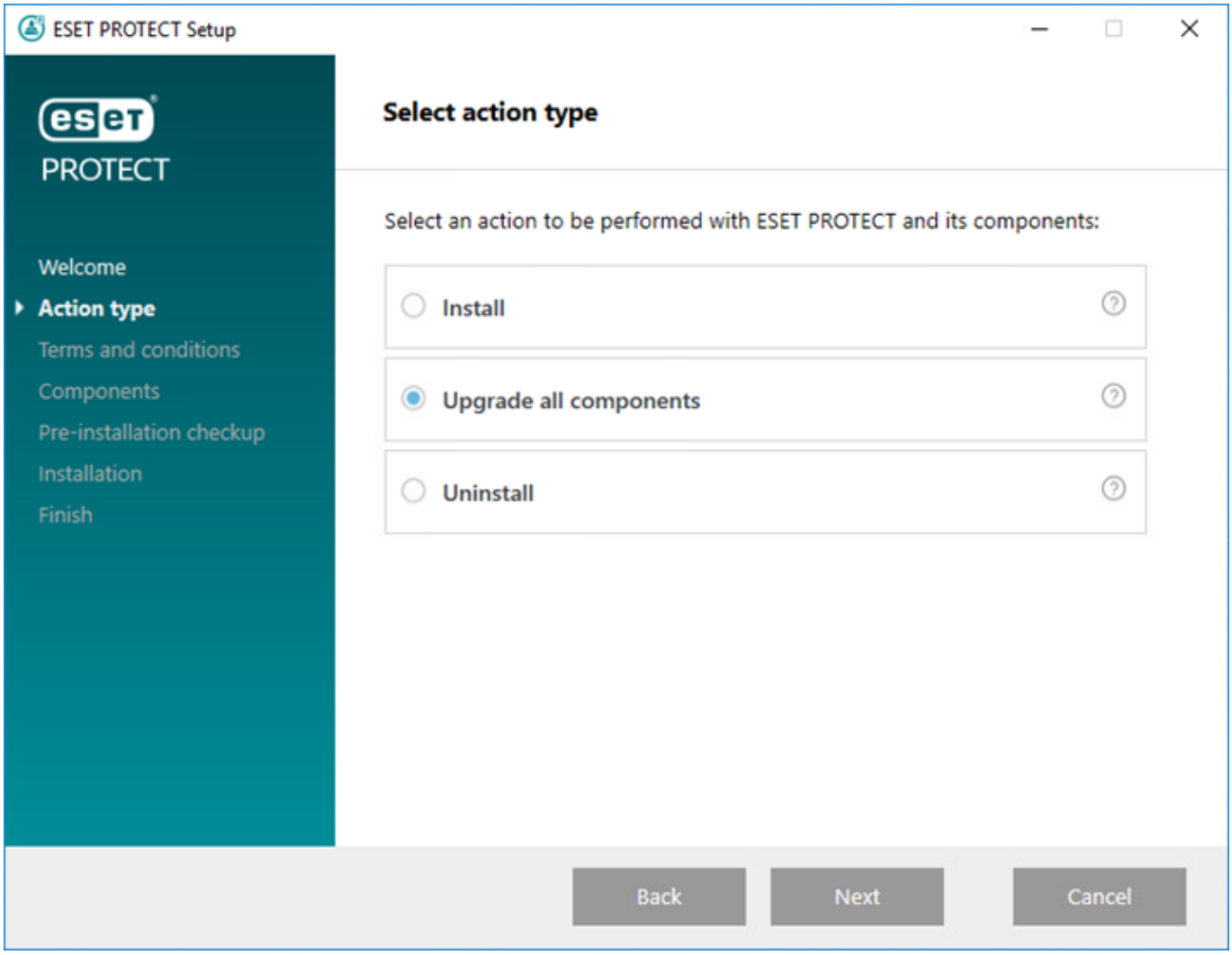
b. Видаліть файл *apache-tomcat-9.0.x-windows-x64.zip*, розташований у папці *installers*.

c. Завантажте ZIP-пакет 64-розрядної версії Apache Tomcat 9 для Windows.

d. Перемістить завантажений ZIP-пакет у папку *installers*.

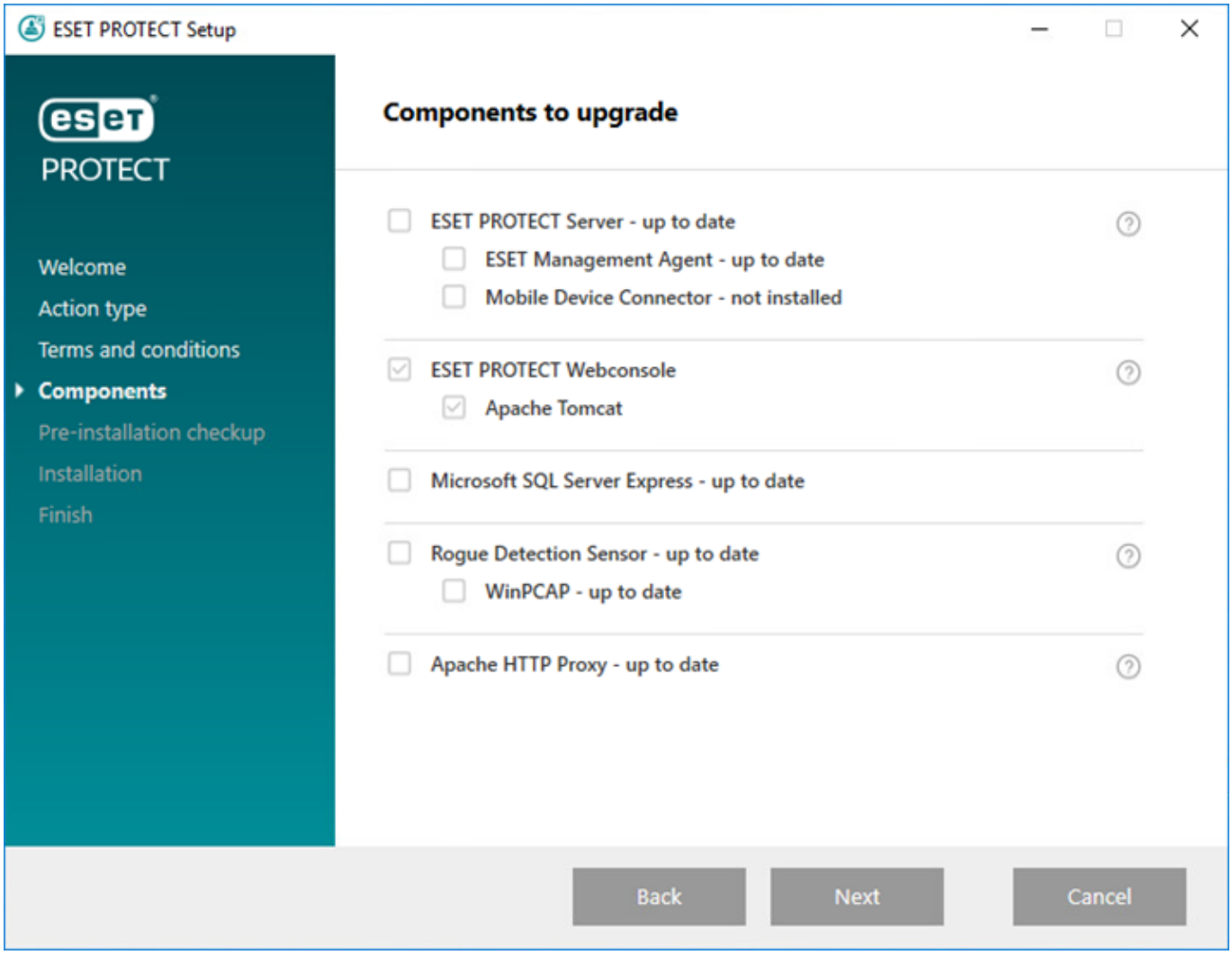
4. Щоб запустити універсальний інсталятор, двічі клацніть файл *Setup.exe* й натисніть клавішу **Далі** на екрані **привітання**.

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. Apache Tomcat потребує 64-розрядної версії Java/OpenJDK. Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

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.

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

b)Відновіть файл *EraWebServerConfig.properties* (з кроку 1) в оригінальному розташуванні.

c) 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 вона завантажується належним чином.

Див. також тему Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи.

Виправлення неполадок

Якщо Apache Tomcat не вдасться оновити, інсталюйте 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. Оновіть Apache Tomcat уручну, якщо наявну інсталяцію Apache Tomcat виконано вручну або у вас немає найновішої версії універсального інсталятора ESET PROTECT.

Якщо інстальовано налаштовувану версію Apache Tomcat (ручна інсталяція служби Tomcat), то подальше оновлення ESET PROTECT Web Console за допомогою універсального інсталятора або завдання «Оновлення компонентів» не підтримується.

