ESET Server Security

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Digital Security
Progress. Protected.

Авторское право ©2024 ESET, spol. s r.o.

ESET Server Security разработано компанией ESET, spol. s r.o.

Дополнительные сведения можно получить на сайте https://www.eset.com.

Все права защищены. Ни одна часть этой документации не может воспроизводиться, храниться в системе получения и передаваться в любой форме или любыми средствами, в том числе электронными и механическими способами, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без письменного разрешения автора.

ESET, spol. s r.o. оставляет за собой право изменять любое описанное прикладное программное обеспечение без предварительного уведомления.

Служба технической поддержки: https://support.eset.com

ПРОВ. 17.01.2024

1 Обзор ... 1
1.1 Основные функции ... 1
1.2 Новые возможности ... 3
1.3 Типы защиты ... 3
2 Подготовка к установке ... 3
2.1 Требования к системе ... 5
2.2 Требование совместимости с алгоритмом SHA-2 ... 6
2.3 Этапы установки программы ESET Server Security ... 7
2.3 Экспорт настроек или удаление установки ... 11
2.4 Автоматическая установка/установка без участия пользователя ... 12
2.4 Установка из командной строки ... 13
2.5 Активация программы ... 16
2.5 ESET Business Account ... 18
2.5 Активация выполнена ... 18
2.5 Сбой активации ... 18
2.5 Лицензия ... 18
2.6 Обновление до последней версии ... 18
2.6 Обновление с помощью ESET PROTECT ... 19
2.6 Обновление с помощью кластера ESET ... 21
2.7 Установка в кластерной среде ... 24
2.8 Сервер терминалов ... 24
2.9 Обновления для обеспечения безопасности и стабильности ... 25
3 Начало работы ... 25
3.1 Управление через ESET PROTECT ... 25
3.2 Мониторинг ... 26
3.2 Состояние ... 28
3.2 Доступны обновления для Windows ... 29
3.2 Изоляция сети ... 30
4 Если использовать ESET Server Security ... 31
4.1 Сканировать ... 32
4.1 Окно и журнал сканирования ... 34
4.2 Файлы журнала ... 36
4.2 Фильтрация журнала ... 39
4.3 Обновление ... 41
4.4 Настройка ... 43
4.4 Сервер ... 44
4.4 Компьютер ... 45
4.4 Сеть ... 46
4.4 Мастер устранения сетевых неисправностей ... 47
4.4 Интернет и электронная почта ... 48
4.4 Сервис — ведение журнала диагностики ... 48
4.4 Импорт и экспорт параметров ... 49
4.5 Сервис ... 50
4.5 Запущенные процессы ... 51
4.5 Мониторинг ... 53
4.5 Статистика системы защиты ... 54
4.5 Кластер ... 56
4.5 Мастер кластеров — выбор узлов ... 58
4.5 Мастер кластеров — настройки кластера ... 59
4.5 Мастер кластеров — параметры настройки кластера ... 59

4.5 Мастер кластеров — проверка узлов ... 60
4.5 Мастер кластеров — установка узлов ... 62
4.5 ESET Shell ... 65
4.5 Использование ... 67
4.5 Команды ... 73
4.5 Пакетные файлы и сценарии ... 76
4.5 ESET SysInspector ... 77
4.5 ESET SysRescue Live ... 78
4.5 Планировщик ... 78
4.5 Добавление задачи в планировщике ... 80
4.5 Тип задачи ... 82
4.5 Время задачи ... 83
4.5 При определенных условиях ... 83
4.5 Запуск приложения ... 84
4.5 Пропущенная задача ... 84
4.5 Обзор запланированных задач ... 84
4.5 Отправка образцов на анализ ... 85
4.5 Подозрительный файл ... 86
4.5 Подозрительный сайт ... 86
4.5 Ложное срабатывание файл ... 87
4.5 Ложное срабатывание сайт ... 87
4.5 Другое ... 87
4.5 Карантин ... 88
4.6 Настройка сканирования OneDrive ... 89
4.6 Регистрация модуля сканирования ESET OneDrive ... 92
4.6 Отмена регистрации модуля сканирования ESET OneDrive ... 97
5 Общие параметры ... 102
5.1 Detection engine ... 103
5.1 Обнаружение с помощью машинного обучения ... 105
5.1 Исключения ... 108
5.1 Исключения для быстродействия ... 108
5.1 Мастер исключений ... 111
5.1 Расширенные параметры ... 112
5.1 Автоматические исключения ... 112
5.1 Общий локальный кэш ... 113
5.1 Действия при обнаружении заражения ... 113
5.1 Защита файловой системы в режиме реального времени ... 114
5.1 ThreatSenseПараметры ... 116
5.1 Дополнительные параметры ThreatSense ... 120
5.1 Исключенные из сканирования расширения файлов ... 121
5.1 Исключения для процессов ... 121
5.1 Облачная защита ... 122
5.1 Фильтр исключений ... 124
5.1 Процессы сканирования вредоносных программ ... 125
5.1 Диспетчер профилей ... 126
5.1 Объекты профиля ... 127
5.1 Объекты сканирования ... 129
5.1 Сканирование в состоянии простоя ... 132
5.1 Сканирование файлов, исполняемых при запуске системы ... 132
5.1 Автоматическая проверка файлов при запуске системы ... 132
5.1 Съемные носители ... 133

5.1 Защита документов ... 134
5.1 Сканирование Hyper-V ... 135
5.1 Сканирование OneDrive ... 137
5.1 Система HIPS ... 138
5.1 Параметры правил HIPS ... 140
5.1 Дополнительные параметры системы HIPS ... 143
5.2 Обновить конфигурацию ... 144
5.2 Откат обновления ... 148
5.2 Запланированная задача — обновление. ... 148
5.2 Зеркало обновлений ... 148
5.3 Защита сети ... 150
5.3 Известные сети ... 150
5.3 Добавление сети ... 151
5.3 Зоны ... 152
5.4 Защита от сетевых атак ... 153
5.4 Исключения IDS ... 154
5.4 Возможна угроза заблокирована ... 155
5.4 Черный список временных IP-адресов ... 155
5.4 Защита от атак методом подбора ... 156
5.4 Правила Защиты от атак методом подбора ... 156
5.4 Исключения в защите от атак методом подбора ... 157
5.5 Интернет и электронная почта ... 157
5.5 Фильтрация протоколов ... 158
5.5 Веб-клиенты и почтовые клиенты ... 158
5.5 SSL/TLS ... 159
5.5 Список известных сертификатов ... 161
5.5 Шифрованное соединение SSL ... 161
5.5 Защита почтового клиента ... 162
5.5 Протоколы электронной почты ... 163
5.5 Предупреждения и уведомления ... 164
5.5 Панель инструментов Microsoft Outlook ... 165
5.5 Панель инструментов Outlook Express и Почты Windows ... 166
5.5 Окно подтверждения ... 166
5.5 Повторное сканирование сообщения ... 166
5.5 Защита доступа в Интернет ... 167
5.5 Управление URL-адресами ... 167
5.5 Создание списка ... 169
5.5 Веб-защита от фишинга ... 171
5.6 Контроль устройств ... 172
5.6 Правила устройств ... 172
5.6 Группы устройств ... 175
5.7 Конфигурация служебных программ ... 176
5.7 Временные интервалы ... 176
5.7 Центр обновления Windows ... 177
5.7 Сканер командной строки ... 177
5.7 ESET CMD ... 179
5.7 ESET RMM ... 181
5.7 Лицензия ... 182
5.7 Поставщик инструментария WMI ... 183
5.7 Предоставляемые данные ... 183
5.7 Получение доступа к предоставляемым данным ... 194

5.7 Объекты сканирования в консоли управления ESET 195
5.7 Режим переопределения 195
5.7 Файлы журнала 198
5.7 Прокси-сервер 201
5.7 Уведомления 201
5.7 Уведомления приложения 202
5.7 Уведомления на рабочем столе 202
5.7 Уведомления по электронной почте 203
5.7 Настройка 205
5.7 Режим презентации 205
5.7 Диагностика 206
5.7 Техническая поддержка 207
5.7 Кластер 207
5.8 Интерфейс пользователя 209
5.8 Окна предупреждений и сообщений 211
5.8 Настройка доступа 211
5.8 ESET Shell 212
5.8 Отключение графического интерфейса пользователя на сервере терминалов 213
5.8 Отключенные сообщения и состояния 213
5.8 Параметры состояний приложения 213
5.8 Значок в области уведомлений Windows 214
5.9 Восстановление параметров по умолчанию 216
5.10 Справка и поддержка 217
5.10 Отправка запроса в службу поддержки клиентов 218
5.10 О программе ESET Server Security 218
5.11 Глоссарий 218
6 Лицензионное соглашение с конечным пользователем 218
7 Политика конфиденциальности 228

Обзор

ESET Server Security — это интегрированное решение, разработанное специально для среды Microsoft Windows Server. ESET Server Security обеспечивает эффективную и надежную защиту от разных типов вредоносных программ, предлагая два вида защиты: от вредоносных и шпионских программ.

См. разделы Основные функции и Новые возможности в последней версии.

Основные функции

В таблице ниже приведен список функций, доступных в ESET Server Security. Программа ESET Server Security поддерживает большинство выпусков Microsoft Windows Server 2008 R2 SP1, 2012, 2016 и 2019 в автономных и кластерных средах. В более крупных сетях для дистанционного управления ESET PROTECT можно использовать ESET Server Security.

True 64-bit product core (Оптимизация компонентов ядра 64-разрядной версии)	**Эта функция позволяет повысить производительность и стабильность компонентов ядра 64-разрядной версии.**
Защита от вредоносных программ	Это отмеченное наградами инновационное средство защиты от вредоносных программ. Эта передовая технология предотвращает атаки и устраняет угрозы любого типа, в том числе вирусы, программы-вымогатели, руткиты, черви и шпионские программы, с помощью сканирования на основе облака, что позволяет обеспечить более высокую скорость обнаружения. Использование этой технологии не влияет на производительность и не требует большого количества системных ресурсов. В ней используется многоуровневая модель безопасности. На каждом уровне или этапе используется ряд основных технологий. На этапе перед выполнением используются такие технологии, как Модуль сканирования UEFI, защита от сетевых атак, репутация и кэш, встроенная песочница, ДНК-обнаружение. На этапе выполнения используются технологии Блокировщик эксплойтов, Защита от программ-вымогателей, Расширенный модуль сканирования памяти и модуль сканирования сценариев (AMSI), а на этапе после выполнения используются такие технологии, как защита от ботнетов, облачная система защиты от вредоносных программ и песочница. Этот широкофункциональный набор основных технологий обеспечивает беспрецедентный уровень защиты.
Сканирование OneDrive	Новая функция, позволяющая сканировать файлы, хранимые в облачном хранилище OneDrive. Предназначена для учетных записей Office 365 для бизнеса.
Сканирование Hyper-V	Новая технология, с помощью которой можно сканировать диски виртуальных машин на сервере Microsoft Hyper-V Server без необходимости установки агентов на соответствующие виртуальные машины.

True 64-bit product core (Оптимизация компонентов ядра 64-разрядной версии)	**Эта функция позволяет повысить производительность и стабильность компонентов ядра 64-разрядной версии.**
ESET LiveGuard Advanced	Облачная служба ESET. Когда решение ESET Server Security обнаруживает подозрительный код или поведение, оно предотвращает дальнейшую активность угрозы, временно помещая ее в карантин ESET LiveGuard Advanced. Подозрительный образец автоматически отправляется на сервер ESET LiveGuard Advanced для анализа с использованием новейших механизмов обнаружения вредоносных программ. Результат анализа отправляется обратно в ESET Server Security. Действия, выполняемые с подозрительным файлом, зависят от результатов.
Кластер ESET	Кластер ESET дает возможность централизованно управлять несколькими серверами из одного расположения. Подключение рабочих станций к узлам дополнительно автоматизирует управление, так как становится возможным распределять политики конфигурации по всем элементам кластера. Создавать кластеры можно с помощью установленного узла, который может затем установить и запустить все узлы удаленно. При этом серверные продукты ESET могут обмениваться данными, например сведениями о конфигурации и уведомлениями, и могут синхронизировать данные, необходимые для надлежащей работы группы экземпляров продуктов. Это позволяет применять одну конфигурацию продукта для всех элементов кластера. Отказоустойчивый кластер Windows и кластер балансировки сетевой нагрузки (NLB) поддерживаются продуктом ESET Server Security. Кроме того, можно добавить элементы кластера ESET вручную без необходимости использовать определенный кластер Windows. Кластеры ESET работают в средах с доменами и рабочими группами.
Автоматические исключения	Автоматическое обнаружение и исключение приложений и файлов на сервере, имеющих критическое значение для беспрепятственной и эффективной работы.
Исключения для процессов	Этот параметр исключает определенные процессы из сканирования на наличие вредоносных программ по доступу. В некоторых ситуациях сканирование на наличие вредоносных программ по доступу может вызывать конфликты, например во время резервного копирования или динамического переноса виртуальных машин. Исключения процессов помогают свести к минимуму риск возможных конфликтов и улучшить производительность исключенных приложений, что, в свою очередь, улучшает общую производительность операционной системы и повышает уровень ее стабильности. Исключение процесса или приложения исключает его исполняемый файл (.exe).
Оболочка ESET eShell	Оболочка eShell — это интерфейс командной строки, в котором опытные пользователи и администраторы найдут исчерпывающий спектр параметров управления серверными продуктами ESET.
ESET PROTECT	Улучшенная интеграция с ESET PROTECT, в том числе возможность добавить в расписание сканирование по требованию. Дополнительные сведения см. в онлайн-справке ESET PROTECT.
Компонентная установка	Можно настроить установку только выбранных компонентов продукта.

Новые возможности

Новые функции и улучшения в ESET Server Security:

- True 64-bit product core (Оптимизация компонентов ядра 64-разрядной версии)
- Сканирование OneDrive
- ESET LiveGuard Advanced
- ESET Inspect поддержка
- ESET RMM
- Изоляция сети
- Обнаружение с помощью машинного обучения
- Журналы аудита
- Микрообновление компонентов программы
- Защита от атак методом подбора

Типы защиты

Существует два типа защиты.

- Защита от вредоносных программ
- Защита от шпионских программ

Защита от вредоносных и шпионских программ — одна из основных функций продукта ESET Server Security. Такая защита предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и подключений к Интернету. Если обнаруживается угроза, модуль обнаружения может обезвредить ее, сначала заблокировав, а затем очистив, удалив или переместив в папку карантина.

Подготовка к установке

Ниже приведены действия, рекомендуемые в процессе подготовки продукта к установке.

- После приобретения ESET Server Security загрузите установочный пакет *.msi* с веб-сайта ESET .
- Убедитесь, что сервер, на котором вы планируете установить ESET Server Security, отвечает системным требованиям.
- Авторизуйтесь на сервере с помощью учетной записи администратора.

Обратите внимание, что установщик необходимо запускать с помощью встроенной учетной записи администратора или учетной записи администратора домена (если локальная учетная запись администратора отключена). Другие пользователи, даже если они являются участниками группы администраторов, не располагают достаточными правами доступа. Необходимо использовать встроенную учетную запись администратора, поскольку вы не сможете выполнить установку с помощью какой-либо другой учетной записи пользователя, кроме учетной записи локального администратора или администратора домена.

- Если вы собираетесь обновить имеющуюся установку ESET Server Security, советуем создать резервную копию ее текущей конфигурации с помощью функции Экспортировать параметры.

- Удалите все сторонние антивирусные программы с компьютера (если таковые есть). Рекомендуется использовать средство ESET AV Remover. Список сторонних антивирусных программ, которые можно удалить с помощью средства ESET AV Remover, см. в этой статье базы знаний .

- Если установка ESET Server Security выполняется в Windows Server 2016, корпорация Майкрософт рекомендует удалить функции Защитника Windows и отменить регистрацию в ATP в Защитнике Windows, чтобы предотвратить проблемы, которые могут возникнуть при наличии нескольких программ защиты от вирусов, установленных на компьютере.

- Если установка ESET Server Security выполняется в Windows Server 2019 или Windows Server 2022, корпорация Майкрософт рекомендует перевести Защитник Windows в пассивный режим во избежание проблем, связанных с наличием на одном компьютере нескольких антивирусных продуктов.

Установщик ESET Server Security можно запустить в двух режимах:

- Графический интерфейс пользователя (GUI)
  Это рекомендуемый режим установки в мастере.

- Автоматическая установка/установка без участия пользователя
  В дополнение к мастеру установки вы можете автоматически установить ESET Server Security из командной строки.

- Обновление до последней версии
  При использовании старой версии ESET Server Security вы можете выбрать подходящий метод обновления.

Настоятельно рекомендуем устанавливать программу ESET Server Security в только что установленной и настроенной операционной системе, если это возможно. Если необходимо установить программу в существующую систему, рекомендуется удалить предыдущую версию ESET Server Security, перезапустить сервер и после этого установить новую версию ESET Server Security.

После установки или обновления ESET Server Security сделайте следующее:

- Активация программы
  Доступность того или иного варианта в окне активации может зависеть от страны, а также от способа получения продукта.

- Настройка общих параметров

Решение ESET Server Security можно настроить, изменив расширенные параметры каждой функции в соответствии со своими потребностями.

Требования к системе

Поддерживаемые операционные системы

- Microsoft Windows Server 2022 (для серверов и настольных ПК)
- Microsoft Windows Server 2019 (для серверов и настольных ПК)
- Microsoft Windows Server 2016 (для серверов и настольных ПК)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 с установленными обновлениями KB4474419 и KB4490628 (см. Требование совместимости с алгоритмом SHA-2)
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2)

> В ОС Windows Server 2008 R2 SP1 компонент **Защита сети** по умолчанию отключен для **обычной** установки. Чтобы установить этот компонент, используйте **выборочную** установку.

> Чтобы устанавливать или обновлять продукты ESET, выпущенные по окончании июля 2023 года, необходимо установить поддержку подписывания кода Azure во всех операционных системах Windows. Дополнительные сведения.
> Если вы используете Windows Server 2008 R2 SP1, убедитесь, что у вас установлено обновление KB5006728 для поддержки подписывания кода Azure. Для установки KB5006728 требуются расширенные обновления безопасности (ESU).

Серверы Storage, Small Business и MultiPoint:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation

- Microsoft Windows Small Business Server 2011 SP1 (x64) с установленными обновлениями KB4474419 и KB4490628
- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

Поддерживаемые серверные операционные системы с ролью Hyper-V:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 — виртуальные машины можно сканировать только тогда, когда они не в сети.

Требования к оборудованию зависят от используемой версии операционной системы. Рекомендуется ознакомиться с документацией на Microsoft Windows Server для получения дополнительных сведений о требованиях к оборудованию.

> i Прежде чем устанавливать решение ESET по обеспечению безопасности, настоятельно рекомендуем установить последний пакет обновления для ОС Microsoft Server и серверного приложения. Кроме того, мы рекомендуем устанавливать последние обновления и исправления Windows по мере их появления.

Минимальные требования к оборудованию:

Компонент	Требование
Процессор	64-разрядный одноядерный процессор Intel или AMD
Объем памяти	256 МБ свободной памяти
Жесткий диск	700 МБ свободного места на диске
Разрешение экрана	800 x 600 пикселей или выше

Требование совместимости с алгоритмом SHA-2

В начале 2019 года корпорация Майкрософт объявила о прекращении использования алгоритма хеширования SHA-1 и начала процесс перехода на алгоритм SHA-2. Поэтому все сертификаты, подписанные с помощью алгоритма SHA-1, больше не признаются и будут вызывать предупреждения системы безопасности. К сожалению, с течением времени надежность алгоритма хеширования SHA-1 снизилась из-за наличия слабых мест в алгоритме, повышения производительности процессоров и перехода к облачным вычислениям.

Теперь предпочтительным методом, который гарантирует надежность защиты SSL, является алгоритм хеширования SHA-2 (пришедший на смену SHA-1). Для получения дополнительных сведений см. статью об алгоритмах хеширования и подписания в Документации Майкрософт.

> Это изменение означает, что в операционных системах без поддержки SHA-2 ваше решение для обеспечения безопасности ESET больше не сможет обновлять свои модули, в том числе модуль обнаружения, в результате чего приложение ESET Server Security не будет полностью функциональным и не сможет обеспечить достаточную защиту.

Если вы используете Windows Server 2008 R2 SP1 или Microsoft Windows Small Business Server 2011 SP1, убедитесь, что система совместима с SHA-2. Примените исправления в соответствии с конкретной версией вашей операционной системы, как указано ниже.

- **Microsoft Windows Server 2008 R2 SP1**: примените KB4474419 и KB4490628 (может потребоваться дополнительный перезапуск системы)

- **Microsoft Windows Small Business Server 2011 SP1 (x64)**: примените KB4474419 и KB4490628 (может потребоваться дополнительный перезапуск системы)

> После установки обновлений и перезапуска системы откройте графический интерфейс приложения ESET Server Security и проверьте его состояние. Если состояние обозначено оранжевым цветом, выполните дополнительный перезапуск системы. Состояние должно обозначаться зеленым цветом, что указывает на максимальную защиту.

> Рекомендуем установить последний пакет обновления для серверной операционной системы Microsoft и приложения. Рекомендуем устанавливать последние обновления и исправления Windows по мере их появления.

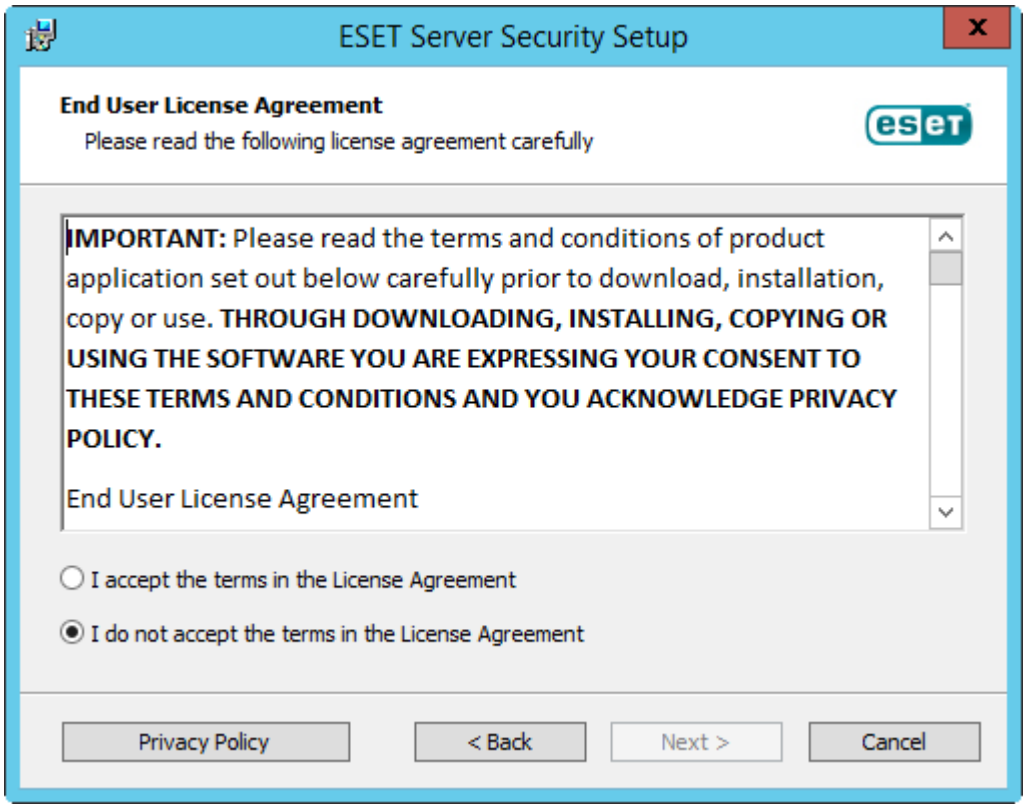
Этапы установки программы ESET Server Security

Это стандартный мастер установки с графическим пользовательским интерфейсом. Дважды щелкните пакет *.msi* и следуйте указаниям по установке ESET Server Security.

1. Нажмите кнопку **Далее**, чтобы продолжить, или **Отмена**, чтобы выйти из окна установки.

2. Мастер установки запускается на языке, указанном в поле **Home location** (Основное расположение) в разделе **Region** (Регион) > **Location** (Расположение) операционной системы (или в поле **Current location** (Текущее расположение) в разделе **Region and Language** (Язык и регион) > **Location** (Расположение) в предыдущих версиях операционной системы). Выберите из раскрывающегося меню **язык**, на котором будет установлен продукт ESET Server Security. Выбранный язык программы ESET Server Security не влияет на язык мастера установки.

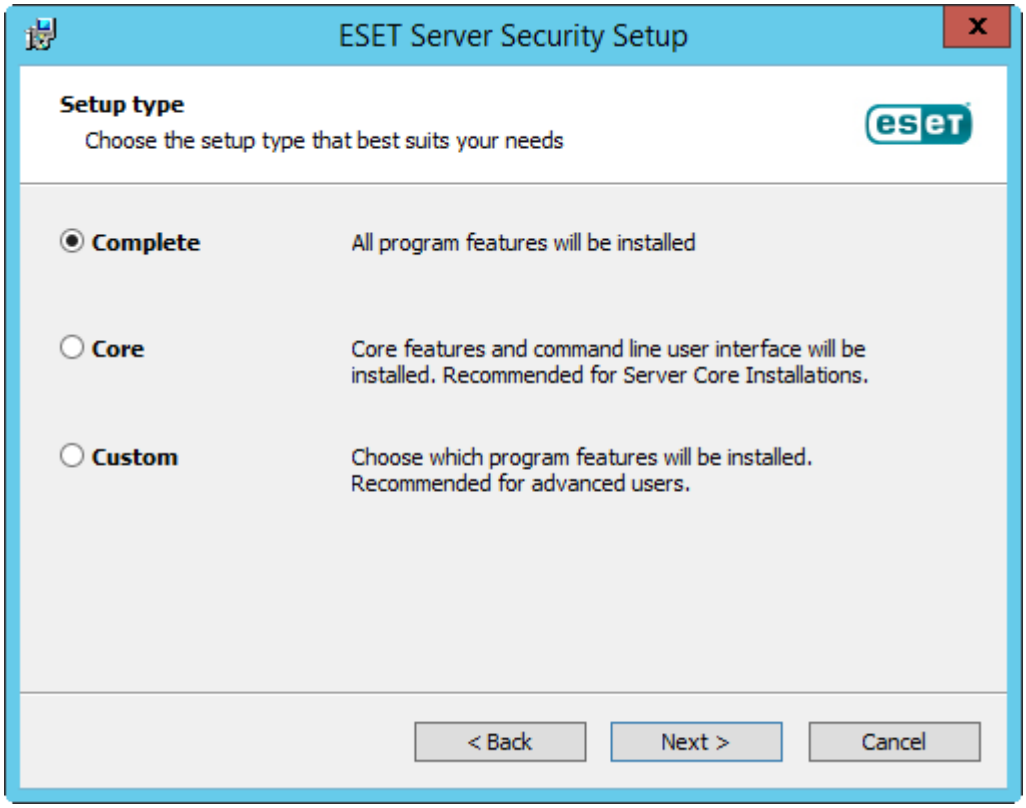
3. Щелкните **Далее**, после чего отобразится лицензионное соглашение с конечным пользователем. Приняв условия лицензионного соглашения и политики конфиденциальности, щелкните **Далее**.



4. Выберите один из доступных типов установки (доступные типы зависят от операционной системы):

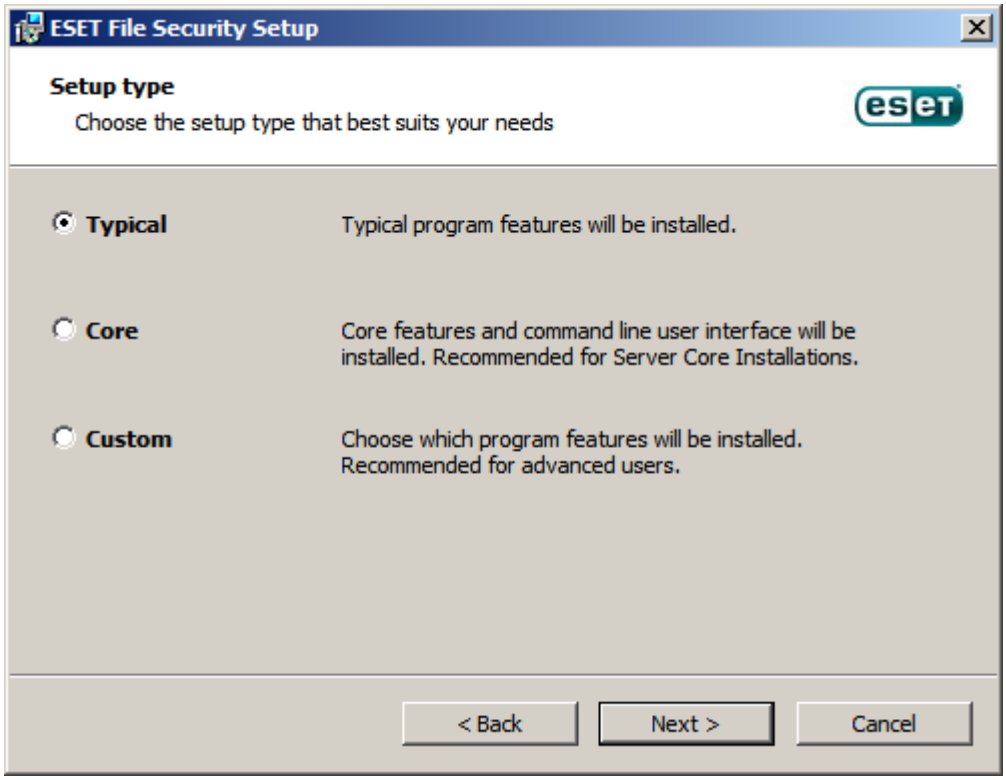
Полная

Установка всех компонентов ESET Server Security. Это рекомендуемый тип установки, доступный для ОС Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials and 2019 Essentials.



Обычная

Установка рекомендуемых компонентов ESET Server Security. Этот способ установки доступен для 2008 R2 SP1 и 2011.



Базовая

Этот тип установки предназначен для выпусков Windows Server Core. Этапы установки такие же, как и во время полной установки, но устанавливаются только основные компоненты и интерфейс командной строки. Хотя установка основных компонентов предназначена главным образом для выпусков Windows Server Core, ее при необходимости можно использовать и в обычной системе Windows Server. В таком режиме продукты ESET по обеспечению безопасности устанавливаются без графического пользовательского интерфейса. Это означает, что при работе с ESET Server Security можно использовать только командную строку. Более подробную информацию и сведения о других особых параметрах см. в разделе Установка из командной строки.

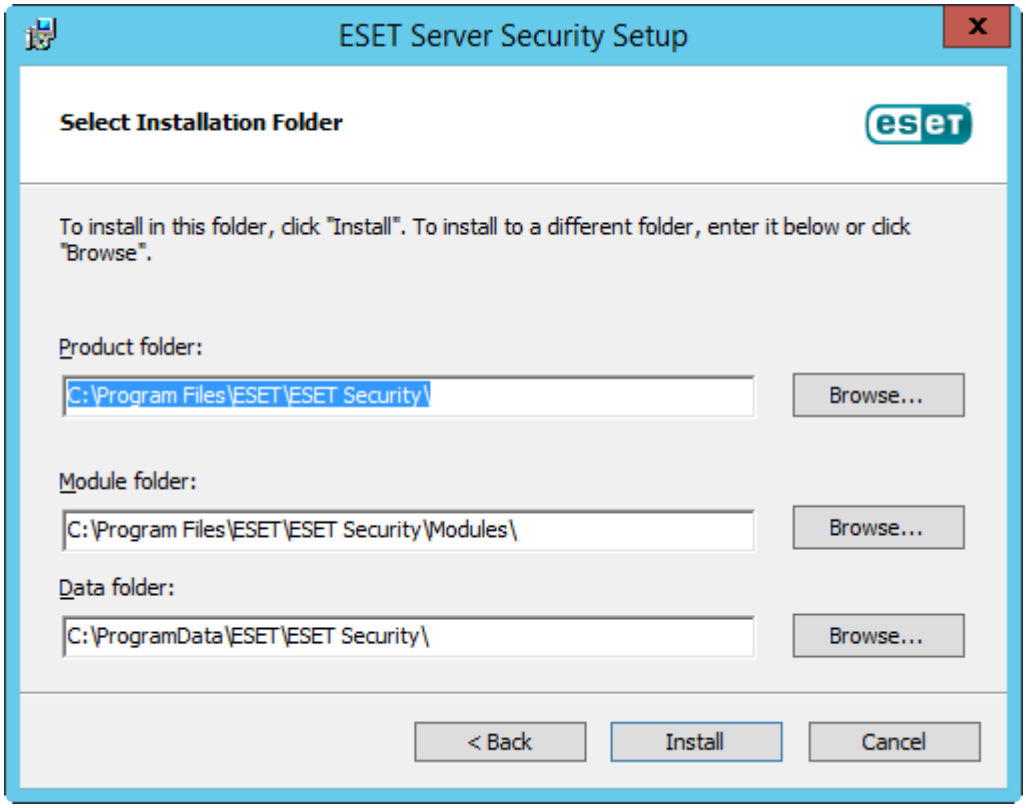
Чтобы выполнить установку основных компонентов из командной строки, используйте следующий пример команды:
`msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base`

Выборочная

Позволяет выбрать компоненты ESET Server Security, которые будут установлены в системе. Перед началом установки отобразится список модулей и компонентов продукта. Такая возможность полезна, когда нужно установить только необходимые компоненты ESET Server Security.

В ОС Windows Server 2008 R2 SP1 установка компонента **Защита сети** отключена по умолчанию (**обычная** установка). Если нужно установить этот компонент, выберите тип установки **Выборочная**.

5. Вам будет предложено выбрать расположение, в которое нужно установить ESET Server Security. По умолчанию программа устанавливается в папку *C:\Program Files\ESET\ESET Server Security*. Нажмите кнопку **Обзор**, чтобы изменить папку (не рекомендуется).

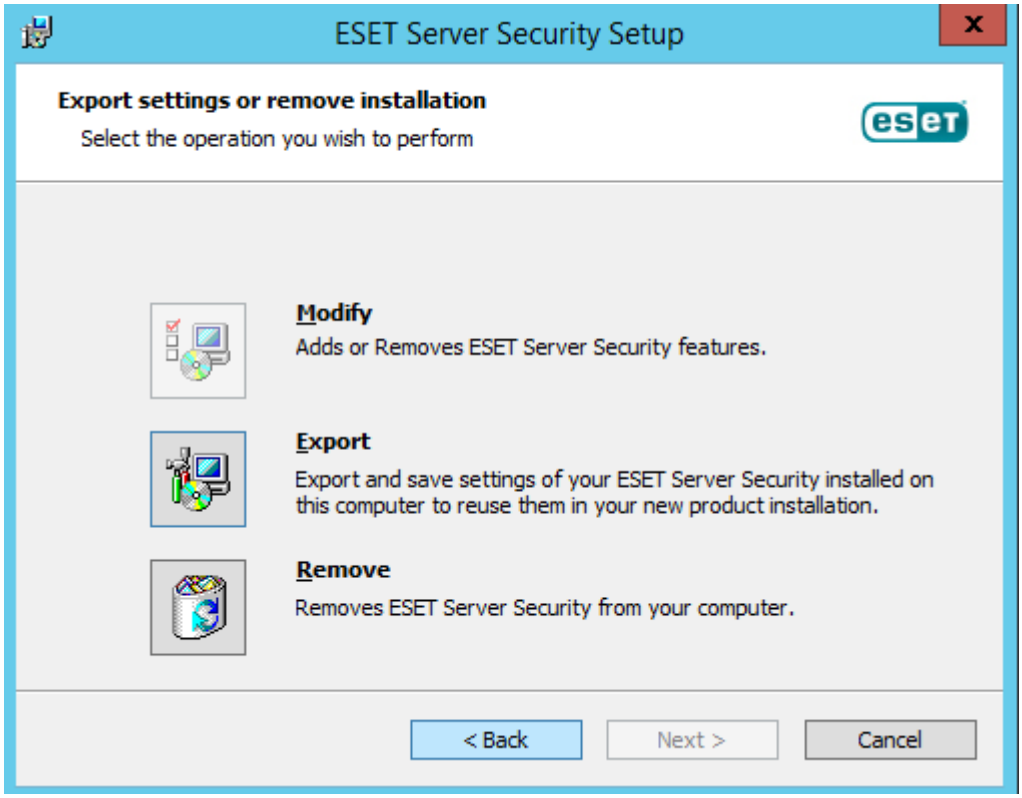


6. Щелкните **Установить**, чтобы начать установку. По завершении установки запустится графический интерфейс ESET и отобразится значок в области уведомлений Windows.

Экспорт настроек или удаление установки

Вы можете экспортировать и сохранить настройки или полностью удалить установку. Чтобы сделать это, нужно запустить установочный пакет с расширением .msi, который использовался при первой установке, или перейти в раздел **Программы и компоненты** (доступен в панели управления Windows), щелкнуть ESET Server Security правой кнопкой мыши и выбрать **Изменить**.

Вы можете **экспортировать** настройки ESET Server Security или полностью **удалить** ESET Server Security.



Автоматическая установка/установка без участия пользователя

Выполните следующую команду, чтобы завершить установку из командной строки: `msiexec /i <packagename> /qn /l*xv msi.log`

> ℹ В Windows Server 2008 R2 SP1 компонент **Защита сети** не устанавливается.

Если у вас возникли проблемы с установкой или вам нужно убедиться, что установка выполнена успешно, с помощью средства просмотра событий Windows проверьте **журнал приложения** (найдите записи из источника MsiInstaller).

> ✓ **Полная установка** в 64-разрядной системе:
> `msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^ DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula`

> ✓ Установка программы на **выбранном языке** (немецкий):
> `msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^ DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^ SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de`
> Дополнительные сведения и список кодов языков см. в подразделе **Параметры языка** в разделе Установка из командной строки.

По завершении установки запустится графический интерфейс ESET и отобразится значок в области уведомлений Windows.

При указании значений для параметра REINSTALL необходимо перечислить оставшиеся неиспользуемые компоненты в виде значений ADDLOCAL или REMOVE. Чтобы установка из командной строки выполнилась надлежащим образом, необходимо указать все компоненты в виде значений параметров REINSTALL, ADDLOCAL и REMOVE. Если не использовать параметр REINSTALL, добавление или удаление компонентов может завершиться ошибкой.
Полный список функций см. в разделе Установка из командной строки.

Полное удаление из 64-разрядной системы:
`msiexec /x efsw_nt64.msi /qn /l*xv msi.log`

После успешного удаления сервер автоматически перезапустится.

Установка из командной строки

Все приведенные ниже параметры должны использоваться только с **сокращенным**, **основным** и **отсутствующим** уровнями интерфейса. Сведения о версии **msiexec**, используемой для соответствующих параметров командной строки, см. в этой документации .

Поддерживаемые параметры:

APPDIR=<path>

- путь — допустимый путь к каталогу
- Каталог установки приложения.
- Например, `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- путь — допустимый путь к каталогу
- Каталог установки данных приложения.

MODULEDIR=<path>

- путь — допустимый путь к каталогу
- Каталог установки модуля.

ADDLOCAL=<list>

- Установка компонентов — список необязательных функций, которые нужно установить локально.
- Использование с пакетами ESET `.msi`: `efsw_nt64.msi /qn ADDLOCAL=<list>`
- Дополнительные сведения о свойстве ADDLOCAL см. на странице https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- Список ADDLOCAL — это разделенный запятыми список всех функций, которые

устанавливаются.

• Если выбрать компонент, который будет установлен, в список необходимо явно добавить полный путь (все родительские компоненты).

REMOVE=<list>

• Установка компонентов — родительский компонент, который вы не хотите устанавливать локально.

• Использование с пакетами ESET `.msi`: `efsw_nt64.msi /qn REMOVE=<list>`

• Дополнительные сведения о свойстве `REMOVE` см. на странице https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove

• Список `REMOVE` — это разделенный запятыми список родительских компонентов, которые не будут установлены (либо будут удалены, если они уже установлены).

• Достаточно указать только родительский компонент. Не требуется в явном виде включать в список все дочерние компоненты.

ADDEXCLUDE=<list>

• Список `ADDEXCLUDE` — это разделенный запятыми список имен всех компонентов, которые не устанавливаются.

• Если выбрать компонент, который не нужно устанавливать, в список необходимо явно добавить полный путь (например, все вложенные компоненты) и связанные невидимые компоненты.

• Использование с пакетами ESET `.msi`: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> Свойство `ADDEXCLUDE` нельзя использовать вместе со свойством `ADDLOCAL`.

Наличие функции

• **Обязательный**: компонент устанавливается всегда.

• **Необязательный**: компонент можно не выбирать для установки.

• **Невидимый**: логический компонент, который обязательно устанавливается, чтобы другие компоненты работали надлежащим образом.

Список компонентов ESET Server Security:

> Названия всех компонентов чувствительны к регистру, например `RealtimeProtection` — это не то же самое, что `REALTIMEPROTECTION`.

Имя функции	Наличие функции
`SERVER`	Обязательная
`RealtimeProtection`	Обязательная
`WMIProvider`	Обязательная

Имя функции	Наличие функции
HIPS	Обязательная
Updater	Обязательная
eShell	Обязательная
UpdateMirror	Обязательная
DeviceControl	Необязательная
DocumentProtection	Необязательная
WebAndEmail	Необязательная
ProtocolFiltering	Невидимая
NetworkProtection	Необязательная
IdsAndBotnetProtection	Необязательная
Rmm	Необязательная
WebAccessProtection	Необязательная
EmailClientProtection	Необязательная
MailPlugins	Невидимая
Cluster	Необязательная
_Base	Обязательная
eula	Обязательная
ShellExt	Необязательная
_FeaturesCore	Обязательная
GraphicUserInterface	Необязательная
SysInspector	Необязательная
SysRescue	Необязательная
EnterpriseInspector	Необязательная

Если необходимо удалить какой-либо из следующих компонентов, удалите всю группу, указав каждый компонент из группы. В противном случае компонент не будет удален. Вот две группы (каждая строка представляет одну группу):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

Исключение раздела **NetworkProtection** (вместе с дочерними компонентами) из установки с помощью параметра `REMOVE` и с указанием только родительского компонента:
`msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection`
Также можно использовать параметр `ADDEXCLUDE`, но при этом также следует указать все дочерние компоненты:
`msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^ ProtocolFiltering,MailPlugins,EmailClientProtection`

Пример базовой установки:
`msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm`

Если вы хотите, чтобы после установки ESET Server Security был автоматически настроен, вы можете указать основные параметры конфигурации в команде установки.

Установите ESET Server Security и отключите ESET LiveGrid®:
`msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0`

Список свойств конфигурации:

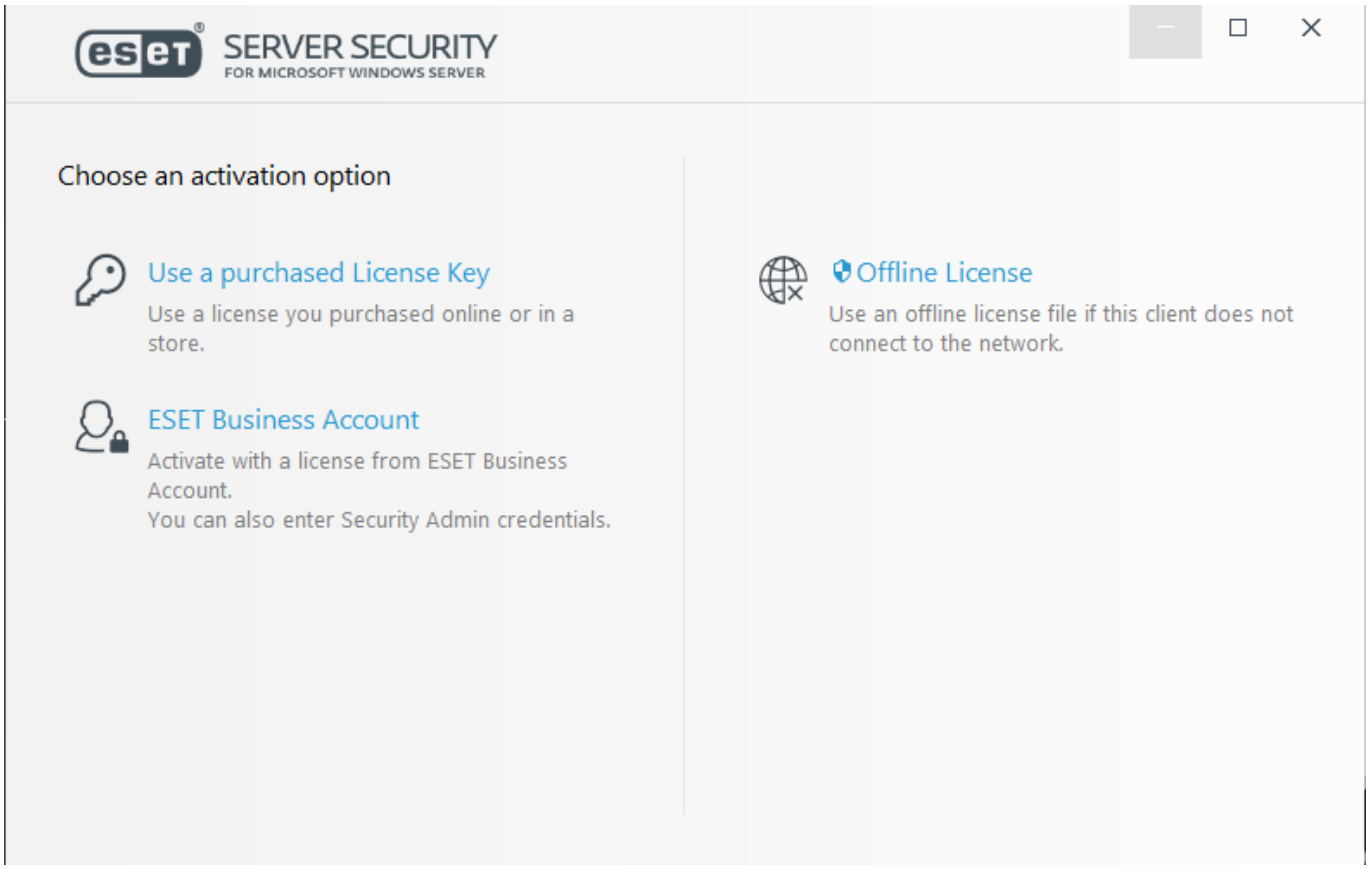
Переключение	Значение
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 — отключено, 1 — включено.
CFG_LIVEGRID_ENABLED=1/0	0 — отключено, 1 — включено.
FIRSTSCAN_ENABLE=1/0	0 — отключить, 1 — включить;
CFG_PROXY_ENABLED=0/1	0 — отключено, 1 — включено.
CFG_PROXY_ADDRESS=<ip>	IP-адрес прокси-сервера.
CFG_PROXY_PORT=<port>	Номер порта прокси-сервера.
CFG_PROXY_USERNAME=<user>	Имя пользователя для проверки подлинности
CFG_PROXY_PASSWORD=<pass>	Пароль для проверки подлинности.

Параметры языка: Язык продукта (необходимо указать оба параметра)

Переключение	Значение
PRODUCT_LANG=	Десятичное значение LCID (код языка), например 1033 для English - United States. См. список кодов языков.
PRODUCT_LANG_CODE=	Строка LCID (язык и региональные параметры) строчными буквами, например en-us для English - United States. См. список кодов языков.

Активация программы

По завершении установки вам будет предложено активировать установленный продукт.



Для активации ESET Server Security можно воспользоваться любым из перечисленных ниже способов.

Введите лицензионный ключ

Уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.

ESET Business Account

Используйте этот параметр, если вы зарегистрированы и у вас есть учетная запись ESET Business Account (EBA) , в которую импортирована лицензия ESET Server Security. Также можно указать учетные данные администратора безопасности, используемые на портале ESET License Administrator .

Автономный файл лицензии

Автоматически создаваемый файл со сведениями о лицензии, который передается в продукт ESET. Автономный файл лицензии создается на портале лицензирования и используется в средах, в которых приложение не может подключиться к центру лицензирования.

Щелкните **Активировать позже** для ESET PROTECT, если компьютер находится в управляемой сети и администратор выполнит удаленную активацию через ESET PROTECT. Этот параметр можно использовать и в тех случаях, когда клиент нужно активировать позже.

Чтобы управлять сведениями о лицензии, в главном окне программы последовательно щелкните элементы **Справка и поддержка** > **Управление лицензией**. Отобразится открытый идентификатор лицензии, используемый компанией ESET для идентификации продукта и лицензии. Имя пользователя, с помощью которого зарегистрирован компьютер, можно найти в разделе О программе (в области уведомлений щелкните значок правой кнопкой мыши).

После активации ESET Server Security на странице Мониторинг откроется главное окно программы, в котором отобразится ваше текущее состояние. Возможно, в самом начале нужно будет уделить продукту немного времени: к примеру, вам будет предложено присоединиться к ESET LiveGrid®.

Кроме того, в главном окне программы отображаются уведомления о таких элементах, как обновления системы (обновления Windows) и обновления модуля обнаружения. Когда все вопросы, требующие внимания, решены, состояние мониторинга становится зеленым и для него отображается значение **Вы защищены**.

Активацию продукта также можно выполнить, последовательно щелкнув в главном меню элементы **Справка и поддержка** > **Активировать продукт** или состояние **Мониторинг** > **Продукт не активирован**.

> Используя предоставленные администратором лицензии, приложение ESET PROTECT может активировать клиентские компьютеры в автоматическом режиме.

ESET Business Account

В ESET Business Account можно управлять несколькими лицензиями. Если у вас нет учетной записи ESET Business Account, щелкните Создать учетную запись, после чего откроется портал ESET Business Account, на котором можно ее зарегистрировать.

> ℹ Дополнительные сведения см. в интернет-справке ESET Business Account.

Если используете учетные данные администратора безопасности и забыли пароль, щелкните **Восстановление пароля**, и система перенаправит вас на портал ESET License Administrator. Введите адрес электронной почты и щелкните Передать для подтверждения. Вам будет отправлено сообщение с указаниями по сбросу пароля.

Активация выполнена

Продукт ESET Server Security успешно активирован. Теперь ESET Server Security будет регулярно загружать обновления, следить за безопасностью компьютера и устранять все известные угрозы. Чтобы завершить активацию продукта, нажмите кнопку **Готово**.

Сбой активации

Не удалось выполнить активацию ESET Server Security. Проверьте, правильно ли введен **лицензионный ключ** либо вложена **офлайн-лицения**. Если у вас есть другая **офлайн-лицензия**, введите ее. Чтобы проверить введенный лицензионный ключ, щелкните элемент **Перепроверить лицензионный ключ** или **Ввести другую лицензию**.

Если вам не удается выполнить активацию, воспользуйтесь мастером устранения неполадок активации.

Лицензия

Отобразится запрос, и нужно будет выбрать лицензию, связанную с вашей учетной записью, которая будет использоваться для ESET Server Security. Щелкните **Продолжить**, чтобы продолжить активацию.

Обновление до последней версии

Новые версии ESET Server Security выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Способы обновления:

Удаление/установка

Удаление старой версии перед установкой новой. Загрузите последнюю версию ESET Server Security. Экспортируйте параметры из используемой версии ESET Server Security, чтобы сохранить конфигурацию. Удалите ESET Server Security и перезапустите сервер. Выполните новую установку

с помощью загруженного установщика. Импортируйте параметры, чтобы загрузить конфигурацию. Эта процедура рекомендуется в том случае, если ESET Server Security работает на одном сервере.

Поверх

Способ обновления, не требующий удаления имеющейся версии, при котором установка новой версии ESET Server Security выполняется поверх старой.

> Обязательное условие: на вашем сервере не должно быть ожидающих обновлений Windows, а также ожидающего перезапуска в связи с обновлениями Windows или любыми другими причинами. Если вы попытаетесь выполнить обновление на месте при наличии ожидающих обновлений Windows или перезапуске, имеющаяся версия ESET Server Security может быть удалена некорректно. Кроме того, если после этого вы решите удалить старую версию ESET Server Security вручную, могут возникнуть другие проблемы.

> В процессе обновления программы ESET Server Security потребуется перезагрузка сервера.

Удаленные

Для использования в крупных сетевых средах под управлением ESET PROTECT. По сути, это способ прямого обновления, который выполняется удаленно. Его удобно использовать в тех случаях, когда ESET Server Security работает на нескольких серверах.

С помощью мастера кластеров ESET

Также можно использовать для обновления. Этот способ рекомендуется, если программа ESET Server Security используется как минимум на двух серверах. По сути, это способ обновления на месте, который выполняется через кластер ESET. Кроме того, после обновления можно продолжить использование всех возможностей кластера ESET.

> По завершении обновления ESET Server Security рекомендуется проверить все параметры и убедиться, что они настроены правильно и в соответствии с вашими потребностями.

Обновление с помощью ESET PROTECT

ESET PROTECT позволяет обновлять несколько серверов, на которых работают более ранние версии программы ESET Server Security. Преимуществом данного способа является возможность одновременного обновления большого количества серверов, при котором все экземпляры программы ESET Server Security имеют одинаковые настройки (если это необходимо).

Процедура требует выполнения следующих действий:

- **Обновите первый сервер** вручную путем установки последней версии программы ESET Server Security поверх имеющейся версии, чтобы полностью сохранить конфигурацию, в том числе правила, многочисленные «белые» и «черные» списки и т. д. Это действие выполняется локально на сервере, на котором работает программа ESET Server Security.

- **Запросите конфигурацию** программы ESET Server Security, обновленной до версии 7.x, и преобразуйте ее в политику в ESET PROTECT. Впоследствии эта политика будет применена ко всем обновляемым серверам. Этот и последующие этапы выполняются удаленно в ESET

PROTECT.

• Запустите задачу **удаления программного обеспечения** на всех серверах, на которых работает старая версия ESET Server Security.

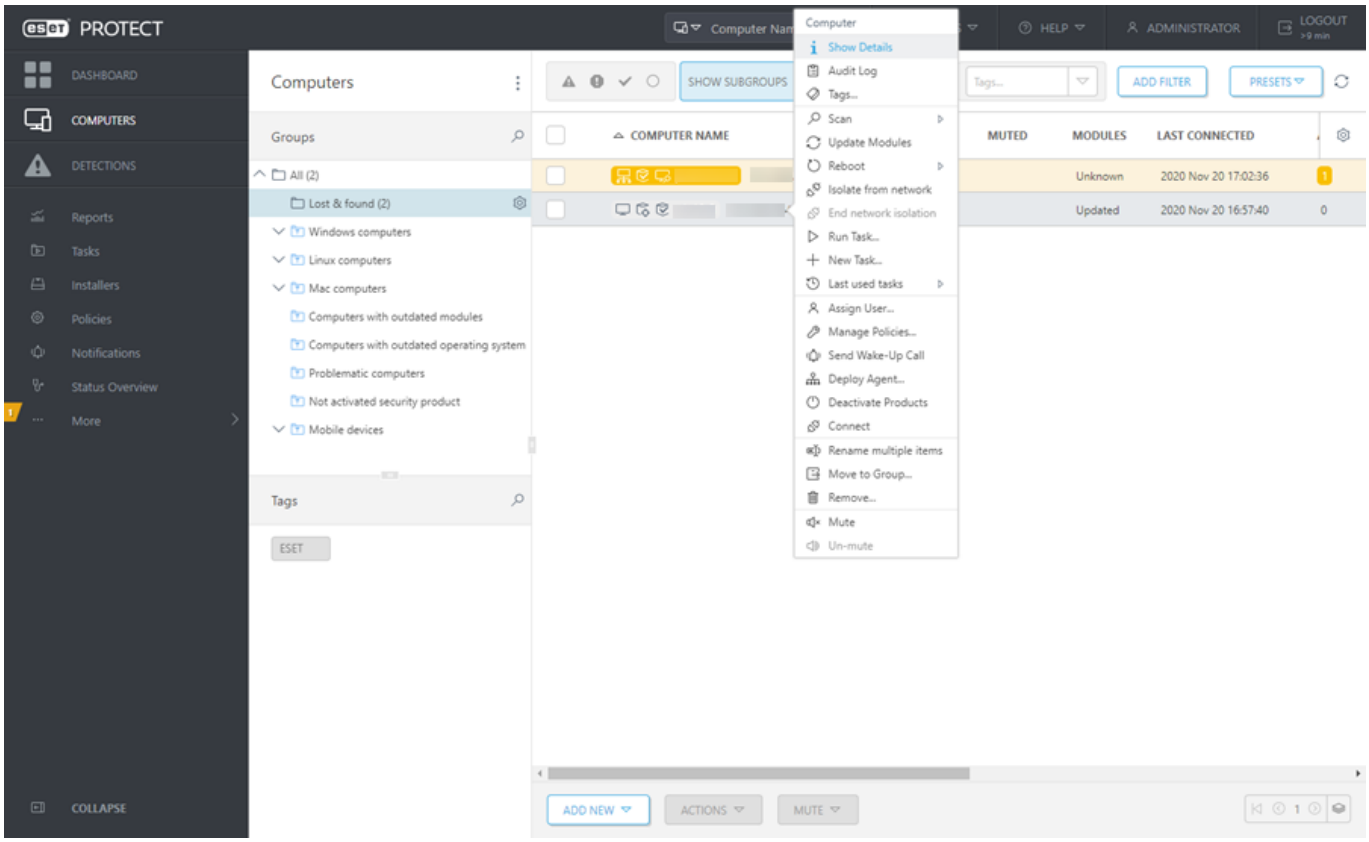
• Запустите задачу **установки программного обеспечения** на всех серверах, на которых должна работать новая версия ESET Server Security.

• **Назначьте политику конфигурации** для всех серверов, на которых работает новая версия программы ESET Server Security.

Пошаговая процедура:

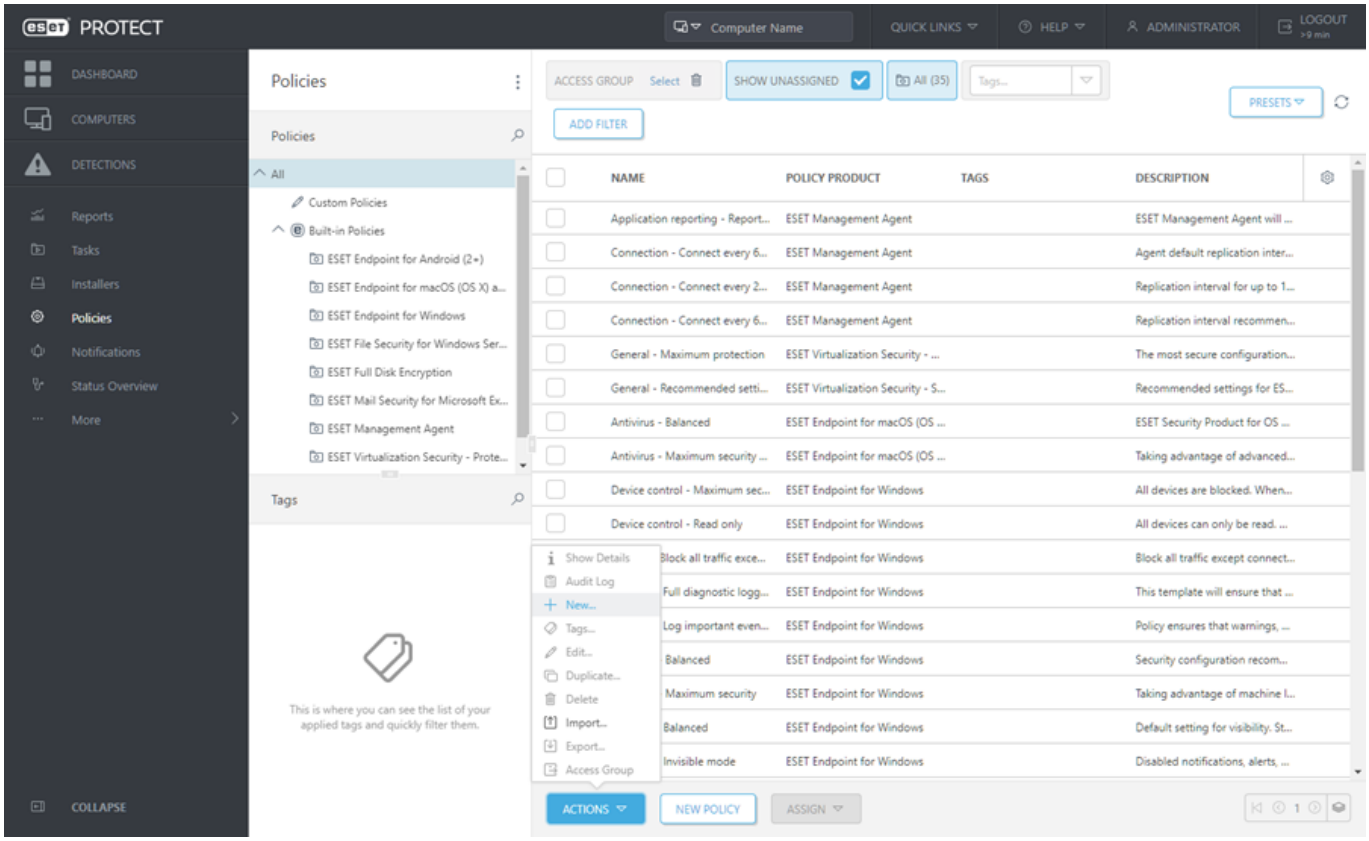
1. Войдите на один из серверов, на котором работает программа ESET Server Security, и обновите ее, загрузив и установив последнюю версию поверх существующей. Следуйте инструкциям по обычной установке. При установке исходная конфигурация старой версии программы ESET Server Security будет сохранена. При установке исходная конфигурация старой версии программы ESET Server Security будет сохранена.

2. Откройте ESET PROTECTWeb Console, выберите клиентский компьютер в статической или динамической группе, а затем щелкните **Показать подробности**.



3. Перейдите на вкладку Конфигурация и нажмите кнопку **Запросить конфигурацию**, чтобы собрать всю конфигурацию управляемого продукта. Получение конфигурации может занять некоторое время. После появления в списке последней конфигурации щелкните **Программа по обеспечению безопасности** и выберите **Открыть конфигурацию**.

4. Создайте политику конфигурации, нажав кнопку **Преобразовать в политику**. Укажите **имя** для новой политики и нажмите кнопку **Готово**.



5. Перейдите в раздел **Клиентские задачи** и выберите задачу Удаление программного обеспечения. При создании задачи по удалению рекомендуем перезагрузить сервер после удаления. Чтобы сделать это, установите флажок **Выполнить автоматическую перезагрузку при необходимости**. Создав задачу, добавьте все целевые компьютеры, на которых необходимо выполнить удаление.

6. Убедитесь, что программа ESET Server Security удалена на всех целевых компьютерах.

7. Создайте задачу Установка программного обеспечения, чтобы установить новую версию ESET Server Security на все целевые компьютеры.

8. **Назначьте политику конфигурации** для всех серверов, на которых работает ESET Server Security (по возможности сделайте это для группы серверов).