Перед оновленням

- Apache Tomcat потребує 64-розрядної версії Java/OpenJDK. Якщо в системі інстальовано кілька версій Java, рекомендуємо видалити старіші версії Java і залишити лише останню версію підтримувану версію Java.

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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

- Перевірте, яка версія Apache Tomcat наразі доступна.

    a.Перейдіть у папку інсталяції Apache Tomcat:
    C:\Program Files\Apache Software Foundation\[Tomcat папка *]*

    b.Відкрийте файл RELEASE-NOTES у текстовому редакторі та перевірте номер версії (наприклад, 9.0.34).

    c.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 налаштовуваний 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 інсталятора Apache Tomcat (32-рядна або 64-розрядна версія інсталятора для Windows) `apache-tomcat-[версія].exe` із сайту https://tomcat.apache.org.

6. Інсталюйте нову завантажену версію Apache Tomcat.

- Якщо інстальовано кілька версій Java, під час інсталяції виберіть шлях до останньої версії Java.
- Після завершення інсталяції 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-консолі – Windows).

11. Відновіть *EraWebServerConfig.properties* в оригінальному розташуванні.

12. Запустіть Apache Tomcat і задайте правильну віртуальну машину Java.

a)Перейдіть у папку *C:\Program Files\Apache Software Foundation\[Tomcat* папка *]\bin* і запустіть *Tomcat9w.exe*.

b)На вкладці **Загальне** виберіть для параметра **Тип запуску** значення **Автоматично** й натисніть **Запустити**.

c)Відкрийте вкладку **Java**, зніміть прапорець **Використовувати значення за замовчуванням** і переконайтеся, що **віртуальна машина Java** містить шлях до файлу *jvm.dll* (див. ілюстровані інструкції в базі знань), а потім клацніть **OK**.

13. Підключіться до веб-консолі ESET PROTECT і переконайтеся, що вона завантажується належним чином.

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 ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 9.0. Це необхідно для того, що ви мали найновішу автономну довідку, яка 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. Щоб переглянути інстальовану версію Apache Tomcat (у деяких випадках відповідна папка має ім'я `tomcat7` або `tomcat8`), виконайте таку команду:

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Якщо доступна новіша версія:

   a. Переконайтеся, що підтримується новіша версія.

   b. Створіть резервну копію файлу конфігурації Tomcat */etc/tomcat7/server.xml*.

Інструкції з оновлення

1. Щоб зупинити роботу служби Apache Tomcat (у деяких випадках, служба має назву `tomcat7`), виконайте таку команду:

```
service tomcat stop
```

2. Оновіть Apache Tomcat і Java. Наведені нижче приклади назв пакетів можуть відрізнятися від пакетів, доступних у репозиторії дистрибутива Linux.

Дистрибутив Linux	Команди термінала
Дистрибутиви Debian і Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-11-jdk tomcat9`

Дистрибутив Linux	Команди термінала
Дистрибутиви CentOS і Red Hat	`yum update` `yum install java-1.8.0-openjdk tomcat`
OpenSUSE	`zypper refresh` `zypper install java-1_8_0-openjdk tomcat`

3. Замініть файл */etc/tomcat9/server.xml* на файл *server.xml* з резервної копії.

4. Відкрийте файл *server.xml* і переконайтеся, що шлях *keystoreFile* указано правильно.

5. Переконайтеся, що підключення HTTPS для Apache Tomcat налаштовано належним чином.

Див. також тему Конфігурація Web Console для корпоративних рішень або систем із низькою продуктивністю роботи.

Після оновлення Apache Tomcat до останньої основної версії (наприклад, з версії 7.x до 9.x):
1.розгорніть веб-консоль ESET PROTECT ще раз (див. розділ Інсталяція веб-консолі ESET PROTECT – Linux);
2.повторно використайте *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*, щоб зберегти налаштовувані параметри у веб-консолі ESET PROTECT.
Після оновлення Web Console і Apache Tomcat файли автономної довідки видаляються. Якщо ви використовували автономну довідку з ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 9.0. Це необхідно для того, що ви мали найновішу автономну довідку, яка 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 ESMC/ESET PROTECT, інстальованого у відмовостійкому кластері в Linux

Якщо сервер ESET PROTECT інстальовано в середовищі відмовостійкого кластера в Linux і потрібно оновити інстальований екземпляр до найновішого ESET PROTECT, дотримуйтеся наведених нижче інструкцій.

1. Вимкніть службу *EraService* у Conga (графічний інтерфейс адміністрування кластера) у розділі **Групи служб** і зупиніть роботу агента та сервера на обох вузлах.

2. Оновіть сервер ESMC/ESET PROTECT на вузлі node1, виконавши дії нижче.

   a)Підключіть спільне сховище до цього вузла.

   b)Оновіть серверний компонент уручну 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. Для цього змініть 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 ESMC/ESET PROTECT на вузлі node2.

4. Запустіть службу *EraService* у Conga (графічний інтерфейс адміністрування кластера) у розділі «Групи служб».

5. Оновіть агент 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 і його компоненти, виберіть один із вказаних нижче розділів.

- Видалення агента ESET Management
- 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 ESMC/ESET PROTECT/MDM після перенесення на новий сервер

Видалення агента ESET Management

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).

Після видалення агента ESET Management з клієнтського комп'ютера ESET PROTECT більше не керує пристроєм.
• Продукт ESET для захисту може зберегти деякі налаштування після видалення агента ESET Management.
• Якщо агент захищено паролем, його не вдасться видалити. Перш ніж вимкнути керування пристроєм, рекомендуємо скинути деякі параметри, які ви не хочете зберігати (наприклад, захист паролем), до значень за замовчуванням за допомогою політики.
• Усі завдання, які виконуються на агенті, буде припинено. Залежно від реплікації статус виконання цього завдання (**Виконується**, **Завершено** або **Не виконано**) може не відображатися належним чином у веб-консолі ESET PROTECT.
• Після видалення агента ви можете керувати продуктом для захисту за допомогою вбудованого графічного інтерфейсу EGUI або команди eShell.

6. Перевірте **зведення** завдання й натисніть «**Готово**».

7. Клацніть Створити тригер, щоб вказати, коли має виконатися клієнтське завдання та на яких **комп'ютерах**.

Локальне видалення (Windows)

Див. також інструкції з локального видалення агента ESET Management в Linux або macOS. Щоб дізнатися про виправлення неполадок із видаленням агента, див. Виправлення неполадок із видаленням агента ESET Management.

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.

Якщо ви встановили пароль за допомогою політики для агентів ESET Management, у вас є три варіанта:
- Пароль потрібно буде ввести під час видалення.
- Перед видаленням агента ESET Management скасувати призначення політики.
- Повторно розгорнути агент ESET Management на наявному агенті, який захищено паролем (стаття бази знань).

Windows - Видалення сервера ESET PROTECT і його компонентів

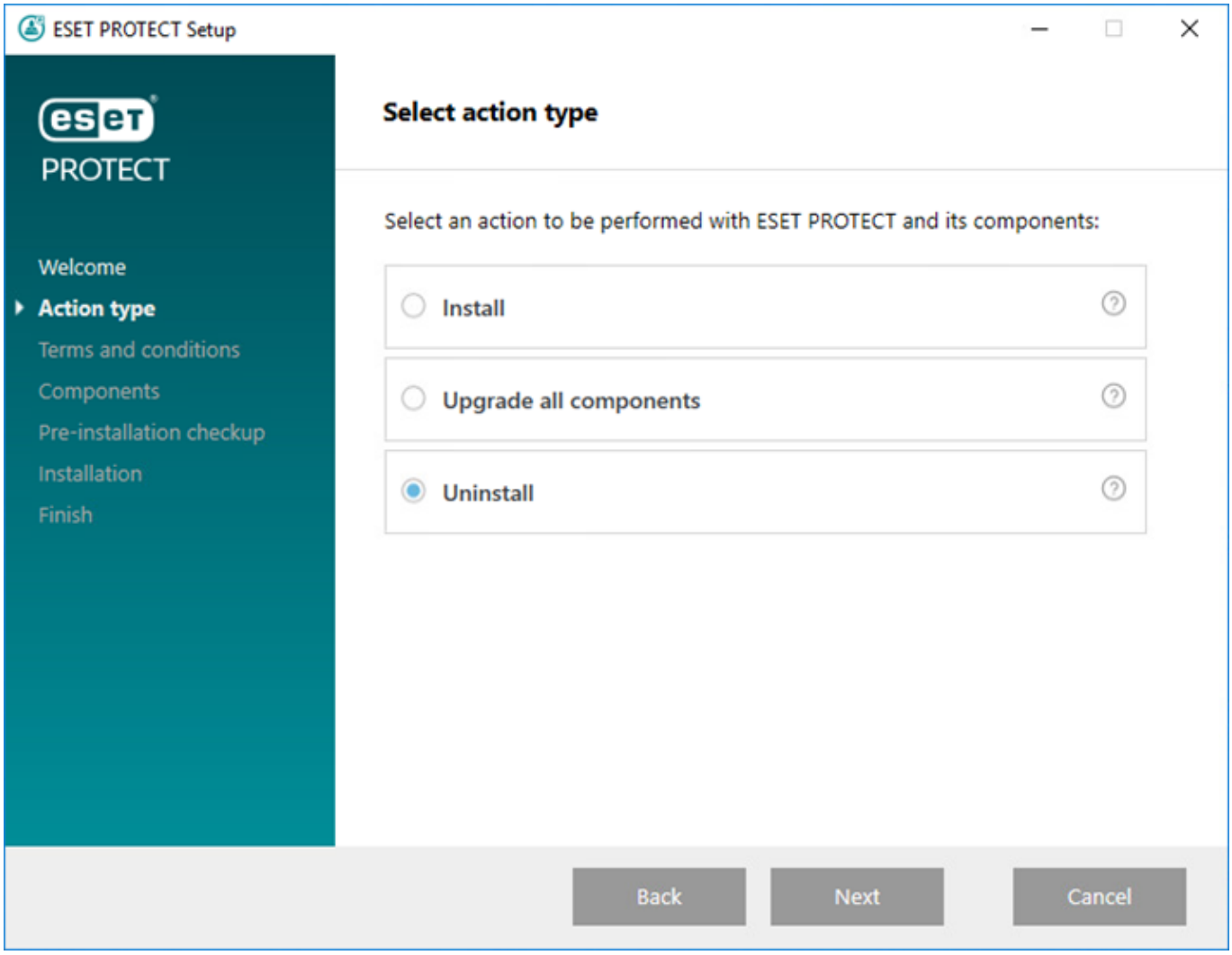
Перед видаленням ESET PROTECT видаліть агенти на керованих комп'ютерах.
Перед видаленням Mobile Device Connector перегляньте розділ Ліцензування iOS в MDM.

Щоб видалити сервер ESET PROTECT і його компоненти у Windows, дотримуйтеся таких інструкцій:

1. Завантажте універсальний інсталятор ESET PROTECT і розархівуйте пакет.

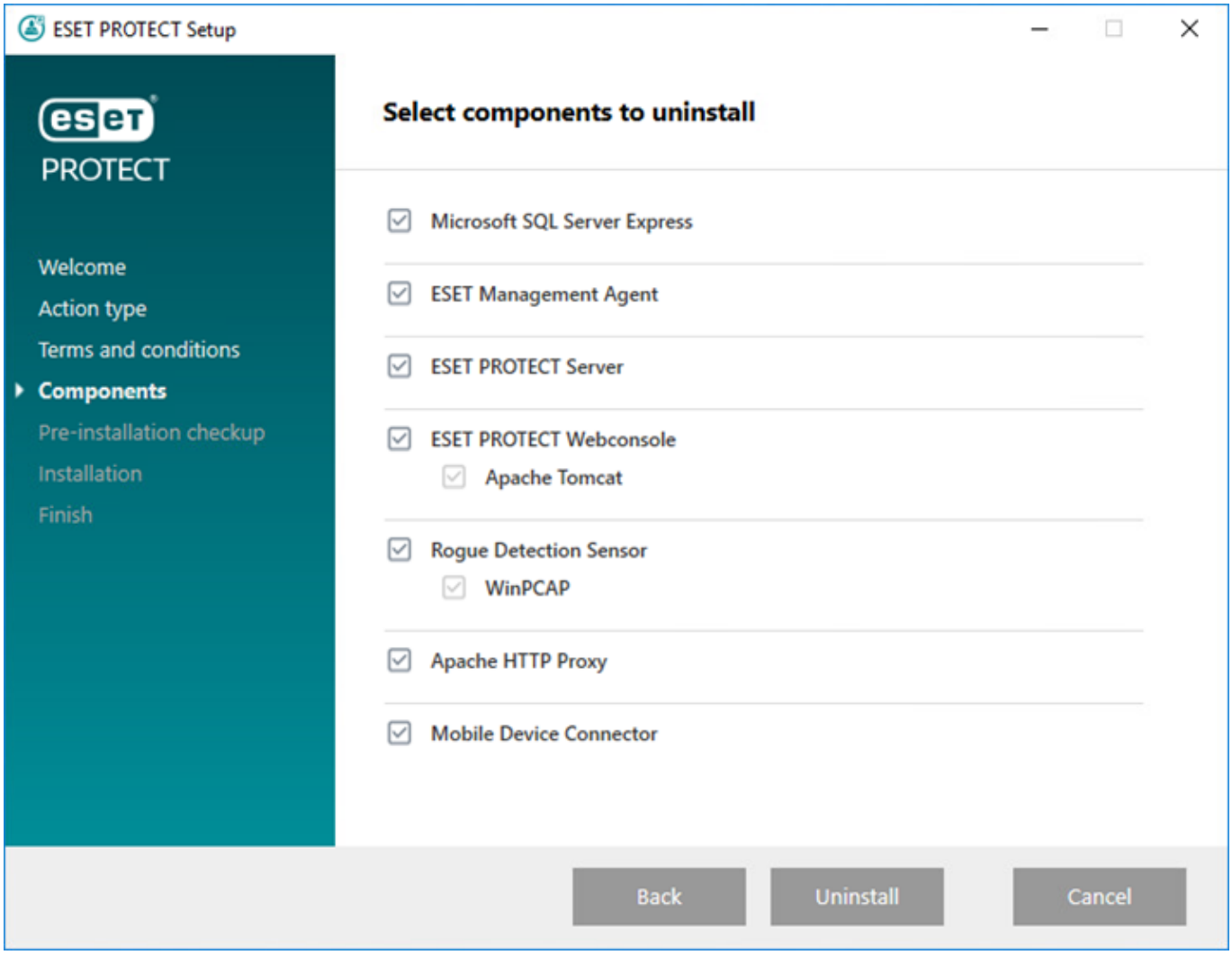
2. Запустіть файл *Setup.exe*. У розкривному меню виберіть пункт **Мова**. Натисніть кнопку **Далі**.

3. Виберіть **Видалити** й натисніть **Далі**.



4. Прийміть ліцензійну угоду з кінцевим користувачем і натисніть **Далі**.

5. Виберіть компоненти, які потрібно видалити, і натисніть **Далі**.



6. Щоб завершити видалення певних компонентів, можливо, знадобиться перезавантажити комп'ютер.

Перегляньте також розділ Видалення старого сервера 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
```

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/`.

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.
Щоб дізнатися про виправлення неполадок із видаленням агента, див. Виправлення неполадок із видаленням агента ESET Management.

macOS: видалення ESET Management Agent і продукту ESET Endpoint

Видаліть ESET Management Agent і продукт ESET Endpoint локально або віддалено за допомогою ESET PROTECT.

Більш докладні інструкції щодо локального видалення ESET Management Agent і продукту ESET Endpoint див. в цій статті нашої бази знань.

Якщо потрібно видалити продукт ESET Endpoint віддалено, зробіть це до видалення ESET Management Agent.

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\ Management\ 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.

Щоб дізнатися про виправлення неполадок із видаленням агента, див. Виправлення неполадок із видаленням агента ESET Management.

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). Натисніть **Закрити**.

Локальне видалення продукту ESET Endpoint у Terminal

1. Відкрийте **Finder** > **Програми** > **Утиліти** > **Terminal**.

2. Уведіть указану нижче команду й натисніть клавішу **Enter**:

- Видалити ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- Видалити ESET Endpoint Security:

```
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** > **Інстальовані програми** > виберіть **ESET Endpoint Security** або **ESET Endpoint Antivirus** і натисніть кнопку **Видалити**.

- За допомогою завдання **Видалення програми** ***.

Видалення старого сервера ESMC/ESET PROTECT/MDM після перенесення на новий сервер

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 ESMC/ESET PROTECT/MDM після перенесення на новий.

I.**Зберегти ОС серверного комп'ютера й повторно використати її**

1. Зупиніть роботу служби старого сервера ESMC/ESET PROTECT.

2. Видаліть (`DROP DATABASE`) старий екземпляр бази даних ESMC/ESET PROTECT Server (MS SQL або MySQL).

Якщо ви перенесли базу даних на новий ESET PROTECT, перед її видаленням переконайтеся, що видалили її зі старого 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 ESMC/ESET PROTECT/MDM і всі його компоненти (зокрема, агент ESET Management, Rogue Detection Sensor, MDM тощо).

- Видалити ESMC 7.x – Windows
- Видалити ESET PROTECT 8.x – Windows
- Видалити ESET PROTECT 9.x – Windows
- Видалити ESET PROTECT – Linux

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 ESMC/ESET PROTECT/MDM — відформатувати диск, на якому інстальовано цей продукт.

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 ESET PROTECT. Інформацію щодо вирішення поширених проблем ESET PROTECT див. в розділі Рішення поширених проблем під час інсталяції. Див. також відомі проблеми з продуктами ESET для бізнесу.