Обновление с помощью кластера ESET

Создание кластера ESET позволяет обновить несколько серверов, на которых установлены более старые версии программы ESET Server Security. Этот способ является альтернативой обновлению с помощью ESET PROTECT. Если в вашей среде есть как минимум два сервера с ESET Server Security, рекомендуется использовать способ с применением кластера ESET.

Другое преимущество этого способа обновления заключается в возможности дальнейшего использования кластера ESET. Это позволит синхронизировать конфигурацию программы ESET Server Security на всех вовлеченных узлах.

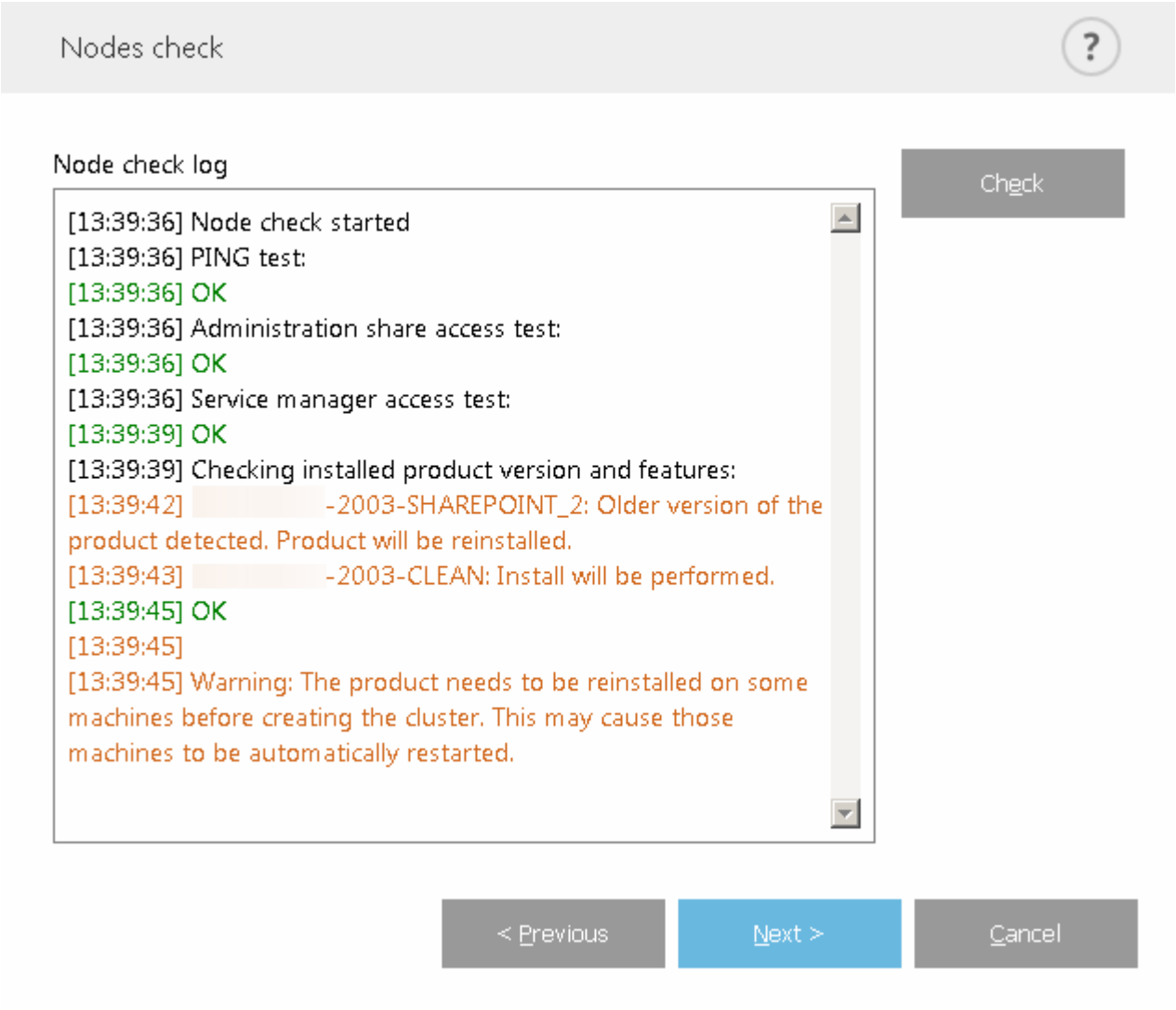
Чтобы выполнить обновление с помощью этого способа, выполните следующие действия.

1. Войдите на один из серверов, на которых работает программа ESET Server Security, и

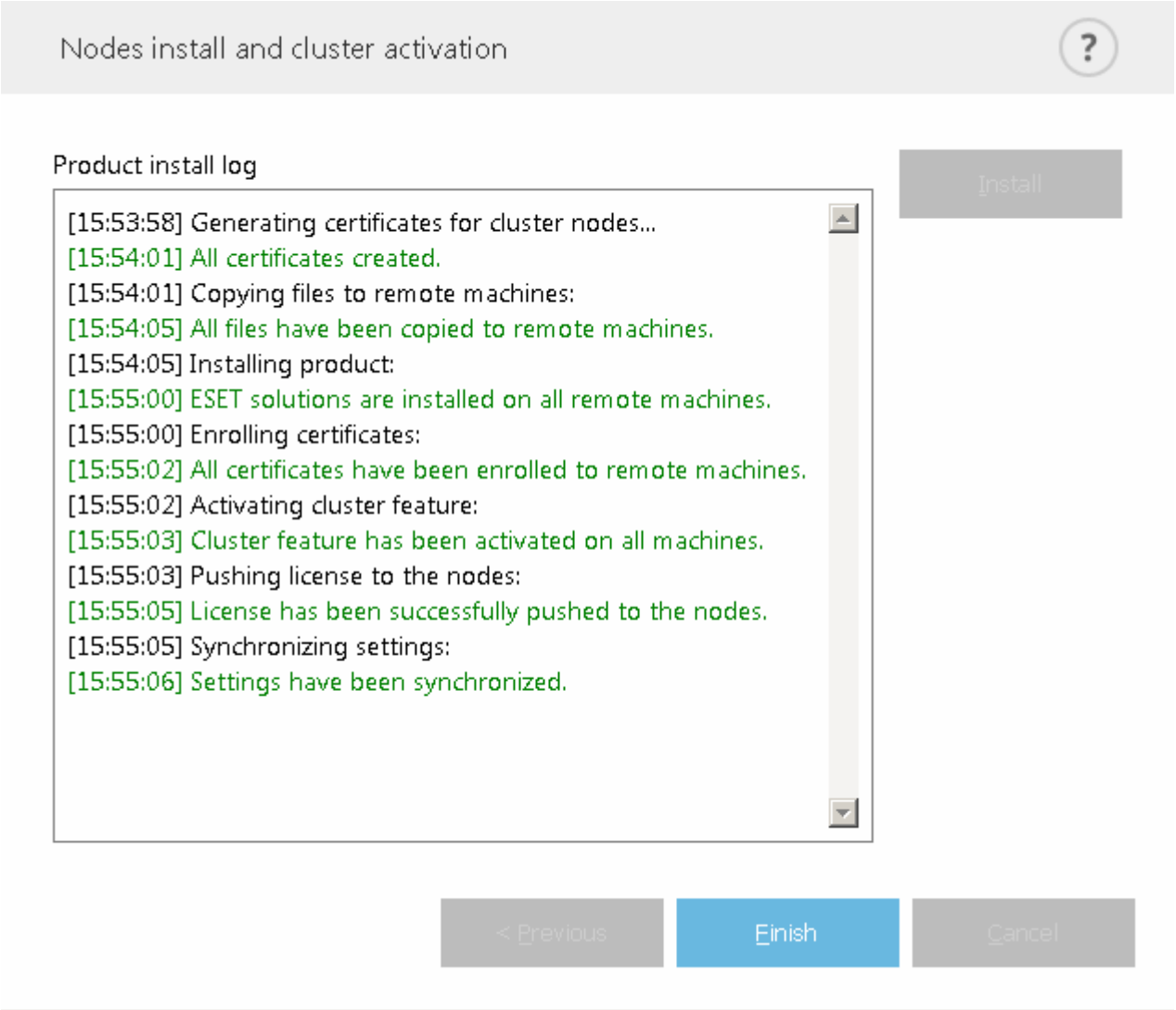
обновите ее, загрузив и установив новую версию поверх существующей. Следуйте инструкциям по обычной установке. При установке исходная конфигурация старой версии программы ESET Server Security будет полностью сохранена.

2. Запустите мастер кластеров ESET и добавьте узлы кластера (серверы, на которых необходимо обновить ESET Server Security). При необходимости можно добавить другие серверы, на которых еще не установлена программа ESET Server Security (на них будет выполнена установка). При указании имени кластера и типа установки рекомендуется оставить значения по умолчанию (убедитесь, что установлен флажок **Передать лицензию на узлы без активированного продукта**).

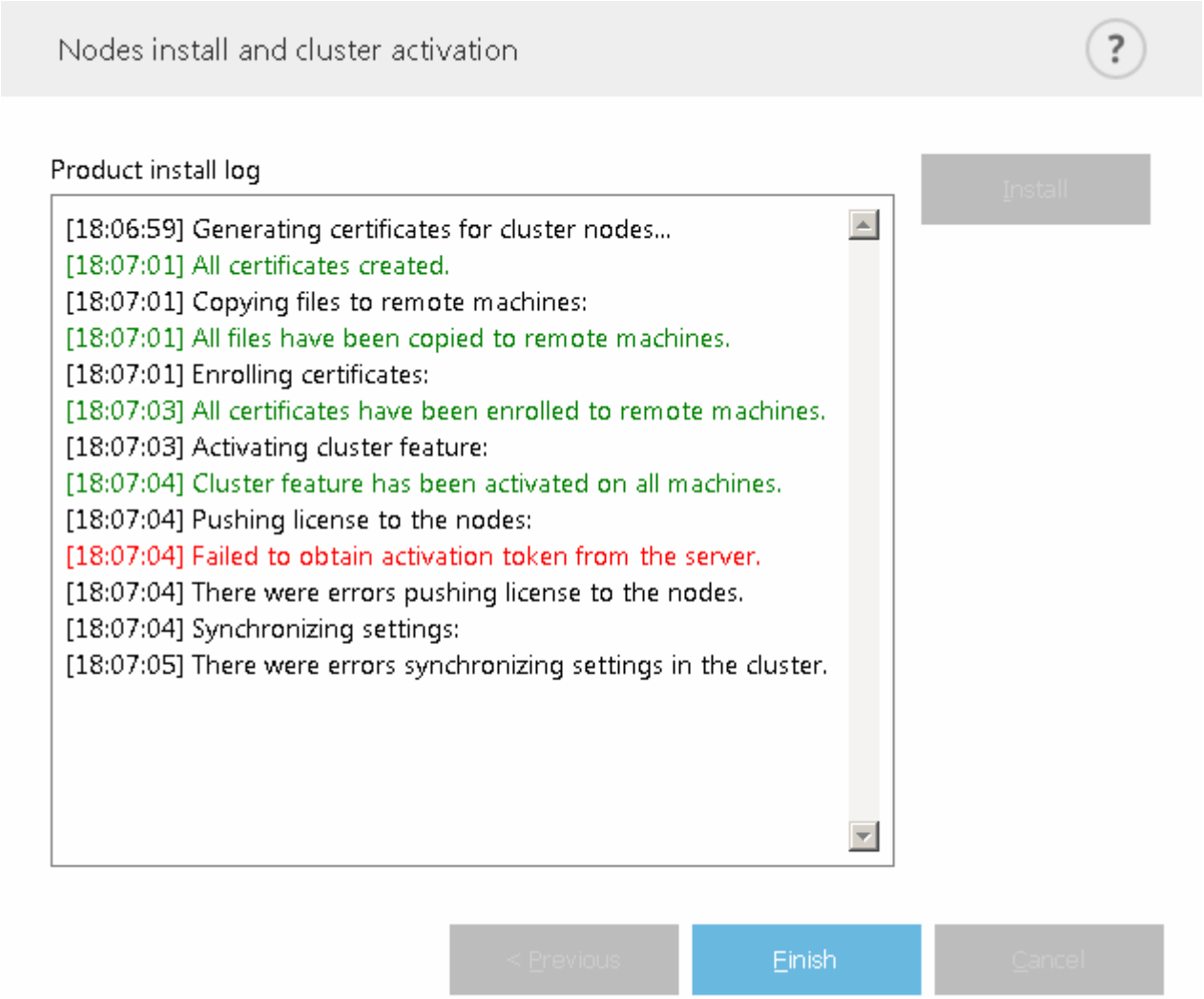
3. Просмотрите экран **Журнал проверки узлов**. На нем будет отображаться список серверов с более ранними версиями продукта с пометкой об обновлении (переустановке). Программа ESET Server Security будет также установлена на все добавленные серверы, на которых еще нет ESET Server Security.



4. На экране **Установка узлов и активация кластера** отобразится ход установки. В случае успешного завершения установки результат должен выглядеть следующим образом:



В случае неправильной настройки сети или службы DNS может отобразиться следующее сообщение об ошибке: **Не удалось получить от сервера маркер активации**. Попробуйте снова запустить мастер кластеров ESET. В результате этого старый кластер будет удален, а вместо него будет создан новый (без необходимости переустановки программы), и в этот раз активация должна завершиться успешно. Если это не поможет, проверьте параметры сети и службы DNS.



Установка в кластерной среде

ESET Server Security можно развернуть в кластерной среде (например, в отказоустойчивом кластере). Рекомендуем установить ESET Server Security на активном узле, а затем распределить установку по пассивным узлам с помощью функции Кластер ESET решения ESET Server Security.

Помимо установки, кластер ESET выполняет репликацию конфигурации ESET Server Security, обеспечивая согласованность между узлами кластера, необходимыми для корректной работы.

Сервер терминалов

Если приложение ESET Server Security устанавливается на сервере Windows Server, который выступает в качестве сервера терминалов, полезно будет отключить главное окно программы ESET Server Security, чтобы предотвратить его запуск при каждой авторизации пользователя. Конкретные инструкции по отключению приводятся в главе Отключение графического интерфейса пользователя на сервере терминалов.

Обновления для обеспечения безопасности и стабильности

Обновление решения ESET Server Security является важнейшим процессом для обеспечения полной защиты от вредоносного кода. Каждая новая версия ESET Server Security содержит множество улучшений и исправлений ошибок. Настоятельно рекомендуем периодически обновлять решение ESET Server Security, чтобы защититься от уязвимостей системы безопасности и угроз.

Решение ESET Server Security, как и любой другой продукт ESET, проходит определенные стадии жизненного цикла. Дополнительные сведения можно найти в разделе Политика касательно окончания срока службы (бизнес-продукты) .

Для получения дополнительных сведений об изменениях ознакомьтесь со следующей статьей базы знаний ESET ESET Server Security.

> Автоматическое обновление обеспечивает максимальную безопасность и стабильность вашего продукта. Обновления для обеспечения безопасности и стабильности отключить нельзя.

Начало работы

Следующая часть должна помочь вам начать работу с ESET Server Security.

Мониторинг

Позволяет быстро просмотреть текущее состояние ESET Server Security. Вы сможете сразу увидеть, есть ли какие-либо проблемы, требующие вашего внимания.

Управление через ESET PROTECT

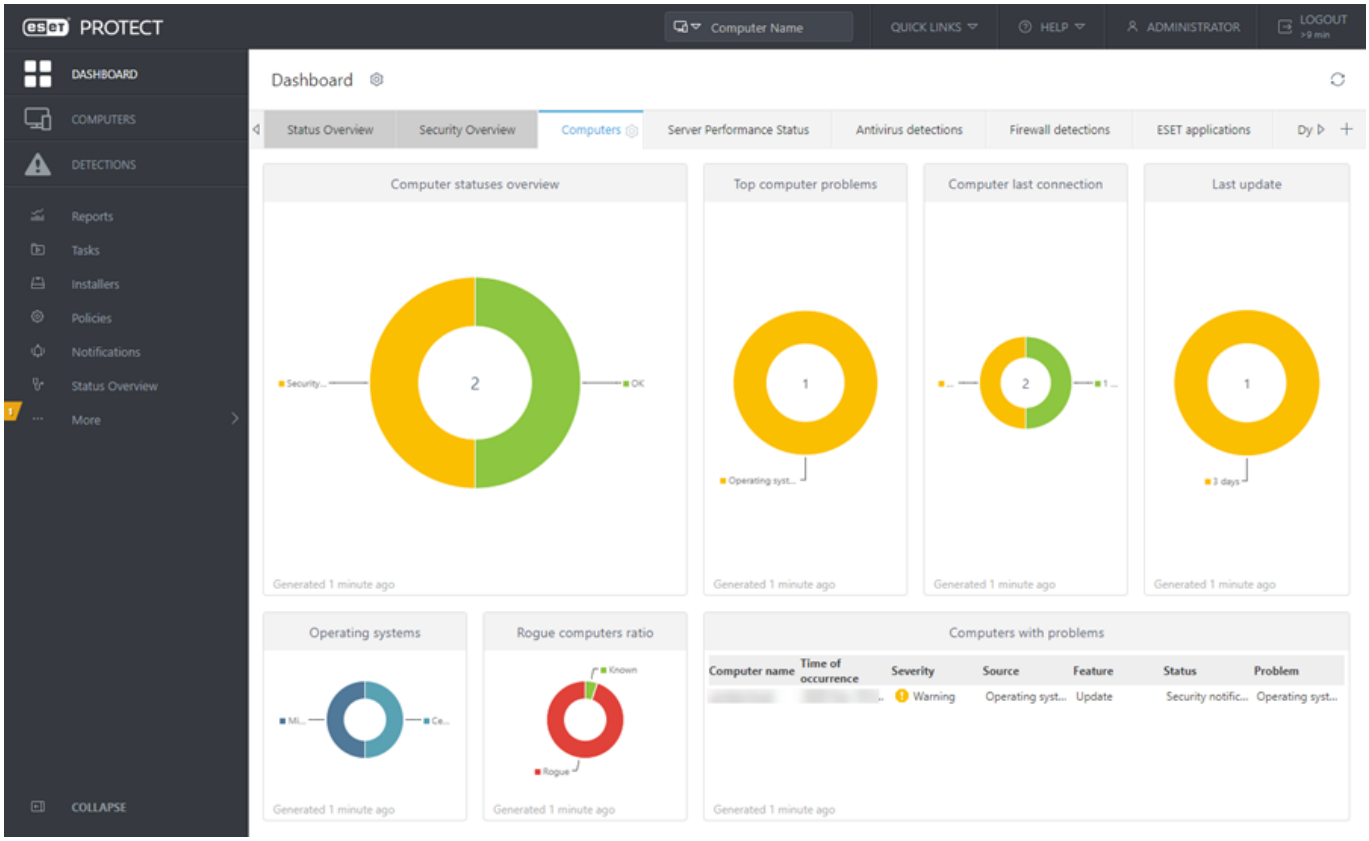
Для дистанционного управления ESET PROTECT можно использовать ESET Server Security.

Управление через ESET PROTECT

ESET PROTECT — это приложение, позволяющее осуществлять централизованное управление продуктами ESET, установленными в сетевой среде. Система управления задачами ESET PROTECT позволяет установить решения ESET для обеспечения безопасности на удаленные компьютеры и быстро реагировать на новые проблемы и угрозы.

Система ESET PROTECT не предоставляет защиту от вредоносного кода — чтобы обеспечить защиту, на каждом клиенте требуется установить отдельное решение ESET для обеспечения безопасности.

В решениях ESET для обеспечения безопасности предусмотрена поддержка сетей, использующих несколько платформ различных типов. Ваша сеть может состоять из комбинации текущих операционных систем Microsoft, Linux, Mac OS и мобильных операционных систем.



Дополнительные сведения о ESET PROTECT см. в интернет-справке ESET PROTECT.

Мониторинг

Состояние защиты, отображаемое в разделе **Мониторинг**, информирует о текущем уровне защиты компьютера. В основном окне отображается сводная информация о работе ESET Server Security.

Зеленый значок **Вы защищены** означает, что обеспечивается максимальная степень защиты.

Красный значок указывает на наличие критических проблем, из-за которых максимальная степень защиты компьютера не обеспечивается. Список возможных состояний защиты см. в разделе Состояние.

Оранжевый значок указывает на то, что продукт ESET требует вашего внимания в связи с некритичной проблемой.

Модули, работающие правильно, обозначаются зеленым флажком. Модули, работающие неправильно, обозначаются красным восклицательным знаком или оранжевым значком уведомления. В верхней части окна выводятся дополнительные сведения о модуле.

Кроме того, предлагается решение проблемы. Чтобы изменить состояние отдельного модуля, выберите в главном меню пункт Настройка и щелкните нужный модуль.

На странице «Мониторинг» также содержится информация о вашей системе, включая следующее:

- **Версия продукта** — номер версии приложения ESET Server Security.
- **Имя сервера** — имя хоста или полное доменное имя компьютера.
- **Система** — информация об операционной системе.
- **Компьютер** — сведения об оборудовании.
- **Время работы сервера** — информация о том, сколько система работает без остановки на данный момент. По сути, это антоним слова «простой».

Если предложенные варианты решений не позволяют устранить проблему, выберите пункт **Справка и поддержка**, чтобы получить доступ к файлам справки или воспользоваться поиском по базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте запрос в службу технической поддержки ESET. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

Состояние

В основном окне отображается сводная информация о работе ESET Server Security, а также подробные сведения о системе. Как правило, когда нет никаких проблем, отображается зеленый значок состояния защиты . Но при определенных условиях это состояние может измениться. В случае возникновения одной из следующих ситуаций цвет значка состояния защиты изменяется на оранжевый или красный и отображается предупреждение:

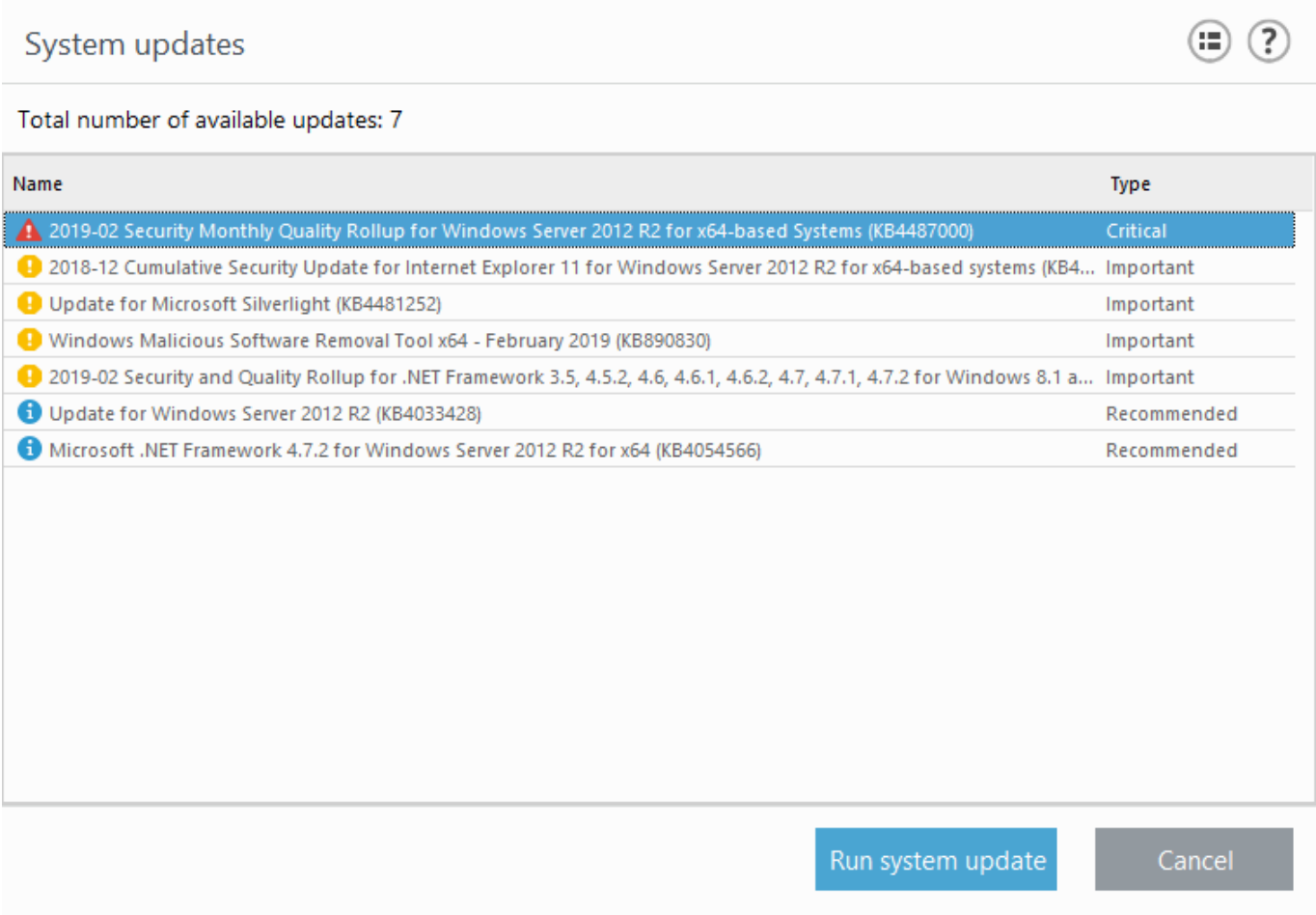
Предупреждение	Сведения о предупреждении
Не настроено обнаружение потенциально нежелательных приложений	Потенциально нежелательное приложение — это программа, которая содержит рекламу, устанавливает панели инструментов или выполняет другие сомнительные функции. В некоторых ситуациях может показаться, что преимущества такого приложения перевешивают риски.
Защита файловой системы в реальном времени приостановлена	В главном окне программы на вкладке Мониторинг щелкните **Включить защиту в режиме реального времени** или на вкладке Настройка повторно включите параметр **Защита файловой системы в режиме реального времени**.
Защита от фишинга не работает	Этот компонент не работает, так как не активны другие нужные модули программы.
Система ESET LiveGrid® отключена	Возникает оповещение о проблеме, если система ESET LiveGrid® отключена в **расширенных параметрах**.
Фильтрация протоколов отключена	Щелкните элемент Включить фильтрацию протоколов, чтобы повторно включить эту функцию.
Существует более новая версия операционной системы	В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки.
Защита вашего устройства скоро прекратится	Щелкните См. варианты действий для отображения сведений о том, как обновить вашу версию Microsoft Windows. Если вы используете Microsoft Windows Server 2008 R2 SP1 или Microsoft Windows Small Business Server 2011 SP1, убедитесь, что система совместима с SHA-2. Примените исправления в соответствии с конкретной версией вашей операционной системы.
Режим презентации включен	Вывод всех всплывающих окон на экран будет отключен, а запланированные задачи приостановлены.
Защита от сетевых атак (IDS) приостановлена	Щелкните элемент Включить защиту от сетевых атак (IDS), чтобы повторно включить эту функцию.
Защита от ботнетов приостановлена	Щелкните элемент Включить защиту от ботнетов, чтобы повторно включить эту функцию.
Защита доступа в Интернет приостановлена	В главном окне программы на вкладке Мониторинг щелкните **Включить защиту доступа в Интернет** или на панели Настройка повторно включите параметр **Защита доступа в Интернет**.
Контроль устройств приостановлен	Щелкните элемент Включить контроль устройств, чтобы повторно включить эту функцию.
«Продукт не активирован» или «Срок действия лицензии истек»	Об этих проблемах свидетельствует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Для продления лицензии следуйте инструкциям в окне предупреждения.

Предупреждение	Сведения о предупреждении
Действует переопределение политики	Конфигурация, заданная политикой, временно переопределена, возможно, до завершения устранения неполадок. Если вы управляете программой ESET Server Security с помощью решения ESET PROTECT и назначили этой программе политику , ссылка на состояние блокируется (отображается как неактивная) в зависимости от того, какие функции включает в себя политика.
Требуется перезапуск устройства	Щелкните **Перезапустить устройство**, если нужно перезапустить систему незамедлительно, или щелкните Закрыть, если перезапуск планируется позже. Это сообщение может появиться после того, как были применены обновления и микрообновления компонентов программы. Сведения об обновлениях и микрообновлениях компонентов программы можно найти в разделе Конфигурация обновления.

Если у вас не получается устранить проблему, воспользуйтесь функцией поиска по базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте запрос в службу технической поддержки ESET . Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

Доступны обновления для Windows

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Уровень приоритета обновления отображается справа от его названия. Щелкните правой кнопкой мыши любую строку обновления и нажмите кнопку **Дополнительные сведения**, чтобы вывести на экран всплывающее окно с дополнительной информацией:



Щелкните элемент **Запустить обновление системы**, чтобы открыть окно **Центр обновления Windows** и продолжить работу с обновлениями системы.

Изоляция сети

Решение ESET Server Security предоставляет возможность блокировать сетевое соединение сервера — это называется сетевой изоляцией. При некоторых экстремальных сценариях вам может быть необходимо изолировать сервер от сети в качестве профилактической меры, например, если вы обнаружили, что сервер заражен вредоносными программами или компьютер был атакован каким-либо иным способом.

После активации сетевой изоляции весь сетевой трафик блокируется за исключением нижеперечисленного.

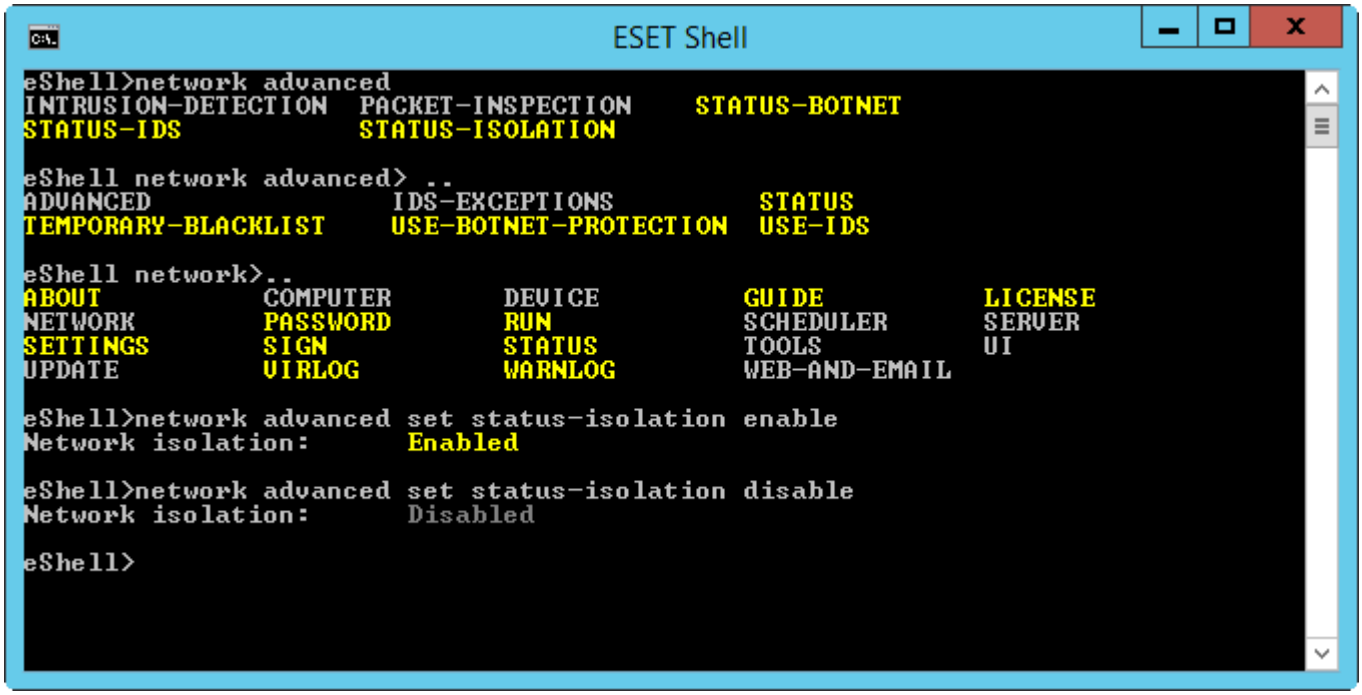
- Сохраняется подключение к контроллеру домена.
- ESET Server Security сохраняет возможность обмена данными.
- Агент ESET Management Agent и ESET Inspect Connector (при их наличии) могут обмениваться данными по сети

Активация и деактивация сетевой изоляции выполняется с помощью команды eShell или клиентской задачи ESET PROTECT.

eShell

В интерактивном режиме:

- Активация сетевой изоляции: `network advanced set status-isolation enable`
- Деактивация сетевой изоляции: `network advanced set status-isolation disable`



Кроме того, вы можете создать и запустить пакетный файл с помощью пакетного режима/режима сценария.

ESET PROTECT

- Активация сетевой изоляции с помощью клиентской задачи.
- Деактивация сетевой изоляции с помощью клиентской задачи.

Когда активирована сетевая изоляция, состояние ESET Server Security становится красным и отображается сообщение **Доступ к сети заблокирован**.

Если использовать ESET Server Security

В этой части содержится подробное описание интерфейса программы ESET Server Security, а также приведены сведения о ее использовании.

С помощью интерфейса вы можете быстро получить доступ к распространенным функциям:

- Мониторинг
- Файлы журнала
- Сканирование

- Обновление
- Настройка
- Служебные программы

Сканирование

Сканер по требованию является важной частью ESET Server Security. Он используется для сканирования файлов и папок на компьютере. Для обеспечения безопасности сети принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений.

Рекомендуется выполнять регулярные (например, раз в месяц) операции тщательного сканирования системы на предмет обнаружения вирусов, которые не были обнаружены при помощи функции защиты файловой системы в реальном времени. Это могло произойти, если в момент появления угрозы защита файловой системы в режиме реального времени была отключена, модуль обнаружения устарел или же файл не был распознан при первом сохранении на диск.

Выберите доступное сканирование по требованию для ESET Server Security.

Сканирование хранилища

Сканирование всех общих папок на локальном сервере. Если элемент Сканирование хранилища недоступен, это означает, что на сервере нет общих папок.

Просканировать компьютер

Позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество команды «Просканировать компьютер» заключается в том, что оно удобно в выполнении и не требует тщательной настройки сканирования. При сканировании проверяются все файлы на локальных дисках, а также автоматически очищаются или удаляются обнаруженные заражения. Для автоматического уровня очистки выбрано значение по умолчанию. Дополнительную информацию о типах очистки см. в разделе Очистка.

> Рекомендуется сканировать компьютер не реже одного раза в месяц. Сканирование можно настроить как запланированную задачу .

Выборочное сканирование

Выборочное сканирование является оптимальным решением, когда нужно указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом выборочного сканирования является возможность детальной настройки параметров. Конфигурации можно сохранять в пользовательских профилях сканирования, которые удобно применять, если регулярно выполняется сканирование с одними и теми же параметрами.

Сканирование съемных носителей

Подобно сканированию Smart данная функция быстро запускает сканирование съемных носителей (например, компакт-дисков, DVD-дисков, накопителей USB), которые подключены к

компьютеру. Это может быть удобно при подключении к компьютеру USB-устройства флэш-памяти, содержимое которого необходимо просканировать на наличие вредоносных программ и других потенциальных угроз. Этот тип сканирования можно также запустить, щелкнув элемент Выборочное сканирование, а затем выбрав элемент Съемные носители из раскрывающегося меню Объекты сканирования и нажав кнопку Сканировать.

Сканирование Hyper-V

Этот параметр отображается в меню, только если диспетчер Hyper-V установлен на том же сервере, на котором выполняется средство ESET Server Security. Сканирование Hyper-V позволяет сканировать диски виртуальных машин на сервере Microsoft Hyper-V Server без необходимости установки каких-либо агентов на соответствующие виртуальные машины.

Сканирование OneDrive

Дает возможность выполнять сканирование файлов пользователя, которые хранятся в облаке OneDrive.

Повторить последнее сканирование

Повторение последней операции сканирования с точно такими же настройками.

> Если используется сканирование базы данных по требованию, функция «Повторить последнее сканирование» недоступна.

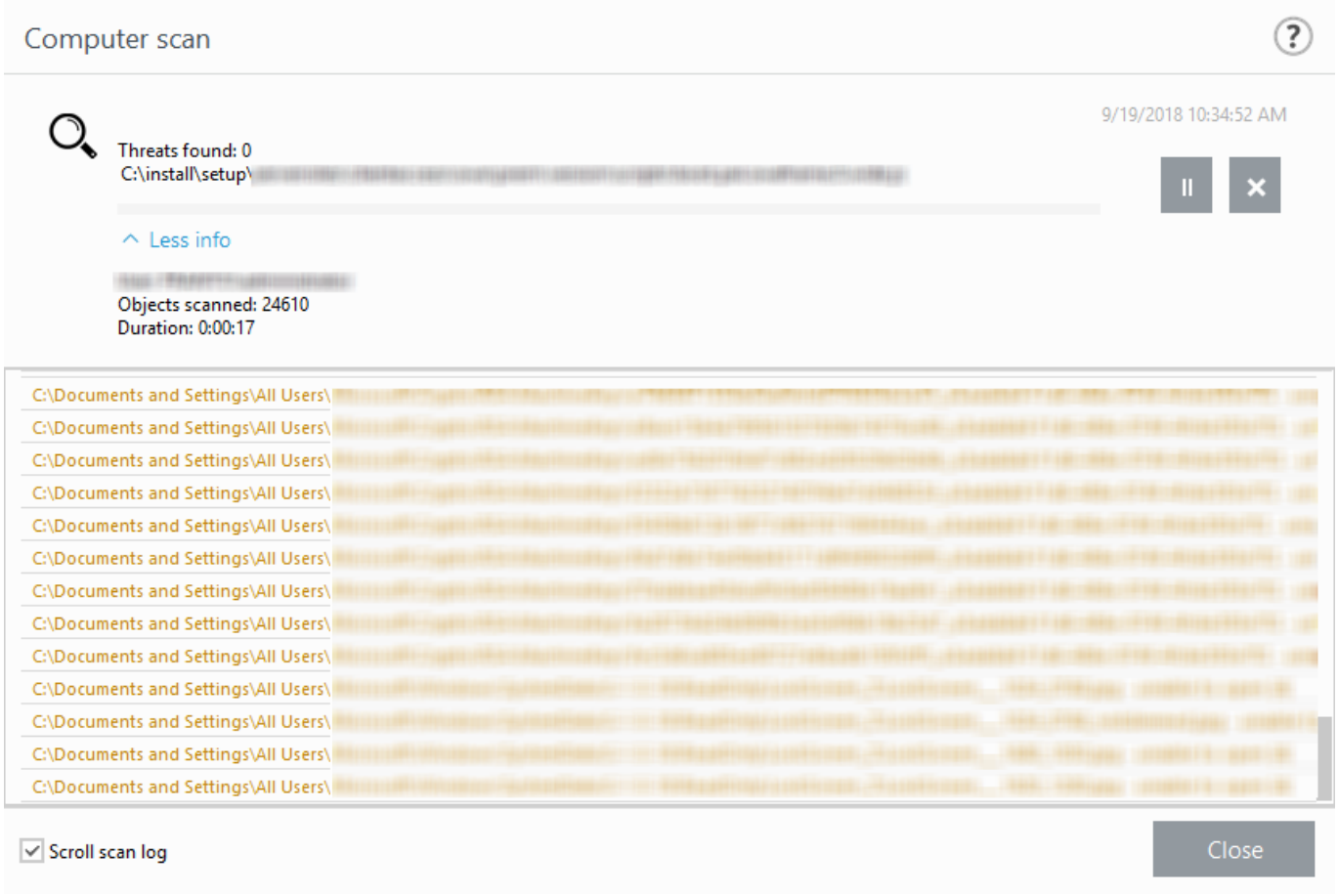
Параметры и дополнительные сведения о состоянии сканирования.

Перетаскивание файлов	Позволяет перетаскивать файлы в окно сканирования ESET Server Security. Эти файлы будут незамедлительно просканированы на наличие вирусов.
Закрыть/Закрыть все	Закрыть данные сообщения.
Состояние сканирования	Отображает состояние первого сканирования. Это сканирование полностью завершено или было прервано пользователем.
Показать журнал	Отображает более подробную информацию.
Дополнительные сведения	Например, просмотреть информацию о пользователе, который запустил сканирование, о количестве просканированных объектов, а также о **продолжительности** сканирования.
Открыть окно сканирования	В окне хода сканирования отображается текущее состояние сканирования и информация о количестве файлов, в которых обнаружен злонамеренный код.

Окно и журнал сканирования

В окне сканирования отображаются объекты, которые сканируются в настоящий момент, включая сведения об их расположении, количество найденных угроз (если они есть), количество просканированных объектов и продолжительность сканирования. В нижней части окна сканирования находится журнал сканирования, в котором отображается номер версии модуля обнаружения, дата и время начала сканирования и объект сканирования.

Нажатие кнопки **Пауза** позволит временно приостановить процесс сканирования. Когда процесс сканирования приостановлен, становится доступен параметр **Возобновить**.

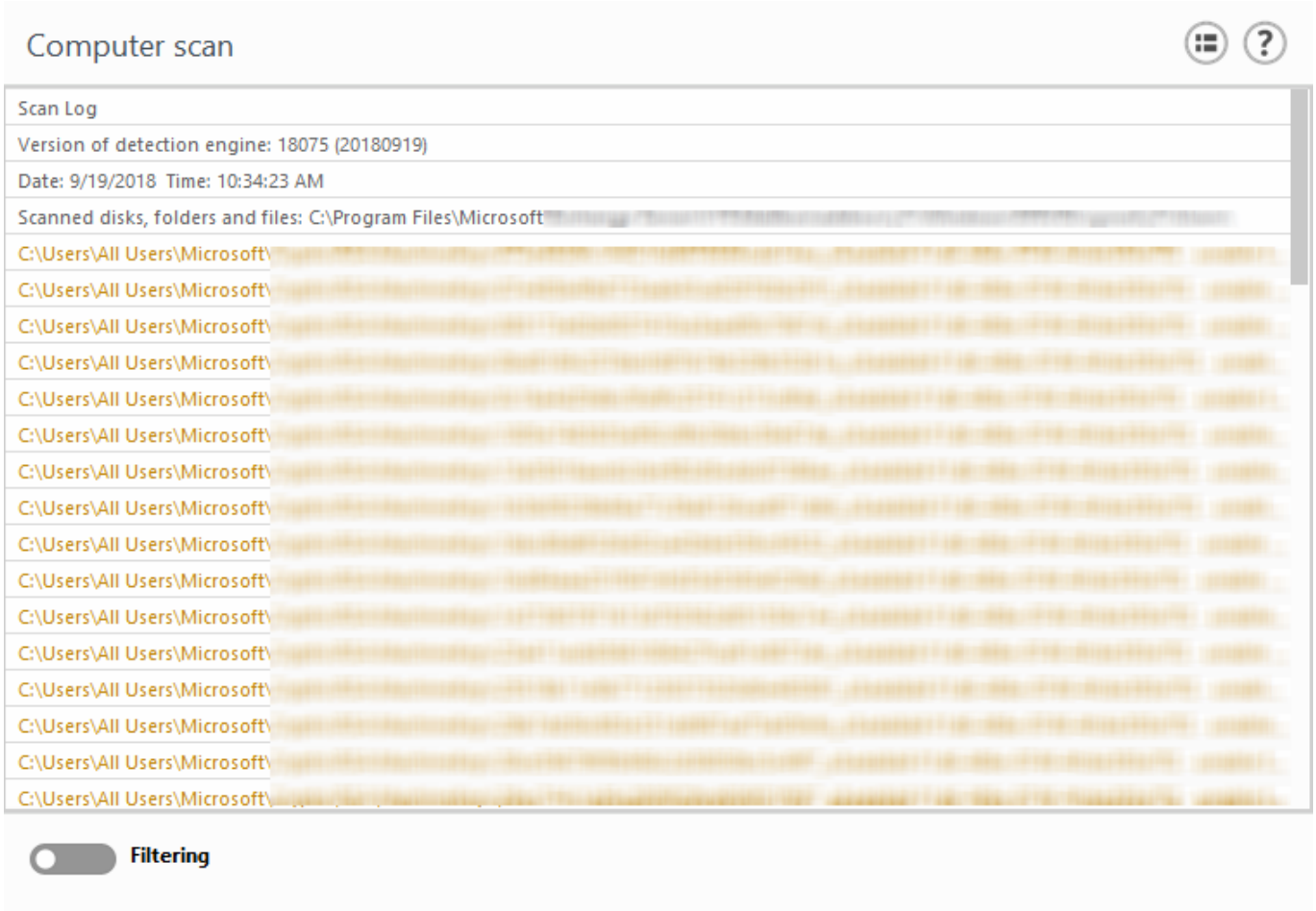


Прокручивать журнал сканирования

Установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне «Файлы журналов» выводились активные журналы.

> Нормально, что некоторые файлы, такие как защищенные паролем файлы или файлы, используемые исключительно операционной системой (обычно *pagefile.sys* и некоторые файлы журналов), не могут сканироваться.

После окончания сканирования отобразится журнал сканирования, со всей необходимой информацией, которая соответствует определенному сканированию.



Чтобы открыть окно Фильтрация журнала, в котором можно задать критерии фильтрации или поиска, щелкните значок переключателя **Фильтрация**.

Действие	Использование	Ярлык	См. также
Фильтрация одинаковых записей	Активация фильтра журнала, который показывает только записи одного выбранного типа.	Ctrl + Shift + F	
Фильтр...	При выборе этого параметра в окне «Фильтрация журнала» можно задать критерии фильтрации для определенных записей журнала.		Фильтрация журнала
Включить фильтр	Активация настроек фильтра. При первой активации фильтрации необходимо задать настройки.		

Действие	Использование	Ярлык	См. также
Отключить фильтр	Отключение фильтрации (такое же действие, как и при использовании переключателя внизу).		
Копировать	Копирование выделенных записей в буфер обмена.	Ctrl + C	
Копировать все	Копирование информации из всех записей в окне.		
Экспорт...	Экспорт информации выбранных записей в XML-файл.		
Экспортировать все...	Экспорт всей информации в окне в XML-файл.		

Файлы журнала

Файлы журналов содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных во время сканирования угрозах. Журналы являются важнейшим элементом анализа, обнаружения угроз, устранения неполадок и т. д. Ведение журнала выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и журналы можно непосредственно в среде ESET Server Security или экспортировав их в локальную среду.

В раскрывающемся меню выберите нужный тип журнала. Доступны следующие журналы.

Обнаружения

Журнал угроз содержит подробную информацию о заражениях, обнаруженных модулями ESET Server Security. Регистрируется информация о времени обнаружения, названии угрозы, месте обнаружения, выполненных действиях и имени пользователя, который находился в системе при обнаружении проникновения.

Дважды щелкните любую запись журнала, чтобы отобразить ее сведения в отдельном окне. При необходимости можно создать исключение обнаружения — щелкните правой кнопкой мыши запись журнала (обнаружение) и выберите команду **Создать исключение**. Откроется Мастер исключений с предварительно заданными критериями. Если рядом с исключенным файлом указано имя обнаружения, это означает, что файл будет исключен только для указанного обнаружения. Если этот файл будет заражен позже другой вредоносной программой, он будет обнаружен.

События

В журнале событий регистрируются все важные действия, выполняемые программой ESET Server Security. Этот журнал содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он помогает системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.

Сканирование компьютера

В этом окне отображаются результаты всех выполненных операций сканирования. Каждая

строка соответствует одной проверке компьютера. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.

Заблокированные файлы

Содержит записи заблокированных и недоступных файлов. Протокол содержит сведения о причине и исходном модуле, который заблокировал файл, а также о приложении, которое выполняло этот файл, и о пользователе, который его запустил.

Отправленные файлы

Содержит записи файлов облачной защиты, ESET LiveGuard Advanced и ESET LiveGrid®.

Журналы аудита

Содержит записи об изменениях в конфигурации или состоянии защиты и создает снимки для дальнейшего использования. Щелкните правой кнопкой мыши любую запись типа Изменение параметров и выберите Показать изменения из контекстного меню, чтобы отобразить подробную информацию о выполненных изменениях. Если нужно использовать предыдущую настройку, выберите Восстановить. Можно также воспользоваться параметром Удалить все для удаления записей журнала. Если необходимо деактивировать ведение журнала аудита, выберите Расширенные параметры > Сервис > Файлы журнала > Журнал аудита.

Система HIPS

Система содержит записи о правилах, помеченных для внесения в журнал. Протокол показывает приложение, которое вызвало операцию, результат (было ли правило разрешено или запрещено) и имя созданного правила.

Защита сети

Содержит записи файлов, заблокированных защитой от ботнетов и IDS (защита от сетевых атак).

Отфильтрованные веб-сайты

Список веб-сайтов, заблокированных функциями защиты доступа в Интернет . В этих журналах отображается время, URL-адрес, пользователь и приложение, с помощью которого установлено соединение с определенным веб-сайтом.

Контроль устройств

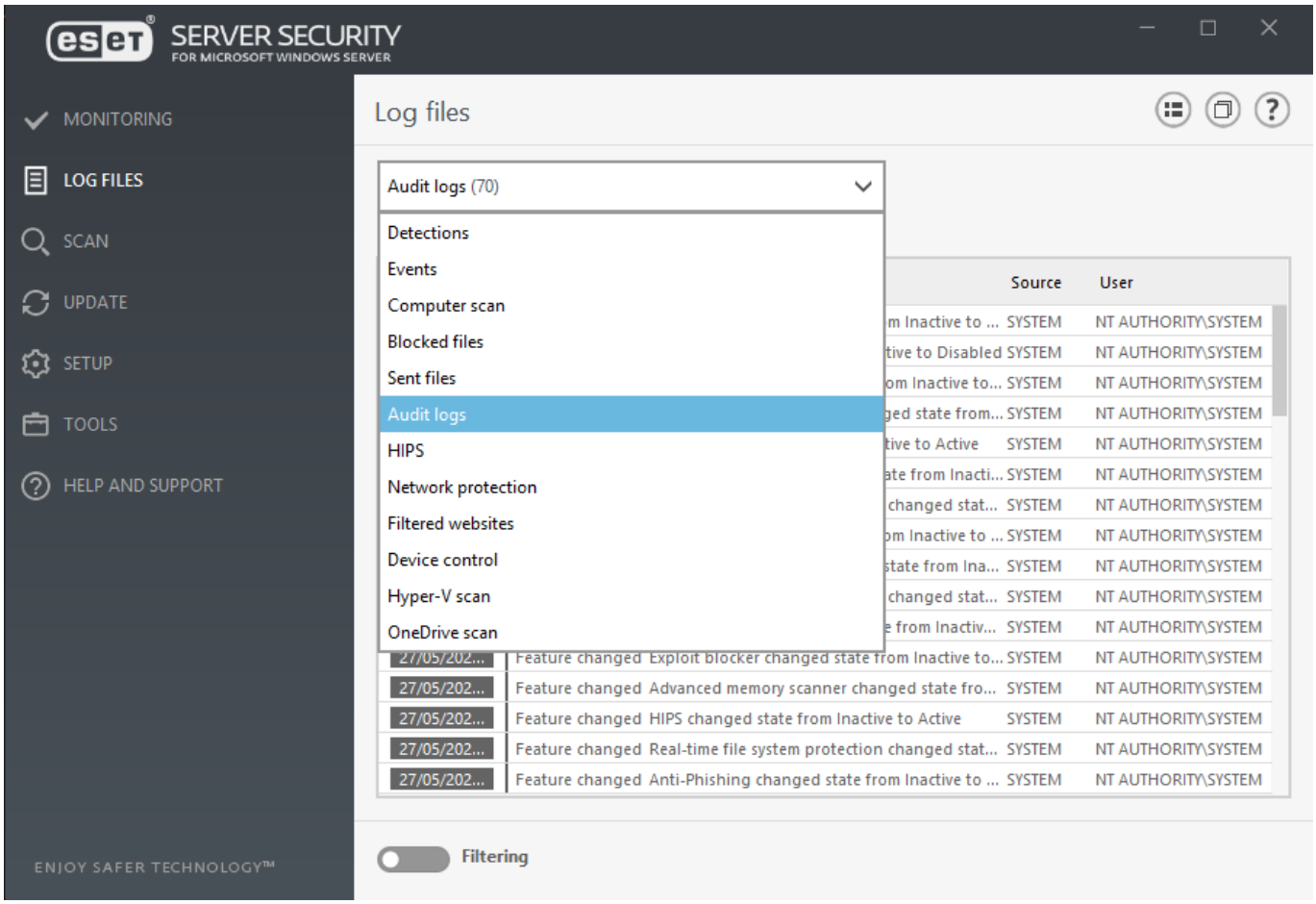
Содержит список подключенных к компьютеру съемных носителей и устройств. Сведения об устройствах в этот журнал вносятся только на основании правила контроля устройств. Запись об устройстве, которое не отвечает условиям правила, в журнале не создается. Здесь отображаются и такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).

Сканирование Hyper-V

Содержит список результатов сканирования Hyper-V. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.

Сканирование OneDrive

Содержит список результатов сканирования OneDrive.



Контекстное меню (щелчок правой кнопкой мыши) позволяет выбирать действие с выбранной записью журнала:

Действие	Использование	Ярлык	См. также
Показать	Просмотр в новом окне более подробной информации о выбранном журнале (как и при двойном щелчке).		
Фильтрация одинаковых записей	Активация фильтра журнала, который показывает только записи одного выбранного типа.	Ctrl + Shift + F	
Фильтр...	При выборе этого параметра в окне «Фильтрация журнала» можно задать критерии фильтрации для определенных записей журнала.		Фильтрация журнала
Включить фильтр	Активация настроек фильтра. При первой активации фильтрации необходимо задать настройки.		
Отключить фильтр	Отключение фильтрации (такое же действие, как и при использовании переключателя внизу).		
Копировать	Копирование выделенных записей в буфер обмена.	Ctrl + C	

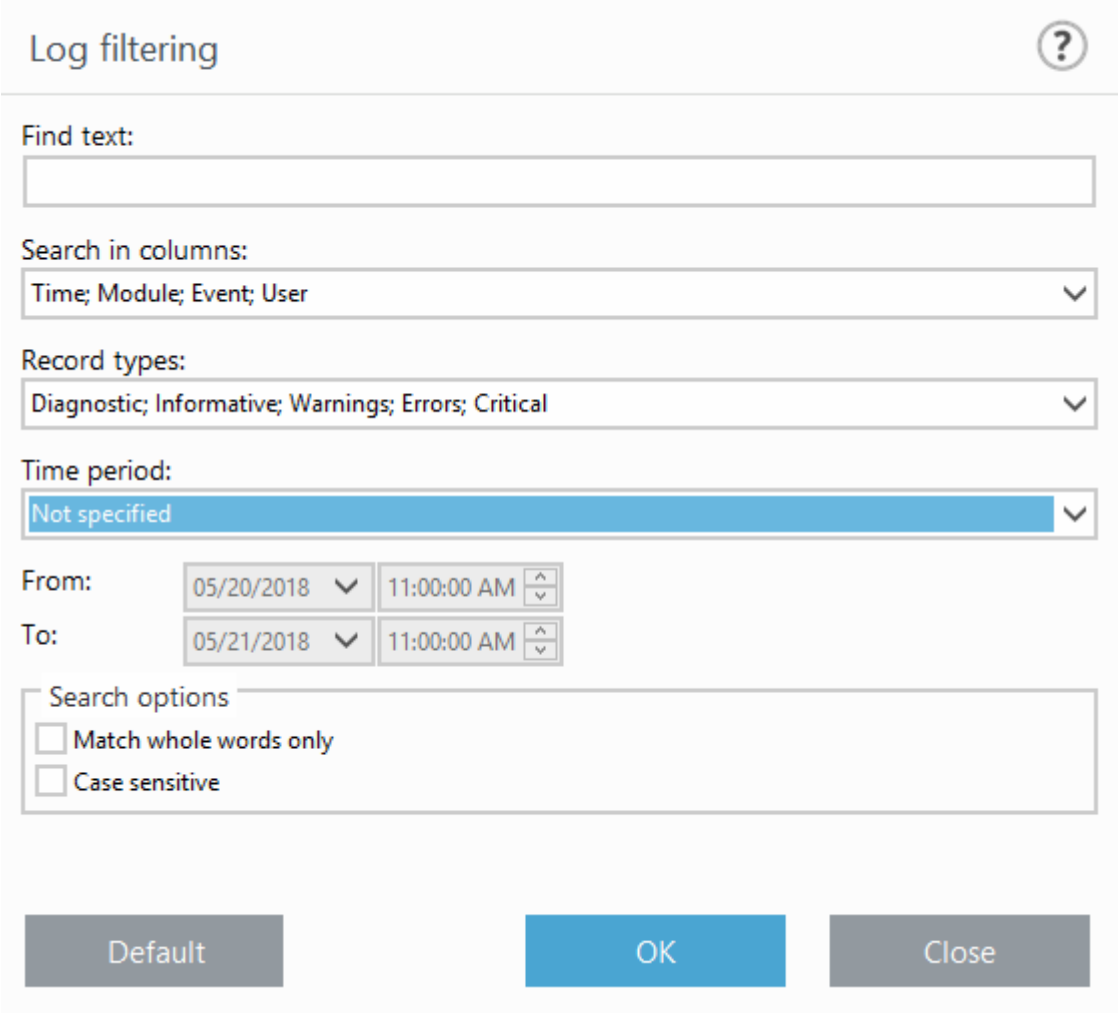
Действие	Использование	Ярлык	См. также
Копировать все	Копирование информации из всех записей в окне.		
Удалить	Удаление выбранных записей (для этого необходимы права администратора).	Del	
Удалить все	Удаление всех записей в окне (для этого необходимы права администратора).		
Экспорт...	Экспорт информации выбранных записей в XML-файл.		
Экспортировать все...	Экспорт всей информации в окне в XML-файл.		
Поиск...	Этот параметр открывает окно поиска в журнале и позволяет определить критерии поиска. С помощью функции поиска можно найти определенную запись даже при включенной фильтрации.	Ctrl + F	Найти в журнале
Найти следующее	Поиск следующего вхождения, соответствующего заданным критериям поиска.	F3	
Найти ранее	Поиск предыдущих вхождений.	Shift + F3	
Создать исключение	Исключение объектов из очистки с использованием имени обнаружения, пути или его хеша.		Создать исключение

Фильтрация журнала

Функция фильтрации журнала позволит найти сведения, особенно при большом количестве записей. Если необходимо найти определенный тип события, состояние или временной период, она позволяет уменьшить количество записей журнала.

Указав определенные параметры поиска, можно отфильтровать записи журнала. В окне «Файлы журнала» будут отображаться только записи, соответствующие этими параметрам поиска).

В поле **Найти текст** введите ключевое слово для поиска. С помощью раскрывающегося меню **Искать в столбцах** уточните поисковый запрос. Выберите одну или несколько записей в раскрывающемся меню **Типы записей журнала**. Задайте **период времени**, результаты за который нужно вывести на экран. Кроме того, можно использовать дополнительные параметры поиска, например, **Только слова целиком** или **С учетом регистра**.



Найти текст

Введите строку (слово целиком или частично). Будут показаны только записи, в которых содержится эта строка. Остальные записи будут опущены.

Искать в столбцах

Выберите, какие столбцы будут учитываться при поиске. Для использования в поиске можно отметить один столбец или сразу несколько.

Типы записей

В раскрывающемся меню выберите один или несколько типов записей журнала.

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения** — в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки** — в журнал вносится информация об ошибках загрузки файлов и критических ошибках.

• **Критические ошибки** — в журнал вносятся только критические ошибки.

Период времени

Задайте период времени, результаты за который нужно вывести на экран.

• Не указано (по умолчанию) — поиск по периоду времени не выполняется, поиск ведется в журнале целиком.

• Последний день

• Последняя неделя

• Последний месяц

• Период времени — для фильтрации только записей из указанного периода времени можно указать точный период времени («От:» и «До:»).

Только слова целиком

Установите этот флажок, если для получения более точных результатов нужно искать слова целиком.

С учетом регистра

Включите эту опцию, если при фильтрации должен учитываться регистр букв. При настройке параметров фильтрации или поиска нажмите кнопку **OK**, чтобы отобразить отфильтрованные записи журнала, или кнопку **Найти**, чтобы начать поиск.

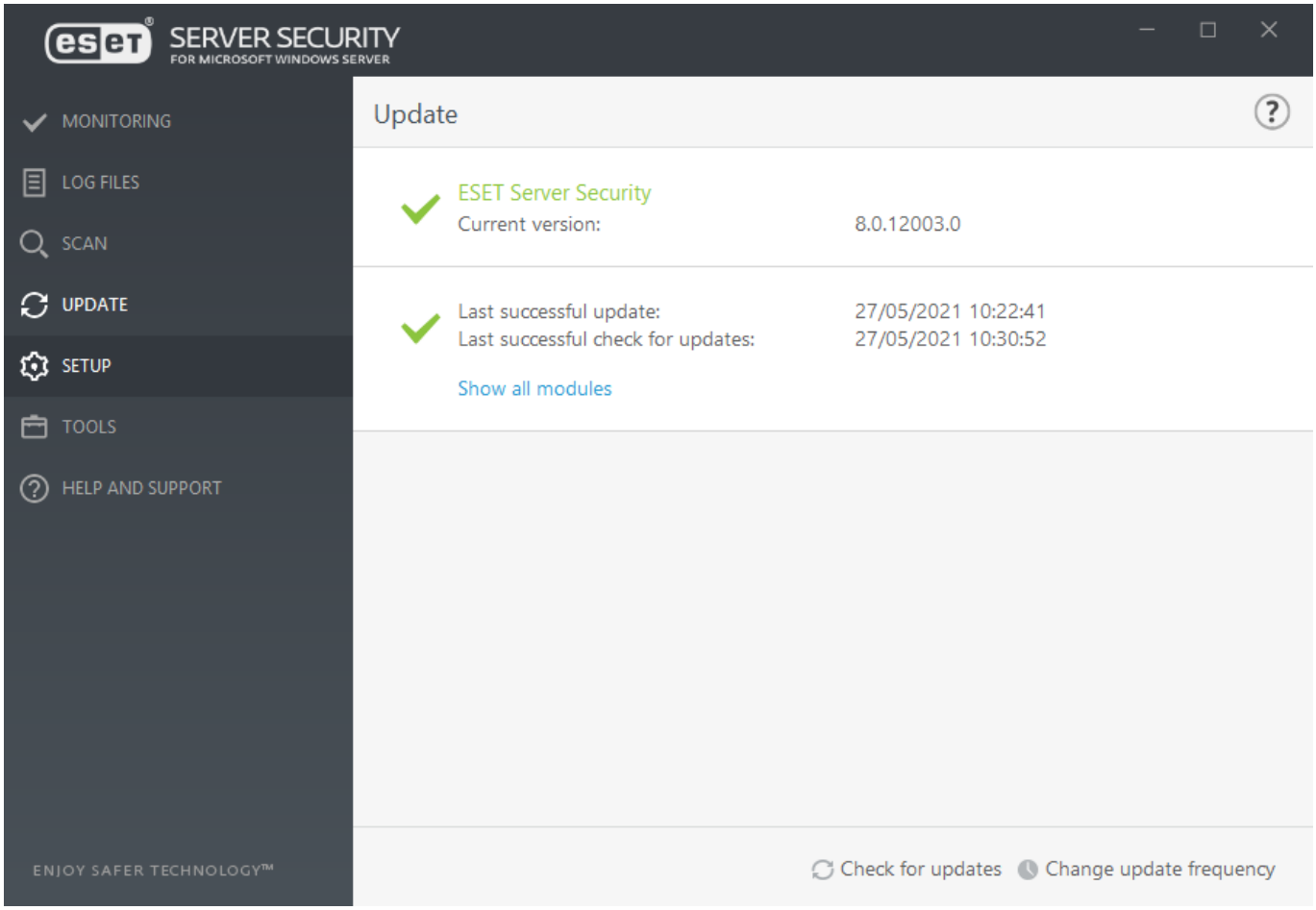
Поиск в файлах журналов ведется сверху вниз, начиная с текущего положения (выделенной записи). Поиск прекращается, когда находится первая соответствующая запись. Чтобы найти следующую запись, нажмите клавишу **F3**, или щелкните правой кнопкой мыши и выберите **Поиск**, чтобы уточнить поисковый запрос.

Обновление

В разделе обновлений можно увидеть информацию о текущем состоянии обновления системы ESET Server Security, в том числе дату и время последнего успешно выполненного обновления. Регулярное обновление ESET Server Security — лучший способ добиться максимального уровня безопасности сервера.

Модуль обновления поддерживает актуальность программы двумя способами: путем обновления модуля обнаружения и путем обновления компонентов программы. Обновление модуля обнаружения и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода.

> i Если Лицензионный ключ еще не был введен, вы не сможете получать обновления и вам будет предложено активировать продукт. Чтобы это сделать, перейдите к элементу **Справка и поддержка** > **Активировать продукт**.



Текущая версия

Версия сборки ESET Server Security.

Последнее успешное обновление

Дата последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что модули актуальны.

Последняя успешная проверка на наличие обновлений

Дата последней попытки обновления компонентов.

Показать все модули

Для открытия списка установленных компонентов.

Проверить наличие обновлений

Обновление компонентов является важнейшей частью обеспечения полной защиты компьютера от вредоносного кода.

Изменить частоту обновления

Можно изменять время задачи для задачи Регулярное автоматическое обновление планировщика.

Если не проверить наличие обновлений как можно скорее, на экран будет выведено одно из

следующих сообщений.

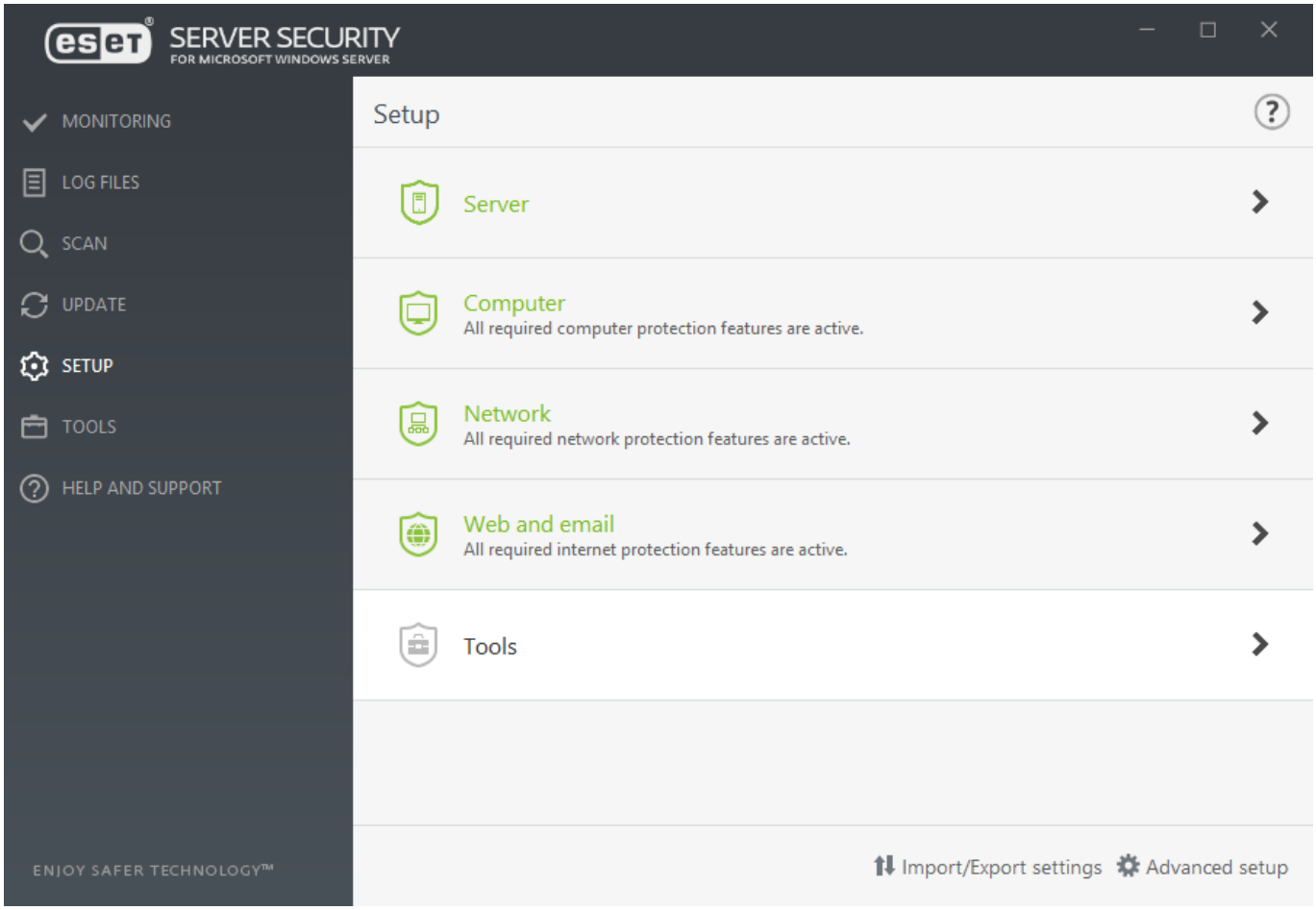
Сообщение об ошибке	Описания
Версия обновления модулей устарела	Эта ошибка появляется после нескольких неудачных попыток обновить модуль. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно настроенные параметры подключения.
Не удалось обновить модуль — продукт не активирован	В разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В **дополнительных настройках** (**F5**) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка** > Управление лицензией и введите новый лицензионный ключ.
Произошла ошибка при загрузке файлов обновлений	Возможная причина этой ошибки — параметры подключения к Интернету. Рекомендуется проверить наличие подключения к Интернету (например, попробуйте открыть любой веб-сайт в браузере). Если веб-сайт не открывается, возможно, не установлено подключение к Интернету или на компьютере возникли какие-либо проблемы с подключением к сети. Обратитесь к поставщику услуг Интернета, чтобы выяснить, имеется ли активное подключение к Интернету.
Обновление модулей не выполнено, ошибка 0073	Выберите пункты **Обновление** > **Проверить наличие обновлений**. Чтобы получить дополнительные сведения, см. статью базы знаний.

> Опции прокси-сервера для различных профилей обновления могут отличаться. В таком случае следует настроить разные профили обновления в разделе **Расширенные параметры** (**F5**), щелкнув **Обновление** > Профиль.

Настройка

Окно меню настроек содержит следующие разделы.

- Сервер
- Компьютер
- Сеть
- Интернет и электронная почта
- Сервис — ведение журнала диагностики



Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок. Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок. Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки.

Импорт и экспорт настроек

Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Сервер

Отобразится список компонентов, которые можно включить или отключить с помощью ползунка.

Автоматические исключения

Эта функция выявляет критически важные файлы серверных приложений и серверной операционной системы и автоматически добавляет их в список исключений. Она позволяет свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе программного обеспечения для обнаружения угрозы.

Кластер

Предназначен для настройки и активации кластера ESET.

Настройка сканирования OneDrive

Вы можете зарегистрировать или отменить регистрацию приложения сканирования ESET OneDrive в Microsoft OneDrive.

Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок. Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок. Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки.

Импорт и экспорт настроек

Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Компьютер

ESET Server Security располагает всеми необходимыми компонентами, чтобы обеспечить надежную защиту сервера как компьютера. В этом модуле можно включать, отключать и настраивать следующие компоненты.

Защита файловой системы в режиме реального времени

Все файлы сканируются на наличие вредоносного кода во время их открытия, создания или запуска. Для защиты в режиме реального времени также предусмотрен параметр **Настройка** или **Изменить исключения**, при выборе которого открывается окно настройки Исключения, в котором можно исключить файлы и папки из сканирования.

Контроль устройств

Данный модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним.

Система предотвращения вторжений на узел (HIPS)

Система отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.

- Advanced memory scanner
- Блокировщик эксплойтов
- Защита от программ-шантажистов

Режим презентации

Функция для пользователей, которым необходимо отсутствие каких-либо перерывов при использовании программного обеспечения и отвлекающих внимание всплывающих окон, а также когда требуется свести к минимуму потребление ресурсов процессора. После включения режима презентации на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.

Приостановить защиту от вирусов и шпионских программ

При каждом временном отключении защиты от вирусов и шпионских программ можно, воспользовавшись раскрывающимся меню, выбрать период времени, на протяжении которого будет отключен выбранный компонент, после чего следует нажать кнопку **Применить**, чтобы отключить компонент безопасности. Чтобы вновь активировать защиту, нажмите кнопку **Включить защиту от вирусов и шпионских программ** или включите, используя ползунок.

Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок . Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок . Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки .

Импорт и экспорт настроек

Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Сеть

Это достигается путем разрешения или отклонения отдельных сетевых подключений на основе правил фильтрации, что позволяет обеспечить защиту от атак с удаленных компьютеров и блокировать некоторые потенциально опасные службы.

В модуле «Сеть» можно включать, отключать и настраивать следующие компоненты.

Защиту от сетевых атак (IDS)

Анализирует содержимое сетевого трафика и защищает от сетевых атак. Любой трафик, расцененный как опасный, будет блокироваться.

Защита от ботнетов

Обнаружение и блокировка связи с ботнетами. Быстро и точно определяет вредоносную программу в системе.

Черный список временных IP-адресов (заблокированных адресов)

Просмотр списка IP-адресов, которые обнаружены как источники атак и добавлены в черный список, чтобы блокировать соединение в течение определенного периода времени.

Мастер устранения неполадок (недавно заблокированные приложения или устройства)

Дает возможность устранять проблемы с подключением, вызванные защитой от сетевых атак.

Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок. Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок. Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки.

Импорт и экспорт настроек

Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Мастер устранения сетевых неисправностей

Мастер устранения неисправностей отслеживает все заблокированные соединения и поможет пройти через процесс устранения неисправностей, чтобы исправить проблемы в защите от сетевых атак с помощью конкретных приложений или устройств. Затем мастер предложит новый набор правил, которые будут применяться, если их одобрят.

Интернет и электронная почта

Интернет и электронная почта позволяют включать, отключать и настраивать следующие компоненты.

Защита доступа в Интернет

Если этот параметр включен, весь трафик по протоколам HTTP и HTTPS сканируется на наличие вредоносных программ.

Защита почтового клиента

Обеспечивает контроль обмена данными по протоколам POP3 и IMAP.

Защита от фишинга

Защита от попыток незаконных веб-сайтов, выдающих себя за законные, получить пароли, банковские данные и прочую конфиденциальную информацию.

Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок. Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок. Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки.

Импорт и экспорт настроек

Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

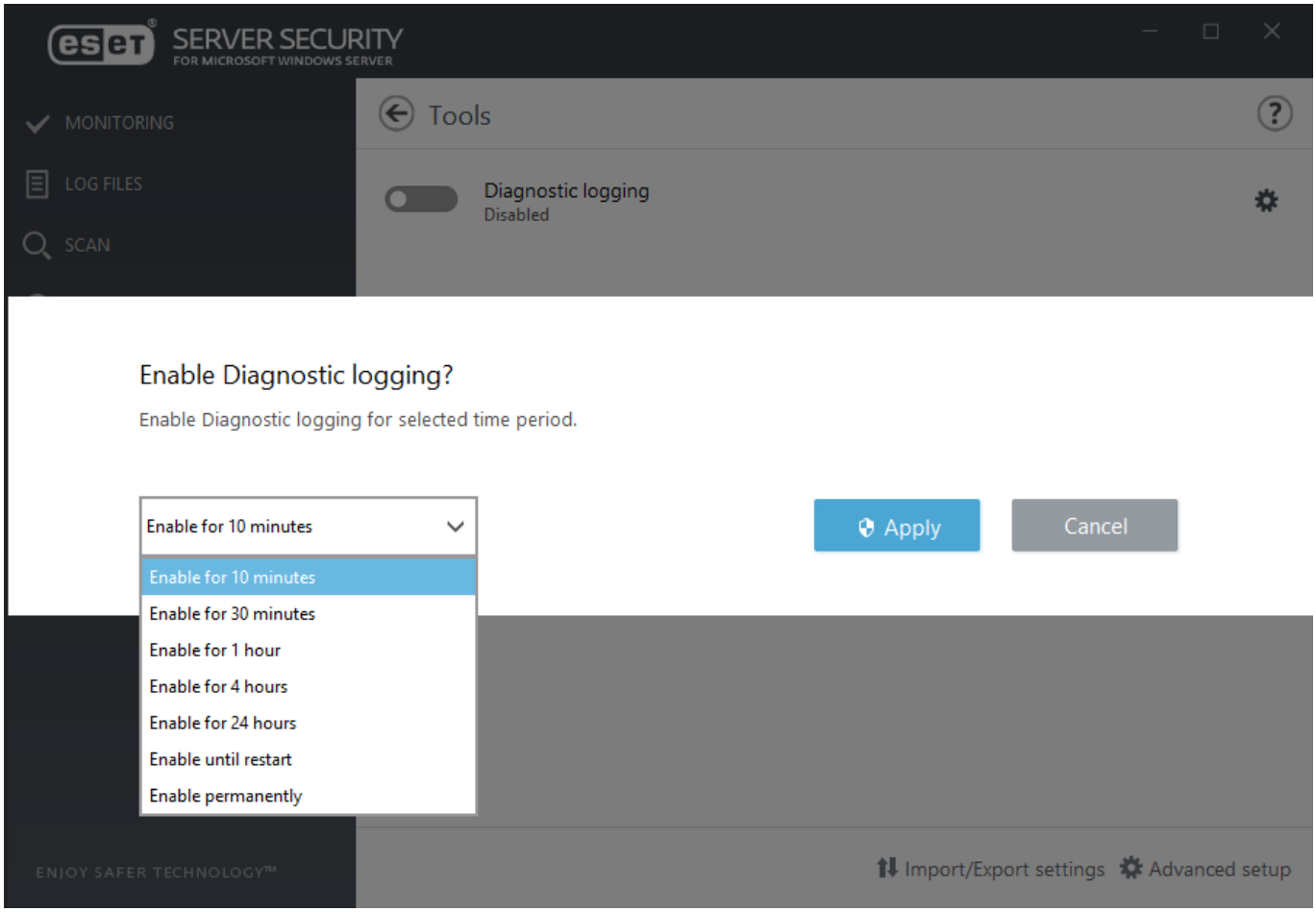
Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Сервис — ведение журнала диагностики

Ведение журнала диагностики можно включить, когда необходимы подробные сведения о поведении выбранного компонента ESET Server Security, например, при устранении неполадок. Если щелкнуть значок шестеренки, то можно настроить, для каких компонентов необходимо собирать журналы диагностики.

Выберите период, на протяжении которого эта функция должна оставаться включенной (10 минут, 30 минут, 1 час, 4 часа, 24 часа, до следующей перезагрузки сервера или постоянно). Когда журнал диагностики включен, ESET Server Security будет собирать подробные журналы в соответствии с тем, какие функции включены.



Чтобы временно отключить тот или иной модуль, рядом с подходящим модулем щелкните зеленый ползунок. Это может привести к ослаблению защиты вашего сервера.

Чтобы возобновить защиту отключенного компонента безопасности, рядом с подходящим модулем щелкните красный ползунок. Компонент снова будет включен.

Чтобы открыть дополнительные настройки определенного компонента безопасности, щелкните значок шестеренки.

Импорт и экспорт настроек

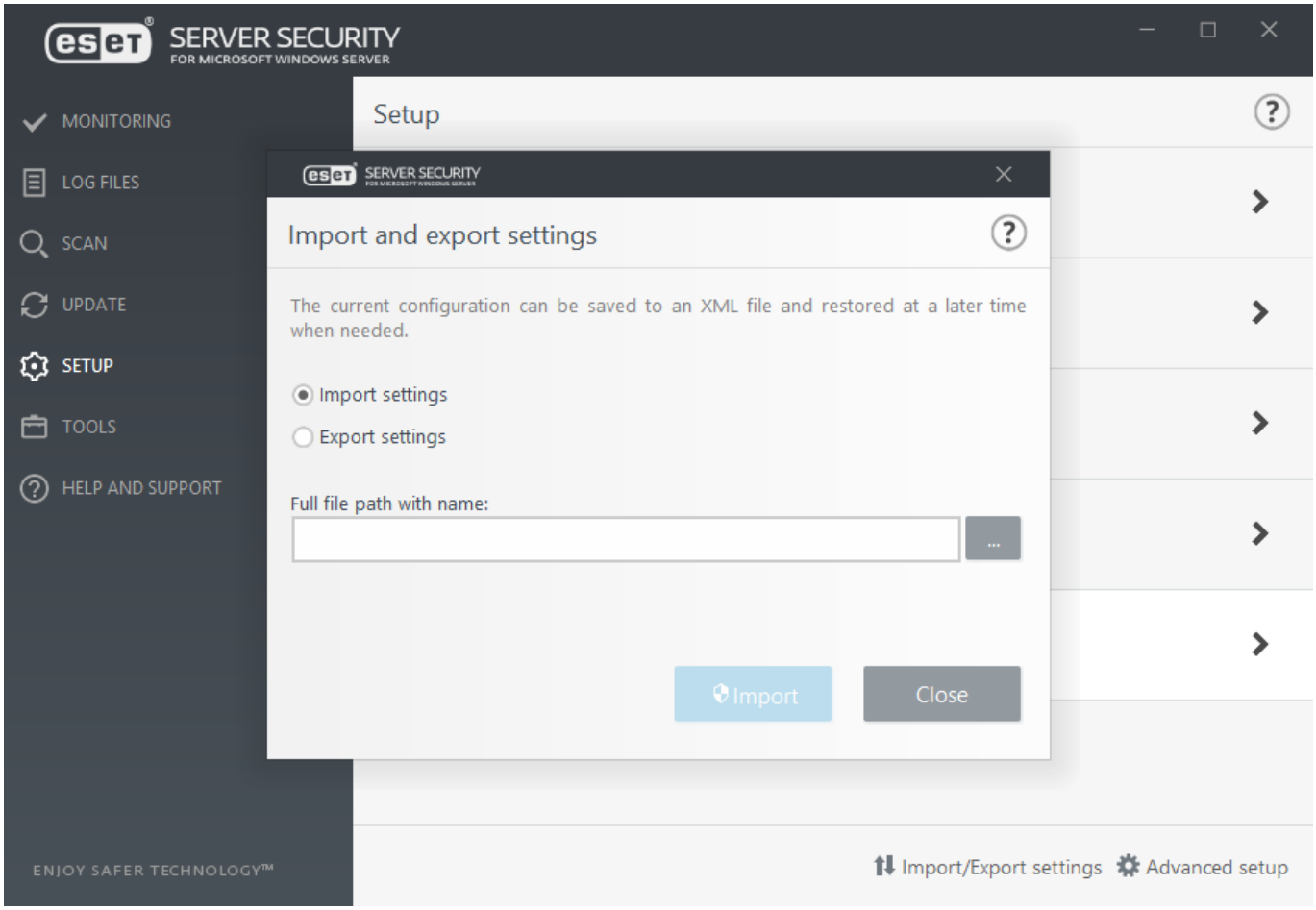
Загрузка параметров настройки из файла конфигурации в формате *.xml* или сохранение текущих параметров настройки в файле конфигурации.

Дополнительные настройки

Дополнительные настройки компонентов и параметров зависят от ваших потребностей. Окно **Расширенные параметры** можно открыть с любой страницы программы, нажав клавишу **F5**.

Импорт и экспорт параметров

Функция импорта и экспорта параметров полезна, если необходимо создать резервные копии текущей конфигурации ESET Server Security. Кроме того, функцию импорта можно использовать для распространения или применения этих же параметров для других серверов с ESET Server Security. Параметры экспортируются в файл *.xml*.



При экспорте параметров может возникнуть ошибка, если у вас нет права для записи экспортируемого файла в указанный каталог.

Служебные программы

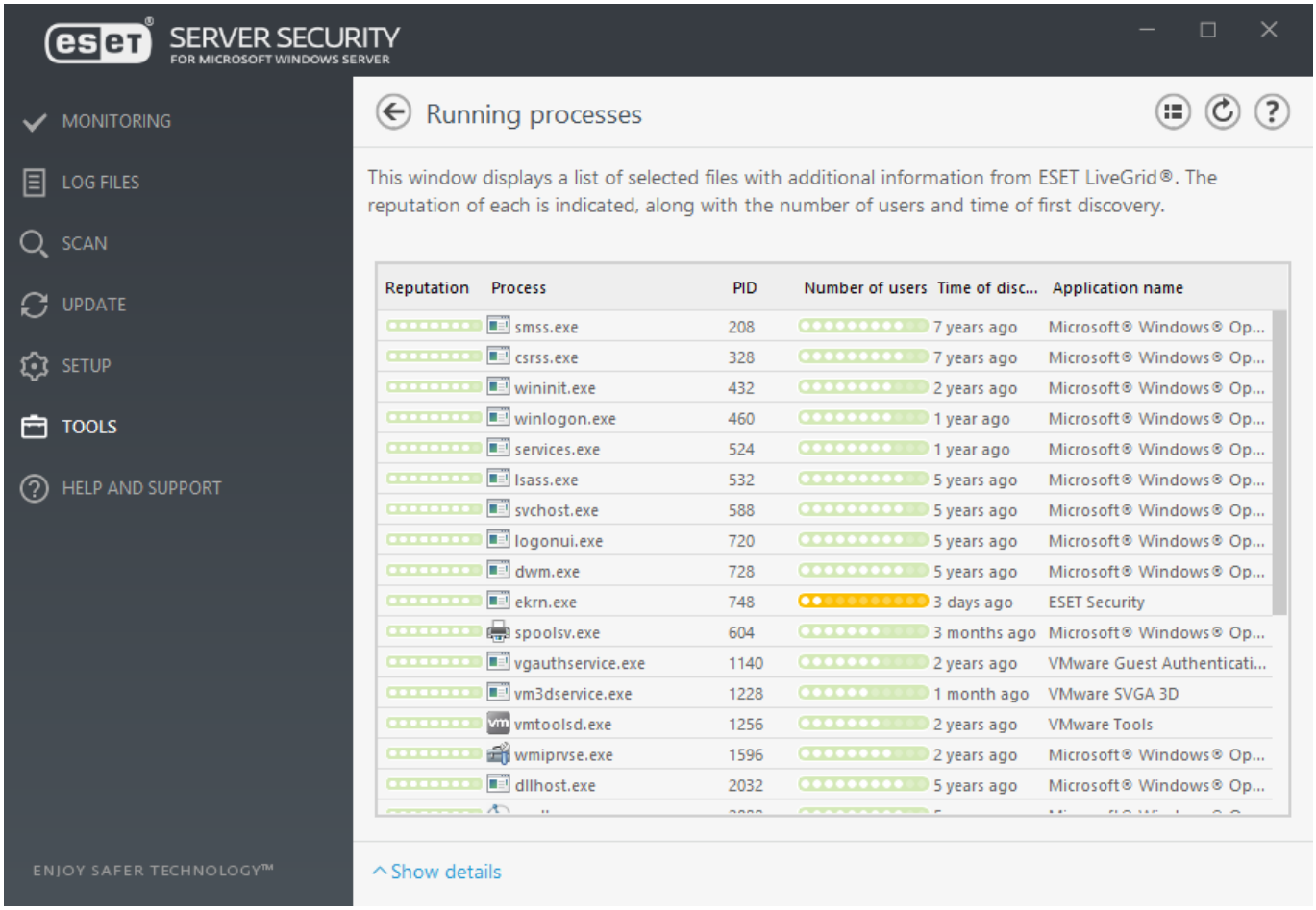
Для администрирования ESET Server Security доступны следующие функции:

- Запущенные процессы
- Мониторинг
- Статистика системы защиты
- Кластер
- ESET Shell
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live
- Планировщик
- Отправить файл для анализа

- Карантин

Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, эта функция позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET Server Security предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии ESET LiveGrid®.



> Известные приложения, помеченные как «Наилучшая репутация» (зеленый), являются безопасными (внесены в белый список) и исключаются из сканирования, благодаря чему увеличивается скорость сканирования компьютера по запросу и улучшается защита файловой системы в реальном времени.

Репутация	**В большинстве случаев ESET Server Security и технология ESET LiveGrid® определяют репутацию объекта на основе наборов эвристических правил, которые изучают характеристики каждого объекта (файла, процесса, раздела реестра и т.п.) и затем оценивают вероятность их вредоносной деятельности. На основе такого эвристического анализа объектам присваивается уровень репутации: от 9 — наилучшая репутация (зеленый) до 0 — наихудшая репутация (красный).**
Процесс	Имя образа программы или процесса, запущенных в настоящий момент на компьютере. Для просмотра всех запущенных на компьютере процессов можно использовать также диспетчер задач Windows. Чтобы открыть диспетчер задач, щелкните правой кнопкой мыши в пустой области на панели задач и выберите пункт «Диспетчер задач» или одновременно нажмите клавиши Ctrl+Shift+Esc на клавиатуре.
PID	Идентификатор процессов, запущенных в операционных системах Windows.
Количество пользователей	Количество пользователей данного приложения. Эта информация собирается технологией ESET LiveGrid®.
Время обнаружения	Время, прошедшее с момента обнаружения приложения технологией ESET LiveGrid®.
Имя приложения	Имя программы, которой принадлежит этот процесс.

> Если для приложения выбран уровень безопасности «Неизвестно» (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией отправки файла на анализ для отправки файла в вирусную лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления модуля обнаружения.

Показать подробности

В нижней части окна отобразится следующая информация.

- Путь: расположение приложения на компьютере.
- Размер: размер файла в КБ (килобайтах) или МБ (мегабайтах).
- Описание: характеристики файла на основе его описания в операционной системе.
- Компания: название поставщика или процесса приложения.
- Версия: информация от издателя приложения.
- Продукт: имя приложения и/или наименование компании.
- Дата создания: дата и время создания приложения.
- Дата изменения: дата и время последнего изменения приложения.

Добавить в исключения для процессов

Щелкните правой кнопкой мыши окно запущенных процессов, чтобы отменить его сканирование. Этот путь будет добавлен в список Исключения для процессов.

Мониторинг

Для мониторинга, содержащего действие в формате графика, выберите из раскрывающегося меню следующее действие.

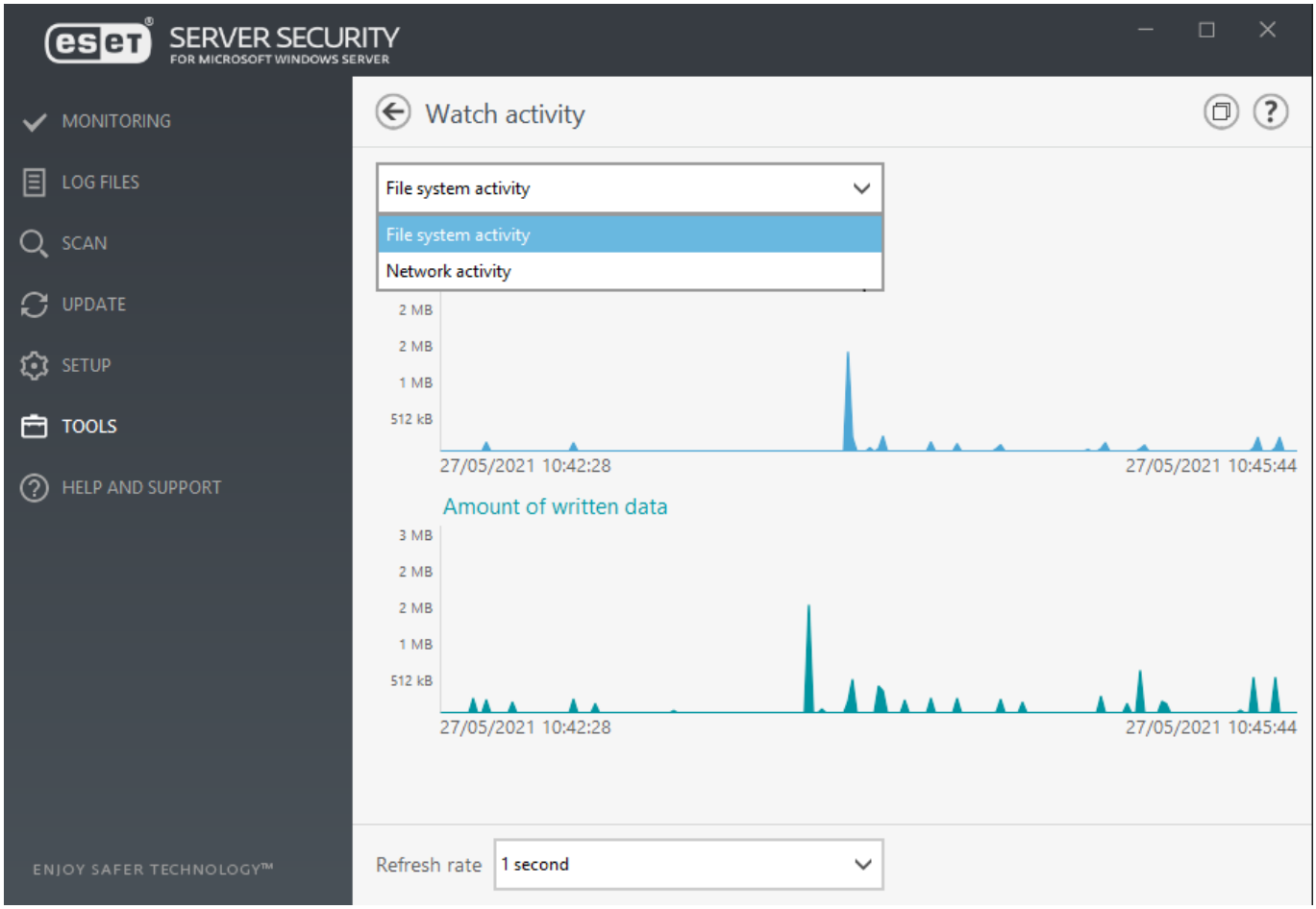
Активность файловой системы

Количество прочитанных или записанных данных. Вертикальная ось графика представляет собой прочитанные (синий цвет) и записанные данные (зеленый цвет).

Сетевая активность

Количество полученных или отправленных данных. Вертикальная ось графика представляет собой полученные (синий цвет) и отправленные данные (зеленый цвет).

В нижней части графика находится временная шкала, на которой отображается активность файловой системы в реальном времени за выбранный временной интервал. Чтобы изменить частоту обновлений, воспользуйтесь раскрывающимся меню Частота обновления.



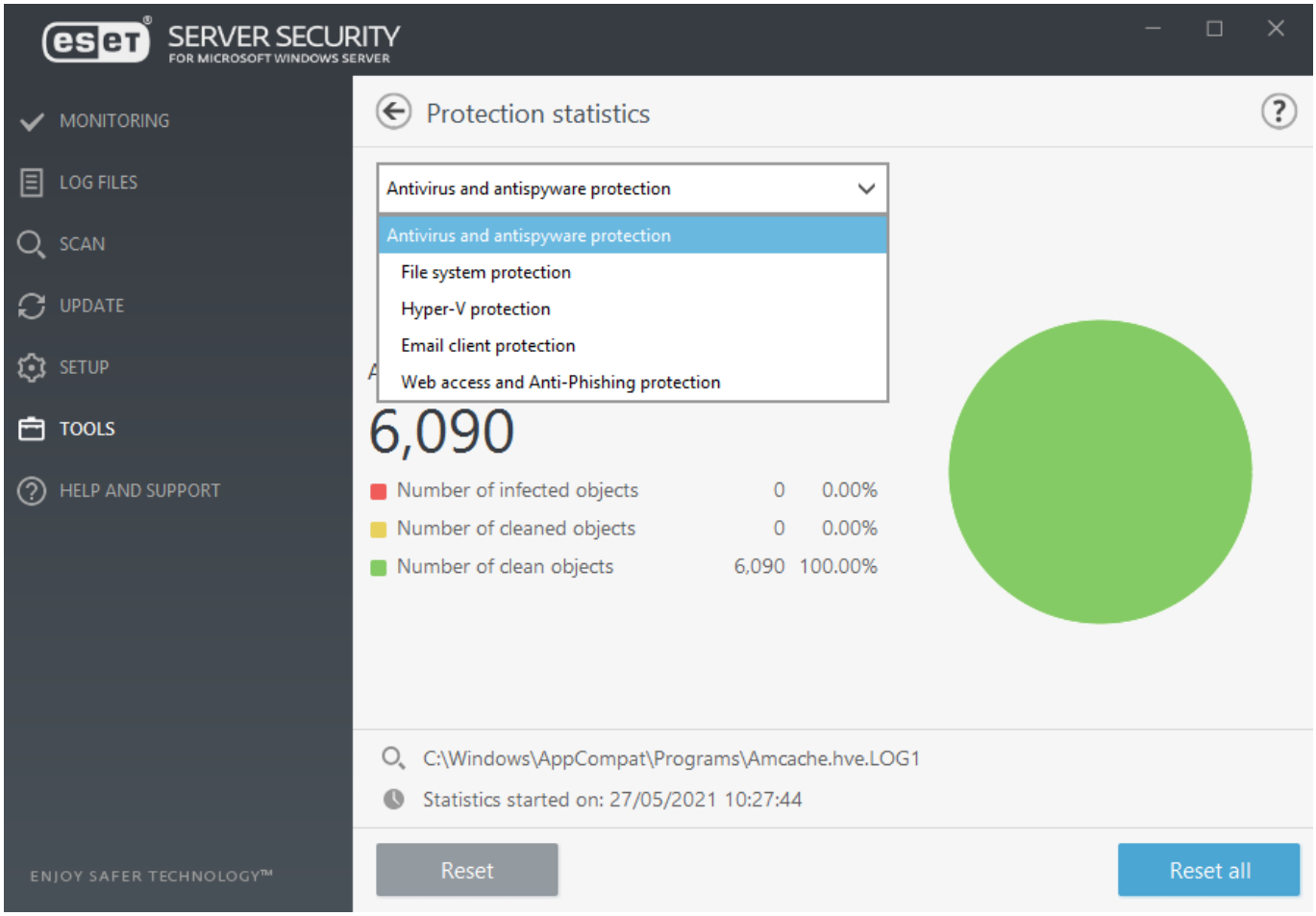
Доступны указанные ниже варианты.

1 секунда	**График обновляется каждую секунду, а временная шкала охватывает последние 10 минут.**
1 минута (последние 24 часа)	График обновляется каждую минуту, а временная шкала охватывает последние 24 часа.
1 час (последний месяц)	График обновляется каждый час, а временная шкала охватывает последний месяц.

Статистика системы защиты

Для просмотра статистических данных, связанных с модулями защиты ESET Server Security, из раскрывающегося меню необходимо выбрать соответствующие модули защиты. К статистике можно отнести такую информацию как количество просканированных, зараженных, очищенных и чистых объектов.

Наведя курсор мыши на объект рядом с графиком, можно увидеть данные этого конкретного объекта. Чтобы очистить данные статистики для текущего модуля защиты, нажмите кнопку **Сброс**. Чтобы очистить все существующие данные, нажмите кнопку **Сбросить все**.



В ESET Server Security доступны следующие статистические диаграммы.

Защита от вирусов и шпионских программ

Отображение общего количества зараженных и очищенных объектов.

Защита файловой системы

Отображение только тех объектов, которые считываются из файловой системы или записываются в нее.

Защита Hyper-V

Отображение общего количества зараженных, очищенных и чистых объектов (только в системах с Hyper-V).

Защита почтового клиента

Отображение только объектов, отправленных или полученных почтовыми клиентами.

Защита доступа в Интернет и защита от фишинга

Отображение только объектов, загруженных веб-браузерами.

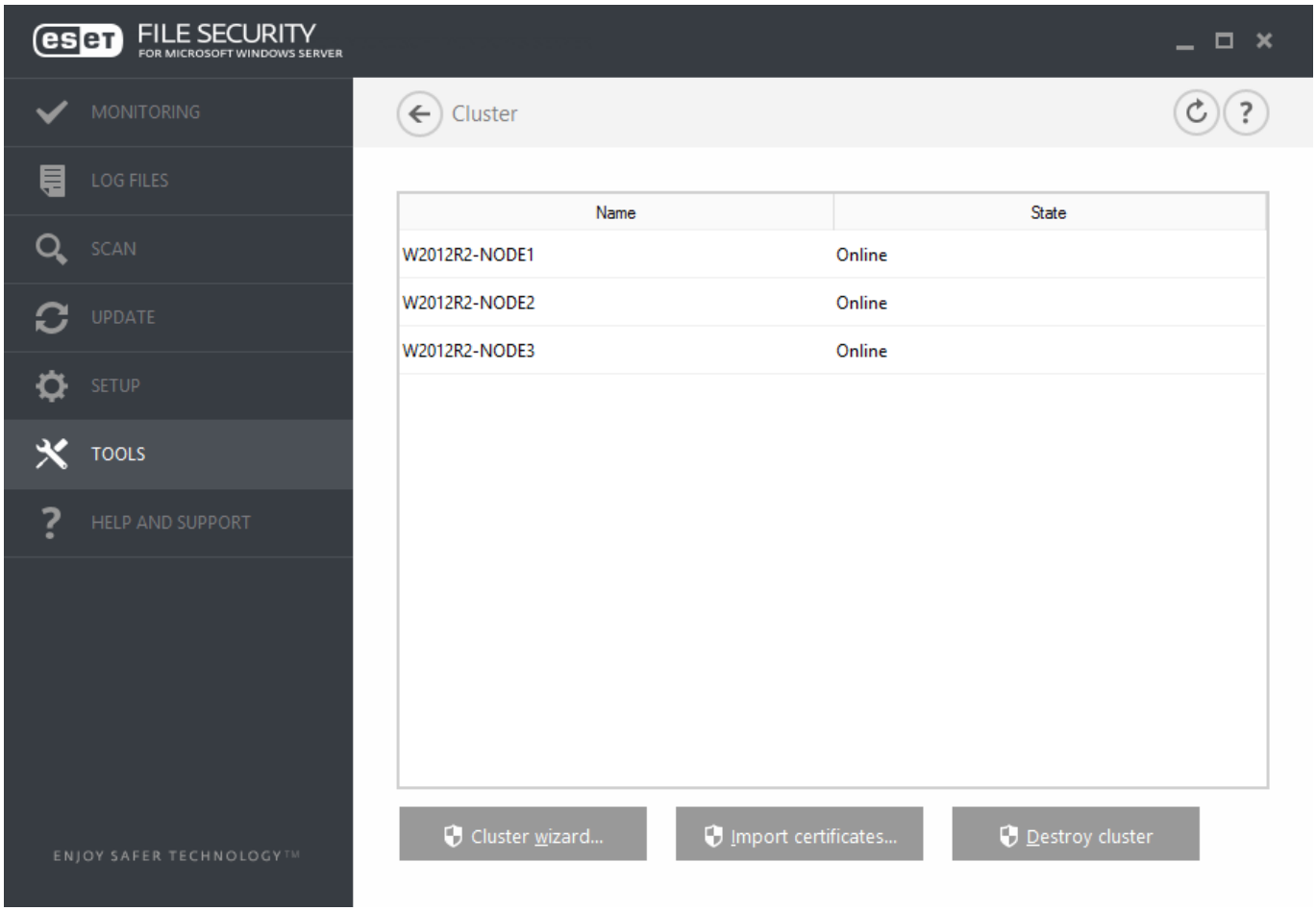
Кластер

Кластер ESET — это одноранговая (P2P) инфраструктура взаимодействия линейки продуктов ESET для Microsoft Windows Server.

Эта инфраструктура позволяет серверным продуктам ESET взаимодействовать друг с другом и обмениваться данными, например сведениями о конфигурации и уведомлениями, синхронизировать данные, необходимые для правильной работы группы экземпляров продуктов. Примером такой группы является группа узлов в отказоустойчивом кластере Windows или кластере балансировки сетевой нагрузки (NLB) с продуктами ESET, установленными там, где необходима одинаковая конфигурация продукта во всем кластере. Кластер ESET обеспечивает единообразие конфигурации в нескольких экземплярах.

> Настройки интерфейса и запланированных задач разных узлов кластера ESET не синхронизируются. Это сделано намеренно.

К странице состояния кластера ESET можно получить доступ из главного меню, последовательно щелкнув элементы **Сервис** > **Кластер**. При правильной настройке страница состояния должна выглядеть следующим образом.



> Создание кластера ESET между ESET Server Security и ESET File Security для Linux не поддерживается.

Есть два способа добавления узлов при настройке кластера ESET:

• **Автообнаружение** — Если у вас есть существующий отказоустойчивый кластер Windows или кластер NLB, автообнаружение автоматически добавит свои узлы-члены в кластер ESET.

• **Обзор** — узлы можно добавить вручную. Для этого нужно ввести имена серверов (участников одной рабочей группы или одного домена).

> При освобождении сообщения электронной почты из карантина, ESET Server Security игнорирует `To:` заголовок MIME, потому что его несложно подделать. Вместо этого программа использует исходную информацию о получателе, содержащуюся в команде `RCPT TO:`, которая была получена при SMTP-подключении. Благодаря этому освобожденное из карантина сообщение электронной почты будет доставлено правильному получателю.

После добавления узлов в кластер ESET необходимо выполнить установку ESET Server Security на каждом их них. Это выполняется автоматически в процессе настройки кластера ESET. Учетные данные, необходимые для удаленной установки программы ESET Server Security на других узлах кластера, следующие.

• **Сценарий домена** — учетные данные администратора домена;

• **Сценарий рабочей группы** — необходимо убедиться, что все узлы используют одинаковые учетные данные локального администратора.

В кластере ESET можно использовать также узлы, которые добавляются автоматически как участники существующего отказоустойчивого кластера Windows или кластера NLB, вместе с узлами, добавляемыми вручную (если они относятся к одному домену).

> Совмещать узлы домена с узлами рабочей группы нельзя.

Еще одним требованием для работы кластера ESET является включение параметра **Общий доступ к файлам и принтерам** в брандмауэре Windows перед передачей ESET Server Security на узлы кластера ESET.

Запустив Мастер кластеров, в кластер ESET в любой момент можно добавить новые узлы.

Импортировать сертификат

Сертификаты используются для обеспечения надежной идентификации от компьютера к компьютеру при использовании протокола HTTPS. Для каждого кластера ESET существует независимая иерархия сертификатов. Иерархия имеет один корневой сертификат и набор сертификатов узлов, подписанных корневым сертификатом. Закрытый ключ корневого сертификата уничтожается после создания всех сертификатов узлов. При добавлении нового узла в кластер, создается новая иерархия сертификатов. Перейдите в папку, содержащую сертификаты (которые были созданы мастером кластеров). Выберите файл сертификата и нажмите **Открыть**.

Уничтожить кластер

Кластер ESET можно демонтировать. В журнал событий каждого узла будет добавлена запись об уничтожении кластера ESET. После этого все правила файервола ESET будут удалены из файервола Windows. Бывшие узлы будут возвращены в прежнее состояние, и, если необходимо, их можно будет снова использовать в другом кластере ESET.

Мастер кластеров — выбор узлов

При настройке кластера ESET необходимо начать с добавления узлов. Чтобы добавить узлы, можно использовать функцию **Автоопределение** или команду **Обзор**. Кроме того, в текстовом поле можно ввести имя сервера и нажать кнопку **Добавить**.

Автообнаружение

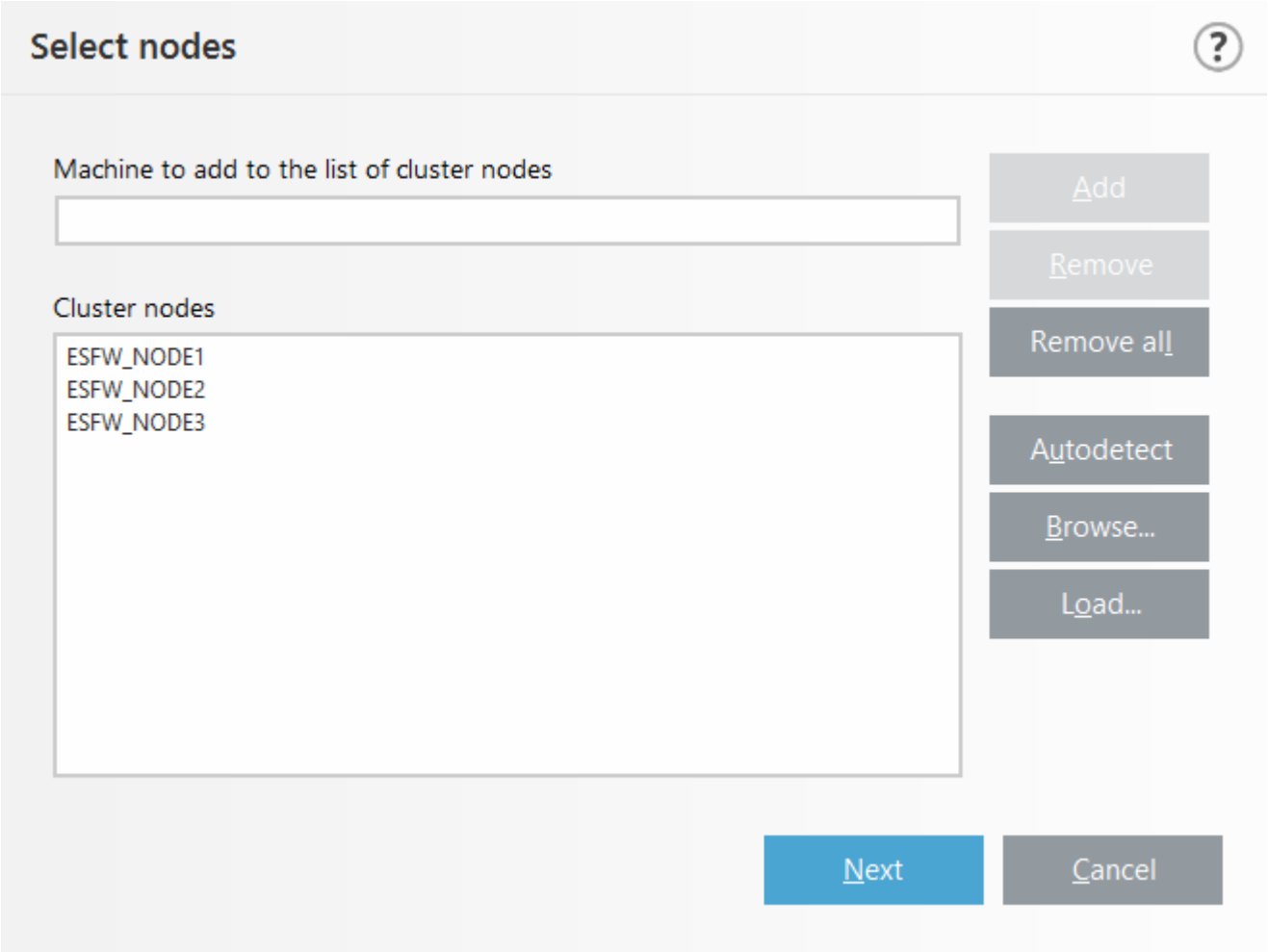
Windows Failover Cluster Или Network Load Balancing (NLB) Cluster. Для автоматического добавления узлов сервер, который используется для создания кластера ESET, должен являться участником этого Windows Failover Cluster или NLB Cluster. Чтобы мог правильно определять узлы, в свойствах кластера NLB должна быть включена функция **Разрешить удаленный контроль**. Получив список недавно добавленных узлов.

Обзор

Чтобы найти и выбрать компьютеры в Domain или в Workgroup, щелкните элемент «Обзор». Этот способ позволяет добавить узлы в кластер ESET вручную. Кроме того, чтобы добавить узлы, можно ввести имя хоста, который необходимо добавить, и нажать кнопку **Добавить**.

Загрузить

Чтобы импортировать список узлов из файла.



Чтобы изменить **узлы кластера** в списке, выберите узел, который следует удалить, и

используйте команду **Удалить**, а чтобы полностью очистить список, выберите команду **Удалить все**.

Если кластер ESET уже используется, в него можно добавить новые узлы в любой момент. Для этого необходимо выполнить действия, описанные выше.

> Все узлы, добавляемые в список, должны находиться в сети и быть доступны. По умолчанию в списке находится узел Localhost.

Мастер кластеров — настройки кластера

Определите имя кластера и особенности сети (при необходимости).

Имя кластера

Укажите имя кластера и нажмите кнопку Далее.

Прослушивающий порт: порт по умолчанию — 9777

Если порт 9777 уже используете в сетевой среде, укажите другой номер порта, который не используется.

Открыть порт в файерволе Windows

Если установлен этот флажок, в файерволе Windows создается правило.

Мастер кластеров — параметры настройки кластера

Выберите режим распространения сертификатов и укажите, нужно ли устанавливать продукт на другие узлы.

Распространение сертификатов

- **Автоматическое** удаленное управление: сертификат будет установлен автоматически.
- **Вручную** — после нажатия кнопки **Создать** откроется окно просмотра, в котором нужно выбрать папку для хранения сертификатов. Создается корневой сертификат, а также сертификат для каждого узла, включая тот, с которого настраивается кластер ESET (локальный компьютер). Затем можно зарегистрировать сертификат на локальном компьютере, нажав кнопку **Да**.

Установка продукта на другие узлы

- **Автоматическое удаленное управление**: установка ESET Server Security на каждый узел будет выполнена автоматически (если операционная система узла поддерживает архитектуру, которой соответствует продукт).
- **Вручную** — этот параметр дает возможность установить программу ESET Server Security вручную (например, если на некоторых узлах используется другая архитектура ОС).

Передать лицензию на узлы без активированного продукта

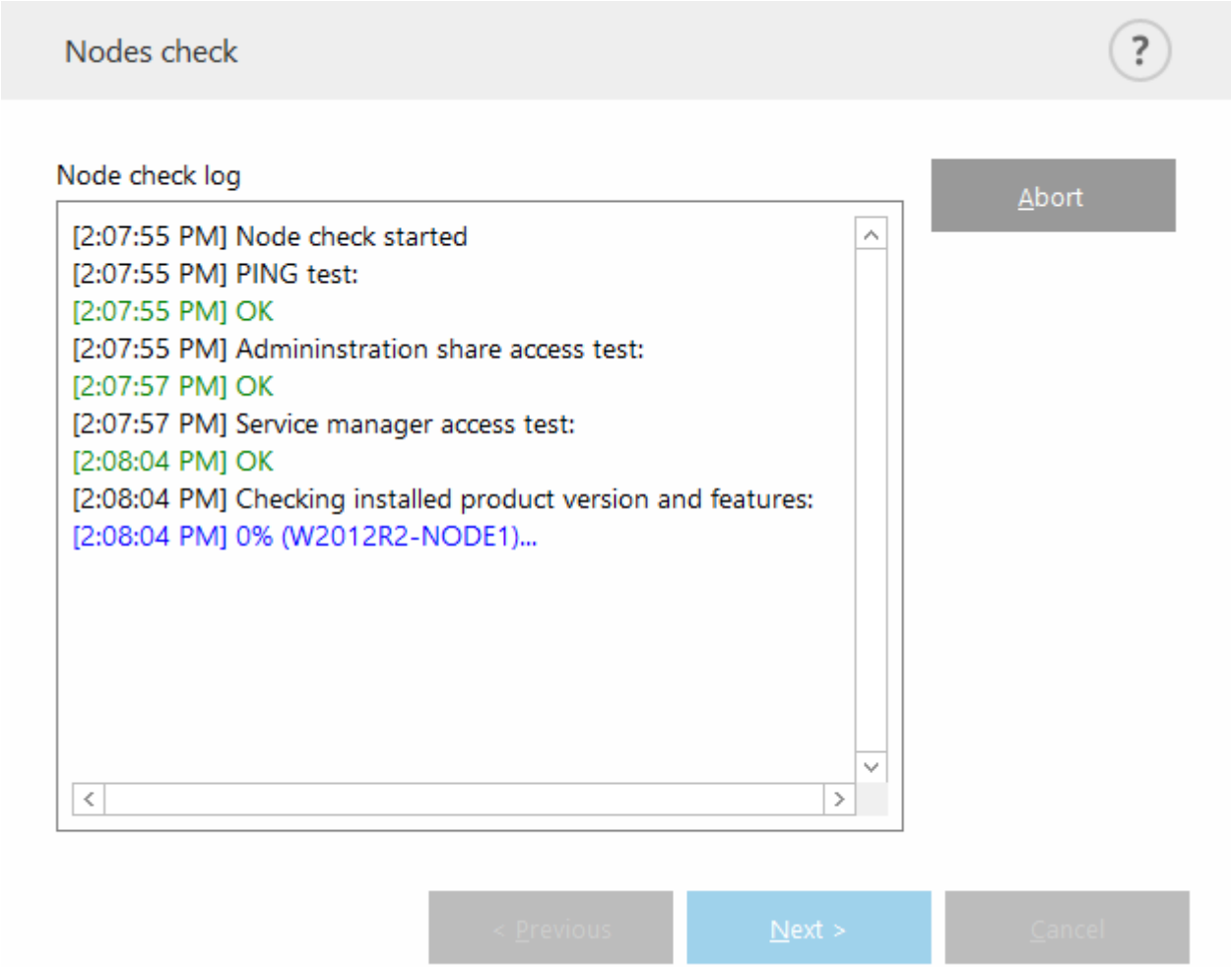
Если выбран этот параметр, ESET Security автоматически активирует решения ESET, которые установлены на узлах и не лицензированы.

> Если необходимо создать кластер ESET с разными архитектурами ОС (32- и 64-разрядная), программу ESET Server Security следует установить вручную. Используемые операционные системы определяются на следующих этапах, и эта информация отображается в окне журнала.

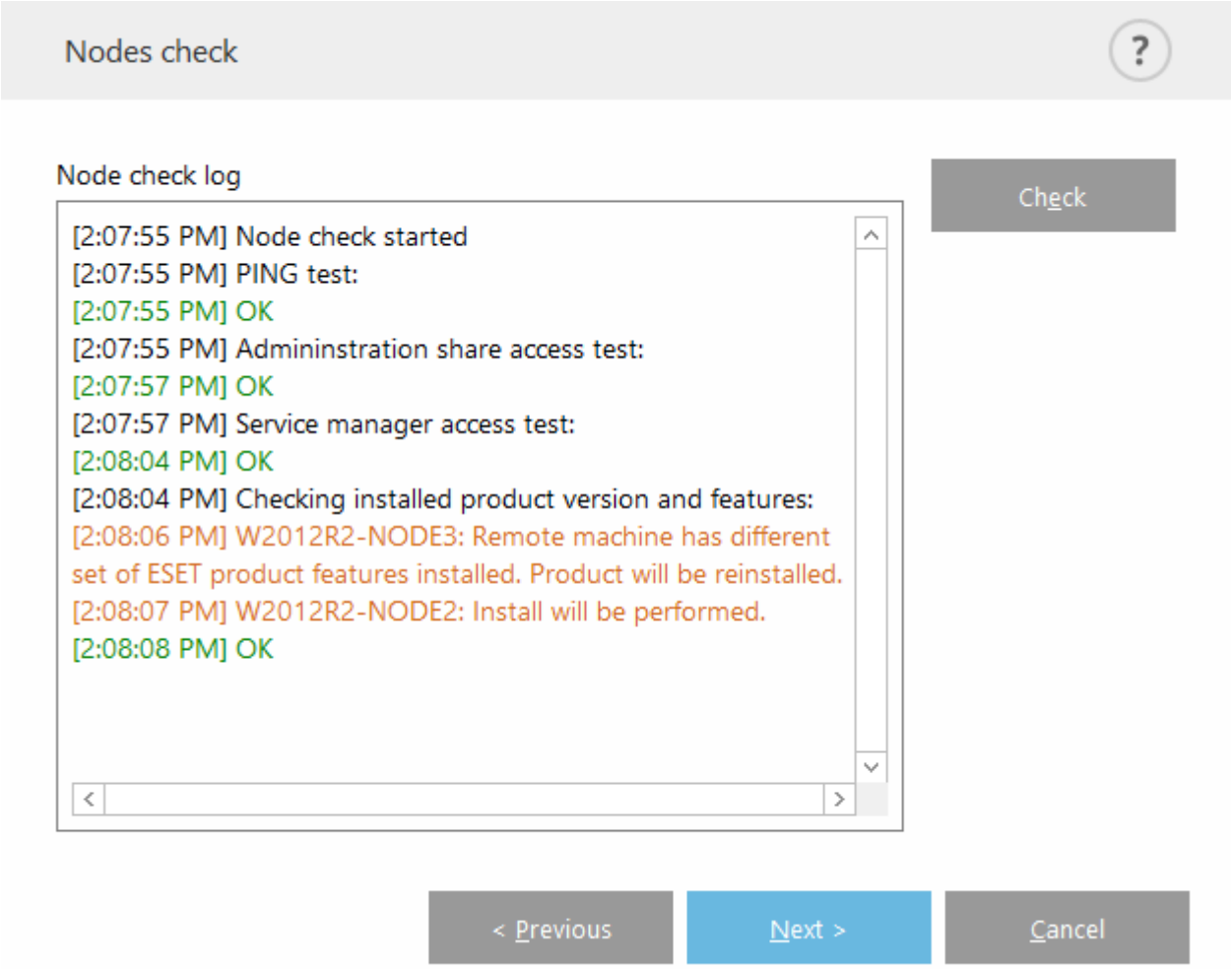
Мастер кластеров — проверка узлов

После указания деталей установки выполняется проверка узлов. В **журнале проверки узла** будут отображены следующие сведения:

- проверка подключения всех существующих узлов к сети;
- проверка доступности новых узлов;
- проверка подключения узла к сети;
- проверка доступности общих ресурсов администратора;
- проверка возможности удаленного выполнения;
- подтверждение правильности установленных версий программы (или того, что программа не установлена);
- проверка наличия новых сертификатов.

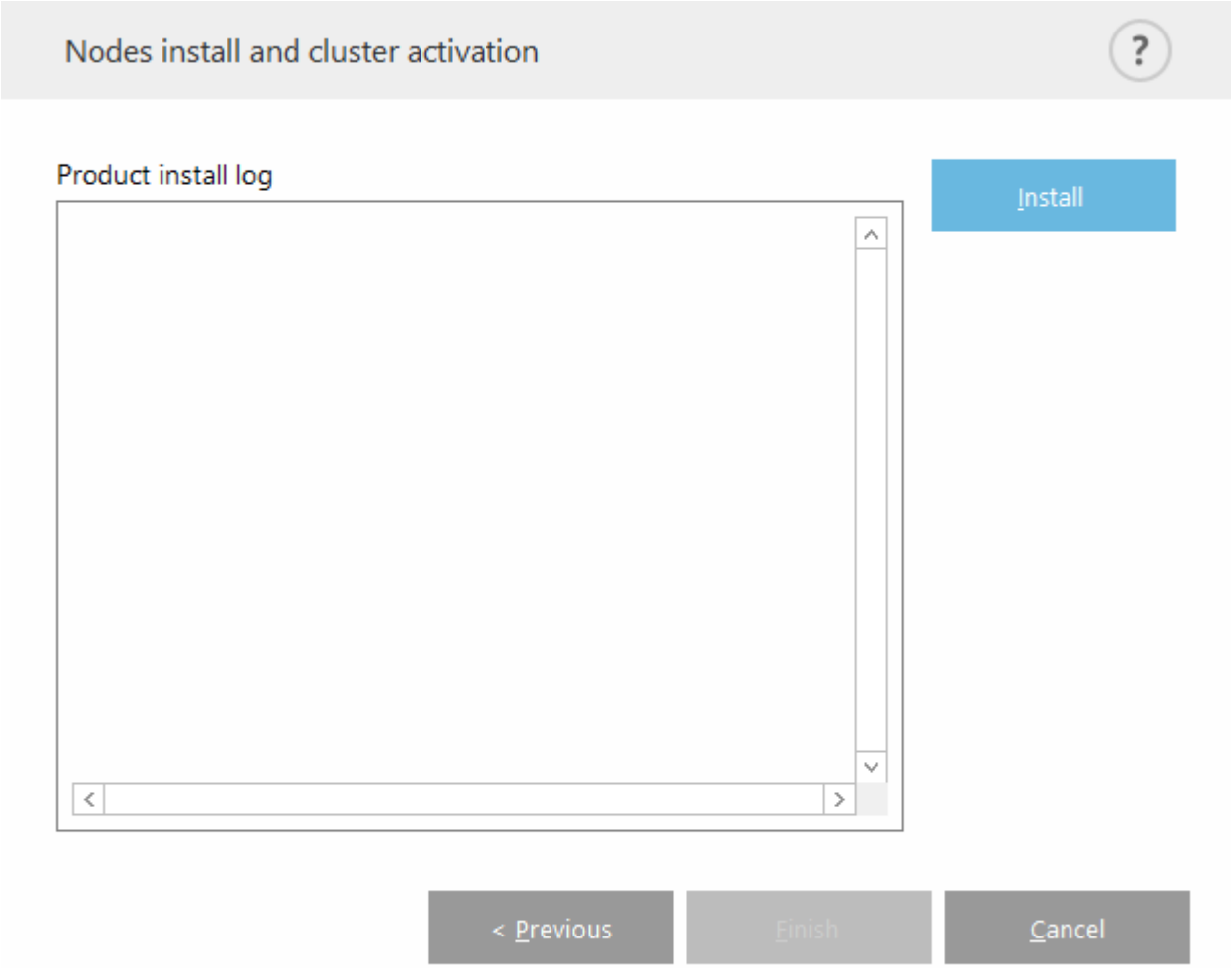


После завершения проверки узлов отобразится следующий отчет.