Не вдалося виправити неполадку?

- У кожного компонента ESET PROTECT є файл журналу, який може бути більш або менш детальним. Переглядайте журнали, щоб визначати, які помилки є причиною неполадки.

- Детальність журналу кожного компонента задається в його політиці > **Додаткові параметри** > **Ведення журналів** > **Детальність журналу трасування** – у параметрах детальності журналу визначте рівень інформації, яка буде збиратися та зберігатися, від **Трасування** (вся інформація) до **Критична** (найважливіша важлива інформація).

  - Політика агента ESET Management: щоб політика набрала чинності, її потрібно застосувати на пристрої. Щоб увімкнути повне ведення журналу для агента ESET Management у файлі *trace.log*, створіть порожній файл з іменем *traceAll* без розширення в папці, де розташовано файл *trace.log*, і перезавантажте комп'ютер (щоб перезавантажити службу агента ESET Management).

  - ESET PROTECT Параметри сервера

  - Політика ESET Mobile Device Connector: щоб політика набрала чинності, її потрібно застосувати на пристрої. Перегляньте також розділ Виправлення неполадок з MDM.

- Якщо вам не вдається виправити неполадку, відвідайте форум безпеки ESET і зверніться до спільноти ESET, щоб отримати інформацію про можливі проблеми.

- Під час звернення до служби технічної підтримки ESET може з'явитися запит на збір файлів журналів за допомогою ESET Log Collector або інструмента 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.

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.

Оновіть сервер ESET PROTECT і веб-консоль.

1. Перевірте, яка версія консолі управління ESET працює на сервері.

2. Завантажте найновішу версію інсталятора для Windows або найновіші автономні інсталятори компонентів ESET PROTECT для Linux на сайті завантажень ESET.

3. Оновіть сервер ESET PROTECT і ESET PROTECT веб-консоль.

   - Windows: оновлення з використанням універсального інсталятора

   - Linux: оновлення компонентів уручну

Після оновлення Web Console і Apache Tomcat файли автономної довідки видаляються. Якщо ви використовували автономну довідку з ESMC або ESET PROTECT старішої версії, після оновлення створіть її заново для ESET PROTECT 9.0. Це необхідно для того, що ви мали найновішу автономну довідку, яка відповідає вашій версії ESET PROTECT.

Продовжуйте автономне оновлення продуктів ESET Endpoint

1. Перегляньте, які продукти ESET інстальовано на клієнтах. Відкрийте веб-консоль ESET PROTECT і перейдіть у меню **Панель інструментів** > **Програми ESET**.

2. Переконайтеся, що маєте найновіші версії продуктів ESET Endpoint.

3. Завантажте інсталятори із сайту завантаження ESET у локальний репозиторій, налаштований під час інсталяції в автономному режимі.

4. Запустіть завдання інсталяції програми з веб-консолі ESET PROTECT.

Рішення поширених проблем під час інсталяції

Розгорніть повідомлення про помилку, яке ви хочете вирішити:

ESET PROTECTСервер

Служба сервера ESET PROTECT не запускається:

Пошкоджений інсталятор

- Можливі причини: відсутні ключі реєстру або файли, недійсні дозволи на доступ до файлів.
- Універсальний інсталятор 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 відображатимуться 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.

ESET Management Агент

Виправлення неполадок із видаленням 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 інстальовано продукт ESET для робочих станцій, ви не зможете здійснити видалення через увімкнену функцію самозахисту.

• Під час видалення агента відображається повідомлення «Не вдається оновити базу даних. Спочатку видаліть продукт». Для виправлення агента ESET Management виконайте вказані нижче дії:

1. Виберіть **Панель управління** > **Програми та функції** та двічі натисніть **агентESET Management**.

2. Виберіть **Далі** > **Виправлення** та дотримуйтесь інструкцій, що відобразяться.

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 регістру. 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 сервера ESET PROTECT

Див. розділ Виправлення неполадок із підключенням агента й статтю нашої бази знань за цим посиланням.

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 інсталювали 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} throwed 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 інсталятора 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.

Переконайтесь, 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

ESET PROTECT компонент	Розташування файлів журналу
ESET PROTECTСервер	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
ESET Management Агент	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Див. також Виправлення неполадок із підключенням агента.
ESET PROTECT Web Console і Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Див. також сторінку https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Mobile Device Connector	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Перегляньте також розділ Виправлення неполадок з MDM.
Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
Проксі-сервер Apache HTTP	*C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs* *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\errorlog*

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 **OK**.

Linux

ESET PROTECT компонент	Розташування файлів журналу
ESET PROTECTСервер	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Management Агент	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Mobile Device Connector	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Перегляньте також розділ Виправлення неполадок з MDM.
Проксі-сервер Apache HTTP	*/var/log/httpd/*
ESET PROTECT Web Console і Apache Tomcat	*/var/log/tomcat/* Див. також сторінку https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

ESET PROTECT Віртуальний пристрій

ESET PROTECT компонент	Розташування файлів журналу
Конфігурація віртуального пристрою ESET PROTECT	*/root/appliance-configuration-log.txt*
ESET PROTECTСервер	*/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 **Diagnostic<product>** (наприклад, **DiagnosticServer** або **DiagnosticAgent**)

Використання (Linux)

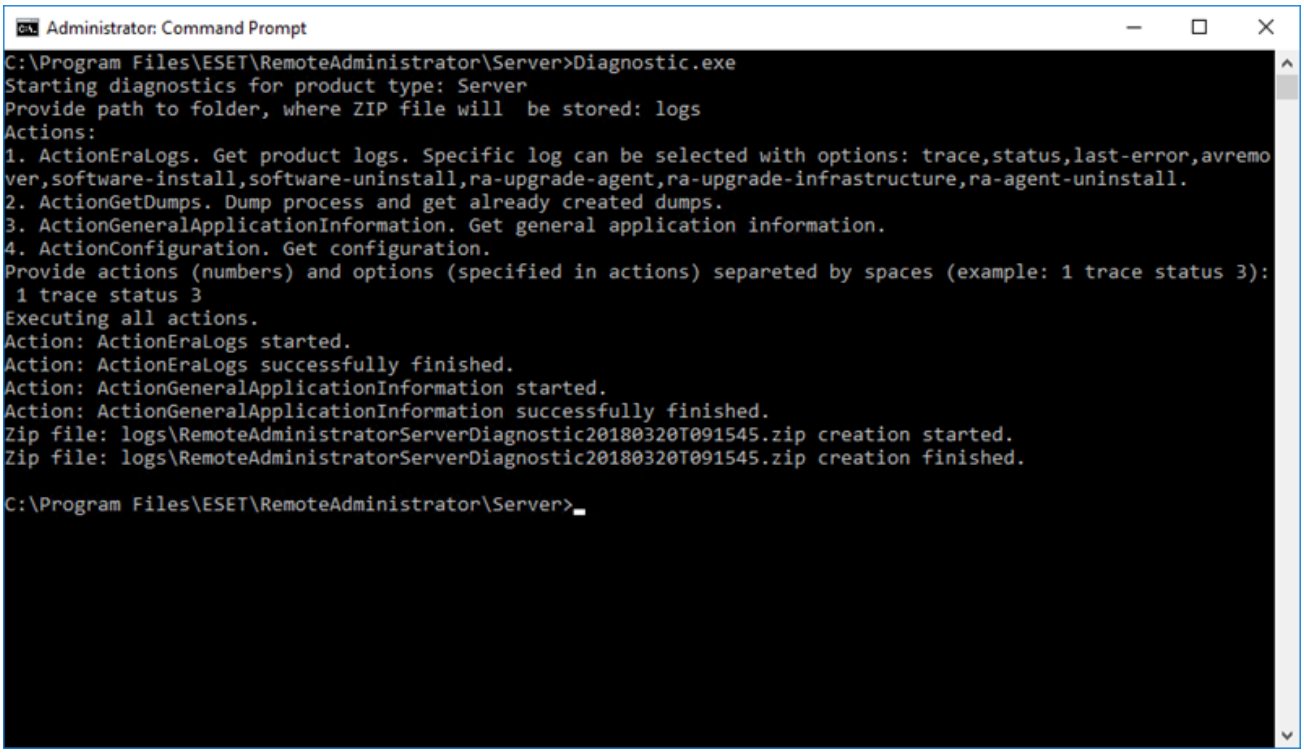
Запустіть виконуваний файл інструменту діагностики в терміналі від імені кореневого користувача та дотримуйтесь інструкцій, що відобразяться на екрані.