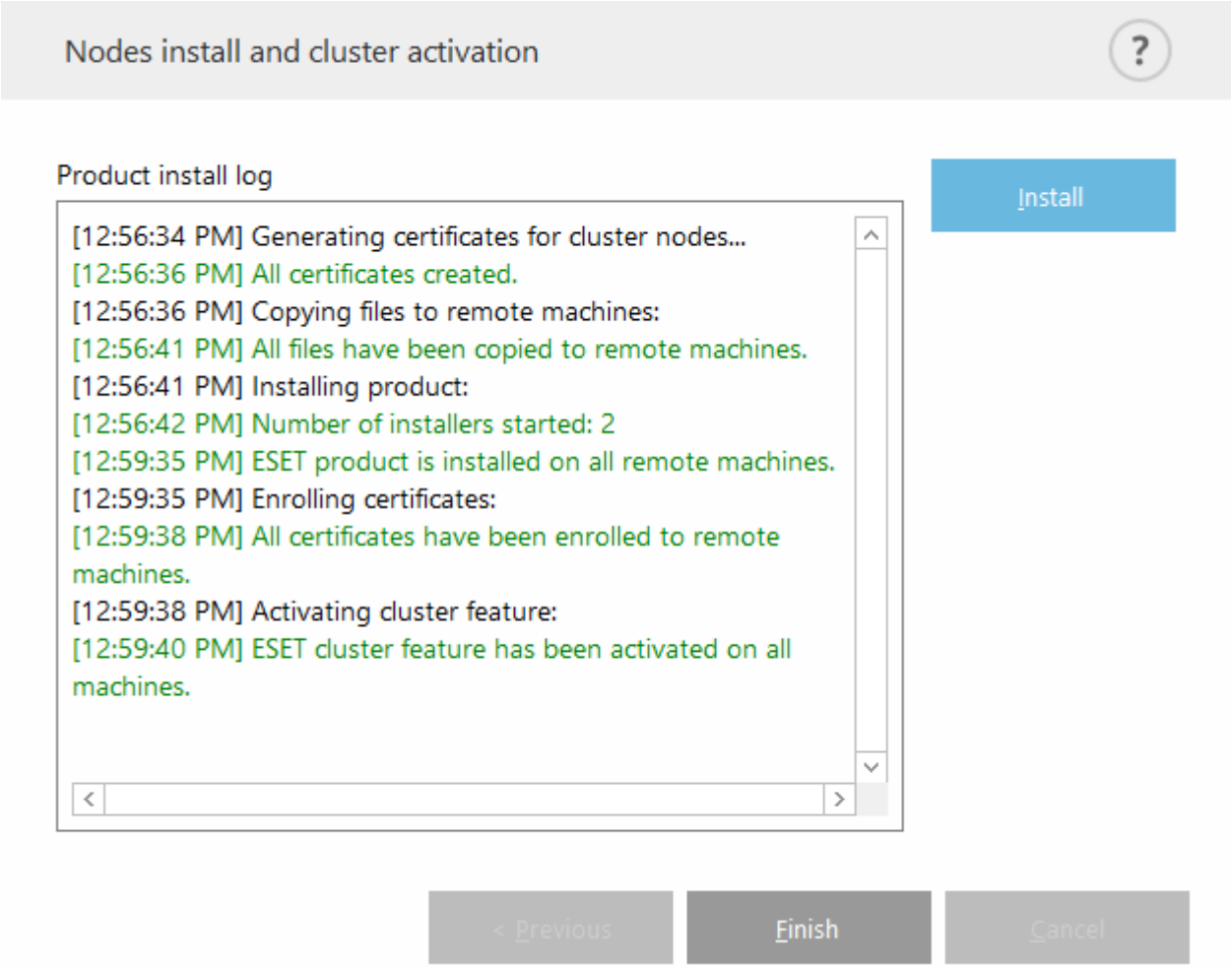


Мастер кластеров — установка узлов

Если установка программы на удаленный компьютер выполняется в процессе инициализации кластера ESET, мастер попытается найти установочный файл в каталоге *%ProgramData%\ESET\ESET Security\Installer*. Если установочный файл не найден в этом каталоге, отображается запрос на поиск его вручную.

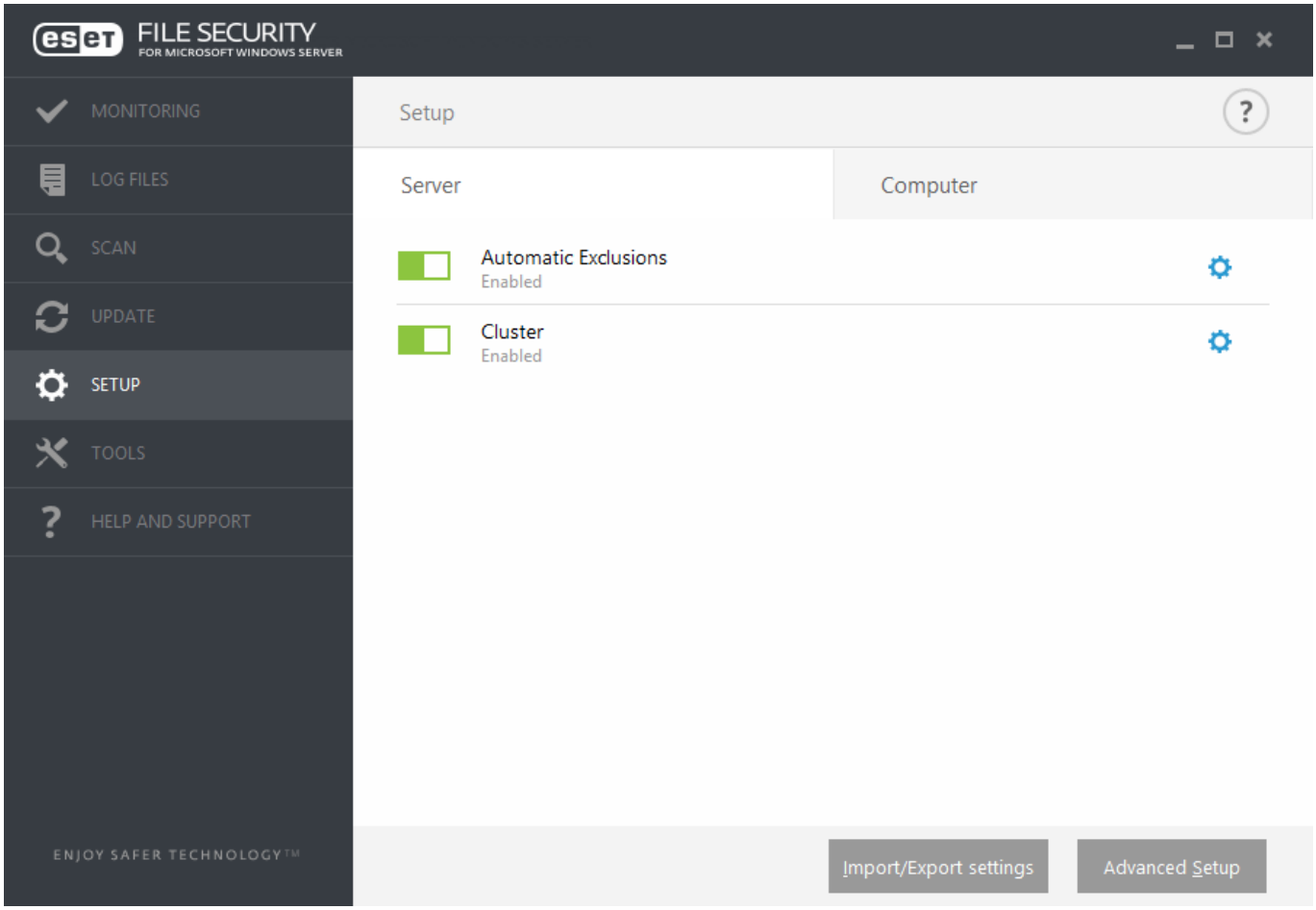


Если выполняется автоматическая удаленная установка на узел с другой архитектурой (конфликт между 32- и 64-разрядной платформами), это будет обнаружено и для такого узла будет предложено выполнить установку вручную.



После правильной настройки кластера ESET он будет отображаться как включенный на странице **Настройка** > **Сервер**.

> Если на некоторых узлах уже установлена более старая версия ESET Server Security, будет выдано уведомление о том, что на эти компьютеры необходимо установить новейшую версию. Обновление программы ESET Server Security может вызвать автоматический перезапуск.



Кроме того, текущее состояние можно проверить на странице состояния кластера (**Сервис** > **Кластер**).

ESET Shell

eShell (сокращение от «ESET Shell») — это интерфейс командной строки для ESET Server Security. Это альтернатива графическому интерфейсу. В eShell есть все функции и возможности, обычно предоставляемые графическим интерфейсом. eShell позволяет конфигурировать и администрировать всю программу, не используя графический интерфейс.

В дополнение ко всем функциям, которые доступны в графическом интерфейсе пользователя, этот интерфейс также предлагает возможности автоматизации за счет выполнения сценариев, которые позволяют конфигурировать, изменять конфигурацию и выполнять какие-либо действия. Кроме того, интерфейс eShell может быть полезен тем пользователям, которые предпочитают командную строку графическому интерфейсу.

> Чтобы получить доступ ко всем функциям, рекомендуется запустить eShell, выбрав пункт Запуск от имени администратора. То же самое рекомендуется сделать при выполнении команды в командной строке Windows (cmd). Откройте командную строку, выбрав пункт Запуск от имени администратора. Если вы не сможете запустить командную строку от имени администратора, вы не сможете выполнять команды из-за отсутствия разрешений.

eShell может запускаться в двух режимах.

1. **Интерактивный режим** полезен, когда нужно именно работать с eShell (а не просто

выполнять одну команду), например при изменении конфигурации, просмотре журналов и т. д. Кроме того, интерактивный режим можно применять, если пользователю еще не знакомы все команды. Интерактивный режим упростит навигацию по интерфейсу eShell. В нем также отображаются доступные команды, которые можно использовать в рамках определенного контекста.

2. **Режим единичной команды/пакетный режим** — этот режим можно использовать, если нужно только выполнить какую-либо команду, не входя в интерактивный режим eShell. Это можно сделать через командную строку Windows. Для этого введите `eshell` и укажите соответствующие параметры.

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

чтобы выполнять некоторые команды (такие как во втором примере вверху) в пакетном режиме или режиме сценария, нужно сконфигурировать определенные параметры. В противном случае появится сообщение **В доступе отказано**. Это нужно из соображений безопасности.

> Изменения настроек необходимы для использования команд eShell в командной строке Windows. Для получения дополнительных сведений о запуске пакетных файлов воспользуйтесь этой ссылкой.

В оболочке eShell войти в интерактивный режим можно двумя способами:

1. Через **меню «Пуск» Windows**: Пуск > Все программы > ESET > ESET File Security > ESET Shell

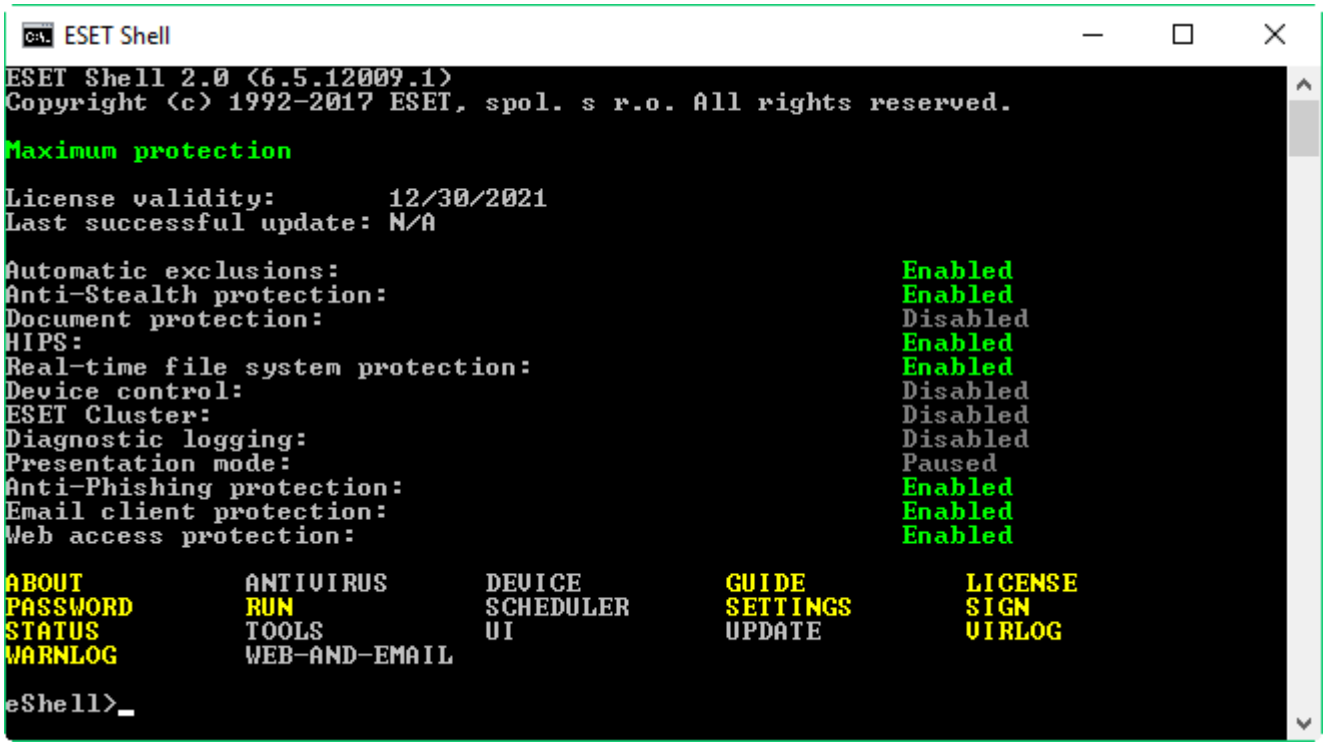
2. Через **командную строку Windows**. Для этого нужно ввести в ней `eshell` и нажать клавишу ВВОД.

> Причиной возникновения ошибки `'eshell' is not recognized as an internal or external command` является то, что ваша система не загрузила новые переменные среды после установки ESET Server Security. Откройте новую командную строку и попробуйте запустить eShell еще раз. Если ошибка не исчезла или у вас остается базовая установка программы ESET Server Security, запустите eShell с применением абсолютного пути, например `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (необходимо использовать кавычки "", чтобы команда работала).

При первом запуске eShell в интерактивном режиме на экран будет выведено окно первого запуска.

> При необходимости в дальнейшем вывести на экран окно первого запуска введите команду `guide`. В нем приводятся основные примеры использования eShell с синтаксисом, префиксами, путями команд, сокращенными формами, псевдонимами и т. д.

При следующем запуске eShell отобразится приведенное ниже окно.



> В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, и это не влияет на их выполнение.

Настройка eShell

Вы можете настроить eShell в контексте `ui eshell`. Вы можете сконфигурировать псевдонимы, цвета, язык, политику выполнения сценариев, настройки скрытых команд и многое другое.

Использование

Синтаксис

Для правильного функционирования команд необходимо соблюдать правильный синтаксис при их форматировании, при этом структура команды может включать в себя префикс, контекст, аргументы, параметры и т. д. Ниже приведен общий синтаксис, используемый в интерфейсе eShell.

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

Пример (команда активирует защиту документов)

`SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

`SET` — префикс

`COMPUTER SCANS DOCUMENT` — путь к конкретной команде, контекст, к которому данная команда относится.

`REGISTER` — непосредственно команда

`ENABLED` — аргумент для команды

Использование ? как аргумента для команды выведет синтаксис непосредственно для этой команды. Например, STATUS ?отображает синтаксис команды STATUS:

СИНТАКСИС

```
[get] status
```

ОПЕРАЦИИ

get — показать состояние всех модулей защиты

Видно, что конструкция [get] заключена в скобки. Это указывает на то, что префикс get используется по умолчанию для команды status. Это означает, что при выполнении команды status без указания префикса используется префикс по умолчанию (в данном случае префиксget status). Использование команд без префиксов позволяет сэкономить время на ввод данных. Обычно get является префиксом по умолчанию для большинства команд, но нужно точно знать префикс по умолчанию для конкретной команды и иметь уверенность в том, что он соответствует задаче, которую необходимо выполнить.

> ℹ В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, и это не влияет на их выполнение.

Префикс/операция

Префикс — это операция. Префикс GET предоставляет сведения о том, как сконфигурирована определенная функция ESET Server Security, или указывает на состояние (например, GET COMPUTER REAL-TIME STATUS покажет текущее состояние защиты модуля в реальном времени). Префикс SET конфигурирует функциональность или меняет состояние (SET COMPUTER REAL-TIME STATUS ENABLED активирует защиту в реальном времени).

Ниже приведены префиксы, которые можно использовать в интерфейсе eShell. Команда может поддерживать или не поддерживать какие-либо из следующих префиксов.

GET	возвращает текущий параметр или состояние
SET	задает значение или состояние
SELECT	выбирается элемент
ADD	добавляется элемент
REMOVE	удаляется элемент
CLEAR	удаляет все элементы или файлы
START	запускается действие
STOP	останавливается действие
PAUSE	приостанавливается действие.
RESUME	возобновляется действие
RESTORE	восстанавливает параметры/объект/файл по умолчанию
SEND	отправляется объект или файл.
IMPORT	выполняется импорт из файла.
EXPORT	выполняется экспорт в файл.

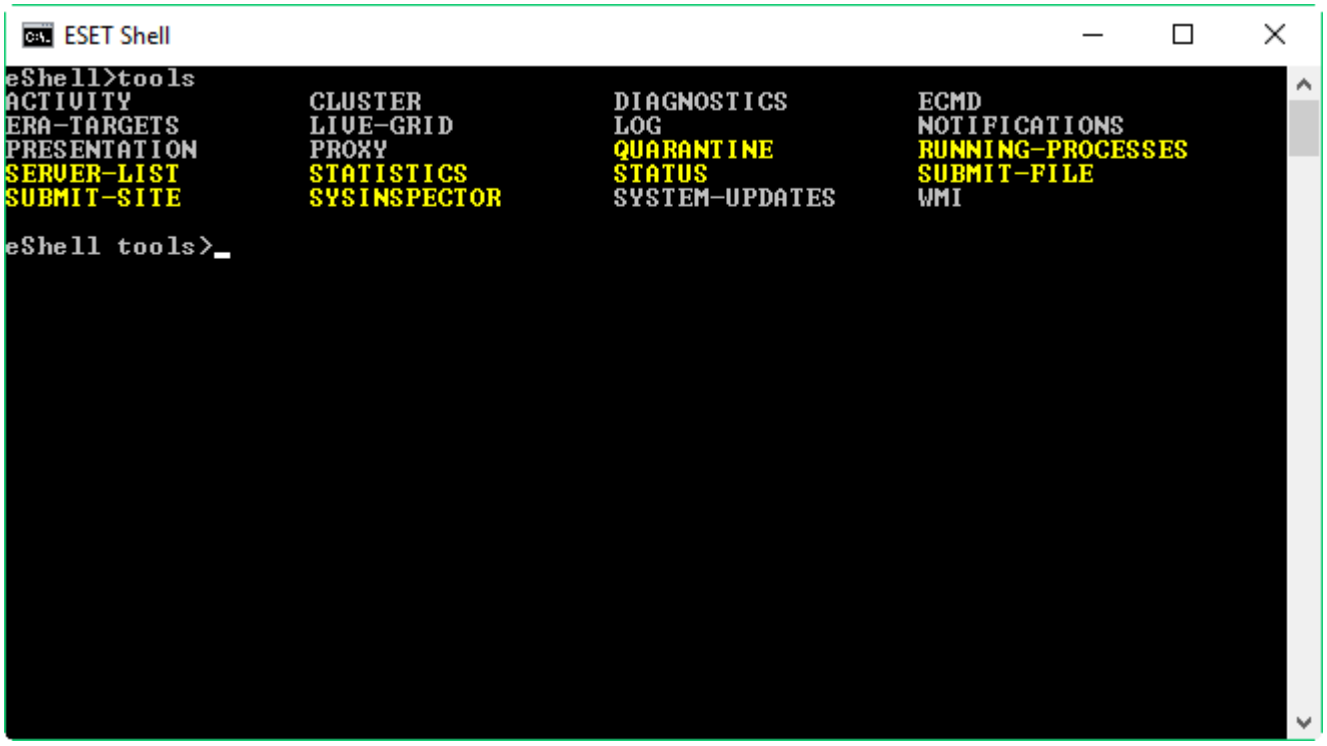
> ℹ Такие префиксы, как GET и SET, используются со многими командами, но в некоторых командах (например, EXIT) префикс не используется.

Путь команды/контекст

Команды размещаются в контекстах, которые образуют древовидную структуру. Верхний уровень древовидной структуры является корневым. При запуске eShell открывается именно корневой уровень.

```
eShell>
```

Можно либо выполнять команды непосредственно здесь или вводить имя контекста, чтобы перемещаться по древовидной структуре. Например, при вводе контекста `TOOLS` на экран будут выведены все команды и подчиненные контексты, доступные в данном контексте.



Желтым цветом обозначены команды, которые можно выполнять, а серым — подчиненные контексты, в которые можно войти. В подчиненном контексте содержатся дальнейшие команды.

Если нужно вернуться на более высокий уровень, следует использовать команду `..` (две точки).

> Допустим, что мы находимся здесь.
> `eShell computer real-time>`
> Введите `..` для перехода вверх на один уровень, на этот:
> `eShell computer>`

Если же необходимо вернуться на корневой уровень с уровня `eShell computer real-time>` (на два уровня ниже корневого уровня), просто введите `.. ..` (две точки, пробел, еще две точки). Это позволит перейти на два уровня вверх, то есть к корневому уровню в данном случае. Чтобы вернуться прямо на корневой уровень с любого уровня (на любой глубине древовидной структуры контекстов), используйте обратную косую черту `\`. Если нужно перейти к какому-либо конкретному контексту верхнего уровня, используйте соответствующее число команд `..` для перехода на необходимый уровень, а в качестве разделителя используйте пробел. Например, если нужно подняться на три уровня вверх, введите `.. .. ..`

Путь указывается относительно текущего контекста. Если команда содержится в текущем контексте, путь вводить не нужно. Например, для выполнения команды `GET COMPUTER REAL-TIME STATUS` введите:

`GET COMPUTER STATUS` — при нахождении в корневом контексте (командная строка показывает eShell>

`GET STATUS` — при нахождении в контексте (командная строка показывает eShell computer>

`.. GET STATUS` — при нахождении в контексте (командная строка показывает eShell computer real-time>

Можно использовать одну `.` (точку) вместо двух `..`, так как одна точка является сокращением для двух.

> ✔ `. GET STATUS` — при нахождении в контексте (командная строка показывает `eShell computer real-time>`

Аргумент

Аргумент — это действие, которое выполняется для конкретной команды. Например, команда `CLEAN-LEVEL` (расположенная в `COMPUTER REAL-TIME ENGINE`) может использоваться со следующими аргументами:

`rigorous` — всегда исправлять обнаружение

`safe` — исправлять обнаружение, если это безопасно, в ином случае не вмешиваться

`normal` — исправлять обнаружение, если это безопасно, в ином случае спрашивать

`none` — всегда спрашивать у конечного пользователя

Другой пример: аргументы `ENABLED` и `DISABLED`, которые используются для включения и отключения определенной функции.

Сокращенная форма/краткие команды

eShell позволяет сокращать контексты, команды и аргументы (при условии, что аргумент является параметром или альтернативным вариантом). Невозможно сократить префикс или аргумент, который является конкретным значением, таким как число, имя или путь. Вы можете использовать цифры`1` и `0`вместо аргументов включения и выключения.

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

Примеры краткой формы

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

Если две команды или контекста начинаются с одних и тех же букв (например, `ADVANCED` и `AUTO-EXCLUSIONS`) и вы введете AA в качестве сокращенной команды, eShell не сможет решить, какую из этих двух команд необходимо выполнить. Поэтому на экран будет выведено

сообщение об ошибке и список команд, начинающихся на букву A, из которого можно выбрать необходимое:

```
eShell>a

The following command is not unique: a
```

В контексте COMPUTER доступны следующие подчиненные контексты:

```
ADVANCED

AUTO-EXCLUSIONS
```

При добавлении одной или нескольких букв (например, AD вместо просто A) eShell введет подчиненный контекст ADVANCED, так как он теперь является уникальным. То же самое касается сокращенных команд.

> Чтобы команда выполнялась надлежащим образом, рекомендуется не сокращать команды, аргументы и т. д., а использовать их полную форму. В этом случае решение eShell будет выполнено именно так, как нужно, и удастся избежать нежелательных ошибок. Это особенно верно для пакетных файлов/сценариев.

Автозаполнение

Эта новая функция была представлена в eShell 2.0, и она очень похожа на функцию автозаполнения в командной строке Windows. В командной строке Windows заполняются пути к файлам, а в eShell заполняются команды, контекст и имена операций. Заполнение аргументов не поддерживается. Чтобы при обычном вводе команды выполнить автозаполнение или просмотреть доступные варианты, нажмите клавишу TAB. Чтобы пролистать варианты назад, нажмите клавиши SHIFT+TAB. Одновременное использование сокращенной формы и автоматического заполнения не поддерживается. Используйте или одно, или другое. Например, если при вводе computer real-time additional нажать клавишу TAB, ничего не произойдет. Эту команду лучше вводить так: введите com, а затем TAB, чтобы завершить computer, затем введите real и нажмите TAB, а затем введите add и опять нажмите TAB. Введите on и снова нажмите TAB. Вы можете просмотреть все доступные варианты: on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default и т. д.

Псевдонимы

Псевдоним — это альтернативное название, которое может использоваться для выполнения команды (при условии, что этой команде присвоен псевдоним). Есть несколько псевдонимов по умолчанию:

(global) close — выход

(global) quit — выход

(global) bye — выход

warnlog — события журнала инструментов

virlog — обнаружения журнала инструментов

Под «(global)» понимается, что такую команду можно использовать в любом месте вне зависимости от текущего контекста. Одной команде может быть назначено несколько псевдонимов. Например, у команды EXIT есть псевдонимы CLOSECLOSE, QUITQUIT и BYEBYE. Для выхода из eShell можно использовать непосредственно команду EXITEXIT или любой из ее псевдонимов. Псевдоним VIRLOGVIRLOG является псевдонимом команды DETECTIONS в контексте TOOLS LOG. Таким образом, команда DETECTIONS доступна из корневого контекста ROOT, что делает ее более доступной (не нужно вводить контекст TOOLS, а затем контекст LOG, и выполнять ее непосредственно в ROOT).

eShell дает пользователям возможность задавать собственные псевдонимы. Команду ALIAS можно найти в контексте UI ESHELL.

Защитить параметры паролем

Параметры ESET Server Security можно защитить паролем. Пароль можно задать с помощью графического интерфейса или в eShell с помощью команды set ui access lock-password.

Для выполнения некоторых команд (например, тех, что изменяют параметры или данные) этот пароль понадобится вводить в интерактивном режиме. Если вы планируете работать в eShell длительное время и не желаете постоянно вводить пароль, решение eShell может запомнить его. Для этого нужно воспользоваться командой set password (выполняется из root). После этого пароль будет вводиться автоматически при каждом выполнении команды, для которой он требуется. Программа eShell помнит пароль, пока вы не вышли из нее. Это значит, что команду set password при запуске нового сеанса нужно будет выполнить еще раз (если нужно, чтобы решение eShell запомнило пароль).

Руководство и справка

При выполнении команды GUIDE или HELP на экран выводится окно первого запуска, в котором объясняется использование eShell. Эта команда доступна в контексте ROOT (eShell>).

История команд

eShell хранит журнал выполненных ранее команд. Это распространяется только на текущий интерактивный сеанс eShell. После завершения сеанса работы eShell журнал команд удаляется. С помощью стрелок вверх и вниз на клавиатуре можно перемещаться по журналу. Обнаружив нужную команду, можно выполнить ее повторно или внести в нее изменения, причем не нужно вводить заново всю команду целиком.

CLS/очистка экрана

CLS можно использовать для очистки экрана. Она работает точно так же, как в командной строке Windows и других аналогичных интерфейсах командной строки.

EXIT / CLOSE / QUIT / BYE

Для того чтобы закрыть eShell или выйти из этого интерфейса, можно воспользоваться любой из этих команд (EXIT, CLOSE, QUIT или BYE).

Команды

В этом разделе приведено несколько основных команд eShell с описаниями.

> ℹ В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, и это не влияет на их выполнение.

Образцы команд (присутствующие в контексте ROOT):

ABOUT

На экран выводятся сведения о программе. Отображается такая информация:

- имя и номер версии установленного решения ESET по обеспечению безопасности;
- операционная система и основные сведения об оборудовании;
- имя пользователя (в том числе домен), полное имя компьютера (полное доменное имя, если сервер входит в домен) и имя рабочего места;
- сведения об установленных компонентах решения ESET по обеспечению безопасности, в том числе номер версии каждого компонента.

ПУТЬ В КОНТЕКСТЕ

```
root
```

PASSWORD

Обычно для выполнения защищенных паролем команд предлагается ввести пароль из соображений безопасности. Это применяется к таким командам, которые отключают защиту или могут повлиять на функциональность ESET Server Security. Пользователю предлагается ввести пароль при каждом выполнении такой команды. Однако можно задать этот пароль, чтобы не вводить его каждый раз. Он будет сохранен в eShell и будет использоваться автоматически при выполнении защищенной паролем команды.

> ℹ Заданный пароль работает только в текущем интерактивном сеансе eShell. После выхода из eShell заданный пароль будет удален. При повторном запуске eShell пароль нужно задать снова.

Заданные пароли можно использовать также при выполнении неподписанных пакетных файлов и сценариев. Выполняя неподписанные пакетные файлы, задайте для политики выполнения ESET Shell значение Полный доступ. Ниже приведен пример такого пакетного файла.

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

Эта соединенная команда задает пароль и отключает защиту.

> Рекомендуется использовать подписанные пакетные файлы всегда, когда возможно, чтобы пароли в пакетных файлах всегда шифровались (при использовании описанного выше способа). Дополнительные сведения см. в разделе Пакетные файлы и сценарии (в подразделе Подписанные пакетные файлы).

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

`[get] | restore password`

`set password [plain <password>]`

ОПЕРАЦИИ

`get` — показать пароль

`set` — задать или очистить пароль

`restore` — очистить пароль

АРГУМЕНТЫ

`plain` — переход ко вводу пароля как параметра

`password` — пароль

ПРИМЕРЫ

`set password plain <yourpassword>` — задается пароль, который будет использоваться для защищенных паролем команд.

`restore password` — очищается пароль

ПРИМЕРЫ

`get password` — эта команда позволяет увидеть, настроен ли пароль (на экран при этом выводятся только символы «звездочка» "*", сам пароль не отображается). Если символов «звездочка» нет, это значит, что пароль не установлен.

`set password plain <yourpassword>`: эта команда позволяет задать пароль.

`restore password` — эта команда очищает заданный пароль

STATUS

Отображает информацию о текущем состоянии защиты ESET Server Security в реальном времени, а также позволяет приостановить или возобновить защиту (аналогично графическому интерфейсу пользователя).

ПУТЬ В КОНТЕКСТЕ

`computer real-time`

СИНТАКСИС

`[get] status`

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

`restore status`

ОПЕРАЦИИ

`get` — возвращается текущий параметр/состояние

`set` — задается значение или состояние

`restore` — восстанавливаются параметры/объект/файл по умолчанию

АРГУМЕНТЫ

`enabled` — включить защиту или компонент

`disabled` — отключить защиту или компонент

`10m` — отключить на 10 минут

`30m` — отключить на 30 минут

`1h` — отключить на 1 час

`4h` — отключить на 4 часа

`temporary` — отключить до перезагрузки

> Отключить все компоненты защиты с помощью одной команды невозможно. Используя команду `status`, можно управлять компонентами и модулями защиты по отдельности. Для каждого компонента или модуля защиты предусмотрена собственная команда `status`.

Список компонентов с командой `status`:

Компонент	Контекст и команда
Автоматические исключения	`COMPUTER AUTO-EXCLUSIONS STATUS`
Система предотвращения вторжений на узел (HIPS)	`COMPUTER HIPS STATUS`
Защита файловой системы в режиме реального времени	`COMPUTER REAL-TIME STATUS`
Контроль устройств	`DEVICE STATUS`
Защита от ботнетов	`NETWORK ADVANCED STATUS-BOTNET`
Защиту от сетевых атак (IDS)	`NETWORK ADVANCED STATUS-IDS`
Изоляция сети	`NETWORK ADVANCED STATUS-ISOLATION`
Кластер ESET	`TOOLS CLUSTER STATUS`
Ведение журнала диагностики	`TOOLS DIAGNOSTICS STATUS`
Режим презентации	`TOOLS PRESENTATION STATUS`
Защита от фишинга	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Защита почтового клиента	`WEB-AND-EMAIL MAIL-CLIENT STATUS`

Компонент	Контекст и команда
Защита доступа в Интернет	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Это псевдоним команды `DETECTIONS`. Эта команда полезна, когда нужно просмотреть информацию об обнаруженных заражениях.

WARNLOG

Это псевдоним команды `EVENTS`. Эта команда полезна, когда нужно просмотреть информацию о различных событиях.

Пакетные файлы и сценарии

Для автоматизации работы решение eShell можно использовать как мощное средство написания сценариев. Чтобы использовать пакетный файл в решении eShell, создайте этот файл, указав в нем слово eShell и команду.

```
✔ eshell get computer real-time status
```

Кроме того, команды можно, а иногда и нужно связывать. Например, если нужно получить определенную запланированную задачу, введите следующее:

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

Выбор элемента (в этом случае это четвертая задача) обычно применяется только к запущенному в это время экземпляру eShell. Если выполнять эти команды одну за другой, выполнение второй команды закончится сбоем и появится сообщение об ошибке «Не выбрано ни одной задачи, или выбранная задача больше не существует».

В целях безопасности по умолчанию для политики выполнения задано значение **Ограниченные сценарии**. Поэтому вы можете использовать решение eShell как инструмент мониторинга, однако не можете изменять конфигурацию ESET Server Security с помощью скриптов. При исполнении сценария, содержащего команды, которые могут нарушить безопасность, например команды отключения защиты, отображается сообщение **Доступ запрещен**. Для исполнения команд, которые вносят изменения в конфигурацию, рекомендуется использовать подписанные пакетные файлы.

Чтобы изменить конфигурацию путем ввода одиночной команды вручную в командной строке Windows, решению eShell необходимо предоставить полный доступ (не рекомендуется). Чтобы предоставить полный доступ, введите команду `ui eshell shell-execution-policy` в интерактивном режиме в eShell или в графическом интерфейсе, выбрав **Расширенные параметры** (**F5**) > **Интерфейс** > Оболочка ESET.

Подписанные пакетные файлы

Решение eShell позволяет защищать обычные пакетные файлы (**.bat*) с помощью подписи. При подписании сценариев используется тот же пароль, что и для защиты настроек. Чтобы подписать сценарий, сначала нужно включить защиту настроек. Это можно сделать с

помощью главного окна программы или в eShell с помощью команды `set ui access lock-password`. Подписывать пакетные файлы можно сразу после установки пароля защиты.

> Если изменен пароль защиты параметров, нужно подписать все сценарии еще раз. В противном случае с момента изменения пароля выполнение сценариев будет заканчиваться неудачей. Пароль, введенный при подписании сценария, должен соответствовать паролю защиты параметров в целевой системе.

Чтобы подписать пакетный файл, выполните команду `sign <script.bat>` из корневого контекста eShell, где *script.bat* — это путь к сценарию, который нужно подписать. Введите и подтвердите пароль, который будет использоваться для подписания. Он должен совпадать с паролем защиты параметров. Подпись ставится в конце пакетного файла в форме комментария. Если сценарий уже подписан, подпись будет заменена на новую.

> При изменении ранее подписанных пакетных файлов подпись нужно ставить еще раз.

Чтобы выполнить подписанный пакетный файл из командной строки Windows или как запланированную задачу, используйте такую команду:

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

В этой команде «script.bat» — это путь к пакетному файлу.

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

ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и собирает подробные сведения о компонентах системы, такие как установленные драйверы и приложения, сетевые подключения и важные записи реестра, а также оценивает уровень риска для каждого компонента.

Эта информация способна помочь определить причину подозрительных действий системы, которые могут быть связаны с несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами.

Щелкните **Создать** и введите краткий **комментарий**, описывающий создаваемый журнал. Дождитесь создания журнала ESET SysInspector (в поле «Состояние» будет показано значение «Создано»). Длительность создания журнала зависит от конфигурации оборудования и системных данных.

В окне ESET SysInspector отображаются следующие данные о созданных журналах.

- **Время**: время создания журнала.
- **Комментарий**: краткий комментарий.
- **Пользователь**: имя пользователя, создавшего журнал.
- **Состояние**: состояние создания журнала.

Доступны перечисленные далее действия.

- **Показать**: открывает созданный журнал. Кроме того, можно щелкнуть журнал правой кнопкой мыши и выбрать в контекстном меню пункт «Показать».

- **Сравнить**: сравнение двух существующих журналов.

- **Создать**: создание журнала. Введите краткий комментарий, описывающий создаваемый журнал, и щелкните **«Создать»**. Дождитесь окончания создания журнала ESET SysInspector (в поле **«Состояние»** будет показано значение Создано).

- **Удалить**: удаление выбранных журналов из списка.

В контекстном меню, которое открывается, если щелкнуть правой кнопкой мыши один или несколько выделенных журналов, доступны перечисленные ниже действия.

- **Показать**: открытие выбранного журнала в ESET SysInspector (аналогично двойному щелчку).

- **Сравнить**: сравнение двух существующих журналов.

- **Создать**: создание журнала. Введите краткий комментарий, описывающий создаваемый журнал, и щелкните **«Создать»**. Дождитесь окончания создания журнала ESET SysInspector (в поле **«Состояние»** будет показано значение Создано).

- **Удалить**: удаление выбранных журналов из списка.

- **Удалить все**: удаление всех журналов.

- **Экспорт**: экспорт журнала в обычный файл *.xml* или заархивированный файл *.xml*.

ESET SysRescue Live

ESET SysRescue Live — это бесплатная утилита, которая позволяет создавать загрузочный компакт-/DVD-диск или USB-накопитель для аварийного восстановления. С загрузочного носителя можно загрузить зараженный компьютер, а затем просканировать его на наличие вредоносных программ и очистить зараженные файлы.

Основным преимуществом ESET SysRescue Live является тот факт, что решение ESET Security работает независимо от операционной системы хоста, но имеет прямой доступ к дисковой и файловой системе. Это позволяет удалить угрозы, которые обычно не могут быть удалены (например, во время работы операционной системы и т. д.).

Планировщик

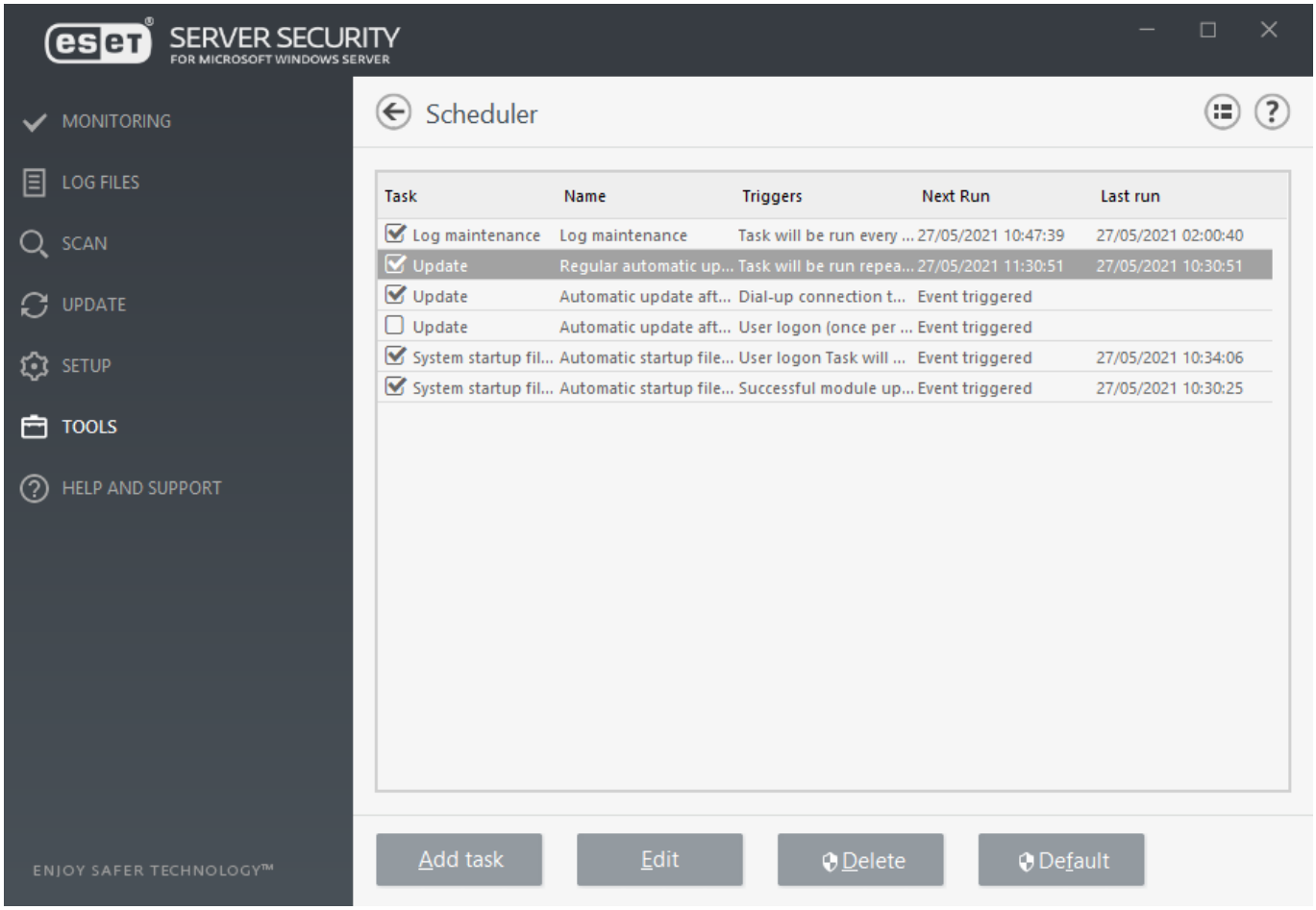
Планировщик управляет запланированными задачами и запускает их выполнение согласно заданным параметрам. Список всех запланированных задач отображается в форме таблицы, в которой указаны их параметры, например тип задачи, ее имя, время запуска и время ее предыдущего выполнения. Кроме того, вы можете создавать новые запланированные задачи, щелкнув Добавить задачу. Чтобы изменить параметры существующей запланированной задачи, нажмите кнопку **Изменить**. Чтобы восстановить параметры по умолчанию для списка

запланированных задач, щелкните **По умолчанию**, а затем **Восстановить параметры по умолчанию**. Это действие приведет к потере всех внесенных изменений без возможности восстановления.

Существует ряд заданных по умолчанию задач.

- Обслуживание журнала
- Регулярное автоматическое обновление (эту задачу можно использовать для обновления частоты)
- Автоматическое обновление после установки модемного соединения
- Автоматическое обновление после входа пользователя в систему
- Автоматическая проверка файлов при запуске системы (после входа пользователя в систему)
- Автоматическая проверка файлов при запуске системы (после выполнения обновления модулей)

Установите соответствующие флажки для активации или отключения задач.



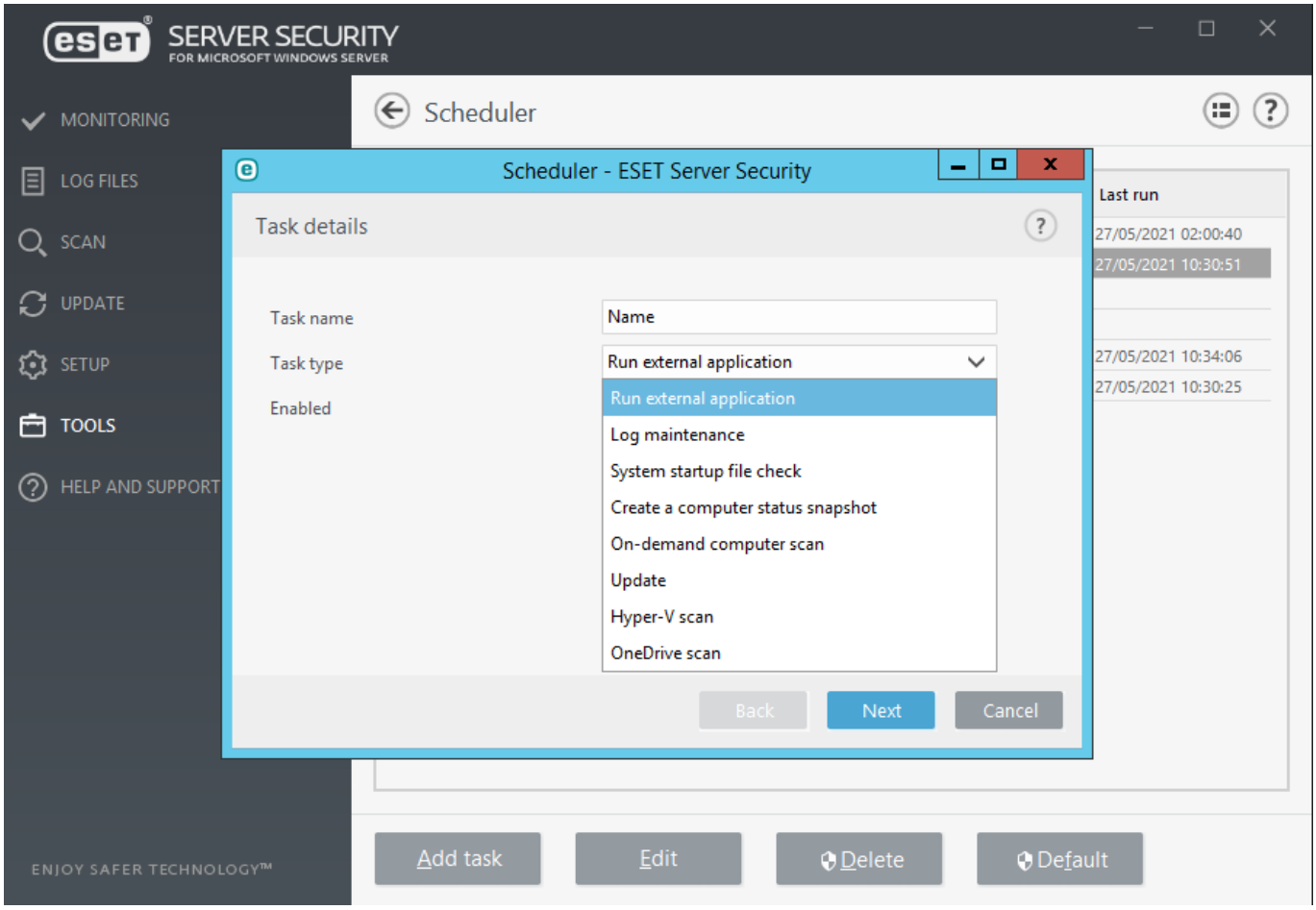
Чтобы выполнить следующие действия, щелкните задачу правой кнопкой мыши.

Показать информацию о задаче	Если запланированную задачу щелкнуть дважды или щелкнуть ее правой кнопкой мыши, отображается подробная информация о ней.
Запустить сейчас	Запустите выбранную задачу планировщика и немедленное ее выполните.
Добавить...	Запускается мастер, с помощью которого можно создать задачу планировщика.
Изменить...	Измените параметры запланированных задач (как определенных по умолчанию, так и пользовательских).
Удалить	Удаление существующей задачи.

Добавление задачи в планировщике

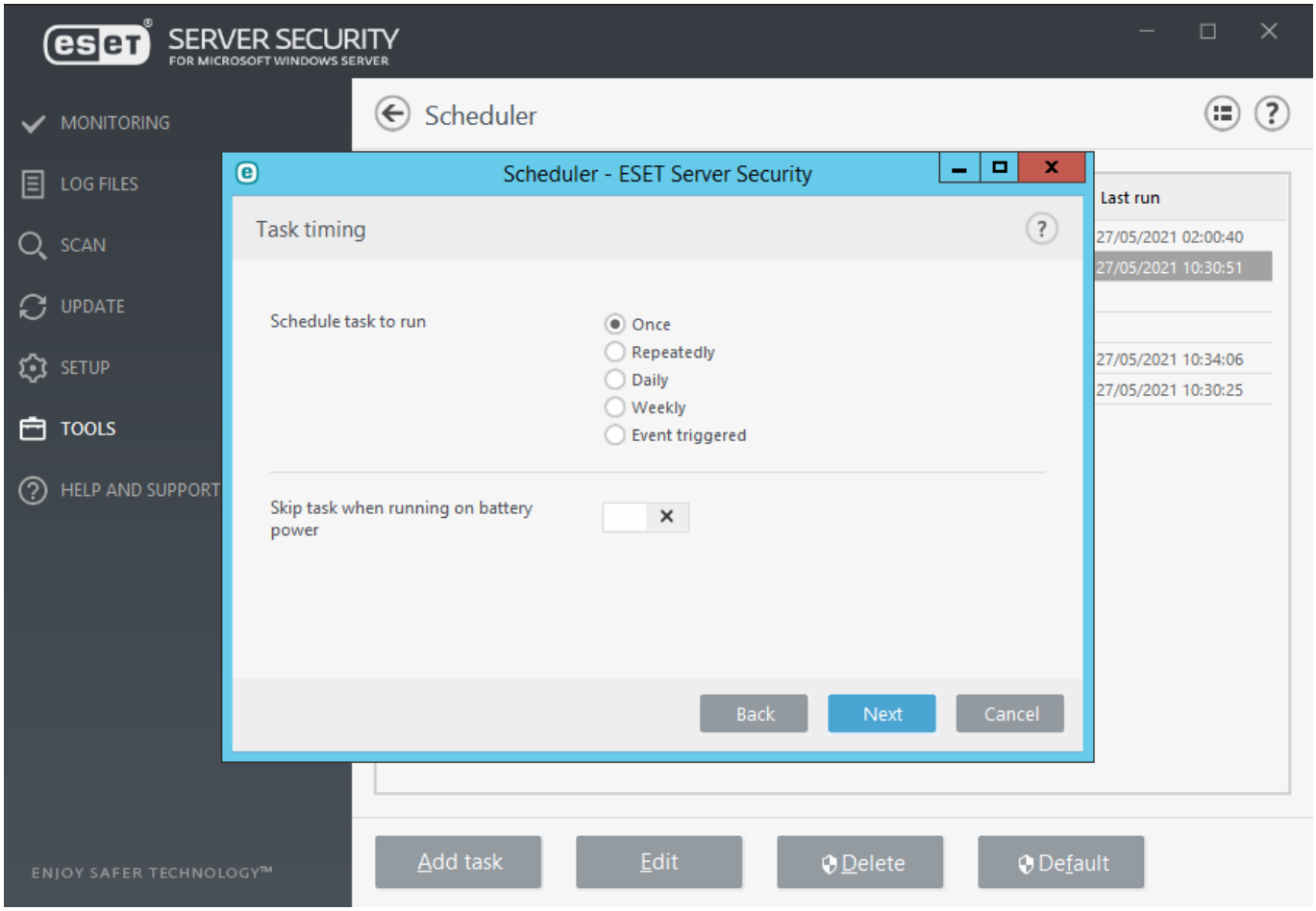
Чтобы создать новую запланированную задачу:

1. Щелкните **Добавить задачу**.
2. Введите **Имя задачи** и настройте задачу, запланированную пользователем.
3. Тип задачи — выберите соответствующий **тип задачи** из раскрывающегося меню.

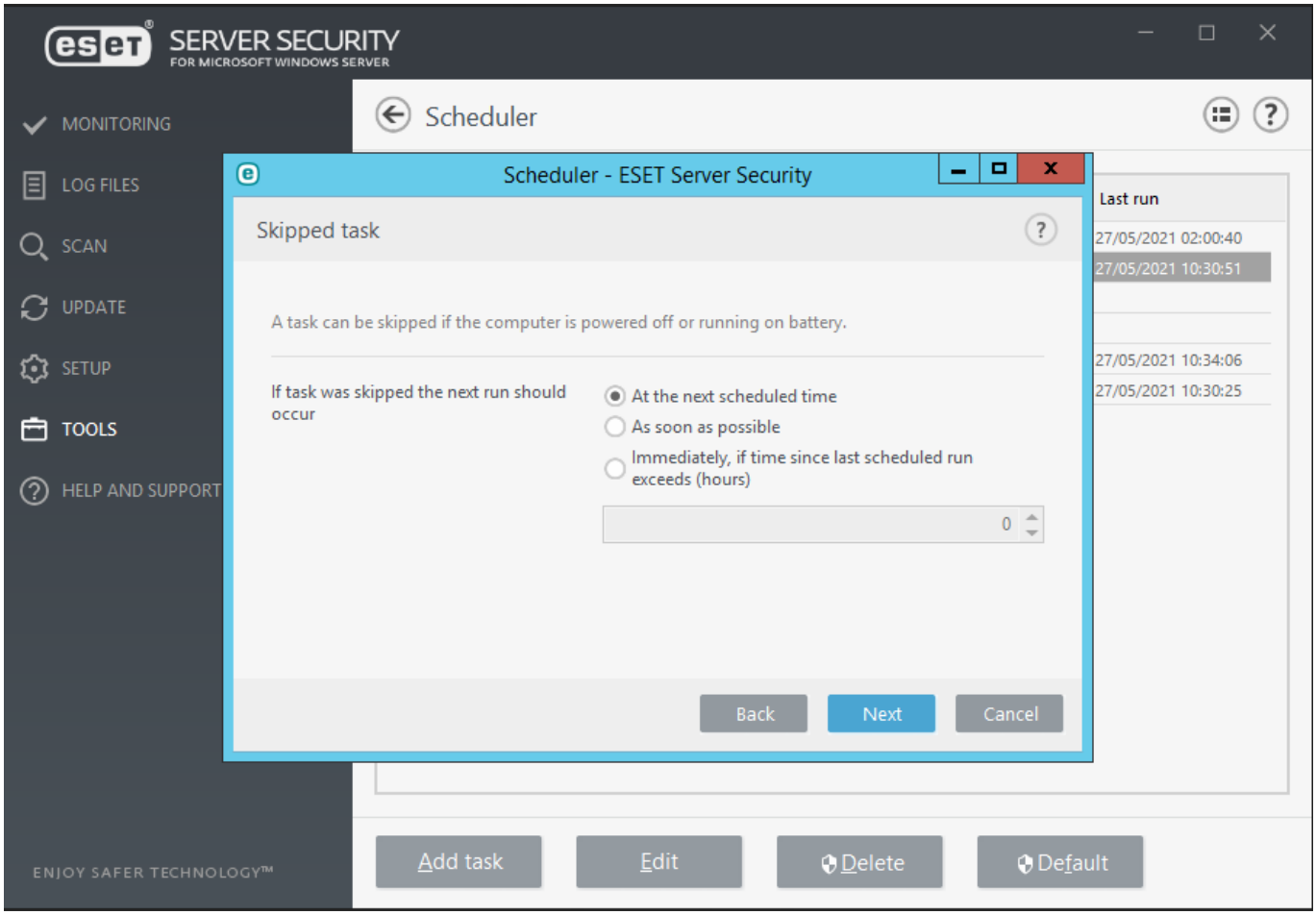


Чтобы отключить задачу, щелкните ползунок возле элемента **Включено**. Чтобы активировать задачу позже, установите соответствующий флажок в представлении планировщика.

4. Время задачи — чтобы определить, когда нужно запустить задачу, выберите один из пунктов. В зависимости от сделанного выбора вам будет предложено выбрать определенное время, день, интервал или событие.



5. Пропущенная задача — если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.



6. Запуск приложения — если в задании запланировано выполнение запуска внешнего приложения, выберите исполняемый файл в дереве каталогов.

7. Если нужно внести изменения, нажмите кнопку **Назад**, чтобы вернуться к предыдущему действию и изменить параметры.

8. Чтобы создать задачу или применить изменения, щелкните **Готово**.

Новая запланированная задача отобразится в представлении планировщика.

Тип задачи

Мастер конфигурации отличается для каждого Типа задачи запланированной задачи. Введите **имя задачи** и выберите в раскрывающемся меню нужный **тип задачи**.

- **Запуск внешнего приложения** — планирование выполнения внешнего приложения.

- **Обслуживание журналов** — в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.

- **Проверка файлов, исполняемых при запуске системы** — проверка файлов, исполнение которых разрешено при запуске системы или входе пользователя в нее.

- **Создать снимок состояния компьютера** — создание снимка состояния компьютера в решении ESET SysInspector, для которого собираются подробные сведения о компонентах

системы (например, о драйверах и приложениях) и оценивается уровень риска для каждого из них.

• **Сканирование компьютера по требованию** — сканирование файлов и папок на компьютере.

• **Обновление** — планирование задачи обновления, в рамках которой обновляются модуль обнаружения и программные модули.

• **Сканирование Hyper-V** — планирование сканирования виртуальных дисков в Hyper-V.

• **Сканирование OneDrive** — планирование сканирования для файлов, которые хранятся в службе OneDrive.

Чтобы отключить задачу сразу после ее создания, щелкните переключатель возле элемента **Включено**. Чтобы активировать задачу позже, установите соответствующий флажок в представлении планировщика. Чтобы перейти к следующему этапу, нажмите кнопку**Далее**.

Время задачи

Выберите один из следующих параметров.

• **Однократно** — задача выполняется один раз в указанные дату и время. Чтобы выполнить задачу только один раз в указанное время, укажите дату и время одноразового выполнения задачи в области **Выполнение задачи**.

• **Многократно** — задача выполняется регулярно через указанный промежуток времени (в минутах). В области **Выполнение задачи** укажите время каждодневного выполнения задачи.

• **Ежедневно** — задача выполняется каждый день в указанное время.

• **Еженедельно** — задача выполняется один или несколько раз в неделю в указанные дни и время. Повторное выполнение задачи возможно только в определенные дни недели, начиная с указанного дня и времени. Укажите время начала в поле «Время» области «Выполнение задачи». Выберите день или дни недели, в которые задача должна выполняться.

• При определенных условиях — задача выполняется при возникновении указанного события.

Пропускать задачу, если устройство работает от аккумулятора — задача не запускается, если на момент ее планируемого запуска система работает от аккумулятора. Например, компьютеры, работающие от источника бесперебойного питания.

При определенных условиях

При планировании задачи по событию пользователь может указать минимальный интервал между двумя окончаниями выполнения задачи.

Задачу может запустить любое из следующих событий:

• При каждом запуске компьютера

• Каждые сутки при первом запуске компьютера

• Модемное подключение к Интернету/VPN

• После успешного обновления модуля

• После успешного обновления программы

• Вход пользователя в систему — задача задействуется при входе пользователя в систему. Если пользователь входит в систему несколько раз в день, укажите 24 часа, чтобы задача выполнялась только при первом входе в систему за сутки, а затем только на следующий день.

• Обнаружение угроз

Запуск приложения

На этой вкладке можно запланировать выполнение внешнего приложения.

• **Исполняемый файл**: выберите исполняемый файл в дереве каталогов, нажмите кнопку обзора (...) или введите путь вручную.

• **Рабочая папка**: задайте рабочий каталог внешнего приложения. Все временные файлы выбранного в поле Исполняемый файл файла будут создаваться в этом каталоге.

• **Параметры** — параметры командной строки для приложения (необязательно).

Пропущенная задача

Если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.

• **В следующее запланированное время**: задача будет выполнена в указанное время (например, через 24 часа).

• **Как можно скорее** — задача будет выполнена при первой возможности, когда условия, предотвращающие ее выполнение, перестанут действовать.

• **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** — Время с момента последнего запуска (ч) — после выбора этих параметров задача всегда будет повторяться через указанный период времени (в часах).

Обзор запланированных задач

В этом диалоговом окне отображается подробная информация о **запланированной задаче**. Чтобы его открыть, дважды щелкните задачу в представлении **планировщика или щелкните ее правой кнопкой мыши и выберите пункт Показать информацию о задаче**.

Отправка образцов на анализ

Диалоговое окно отправки образцов позволяет отправить файл или сайт на анализ в ESET. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в вирусную лабораторию ESET. Если файл окажется вредоносным приложением или веб-сайтом, обнаружение будет включено в последующие обновления.

Чтобы отправить файлы по электронной почте, заархивируйте их с помощью программ, например, WinRAR или WinZip, защитите архив паролем `infected` и отправьте архив по адресу samples@eset.com. Помните, что тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, адрес веб-сайта, с которого он был загружен).

Прежде чем отправлять образец в компанию ESET, убедитесь, что он соответствует как минимум одному из следующих критериев:

- файл или веб-сайт совсем не обнаруживается;
- файл или веб-сайт неправильно обнаруживается как угроза.

Если не выполняется хотя бы одно из указанных выше требований, необходимо отправить дополнительную информацию, чтобы получить ответ.

В раскрывающемся меню **Причина отправки образца** выберите наиболее подходящее описание своего сообщения:

- подозрительный файл;
- подозрительный сайт (веб-сайт, зараженный вредоносной программой);
- ложное срабатывание файл (файл обнаружен как зараженный, хотя не является таковым);
- ложное срабатывание сайт;
- другое.

Файл или сайт

Путь к отправляемому на анализ файлу или веб-сайту.

Контактный адрес электронной почты

Контактный адрес электронной почты отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать контактный адрес электронной почты не обязательно. Поскольку каждый день на серверы ESET поступают десятки тысяч файлов, невозможно отправить ответ на каждый запрос. Вам ответят только в том случае, если для анализа потребуется дополнительная информация.

Отправить анонимно

Чтобы отправить подозрительный файл или веб-сайт без ввода контактного адреса электронной почты, установите флажок рядом с надписью **Отправить анонимно**.

подозрительный файл;

Обнаруженные признаки и симптомы заражения вредоносной программой

Введите описание поведения подозрительного файла, наблюдаемого на компьютере.

Источник файла (URL-адрес или поставщик)

Укажите источник файла и опишите, как он попал на компьютер.

Примечания и дополнительная информация

Здесь можно ввести дополнительную информацию или описание, которые помогут идентифицировать подозрительный файл.

> Хоть требуется заполнять только первое поле (**Обнаруженные признаки и симптомы заражения вредоносной программой**), дополнительная информация является существенным подспорьем при идентификации образцов в лаборатории.

Подозрительный сайт

В раскрывающемся меню Что не так с этим сайтом выберите один из следующих пунктов.

Заражено

Веб-сайт содержит вирусы или другие вредоносные программы, которые распространяются различными способами.

Фишинг

Часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п. Дополнительную информацию об этом типе атаки см. в глоссарии.

Мошеннический

Мошеннический веб-сайт.

другое.

Используйте этот параметр, если ни один из вышеперечисленных вариантов не применяется к сайту, который вы собираетесь отправить.

Примечания и дополнительная информация

Здесь можно ввести дополнительную информацию или описание, которые помогут проанализировать подозрительный сайт.

Ложное срабатывание файл;

Мы просим отправлять файлы, которые обнаруживаются как зараженные, но при этом не являются таковыми, чтобы мы могли улучшить наш модуль обнаружения и обеспечить защиту другим пользователям. Ложное срабатывание возможно, когда графический ключ файла совпадает с таким же графическим ключом, присутствующим в модуле обнаружения.

> i Три параметра обязательно нужно указать, чтобы идентифицировать нормальные приложения и отличить их от вредоносного кода. Предоставление дополнительной информации в значительной степени помогает лаборатории в процессе идентификации и обработки образцов.

Имя и версия приложения

Наименование программы и ее версия (например, номер, псевдоним или кодовое название).