Використання (Windows)

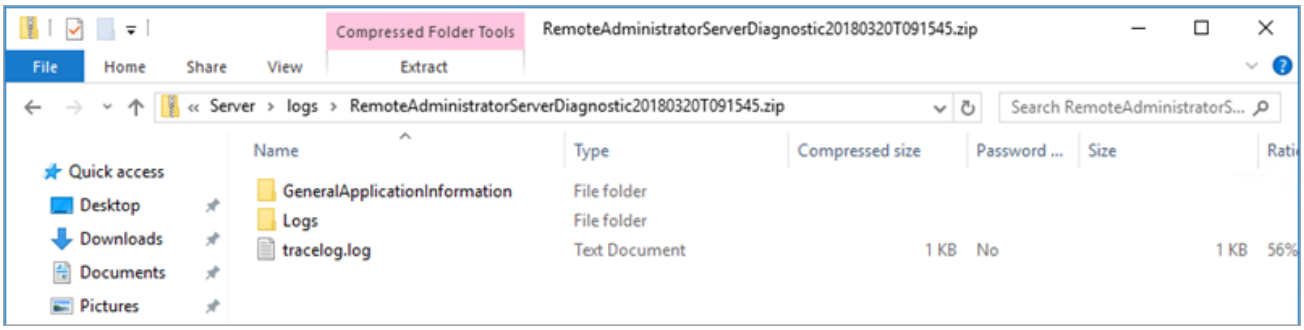
1. Запустіть інструмент за допомогою командного рядка.

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**.



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.

> Необхідно запустити 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 інстальованого 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.

> 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**. Інформацію про підключення до бази даних див. тут: *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Виберіть **Використовувати пароль адміністратора, який уже зберігається в базі даних** і натисніть **Далі**.

5. Виберіть **Зберегти наявні сертифікати** та натисніть **Далі**.

6. Активуйте сервер ESET PROTECT за допомогою дійсного ліцензійного ключа або виберіть **Активувати пізніше** (додаткові інструкції див. в розділі Керування ліцензією) й клацніть **Далі**.

7. Натисніть **Відновити**.

8. 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 PROTECT9

Питання й відповіді

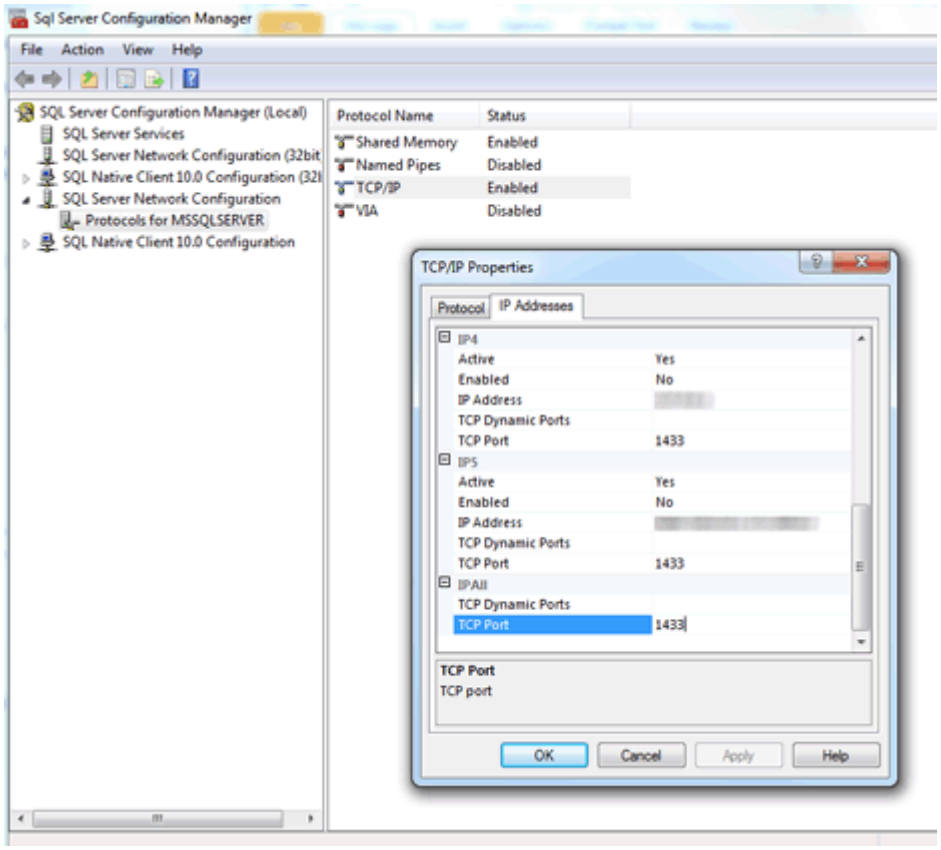
Чому ми встановлюємо Java на сервер? Чи не створює це ризики? Більшість усіх компаній, що надають послуги захисту, і систем безпеки рекомендують видаляти Java з комп'ютерів, особливо із серверів.

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. З міркувань безпеки веб-сервер можна інсталювати на виділений комп'ютер.

⚠ 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 на JAVA SE, можна перейти на безкоштовну альтернативу. Див. підтримувані версії JDK.

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 Базу даних створено інсталятором *Server.msi*, а не інсталятором 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 вказати належну інформацію й облікові дані для підключення до MS SQL Server? Було б зручно, якби інсталятор підтримував різні версії SQL Server (2014, 2019 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 2014 і новіші версії.

ESET PROTECT 9.0 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.
- Інсталятор автоматично генерує випадковий пароль для автентифікації бази даних (зберігається в *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ 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 або великих мережах;
> - якщо ESET PROTECT буде використовуватися з ESET Enterprise Inspector.

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 інсталюйте підтримувану версію MySQL Server та з'єднувача ODBC. Див. керівництво з інсталяції та конфігурації MySQL.

Мені довелося інсталювати Microsoft .NET Framework 4, оскільки інсталятором ESET PROTECT було запропоновано перейти на сторінку (http://www.microsoft.com/en-us/download/details.aspx?id=17851), але це не допомогло для нової інсталяції Windows Server 2012 R2 з пакетом оновлень 1 (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.

- 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.

Ми використовуємо не Apache HTTP Server, а інший продукт – Apache Tomcat.

Чи має ESET PROTECT інтерфейс командного рядка?

Так, ми використовуємо ESET PROTECT ServerApi.

Чи можна інсталювати ESET PROTECT на контролер домену?

Не інсталюйте SQL Server у контролері домену (наприклад, 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).

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 інсталюєте 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?

Див. розділ щодо процедур оновлення.

Як оновити систему без підключення до Інтернету?

Для цього необхідно інсталювати 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?

Якщо ви інсталюєте новий екземпляр сервера ESET PROTECT, використовуючи той самий обліковий запис користувача (наприклад, обліковий запис адміністратора домену), під яким інсталювали 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://\\eraserver\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.

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. Для цього дотримуйтеся таких інструкцій:

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 5 або 6 до ESET PROTECT 9 за допомогою універсального інсталятора?

Пряме оновлення не підтримується: див. тему Перенесення з ERA 5.x або Перенесення з ERA 6.x.

Я отримую повідомлення про помилку або стикаюся з проблемами під час використання ESET PROTECT. Що робити?

Див. Запитання й відповіді щодо виправлення неполадок.

Ліцензійна угода з кінцевим користувачем

Набуває чинності 19 жовтня 2021 року.

УВАГА! Перш ніж завантажувати, інсталювати, копіювати або використовувати продукт, уважно ознайомтеся з наведеними нижче положеннями й умовами його застосування. **ЗАВАНТАЖИВШИ, ІНСТАЛЮВАВШИ, СКОПІЮВАВШИ АБО ЗАСТОСУВАВШИ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИ ПРИЙМАЄТЕ ЦІ ПОЛОЖЕННЯ Й УМОВИ, А ТАКОЖ ПОГОДЖУЄТЕСЯ З ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ.**

Ліцензійна угода з кінцевим користувачем

Ця ліцензійна угода з кінцевим користувачем ("Угода"), укладена між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 85101 Bratislava, Slovak Republic, унесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532 ("ESET" або "Постачальник") і Вами, фізичною або юридичною особою ("Ви" або "Користувач"), надає Вам право використовувати Програмне забезпечення, визначене в статті 1 цієї Угоди. Указане Програмне забезпечення можна отримати на носії даних або електронною поштою, завантажити з Інтернету, серверів Постачальника або отримати з інших джерел відповідно до зазначених нижче умов і положень.

ЦЕ УГОДА ПРО ПРАВА КОРИСТУВАЧА, А НЕ ДОГОВІР КУПІВЛІ. Постачальник залишає за собою право власності на копію Програмного забезпечення та фізичного носія, на якому Програмне забезпечення постачається в товарній упаковці, а також усі інші копії, які Користувач має право створювати відповідно до умов цієї Угоди.

Вибравши під час завантаження, інсталяції, копіювання або використання Програмного забезпечення варіант «Прийняти», Ви засвідчуєте свою згоду дотримуватись умов і положень цієї Угоди та підтверджуєте ознайомлення з Політикою конфіденційності. Якщо Ви не погоджуєтеся з будь-якими положеннями або умовами Угоди та/або Політики конфіденційності, виберіть варіант «Закрити», скасуйте інсталяцію чи завантаження, знищте Програмне забезпечення, інсталяційний носій, супровідну документацію та товарний чек або поверніть їх Постачальнику чи в торгову точку, де Ви отримали Програмне забезпечення.

ВИ ПОГОДЖУЄТЕСЯ, ЩО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАСВІДЧУЄ ФАКТ ПРОЧИТАННЯ ВАМИ ЦІЄЇ УГОДИ, РОЗУМІННЯ ЇЇ УМОВ І ПОЛОЖЕНЬ ТА ВАШУ ЗГОДУ НА ЇХ ДОТРИМАННЯ.

1. **Програмне забезпечення.** Термін "Програмне забезпечення" в цій Угоді означає: (i) комп’ютерну програму, що супроводжується цією Угодою, включно з усіма її компонентами; (ii) увесь вміст дисків, компакт- і DVD-дисків, повідомлень електронної пошти та будь-яких вкладень або інших носіїв, з якими надається ця Угода, разом із формою об’єктного коду Програмного забезпечення, що постачається на носії даних, надається електронною поштою чи

завантажується через Інтернет; (iii) усі письмові пояснення та будь-яку іншу документацію, пов’язану з Програмним забезпеченням, насамперед опис Програмного забезпечення, його характеристик, властивостей і способу використання, опис операційного середовища, у якому використовується Програмне забезпечення, інструкції із застосування або інсталяції Програмного забезпечення чи будь-який опис правил його використання ("Документація"); (iv) копії Програмного забезпечення, виправлення можливих помилок Програмного забезпечення, доповнення до нього, його розширення, змінені версії Програмного забезпечення й усі оновлення його компонентів (якщо є), право на використання яких Вам надає Постачальник згідно з розділом 3 цієї Угоди. Програмне забезпечення постачається виключно як виконуваний об’єктний код.

2. **Інсталяція, комп’ютер і ліцензійний ключ.** Програмне забезпечення, яке надається на носії даних або електронною поштою, завантажується з Інтернету, серверів Постачальника або отримується з інших джерел, необхідно інсталювати. Ви маєте інсталювати Програмне забезпечення на правильно налаштованому комп’ютері відповідно до мінімальних потреб, наведених у відповідній Документації. Метод інсталяції описано в Документації. На Комп’ютері, де Ви інсталюєте Програмне забезпечення, не повинно бути жодних програм або компонентів обладнання, які можуть негативно вплинути на роботу Програмного забезпечення. Під Комп’ютером розуміється обладнання, яке включає в себе, серед іншого, персональні комп’ютери, ноутбуки, робочі станції, надолонні комп’ютери, смартфони, ручні електронні пристрої або інші електронні пристрої, для яких розроблено Програмне забезпечення, на яких воно буде інсталюватися та (або) використовуватися. Ліцензійний ключ — унікальна послідовність символів, літер, цифр або спеціальних символів, що надається Кінцевому користувачу для легального використання Програмного забезпечення, його особливих версій або продовження терміну дії Ліцензії у відповідності до умов цієї Угоди.

3. **Ліцензія**. Якщо Ви погоджуєтеся з положеннями цієї Угоди й дотримуєтесь усіх наведених тут умов і положень, Постачальник надає Вам указані права ("Ліцензію").

а) **Інсталяція та використання.** Вам надається невиняткове та непередаване право інсталювати Програмне забезпечення на жорсткому диску комп’ютера або іншому носії для постійного зберігання даних, інсталяції та збереження Програмного забезпечення в пам’яті комп’ютерної системи, а також застосовувати, зберігати й відображати Програмне забезпечення.

б) **Застереження щодо кількості ліцензій.** Право використання Програмного забезпечення обумовлюється кількістю Користувачів. Наведена нижче інформація стосується одного Користувача: (i) інсталяція Програмного забезпечення на одній комп’ютерній системі або (ii) за умови, що обсяг ліцензії визначається кількістю поштових скриньок, один Користувач означає користувача комп’ютера, який отримує електронну пошту через користувацький поштовий агент («КПА»). Якщо КПА приймає електронну пошту, після чого автоматично розподіляє її між кількома користувачами, кількість Користувачів визначається відповідно до їх фактичного числа, серед якого розподіляється електронна пошта. Якщо поштовий сервер виконує функцію поштового шлюзу, кількість Користувачів дорівнює числу користувачів поштових серверів, яких обслуговує такий шлюз. Якщо адреси електронної пошти (наприклад, псевдоніми), точна кількість яких не визначена, належать одному користувачеві й один користувач приймає всі відповідні повідомлення, а пошта не розподіляється автоматично клієнтом між більшою кількістю користувачів, Ліцензія необхідна лише для одного комп’ютера. Забороняється одночасно використовувати одну й ту саму Ліцензію на кількох комп’ютерах. Кінцевий користувач має право вводити Ліцензійний ключ у Програмному забезпеченні виключно в межах наявних у цього користувача прав на використання Програмного забезпечення та у відповідності до обмеження кількості Ліцензій, наданих Постачальником. Ліцензійний ключ є

конфіденційною інформацією. Ви не маєте права ділитися Ліцензійним ключем із третіми особами або дозволяти їм використовувати Ліцензійний ключ, якщо це не дозволено цією Угодою або Постачальником. У випадку порушення конфіденційності Ліцензійного ключа негайно повідомте про це Постачальника.

c) **Home/Business Edition.** Версія Програмного забезпечення Home Edition має використовуватися виключно в приватному та (або) некомерційному середовищі лише для сімейних і домашніх потреб. Для використання в комерційному середовищі та на поштових серверах, засобах пересилання пошти, поштових або інтернет-шлюзах потрібно придбати версію Програмного забезпечення Business Edition.

г) **Термін дії ліцензії.** Право використання Програмного забезпечення обмежено в часі.

e) **OEM-версія Програмного забезпечення.** OEM-версії Програмного забезпечення мають використовуватися лише на Комп'ютері, з яким постачаються. Його заборонено передавати для використання на іншому комп'ютері.

f) **НДП та ПРОБНА ВЕРСІЯ Програмного забезпечення.** Програмне забезпечення, що визначається як «не для продажу» (НДП), або його ПРОБНА ВЕРСІЯ не підлягає оплаті та має використовуватися лише в демонстраційних цілях чи для тестування функцій Програмного забезпечення.

g) **Припинення дії ліцензії.** Дія ліцензії припиняється автоматично після закінчення періоду, на який вона надається. Якщо Ви не дотримуєтеся положень цієї Угоди, Постачальник має право скасувати Угоду без шкоди для своїх прав або судового захисту, що надається Постачальнику в таких випадках. У разі скасування Ліцензії Ви повинні негайно видалити, знищити чи повернути за власний кошт Програмне забезпечення та всі резервні копії в компанію ESET або торгову точку, де Ви отримали Програмне забезпечення. Якщо дію Ліцензії припинено, Постачальник також має право скасувати право Користувача використовувати функції Програмного забезпечення, для чого потрібне підключення до серверів Постачальника або серверів третіх осіб.

4. **Функції, для яких потрібні дозволи на збір даних та доступ до Інтернету.** Для правильної роботи Програмному забезпеченню потрібно збирати дані (у відповідності до Політики конфіденційності), підключатися до Інтернету і через рівні проміжки часу з'єднуватися з серверами Постачальника або третіх осіб. Для належної роботи та оновлення й модернізації Програмного забезпечення потрібне підключення до Інтернету та дозволи на збирання даних. Постачальник має право випускати оновлення й модернізації Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення інсталюються автоматично, якщо Користувач не вимкнув відповідну функцію. Для надання оновлень нам необхідно перевірити автентичність Ліцензії, включаючи інформацію про комп'ютер та (або) платформу, на якій інстальовано Програмне забезпечення у відповідності до Політики конфіденційності.

На надання Оновлень може поширюватися Політика закінчення терміну служби ("Політика EOL"), доступна за адресою https://go.eset.com/eol_business. Оновлення Програмного забезпечення не надаватимуться після завершення терміну служби будь-яких його функцій, визначених у Політиці EOL.

З метою виконання положень цієї Угоди Постачальнику необхідно збирати, обробляти та зберігати дані, які дають змогу ідентифікувати Вас, у відповідності до Політики

конфіденційності. Ви дозволяєте Постачальнику власними засобами перевіряти, чи використовуєте Ви програмне забезпечення у відповідності до положень цієї Угоди. Ви погоджуєтесь, що з метою виконання положень цієї Угоди для забезпечення функціональності Програмного забезпечення і надання авторизації на його використання, а також для захисту прав Постачальника будуть передаватися дані між Програмним забезпеченням і комп'ютерними системами Постачальника та його бізнес-партнерів, що входять до його мережі підтримки та розповсюдження.