Источник файла (URL-адрес или поставщик)

Укажите источник файла и опишите, как он попал на компьютер.

Цель приложения

Это общее описание приложения, его типа (например, браузер, проигрыватель мультимедиа и т. п.) и функциональности.

Примечания и дополнительная информация

Здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного файла.

Ложное срабатывание сайт

Мы просим отправлять нам сведения о сайтах, которые определены как зараженные, мошеннические или фишинговые, но таковыми не являются. Ложное срабатывание возможно, когда шаблон сайта совпадает с таким же шаблоном, присутствующим в модуле обнаружения. Отправьте нам сведения о таком веб-сайте, чтобы мы могли улучшить наш модуль обнаружения и обеспечить защиту для других пользователей.

Примечания и дополнительная информация

Здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного файла.

другое.

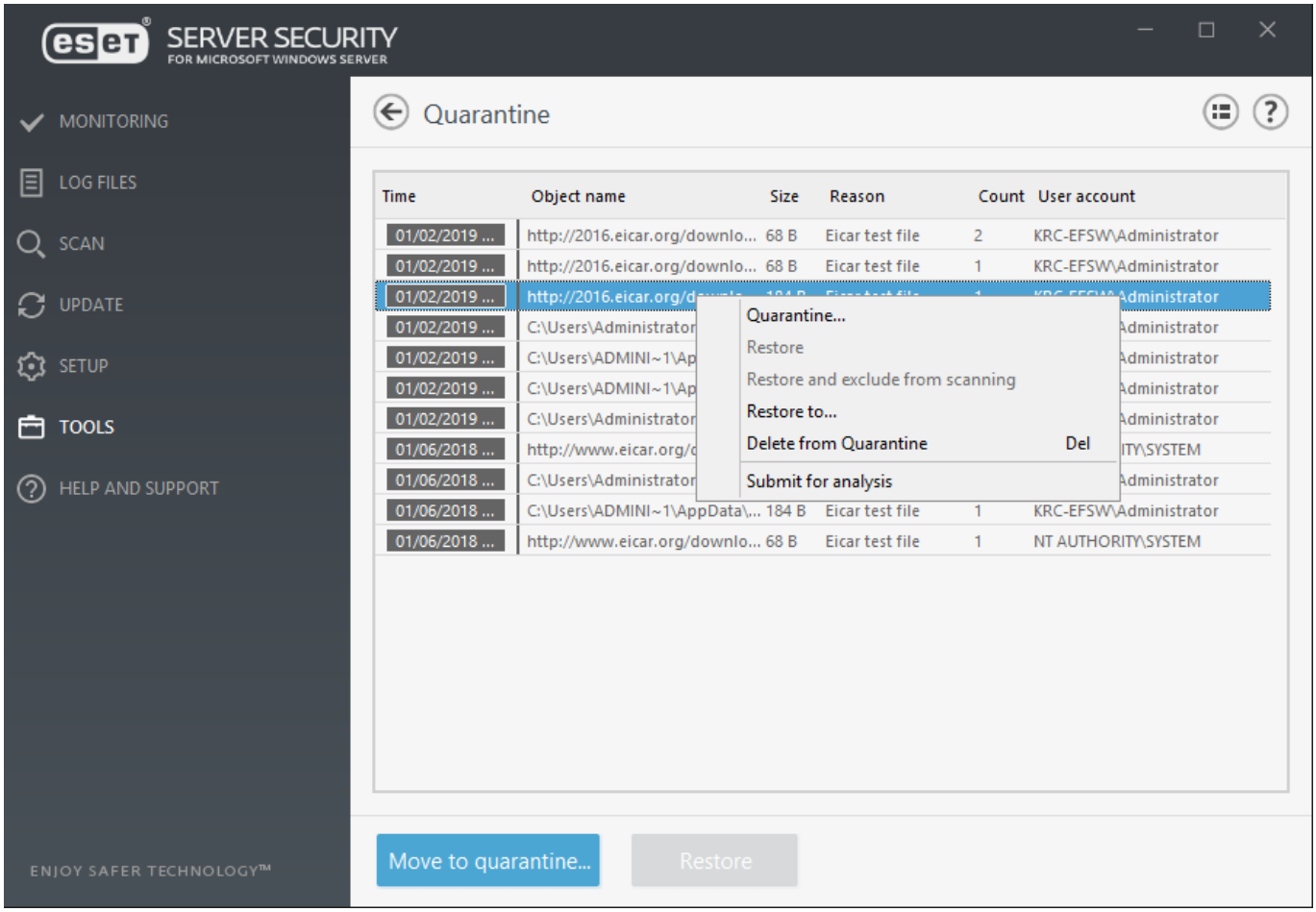
Этот вариант следует использовать, если файл невозможно отнести к категории Подозрительный файл или Ложное срабатывание.

Причина отправки файла

Введите детальное описание и причину отправки файла.

Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя очистить или безопасно удалить, либо если они отнесены программой ESET Server Security к зараженным по ошибке. Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не обнаруживаются модулем сканирования защиты от вредоносных программ. Файлы на карантине можно отправить в вирусную лабораторию ESET на анализ.



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, в которой указаны дата и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причина помещения файла на карантин (например, объект добавлен пользователем) и количество угроз (например, если архив содержит несколько заражений).

В случае помещения объектов сообщений электронной почты в файловый карантин, отображается путь к почтовому ящику/папке/имени файла.

Помещение файлов на карантин

Программа ESET Server Security автоматически помещает удаленные файлы в карантин (если этот параметр не был отменен пользователем в окне предупреждения). Любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин**. При помещении на

карантин файл удаляется из своего исходного расположения. Для этого также можно воспользоваться контекстным меню, щелкнув правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Команда **Восстановить** доступна в контекстном меню, которое открывается правым щелчком мыши нужного файла в окне «Карантин». Если файл помечен как потенциально нежелательное приложение , будет доступен пункт **Восстановить и исключить из сканирования**. Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в месте, отличном от исходного.

> Если программа поместила незараженный файл на карантин по ошибке, после восстановления исключите этот файл из процесса сканирования и отправьте его в службу поддержки клиентов ESET.

Отправка файла из карантина

Если на карантин помещен файл, который не распознан программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода), а затем помещен на карантин, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт Передать на анализ.

Удаление из карантина

Щелкните элемент правой кнопкой мыши и выберите команду **Удалить из карантина** или выберите нужный элемент и нажмите клавишу **Удалить** на клавиатуре.

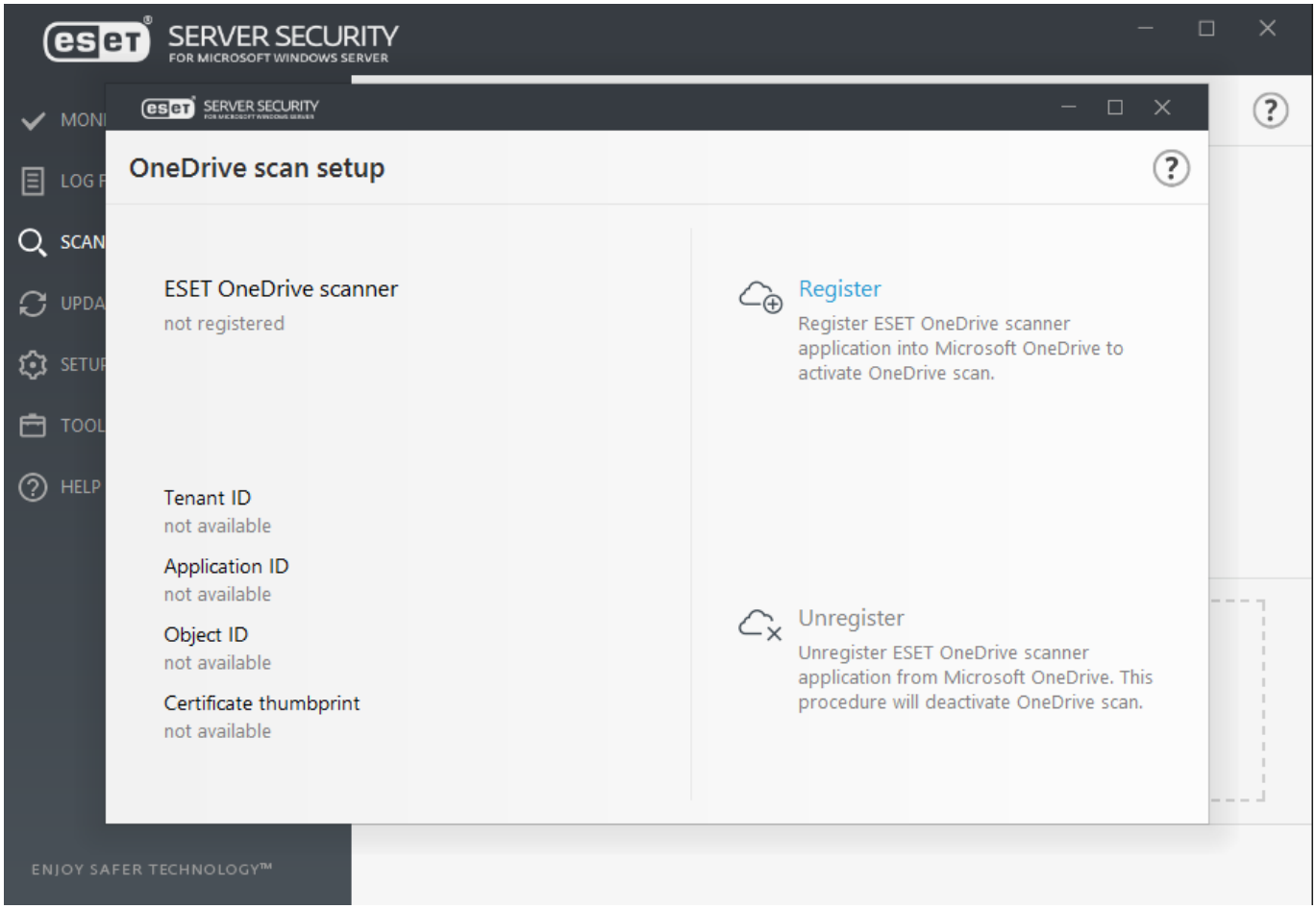
Настройка сканирования OneDrive

С помощью этой функции можно сканировать файлы, хранящиеся в облачном хранилище Microsoft OneDrive для бизнеса. Модуль сканирования ESET Server Security OneDrive обрабатывает только файлы и папки. Другие типы данных, например сообщения электронной почты, файлы SharePoint, контакты или календари, не сканируются.

Быстрые ссылки:

- Регистрация модуля сканирования ESET OneDrive
- Отмена регистрации модуля сканирования ESET OneDrive

Перед началом работы с функцией сканирования ESET Server Security OneDrive, зарегистрируйте приложение для модуля сканирования ESET OneDrive в Microsoft OneDrive, Microsoft Office 365 или Microsoft Azure. На странице настройки функции сканирования OneDrive отображаются сведения о состоянии регистрации. Если регистрация уже выполнена, там будут отображаться такие сведения о регистрации, как идентификатор клиента, идентификатор приложения, идентификатор объекта и отпечаток сертификата. Вы можете выполнить или отменить регистрацию модуля сканирования ESET OneDrive.



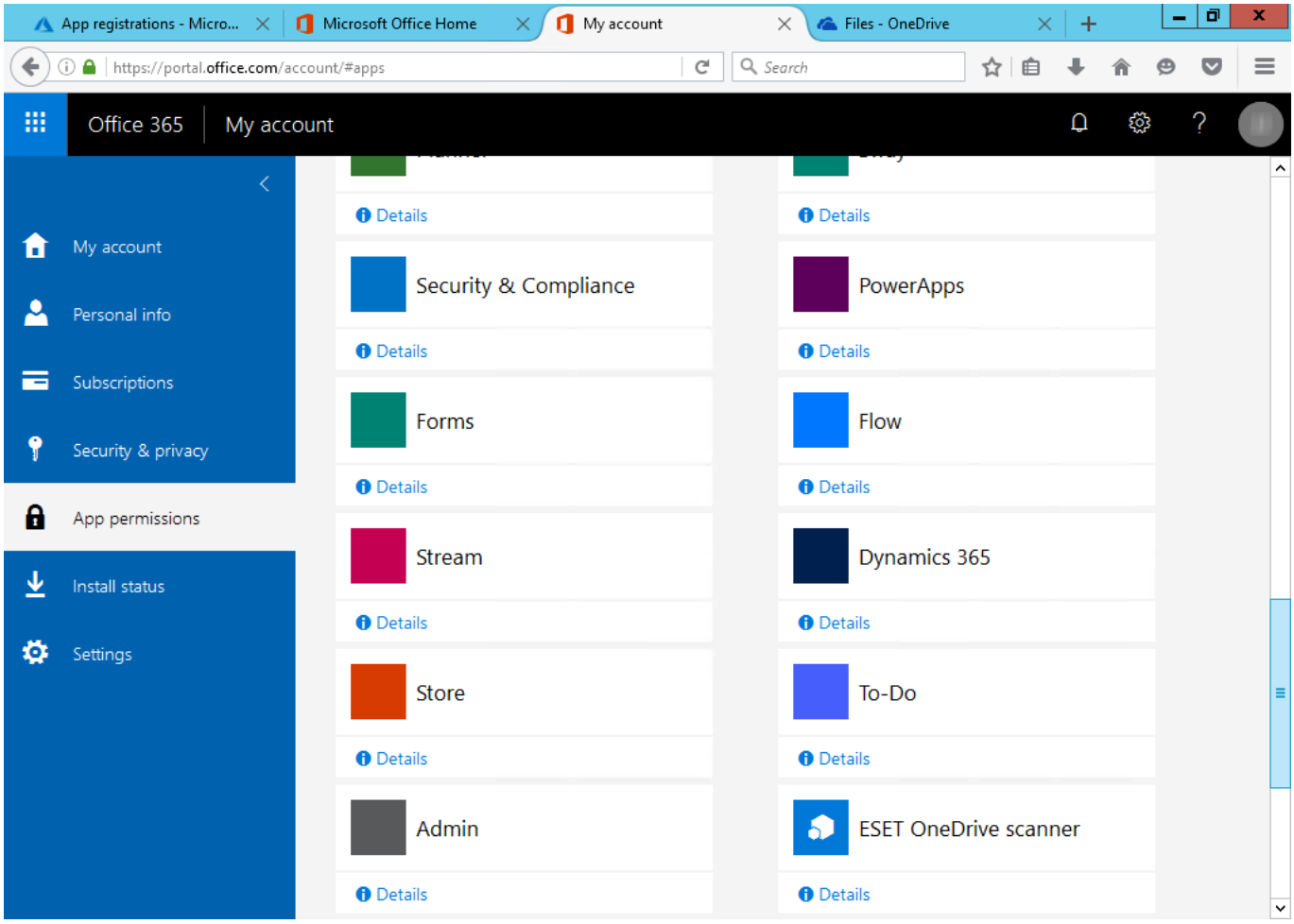
По завершении регистрации функция сканирования OneDrive будет доступна в меню Сканирование, в котором отображается список пользователей, а также структура их папок и файлы, которые доступны для сканирования. Функция сканирования ESET Server Security OneDrive может сканировать любые файлы пользователей в хранилище OneDrive для бизнеса.

> Функция сканирования ESET Server Security OneDrive загружает файлы из облачного хранилища OneDrive для бизнеса и сканирует их локально. По завершении сканирования загруженные файлы удаляются. Загрузка большого объема данных из хранилища OneDrive увеличивает сетевой трафик.

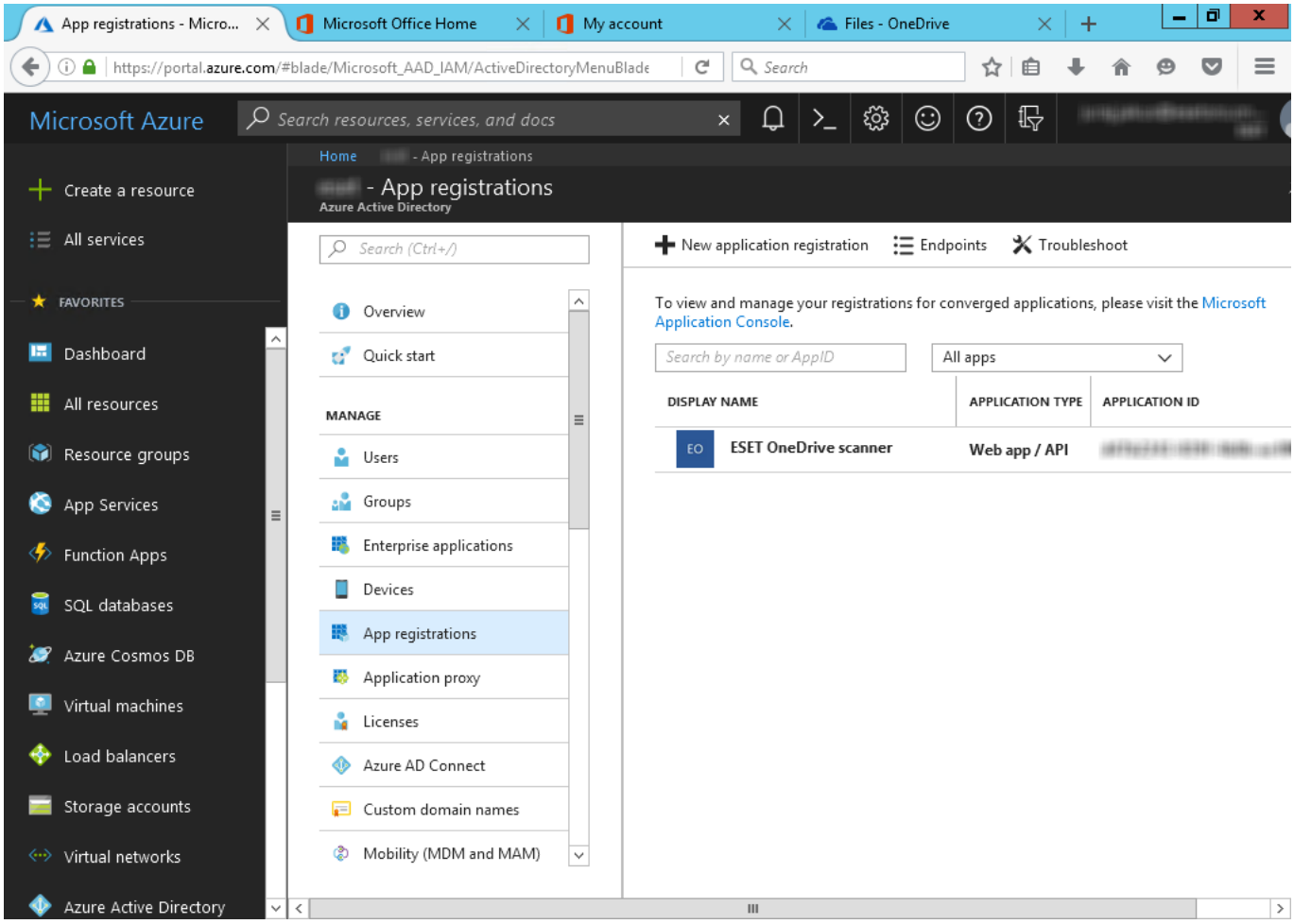
> Повторите регистрацию в другой учетной записи. Чтобы зарегистрировать модуль сканирования ESET Server Security OneDrive в новой учетной записи Microsoft OneDrive для бизнеса или Office 365, необходимо отменить регистрацию модуля сканирования ESET OneDrive, который использовался в предыдущей учетной записи, и зарегистрировать его в новой учетной записи, используя учетные данные администратора Microsoft OneDrive для бизнеса или Office 365.

Чтобы найти модуль сканирования ESET OneDrive, зарегистрированный как приложение, на порталах Office 365 и Azure выполните следующие действия.

Портал Office 365: На странице вашей учетной записи щелкните **App permissions** (Разрешения для приложений), после чего в списке приложений отобразится модуль сканирования ESET OneDrive.



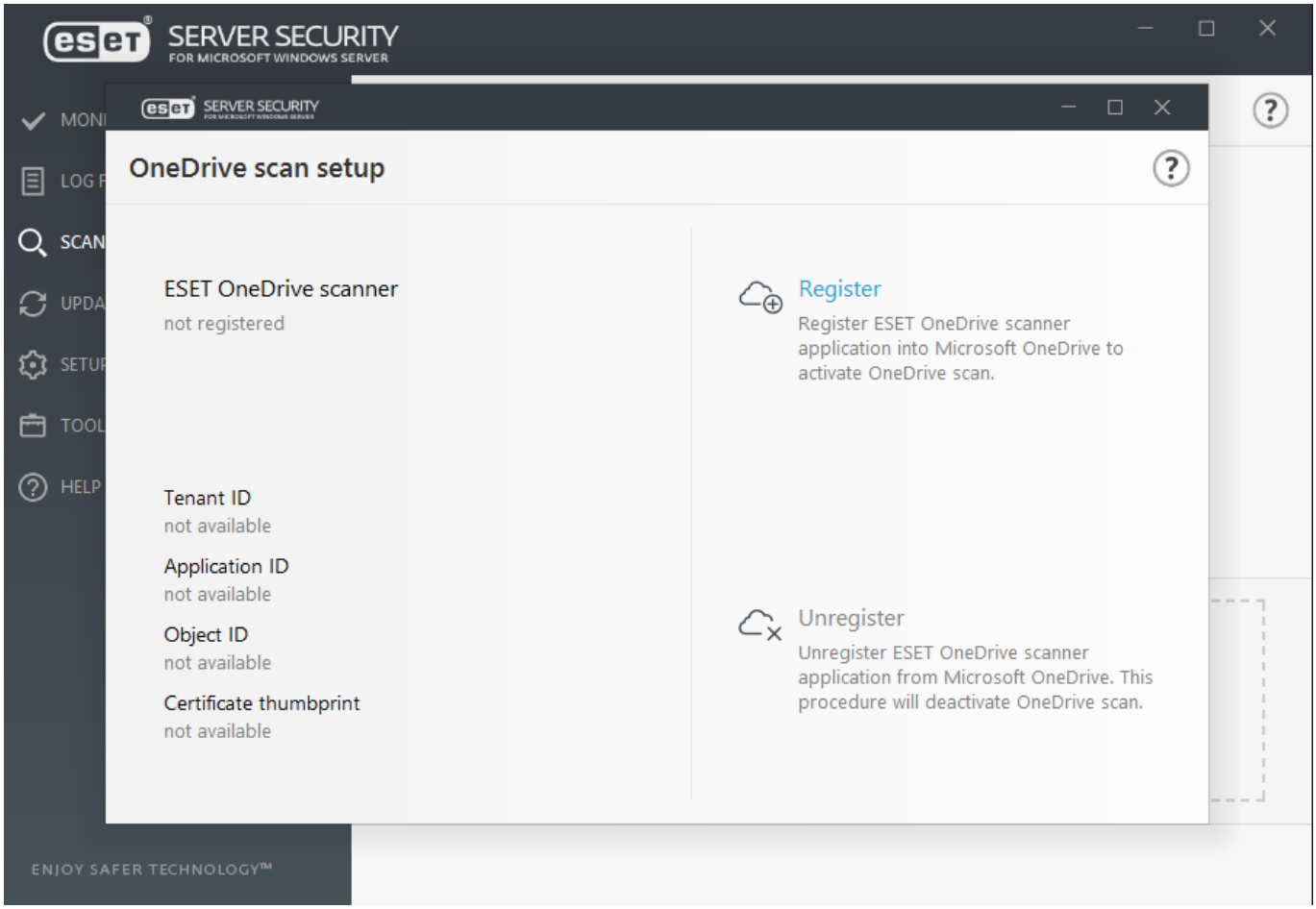
Портал Azure: Откройте **Azure Active Directory** > **App registrations** (Регистрация приложений) и щелкните **View all applications** (Просмотреть все приложения). В списке приложений отобразится модуль сканирования ESET OneDrive. Щелкните приложение, чтобы просмотреть сведения о нем.



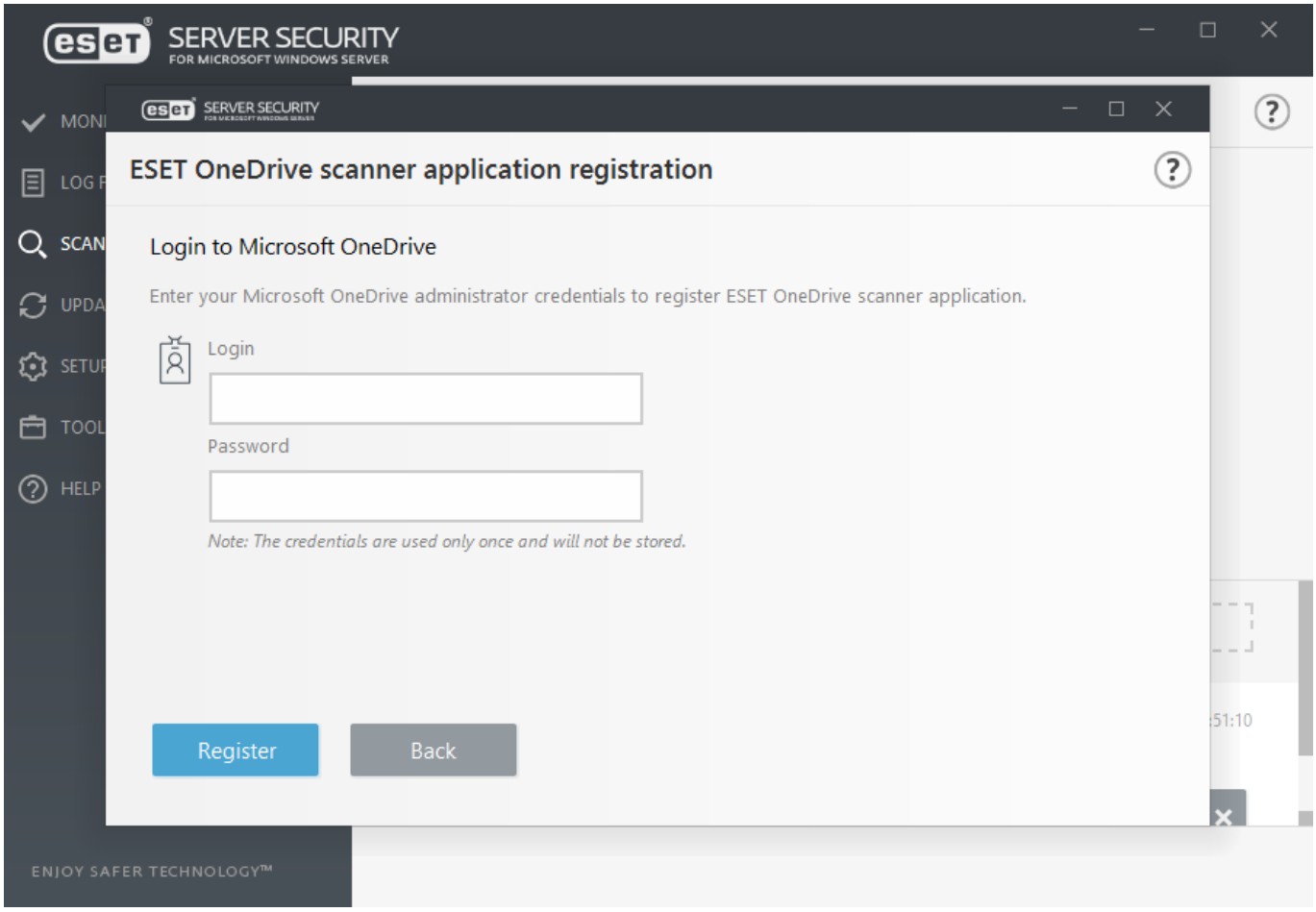
Регистрация модуля сканирования ESET OneDrive

Ниже описана процедура регистрации приложения для модуля сканирования ESET OneDrive в Microsoft OneDrive, Office 365 и Azure.

1. Щелкните **Зарегистрировать**, чтобы открыть мастер регистрации и приступить к регистрации модуля сканирования ESET OneDrive.

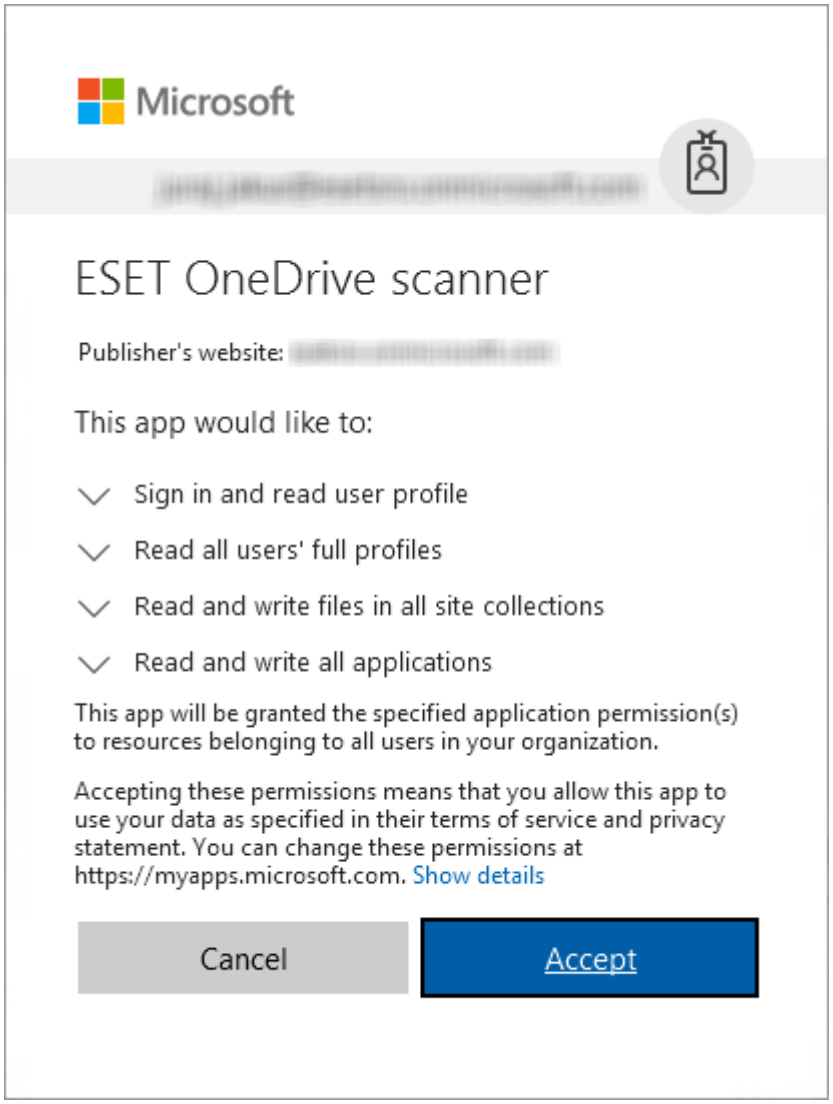


2. Введите учетные данные администратора Microsoft OneDrive или Office 365. Дождитесь завершения регистрации приложения в Microsoft OneDrive.



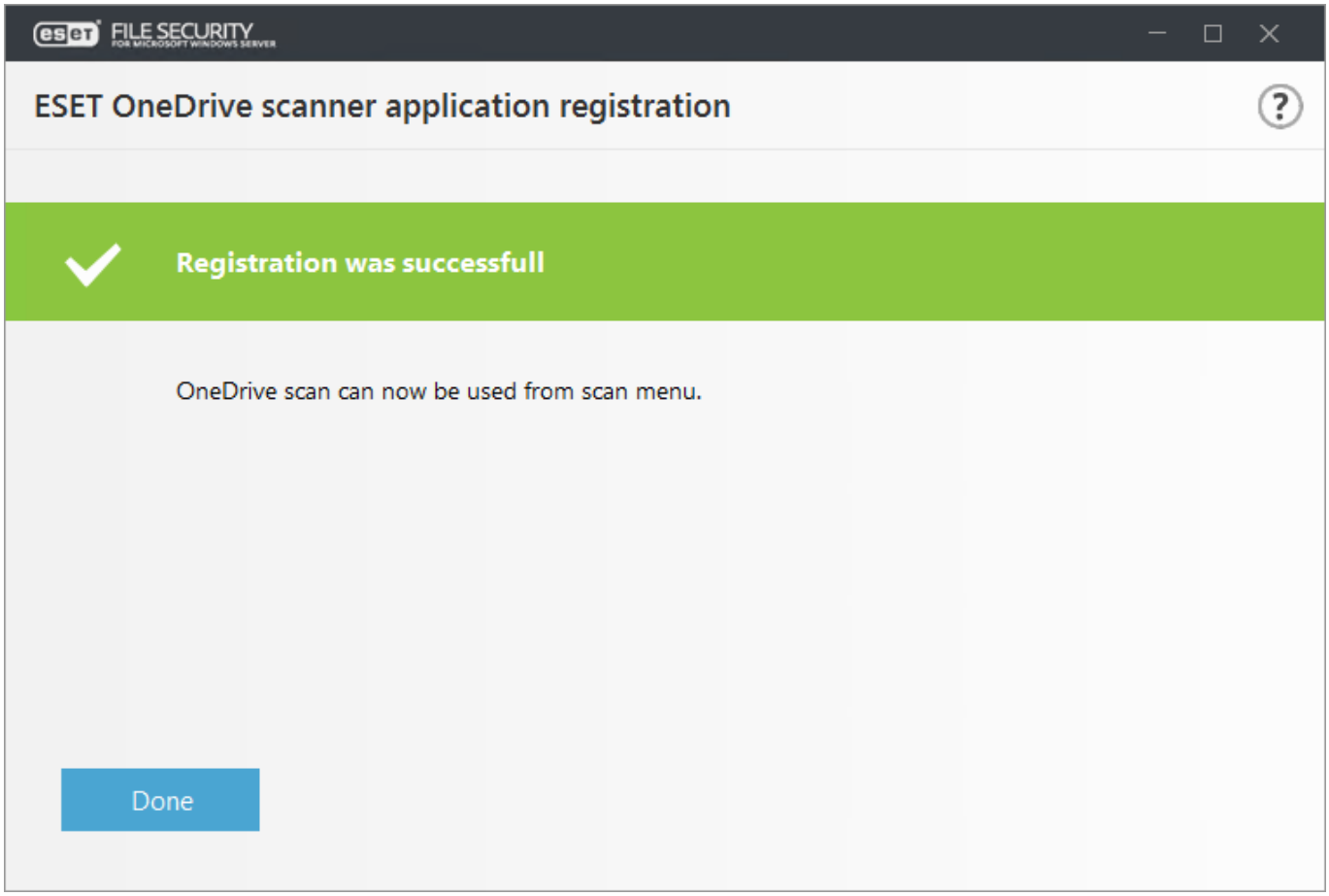
3. В веб-браузере откроется страница выбора учетной записи Microsoft. Щелкните учетную запись, которую вы используете (если она доступна), или введите учетные данные администратора Microsoft OneDrive или Office 365 и нажмите кнопку **Вход**.

4. Приложению для модуля сканирования ESET OneDrive требуются разрешения четырех типов. Все они перечислены в соответствующем запросе. Щелкните **Принять**, чтобы разрешить модулю сканирования ESET Server Security OneDrive подключаться к данным, расположенным в вашем облачном хранилище OneDrive.



5. Щелкните **Продолжить**, если в веб-браузере вам будет предложено отправить эту информацию (данные отправляются только на компьютер localhost, чтобы сообщить ESET Server Security, что приложение зарегистрировано).

6. После закрытия веб-браузера в окне мастера регистрации модуля сканирования ESET OneDrive отобразится сообщение о завершении регистрации. Нажмите кнопку **Готово**.



> Процедура регистрации модуля сканирования ESET OneDrive может отличаться в зависимости от того, выполнен ли вход на один из порталов Microsoft (OneDrive, Office 365, Azure и т. д.) с использованием учетных данных администратора. Следуйте инструкциям на экране и сообщениям в окне мастера регистрации.

Если во время регистрации модуля сканирования ESET OneDrive отобразится какое-либо из указанных далее сообщений об ошибках, см. сведения о соответствующей ошибке, чтобы устранить ее.

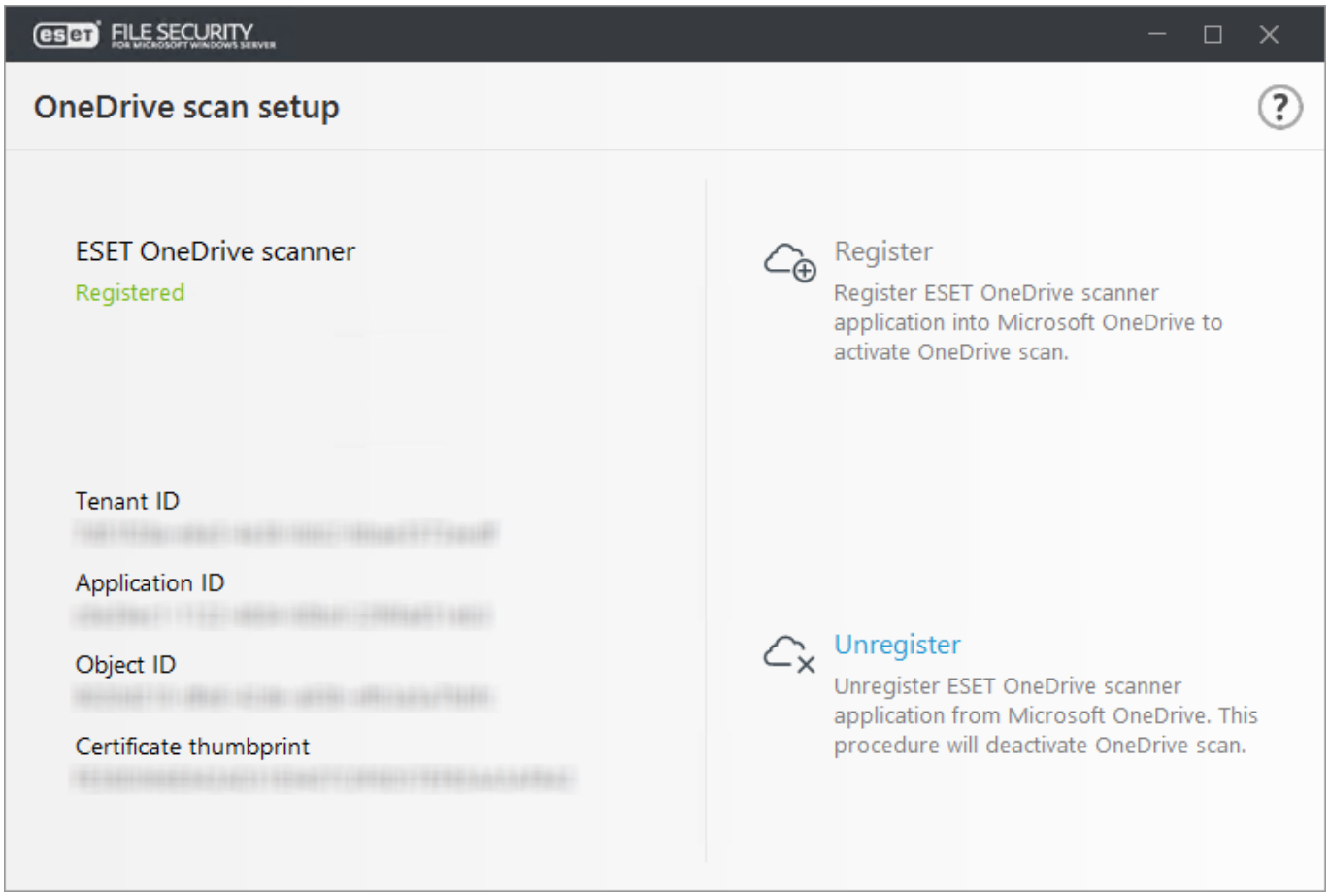
Сообщение об ошибке	Сведения об ошибке
Произошла непредвиденная ошибка.	Возможно, в ESET Server Security произошла ошибка. Попытайтесь зарегистрировать модуль сканирования ESET OneDrive позже. Если проблема не исчезнет, обратитесь в службу технической поддержки ESET.
Не удалось подключиться к Microsoft OneDrive.	Проверьте подключение к сети или Интернету и повторите попытку регистрации модуля сканирования ESET OneDrive.
От службы Microsoft OneDrive получена непредвиденная ошибка.	Возвращена ошибка с кодом HTTP 4xx без какого-либо ответа в ответном сообщении об ошибке. Если проблема не исчезнет, обратитесь в службу технической поддержки ESET.
От службы Microsoft OneDrive получена следующая ошибка.	Сервер Microsoft OneDrive возвратил ошибку с конкретным кодом или наименованием ошибки. Щелкните Показать ошибку.
Время ожидания задачи настройки истекло.	Задача настройки регистрации для модуля сканирования ESET OneDrive занимает слишком много времени. Повторите попытку регистрации модуля сканирования ESET OneDrive позже.

Сообщение об ошибке	Сведения об ошибке
Задача настройки отменена.	Вы отменили выполняющуюся задачу регистрации. Чтобы завершить регистрацию модуля сканирования ESET OneDrive, запустите регистрацию еще раз.
Уже выполняется другая задача настройки.	Задача регистрации уже выполняется. Дождитесь завершения первого процесса регистрации.

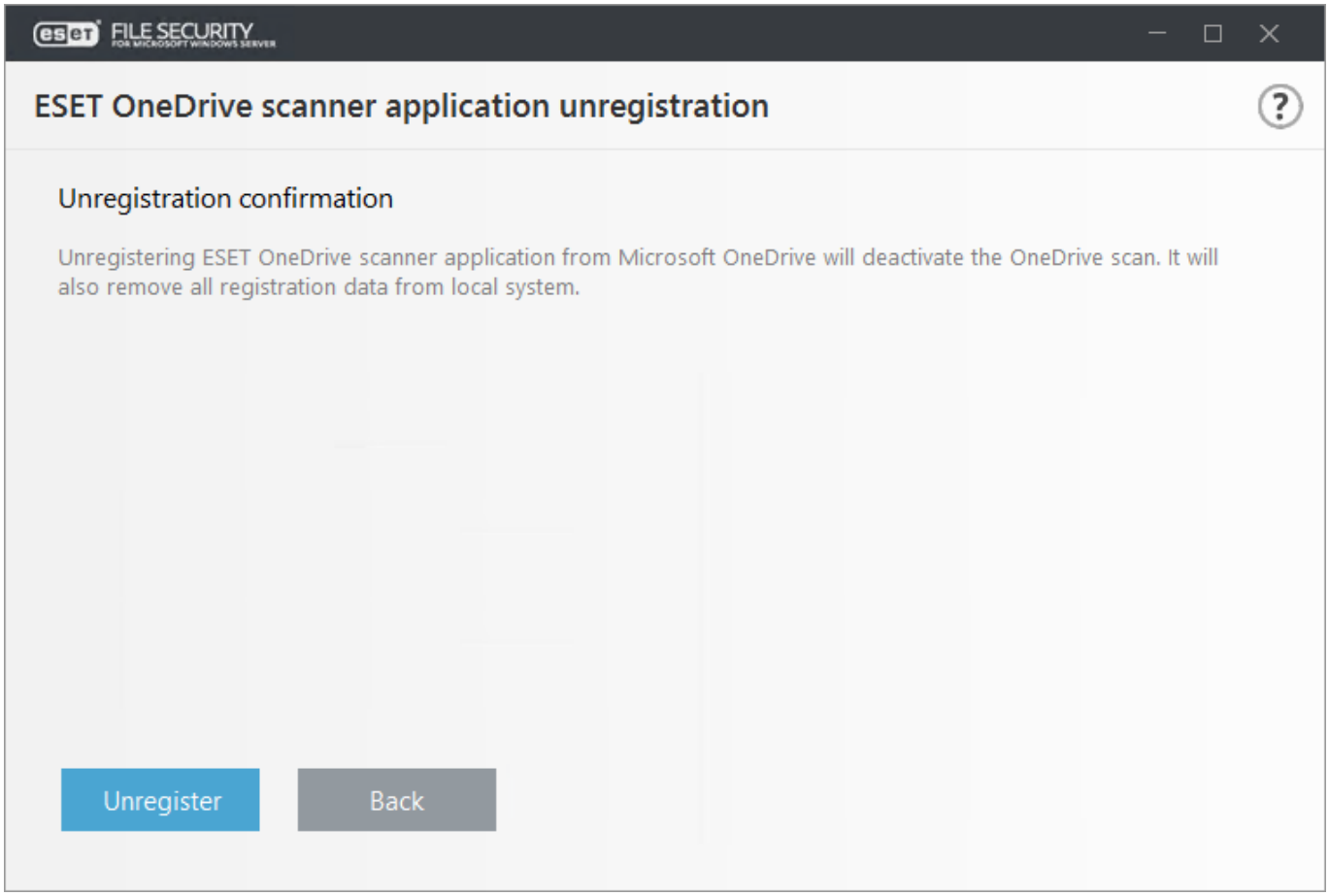
Отмена регистрации модуля сканирования ESET OneDrive

Отмена регистрации дает возможность удалить сертификат и приложение для модуля сканирования ESET OneDrive из Microsoft OneDrive, Office 365 и Azure. Этот процесс также удаляет локальные зависимости и снова делает доступной возможность регистрации.

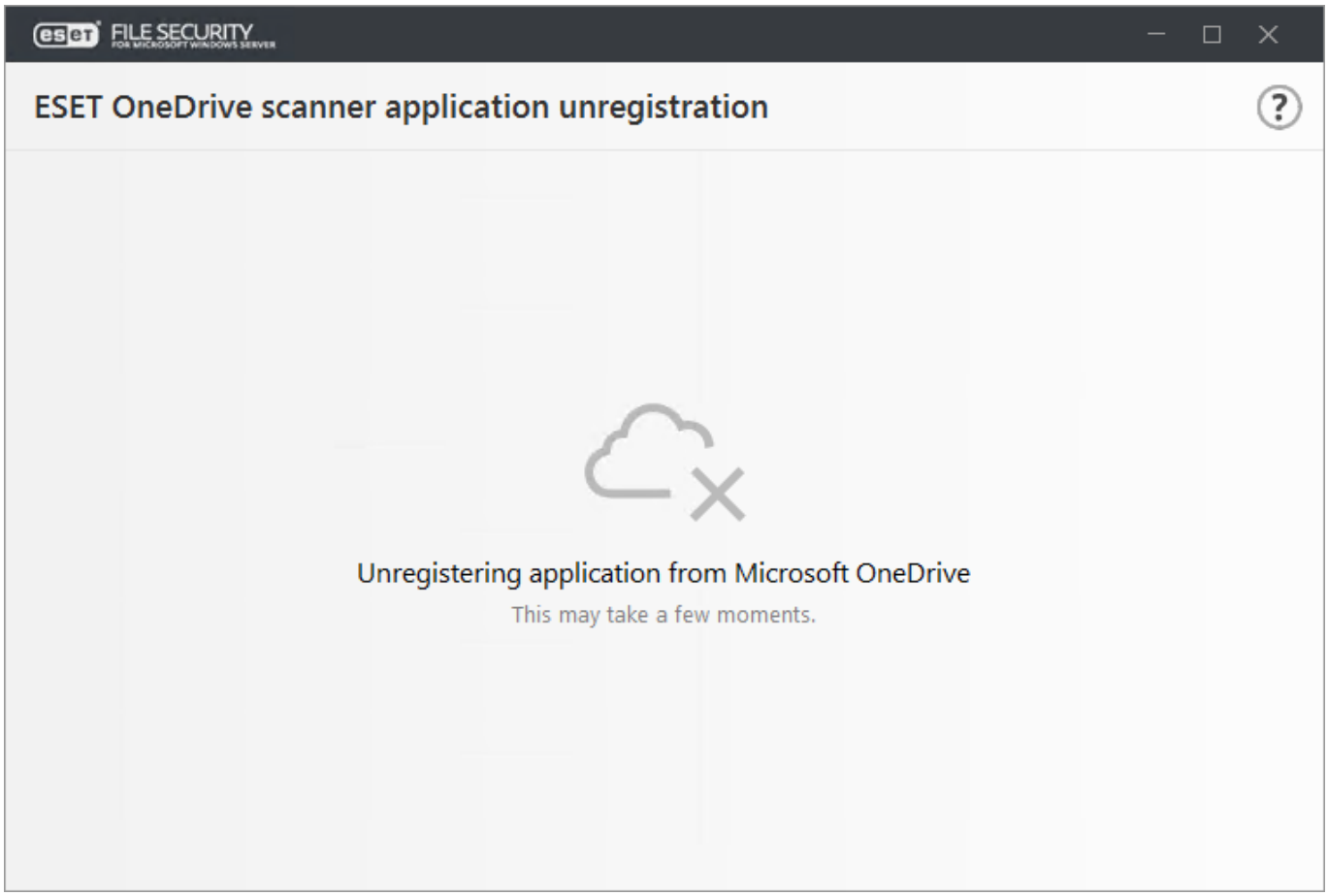
1. Чтобы отменить регистрацию и удалить модуль сканирования ESET OneDrive, щелкните **Отмена регистрации**, после чего откроется мастер отмены регистрации.



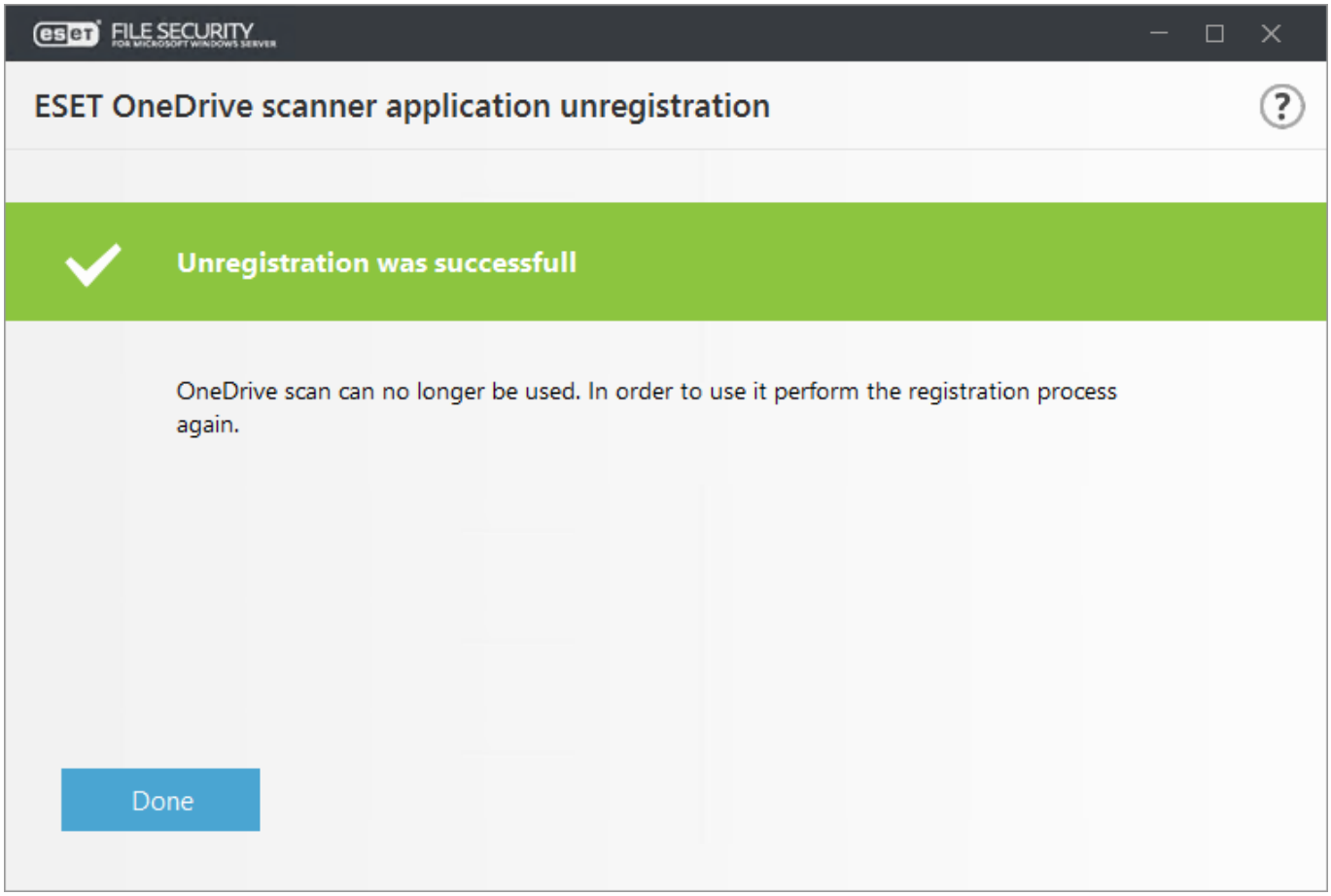
2. Щелкните **Отмена регистрации**, чтобы подтвердить удаление модуля сканирования ESET OneDrive.



3. Дождитесь завершения отмены регистрации в Microsoft OneDrive.



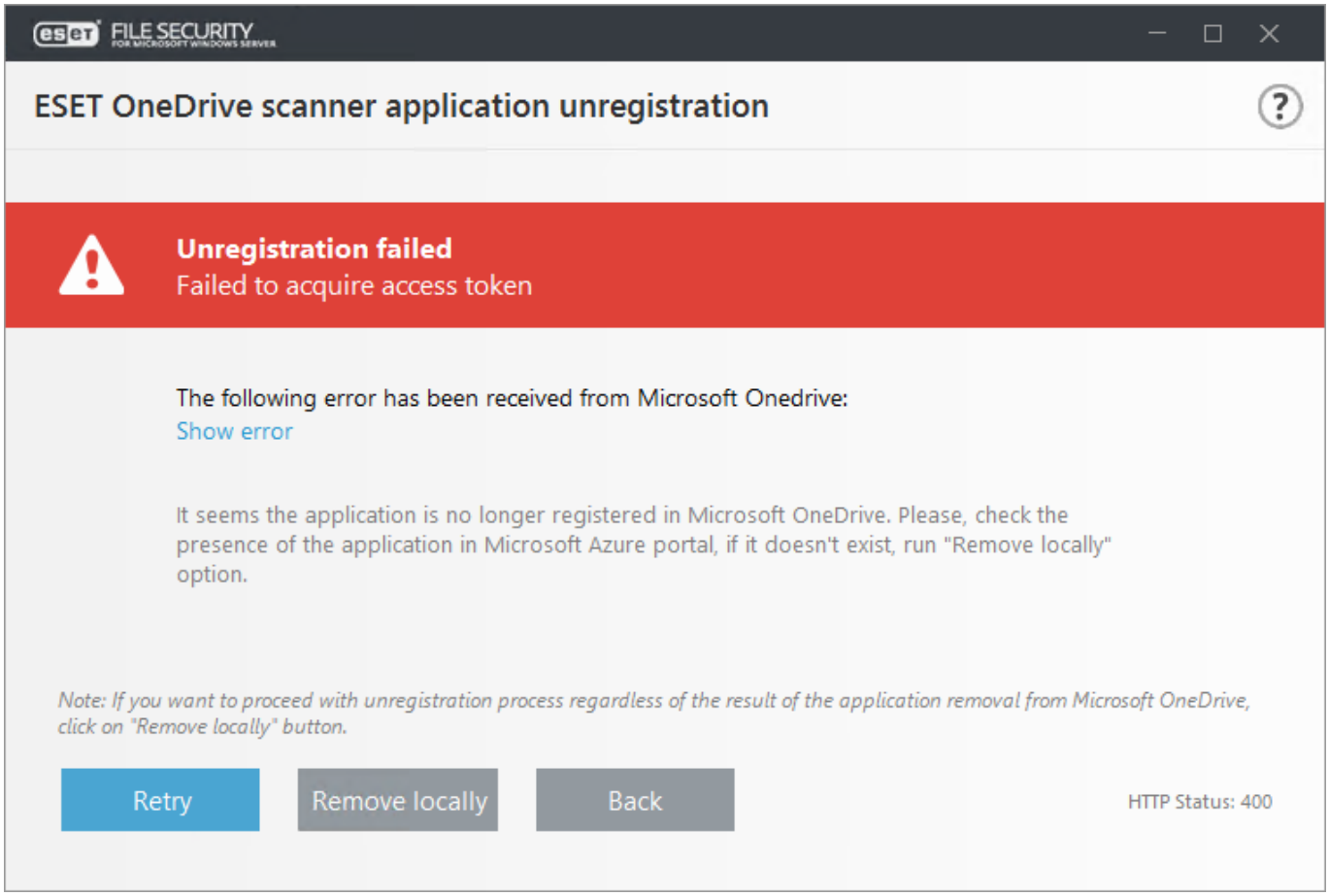
4. Если отмена регистрации завершается успешно, в мастере отмены регистрации появляется соответствующее сообщение.



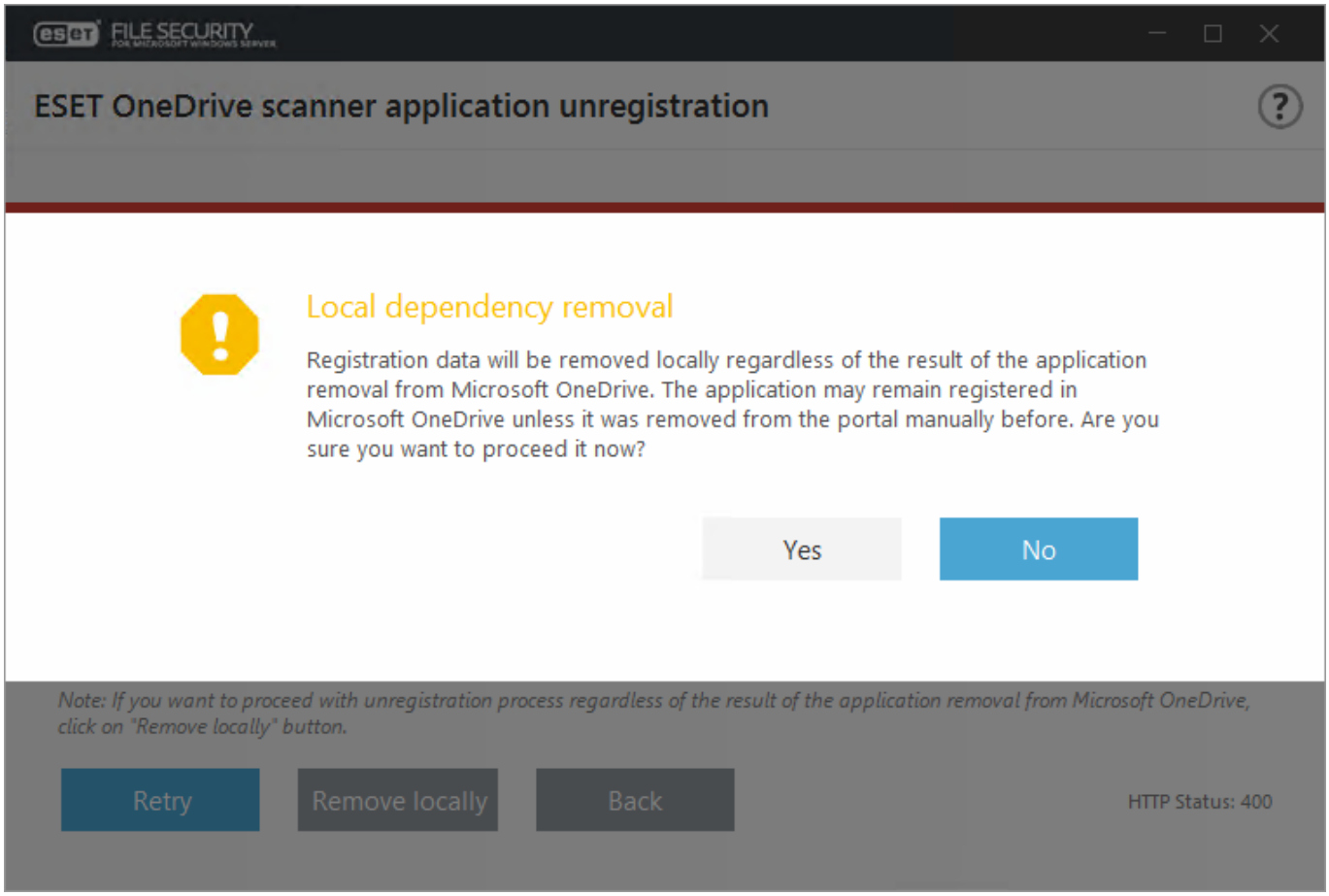
> Во время отмены регистрации может появиться сообщение об ошибке, например о сбое отмены регистрации. Ошибки могут быть вызваны разными причинами, но многие из них связаны с общими проблемами подключения к серверам Microsoft OneDrive. Кроме того, ошибки могут возникать из-за того, что приложение для модуля сканирования ESET OneDrive больше не зарегистрировано в Microsoft OneDrive. В таблице ниже представлен список сообщений об ошибках и описаны способы их решения.

В некоторых сообщениях об ошибке предлагается возможность удалить локальные зависимости (проблемы с подключением, несуществующее приложение в Microsoft OneDrive и т. д.). Чтобы удалить модуль сканирования ESET OneDrive локально, выполните следующие действия.

Если кнопка **Повторить попытку** не работает и проблема не исчезает, щелкните **Удалить локально**, чтобы продолжить отмену регистрации и удалить локальные зависимости модуля сканирования ESET OneDrive.



5. Нажмите кнопку **Да**, чтобы продолжить локальное удаление модуля сканирования ESET OneDrive. Функция сканирования ESET OneDrive будет недоступна, и вам придется снова пройти процедуру регистрации.



Удаление локальных зависимостей не изменяет сведения о регистрации приложения на портале Azure и сведения о разрешениях приложения на портале Office 365. Если вы локально удалили модуль сканирования ESET OneDrive из-за проблем с подключением к серверам Microsoft OneDrive, вам нужно будет вручную удалить приложение для модуля сканирования ESET OneDrive из списка зарегистрированных приложений в Azure. Сведения о том, как вручную найти и удалить модуль сканирования ESET OneDrive на портале Azure, см. на странице Настройка сканирования OneDrive.

Если во время отмены регистрации модуля сканирования ESET OneDrive отобразится какое-либо из перечисленных далее сообщений об ошибках, см. сведения о соответствующей ошибке, чтобы устранить ее.

Сообщение об ошибке	Сведения об ошибке
Не удалось подключиться к приложению Azure. Отсутствует подключение к Интернету.	Проверьте подключение к сети или Интернету и повторите попытку отмены регистрации. Чтобы продолжить отмену регистрации, не удаляя приложение для модуля сканирования ESET OneDrive из службы Microsoft OneDrive, щелкните Удалить локально.
Не удалось получить маркер доступа. От службы Microsoft OneDrive получена непредвиденная ошибка.	Вероятно, приложение для модуля сканирования ESET OneDrive больше не зарегистрировано в службе Microsoft OneDrive. Приложение для модуля сканирования ESET OneDrive, возможно, было вручную удалено на портале Azure. Проверьте, есть ли это приложение в службе Microsoft OneDrive или на портале Azure. Если приложение отсутствует в списке, продолжите отмену регистрации, щелкнув **Удалить локально**.

Сообщение об ошибке	Сведения об ошибке
Не удалось получить маркер доступа. От службы Microsoft OneDrive получена ошибка сервера.	Служба Microsoft OneDrive возвратила ошибку HTTP 5xx. Сейчас невозможно выполнить задачу отмены регистрации. Повторите попытку позже.
От службы Microsoft OneDrive получена следующая ошибка.	Сервер Microsoft OneDrive возвратил ошибку с конкретным кодом или наименованием ошибки. Щелкните Показать ошибку.
Уже выполняется другая задача настройки.	Задача отмены регистрации уже выполняется. Дождитесь завершения первого процесса отмены регистрации.

Общие параметры

Вы можете настраивать общие параметры в соответствии со своими потребностями. В меню слева можно выбрать следующие категории:

Detection engine

Включите или отключите обнаружение потенциально нежелательного, небезопасного, подозрительного приложения и защиты Anti-Stealth. Укажите исключения процессов или файлов и папок. Настройте защиту файловой системы в реальном времени, параметры ThreatSense, облачную защиту (ESET LiveGrid®), сканирование на наличие вредоносных программ (сканирование компьютера по требованию и другие параметры сканирования), сканирование Hyper-V и систему HIPS.

Обновление

Настройте параметры обновления, такие как профили, возраст системы обнаружения, моментальные снимки для отката модулей, тип обновления, пользовательский сервер обновлений, подключение или прокси-сервер, зеркало обновления, доступ к файлам обновлений, HTTP-сервер, данные учетной записи пользователя для подключения к сети и т. д.

Интернет и электронная почта

Позволяет настраивать фильтрацию протоколов и исключения (исключенные приложения и IP-адреса), параметры фильтрации протокола SSL/TLS, защиту почтовых клиентов (интеграция, протоколы электронной почты, оповещения и уведомления), защита веб-доступа (веб-протоколы HTTP/HTTPS и управление URL-адресами) и защиту почтового клиента от фишинга.

Контроль устройств

Включите интеграцию и настройте правила и группы для функции контроля устройств.

Конфигурация служебных программ

Позволяет настраивать инструменты, например ESET CMD, ESET RMM, поставщик WMI, цели сканирования ESET PROTECT, уведомления Центра обновления Windows, файлы журналов, прокси-сервер, уведомления по электронной почте, диагностику, кластер и т. д.

Интерфейс пользователя

Позволяет настраивать поведение GUI программы, состояния, информацию о лицензии, оповещения и уведомления, защиту паролем, политики выполнения eShell и т. д.

Detection engine

Модуль обнаружения защищает от атак злоумышленников на систему путем сканирования файлов, сообщений электронной почты и передаваемых по сети данных. При обнаружении объекта, классифицируемого как вредоносная программа, принимаются меры. Модуль обнаружения может удалить этот объект, сначала заблокировав его, а затем выполнив такие действия, как очистка, удаление или перемещение на карантин.

Защита в режиме реального времени и на основе машинного обучения

Расширенное машинное обучение теперь является дополнительным уровнем защиты модуля обнаружения, который улучшает обнаружение на основе машинного обучения. Подробнее об этом типе защиты см. в глоссарии. Вы можете конфигурировать уровни отчетов и защиты для перечисленных ниже категорий:

Вредоносные программы

Компьютерный вирус — это фрагмент вредоносного кода, который добавляется в начало или конец файлов на вашем компьютере. Однако термин «вирус» часто используется не по назначению. Более точный термин — «вредоносная программа» («вредоносное ПО»). Обнаружение вредоносных программ осуществляется модулем обнаружения в сочетании с компонентом машинного обучения. Более подробные сведения об этих типах приложений см. в глоссарии.

Потенциально нежелательные приложения

Потенциально нежелательное приложение представляет собой программное обеспечение, задачей которого не является однозначно вредоносная деятельность. Однако такое приложение может устанавливать дополнительное нежелательное программное обеспечение, изменять поведение цифрового устройства, выполнять действия без запроса или разрешения пользователя или выполнять иные неясные задачи.

К этой категории относятся: программы для показа рекламы, оболочки загрузок, различные панели инструментов для браузеров, программы с вводящим в заблуждение поведением, пакетное программное обеспечение, программы слежки и т. д. Подробнее о приложениях такого типа можно прочитать в глоссарии.

Потенциально нежелательные приложения

Подозрительным приложением является программное обеспечение, сжатое с помощью упаковщиков или средств защиты, которые часто используются для предотвращения обратной разработки или маскирования содержимого исполняемого файла (например, чтобы скрыть наличие вредоносной программы) при помощи проприетарных методов сжатия и/или шифрования.

К этой категории относятся: все неизвестные приложения, сжатые с помощью упаковщиков или средств защиты, которые часто используются для сжатия вредоносных программ.

Потенциально опасные приложения

Это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. Небезопасное приложение относится к законному коммерческому программному обеспечению, которое может быть неправильно использовано для вредоносных целей.

Эта категория включает: инструменты взлома, генераторы лицензионных ключей, хакерские инструменты, средства удаленного доступа или инструменты управления, приложения для взлома паролей и клавиатурные шпионы (программы, которые записывают каждое нажатие клавиши пользователем). По умолчанию этот параметр отключен.
Дополнительную информацию о приложениях этого типа см. в глоссарии.

Перед изменением порогового значения (или уровня) для составления отчетов или защиты категории, ознакомьтесь с приведенной ниже информацией.

Обнаружение

Составление отчетов выполняется модулем обнаружения и компонентом машинного обучения. Порог для отчетов можно устанавливать в соответствии с потребностями конкретной среды. Единственно верной конфигурации не существует. Поэтому рекомендуется отслеживать поведение в вашей среде и на основе полученной информации принимать решение о том, будет ли лучше использовать другие параметры отчетов.
Модуль отчетов не выполняет действий с объектами, он передает информацию в соответствующий уровень защиты, а уровень защиты принимает соответствующие меры.

Агрессивный	**Отчетность настроена на максимальную чувствительность. Сообщается о большем количестве обнаружений. Хотя агрессивные настройки могут казаться самыми безопасными, уровень их чувствительности часто может быть слишком высоким, что порой сказывается на производительности.** Агрессивные настройки могут приводить к ложным срабатываниям при определении вредоносности объектов. В результате над такими объектами будут выполняться определенные действия (в зависимости от настроек защиты).
Сбалансированный	Оптимальное соотношение между производительностью и скоростью обнаружения и количеством ложных обнаружений.
Осторожный	Уровень функции обнаружения вредоносных программ настроен таким образом, чтобы уменьшить количество ложных обнаружений, но при этом сохранить достаточный уровень защиты. Объекты считаются вредоносными программами, только если их поведение явно классифицируется как вредоносное.
Выкл.	Отчетность не задействована. Выполнение обнаружений, сообщение о них и их очистка не производится. Информирование о вредоносных программах отключить нельзя, поэтому настройка Выкл. недоступна для вредоносных программ.

Если необходимо восстановить параметры по умолчанию в этом разделе, щелкните дугообразную стрелку рядом с заголовком раздела. Все изменения, сделанные в этом разделе, будут потеряны.

Защита

Когда происходит обнаружение объекта с использованием указанного выше параметра и результатов машинного обучения, этот объект блокируется и над ним производится действие (очистка, удаление или перемещение в карантин).

Агрессивный	**Обнаружения агрессивного (или более низкого) уровня блокируются, после чего запускается автоматическое исправление (т. е. очистка).**
Сбалансированный	Обнаружения сбалансированного (или более низкого) уровня блокируются, после чего запускается автоматическое исправление (т.е. очистка).
Осторожный	Обнаружения осторожного уровня блокируются, и запускается автоматическое исправление (т.е. очистка).
Выкл.	Отчетность не задействована, выполнение обнаружений, сообщение о них и их очистка не производится. Сообщение о вредоносных программах отключить нельзя, поэтому настройка Выкл. недоступна для вредоносных программ.

Если необходимо восстановить параметры по умолчанию в этом разделе, щелкните дугообразную стрелку рядом с заголовком раздела. Все изменения, сделанные в этом разделе, будут потеряны.

По умолчанию перечисленные выше параметры защиты на основе машинного обучения относятся также и к сканированию компьютера и по требованию. При необходимости можно настроить параметры **защиты по требованию и защиты на основе машинного обучения** по отдельности. Щелкните значок переключателя, чтобы отключить параметр **Использовать настройки защиты в реальном времени**, и выполните настройку.

Обнаружение с помощью машинного обучения

Модуль обнаружения защищает от атак злоумышленников на систему путем сканирования файлов, сообщений электронной почты и передаваемых по сети данных. При обнаружении объекта, классифицируемого как вредоносная программа, принимаются меры. Модуль обнаружения может удалить этот объект, сначала заблокировав его, а затем выполнив такие действия, как очистка, удаление или перемещение на карантин.

Защита в режиме реального времени и на основе машинного обучения

Расширенное машинное обучение теперь является дополнительным уровнем защиты модуля обнаружения, который улучшает обнаружение на основе машинного обучения. Подробнее об этом типе защиты см. в глоссарии. Вы можете конфигурировать уровни отчетов и защиты для перечисленных ниже категорий:

Вредоносные программы

Компьютерный вирус — это фрагмент вредоносного кода, который добавляется в начало или конец файлов на вашем компьютере. Однако термин «вирус» часто используется не по назначению. Более точный термин — «вредоносная программа» («вредоносное ПО»). Обнаружение вредоносных программ осуществляется модулем обнаружения в сочетании с компонентом машинного обучения. Более подробные сведения об этих типах приложений см. в глоссарии.

Потенциально нежелательные приложения

Потенциально нежелательное приложение представляет собой программное обеспечение, задачей которого не является однозначно вредоносная деятельность. Однако такое приложение может устанавливать дополнительное нежелательное программное обеспечение, изменять поведение цифрового устройства, выполнять действия без запроса или разрешения пользователя или выполнять иные неясные задачи.

К этой категории относятся: программы для показа рекламы, оболочки загрузок, различные панели инструментов для браузеров, программы с вводящим в заблуждение поведением, пакетное программное обеспечение, программы слежки и т. д. Подробнее о приложениях такого типа можно прочитать в глоссарии.

Потенциально нежелательные приложения

Подозрительным приложением является программное обеспечение, сжатое с помощью упаковщиков или средств защиты, которые часто используются для предотвращения обратной разработки или маскирования содержимого исполняемого файла (например, чтобы скрыть наличие вредоносной программы) при помощи проприетарных методов сжатия и/или шифрования.

К этой категории относятся: все неизвестные приложения, сжатые с помощью упаковщиков или средств защиты, которые часто используются для сжатия вредоносных программ.

Потенциально опасные приложения

Это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. Небезопасное приложение относится к законному коммерческому программному обеспечению, которое может быть неправильно использовано для вредоносных целей.

Эта категория включает: инструменты взлома, генераторы лицензионных ключей, хакерские инструменты, средства удаленного доступа или инструменты управления, приложения для взлома паролей и клавиатурные шпионы (программы, которые записывают каждое нажатие клавиши пользователем). По умолчанию этот параметр отключен.
Дополнительную информацию о приложениях этого типа см. в глоссарии.

Перед изменением порогового значения (или уровня) для составления отчетов или защиты категории, ознакомьтесь с приведенной ниже информацией.

Обнаружение

Составление отчетов выполняется модулем обнаружения и компонентом машинного обучения. Порог для отчетов можно устанавливать в соответствии с потребностями конкретной среды. Единственно верной конфигурации не существует. Поэтому рекомендуется отслеживать поведение в вашей среде и на основе полученной информации принимать решение о том, будет ли лучше использовать другие параметры отчетов.
Модуль отчетов не выполняет действий с объектами, он передает информацию в соответствующий уровень защиты, а уровень защиты принимает соответствующие меры.

Агрессивный	**Отчетность настроена на максимальную чувствительность. Сообщается о большем количестве обнаружений. Хотя агрессивные настройки могут казаться самыми безопасными, уровень их чувствительности часто может быть слишком высоким, что порой сказывается на производительности.** i Агрессивные настройки могут приводить к ложным срабатываниям при определении вредоносности объектов. В результате над такими объектами будут выполняться определенные действия (в зависимости от настроек защиты).
Сбалансированный	Оптимальное соотношение между производительностью и скоростью обнаружения и количеством ложных обнаружений.
Осторожный	Уровень функции обнаружения вредоносных программ настроен таким образом, чтобы уменьшить количество ложных обнаружений, но при этом сохранить достаточный уровень защиты. Объекты считаются вредоносными программами, только если их поведение явно классифицируется как вредоносное.
Выкл.	Отчетность не задействована. Выполнение обнаружений, сообщение о них и их очистка не производится. i Информирование о вредоносных программах отключить нельзя, поэтому настройка Выкл. недоступна для вредоносных программ.

Если необходимо восстановить параметры по умолчанию в этом разделе, щелкните дугообразную стрелку рядом с заголовком раздела. Все изменения, сделанные в этом разделе, будут потеряны.

OneDrive и защита на основе машинного обучения

Отчетность
Выполняется модулем обнаружения и компонентом машинного обучения. Отчетность не выполняет действий с объектами (это делается с помощью соответствующего слоя защиты).
Защита
Настройте параметры в разделе OneDrive, чтобы определить действия, выполняемые с объектами из отчетов.
Если необходимо восстановить параметры по умолчанию в этом разделе, щелкните дугообразную стрелку рядом с заголовком раздела. Все изменения, сделанные в этом разделе, будут потеряны.
Настройте обнаружение с помощью машинного обучения с использованием eShell. Имя контекста в eShell — **MLP**. Откройте eShell в интерактивном режиме и перейдите к MLP:
`computer onedrive mlp`
Проверьте текущее значение параметра создания отчетов для подозрительных приложений:
`get suspicious-reporting`
Если вам нужны менее строгие отчеты, измените значение этого параметра на «Осторожный»:
`set suspicious-reporting cautious`

Hyper-V и защита на основе машинного обучения

Обнаружение
Выполняется модулем обнаружения и компонентом машинного обучения. Отчетность не выполняет действий с объектами (это делается с помощью соответствующего слоя защиты).
Защита
Настройте параметры в разделе Сканирование Hyper-V, чтобы определить действия, выполняемые с объектами из отчетов.
Если необходимо восстановить параметры по умолчанию в этом разделе, щелкните дугообразную стрелку рядом с заголовком раздела. Все изменения, сделанные в этом разделе, будут потеряны.
Настройте обнаружение с помощью машинного обучения с использованием eShell. Имя контекста в eShell — **MLP**. Откройте eShell в интерактивном режиме и перейдите к MLP:
```
computer hyperv mlp
```
Проверьте текущее значение параметра создания отчетов для подозрительных приложений:
```
get suspicious-reporting
```
Если вам нужны менее строгие отчеты, измените значение этого параметра на «Осторожный»:
```
set suspicious-reporting cautious
```

Исключения

Исключения позволяют исключить из сканирования файлы и папки. Чтобы на наличие угроз сканировались все объекты, исключения рекомендуется создавать только в случае крайней необходимости. Ситуации, в которых может понадобиться создать исключение, — это, например, сканирование больших баз данных, которые замедляют работу, или программ, конфликтующих с процессом сканирования (например, программное обеспечение для резервного копирования).

> Не путать с исключенными расширениями, исключениями процессов и фильтром исключений!

> Модуль защиты файловой системы в режиме реального времени и модуль сканирования компьютера не обнаружат угрозу в файле, если он соответствует критериям исключения из сканирования.

Выберите тип исключения и нажмите кнопку **Изменить**, чтобы добавить новое или изменить существующее.

- Исключения производительности — исключение файлов и папок из сканирования.
- Исключения обнаружения — исключения объектов из сканирования с помощью определенных критериев: путь, хеш файла или имя обнаружения.

Исключения для быстродействия

Эта функция позволяет исключать файлы и папки из сканирования. Исключения производительности полезны для исключения сканирования на уровне файлов критически важных приложений и сканирования, приводящего к нарушению работы системы или снижению производительности.

Путь

Исключает конкретный путь (файл или каталог) для этого компьютера. Не используйте символ подстановки звездочку (*) в середине пути. Для получения дополнительных сведений см. следующую статью базы знаний .

> Чтобы исключить содержимое папки, добавьте звездочку (*) в конце пути (*C:\Tools**). При использовании строки *C:\Tools* исключение выполняться не будет, так как с точки зрения сканера *Tools* также может быть именем файла.

Комментарий

Можете добавить комментарий, чтобы легко распознавать исключения в будущем.

> Исключение пути с помощью звездочки:
> C:\Tools*: путь должен заканчиваться обратной косой чертой (\) и звездочкой (*), указывая на то, что это папка, и все ее содержимое (файлы и подпапки) должно исключаться.
> C:\Tools*.*: та же ситуация, что и в случае с C:\Tools*. Это означает, что действие выполняется рекурсивно.
> C:\Tools*.dat: исключит DAT-файлы в папке Tools.
> C:\Tools\sg.dat: исключит этот конкретный файл, расположенный по указанному пути.

> Чтобы исключить все файлы в папке, введите путь к папке и используйте маску *.*. Если нужно исключить только файлы с расширением DOC, используйте маску *.doc.
> Если имя исполняемого файла содержит определенное количество символов (которые могут меняться), причем известна только первая буква (скажем, «D»), используйте следующий формат:
> D????.exe (вопросительные знаки заменяют отсутствующие или неизвестные символы).

> Для определения исключений сканирования можно использовать системные переменные, например %PROGRAMFILES%.
> Чтобы исключить папку Program Files с помощью этой системной переменной, используйте путь %PROGRAMFILES%\ (при добавлении в исключения обязательно в конце пути добавляйте обратную косую черту).
> Чтобы исключить все файлы в подкаталоге %HOMEDRIVE%, используйте путь %HOMEDRIVE%\Excluded_Directory*.*.
> Следующие переменные можно использовать в формате исключения пути:
> *%ALLUSERSPROFILE%*
> *%COMMONPROGRAMFILES%*
> *%COMMONPROGRAMFILES(X86)%*
> *%COMSPEC%*
> *%HOMEDRIVE%*
> *%HOMEPATH%*
> *%PROGRAMFILES%*
> *%PROGRAMFILES(X86)%*
> *%SystemDrive%*
> *%SystemRoot%*
> *%WINDIR%*
> *%PUBLIC%*
> Пользовательские системные переменные (например, %TEMP% или %USERPROFILE%) или переменные среды (например, %PATH%) не поддерживаются.

Это еще один способ исключения объектов из сканирования с использованием имени обнаружения, пути или его хеша. Исключения обнаружения не исключают файлы и папки из сканирования (как это делают, например, исключения производительности). Исключения

обнаружения исключают объекты только в том случае, если они обнаружены модулем обнаружения и соответствующее правило присутствует в списке исключений.

Простейший способ создать исключение на основе обнаружения заключается в использовании имеющегося обнаружения из раздела **Файлы журнала** > Обнаружения. Щелкните правой кнопкой мыши запись журнала (обнаружение) и выберите команду **Создать исключение**. Откроется мастер исключений с предварительно заданными критериями.

Чтобы вручную создать исключение обнаружения, выберите пункт **Изменить** > **Добавить** (или **Изменить**, если хотите изменить уже имеющееся исключение) и укажите один или несколько из указанных ниже критериев (которые можно объединять).

Путь

Исключает определенный путь (файл или каталог). Можно выбрать конкретное местоположение или файл в окне обзора или ввести строку вручную. Не используйте подстановочные символы — звездочку (*) — в середине пути. Дополнительные сведения см. в этой статье базы знаний .

> Чтобы исключить содержимое папки, добавьте звездочку (*) в конце пути (C:\Tools*). При использовании строки *C:\Tools* исключение выполняться не будет, так как с точки зрения сканера *Tools* также может быть именем файла.

Хеш

Исключается файл с определенным хешем (SHA1), при этом тип файла, его расположение, имя и расширение не учитываются.

Имя обнаружения

Введите допустимое имя обнаружения (угрозы). Создание исключения на основе только имени обнаружения может представлять угрозу безопасности. Рекомендуется сочетать имя обнаружения и путь. Эти критерии исключения можно использовать только для определенных типов обнаружений.

Комментарий

Можете добавить **комментарий**, чтобы легко распознавать исключения в будущем.

ESET PROTECT содержит управление исключениями обнаружения для создания исключений обнаружения и применения их к нескольким компьютерам или группам.

Для указания групп файлов можно использовать символы шаблона. Вопросительный знак (*?*) обозначает любой один символ, а звездочка (*) — любое количество символов.

> Исключение пути с помощью звездочки:
> C:\Tools*: путь должен заканчиваться обратной косой чертой (\) и звездочкой (*), указывая на то, что это папка, и все ее содержимое (файлы и подпапки) должно исключаться.
> C:\Tools*.*: та же ситуация, что и в случае с C:\Tools*. Это означает, что действие выполняется рекурсивно.
> C:\Tools*.dat: исключит DAT-файлы в папке Tools.
> C:\Tools\sg.dat: исключит этот конкретный файл, расположенный по указанному пути.

Чтобы исключить угрозу, введите допустимое имя обнаружения в следующем формате:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

Чтобы исключить все файлы в папке, введите путь к папке и используйте маску *.*. Если нужно исключить только файлы с расширением DOC, используйте маску *.doc.
Если имя исполняемого файла содержит определенное количество символов (которые могут меняться), причем известна только первая буква (скажем, «D»), используйте следующий формат:
D????.exe (вопросительные знаки заменяют отсутствующие или неизвестные символы).

Для определения исключений сканирования можно использовать системные переменные, например *%PROGRAMFILES%*.
Чтобы исключить папку Program Files с помощью этой системной переменной, используйте путь %PROGRAMFILES%\ (при добавлении в исключения обязательно в конце пути добавляйте обратную косую черту).
Чтобы исключить все файлы в подкаталоге %HOMEDRIVE%, используйте путь %HOMEDRIVE%\Excluded_Directory*.*.
Следующие переменные можно использовать в формате исключения пути:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Пользовательские системные переменные (например, %TEMP% или %USERPROFILE%) или переменные среды (например, %PATH%) не поддерживаются.

Мастер исключений

Рекомендуемое исключение предварительно выбрано на основе типа обнаружения, но вы можете дополнительно указать критерии исключения для обнаружений. Щелкните пункт **Изменить условия**.

- **Точные файлы** — исключение отдельных файлов по их хешу SHA-1.

- **Обнаружение** — укажите имя обнаружения, чтобы исключить все файлы, содержащие такое обнаружение.

- **Путь и обнаружение** — укажите имя обнаружения и путь (включая имя файла), чтобы исключить все файлы с обнаружениями, находящиеся в указанном местоположении.

Можете добавить **комментарий**, чтобы легко распознавать исключения в будущем.

Расширенные параметры

Технология Anti-Stealth

Сложная система, обеспечивающая обнаружение опасных программ, таких как руткиты, которые могут скрываться от операционной системы. Обычно программы такого типа невозможно обнаружить при помощи стандартных методов.

AMSI

Разрешение для программы Microsoft Antimalware Scan Interface (AMSI) сканировать сценарии Powershell, которые исполняются сервером сценариев Windows.

Автоматические исключения

Разработчики серверных приложений и операционных систем рекомендуют исключать наборы критических рабочих файлов и папок из сканирования на наличие вредоносных программ для большинства таких программных продуктов. Сканирование на наличие вредоносных программ может отрицательно повлиять на производительность сервера, что может привести к конфликтам и даже не дать возможности некоторым приложениям работать на сервере. Исключения помогают свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе программного обеспечения защиты от вредоносных программ. См. полный список исключенных файлов из сканирования для продуктов сервера ESET.

Программа ESET Server Security выявляет критические файлы серверных приложений и серверных операционных систем и автоматически добавляет их в список Исключения. По умолчанию все автоматические исключения активированы. Активировать или деактивировать исключение для любого серверного приложения можно с помощью ползунка. Последствия каждого действия приведены ниже.

- Если этот параметр активирован, все соответствующие критические файлы и папки будут добавлены в список файлов, исключенных из сканирования. При каждом перезапуске сервера система автоматически проверяет исключения и обновляет список в случае изменения системы или приложения (например, при установке нового серверного приложения). Эта настройка позволяет обеспечить постоянное применение рекомендованных автоматических исключений.

- Если этот параметр деактивирован, исключенные файлы и папки будут автоматически удалены из списка. Любые пользовательские исключения, введенные вручную, останутся без изменений.

Для выявления и создания автоматических исключений программа ESET Server Security использует выделенное приложение eAutoExclusions.exe, находящееся в папке установки. С вашей стороны не требуется никаких действий, но вы можете использовать командную строку, чтобы вывести список обнаруженных серверных приложений в системе, выполнив eAutoExclusions.exe -servers. Для отображения полного синтаксиса используйте `eAutoExclusions.exe -?`.

Общий локальный кэш

Общий локальный кэш ESET повышает производительность в виртуализированных средах, запрещая повторяющееся сканирование в сети. Благодаря этому каждый файл сканируется только один раз, а затем сохраняется в общем кэше. Чтобы сохранять данные о сканировании файлов и папок в сети в локальный кэш, включите переключатель **Параметры кэширования**. При следующем сканировании продукт ESET Server Security будет искать сканируемые файлы в кэше. Если файлы совпадают, они будут исключены из сканирования.

При настройке сервера кэширования нужно работать с указанными ниже параметрами:

- **Имя хоста** — имя или IP-адрес компьютера, на котором расположен кэш.
- **Порт** — номер порта, используемого для передачи данных (такой же, какой указан для общего локального кэша).
- **Пароль** — пароль общего локального кэша (если понадобится).

Действия при обнаружении заражения

Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET Server Security обнаруживает заражения с помощью перечисленных ниже модулей.

- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- Сканирование компьютера по требованию

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в карантин или прервать подключение. Окно уведомлений отображается в области уведомлений в правом нижнем углу экрана. Дополнительные сведения об уровнях очистки и поведении см. в разделе Очистка.

Очистка и удаление

Если действие по умолчанию для модуля защиты файловой системы в режиме реального времени не определено, пользователю предлагается выбрать его в окне предупреждения. Обычно доступны варианты **Очистить**, **Удалить** или **Ничего не предпринимать**. Не рекомендуется выбирать действие **Ничего не предпринимать**, поскольку при этом зараженные файлы не будут очищены. Исключение допустимо только в том случае, если вы уверены, что файл безвреден и был обнаружен по ошибке.

Очистку следует применять, если файл был атакован вирусом, который добавил к нему

вредоносный код. В этом случае программа сначала пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние до очистки. Если файл содержит только вредоносный код, он будет удален.

Если зараженный файл заблокирован или используется каким-либо системным процессом, обычно он удаляется только после освобождения. Как правило, это происходит после перезапуска системы.

Множественные угрозы

Если какие-либо зараженные файлы при сканировании компьютера не были очищены (или был выбран уровень очистки **Без очистки**), на экран будет выведено окно предупреждения, в котором пользователю предлагается выбрать действие для таких файлов.

Выберите для каждой угрозы, приведенной в списке, отдельное действие или с помощью параметра **Выберите, что нужно сделать с каждой из приведенных угроз** выберите одно действие для всех угроз, приведенных в списке, и щелкните **Выполнить**.

Удаление файлов из архивов

В режиме очистки по умолчанию архив удаляется целиком, только если он содержит лишь зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются.

Однако следует проявлять осторожность при сканировании в режиме тщательной очистки, так как при этом архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

Защита файловой системы в режиме реального времени

Функция защиты файловой системы в реальном времени контролирует все события в системе, связанные с вредоносными программами. Все файлы сканируются на наличие вредоносного кода во время их открытия, создания или запуска на компьютере. По умолчанию защита файловой системы в реальном времени запускается при загрузке операционной системы и обеспечивает беспрерывное сканирование.

В особых случаях (например, при возникновении конфликта с другим модулем сканирования в реальном времени) защиту в реальном времени можно выключить. Для этого нужно отключить параметр **Автоматически запускать защиту файловой системы в реальном времени** в разделе **Расширенные параметры** (F5) > **Защита файловой системы в реальном времени** > **Основная информация**.

Решение ESET Server Security совместимо с компьютерами, на которых используется агент Azure File Sync с включенным распределением по уровням в облаке. ESET Server Security распознает файлы с атрибутом *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Носители для сканирования

По умолчанию на наличие возможных угроз сканируются все типы носителей.

- **Жесткие диски** — контролируются все жесткие диски системы.

- **Съемные носители** — контролируются компакт-/DVD-диски, USB-накопители, Bluetooth-устройства и т. п.

- **Сетевые диски** — сканируются все подключенные сетевые диски.

Рекомендуется оставить параметры по умолчанию, а изменять их только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

Сканировать при

По умолчанию все файлы сканируются при открытии, создании или исполнении. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

- **Открытие файла** — сканирование при открытии файлов или при доступе к ним.

- **Создание файла** — сканирование при создании или изменении файлов.

- **Исполнение файла** — сканирование при исполнении файлов.

- **Доступ к съемным носителям** — сканирование при доступе к съемным носителям. При вставке в устройство съемного носителя, содержащего загрузочный сектор, загрузочный сектор немедленно сканируется. Этот параметр не включает сканирование файлов на съемных носителях. Настройки сканированием файлов на съемных носителях находятся в разделе **Носители для сканирования** > **Съемные носители**. Для корректного доступа к загрузочному сектору съемного носителя необходимо включить в параметрах ThreatSense пункт Загрузочные секторы/UEFI.

Исключения для процессов

Эта функция позволяет исключить конкретные процессы. Например, если исключить процессы в решении резервного копирования, то все те операции с файлами, которые касаются исключенных процессов, игнорируются и считаются безопасными. Таким образом, факторы, мешающие резервному копированию, сводятся к минимуму.

Параметры ThreatSense

Защита файловой системы в реальном времени проверяет все типы носителей, и ее могут запустить различные системные события, например получение доступа к файлу. Защиту файловой системы в реальном времени можно настроить для создаваемых и уже существующих файлов по-разному. Например, можно настроить защиту файловой системы в реальном времени так, чтобы она более тщательно отслеживала вновь созданные файлы.

файлы, которые уже сканировались, не сканируются повторно (если с момента последнего сканирования они не были изменены). Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение контролируется с помощью **оптимизации Smart**. Если **оптимизация Smart отключена**, все файлы сканируются при каждом получении доступа к ним.

Для изменения этой настройки нажмите **F5**, чтобы открыть **расширенные параметры**, и

разверните **Detection engine** > **Защита файловой системы в реальном времени**. Щелкните **Параметры ThreatSense** > **Другое** и установите или снимите флажок **Включить интеллектуальную оптимизацию**.

Дополнительные параметры ThreatSense

Вы можете детально настраивать **Дополнительные параметры ThreatSense для только что созданных и измененных файлов** или **Дополнительные параметры ThreatSense для исполняемых файлов**.

ThreatSenseПараметры

ThreatSense — это технология, состоящая из множества сложных способов обнаружения угроз. Это упреждающая технология, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используются: анализ и эмуляция кода, универсальные сигнатуры и сигнатуры вирусов. Вместе все эти средства значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает количество обнаруживаемых угроз и эффективность максимальными. Кроме того, технология ThreatSense успешно уничтожает руткиты.

> Сведения об автоматической проверке файлов при запуске см. в разделе Сканирование при запуске.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- типы и расширения файлов, подлежащих сканированию;
- сочетание различных способов обнаружения;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните элемент **в окне Дополнительные настройки** (**F5**) любого модуля, использующего технологию ThreatSense (см. ниже). Для разных сценариев обеспечения безопасности могут требоваться различные конфигурации. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Сканирование Hyper-V
- Сканирование OneDrive
- Защита файловой системы в режиме реального времени
- Процессы сканирования вредоносных программ
- Сканирование в состоянии простоя
- Сканирование файлов, исполняемых при запуске системы
- Защита документов
- Защита почтового клиента

- Защита доступа в Интернет

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, если настроить сканирование программ сжатия исполняемых файлов или включить расширенную эвристику в модуле защиты файловой системы в реальном времени, работа системы может замедлиться (обычно только новые файлы сканируются с применением этих способов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

В этом разделе можно указать компоненты и файлы компьютера, которые будут сканироваться на наличие заражений.

Оперативная память

Сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы/UEFI

Загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи. Основная загрузочная запись диска виртуальной машины Hyper-V сканируется в режиме только для чтения.

База данных WMI

Сканирование всей базы данных WMI, поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.

Системный реестр

Сканирование системного реестра, всех разделов и подразделов, поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.

Почтовые файлы

Программа поддерживает расширения DBX (Outlook Express) и EML.

Архивы

Программа поддерживает расширения *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE* и многие другие.

Самораспаковывающиеся архивы

Самораспаковывающиеся архивы (файлы с расширением SFX) — это архивы, которым для распаковки не нужны специальные программы.

Упаковщики

В отличие от стандартных типов архивов, программы сжатия, будучи выполненными, распаковываются в память. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические программы сжатия (UPX, yoda, ASPack, FGS и т. д.), но и множество других типов таких программ.

Параметры сканирования

Выберите способы сканирования системы на предмет заражений. Доступны указанные ниже варианты.

Эвристический анализ

Эвристический анализ — это анализ вредоносной активности программ с помощью специального алгоритма. Главным преимуществом этой технологии является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующем модуле обнаружения.

Расширенный эвристический анализ/распределенные сетевые атаки сигнатуры

Для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Очистка

Настройки очистки определяют поведение сканера при очистке зараженных файлов. Защита в реальном времени и другие модули защиты имеют следующие уровни исправления (т. е. очистки).

Всегда исправлять обнаружение

Пытаться исправлять обнаружение при очистке объектов без какого-либо вмешательства пользователя. Исключение составляют системные файлы. Такие объекты остаются в исходном расположении, если обнаружение не может быть исправлено.

Исправлять обнаружение, если это безопасно, в ином случае не вмешиваться

Пытаться исправлять обнаружение при очистке объектов без какого-либо вмешательства пользователя. Если обнаружение не может быть исправлено в случае системных файлов или архивов (с чистыми и зараженными файлами), обнаруженный объект остается в исходном расположении.

Исправлять обнаружение, если это безопасно, в ином случае спрашивать

Пытаться исправлять обнаружение при очистке объектов. В некоторых случаях, если ESET Server Security не может выполнить автоматическое действие, пользователю предлагается выбрать действие (удалить или пропустить). Эта настройка рекомендуется для большинства случаев.

Всегда спрашивать у конечного пользователя

ESET Server Security не выполняет никаких автоматических действий. Выбрать действие предлагается пользователю.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел параметров модуля ThreatSense позволяет определить типы файлов, которые не нужно сканировать.

другое.

При настройке модуля ThreatSense также доступны представленные ниже параметры раздела **Другое**.

Сканировать альтернативные потоки данных (ADS)

Альтернативные потоки данных, используемые файловой системой NTFS, — это связи файлов и папок, которые не обнаруживаются при использовании обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запускать фоновое сканирование с низким приоритетом

Каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

Регистрировать все объекты

Если этот параметр выбран, в журнал будут записываться все просканированные файлы, включая незараженные.

Включить интеллектуальную оптимизацию

При включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense конкретных модулей.

Сохранить отметку о времени последнего доступа

Установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Параметры объектов по умолчанию

Включите для использования настроек по умолчанию (без ограничений). ESET Server Security будет игнорировать пользовательские настройки.

Максимальный размер объекта

Определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты будет сканировать только объекты меньше указанного размера. Эту опцию рекомендуется изменять только опытным пользователям, у которых есть веские основания для исключения больших объектов из сканирования. Значение по умолчанию: не ограничено.

Максимальная продолжительность сканирования объекта (с)

Определяет максимальное значение времени сканирования объекта. Если значение здесь укажет пользователь, модуль защиты прекратит сканирование объекта по истечении указанного времени, вне зависимости от того, было ли сканирование завершено. Значение по умолчанию: не ограничено.

Настройки сканирования архивов

Чтобы изменить параметры сканирования архивов, снимите флажок **Параметры сканирования архивов по умолчанию**.

Уровень вложенности архивов

Определяет максимальную глубину проверки архивов. Значение по умолчанию: 10. Для объектов, обнаруженных защитой почтового транспорта, фактическая глубина вложенности составляет +1 уровень, поскольку архив, вложенный в почтовое сообщение, считается первым уровнем.

> ✓ Если указан уровень вложенности 3, файл архива с уровнем вложенности 3 будет сканироваться на транспортном уровне только до фактического уровня 2. Поэтому, если необходимо сканировать архивы защитой почтового транспорта до уровня 3, установите для параметра **Уровень вложенности архивов** значение 4.

Максимальный размер файла в архиве

Этот параметр позволяет задать максимальный размер файлов в архиве (когда они извлечены), которые должны сканироваться. Значение по умолчанию: не ограниченно.

> i Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

Дополнительные параметры ThreatSense

Дополнительные параметры ThreatSense для только что созданных и измененных файлов

Вероятность заражения вновь созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на сигнатурах, применяется расширенная эвристика, что делает возможным обнаружение новых угроз еще до выпуска обновлений модуля. В дополнение ко вновь созданным файлам выполняется также сканирование самораспаковывающихся файлов (.sfx) и программ-упаковщиков (исполняемых файлов с внутренним сжатием).

По умолчанию архивы сканируются до 10-го уровня вложенности и проверяются независимо от их фактического размера. Для изменения настроек проверки архивов отключите параметр **Настройки проверки архивов по умолчанию**.

Дополнительные параметры ThreatSense для исполняемых файлов

По умолчанию расширенная эвристика при исполнении файлов не применяется. Если этот параметр включен, настоятельно рекомендуется включить оптимизацию Smart и ESET LiveGrid®, чтобы уменьшить воздействие на производительность системы.

Исключенные из сканирования расширения файлов

Расширение является частью имени файла, разделенного точкой. Расширение определяет тип файла. Обычно проверяются все файлы. Однако если нужно исключить файлы с определенным расширением, чтобы не применять к ним сканирование, можно настроить параметр ThreatSense. Исключение может быть полезно, если сканирование определенных типов файлов препятствует правильному запуску приложения.

Чтобы добавить новое расширение в список, щелкните **Добавить**. Введите расширение в текстовое поле (например, tmp) и нажмите кнопку **OK**. Если выбрать **Добавить несколько значений**, можно добавить несколько расширений файлов, разделенных линиями, запятыми или точками с запятой (например, в раскрывающемся меню в качестве разделителя выберите **Точка с запятой** и введите `edb;eml;tmp`).
Также можно использовать специальный символ «?» (вопросительный знак). Вопросительный знак заменяет любой символ (например, `?db`).

Чтобы отобразить расширение (тип файла) для всех файлов в операционной системе Windows, снимите флажок **Скрыть расширения для известных типов файлов** в разделе **Панель управления** > **Параметры папки** > **Просмотр**.

Исключения для процессов

Функция исключения процессов позволяет исключать процессы приложений только из сканирования по доступу, которое выполняется для защиты от вредоносных программ. Из-за высокой важности выделенных серверов (сервера приложений, сервера хранилища и т. д.) необходимо регулярно выполнять резервное копирование, чтобы гарантировать своевременное восстановление данных после инцидентов любого рода.

Чтобы ускорить резервное копирование, сделать процесс целостнее, а службу — доступнее, во время резервного копирования используются техники, которые могут конфликтовать с защитой от вредоносных программ, действующей на файловом уровне. Подобные проблемы могут возникать и при попытке динамического переноса виртуальных машин.

Единственный эффективный способ избежать обеих ситуаций — отключить программное обеспечение защиты от вредоносных программ. Если исключить некоторые процессы (например, процессы в решении резервного копирования), то все операции с файлами, которые касаются исключенных процессов, игнорируются и считаются безопасными. Таким образом факторы, мешающие резервному копированию, сводятся к минимуму. Рекомендуется проявлять осторожность при создании исключений, так как исключенное средство резервного копирования может взаимодействовать с зараженными файлами, не вызывая предупреждений (поэтому расширенные разрешения можно использовать только в модуле защиты в реальном времени).

Исключения процессов помогают свести к минимуму риск возможных конфликтов и улучшить

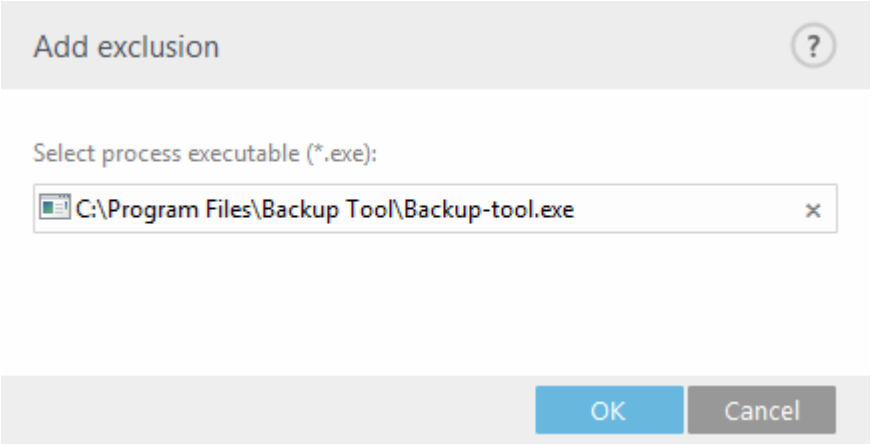
производительность исключенных приложений, что, в свою очередь, улучшает общую производительность операционной системы и повышает уровень ее стабильности. Исключение процесса или приложения исключает его исполняемый файл (*.exe*).

Исполняемые файлы можно добавить в список исключенных процессов с помощью элемента **Расширенные параметры (F5)** > **Detection engine** > **Защита файловой системы в реальном времени** > **Основное** > **Исключения для процессов**, или используя список запущенных процессов из основного меню **Инструменты** > **Запущенные процессы**.

Эта функция была разработана для исключения инструментов резервного копирования. Исключение процесса резервного копирования из процесса сканирования не только обеспечивает стабильность системы, но также не влияет на производительность резервного копирования, так как резервная копия не замедляется во время работы.

Щелкните элемент **Изменить**, чтобы открыть окно управления **Исключения для процессов**, где можно **Добавить** исключения и просмотреть исполняемый файл (например, Backup-tool.exe), который будет исключен из сканирования.
Когда процесс *.exe* исключен, мониторинг его исполняемого файла не выполняется. Программа ESET Server Security не контролирует активность исключенного процесса. Не сканируются также и операции с файлами, которые выполняет процесс.

Если функция просмотра при выборе исполняемого файла процесса не используется, необходимо вручную ввести полный путь к исполняемому файлу. В противном случае исключение не будет работать корректно, а HIPS может сообщать об ошибках.



Также можно **изменить** существующие процессы или **удалить** их из исключений.

Защита доступа в Интернет не учитывает эти исключения. Поэтому если исключить исполняемый файл веб-браузера, загружаемые файлы все равно будут сканироваться. То есть заражение все же можно обнаружить. Этот сценарий — всего лишь пример. Не рекомендуется создавать исключения для веб-браузеров.

Облачная защита

ESET LiveGrid® — это современная система раннего обнаружения угроз, состоящая из нескольких облачных технологий. Она обнаруживает возникающие угрозы, пользуясь принципом репутации, и оптимизирует процесс сканирования благодаря использованию «белого» списка. За счет потоковой передачи информации об угрозах в облако вирусная лаборатория ESET своевременно реагирует на угрозы и предоставляет актуальную и постоянную защиту.

Пользователь может проверять репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET LiveGrid®.

При установке ESET Server Security выберите один из описанных ниже вариантов.

- Систему ESET LiveGrid® можно не включать. Функциональность программного обеспечения при этом не теряется, но в некоторых случаях решение ESET Server Security может реагировать на новые угрозы медленнее, чем обновление модуля обнаружения.

- В ESET LiveGrid® можно настроить отправку анонимной информации о новых угрозах и файлах, содержащих неизвестный опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.

ESET LiveGrid® собирает о компьютерах пользователей информацию, которая связана с новыми обнаруженными угрозами. Это может быть образец или копия файла, в котором возникла угроза, путь к такому файлу, его имя, дата и время, имя процесса, в рамках которого угроза появилась на компьютере, и сведения об операционной системе.

По умолчанию программа ESET Server Security отправляет подозрительные файлы в вирусную лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как .docx и .xlsx. Добавить можно также другие расширения, если вы или ваша организация предпочли бы не отправлять некоторые файлы.

Включить систему репутации ESET LiveGrid® (рекомендуется)

Система репутации ESET LiveGrid® увеличивает эффективность решений ESET для защиты от вредоносных программ, так как благодаря ей сканируемые файлы сопоставляются с элементами «белого» и «черного» списков в облаке.

Включить систему обратной связи ESET LiveGrid®

Данные будут отправлены в исследовательскую лабораторию ESET для дальнейшего анализа.

Отправлять отчеты об аварийном завершении и данные диагностики

Отправляйте такие данные, как отчеты об аварийном завершении работы, дампы памяти или модулей.

Отправить анонимную статистическую информацию

Разрешить ESET собирать информацию о недавно обнаруженных угрозах: информацию о названии угрозы, дате и времени обнаружения, способе обнаружения и связанных метаданных, отсканированных файлах (хэш, имя файла, источник файла, телеметрия), заблокированных и подозрительных URL-адресах, версии и конфигурации продукта, включая информацию об операционной системе.

Контактный адрес электронной почты (необязательно)

Адрес электронной почты можно отправить вместе с подозрительными файлами, чтобы специалисты ESET могли связаться с вами, если для анализа потребуется дополнительная информация. Обратите внимание, что компания ESET связывается с пользователями только для

уточнения информации.

Отправка образцов

Автоматическая отправка зараженных образцов
Все зараженные образцы будут отправлены в ESET для анализа, чтобы улучшить обнаружение в будущем.
• Все зараженные образцы
• Все образцы, кроме документов
• Не отправлять
Автоматическая отправка подозрительных образцов
Компании ESET на анализ отправляются подозрительные образцы, похожие на угрозы, и/или образцы с необычными характеристиками или поведением.
• **Исполняемый файл** — включает исполняемые файлы: .exe, .dll, .sys
• **Архивы** — включает файлы архивов следующих типов: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
• **Сценарии** — включает файлы сценариев следующих типов: .bat, .cmd, .hta, .js, .vbs, .js, .ps1
• **Другие** — включает файлы следующих типов: .jar, .reg, .msi, .swf, .lnk
• **Возможный спам** — улучшает глобальное обнаружение спама.
• **Документы** — Включает документы Microsoft Office или PDF-файлы с активным контентом
Исключения
Нажав параметр Изменить рядом с элементом «Исключения» в ESET LiveGrid®, можно настроить способ отправки сведений об угрозах в антивирусную лабораторию ESET для анализа.
Максимальный размер образцов (МБ)
Определите максимальный размер проверяемых образцов.

ESET LiveGuard Advanced

Чтобы включить службу ESET LiveGuard Advanced на клиентском компьютере, в веб-консоли ESET PROTECT создайте новую политику в веб-консоли ESET PROTECT или измените имеющуюся и назначьте ее на компьютерах, где нужно использовать ESET LiveGuard Advanced.

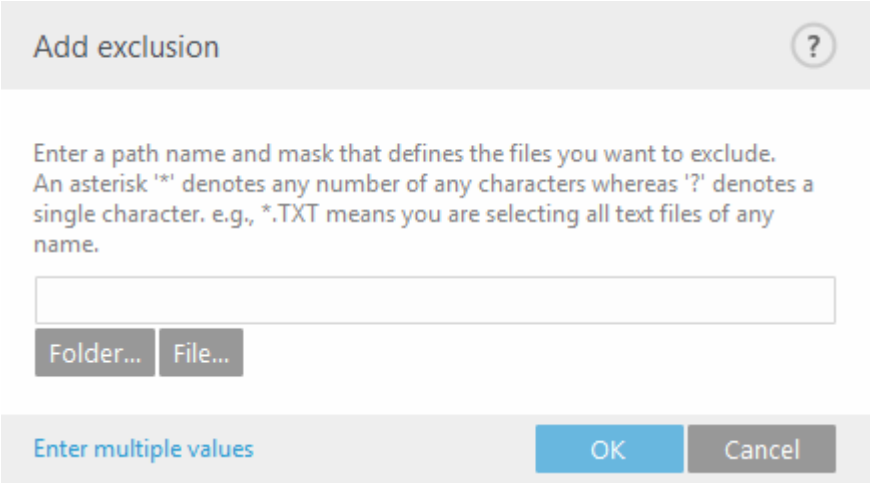
Фильтр исключений

Фильтр исключений дает возможность указать папки и файлы, которые не нужно отправлять на анализ (например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, например документы и электронные таблицы).

Указанные в списке файлы никогда не будут отправляться в лаборатории ESET на анализ, даже если они содержат подозрительный код.

Файлы наиболее распространенных типов (*.doc* и т. п.) исключаются по умолчанию. При желании список исключенных файлов можно дополнять.

Если система ESET LiveGrid® использовалась ранее, но была отключена, могут существовать пакеты данных, предназначенные для отправки. Эти пакеты будут отправлены в ESET даже после выключения системы. После отправки всей текущей информации новые пакеты создаваться не будут.



При обнаружении подозрительного файла его можно отправить в лабораторию ESET на анализ. Если это вредоносное приложение, его обнаружение будет включено в следующее обновление модуля обнаружения.

Процессы сканирования вредоносных программ

В этом разделе приведены варианты выбора параметров сканирования.

> Этот переключатель профилей сканирования применяется к **сканированию компьютера по требованию**, сканированию Hyper-V и к сканированию OneDrive.

Выбранный профиль

Определенный набор параметров, используемых сканером по требованию. Вы можете использовать один из предопределенных профилей сканирования или создать новый. Профили сканирования используют разные параметры модуля ThreatSense.

Список профилей

Чтобы создать профиль, нажмите кнопку **Изменить**. Введите имя профиля и нажмите кнопку **Добавить**. Новый профиль отобразится в раскрывающемся меню **Выбранный профиль**, в котором отображаются существующие профили сканирования.

Объекты сканирования

Чтобы просканировать определенный целевой объект, нажмите кнопку **Изменить** и выберите один из вариантов в раскрывающемся меню или определенные целевые объекты в дереве папок.

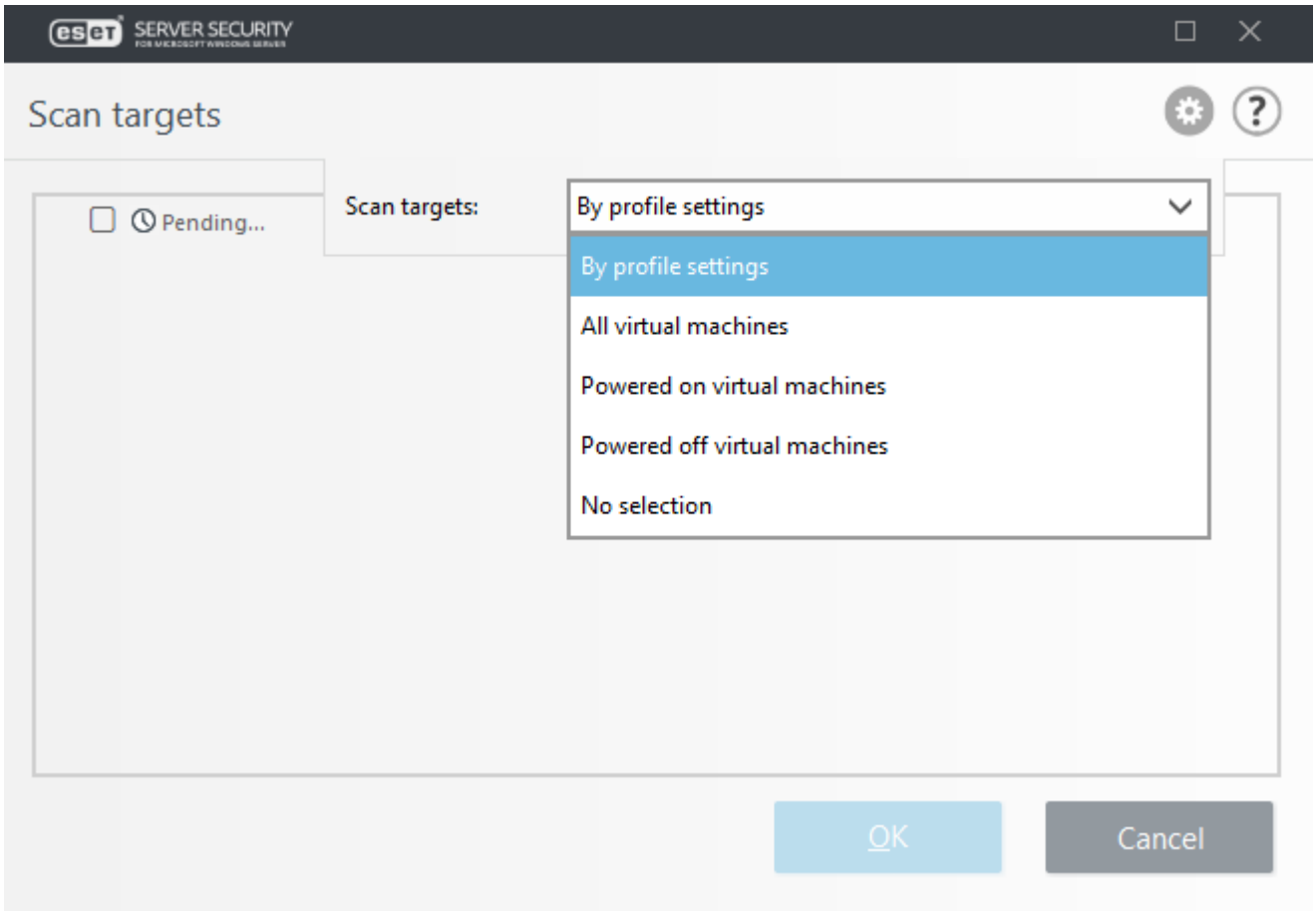
Параметры ThreatSense

Измените параметры сканирования для модуля сканирования компьютера по требованию.

Защита по требованию и на основе машинного обучения

Создание отчетов выполняется модулем обнаружения и компонентом машинного обучения.

Окно сканирования Hyper-V:



В раскрывающемся меню **Объекты сканирования** для **Hyper-V** можно выбрать предварительно выбранные объекты сканирования.

По параметрам профиля	Выбираются объекты, указанные в выбранном профиле сканирования.
Все виртуальные машины	Выбираются все виртуальные машины.
Включенные виртуальные машины	Выбираются все активные виртуальные машины.
Выключенные виртуальные машины	Выбираются все неактивные виртуальные машины.
Ничего не выбирать	Выбор объектов отменяется.

Чтобы выполнить сканирование с выбранными параметрами, нажмите кнопку **Сканировать**. После завершения сканирования проверьте расположение **Файлы журналов** > Сканирование Hyper-V.

Диспетчер профилей

В раскрывающемся меню Профиль сканирования можно выбрать предварительно заданные профили сканирования.

- Сканирование Smart
- Сканирование через контекстное меню
- Детальное сканирование

- Мой профиль (применяется к сканированию Hyper-V, профилям обновления и сканированию OneDrive)

Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Диспетчер профилей используется в трех разделах ESET Server Security.

Сканирование компьютера по требованию

Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Обновление

Редактор профилей дает пользователям возможность создавать новые профили обновления. Пользовательские профили обновлений нужны только в том случае, если компьютер подключается к серверам обновлений с помощью разных средств.

Сканирование Hyper-V

Создайте новый профиль, нажав кнопку **Изменить** рядом с элементом **Список профилей**. Новый профиль отобразится в раскрывающемся меню **Выбранный профиль**, в котором содержатся существующие профили сканирования.

Сканирование OneDrive

Создайте новый профиль, нажав кнопку **Изменить** рядом с элементом **Список профилей**. Новый профиль отобразится в раскрывающемся меню **Выбранный профиль**, в котором содержатся существующие профили сканирования.

Объекты профиля

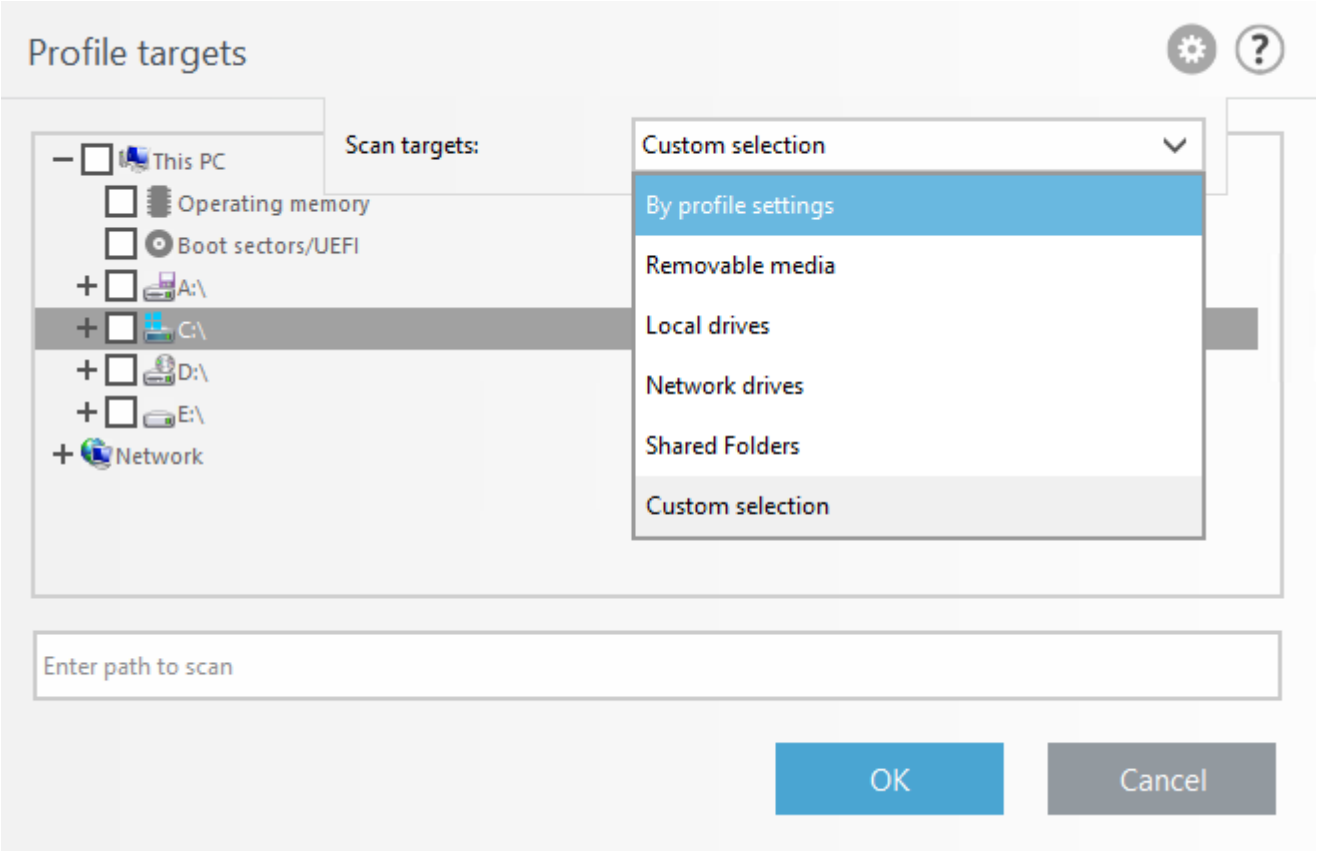
Можно указать, что необходимо сканировать на наличие заражений. Выберите объекты (память, загрузочные сектора и UEFI, диски, файлы и папки, сеть) из древовидной структуры, в которой перечислены все доступные объекты системы. Щелкните значок шестеренки в левом верхнем углу, чтобы получить доступ к раскрывающимся меню **Объекты сканирования** и **Профиль сканирования**.

> i Этот переключатель профилей сканирования применяется к сканированию компьютера по требованию, сканированию Hyper-V и к сканированию OneDrive.

Оперативная память	Сканирование всех процессов и данных, которые в настоящее время используются оперативной памятью.
Загрузочные секторы/UEFI	Сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI можно прочитать в глоссарии.

Оперативная память	Сканирование всех процессов и данных, которые в настоящее время используются оперативной памятью.
База данных WMI	Сканирование всей базы данных инструментария управления Windows (WMI), всех пространств имен, всех экземпляров класса и всех свойств. Поиск ссылок на зараженные файлы и вредоносные программы, внедренные в виде данных.
Системный реестр	Сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы и вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери важных данных.

Чтобы быстро перейти к объекту сканирования или добавить целевую папку или файлы, укажите целевой каталог в пустом поле под списком папок.



В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

По параметрам профиля	Выбираются объекты, указанные в выбранном профиле сканирования.
Съемные носители	Выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
Жесткие диски	Выбираются все жесткие диски системы.
Сетевые диски	Выбираются все подключенные сетевые диски.
Общие папки	Выбираются все общие папки на локальном сервере.
Пользовательский выбор	Выбор всех объектов отменяется. После этого вы сможете выбрать элементы, как вам нужно.

Для быстрого перехода к какому-либо объекту сканирования (файлу или папке) с

последующим его добавлением в список сканирования введите путь к этому объекту в поле, которое находится ниже древовидной структуры. Путь к объекту указывается с учетом регистра.

В раскрывающемся меню **Профиль сканирования** можно выбрать предварительно определенные профили сканирования.

- Сканирование Smart
- Сканирование через контекстное меню
- Детальное сканирование

В этих профилях сканирования используются другие параметры модуля ThreatSense.

Отобразить ход выполнения сканирования

Если нужно выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Этот параметр полезен, если нужен только обзор зараженных файлов и сведения об этих заражениях (если они вообще есть). Можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройки** > **Параметры ThreatSense** > **Очистка**. Информация о сканировании сохраняется в журнале сканирования.

Пропустить исключения

Если выбрать Пропустить исключения, при сканировании игнорируются исключения, которые в противном случае применяются.

Объекты сканирования

Если нужно просканировать только определенный объект, можно использовать **Выборочное сканирование** и выбрать один из вариантов в раскрывающемся меню **Объекты сканирования**, или выбрать определенные объекты в дереве папок.

Селектор профиля объектов сканирования применяется к:

- Сканирование по требованию
- Сканирование Hyper-V
- Сканирование OneDrive

Для быстрого перехода к какому-либо объекту сканирования или для добавления нового объекта (файла или папки) укажите нужный объект в пустом поле под списком папок. Это возможно только в том случае, если в древовидной структуре не выбраны никакие объекты, а в меню **Объекты сканирования** выбран пункт **Ничего не выбирать**.