Після укладання цієї Угоди Постачальник або його бізнес-партнери (які входять до мережі підтримки і розповсюдження Постачальника) матимуть право передавати, обробляти й зберігати важливі дані, що ідентифікують Вас, для виставлення рахунків, виконання цієї Угоди та передавання сповіщень на Ваш комп'ютер.

Докладні відомості про конфіденційність, захист персональних даних і Ваші права як суб'єкта даних можна знайти в документі "Політика конфіденційності" на веб-сайті Постачальника. Окрім того, ця інформація доступна безпосередньо в процесі інсталяції. Також можна ознайомитися з цим документом у довідці Програмного забезпечення.

5. **Реалізація прав Користувача**. Ви зобов'язуєтеся реалізувати права Користувача особисто або через своїх співробітників. Ви маєте право використовувати Програмне забезпечення лише для захисту безпеки своєї роботи та тих комп'ютерів і комп'ютерних систем, для яких надано Ліцензію.

6. **Обмеження прав.** Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Програмного забезпечення. Використовуючи Програмне забезпечення, Ви зобов'язуєтеся дотримуватися наведених нижче обмежень.

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

b) Ви не маєте права використовувати, змінювати, перебудовувати Програмне забезпечення, робити його копії або передавати право на використання Програмного забезпечення чи його копій будь-яким способом, окрім чітко передбаченого положеннями цієї Угоди.

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

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

e) Ви погоджуєтеся використовувати Програмне забезпечення лише таким способом, що відповідає всім застосовним юридичним нормам законодавства, яке регулює його застосування, включно з відповідними обмеженнями згідно із законом про авторське право й інші права на інтелектуальну власність, але не обмежуючись цим.

f) Ви даєте свою згоду використовувати Програмне забезпечення та його функції лише таким способом, що не обмежує можливостей доступу до них інших кінцевих користувачів. Постачальник зберігає за собою право обмежити перелік доступних послуг, що надаються

окремим кінцевим користувачам, з метою надання своїх послуг максимальній кількості кінцевих користувачів. Обмеження переліку доступних послуг також передбачає повну заборону на використання будь-яких функцій Програмного забезпечення й видалення Даних та інформації із серверів Постачальника або серверів третьої сторони, пов'язаних із конкретною функцією Програмного забезпечення.

g) Ви погоджуєтеся не вчиняти будь-які дії щодо використання Ліцензійного ключа, які суперечать положенням цієї Угоди або можуть призвести до передачі Ліцензійного ключа будь-якій особі, яка не має права використовувати Програмне забезпечення. Зокрема, Ви погоджуєтеся не передавати використовуваний або невикористовуваний Ліцензійний ключ у будь-якій формі, а також утриматися від несанкціонованого відтворення або розповсюдження дублікатів Ліцензійних ключів або створених Ліцензійних ключів або від використання Програмного забезпечення з Ліцензійним ключем, отриманим із будь-якого іншого джерела, окрім Постачальника.

7. **Авторське право**. Програмне забезпечення та всі права, включно із правами власності та відповідними правами на інтелектуальну власність без обмежень, належать компанії ESET та/або її ліцензіарам. Ці права захищено положеннями міжнародного договірного права та всіма іншими застосовними законами країни, у якій використовується Програмне забезпечення. Структура, організація та код Програмного забезпечення є комерційною таємницею та конфіденційною інформацією компанії ESET і/або її ліцензіарів. Ви не маєте права копіювати Програмне забезпечення, за винятком визначених у розділі 6 (a) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосовуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то погоджуєтеся, що будь-яка отримана таким чином інформація буде автоматично й безповоротно вважатися належною для передавання Постачальнику та цілком належатиме йому з моменту її отримання, незалежно від права Постачальника на розірвання цієї Угоди.

8. **Захист прав**. Постачальник залишає за собою всі права на Програмне забезпечення, за винятком тих, що чітко надані Вам як Користувачу Програмного забезпечення відповідно до умов цієї Угоди.

9. **Багатомовні версії, програмне забезпечення, що постачається на носіях двох типів, кілька копій**. Якщо Програмне забезпечення підтримує кілька платформ чи мов, або Ви одержали кілька копій Програмного забезпечення, Ви не маєте права інсталювати Програмне забезпечення на більшій кількості комп'ютерних систем або інші версії ніж ті, на які розповсюджується Ліцензія. Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, укладати договір лізингу, надавати право на користування чи передавати версії або копії Програмного забезпечення, які Ви не використовуєте.

10. **Набуття Угодою чинності та припинення дії Угоди.** Ця Угода набуває чинності з дати погодження з її умовами. Ви можете припинити дію цієї Угоди, остаточно видаливши, знищивши або повернувши за власний кошт Програмне забезпечення, усі резервні копії та всі пов'язані матеріали, отримані від Постачальника або його ділових партнерів. На право використання Програмного забезпечення та його функцій може поширюватися Політика EOL. Після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL, ваше право на використання Програмного забезпечення буде скасовано. Незалежно від способу припинення дії цієї Угоди, умови розділів 7, 8, 11, 13, 19 і 21 є чинними без обмежень у часі.

11. **ЗАЯВА КОРИСТУВАЧА**. ЯК КОРИСТУВАЧ, ВИ ВИЗНАЄТЕ, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАДАЄТЬСЯ «ЯК Є» БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОПУСКАЄТЬСЯ ЧИННИМ ЗАКОНОДАВСТВОМ. НІ ПОСТАЧАЛЬНИК РАЗОМ ІЗ ЙОГО ЛІЦЕНЗІАРАМИ Й ДОЧІРНІМИ КОМПАНІЯМИ, НІ ВЛАСНИКИ АВТОРСЬКОГО ПРАВА НЕ НАДАЮТЬ БУДЬ-ЯКИХ ТВЕРДЖЕНЬ АБО СПЕЦІАЛЬНИХ ЧИ НЕПРЯМИХ ГАРАНТІЙ, ЗОКРЕМА ГАРАНТІЙ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ ЧИ КОНКРЕТНОГО ЗАСТОСУВАННЯ АБО ГАРАНТІЙ ТОГО, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НЕ ПОРУШУЄ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЄ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ АБО ВОНО ФУНКЦІОНУВАТИМЕ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ’ЯЗАНІ З ВИБОРОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ, А ТАКОЖ ЗА ІНСТАЛЯЦІЮ, ВИКОРИСТАННЯ ТА НАСЛІДКИ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

12. **Відсутність інших зобов’язань**. Ця Угода не створює жодних зобов’язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

13. **ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ**. У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ЛІЦЕНЗІАРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ВТРАЧЕНІ ПРИБУТКИ, ДОХОДИ, ЗНИЖЕННЯ ОБСЯГІВ ПРОДАЖІВ АБО ВТРАТУ ДАНИХ, А ТАКОЖ ДОДАТКОВІ ВИТРАТИ, ПОВ’ЯЗАНІ З ПРИДБАННЯМ ЗАПАСНИХ ТОВАРІВ АБО ПОСЛУГ, ЗАПОДІЯНУ МАЙНУ ШКОДУ, ОСОБИСТУ ШКОДУ, ПРИПИНЕННЯ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, ВТРАТУ ДІЛОВОЇ ІНФОРМАЦІЇ ЧИ БУДЬ-ЯКІ СПЕЦІАЛЬНІ, ПРЯМІ, НЕПРЯМІ, ВИПАДКОВІ, КОМЕРЦІЙНІ, ШТРАФНІ ЧИ ОПОСЕРЕДКОВАНІ ЗБИТКИ, БУДЬ-ЯКИМ ЧИНОМ ОБУМОВЛЕНІ ДІЄЮ УГОДИ, ЦИВІЛЬНЕ ПРАВОПОРУШЕННЯ, НЕДБАЛІСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ІНСТАЛЯЦІЇ, ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНІМ КОМПАНІЯМ ВІДОМО ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ. В ОКРЕМИХ КРАЇНАХ І ЮРИСДИКЦІЯХ НЕ ПЕРЕДБАЧЕНО ВИНЯТКИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ, АЛЕ ЇЇ МОЖЕ БУТИ ОБМЕЖЕНО. ТОБТО ВІДПОВІДАЛЬНІСТЬ ПОСТАЧАЛЬНИКА, ЙОГО СПІВРОБІТНИКІВ, ЛІЦЕНЗІАРІВ АБО ДОЧІРНІХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ЛІЦЕНЗІЮ.

14. Жодна умова цієї Угоди не має порушувати законні права будь-якої сторони, що виступає як клієнт, у тих випадках, коли вони їм суперечать.

15. **Технічна підтримка**. Компанія ESET або вповноважені нею треті сторони надають технічну підтримку на власний розсуд без жодних гарантій або заяв. Технічна підтримка не надаватиметься після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL. Перед наданням технічної підтримки Користувач повинен створити резервні копії всіх поточних даних, програмного забезпечення та програмних засобів. Компанія ESET або вповноважені нею треті сторони не несуть відповідальності за пошкодження або втрату даних, майна, програмного чи апаратного забезпечення, а також комерційні збитки, що виникають унаслідок надання технічної підтримки. Компанія ESET і/або вповноважені нею треті сторони залишають за собою право приймати рішення щодо того, чи належить проблема до обсягу послуг, які надаються в рамках технічної підтримки. Компанія ESET залишає за собою право на власний розсуд приймати рішення щодо відмови в наданні технічної підтримки, її призупинення чи скасування. Для забезпечення технічного обслуговування може знадобитися інформація про Ліцензію та інші дані у відповідності до Політики конфіденційності.

16. **Передача Ліцензії**. Програмне забезпечення може передаватися з однієї комп’ютерної

системи на іншу, якщо такі дії не суперечать умовам Угоди. За умови дотримання положень Угоди Користувач має право остаточної передачі Ліцензії та всіх прав, що виникають унаслідок укладання цієї Угоди, іншому Користувачеві за згоди Постачальника, якщо (i) вихідний Користувач не зберігає жодних копій Програмного забезпечення; (ii) виконується пряма передача прав, наприклад, від вихідного Користувача до нового; (iii) новий Користувач приймає від вихідного всі права, що надаються відповідно до умов цієї Угоди; (iv) вихідний Користувач надає новому документацію, що дозволяє підтвердити автентичність Програмного забезпечення відповідно до розділу 17.

17. **Підтвердження автентичності Програмного забезпечення.** Кінцевий користувач може підтвердити своє право застосовувати Програмне забезпечення одним із таких способів: (i) за допомогою ліцензійного сертифіката, наданого Постачальником або вповноваженою ним третьою особою; (ii) за допомогою ліцензійної угоди в письмовій формі (якщо така укладалася); (iii) надавши надісланий Постачальником електронний лист із ліцензійними даними (ім’я користувача та пароль). Для підтвердження автентичності Програмного забезпечення може знадобитися інформація про Ліцензію та ідентифікаційні дані Кінцевого споживача у відповідності до Політики конфіденційності.

18. **Надання ліцензії органам державної влади й уряду США**. Програмне забезпечення надається органам державної влади, включно з урядом США, з урахуванням ліцензійних прав і обмежень, наведених у цій Угоді.

19. **Дотримання процедур із контролю за торгівлею**.

a) Забороняється в прямий чи непрямий спосіб експортувати, реекспортувати, передавати або іншим чином надавати програмне забезпечення будь-яким іншим особам. Ви зобов’язуєтеся утриматися від будь-яких способів використання цього програмного забезпечення й (або) не брати участь у жодних діях, які можуть призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET, її холдингових і дочірніх компаній або дочірніх компаній будь-яких холдингових компаній ESET, відповідно до законів із контролю за торгівлею, зокрема тих, що наведені нижче:

i. Усі закони, які регулюють, обмежують або накладають ліцензійні вимоги для експорту, реекспорту або передачі товарів, програмного забезпечення, технологій або послуг, що видані або прийняті будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов’язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії

ii. Усі економічні, фінансові, торгові або інші санкції, обмеження, ембарго, заборони експорту або імпорту, заборони передачі коштів або активів чи надання послуг або рівнозначні заходи, які запроваджуються будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов’язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії.

(законні акти, зазначені в пунктах i та ii вище, разом згадуються як "Закони з контролю за торгівлею").

b) ESET має право призупинити виконання зобов’язань за цими Умовами або припинити їх дію з негайним набуттям чинності за таких умов:

i. ESET має обґрунтовані підстави вважати, що Користувачем уже порушено, або, імовірно, буде порушено умови Статті 19 a) Угоди; або

ii. Користувач і (або) Програмне забезпечення стали предметом законів із контролю за торгівлею, і через це ESET має обґрунтовані підстави вважати, що подальше виконання зобов'язань за цією Угодою може призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET або афілійованих із нею компаній відповідно до законів із контролю за торгівлею.

c) Жодна умова Угоди в жодному разі не має тлумачитися як така, що має на меті спонукати будь-яку зі сторін або вимагати від неї вчинити дії або утриматися від вчинення дій (чи погодитися на це) у будь-який спосіб, який буде суперечити законам із контролю за торгівлею або заборонений цими законами.

20. **Примітки**. Усі зауваження та запити на повернення Програмного забезпечення та Документації слід надсилати на адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic без шкоди для права ESET повідомляти Вам про зміни цієї Угоди, Політики конфіденційності, Політики EOL та Документації відповідно до ст. 22 Угоди. ESET може надсилати Вам електронні листи, сповіщення в програмі через Програмне забезпечення або розміщувати повідомлення на Вашому веб-сайті. Ви погоджуєтеся отримувати сповіщення правового характеру від ESET в електронній формі, зокрема всі сповіщення про внесення змін в Умови, Спеціальні Умови або Політики конфіденційності, будь-які пропозиції укласти (прийняти) договір або запрошення до початку ділових відносин, сповіщення з правовою інформацією або будь-які інші повідомлення правового характеру. Отримання таких повідомлень в електронній формі прирівнюється до їх отримання в письмовий формі, якщо інше явно не вимагається застосовними законами.

21. **Чинне законодавство.** Ця Угода регулюється та тлумачиться відповідно до законодавства Словацької Республіки. Користувач і Постачальник погоджуються, що суперечливі положення регулюючого законодавства та Конвенції Організації Об'єднаних Націй щодо контрактів для міжнародної торгівлі товарами не мають застосовуватися. Ви повністю погоджуєтеся, що розгляд будь-яких заяв до Постачальника чи суперечок із ним, які викликано цією Угодою, або заяв чи суперечок, будь-яким чином пов'язаних із використанням Програмного забезпечення, і прийняття відповідних рішень здійснюється окружним судом м. Братислава I, а також підтверджуєте виконання юрисдикції вказаним судом.

22. **Загальні положення**. Якщо будь-яке з положень цієї Угоди юридично не дійсне або не має позовної сили, це не повинно впливати на законність інших положень Угоди. Вони повинні залишатися чинними й такими, що мають законну силу, відповідно до передбачених тут умов. Цю Угоду укладено англійською. У разі розбіжностей між англійською й перекладеною версією Угоди (наданою для зручності або з будь-якою іншою метою) перевага надається документу англійською мовою.

Компанія ESET зберігає за собою право в будь-який час змінювати Програмне забезпечення, а також змінювати текст цієї Угоди, Додатків і Доповнень до неї, Політики конфіденційності, Політики закінчення терміну служби та документації або будь-яких їхніх складових шляхом оновлення застосовного документа (i) відповідно до змін, внесених в Програмне забезпечення або в спосіб ведення бізнесу ESET, (ii) із юридичних, регуляторних причин та з міркувань безпеки або (iii) для запобігання несанкціонованому використанню або нанесенню шкоди. Ми сповістимо Вас про будь-яке внесення змін в Угоду в електронному листі, сповіщенням в програмі або через інші електронні способи зв'язку. Якщо Ви не згодні із запропонованими змінами в Угоді, то можете припинити її дію відповідно до ст. 10 протягом 30 днів після отримання сповіщення

про зміну. Якщо Ви не припинете дію Угоди протягом цього терміну, запропоновані зміни вважатимуться прийнятими й наберуть чинності з дати отримання Вами сповіщення про зміну.

Цей документ становить повну Угоду між Вами й Постачальником щодо Програмного забезпечення та цілком заміняє будь-які попередні подання, обговорення, зобов'язання, повідомлення й рекламні матеріали, пов'язані з Програмним забезпеченням.

ДОДАТОК ДО УГОДИ

Надсилання Даних Постачальнику. Додаткові положення застосовуються до Надсилання Даних Постачальнику таким чином:

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.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Політика конфіденційності

Компанія ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic), внесена до комерційного реєстру окружного суду м. Братислави I, Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532) як Контролер Даних (далі "ESET" або "Ми") прагне прозорості в справах, що стосуються обробки персональних даних і збереження конфіденційності наших клієнтів. З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів ("Кінцевий користувач" або "Ви") про такі теми:

- Обробка персональних даних
- Конфіденційність даних
- Права суб'єкта захисту даних

Обробка персональних даних

Служби, які надаються ESET, реалізовані в нашому продукті й надаються згідно з Ліцензійною угодою з кінцевим користувачем (далі "Ліцензійна угода"). Однак деякі аспекти потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов'язаний із наданням наших послуг. Ми надаємо різні служби, наведені в Ліцензійній угоді й документації

для відповідного продукту. Ідеться, зокрема, про службу оновлення/модернізації, ESET LiveGrid®, захист від несанкціонованого використання даних, служби підтримки тощо. Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

• 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 стиснутій і анонімній формі, а також інші дані від ESET LiveGrid® можуть оброблятися для статистичних цілей.

ESET впроваджує відповідні технічні та організаційні заходи, щоб забезпечити безпеку на тому рівні, якій відповідає потенційним ризикам. Ми докладаємо 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