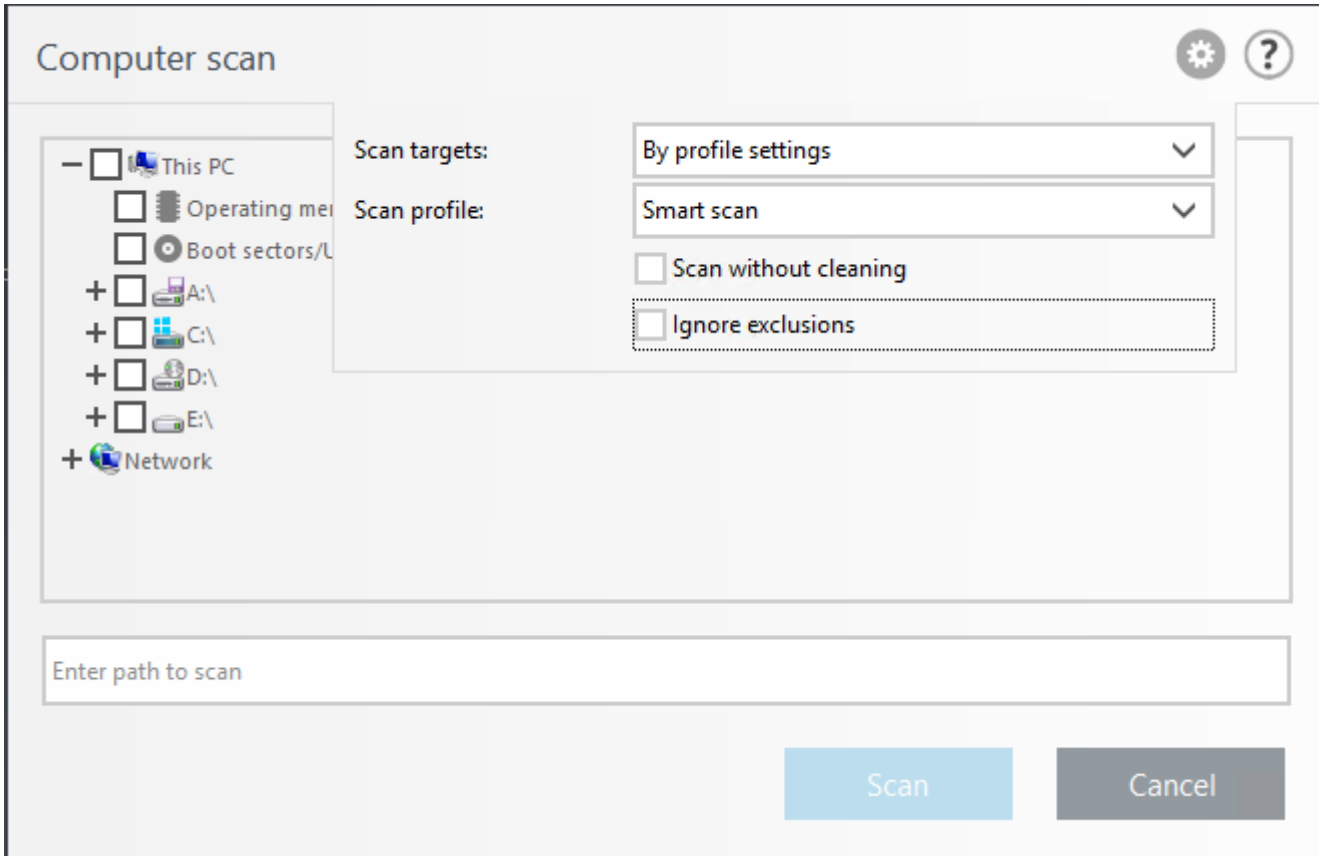
Оперативная память	Сканирование всех процессов и данных, которые в настоящее время используются оперативной памятью.
Загрузочные секторы/UEFI	Сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI можно прочитать в глоссарии.
База данных WMI	Сканирование всей базы данных инструментария управления Windows (WMI), всех пространств имен, всех экземпляров класса и всех свойств. Поиск ссылок на зараженные файлы и вредоносные программы, внедренные в виде данных.
Системный реестр	Сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы и вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери важных данных.

В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно выбранные объекты сканирования.

По параметрам профиля	Выбираются объекты, указанные в выбранном профиле сканирования.
Съемные носители	Выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
Жесткие диски	Выбираются все жесткие диски системы.
Сетевые диски	Выбираются все подключенные сетевые диски.
Общие папки	Выбираются все общие папки на локальном сервере.
Пользовательский выбор	Выбор всех объектов отменяется. После этого вы сможете выбрать элементы, как вам нужно.

В раскрывающемся меню Профиль сканирования можно выбрать профиль, который будет использован для сканирования выбранных объектов. По умолчанию используется профиль **Интеллектуальное сканирование**. Существует еще два предварительно заданных профиля сканирования: Детальное сканирование и **Сканирование через контекстное меню**. В этих профилях сканирования используются другие параметры модуля ThreatSense.

Окно **Выборочное сканирование**:



Отобразить ход выполнения сканирования

Если нужно выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Этот параметр полезен, если нужен только обзор зараженных файлов и сведения об этих заражениях (если они вообще есть). Можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройки** > **Параметры ThreatSense** > **Очистка**. Информация о сканировании сохраняется в журнале сканирования.

Пропустить исключения

Можно выбрать сканирование с игнорированием исключений, которые в противном случае применяются.

Сканирование

Выполняется сканирование с выбранными параметрами.

Сканировать как админ

Позволяет выполнять сканирование под учетной записью администратора. Воспользуйтесь этой функцией, если текущая учетная запись пользователя не имеет достаточных прав на доступ к файлам, которые следует сканировать. Обратите внимание, что данная кнопка недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

Сканирование в состоянии простоя

Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование всех локальных дисков. **Сканирование в состоянии простоя** запускается в случае пребывания компьютера в одном из следующих режимов:

- Выключенный экран или заставка
- блокировка компьютера;
- выход пользователя.

Сканировать даже в случае работы компьютера от аккумулятора

По умолчанию в состоянии простоя сканирование не работает, если компьютер (ноутбук) работает от батареи.

Включить ведение журналов

Чтобы результаты сканирования компьютера регистрировались в разделе Файлы журнала (в главном окне программы щелкните «Файлы журнала» и из раскрывающегося меню выберите тип журнала «Сканирование компьютера»).

Параметры ThreatSense

Изменение параметров сканирования в состоянии простоя.

Сканирование файлов, исполняемых при запуске системы

Проверка автоматического запуска по умолчанию будет выполняться при запуске системы (вход пользователя в систему) и после успешного обновления модуля. Параметры этого сканирования определяются конфигурацией и задачами планировщика.

Параметры проверки запуска являются частью задачи планировщика **Проверка файлов при загрузке системы**.

Чтобы изменить параметры такого сканирования, последовательно выберите элементы **Сервис** > **Планировщик**, выберите задание **Автоматическая проверка файлов при запуске системы** (вход пользователя или обновление модуля) и нажмите кнопку **Изменить**. На последнем этапе можно настроить более подробные параметры автоматической проверки файлов при запуске системы.

Автоматическая проверка файлов при запуске системы

При создании запланированной задачи «Проверка файлов, исполняемых при запуске системы» предоставляется несколько вариантов настройки следующих параметров.

Раскрывающееся меню Объект сканирования задает глубину сканирования файлов, исполняемых при запуске системы. Файлы упорядочены по возрастанию в соответствии с указанными ниже критериями.

- Все зарегистрированные файлы (сканируется больше всего файлов)
- Редко используемые файлы
- Обычно используемые файлы
- Часто используемые файлы
- Только наиболее часто используемые файлы (сканируется меньше всего файлов)

Кроме того, существуют две особые группы объектов сканирования.

Файлы, которые запускаются перед входом пользователя

Содержит файлы из таких папок, которые можно открыть без входа пользователя в систему (в том числе большинство элементов, исполняемых при запуске системы: службы, объекты модуля поддержки браузера, уведомления Winlogon, задания в планировщике Windows, известные библиотеки DLL и т. д.).

Файлы, которые запускаются после входа пользователя

Содержит файлы из таких папок, которые можно открыть только после входа пользователя в систему (в том числе файлы, запускаемые под определенными учетными записями, обычно это файлы из папки *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Списки подлежащих сканированию файлов являются фиксированными для каждой описанной выше группы.

Приоритет сканирования

Уровень приоритета, используемый для определения условий начала сканирования.

- **Обычный** — средняя нагрузка на систему.
- **Более низкий** — низкая нагрузка на систему.
- **Самый низкий** — минимальная нагрузка на систему.
- **При простое** — задача будет выполняться только при бездействии системы.

Съемные носители

Программа ESET Server Security обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств). Данный модуль позволяет сканировать вставленный носитель. Это может быть удобно, если администратору компьютера нужно, чтобы пользователи не подключали съемные носители с нежелательным содержимым.

Действие, которое следует предпринять после подключения съемного носителя

Выбор действия, которое будет выполняться после подключения съемного носителя к компьютеру (CD/DVD/USB).

- **Не сканировать** — не будет выполнено никаких действий, а окно Обнаружено новое устройство будет закрыто.

- **Автоматическое сканирование устройств** — выполняется сканирование подключенного съемного носителя по требованию.

- **Показать параметры сканирования** — переход в раздел настройки работы со съемными носителями.

Когда вставляется съемный носитель, отображается указанное ниже диалоговое окно.

- **Сканировать сейчас** — начнется сканирование съемного носителя.

- **Сканировать позже** — сканирование съемного носителя будет отложено.

- **Настройки** — вызов дополнительных настроек.

- **Всегда использовать выбранный вариант** — если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

Кроме того, в ESET Server Security есть модуль контроля устройств, дающий возможность задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Функция защиты документов обеспечивает безопасность в дополнение к функции защиты файловой системы в реальном времени. Ее можно отключить, чтобы улучшить производительность систем, которые не содержат большого количества документов Microsoft Office.

Интегрировать в систему

Этот параметр улучшает защиту документов Microsoft Office (не требуется в обычных условиях).

Параметры ThreatSense

Измените параметры защиты документа.

> Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздние версии или Microsoft Internet Explorer 5.0 и более поздние версии).

Сканирование Hyper-V

Текущая версия функции сканирования Hyper-V поддерживает сканирование сетевой и автономной виртуальных систем в Hyper-V. Поддерживаемые типы сканирования в соответствии с размещенной системой Windows Hyper-V и состояния виртуальной системы показаны ниже.

Виртуальные системы с функцией Hyper-V	Активная ВМ	Неактивная ВМ
Windows Server 2022 Hyper-V	только чтение	только чтение/очистка
Windows Server 2019 Hyper-V	только чтение	только чтение/очистка
Windows Server 2016 Hyper-V	только чтение	только чтение/очистка
Windows Server 2012 R2 Hyper-V	только чтение	только чтение/очистка
Windows Server 2012 Hyper-V	только чтение	только чтение/очистка
Windows Server 2008 R2 с пакетом обновления 1 с функцией Hyper-V	нет сканирования	только чтение/очистка

Требования к оборудованию

На сервере не должно возникать проблем с производительностью из-за работы виртуальных машин. Сканирование использует в основном ресурсы ЦП. Для сканирования подключенных к Интернету виртуальных машин требуется наличие свободного места на диске. Объем доступного места на диске должен быть по крайней мере вдвое больше пространства, используемого контрольными точками или моментальными снимками и виртуальными дисками.

Определенные ограничения

- Сканирование хранилищ RAID, составных томов и динамических дисков не поддерживается, так как таков характер динамических дисков. Поэтому динамические диски, если возможно, рекомендуется не использовать в виртуальных машинах.

- Сканирование всегда выполняется на текущей виртуальной машине. Сканирование не затрагивает ее контрольные точки и моментальные снимки.

- Сейчас решение ESET Server Security не поддерживает работу системы Hyper-V на сервере в кластере.

- Виртуальные машины на хосте Hyper-V, находящемся под управлением Windows Server 2008 R2 с пакетом обновления 1, можно сканировать лишь в режиме только для чтения (без очистки) вне зависимости от того, какой уровень очистки выбран в разделе Параметры ThreatSense.

> Хотя ESET Security поддерживает сканирование MBR-секторов виртуального диска, из способов сканирования для данных объектов поддерживается лишь сканирование в режиме только для чтения. Этот параметр можно изменить, последовательно щелкнув элементы **Расширенные параметры** (F5) > **Detection engine** > **Сканирование Hyper-V** > Параметры ThreatSense > **Загрузочные секторы**.

Подлежащая сканированию виртуальная машина не подключена к Интернету: выключенное состояние

ESET Server Security использует управление Hyper-V для обнаружения виртуальных дисков и подключения к ним. Таким образом, программа ESET Server Security имеет такой же доступ к содержимому виртуальных дисков, что и к содержимому любого обычного диска.

Подлежащая сканированию виртуальная машина подключена к Интернету: запущена, приостановлена, сохранена

Решение ESET Server Security использует управление Hyper-V для обнаружения виртуальных дисков. Подключение к этим дискам невозможно. Поэтому решение ESET Server Security создает контрольную точку/моментальный снимок виртуальной машины, а затем подключается к ней. После сканирования контрольная точка или моментальный снимок удаляется. Это означает, что сканирование в режиме только для чтения возможно, потому что на запущенные виртуальные машины сканирование не влияет.

Выделите продукту ESET Server Security до одной минуты на создание моментального снимка или контрольной точки в ходе сканирования. Примите это к сведению при выполнении сканирования Hyper-V на большом количестве виртуальных машин.

Принципы именования

Модуль сканирования Hyper-V использует следующее соглашение об именовании:

```
VirtualMachineName\DiskX\VolumeY
```

Где X — это номер диска, а Y — номер тома. Например:

```
Computer\Disk0\Volume1
```

Числовой суффикс соответствует порядку обнаружения, который идентичен порядку, отображаемому в диспетчере дисков виртуальной машины. Такой принцип именования используется в древовидном списке объектов, подлежащих сканированию, а также в индикаторе выполнения и файлах журналов.

Выполнение сканирования

- По требованию — щелкните **Сканирование Hyper-V** для просмотра списка виртуальных машин и томов, доступных для сканирования. Выберите виртуальные машины, диски или тома, которые нужно просканировать, и нажмите кнопку **Сканировать**.

- Создание задач в планировщике.

- С помощью ESET PROTECT в качестве клиентской задачи под названием Сканирование сервера.

- Управление и запуск сканирования Hyper-V осуществляется через eShell.

Кроме того, можно запустить несколько процессов сканирования Hyper-V одновременно. После завершения сканирования вы получите уведомление со ссылкой на файлы журнала.

Возможные проблемы

- В случае сканирования виртуальной машины, подключенной к Интернету, необходимо создать контрольную точку или моментальный снимок соответствующей виртуальной машины. При этом в процессе создания точки или снимка некоторые основные действия

виртуальной машины могут быть ограничены или отключены.

• В случае сканирования виртуальной машины, не подключенной к Интернету, вы не сможете включить ее до завершения сканирования.

• Диспетчер Hyper-V позволяет присвоить двум разным виртуальным машинам одинаковые имена, и это может стать проблемой, когда, просматривая журналы сканирования, вы пытаетесь различить компьютеры.

Hyper-V и защита на основе машинного обучения

Создание отчетов выполняется модулем обнаружения и компонентом машинного обучения.

Параметры ThreatSense

Для изменения параметров сканирования Hyper-V.

Сканирование OneDrive

Основная информация

Можно настроить действие и карантин.
Предпринимаемое действие, если файл заражен:
• **Ничего не предпринимать**. Изменения в файле не будут применяться.
• **Удалить**. Выполняется перемещение в папку карантина и удаление файлов из хранилища OneDrive. При этом файлы остаются доступными в корзине хранилища OneDrive.
Поместить зараженные файлы на карантин
Когда этот параметр включен, помеченные для удаления файлы перемещаются на карантин. Отмените выбор этой настройки, чтобы отключить карантин и предотвратить накопление файлов в папке карантина.

Дополнительные параметры

В этом разделе содержится информация о регистрации для функции сканирования OneDrive (идентификатор приложения, идентификатор объекта на портале Azure, отпечаток сертификата). Можно настроить время ожидания и ограничения для одновременной загрузки.

Профили

Чтобы создать профиль, нажмите кнопку **Изменить** рядом с элементом **Список профилей**, введите **имя профиля** и нажмите кнопку **Добавить**. Новый профиль отобразится в раскрывающемся меню **Выбранный профиль**, в котором отображаются существующие профили сканирования.
В раскрывающемся меню **Объект сканирования** можно выбрать предварительно заданный объект сканирования.
• **По профилю**. Выбираются объекты, указанные в выбранном профиле сканирования.
• **Все пользователи**. Выбираются все пользователи.
• **Ничего не выбирать**. Отмена всех выбранных объектов.
Чтобы выполнить сканирование с выбранными параметрами, щелкните **Сканировать**. После завершения всех операций сканирования проверьте расположение **Файлы журнала** > Сканирование OneDrive.
Параметры ThreatSense
Изменение параметров сканирования для модуля сканирования OneDrive.
Сканирование OneDrive и защита на основе машинного обучения
Создание отчетов выполняется модулем обнаружения и компонентом машинного обучения.

Система HIPS

Система предотвращения вторжений на узел защищает от вредоносных программ и нежелательных процессов, которые пытаются отрицательно повлиять на безопасность компьютера. В системе HIPS используется расширенный анализ поведения в сочетании с возможностями сетевой фильтрации по обнаружению, благодаря чему отслеживаются запущенные процессы, файлы и разделы реестра. Система HIPS отличается от защиты файловой системы в режиме реального времени и не является файерволом — она отслеживает только процессы, запущенные в операционной системе.

> ⚠ Изменения в параметры системы HIPS должны вносить только опытные пользователи. Неправильная настройка этих параметров может привести к нестабильной работе системы.

Включить модуль самозащиты

В программе ESET Server Security есть встроенная технология самозащиты, которая не позволяет вредоносным программам повредить или отключить защиту от таких программ, благодаря чему пользователь всегда уверен в защите компьютера. Изменения параметров «Включить систему HIPS» и «Включить модуль самозащиты» вступают в силу после перезапуска операционной системы Windows. Перезагрузить компьютер нужно и для полного отключения системы предотвращения вторжений на узел.

Включить защищенную службу

Корпорация Майкрософт предоставила концепцию защищенных служб с Microsoft Windows Server 2012 R2. Она защищает службы от вредоносных программ. Ядро ESET Server Security по умолчанию работает как защищенная служба. Эта функция доступна на Microsoft Windows Server 2012 R2 и новых операционных системах сервера.

Включить Advanced Memory Scanner

Работает в сочетании с блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения продуктами для защиты от вредоносных программ за счет использования умышленного запутывания или шифрования. Расширенный модуль сканирования памяти по умолчанию включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

Включить блокировщик эксплойтов

Предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов Microsoft Office. Блокировщик эксплойтов по умолчанию включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

Включить защита от программ-вымогателей

Чтобы использовать эту функцию, включите HIPS и ESET Live Grid. Дополнительные сведения о программах-шантажистках см. в глоссарии.

Режим фильтрации

Доступны следующие режимы фильтрации.

• **Автоматический режим** — включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер. Можно выполнять любые действия, кроме тех, которые запрещены правилом.

• **Интеллектуальный режим** — пользователь будет получать уведомления только об очень подозрительных событиях.

• **Интерактивный режим** — будут отображаться запросы на подтверждение операций: разрешить или запретить доступ, создать правило или временно запомнить это действие.

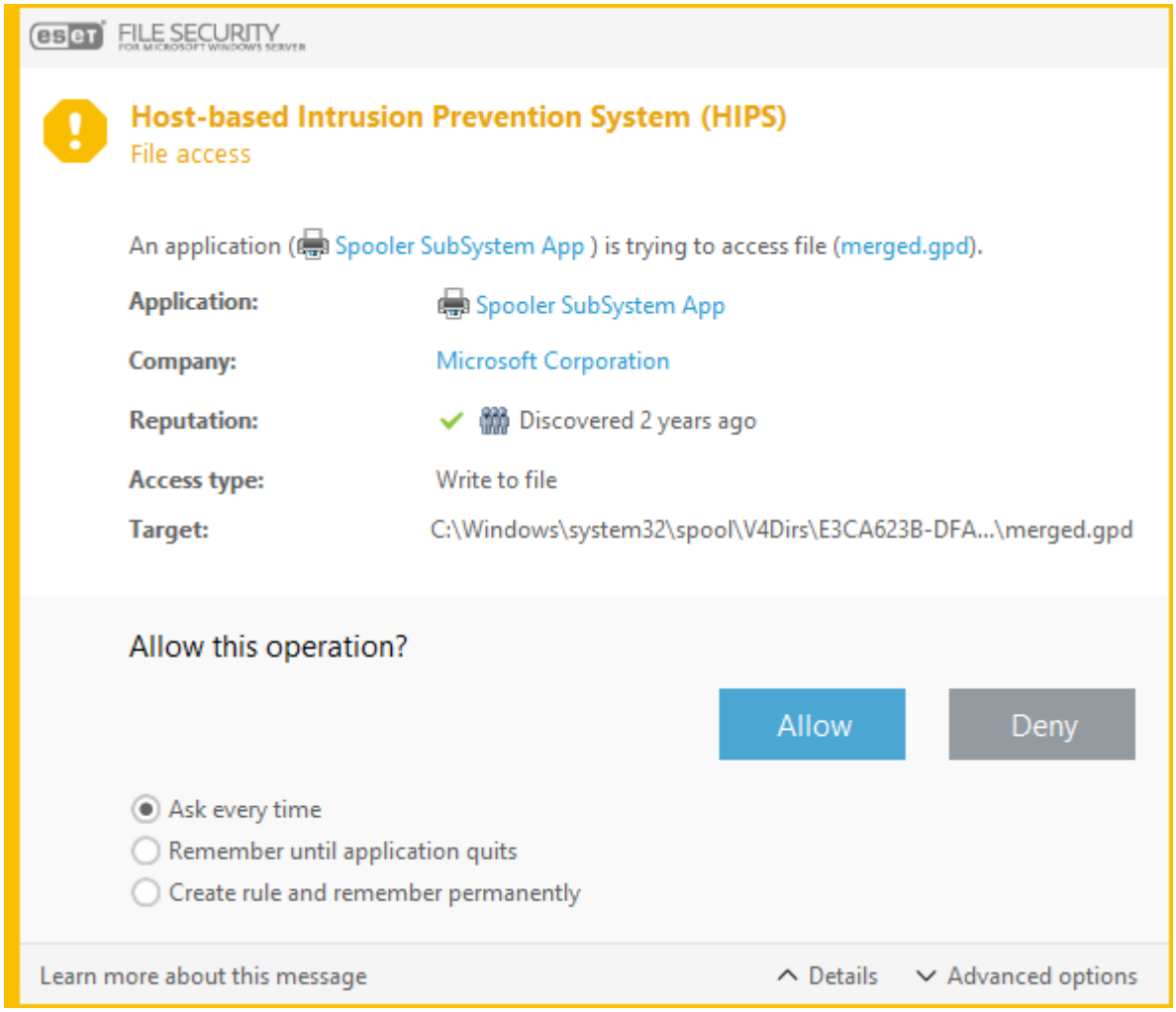
• **Режим на основе политики** — операции блокируются. Разрешаются только пользовательские и предварительно заданные правила.

• **Режим обучения** — операции включены, и после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе правил, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе режима обучения в раскрывающемся меню «Режим фильтрации HIPS» становится доступным параметр Режим обучения закончится с. Выберите длительность режима обучения. Максимальная длительность — 14 дней. Когда указанный период завершится, будет предложено изменить правила, созданные системой HIPS в режиме обучения. Кроме того, можно выбрать другой режим фильтрации или отложить решение и продолжить использовать режим обучения.

Правила

Правила определяют, каким приложениям будет предоставлен доступ к определенным файлам, частям реестра или другим приложениям. Система HIPS отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам персонального файервола. Нажмите кнопку Изменить, чтобы открыть окно управления правилами системы HIPS. Если для правила по умолчанию установлено действие **Запросить**, то при каждом запуске правила будет отображаться диалоговое окно. Для операции можно выбрать и другие действия: **Блокировать** или **Разрешить**. Если пользователь не выбирает действие в течение определенного времени, на основе правил выбирается новое действие.

В диалоговом окне можно создать правило на основе нового действия, обнаруживаемого системой HIPS, а затем определить условия, в соответствии с которыми это действие будет **разрешено** или **заблокировано**. Щелкните элемент **Подробности**, чтобы ознакомиться с дополнительной информацией. Правила, создаваемые таким способом, считаются равнозначными правилам, созданным вручную, поэтому правило, созданное в диалоговом окне, может быть менее подробным, чем правило, которое вызвало появление такого диалогового окна. Это значит, что после создания такого правила эта же операция может вызвать появление такого же окна.



Спрашивать каждый раз

При каждом запуске правила будет отображаться диалоговое окно. Для этой операции можно выбрать действия **Запретить** или **Разрешить**.

Запомнить до закрытия приложения

Если выбрать действие **Запретить** или **Разрешить**, будет создано временное правило системы HIPS, которое будет использоваться до закрытия соответствующего приложения. Кроме того, если изменить режим фильтрации, внести изменения в правила либо обновить модуль системы HIPS, после перезапуска системы временные правила будут удалены.

Создать правило и запомнить навсегда

Создание нового правила системы HIPS. Вы сможете позднее внести изменения в разделе управления правилами системы HIPS.

Параметры правил HIPS

В этом окне отображаются общие сведения об имеющихся правилах HIPS.

Правило	Указанное пользователем или автоматически выбранное имя правила.

Правило	Указанное пользователем или автоматически выбранное имя правила.
Включено	Отключите этот параметр, если следует оставить правило в списке, но при этом не использовать его.
Действие	Правило задает действие (Разрешить, Блокировать или Запросить), которое должно быть выполнено при соблюдении условий.
Источники	Правило будет использоваться только в том случае, если событие вызывается приложениями.
Объекты	Правило будет использоваться только в том случае, если операция связана с тем или иным файлом, приложением или записью реестра.
Серьезность регистрируемых событий	Если включить этот параметр, информация о данном правиле будет записываться в журнал HIPS.
Уведомить	Если запускается событие, в области уведомлений Windows отображается маленькое окно.

Создайте новое правило, щелкнув **добавить** новые правила HIPS или **изменить** выделенные записи.

Имя правила

Указанное пользователем или автоматически выбранное имя правила.

Действие

Правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.

Операции влияния

Выберите тип операции, к которому будет применяться правило. Правило будет использоваться только для этого типа операции и для выбранного объекта. Правило состоит из частей, в которых описываются условия выполнения этого правила.

Исходные приложения

Правило будет использоваться только в том случае, если событие вызывается указанными приложениями. Выберите **Определенные приложения** из раскрывающегося меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все приложения**, чтобы добавить все приложения.

> Некоторые операции определенных правил, предварительно заданных системой HIPS, невозможно заблокировать, и они разрешены по умолчанию. Кроме того, не все системные операции отслеживаются системой HIPS. Система HIPS отслеживает операции, которые могут считаться небезопасными.

Описание важных операций

Операции с файлами

Удалить файл	Приложение запрашивает разрешение на удаление целевого файла.

Удалить файл	Приложение запрашивает разрешение на удаление целевого файла.
Выполнить запись в файл	Приложение запрашивает разрешение на запись в целевой файл.
Непосредственный доступ к диску	Приложение пытается выполнить чтение с диска или запись на диск нестандартным образом, в обход стандартных алгоритмов Windows. Это может привести к изменению файлов без применения соответствующих правил. Эта операция может быть вызвана вредоносной программой, которая пытается избежать обнаружения, программным обеспечением резервного копирования, которое пытается создать точную копию диска, или диспетчером разделов, который пытается реорганизовать тома диска.
Установить глобальную ловушку	Вызов функции SetWindowsHookEx из библиотеки MSDN.
Загрузить драйвер	Установка и загрузка драйверов в системе.

Это правило будет использоваться, только если операция относится к данному объекту. Чтобы добавить новые файлы или папки, из раскрывающегося меню выберите **Определенные файлы** и нажмите **Добавить**. Чтобы добавить все приложения, можно выбрать пункт **Все файлы**.

Операции с приложениями

Выполнить отладку другого приложения	Прикрепление отладчика к процессу. При отладке приложения можно просмотреть и изменить многие сведения о его поведении и получить доступ к его данным.
Перехватывать события другого приложения	Исходное приложение пытается записать события, направленные на другое приложение (например, клавиатурный шпион, пытающийся записать события браузера).
Завершить/приостановить работу другого приложения	Приостановка, возобновление или завершение процесса (можно получить доступ непосредственно из обозревателя процессов или окна «Процессы»).
Запустить новое приложение	Запуск новых приложений или процессов.
Изменить состояние другого приложения	Исходное приложение пытается осуществить запись в память целевого приложения или выполнить код от его имени. Эта функциональность может быть полезна, если нужно защитить важное приложение путем конфигурирования его в качестве целевого приложения в правиле, которое блокирует использование этой операции.

Это правило будет использоваться, только если операция относится к данному объекту. Чтобы добавить новые файлы или папки, из раскрывающегося меню выберите **Определенные приложения** и нажмите **Добавить**. Чтобы добавить все приложения, можно выбрать пункт **Все приложения**.

Операции с реестром

Изменить параметры запуска	Любые изменения в настройках, определяющие, какие приложения будут запускаться при запуске Windows. Их можно найти, например, выполнив поиск раздела «Запуск» в реестре Windows.
Удалить из реестра	Удаление раздела реестра или его значения.
Переименовать раздел реестра	Переименование разделов реестра.
Изменить реестр	Создание новых значений разделов реестра, изменение существующих значений, перемещение данных в древовидной структуре базы данных или настройка прав пользователя или группы для разделов реестра.

Это правило будет использоваться, только если операция относится к данному объекту. Чтобы добавить новые файлы или папки, из раскрывающегося меню выберите **Определенные записи** и нажмите **Добавить**. Чтобы добавить все приложения, можно выбрать пункт **Все записи**.

> При вводе объекта можно использовать подстановочные знаки с определенными ограничениями. Вместо конкретного раздела в пути реестра можно использовать символ звездочки («*»). Например, *HKEY_USERS*\software can mean HKEY_USER\.default\software*, но не *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
> Путь *HKEY_LOCAL_MACHINE\system\ControlSet** не является допустимым путем раздела реестра. Путь, в котором содержится сочетание символов ***, означает «этот путь или любой путь на любом уровне после этого символа». Это единственный способ использования подстановочных знаков для обозначения целевых файлов. Сначала оценивается точный путь, а затем путь после подстановочного знака (*).

> ⚠ Если созданное правило будет слишком общим, появится соответствующее уведомление.

Дополнительные параметры системы HIPS

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

Драйверы, загрузка которых разрешена всегда

Загрузка выбранных драйверов разрешена всегда, вне зависимости от настроенного режима фильтрации, если они не заблокированы в явном виде правилом пользователя. Загрузка драйверов, отображенных в этом списке, разрешена всегда вне зависимости от режима фильтрации HIPS. Это не касается случаев, когда загрузка драйвера явным образом заблокирована правилом пользователя. Вы можете **добавить** новый драйвер, **изменить** или **удалить** выбранный драйвер из списка.

> Если щелкнуть элемент **Сброс**, драйверы, добавленные вручную, будут удалены из списка. Это может пригодиться, если вы добавили несколько драйверов и не можете удалить их из списка вручную.

Регистрировать все заблокированные операции

Все заблокированные операции будут записываться в журнал HIPS.

Сообщать об изменениях приложений, загружаемых при запуске системы

При добавлении или удалении приложения, загружаемого во время запуска системы, на рабочем столе отображается уведомление.

Обновить конфигурацию

В этом разделе указывается информация об источниках обновления, например сведения о серверах обновления и данные аутентификации для них.

> Для обеспечения правильной загрузки обновлений необходимо корректно задать все параметры обновлений. Если используется файервол, программе должно быть разрешено обмениваться данными через Интернет (например, через HTTP-соединение).

Основная информация

Выбрать профиль обновления по умолчанию
Выберите существующий или создайте новый профиль, который будет применяться для обновлений по умолчанию.
Очистить кэш обновлений
При возникновении проблем с обновлением нажмите кнопку **Очистить** для удаления из кэша временных файлов обновления.
Обновление программы/автоматическое обновление
Включено по умолчанию. Используйте ползунок для отключения автоматического обновления, если нужно временно не обновлять ESET Server Security. Рекомендуем оставить этот параметр включенным, чтобы в решении ESET Server Security применялись новейшие обновления и микрообновления компонентов программы, когда они становятся доступными.

> Обновления применяются после следующего перезапуска сервера.

Предупреждения об устаревшем модуле обнаружения

Автоматическая настройка максимального возраста модуля обнаружения / Максимальный возраст модуля обнаружения (в днях)
Используйте ползунок, чтобы отключить автоматическое устаревание модуля обнаружения и вручную задать максимальное время (в днях), по истечении которого модуль обнаружения будет считаться устаревшим. Значение по умолчанию — 7.
Откат модуля
Если вы подозреваете, что последнее обновление модуля обнаружений и/или модулей программы повреждено или работает нестабильно, можно выполнить откат к предыдущей версии и отключить обновления на определенный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени. ESET Server Security записывает моментальные снимки модуля обнаружений и программных модулей для использования с функцией Откат. Если нужно, чтобы снимки модуля обнаружений создавались, оставьте установленным флажок Создать снимки модулей.
Количество локально хранимых снимков
Определение количества хранящихся предыдущих снимков модулей.
Откат к предыдущим модулям
Щелкните Откатить, чтобы восстановить предыдущую версию модулей программы и временно отключить обновление.

Чтобы создать пользовательский профиль обновления, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**. Выберите профиль, который нужно изменить и измените параметры для типов обновлений модуля или создайте **зеркало обновлений**.

Обновления

Выберите в раскрывающемся меню тип обновления, который нужно использовать.
• **Регулярное обновление** — задаваемый по умолчанию, такой тип обновления обеспечивает автоматическую загрузку файлов обновлений с сервера ESET с минимальным расходом сетевого трафика.
• **Тестовое обновление** — обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на рабочих серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность.
• **Отложенное обновление** — позволяет загружать обновления со специальных серверов, предоставляя новые версии базы данных вирусов, с задержкой в несколько часов (т. е. после того, как обновления будут протестированы в реальных средах и признаны стабильными).

Включить оптимизацию доставки обновлений
Если этот параметр включен, файлы обновления загружаются из сети доставки содержимого. Отключение этого параметра может привести к перебоям и замедлению загрузки, когда выделенные серверы обновления ESET перегружены. Отключение этого параметра полезно, когда файервол имеет доступ только к IP-адресам сервера обновления ESET или не работает подключение к службам сети доставки содержимого.

Запрашивать подтверждение перед загрузкой обновления
При наличии доступного обновления будет предложено запросить подтверждение перед загрузкой.

Запрашивать подтверждение, если размер обновления превышает (КБ)
Если размер файла обновления больше значения, указанного в поле, появится соответствующее уведомление.

Обновления модулей
Для обновлений модулей по умолчанию задан параметр **Выбирать автоматически**. Сервер обновлений — это компьютер, на котором хранятся файлы обновлений. При использовании сервера ESET рекомендуется оставить параметры по умолчанию.

При использовании локального HTTP-сервера, который называется также зеркалом, сервер обновлений должен быть указан следующим образом: **http://computer_name_or_its_IP_address:2221**
Если используется локальный HTTP-сервер с поддержкой SSL, сервер обновлений должен быть указан следующим образом: https://computer_name_or_its_IP_address:2221
Если используется локальная общая папка, сервер обновлений должен быть указан следующим образом: \\computer_name_or_its_IP_address\shared_folder

Включить более частые обновления сигнатур обнаружения
Модуль обнаружения будет обновляться чаще. Если отключить этот параметр, качество обнаружения может ухудшиться.

Разрешить обновление модуля со съемных носителей
Выполняет обновление со съемного носителя, если он содержит созданное зеркало. Если установлен флажок**Автоматически**, обновления будут выполняться в фоновом режиме. Если диалоговые окна обновления должны отображаться, выберите **Всегда спрашивать**.

Обновление программы
Приостановка автоматического обновления для определенных профилей обновления временно отключает автоматическое обновление программы, например при подключении к Интернету с помощью других сетей или лимитных подключений. Чтобы иметь постоянный доступ к новейшим функциям и обеспечить максимальную защиту, следует включить этот параметр.

> В некоторых случаях для обновления может потребоваться перезапуск сервера.

Параметры подключения

Прокси-сервер
Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните Режим прокси-сервера и выберите один из трех перечисленных далее вариантов.
• **Не использовать прокси-сервер** — во время выполнения обновлений ESET Server Security не будет использоваться прокси-сервер.
• **Использовать общие параметры прокси-сервера** — будут использоваться параметры прокси-сервера, уже заданные в разделе Расширенные параметры (F5) > Сервис > Прокси-сервер.
• **Подключение через прокси-сервер** — используйте этот вариант в следующих случаях.

Для обновления ESET Server Security должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (Сервис > Прокси-сервер). В этом случае нужно указать следующие параметры: адрес прокси-сервера, порт передачи данных (3128 по умолчанию), а также имя пользователя и пароль для прокси-сервера (если необходимо).

Не были заданы общие параметры прокси-сервера, однако ESET Server Security будет подключаться к прокси-серверу для получения обновлений.

Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из браузера Internet Explorer в процессе установки программы, но если впоследствии они будут изменены (например, при смене поставщика услуг Интернета), нужно будет убедиться в том, что указанные в этом окне параметры прокси-сервера HTTP верны. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

Данные для аутентификации, такие как **имя пользователя** и **пароль**, предназначены для доступа к прокси-серверу. Заполнять эти поля необходимо только в том случае, если требуются имя пользователя и пароль. Обратите внимание, что эти поля не имеют отношения к имени пользователя и паролю для программы ESET Server Security и должны быть заполнены только в том случае, если подключение к Интернету осуществляется через защищенный паролем прокси-сервер.

Использовать прямое подключение, если прокси-сервер недоступен
Если в программе настроено использование прокси-сервера HTTP, а он недоступен, программа будет обходить прокси-сервер и подключаться к серверам ESET напрямую.
Общие ресурсы Windows
При обновлении с локального сервера под управлением ОС Windows по умолчанию требуется аутентификация всех сетевых подключений.
Подключаться к локальной сети как
Чтобы настроить учетную запись, выберите один из следующих вариантов.
• Чтобы для аутентификации использовать системную учетную запись, выберите вариант **Системная учетная запись (по умолчанию)**. Если данные аутентификации в главном разделе параметров обновлений не указаны, то процесс аутентификации, как правило, не выполняется.
• Чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.
• Если нужно указать учетную запись определенного пользователя для аутентификации, выберите элемент **Указанный пользователь**. Этот метод следует использовать, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание на то, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. Если у пользователя нет доступа, программа не сможет установить соединение или загрузить обновления.

Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. Данные для аутентификации в локальной сети рекомендуется указывать в главном разделе параметров обновлений. В этом разделе укажите данные аутентификации следующим образом: domain_name\user (а для рабочей группы укажите workgroup_name\name) и пароль. При обновлении по протоколу HTTP с локального сервера аутентификация не требуется.

Отключиться от сервера после завершения обновления
Если подключение к серверу остается активным даже после загрузки обновлений, выберите этот вариант для принудительного отключения.

Зеркало обновлений

Параметры конфигурации локального сервера зеркала расположены в разделе **Дополнительные настройки** (F5) на вкладке **Обновление** > **Профили** > Зеркало обновлений.

Откат обновления

Щелкнув параметр **Откат**, в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление базы данных модуля обнаружения и модулей программы.

Чтобы отложить регулярные обновления на неопределенный период времени, пока функция обновлений не будет восстановлена вручную, выберите вариант **До отзыва**. Поскольку этот вариант подвергает систему опасности, его не рекомендуется использовать.

Программа возвращается к самой старой версии базы данных модуля обнаружения, которая хранится в качестве снимка в файловой системе локального компьютера.

Запланированная задача — обновление.

Если нужно иметь возможность обновлять программу с двух серверов обновлений, нужно создать два разных профиля обновления. Если не удастся загрузить файлы обновлений с одного сервера, программа автоматически переключится на другой. Этот вариант подходит, например, для ноутбуков, которые обычно обновляются с сервера обновлений в локальной сети, но часто подключаются к Интернету в других сетях. Таким образом, если с первым профилем возникнет ошибка, файлы обновлений с серверов обновлений ESET автоматически будут загружены через второй профиль.

Приведенные ниже шаги проведут по заданию изменения существующего **постоянного автоматического обновления**.
1. На главном экране **планировщика** выберите задачу **Обновить** с именем **Регулярное автоматическое обновление** и нажмите кнопку **Изменить**. Откроется мастер настройки.
2. Задайте задачу планировщика для запуска, выберите время для запуска, чтобы определить момент времени запуска запланированной задачи.
3. Если нужно, чтобы задача не запускалась тогда, когда устройство работает от аккумулятора (например, от источника бесперебойного питания), щелкните переключатель **Пропускать задачу, если устройство работает от аккумулятора**.
4. Выберите профиль обновления, который будет использоваться. Выберите действие, которое будет выполняться, если по какой-либо причине не удается выполнить запланированную задачу.
5. Для применения задачи нажмите кнопку **Готово**.

Зеркало обновлений

ESET Server Security дает возможность создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Использование зеркала (копии файлов обновлений в локальной сети) позволяет избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Обновления загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет

избежать перегрузки трафика. Обновление клиентских рабочих станций с зеркала оптимизирует балансировку сетевой нагрузки и уменьшает процент используемой пропускной способности подключения к Интернету.

Зеркало обновлений

Создание зеркала обновления
Активирует параметры конфигурации зеркала.
Папка хранения
Если необходимо изменить заданную по умолчанию папку для хранения зеркальных копий файлов , щелкните **Очистить**. Чтобы выбрать папку на локальном компьютере или общую сетевую папку, щелкните **Изменить**. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях «Имя пользователя» и «Пароль». Если выбранная папка назначения расположена на сетевом диске компьютера под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку.
Имя пользователя и пароль следует вводить в формате Domain/User илиWorkgroup/User. Не забудьте ввести соответствующие пароли.

Обновление компонентов программы

Файлы
При настройке зеркала можно указать предпочитаемые языки обновлений. Выбранные языки должны поддерживаться сервером зеркала, который настроил пользователь.
Автоматическое обновление компонентов
Разрешает установку новых компонентов и обновление существующих. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления продукта может потребоваться перезагрузка компьютера.
Обновить компоненты сейчас
Обновляет компоненты программы до последней версии.

HTTP-сервер

Порт сервера
Порт по умолчанию — 2221. Если вы используете другой порт, измените это значение.
Аутентификация
Определяет способ аутентификации, используемый для доступа к файлам обновлений. Доступны следующие варианты: **Нет**, **Основная** и **NTLM**.
• Выберите вариант **Обычная**, чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю.
• Вариант **NTLM** обеспечивает шифрование с использованием безопасного способа шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений.
• Значение по умолчанию — **Нет**. Этот вариант обеспечивает доступ к файлам обновлений без аутентификации.

> Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET Server Security, который ее создает.

SSL для HTTP-сервера
Чтобы использовать HTTP-сервер с поддержкой протокола HTTPS (SSL), прикрепите свой **файл цепочки сертификатов** или создайте самозаверяющий сертификат. Доступны следующие типы сертификатов: PEM, PFX и ASN. Из соображений дополнительной безопасности для загрузки файлов обновления можно использовать протокол HTTPS. При его использовании практически невозможно отследить передаваемые сведения и учетные данные.
Для параметра **Тип закрытого ключа** по умолчанию задается значение **Интегрированный** (поэтому параметр Файл закрытого ключа по умолчанию неактивен). Это означает, что закрытый ключ является частью выбранного файла цепочки сертификатов.

Параметры подключения

Общие ресурсы Windows
При обновлении с локального сервера под управлением ОС Windows по умолчанию требуется аутентификация всех сетевых подключений.
Подключаться к локальной сети как
Чтобы настроить учетную запись, выберите один из следующих вариантов.
• Чтобы использовать для аутентификации системную учетную запись, выберите вариант **Системная учетная запись** (по умолчанию). Если данные аутентификации в главном разделе параметров обновлений не указаны, то процесс аутентификации, как правило, не происходит.
• Чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.
• Если нужно указать учетную запись определенного пользователя для аутентификации, выберите элемент **Указанный пользователь**. Этот метод следует использовать, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. Если у пользователя нет доступа, программа не сможет установить соединение и загрузить обновления.

> Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. Данные для аутентификации в локальной сети рекомендуется указывать в главном разделе параметров обновлений. В этом разделе укажите данные аутентификации следующим образом: *domain_name\user* (а для рабочей группы укажите *workgroup_name\name*) и пароль. При обновлении по протоколу HTTP с локального сервера аутентификация не требуется.

Отключиться от сервера после завершения обновления
Если подключение к серверу остается активным даже после загрузки обновлений, выберите этот вариант для принудительного отключения.

Защита сети

Управляйте защитой сети, щелкните Изменить, чтобы добавить новую или изменить существующую:

- Известные сети: можно настроить вручную в разделе «Расширенные параметры» > «Защита сети» > «Основное» > «Известные сети» > «Изменить».

- Зоны: можно настроить вручную в разделе «Расширенные параметры» > «Защита сети» > «Основное» > «Зоны» > «Изменить».

Известные сети

При использовании компьютера, который часто подключается к общедоступным сетям или сетям за пределами обычной рабочей сети, рекомендуем проверять надежность новых сетей, к которым вы подключаетесь. После настройки сетей решение ESET Server Security может распознавать доверенные (домашние или офисные) сети, используя различные параметры сети, настроенные в разделе Сетевая идентификация.

Компьютеры часто подключаются к сетям с IP-адресами, которые похожи на адреса доверенных сетей. В таких случаях решение ESET Server Security может посчитать неизвестную сеть доверенной (домашней или офисной). Во избежание таких ситуаций рекомендуем

использовать аутентификацию сети.

При подключении сетевого адаптера к сети или изменении его сетевых настроек решение ESET Server Security ищет в списке известных сетей запись, которая соответствует новой сети. Если параметры «Сетевая идентификация» и «Аутентификация сети» (необязательно) совпадают, сеть будет отмечена как подключенная в этом интерфейсе.

Если известные сети не найдены, конфигурация сетевой идентификации создаст новое сетевое подключение, чтобы идентифицировать эту сеть при следующем подключении к ней. По умолчанию для нового сетевого подключения используется тип защиты «Общедоступная сеть».

В диалоговом окне «Обнаружено новое сетевое подключение» вам будет предложено выбрать тип защиты: «Общедоступная сеть», «Домашняя или офисная сеть» либо «Использовать параметр Windows». Если сетевой адаптер подключен к известной сети и эта сеть отмечена как домашняя или офисная, локальные подсети этого адаптера будут добавлены в доверенную зону.

Тип защиты для новых сетей

Выберите, какой из следующих вариантов следует использовать по умолчанию для новых сетей: **Использовать параметр Windows**, **Спросить пользователя** или **Отметить как общедоступную**. Если выбран вариант **Использовать параметр Windows**, диалоговое окно не откроется, а сеть, к которой вы подключены, будет автоматически отмечена в соответствии с настройками ОС Windows. В связи с этим некоторые функции (например, общий доступ к файлам и удаленный рабочий стол) станут доступными из новых сетей.

Известные сети можно настроить вручную в окне Редактор известных сетей.

Добавление сети

Параметры конфигурации сети разделены на следующие вкладки:

Сеть

Можно указать **имя сети** и выбрать **тип защиты** для сети. Кроме того, адреса, добавленные в разделе **Дополнительные доверенные адреса**, всегда добавляются в доверенную зону адаптеров, подключенных к этой сети (вне зависимости от типа защиты сети).

- Предупреждать о слабом шифровании Wi-Fi: ESET Server Security будет сообщать о подключении к незащищенной беспроводной сети или сети со слабой защитой.
- Профиль файервола будет получен от сетевого адаптера.
- Профиль обновления: выберите профиль обновления, который будет использоваться при подключении к этой сети.

Сетевая идентификация

Выполняется согласно параметрам локального сетевого адаптера. Все выбранные параметры сравниваются с фактическими параметрами активных сетевых подключений. IPv4- и IPv6-адреса разрешены.

Аутентификация сети

Выполняет поиск определенного сервера в сети и использует асимметричное шифрование (RSA) для аутентификации этого сервера. Имя сети, которая проходит аутентификацию, должно совпадать с именем зоны, указанным в настройках сервера аутентификации. В имени учитывается регистр. Укажите имя сервера, прослушивающий порт сервера и открытый ключ, соответствующий закрытому ключу сервера. Имя сервера можно ввести в виде IP-адреса, DNS- или NetBios-имени, и после него может следовать путь, который указывает на расположение ключа на сервере (например, *server_name_/directory1/directory2/authentication*). Можно указать альтернативные серверы, которые следует использовать. Для этого их нужно добавить в путь, разделяя точкой с запятой.

Открытый ключ можно импортировать, используя один из следующих типов файлов:

- Зашифрованный открытый ключ PEM (.pem). Этот ключ можно создать с помощью сервера ESET Authentication Server.
- Зашифрованный открытый ключ
- Файл сертификата открытого ключа (.crt)

Щелкните **Проверить**, чтобы проверить настройки. Если аутентификация будет успешной, отобразится сообщение «Аутентификация сервера завершена». Если аутентификация настроена неправильно, отобразятся следующие сообщения об ошибках:

Сбой аутентификации сервера. Недопустимая или несовпадающая подпись.	**Подпись сервера не соответствует введенному открытому ключу.**
Аутентификация сервера не выполнена. Не совпадает имя сети.	Отключите этот параметр, если следует оставить правило в списке, но при этом не использовать его.
Сбой аутентификации сервера. Нет ответа от сервера, или получен недопустимый ответ.	Ответ не будет получен, если сервер не работает или недоступен. Может быть получен недопустимый ответ, если по указанному адресу работает другой HTTP-сервер.
Указан недействительный открытый ключ.	Убедитесь, что введенный файл открытого ключа не поврежден.

Зоны

Зона представляет собой набор сетевых адресов, которые составляют одну логическую группу IP-адресов. Зона может быть полезна, когда нужно повторно использовать один и тот же набор адресов в нескольких правилах. Каждому адресу в определенной группе назначаются одинаковые правила, определяемые централизовано для всей группы. Одним из примеров такой группы является доверенная зона. Доверенная зона — это группа сетевых адресов, которые никак не блокируются файерволом.

Щелкните **Добавить**, введите **имя** и **описание** для новой зоны и добавьте удаленный IP-адрес в поле «Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска)».

Защита от сетевых атак

Включить защиту от сетевых атак (IDS)

Позволяет настроить доступ к некоторым службам, запущенным на компьютере из доверенной зоны и включить или отключить обнаружение нескольких типов атак и эксплойтов, которые могут быть предприняты, чтобы навредить компьютеру.

Включить защиту от ботнетов

Обнаруживает и блокирует связь с вредоносными командами и сканированием серверов на основе типичных шаблонов, когда компьютер заражен, а бот пытается установить соединение

Исключения IDS

Исключения системы обнаружения вторжений (IDS) можно воспринимать как правила защиты сети. Щелкните Изменить, чтобы настроить исключения IDS.

> Если в вашей среде используется высокоскоростная сеть (10GbE и мощнее), прочитайте статью базы знаний для получения сведений о быстродействии сети и ESET Server Security.

Защита от атак методом подбора

ESET Server Security проверяет содержимое сетевого трафика и блокирует попытки атак, предусматривающих угадывание пароля.

Расширенные параметры

Настройте расширенные параметры фильтрации для обнаружения различных типов атак и уязвимостей, которые могут использоваться против вашего компьютера.

Обнаружение вторжений:

Протокол SMB — обнаруживает и блокирует различные проблемы безопасности в протоколе SMB
Протокол RPC — обнаруживает и блокирует различные CVE в системе обработки удаленных процедур, разработанной для распределенной вычислительной среды (DCE).
Протокол RDP — обнаруживает и блокирует различные CVE в протоколе RDP (см. выше).
Блокировать небезопасный адрес после обнаружения атаки — просмотр списка IP-адресов, которые обнаружены как источники атак и добавлены в черный список, чтобы блокировать соединение в течение определенного периода времени.
Показывать уведомление при обнаружении атаки — включает использование области уведомлений Windows в правом нижнем углу экрана.
Показывать уведомление при обнаружении атаки, использующей бреши в системе безопасности — оповещает, если обнаружены атаки на бреши в системе безопасности, или если попытка войти в систему таким образом создает угрозу.

Проверка пакетов:

Разрешить входящее подключение к общим ресурсам администратора по протоколу SMB — общие ресурсы администратора (админ-ресурсы) являются по умолчанию сетевыми папками, которые совместно используют разделы жесткого диска (C$, D$, ...) в системе вместе с системной папкой (ADMIN$). Отключение подключения к админ-ресурсам должно уменьшить многие риски безопасности. Например, червь Conficker выполняет словарные атаки, чтобы подключиться к общим админ-ресурсам.
Запретить старые (неподдерживаемые) диалекты SMB — отказ от сеансов SMB, которые используют старый SMB-диалект, не поддерживаемые IDS. Современные операционные системы Windows поддерживают старые диалекты SMB из-за обратной совместимости со старыми операционными системами, такими как Windows 95. Чтобы избежать инспекции трафика, злоумышленник может использовать старый диалект в сеансе SMB. Откажитесь от старых диалектов SMB, если вашему компьютеру не нужно обмениваться файлами (или использовать SMB-связь вообще) с компьютером со старой версией Windows.
Запретить сеансы SMB без расширенной безопасности — расширенная безопасность может использоваться во время согласования сеанса SMB, чтобы обеспечить более безопасный механизм аутентификации, чем аутентификация LAN Manager Challenge или Response (LM). Схема LM считается слабой и ее не рекомендуется использовать.
Разрешить подключение к службе диспетчера учетных записей безопасности — дополнительные сведения об этой службе см. в разделе [MS-SAMR].
Разрешить подключение к службе локальной системы безопасности — дополнительные сведения об этой службе см. в разделах [MS-LSAD] и [MS-LSAT].
Разрешить подключение к службе удаленного управления реестром — дополнительные сведения об этой службе см. в разделе [MS-RRP].
Разрешить подключение к службе диспетчера служб — дополнительные сведения об этой службе см. в разделе [MS-SCMR].
Разрешить подключение к службе сервера — дополнительные сведения об этой службе см. в разделе [MS-SRVS].
Разрешить подключение к другим службам — другие службы MSRPC.

Исключения IDS

Исключения системы обнаружения вторжений (IDS), по сути, являются правилами защиты сети. Эти исключения обрабатываются сверху вниз. Редактор исключений IDS позволяет настроить поведение защиты сети при различных исключениях IDS. Первое соответствующее исключение применяется для каждого типа действия (блокировка, уведомление, запись в журнал) отдельно. С помощью функций **На самый верх**/**Поднять**/**Опустить**/**В самый низ** можно указать уровень приоритета исключений. Чтобы создать новое исключение IDS, щелкните элемент **Добавить**. Щелкните элемент **Изменить**, чтобы редактировать существующее исключение IDS. Щелкните **Удалить**, чтобы удалить исключение.

Выберите тип **оповещения** в раскрывающемся списке. Укажите **Имя угрозы** и **Направление**. Найдите **приложение**, для которого нужно создать исключение. Укажите список IP-адресов (IPv4 или IPv6) либо подсетей. Чтобы ввести несколько записей, разделяйте их запятыми.

Настройте **действие** для исключения IDS, выбрав один из параметров в раскрывающемся меню (**По умолчанию**, **Да**, **Нет**). Выполните это для каждого типа действий (**блокировка**, **уведомление**, **запись в журнал**).

Если вы хотите, чтобы при оповещении об исключении IDS отображалось уведомление, а также чтобы время события заносилось в журнал, оставьте для типа действия **Блокировка** значение **По умолчанию**, а для оставшихся двух типов действий (**Уведомление** и **Запись в журнал**) в раскрывающемся меню выберите **Да**.

Возможна угроза заблокирована

Такая ситуация может произойти, когда приложение на компьютере пытается передать вредоносный трафик на другой компьютер в сети, используя уязвимость в системе безопасности, или если кто-то пытается просканировать порты в вашей сети.

- Угроза — Имя угрозы.
- Источник — сетевой адрес источника.
- Объект — сетевой адрес целевого объекта.
- Прекратить блокировку — создание правила IDS для возможной угрозы с настройками, которые разрешают обмен данными.
- Продолжать блокировать — блокировка обнаруженной угрозы. Чтобы создать правило IDS с настройками, которые блокируют обмен данными для этой угрозы, выберите Не уведомлять меня снова.

Информация, которая отображается в этом окне уведомления, зависит от типа обнаруженной угрозы. Дополнительные сведения об угрозах и других связанных терминах можно найти в разделах Типы удаленных атак и Типы обнаружений.

Черный список временных IP-адресов

Просмотр списка IP-адресов, которые были обнаружены как источники атак и добавлены в черный список, чтобы блокировать соединение в течение определенного периода времени (до одного часа). Отображает заблокированный **IP-адрес**.

Причина блокировки

Отображает тип предотвращенной из адреса атаки (например, атака сканирования портов TCP).

Время ожидания

Отображает дату и время, когда адрес будет удален из черного списка.

Удалить/Удалить все

Удаляет выбранный IP-адрес из временного черного списка до истечения срока или немедленно удаляет все адреса из черного списка.

Добавить исключение

Добавляет исключение файервола в фильтрацию IDS для выбранного IP-адреса.

Защита от атак методом подбора

Защита от атак методом подбора блокирует атаки, которые предусматривают угадывание пароля, для служб RDP и SMB. Атака методом подбора — это способ определения пароля путем систематического перебора всех возможных комбинаций букв, цифр и символов.

• **Включить защиту от атак методом подбора** — ESET Server Security проверяет содержимое сетевого трафика и блокирует попытки атак, предусматривающих угадывание пароля.

• Правила — создание, изменение и просмотр правил для входящих и исходящих сетевых подключений.

• Исключения — Список исключенных обнаружений, определенных с помощью IP-адреса или пути приложения. Исключения можно создавать и изменять в Веб-консоль ESET PROTECT .

Правила Защиты от атак методом подбора

Раздел «Правила защиты от атак методом подбора» позволяет создавать, изменять и просматривать правила для входящих и исходящих сетевых подключений. Предварительно заданные правила нельзя изменить или удалить.

Щелкните **Добавить**, чтобы создать правило защиты от атак методом подбора, или щелкните **Изменить**, чтобы изменить выбранные записи.

В этом окне приведены общие сведения о существующих правилах защиты от атак методом подбора.

Имя	Указанное пользователем или автоматически выбранное имя правила.
Включено	Отключите этот параметр, если следует оставить правило в списке, но при этом не использовать его.
Действие	Правило задает действие (Разрешить или Запретить), которое должно быть выполнено при соблюдении условий.
Протокол	Протокол связи, который будет проверяться этим правилом.
Профиль	Для определенных профилей можно устанавливать и применять пользовательские правила.
Макс. кол-во попыток	Максимальное количество разрешенных попыток повторения атаки, по достижении которого IP-адрес будет заблокирован и добавлен в черный список.
Период хранения черного списка (мин)	Установка времени, по истечении которого адрес будет исключен черного списка. Период времени, который используется для подсчета количества попыток, по умолчанию составляет 30 минут.
IP-адрес источника	Список IP-адресов, диапазонов или подсетей. Несколько адресов следует разделять запятой.
Зоны источника	Здесь можно добавить предварительно заданную или созданную зону с диапазоном IP-адресов, нажав кнопку "Добавить".

Исключения в защите от атак методом подбора

Исключения в защите от атак методом подбора могут использоваться, чтобы избежать обнаружения при определенных условиях. Эти исключения создаются в ESET PROTECT на основе обнаружений системы защиты от атак методом подбора. Исключения будут отображаться, если администратор создал их в веб-консоли ESET PROTECT. Такие исключения могут содержать только разрешающие правила и оцениваются перед правилами IDS.

- **Обнаружение** – Тип обнаружения
- **Приложение** — выберите путь к файлу исключаемого приложения, щелкнув «...» (например, *C:\Program Files\Firefox\Firefox.exe*). Не следует вводить имя приложения.
- **Удаленный IP-адрес** — список удаленных IPv4- или IPv6-адресов, диапазонов или подсетей. Несколько адресов следует разделять запятой.

Интернет и электронная почта

Чтобы защитить сервер во время связи через Интернет, можно настраивать фильтрацию протоколов, защиту почтового клиента, защиту доступа в Интернет и защиту от фишинга.

Защита почтового клиента

Контролирует весь обмен данными по электронной почте, защищает от вредоносного кода и позволяет выбрать действие, которое следует выполнять при обнаружении заражения.

Защита доступа в Интернет

Отслеживает обмен данными между веб-браузерами и удаленными серверами и соответствует правилам для протоколов HTTP и HTTPS. Эта функция также позволяет блокировать, разрешать и исключать определенные URL-адреса.

Фильтрация протоколов

Предлагает расширенную защиту протоколов приложений, которую предоставляет модуль сканирования ThreatSense. Эта функция работает автоматически вне зависимости от того, используется или нет веб-браузер или почтовый клиент. Кроме того, она работает для зашифрованных соединений (SSL/TLS).

Защита от фишинга

Позволяет блокировать веб-страницы, через которые распространяется фишинговое содержание.

Фильтрация протоколов

Защиту протоколов приложений от вредоносных программ обеспечивает модуль сканирования ThreatSense, в котором объединено множество современных методов сканирования для выявления вредоносных программ. Функция фильтрации протоколов работает автоматически, вне зависимости от используемого веб-браузера и почтового клиента. Если фильтрация протоколов включена, модуль ESET Server Security будет проверять соединения, использующие протокол SSL или TLS. Выберите **Интернет и электронная почта** > SSL/TLS.

Включить фильтрацию содержимого, передаваемого по протоколам приложений

В случае отключения фильтрации протоколов, обратите внимание, что от нее зависят многие компоненты ESET Server Security (защита доступа в Интернет, защита протоколов электронной почты и защита от фишинга) и не все их функции будут доступны.

Исключенные приложения

Чтобы исключить подключение определенных приложений, ориентированных на сеть, из фильтрации содержимого, выберите их в списке. Подключение выбранных приложений по протоколу HTTP/POP3 не будет проверяться на наличие угроз, позволяя исключать определенные приложения из фильтрации протоколов. Щелкните**Изменить** и **Добавить** для выбора исполняемого файла из списка приложений, чтобы исключить его из фильтрации протоколов.

> Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Исключенные IP-адреса

Позволяет исключить конкретные удаленные адреса из фильтрации протоколов. IP-адреса в этом списке будут исключены из фильтрации содержимого протокола. Подключение HTTP/POP3/IMAP из (к) выбранных адресов не будет проверяться на наличие угроз.

> Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Щелкните **Изменить** и **Добавить**, чтобы указать IP-адрес, диапазон адресов или подсеть, к которым будет применяться исключение. Когда выбрано **Ввести несколько значений**, можно добавить несколько IP-адресов, разделенных символами новой строки, запятыми или точками с запятой. Если включен множественный выбор, адреса будут отображаться в списке исключенных IP-адресов.

> Исключения полезны, если фильтрация протоколов вызывает проблемы совместимости.

Веб-клиенты и почтовые клиенты

В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему.

Именно поэтому в программном обеспечении ESET Server Security основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Приложения, которые уже использовали протоколы для передачи данных, и приложения, находящиеся по выбранному адресу, можно внести в список веб-клиентов и почтовых клиентов.

SSL/TLS

Программа ESET Server Security может проверять на наличие угроз соединения, в которых используются протоколы SSL/TLS.

Для защищенных SSL-соединений можно использовать различные режимы сканирования с использованием доверенных сертификатов, неизвестных сертификатов или сертификатов, исключенных из проверки защищенных SSL-соединений.

Включить фильтрацию протокола SSL/TLS

Если фильтрация протоколов отключена, программа не будет проверять связь по протоколам SSL/TLS. Режим фильтрации протоколов Secure Sockets Layer (SSL)/Transport Layer Security (TLS) доступен в следующих вариантах.

- **Автоматический режим**: выберите этот вариант, чтобы сканировать все защищенные SSL/TLS-соединения, за исключением тех, которые защищены сертификатами, исключенными из проверки. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

- **Интерактивный режим**: при выполнении входа на новый защищенный протоколами SSL/TLS сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора действий. Этот режим позволяет создавать список сертификатов SSL/TLS, которые будут исключены из сканирования.

- В **режиме политики** фильтруются все соединения SSL/TLS, кроме настроенных исключений.

Список приложений, отфильтрованных с помощью SSL/TLS

Добавьте отфильтрованное приложение и установите одно из действий сканирования. Список приложений, отфильтрованных с помощью SSL/TLS можно использовать для настройки поведения ESET Server Security для определенных приложений и для запоминания действий, выбранных, если в **режиме фильтрации протоколов TCP/TLS** выбран **Интерактивный режим**.

Список известных сертификатов

Позволяет настроить поведение ESET Server Security для определенных сертификатов SSL. Список можно просмотреть и управлять им, щелкнув Изменить рядом с элементом **Список известных сертификатов**.

Исключить соединение с доверенными доменами

Чтобы исключить подключение, используйте расширенные сертификаты проверки из проверки протокола (интернет-банкинг).

Блокировать шифрованные подключения, использующие устаревший протокол SSL версии 2

Подключение с использованием этой более ранней версии протокола SSL будет автоматически заблокировано.

Корневой сертификат

Для нормальной работы SSL/TLS-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). Параметр добавления корневого сертификата к известным браузерам должен быть активирован.

Выберите этот параметр, чтобы автоматически добавить корневой сертификат ESET в известные браузеры (например, Opera и Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически.

Для установки сертификата в неподдерживаемые браузеры выберите элементы **Просмотреть сертификат** > **Подробности** > **Копировать в файл**, а затем вручную импортируйте его в браузер.

Срок действия сертификата

Если проверить сертификат с помощью хранилища сертификатов TRCA не удается

В некоторых случаях сертификат невозможно проверить с помощью **хранилища доверенных корневых центров сертификации**. Это значит, что сертификат уже подписан (например, администратором веб-сервера или небольшой компании) и принятие решения о выборе такого сертификата как доверенного не всегда представляет опасность. Большинство крупных компаний (например, банки) используют сертификаты, подписанные хранилищем доверенных корневых центров сертификации.

Если установлен флажок **Запрашивать срок действия сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. Можно выбрать вариант **Блокировать подключения, использующие данный сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтами, использующими непроверенные сертификаты.

Если сертификат недействителен или поврежден

Это значит, что истек срок действия сертификата или же используется недопустимая подпись. В этом случае рекомендуется выбрать элемент **Блокировать подключения, использующие данный сертификат**.

Список известных сертификатов

Чтобы настроить поведение ESET Server Security для определенных сертификатов SSL/TLS и запомнить действия, выбранные, если в режиме фильтрации протокола SSL/TLS выбран **Интерактивный режим**. Выбранный сертификат можно настроить или можно **Добавить** сертификат из URL-адреса или файла.

После открытия окна **Добавление сертификата** нажмите кнопку **URL-адрес** или **Файл** и укажите URL-адрес сертификата либо найдите файл сертификата. На основе данных этого сертификата автоматически заполняются следующие поля:

- **Имя сертификата** — собственно имя сертификата.
- **Издатель сертификата** — имя создателя сертификата.
- **Субъект сертификата** — в этом поле можно указать сущность, которой принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

Действие доступа

- **Автоматически** — разрешить доверенные сертификаты и запрашивать ненадежные.
- **Разрешить или заблокировать** — чтобы разрешить или заблокировать подключение, защищенное этим сертификатом, независимо от его надежности.
- **Спросить** — получать приглашение, когда обнаруживается конкретный сертификат.

Действие сканирования

- **Автоматически** — сканировать в автоматическом режиме и запрашивать в интерактивном режиме.
- **Сканировать или игнорировать** — сканировать или игнорировать подключение, защищенное этим сертификатом.
- **Спросить** — получать приглашение, когда обнаруживается конкретный сертификат.

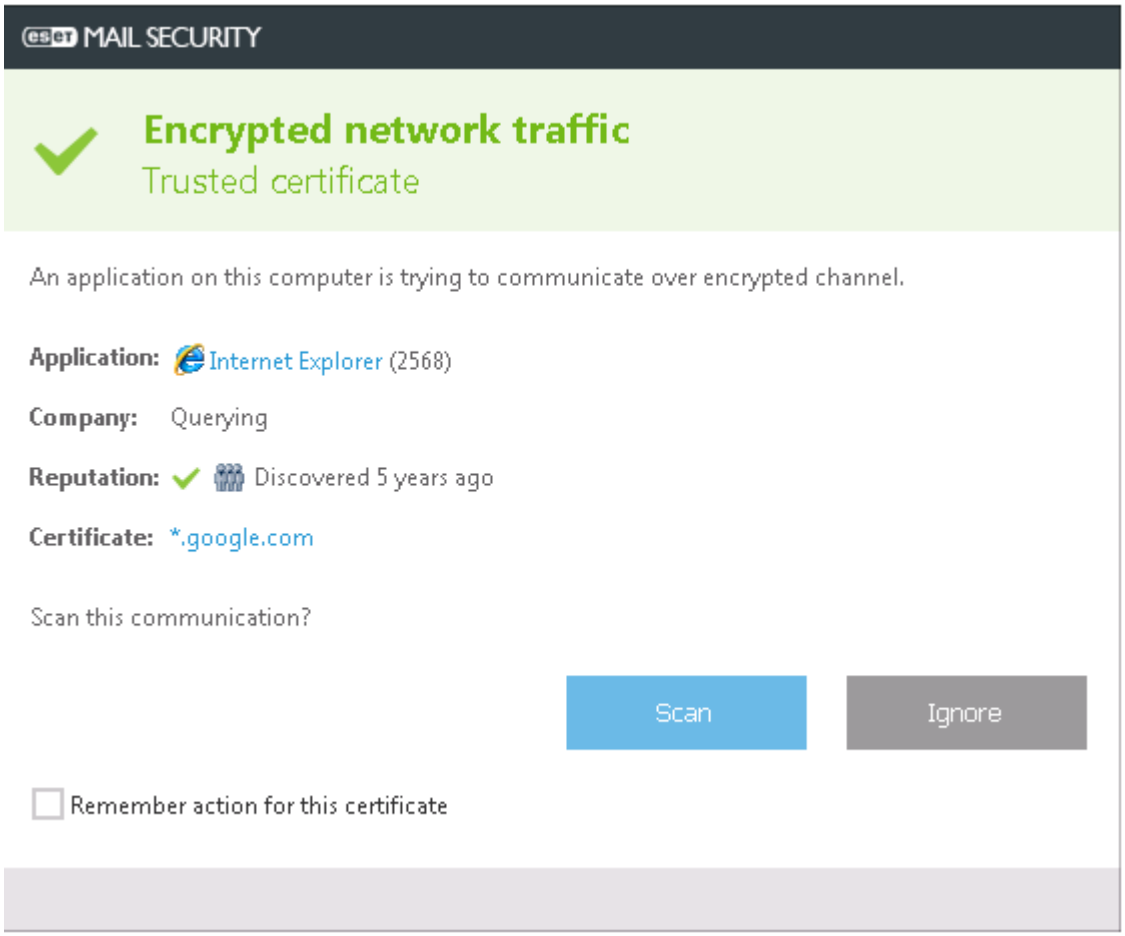
Шифрованное соединение SSL

Если в системе настроено сканирование протокола SSL, диалоговое окно с запросом на выбор действия будет отображаться в двух случаях.

Во-первых, если веб-сайт использует непроверенный или недействительный сертификат, а продукт ESET Server Security настроен на выдачу запросов в таких случаях (по умолчанию запросы отображаются для непроверенных сертификатов, а для недействительных — нет), появится запрос на **блокирование** или **разрешение** подключения.

Во-вторых, если в качестве **режима фильтрации протокола SSL** выбран **интерактивный режим**, то при подключении к любому веб-сайту будет отображаться запрос на **сканирование** или **игнорирование**. Некоторые приложения проверяют SSL-трафик на предмет изменений и мониторинга. В таких случаях для сохранения работоспособности приложения программа ESET

Server Security должна SSL-трафик **игнорировать**.



В каждом их этих случаев пользователь может сохранить в системе выбранное действие. Сохраненные действия хранятся в списке Список известных сертификатов.

Защита почтового клиента

Интеграция ESET Server Security с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET Server Security можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET Server Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты (панель инструментов для последних версий Windows Live Mail не вставляется).

Интеграция с почтовым клиентом

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows и почта Windows Live. Защита электронной почты реализована в этих программах в виде подключаемого модуля. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования. Даже если интеграция отключена, почтовые клиенты остаются защищены соответствующим модулем (для протоколов POP3, IMAP).

Полный список поддерживаемых почтовых клиентов и их версий можно найти в следующей статье базы знаний.

Не выполнять проверку при изменении содержимого папки "Входящие"

Если при работе с почтовым клиентом наблюдается замедление работы системы (только для Microsoft Outlook). Это возможно при извлечении сообщения электронной почты из хранилища Kerio Outlook Connector Store.

Включить защиту электронной почты с помощью подключаемых модулей клиента

Позволяет отключить защиту почтового клиента, не удаляя интеграцию с почтовым клиентом. Вы можете отключить все плагины сразу или выборочно отключить следующие.

- **Полученные сообщения** — включает или отключает проверку входящих сообщений.
- **Отправленные сообщения** — включает или отключает проверку отправленных сообщений.
- **Прочитанные сообщения** — включает или отключает проверку прочитанных сообщений.

Действие, применяемое к зараженному сообщению

- **Ничего не предпринимать** — в этом случае программа будет выявлять зараженные вложения, но не будет выполнять никаких действий с сообщениями электронной почты.
- **Удалить сообщение** — программа будет уведомлять пользователя о заражениях и удалять сообщения.
- **Переместить сообщение в папку "Удаленные"** — зараженные сообщения будут автоматически перемещаться в папку «Удаленные».
- **Переместить сообщение в папку** — зараженные сообщения будут автоматически перемещаться в указанную папку.
- **Папка** — выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

Повторить сканирование после обновления

Включение или отключение повторного сканирования после обновления модуля обнаружения.

Принять результаты сканирования из других модулей

Если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты (сканирование каталогов POP3, IMAP).

Протоколы электронной почты

Включить защиту электронной почты с помощью фильтрации протоколов

IMAP и POP3 — самые распространенные протоколы, используемые для получения электронной почты в почтовых клиентах. ESET Server Security обеспечивает защиту этих протоколов вне зависимости от используемого почтового клиента.

ESET Server Security также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET Server Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа будет выполнять сканирование трафика только на портах, которые указаны как использующие **протокол IMAPS/POP3S**, вне зависимости от версии операционной системы.

Настройка модуля сканирования POP3S EPFW

Зашифрованные соединения не будут сканироваться, если используются параметры по умолчанию. Чтобы включить сканирование зашифрованных соединений, перейдите к элементу Проверка протоколов SSL/TLS.

По номеру порта определяется тип порта. Ниже приведены порты, используемые по умолчанию.

Имя порта	Номер порта	Описание
POP3	110	Используемый по умолчанию незашифрованный порт POP3.
IMAP	143	Используемый по умолчанию незашифрованный порт IMAP.
Защищенный протокол IMAP (IMAP4-SSL)	585	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.
IMAP4 по SSL (IMAPS)	993	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.
Защищенный протокол POP3 (SSL-POP)	995	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.

Предупреждения и уведомления

Защита электронной почты обеспечивает контроль безопасности соединений по протоколам POP3 и IMAP. При использовании подключаемого модуля для Microsoft Outlook и других почтовых клиентов ESET Server Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

ЗПри проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в базу данных обнаруженных вирусов. Сканирование соединений по протоколам POP3 и IMAP не зависит от используемого почтового клиента.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Можно выбрать такие варианты: **Добавлять уведомление к полученным и прочитанным сообщениям электронной почты**, **Добавлять примечание в поле темы полученных и прочитанных зараженных сообщений** или **Добавлять уведомление к отправленным сообщениям**.

Обратите внимание, что в некоторых случаях уведомления могут быть опущены в проблемных HTML-сообщениях или сфабрикованы некоторыми вирусами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем,

и к другим). Доступны следующие варианты.

Доступны такие варианты:

- **Никогда** : уведомления не будут добавляться вообще.
- **Только к зараженным сообщениям** : будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).
- **Ко всем сканируемым сообщениям**: программа будет добавлять уведомления ко всем сканируемым сообщениям электронной почты.

Добавлять примечание в поле темы отправленных зараженных сообщений

Установите этот флажок, если необходимо, чтобы защита электронной почты добавляла предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Кроме того, она повышает уровень доверия получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.

Шаблон, добавляемый в поле темы зараженных сообщений

Этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого ко всем зараженным сообщениям. Эта функция заменит тему сообщения `"Hello"` при заданном значении префикса "[virus]" на такой формат: `"[virus] Hello"`. Переменная `%VIRUSNAME%` обозначает обнаруженную угрозу.

Панель инструментов Microsoft Outlook

Защита Microsoft Outlook работает в виде подключаемого модуля. После установки ESET Server Security панель инструментов, содержащая приведенные ниже опции защиты от вредоносных программ, добавляется в Microsoft Outlook:

ESET Server Security

Щелкните значок, чтобы открыть главное окно программы ESET Server Security.

Повторное сканирование сообщения

Позволяет запустить проверку электронной почты вручную. Кроме того, можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования

На экран выводятся параметры защиты почтового клиента.

Панель инструментов Outlook Express и Почты Windows

Защита для Outlook Express и Почты Windows работает в виде подключаемого модуля. После установки ESET Server Security панель инструментов, содержащая приведенные ниже опции защиты от вредоносных программ, добавляется в Outlook Express или Почту Windows:

ESET Server Security

Щелкните значок, чтобы открыть главное окно программы ESET Server Security.

Повторное сканирование сообщения

Позволяет запустить проверку электронной почты вручную. Кроме того, можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования

На экран выводятся параметры защиты почтового клиента.

Настроить вид

Этот параметр позволяет изменить внешний вид панели инструментов в почтовом клиенте. Чтобы настроить внешний вид независимо от параметров почтового клиента, снимите этот флажок.

- **Показывать надписи** : отображение описаний значков.
- **Текст справа**: описания размещаются не снизу, а справа от значков.
- **Большие значки**: отображение в меню значков крупного размера.

Окно подтверждения

Это уведомление предназначено для подтверждения того, что пользователю действительно нужно выполнить выбранное действие, и для предотвращения тем самым возможных ошибок. В окне также есть возможность отключить подтверждения.

Повторное сканирование сообщения

Панель инструментов ESET Server Security, интегрированная в почтовые клиенты, дает пользователю возможность указать ряд параметров для проверки электронной почты. С помощью параметра **Повторно сканировать сообщения** можно включить два описанные далее режима сканирования.

- **Все сообщения в текущей папке** : сканируются сообщения в отображаемой в данный момент папке.

• **Только выбранные сообщения**: сканируются только помеченные пользователем сообщения.

• **Повторно сканировать уже сканированные сообщения** — дает пользователю возможность выполнить еще одно сканирование сообщений, которые уже были просканированы ранее.

Защита доступа в Интернет

Функция защиты доступа в Интернет отслеживает соединения между веб-браузерами и удаленными серверами, чтобы обеспечить защиту от интернет-угроз. Данная функция работает в соответствии с правилами протоколов HTTP (протокол передачи гипертекста) и HTTPS (зашифрованный обмен данными).

Доступ к веб-страницам, которые содержат заведомо вредоносное содержимое, блокируется перед его загрузкой. Если обнаруживается вредоносное содержимое, все другие веб-страницы сканируются модулем сканирования ThreatSense. Защита доступа в Интернет предполагает два уровня: блокировка по «черному» списку и блокировка по содержимому.

Основная информация

Настоятельно рекомендуется не отключать **защиту доступа в Интернет**. Чтобы получить доступ к этой функции, в главном окне программы ESET Server Security выберите **Настройка** > **Интернет и электронная почта** > **Защита доступа в Интернет**.
Включить расширенное сканирование сценариев браузера
По умолчанию все программы JavaScript, выполняемые веб-браузерами, будут проверяться модулем обнаружения.

Веб-протоколы

Дает возможность настроить отслеживание для стандартных протоколов, которые используются в большинстве веб-браузеров. По умолчанию ESET Server Security настроен на отслеживание протокола HTTP, используемого большинством интернет-браузеров.
ESET Server Security также поддерживает проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Server Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа осуществляет сканирование только **портов, помеченных как используемые протоколом** HTTPS, вне зависимости от версии операционной системы.
По умолчанию сканирование зашифрованных соединений отключено. Чтобы включить сканирование зашифрованных соединений, перейдите к элементу **Дополнительные настройки** (**F5**)**, выберите элементы Интернет и электронная почта** > SSL/TLS.

Параметры ThreatSense

Настраивает определенные параметры, например тип сканирования (сообщения электронной почты, архивы, исключения, ограничения и т. д.) и метод обнаружения для защиты доступа в Интернет.

Управление URL-адресами

Управление URL-адресами позволяет указывать HTTP-адреса для блокировки, разрешения или исключения из проверки. Сайты в списке заблокированных адресов не будут доступны, если

они не включены в список разрешенных адресов. Веб-сайты в списке адресов, исключенных из проверки, не сканируются на наличие вредоносного кода при доступе. Для фильтрации HTTPS-адресов в дополнение к веб-страницам HTTP необходимо включить фильтрацию протоколов SSSL/TLS. В противном случае будут добавлены только домены сайтов HTTPS, которые вы посетили, полный URL-адрес будет отсутствовать.

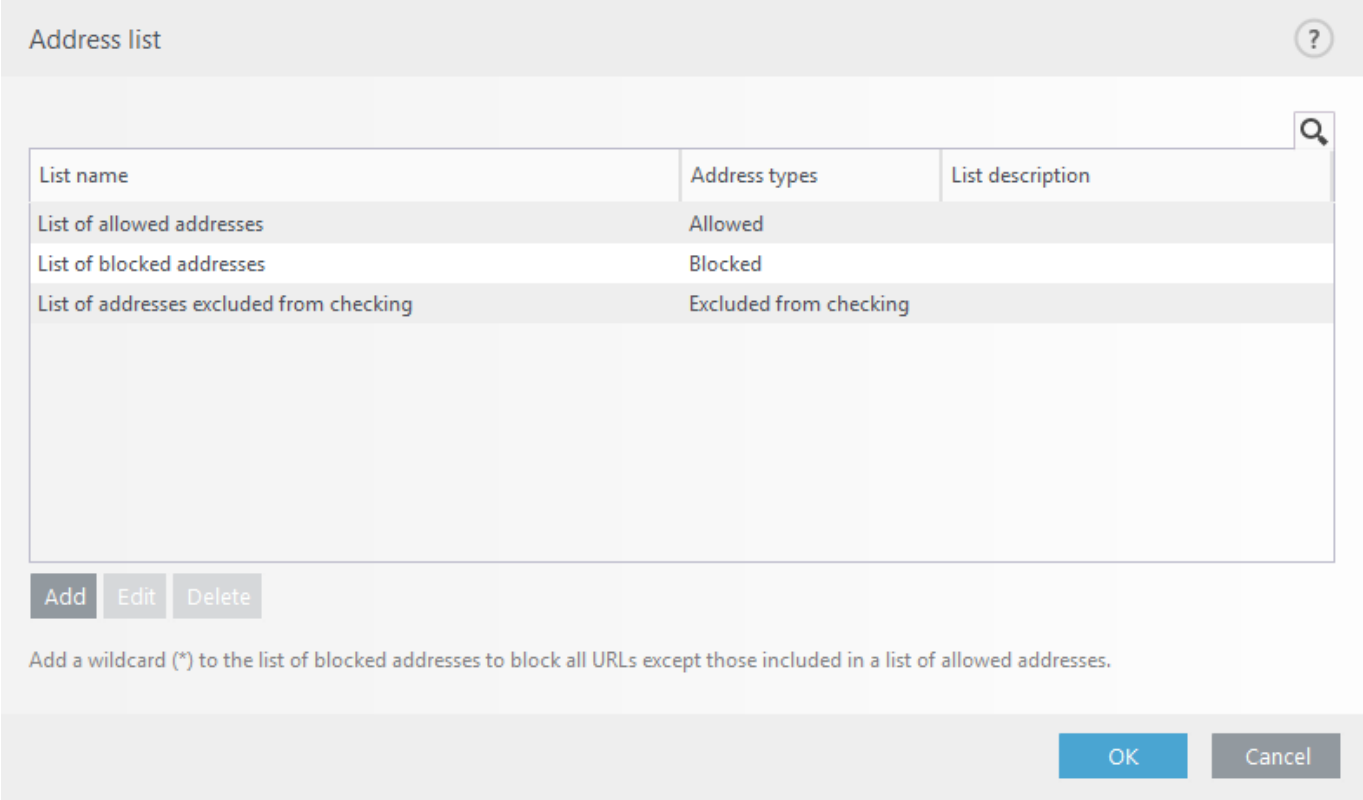
Один список заблокированных адресов может содержать адреса, полученные из внешнего общедоступного черного списка, а второй — адреса, добавленные вами. Таким образом внешний список можно легко обновить, не внося изменений в ваш личный список.

Щелкните **Изменить** и **Добавить**, чтобы создать новый список адресов в дополнение к предопределенным. Это может быть полезно, если вы хотите логически разделить разные группы адресов. По умолчанию доступны следующие три списка.

- **Список адресов, для которых отключена проверка**. Для всех добавленных в этот список адресов не будет выполняться проверка на наличие вредоносного кода.

- **Список разрешенных адресов** — если установлен флажок «Предоставить доступ только к разрешенным HTTP-адресам», а в списке заблокированных адресов указан символ звездочки («*» — блокировать все адреса без исключений), пользователю будет предоставлен доступ только к разрешенным адресам. Адреса в этом списке остаются доступными, даже если они включены в список заблокированных адресов.

- **Список заблокированных адресов** — пользователь не сможет получить доступ к адресам из этого списка, если они не включены также в список разрешенных адресов.



Вы можете **добавить** новый URL-адрес в список. Также можно ввести несколько значений с разделителем. Щелкните **Изменить**, чтобы изменить существующий адрес в списке, или **Удалить**, чтобы удалить его. Удаление возможно только для адресов, созданных с помощью команды **Добавить**, а не для импортированных адресов.

Во всех списках можно использовать символы «*» (звездочка) и «?» (вопросительный знак). Звездочка означает любое количество символов, а вопросительный знак — только один символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные и безопасные адреса. Точно так же нужно убедиться в том, что символы «*» и «?» в этом списке используются правильно.

> i Если вы хотите заблокировать все HTTP-адреса, кроме адресов, включенных в активный список разрешенных адресов, добавьте «*» в активный список заблокированных адресов.

Создание списка

Это список содержит требуемые URL-адреса или маски доменов, которые будут блокироваться, разрешаться или исключаться из проверки. При создании нового списка укажите следующие параметры.

- **Тип списка адресов** — выберите тип (Исключены из проверки, Заблокированы или Разрешены) в раскрывающемся списке.
- **Имя списка** — укажите название списка. При изменении одного из трех предварительно заданных списков это поле будет неактивно.
- **Описание списка** — введите краткое описание списка (необязательно). При изменении одного из трех предварительно заданных списков поле будет неактивно.
- **Список активен** — данный переключатель позволяет деактивировать список. При необходимости его можно позже активировать.
- **Уведомлять о применении** — воспользуйтесь этим параметром, если требуется получать уведомления о том, что при оценке посещенного HTTP/HTTPS-сайта использовался определенный список. Когда доступ к веб-сайту блокируется или разрешается по причине его присутствия в списке заблокированных или разрешенных адресов, отображается соответствующее уведомление, в котором указывается имя списка, где фигурирует этот веб-сайт.
- **Серьезность регистрируемых событий** — из раскрывающегося списка выберите степень серьезности регистрируемых событий (нет, диагностика, информация или предупреждение). ESET PROTECT может собирать записи со степенью детализации Предупреждение.

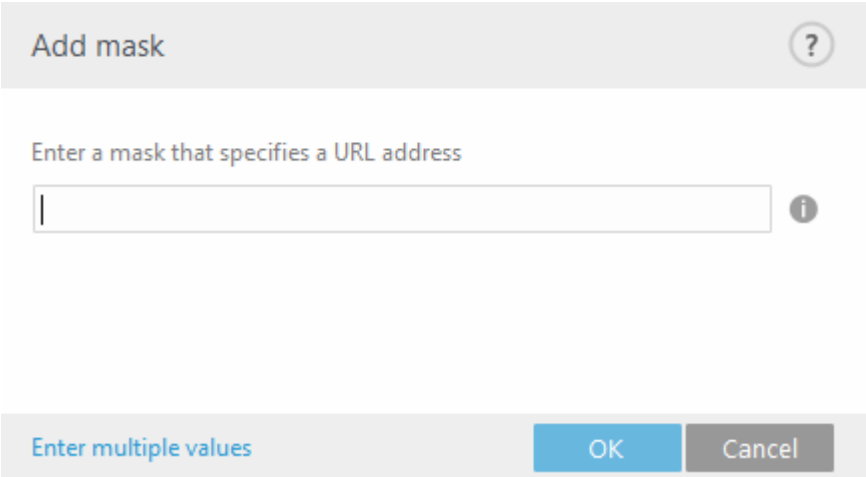
ESET Server Security позволяет пользователям блокировать доступ к указанным веб-узлам и предотвращать отображение их содержимого в веб-браузере. Пользователь может указать адреса, которые необходимо исключить из проверки. Если полное имя удаленного сервера неизвестно или пользователь хочет указать группу удаленных серверов, то для идентификации такой группы можно использовать так называемые маски.

Эти маски обозначаются символами «?» и «*».

- Используйте «?», чтобы заменить любой символ.
- Используйте «*», чтобы заменить текстовую строку.

**.c?m* применяется ко всем адресам, у которых последняя часть начинается с буквы c, заканчивается буквой «m» и содержит неизвестный символ между ними (например, *.com*, *.cam* и т. д.).

Начальная последовательность «*.» перед именем домена интерпретируется особым образом. Прежде всего, в данном случае подстановочный знак «*» не может представлять символ косой черты («/»). Смысл этого исключения — избежать обхода маски, например маска *.domain.com не будет соответствовать адресу *http://*любой_домен*.com/*любой_путь*#.domain.com* (такой суффикс можно присоединить к любому URL-адресу, не влияя на загрузку). Вторая особенность в том, что «*.» в этом особом случае также соответствует пустой строке. Это дает возможность обозначить одной маской целый домен, включая все возможные поддомены. Например, маска *.domain.com также соответствует *https://domain.com*. Использовать маску *domain.com было бы неверно, поскольку она также совпала бы с https://anotherdomain.com..

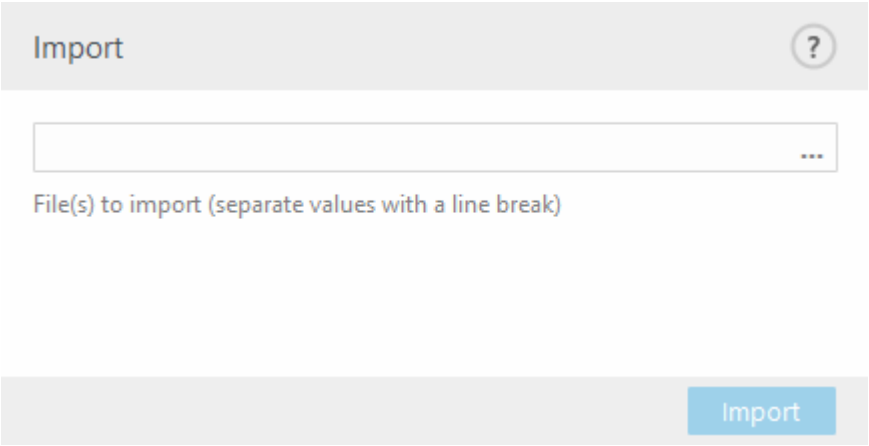


Добавить несколько значений

Добавление нескольких URL-адресов, разделенных переводом строки, запятыми или точками с запятой. Если разрешен выбор нескольких значений, адреса будут отображаться в виде списка.

Импорт

Импортируемый текстовый файл с URL-адресами (в качестве разделителя следует использовать разрыв строки, например в `*.txt` в кодировке UTF-8).

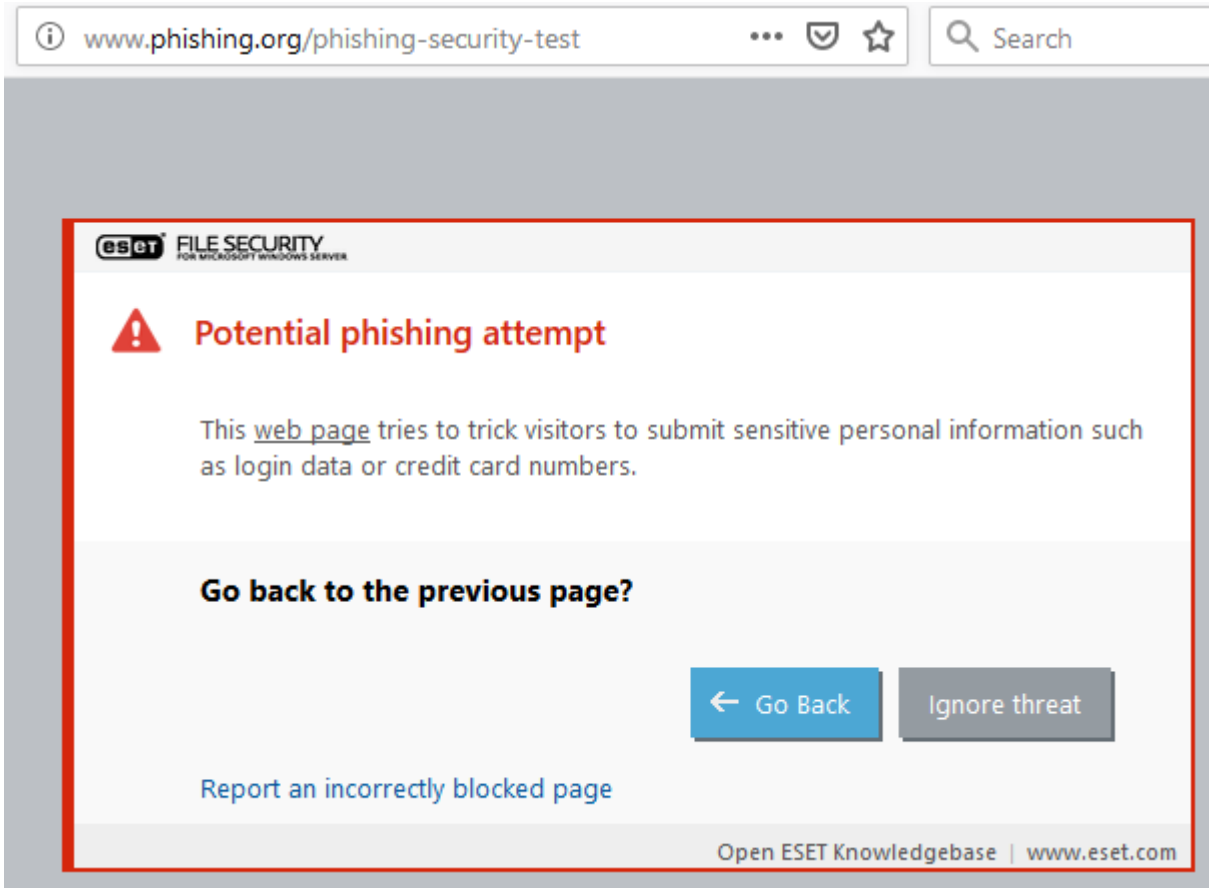


Веб-защита от фишинга

Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п.

Программа ESET Server Security обеспечивает защиту от фишинга, блокируя веб-страницы, о которых известно, что они распространяют такой тип содержимого. Мы настоятельно рекомендуем включить защиту от фишинга в ESET Server Security. Дополнительные сведения о защите от фишинга в программе ESET Server Security см. в статье нашей базы знаний .

Когда открывается фишинговый веб-сайт, в веб-браузере отображается следующее диалоговое окно. Если вы все равно хотите открыть этот веб-сайт, щелкните элемент **Игнорировать угрозу** (не рекомендуется).



> Время, в течение которого можно получить доступ к потенциальному фишинговому веб-сайту, занесенному в «белый» список, по умолчанию ограничивается несколькими часами. Чтобы разрешить доступ к веб-сайту на постоянной основе, используйте инструмент Управление URL-адресами.

Сообщить о фишинговом сайте

Если вы столкнетесь с подозрительным веб-сайтом, который кажется фишинговым или иным образом вредоносным, об этом можно сообщить ESET для анализа. Прежде чем отправлять адрес веб-сайта в компанию ESET, убедитесь, что он соответствует хотя бы одному из следующих критериев:

- веб-сайт совсем не обнаруживается;
- веб-сайт неправильно обнаруживается как угроза. В таком случае можно сообщить о ложной метке фишингового сайта.

Или же адрес веб-сайта можно отправить по электронной почте. Отправьте письмо на адрес samples@eset.com. Помните, что тема письма должна описывать проблему, а в тексте письма следует указать максимально полную информацию о веб-сайте (например, веб-сайт, с которого вы попали на этот сайт, как вы узнали об этом сайте и т. д.).

Контроль устройств

ESET Server Security обеспечивает автоматический контроль устройств (компакт- и DVD-дисков, USB-устройств). Данный модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если администратор компьютера хочет предотвратить использование устройств с нежелательным содержимым.

> ℹ При включении управления устройством с использованием переключателя **Интегрировать в систему** будет активирована функция управления устройством ESET Server Security. Однако для того, чтобы это изменение вступило в силу, необходимо перезагрузить систему.

Управление устройством станет активным, позволяя редактировать его настройки. При обнаружении устройства, заблокированного существующим правилом, отобразится окно уведомления и доступ к устройству будет заблокирован.

Правила

Правило контроля устройств определяет действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.

Группы

Нажимая кнопку Изменить, можно управлять группами устройств. Создайте новую группу устройств или выберите существующую, чтобы добавить или удалить устройства из списка.

> ℹ Вы можете просматривать записи журнала контроля устройств в файлах журналов.

Правила устройств

Вы можете разрешить или заблокировать определенные устройства для конкретных пользователей, их групп или в соответствии с несколькими дополнительными параметрами, которые задаются в конфигурации правил. Список правил содержит несколько описаний для каждого правила, в частности его имя, тип внешнего устройства, выполняемое действие при обнаружении устройства и серьезность для записи в журнал.

Можно **добавить** новое правило или изменить настройки существующего. Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните переключатель рядом с элементом **Правило включено**. Это может

быть полезно, если не нужно полностью удалять правило.

Применять во время

Используя временные интервалы, можно ограничивать правила. Сначала создайте временной интервал, затем он появится в раскрывающемся меню.

Тип устройства

В раскрывающемся меню выберите тип внешнего устройства (дисковый накопитель, портативное устройство, Bluetooth, FireWire и т. д.). Список типов устройств предоставляет операционная система. Их можно просмотреть с помощью диспетчера устройств, в котором отображается все подключенное к компьютеру оборудование. К накопителям относятся внешние диски и традиционные устройства чтения карт памяти, подключенные по протоколу USB или FireWire. Устройства чтения смарт-карт позволяют читать карты со встроенными микросхемами, такие как SIM-карты или идентификационные карточки. Примерами устройств создания изображений являются сканеры или камеры, эти устройства не предоставляют информацию о пользователях, а только информацию об их действиях. Это означает, что устройства обработки изображений могут быть заблокированы только глобально.

Действие

Доступ к устройствам, не предназначенным для хранения данных, можно только разрешить или заблокировать. Напротив, правила для устройств хранения данных позволяют выбрать одно из указанных ниже прав.

- **Чтение и запись** — будет разрешен полный доступ к устройству.
- **Блокировать** — доступ к устройству будет заблокирован.
- **Только чтение** — будет разрешено только чтение данных с устройства.
- **Предупредить** — при каждом подключении устройства пользователь получает уведомление, разрешено это устройство или заблокировано, и при этом создается запись журнала. Устройства не запоминаются. Уведомления отображаются при каждом повторном подключении одного и того же устройства.

> Обратите внимание, что не для всех типов устройств доступен полный список прав (действий). Если на устройстве есть место для хранения данных, будут доступны все четыре действия. Если устройства не предназначены для хранения данных, доступны только два действия (например, право **только чтение** неприменимо к Bluetooth-устройствам: доступ к ним можно только разрешить или заблокировать).

С помощью указанных ниже дополнительных параметров можно точно настраивать и изменять правила для конкретных устройств. Все параметры не зависят от регистра.

- **Производитель** — фильтрация по имени или идентификатору производителя.
- **Модель** — наименование устройства.
- **Серийный номер** — у внешних устройств обычно есть серийные номера. Когда речь идет о компакт- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода компакт-дисков.

> Если не указать три описанные выше дескриптора, то правило будет игнорировать их при поиске соответствий. Для параметров фильтрации во всех текстовых полях не учитывается регистр и не поддерживаются подстановочные знаки (*, ?).

Для просмотра сведений об этом устройстве создайте правило для соответствующего типа устройств, подключите устройство к компьютеру и ознакомьтесь со сведениями об устройстве в журнале контроля устройств.

В раскрывающемся списке выберите **Серьезность регистрируемых событий**:

- **Всегда** — записываются все события.
- **Диагностика** — регистрируется информация, необходимая для тщательной настройки программы.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение** — записывается информация обо всех критических ошибках и предупреждениях.
- **Ничего** — журналы не создаются.

Правила можно назначать только для некоторых пользователей или их групп, добавленных в список пользователей. Щелкните элемент **Изменить**, чтобы управлять **списком пользователей**.

- **Добавить** — открывается диалоговое окно Типы объектов: пользователи и группы, в котором можно выбрать нужных пользователей.
- **Удалить** — выбранный пользователь удаляется из фильтра.

> С помощью правил пользователя можно фильтровать все устройства (например, устройства обработки изображений предоставляют информацию только о вызванных действиях, но не о пользователях).

Доступны указанные ниже функции.

Изменить

Позволяет изменить имя выбранного правила или параметры устройств, которые оно содержит (производитель, модель, серийный номер).

Копировать

С помощью этой команды создается правило на основе параметров выбранного правила.

Удалить

Удаление выбранного правила. Кроме того, можно воспользоваться флажком рядом с тем или иным правилом, чтобы отключить его. Это может быть полезно, если вы не хотите полностью удалять правило и собираетесь воспользоваться им позднее.

Заполнить

Команда предоставляет обзор всех подключенных в настоящее время устройств со следующей информацией: тип устройства, производитель, модель и серийный номер (если есть). Если выбрать устройство в списке обнаруженных устройств и нажать кнопку **OK**, в открывшемся окне редактора правил можно ознакомиться с предварительно заданной информацией (все параметры можно настраивать).

Правила приведены в порядке их приоритета: правила с более высоким приоритетом располагаются вверху. Чтобы выделить несколько правил и применить к ним необходимые действия, например удалить или переместить к началу либо концу списка, воспользуйтесь элементами **Сверху**/**Вверх**/**Вниз**/**Снизу** (кнопки со стрелками).

Группы устройств

Окно групп устройств разделено на две части. В правой части окна отображается список устройств, входящих в выбранную группу, а в левой части — список созданных групп. Выберите группу, содержащую устройства, которые нужно отобразить на правой панели.

Вы можете создать разные группы устройств, к которым будут применяться разные правила. Можно также создать одну группу устройств, настроенную для **чтения** и **записи** или **только для чтения**. Благодаря этому, когда к компьютеру подключаются нераспознанные устройства, функция контроля устройств их блокирует.

> ⚠ Наличие внешнего устройства, подключенного к компьютеру, может представлять угрозу безопасности.

Доступны указанные ниже функции.

Добавить

Создание новой группы устройств путем ввода имени или добавлением устройства в существующую группу (в зависимости от того, где именно нажата кнопка). При необходимости можно указать такие сведения, как имя поставщика, модель и серийный номер.

Изменить

Позволяет изменить имя выбранной группы или параметры устройств, которые она содержит (производитель, модель, серийный номер).

Удалить

Удаление выбранного правила. Кроме того, можно воспользоваться флажком рядом с тем или иным правилом, чтобы отключить его. Это может быть полезно, если вы не хотите полностью удалять правило и собираетесь воспользоваться им позднее.

Импорт

Импортирует список серийных номеров устройств из файла.

Заполнить

Команда предоставляет обзор всех подключенных в настоящее время устройств со следующей информацией: тип устройства, производитель, модель и серийный номер (если есть). Если

выбрать устройство в списке обнаруженных устройств и нажать кнопку **OK**, в открывшемся окне редактора правил можно ознакомиться с предварительно заданной информацией (все параметры можно настраивать).

Завершив настройки, нажмите кнопку **OK**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, нажмите кнопку **Отмена**.

> i Обратите внимание, что не для всех типов устройств доступен полный список прав (действий). Если на устройстве есть место для хранения данных, будут доступны все четыре действия. Если устройства не предназначены для хранения данных, доступны только два действия (например, право только чтение неприменимо к Bluetooth-устройствам: доступ к ним можно только разрешить или заблокировать).

Конфигурация сервиса

Для следующих целей можно настроить дополнительные параметры.

- Временные интервалы
- Microsoft Windows® Update
- ESET CMD
- ESET RMM
- Лицензия
- Поставщик инструментария WMI
- Объекты сканирования в консоли управления ESET
- Файлы журнала
- Прокси-сервер
- Уведомления
- Режим презентации
- Диагностика
- Кластер

Временные интервалы

Вместе с правилами контроля устройств применяются временные интервалы, которые их ограничивают. Создание временного интервала и его выбор во время добавления новых правил или изменения существующих (параметр **Применять во время**). Это позволяет определить часто используемые временные интервалы (рабочее время, выходные и т. д.) и с легкостью повторно их использовать без переопределения диапазонов времени для каждого правила. Временной интервал должен быть применим к любому соответствующему типу

правил, в которых поддерживается контроль, основанный на времени.

Центр обновления Windows

Обновления Windows содержат важные исправления потенциально опасных уязвимостей и повышают общий уровень безопасности компьютера. По этой причине обновления Microsoft Windows следует устанавливать сразу после их появления. Программное обеспечение ESET Server Security уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений**: запросы на загрузку обновлений системы не отображаются.
- **Необязательные обновления**: отображаются запросы на загрузку обновлений, имеющих низкий и более высокие уровни приоритета.
- **Рекомендуемые обновления**: отображаются запросы на загрузку обновлений, имеющих обычный и более высокие уровни приоритета.
- **Важные обновления**: отображаются запросы на загрузку обновлений, помеченных как важные и имеющих более высокий уровень приоритета.
- **Критические обновления**: пользователю предлагается загрузить только критические обновления.

Для сохранения изменений нажмите кнопку **OK**. После проверки статуса сервера обновлений на экран будет выведено окно «Обновления системы», и непосредственно после сохранения изменений данные об обновлении системы могут быть недоступны.

Сканер командной строки

В качестве альтернативы для eShell можно запустить модуль сканирования по требованию ESET Server Security из командной строки с помощью файла `ecls.exe`, который расположен в папке установки.

Ниже приводится список параметров и переключателей.

Параметры:

`/base-dir=FOLDER`	загрузить модули из ПАПКИ
`/quar-dir=FOLDER`	ПАПКА карантина
`/exclude=MASK`	не сканировать файлы, соответствующие МАСКА
`/subdir`	сканировать вложенные папки (по умолчанию)
`/no-subdir`	не сканировать вложенные папки
`/max-subdir-level=LEVEL`	максимальная степень вложенности папок для сканирования (по умолчанию 0 — без ограничений)
`/symlink`	следовать по символическим ссылкам (по умолчанию)
`/no-symlink`	пропускать символические ссылки
`/ads`	сканировать ADS (по умолчанию)

/no-ads	не сканировать ADS
/log-file=FILE	вывод журнала в ФАЙЛ
/log-rewrite	перезаписывать выходной файл (по умолчанию — добавлять)
/log-console	вывод журнала в окно консоли (по умолчанию)
/no-log-console	не выводить журнал в консоль
/log-all	регистрировать чистые файлы
/no-log-all	не регистрировать чистые файлы (по умолчанию)
/aind	показывать индикатор работы
/auto	Сканирование и автоматическая очистка всех локальных дисков

Параметры модуля сканирования:

/files	сканировать файлы (по умолчанию)
/no-files	не сканировать файлы
/memory	сканировать память
/boots	сканировать загрузочные секторы
/no-boots	не сканировать загрузочные секторы (по умолчанию)
/arch	сканировать архивы (по умолчанию)
/no-arch	не сканировать архивы
/max-obj-size=SIZE	сканировать файлы, только если их размер не превышает РАЗМЕР Мб (по умолчанию 0 = без ограничений)
/max-arch-level=LEVEL	максимальная степень вложенности архивов для сканирования
/scan-timeout=LIMIT	сканировать архивы в ПРЕДЕЛЕ с.
/max-arch-size=SIZE	сканировать файлы в архивах, только если их размер не превышает РАЗМЕР (по умолчанию 0 = без ограничений)
/max-sfx-size=SIZE	сканировать файлы в самораспаковывающихся архивах, только если их размер не превышает РАЗМЕР Мб (по умолчанию 0 = без ограничений)
/mail	сканировать файлы электронной почты (по умолчанию)
/no-mail	не сканировать файлы электронной почты
/mailbox	сканировать почтовые ящики (по умолчанию)
/no-mailbox	Не сканировать почтовые ящики
/sfx	сканировать самораспаковывающиеся архивы (по умолчанию)
/no-sfx	не сканировать самораспаковывающиеся архивы
/rtp	сканировать упаковщики в реальном времени (по умолчанию)
/no-rtp	не сканировать упаковщики в реальном времени
/unsafe	сканировать потенциально опасное ПО
/no-unsafe	не сканировать потенциально опасное ПО (по умолчанию)
/unwanted	сканировать потенциально нежелательное ПО
/no-unwanted	не сканировать потенциально нежелательное ПО (по умолчанию)
/suspicious	Сканировать на предмет наличия подозрительных приложений (по умолчанию)

/no-suspicious	Не сканировать на предмет наличия подозрительных приложений
/pattern	использовать сигнатуры (по умолчанию)
/no-pattern	не использовать сигнатуры
/heur	включить эвристику (по умолчанию)
/no-heur	отключить эвристику
/adv-heur	включить расширенную эвристику (по умолчанию)
/no-adv-heur	отключить расширенную эвристику
/ext-exclude=EXTENSIONS	исключить из сканирования РАСШИРЕНИЯ файлов, разделенные точкой с запятой
/clean-mode=MODE	использовать РЕЖИМ очистки для зараженных объектов Доступны указанные ниже варианты. • none (по умолчанию): автоматическая очистка не выполняется. • standard: ecls.exe попытается автоматически очистить или удалить зараженные файлы. • strict: ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (перед удалением файлов не отображается запрос для пользователя). • rigorous: ecls.exe будет удалять файлы, не пытаясь очистить их, независимо от того, что это за файлы. • delete: ecls.exe будет удалять файлы, не пытаясь очистить их, но не будет удалять важные файлы, например системные файлы Windows.
/quarantine	копировать зараженные файлы (если они очищены) в карантин (дополнение к действию, выполняемое при очистке)
/no-quarantine	не копировать зараженные файлы в папку карантина

Общие параметры:

/help	показать справку и выйти
/version	показать сведения о версии и выйти
/preserve-time	сохранить отметку о времени последнего доступа

Коды выхода:

0	угрозы не найдены
1	угрозы обнаружены и очищены
10	не удалось просканировать некоторые файлы (могут содержать угрозы)
50	обнаружена угроза
100	ошибка (коды выхода, превышающие 100, означают, что файл не был просканирован и не может считаться чистым)

ESET CMD

Это функция, позволяющая применять расширенные команды ECMD. Она позволяет экспортировать и импортировать параметры с помощью командной строки (ecmd.exe). До недавнего времени экспортировать параметры можно было только через графический интерфейс пользователя. Конфигурацию ESET Server Security можно экспортировать в файл с

расширением *.xml*.

Если включена функция ESET CMD, доступны два метода авторизации:

- **Нет** — без авторизации. Этот метод не рекомендуется, так как он разрешает импортировать любую неподписанную конфигурацию, что представляет собой потенциальный риск.

- **Пароль для расширенной настройки** — пароль требуется для импорта конфигурации из файла с расширением .xml. Этот файл должен быть подписан (сведения о подписании файла конфигурации с расширением .xml представлены далее). Новую конфигурацию можно импортировать только после того, как будет указан пароль, заданный в разделе Настройка доступа. Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате .xml не подписан, импорт конфигурации выполнен не будет.

После включения ESET CMD можно использовать командную строку для импорта и экспорта конфигураций программы ESET Server Security. Это можно сделать вручную или создать сценарий с целью автоматизации.

Для использования расширенных команд ECMD необходимо запустить их с правами администратора или открыть командную строку Windows (cmd) командой **Запуск от имени администратора**. В противном случае появляется сообщение **Ошибка выполнения команды**. Кроме того, при экспорте конфигурации папка назначения должна существовать. Команда экспорта работает даже при отключенном параметре ESET CMD.

Команда экспорта настроек:
```
ecmd /getcfg c:\config\settings.xml
```

Команда импорта настроек:
```
ecmd /setcfg c:\config\settings.xml
```

Расширенные команды ECMD можно выполнять только локально. Запуск клиентской задачи **Выполнение команды** с помощью ESET PROTECT является невозможным.

Для подписания файла конфигурации в формате *.xml* выполните следующие действия.

1. Загрузите исполняемый файл XmlSignTool.

2. Откройте командную строку Windows (cmd) в режиме **Запуск от имени администратора**.

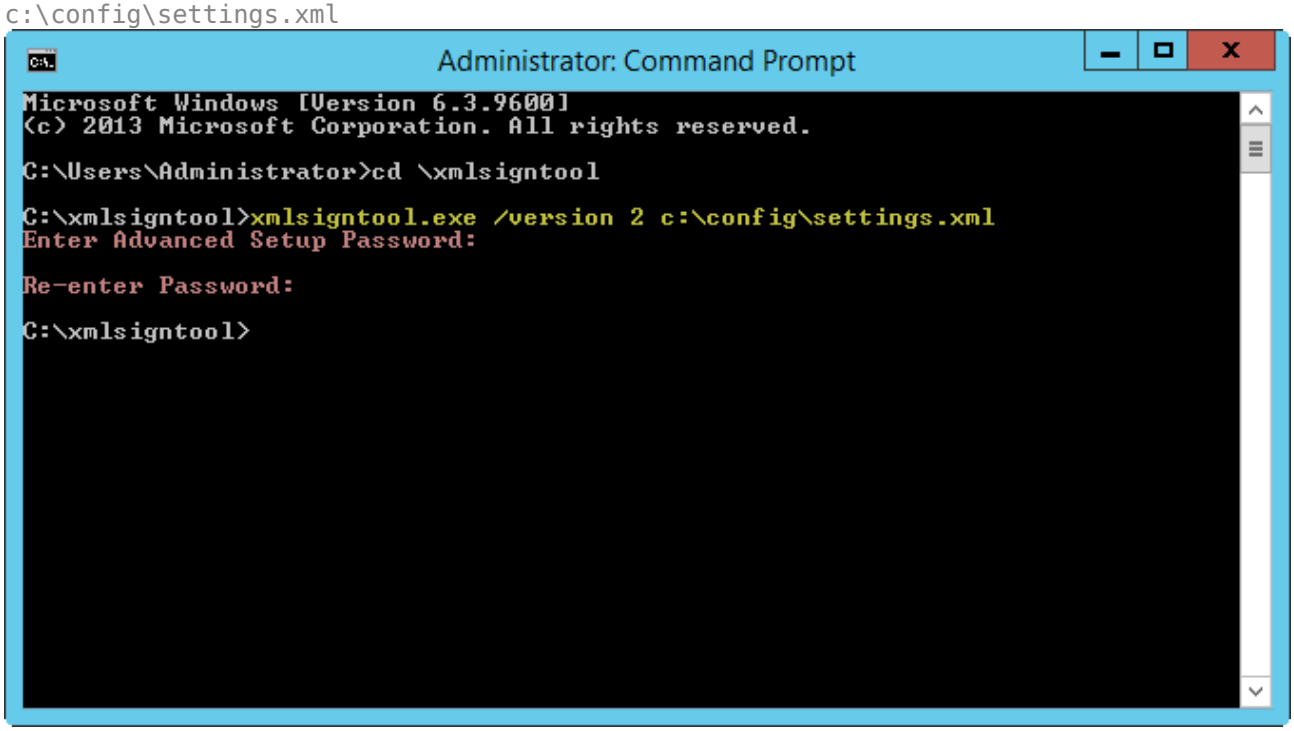
3. Перейдите в расположение файла `xmlsigntool.exe`.

4. Выполните команду для подписания файла *.xml* конфигурации, расположенного по пути `xmlsigntool /version 1|2 <xml_file_path>`.

Значение параметра `/version` определяется версией ESET Server Security. Используйте для ESET Server Security 7 `/version 2` или более новую.

5. Введите пароль для дополнительных настроек, а затем введите его еще раз по запросу средства XmlSignTool. Теперь файл конфигурации в формате *.xml* подписан и может использоваться для импорта в другом экземпляре ESET Server Security с функцией ESET CMD с помощью метода парольной авторизации.

Команда подписания экспортированного файла конфигурации: `xmlsigntool /version 2 c:\config\settings.xml`



Если пароль в разделе Настройка доступа изменится и потребуется импортировать конфигурацию, подписанную ранее с помощью старого пароля, можно подписать файл конфигурации в формате *.xml* заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другой компьютер с работающей программой ESET Server Security перед импортом.

ESET RMM

Удаленный мониторинг и управление (RMM) — это процесс наблюдения и контроля за системами программного обеспечения (например, на настольных компьютерах, серверах и мобильных устройствах) с помощью локально установленного агента, к которому может обратиться поставщик услуг управления.

Включить RMM

Включение функции удаленного мониторинга и управления. Для использования утилиты RMM необходимы права администратора.

Режим работы

В раскрывающемся меню выберите рабочий режим RMM:

- **Только безопасное разделение** — если необходимо включить интерфейс RMM для безопасных операций и только для чтения;
- **Все операции** — если хотите включить интерфейс RMM для всех операций.

Метод авторизации

В раскрывающемся меню выберите способ авторизации RMM:

- **Нет** — проверка пути приложения выполняться не будет, *ermm.exe* можно запустить из любого приложения

- **Путь приложения** — укажите приложение, которому разрешено запускать *ermm.exe*

Установка ESET Server Security по умолчанию содержит файл *ermm.exe*, расположенный в ESET Server Security (путь по умолчанию *c:\Program Files\ESET\ESET Server Security*). *ermm.exe* обменивается данными с плагином RMM, который связывается с агентом RMM, связанным с сервером RMM.

- *ermm.exe* — утилита командной строки, разработанная ESET, которая позволяет управлять продуктами для конечных точек и взаимодействовать с любым плагином RMM.

- Плагин RMM — приложение стороннего производителя, работающее локально в системе конечных точек Windows. Плагин был разработан для связи с конкретным агентом RMM (например, только с Kaseya) и с *ermm.exe*.

- Агент RMM — стороннее приложение (например, от Kaseya), работающее локально в системе конечных точек Windows. Агент взаимодействует с плагином RMM и с сервером RMM.

- Сервер RMM — выполняется как служба на стороннем сервере. Поддерживаемые системы RMM — Kaseya, Labtech, Autotask, Max Focus и Solarwinds N-able.

Дополнительные сведения о ESET RMM в ESET Server Security см. в статье нашей базы знаний.

Плагин ESET Direct Endpoint Management для сторонних RMM решений

Сервер RMM работает как служба на сервере стороннего производителя. Дополнительные сведения см. в указанных ниже интерактивных руководствах пользователя ESET Direct Endpoint Management.

- Плагин ESET Direct Endpoint Management для ConnectWise Automate

- Плагин ESET Direct Endpoint Management для DattoRMM

- ESET Direct Endpoint Management для Solarwinds N-Central

- ESET Direct Endpoint Management для NinjaRMM

Лицензия

ESET Server Security подключается к серверу лицензий ESET несколько раз в час для проведения проверок. По умолчанию для параметра **Интервал проверки** установлено значение **Автоматически**. Если необходимо уменьшить сетевой трафик, создаваемый проверками лицензии, измените интервал проверки на **Ограниченный**, и проверка лицензии будет выполняться только один раз в день (а также после перезагрузки сервера).

Если для интервала проверки установлено значение **Ограниченный**, реализация всех связанных с лицензиями изменений, выполняемых с вашей системой ESET Server Security через ESET Business Account и ESET MSP Administrator, может занимать до одного дня.

Поставщик инструментария WMI

Инструментарий управления Windows (WMI) — это реализация корпорацией Майкрософт инициативы «управление предприятием через Интернет». Это отраслевая инициатива, направленная на разработку стандартной технологии, с помощью которой в корпоративной среде можно было бы получать доступ к административной информации.

Дополнительные сведения об инструментарии WMI см. в статье по адресу http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Поставщик инструментария ESET WMI

Поставщик инструментария ESET WMI нужен для удаленного мониторинга программ ESET, работающих в корпоративной среде, без использования специальных программ или средств ESET. Делая доступными с помощью инструментария WMI базовые сведения о программе, состоянии и статистике, мы значительно расширяем возможности мониторинга программ ESET для администраторов предприятий.

Инструментарий WMI позволяет администраторам пользоваться рядом методов доступа (командной строкой, сценариями и сторонними инструментами корпоративного мониторинга), чтобы отслеживать состояние программ ESET.

Текущая версия инструментария предоставляет доступ только для чтения к базовым сведениям о программе, установленных компонентах и состоянии защиты, данным статистики отдельных модулей сканирования, а также к журналам программы.

Поставщик инструментария WMI дает возможность считывать состояния и журналы продукта с помощью стандартных средств и инфраструктуры Windows WMI.

Предоставляемые данные

Все классы WMI, связанные с продуктом ESET, расположены в пространстве имен «root\ESET». Ниже приводится более подробное описание классов, которые используются в настоящее время.

Общие сведения

- ESET_Product
- ESET_Features
- ESET_Statistics

Журналы

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs

- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

Класс ESET_Product

Класс ESET_Product может существовать только в одном экземпляре. Свойства этого класса относятся к основной информации об установленном продукте ESET:

- ID — идентификатор типа продукта, например emsl
- Name — название продукта, например «ESET Mail Security»
- FullName — полное название продукта, например «ESET Mail Security for IBM Domino».
- Version — версия продукта, например 6.5.14003.0.
- VirusDBVersion — версия базы данных вирусов, например 14533 (20161201).
- VirusDBLastUpdate — отметка о времени последнего обновления вирусной базы данных. В строке содержится отметка о времени в формате даты и времени WMI, например 20161201095245.000000+060.
- LicenseExpiration — время окончания срока действия лицензии. В строке содержится отметка о времени в формате даты и времени WMI..
- KernelRunning — логическое значение, указывающее, запущена ли служба на компьютере, например «TRUE».
- StatusCode — цифра, указывающая на состояние защиты программы: 0 — зеленый (OK), 1 — желтый (предупреждение), 2 — красный (ошибка).
- StatusText — сообщение, объясняющее, почему код состояния (StatusCode) не равняется нулю (это сообщение не отображается, если код состояния равняется нулю).

Класс ESET_Features

Класс ESET_Features имеет несколько экземпляров. Их число зависит от количества компонентов

программы. Каждый экземпляр содержит следующие сведения:

- Name — имя компонента (список имен приведен ниже).
- Status — состояние компонента: 0 — неактивно, 1 — отключено, 2 — включено.

Список строк с компонентами программы, которые сейчас признаются:

- CLIENT_FILE_AV — защита файловой системы от вирусов в реальном времени.
- CLIENT_WEB_AV — защита клиента от вирусов при доступе в Интернет.
- CLIENT_DOC_AV — защита документов клиента от вирусов
- CLIENT_NET_FW — персональный файервол клиента.
- CLIENT_EMAIL_AV — защита электронной почты клиента от вирусов
- CLIENT_EMAIL_AS — защита электронной почты клиента от спама.
- SERVER_FILE_AV — защита файлов, хранящихся в защищенном серверном продукте, от вирусов в режиме реального времени, например файлов в базе данных контента SharePoint при использовании программы ESET Server Security.
- SERVER_EMAIL_AV — защита от вирусов сообщений электронной почты в защищенном серверном продукте, например сообщений в Microsoft Exchange или IBM Domino.
- SERVER_EMAIL_AS — защита от спама сообщений электронной почты в защищенном серверном продукте, например сообщений в Microsoft Exchange или IBM Domino.
- SERVER_GATEWAY_AV — защита защищенных сетевых протоколов в шлюзе от вирусов.
- SERVER_GATEWAY_AS — защита защищенных сетевых протоколов в шлюзе от спама.

Класс ESET_Statistics

Класс ESET_Statistics имеет несколько экземпляров. Их число зависит от количества модулей сканирования в программе. Каждый экземпляр содержит следующие сведения:

- Scanner — код строки для конкретного сканера, например «CLIENT_FILE».
- Total — общее количество просканированных файлов.
- Infected — количество найденных зараженных файлов.
- Cleaned — количество очищенных файлов.
- Timestamp — отметка о времени последнего изменения этой статистики. В формате даты и времени WMI эта отметка выглядит так: 20130118115511.000000+060.
- ResetTime — отметка о времени последнего сброса счетчика статистики. В формате даты и времени WMI эта отметка выглядит так: 20130118115511.000000+060.

Список строк с модулями сканирования, которые сейчас признаются:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Класс ESET_ThreatLog

Класс ESET_ThreatLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «Обнаруженные угрозы». Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор записи журнала сканирования.
- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- Scanner — имя модуля сканирования, создавшего данное событие журнала.
- ObjectType — тип объекта, сгенерировавшего это событие журнала.
- ObjectName — имя объекта, сгенерировавшего это событие журнала.
- Threat — имя угрозы, найденной в объекте, который описывают свойства ObjectName и ObjectType.
- Action — действие после идентификации угрозы.
- User — учетная запись пользователя, обусловившая создание события журнала.
- Information — дополнительное описание события.
- Hash — хеш объекта, создавшего это событие журнала.

ESET_EventLog

Класс ESET_EventLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «События». Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор записи журнала сканирования.
- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация,

важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

- Module — имя модуля сканирования, создавшего данное событие журнала.

- Event: описание события.

- User — учетная запись пользователя, обусловившая создание события журнала.

ESET_ODFileScanLogs

Класс ESET_ODFileScanLogs имеет несколько экземпляров, каждый из которых представляет запись о сканировании файлов по требованию. Этот список идентичен показываемому в графическом интерфейсе списку журналов «Сканирование ПК по требованию». Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор записи журнала сканирования.

- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).

- Targets — просканированные папки и объекты.

- TotalScanned — общее количество просканированных объектов.

- Infected — количество найденных зараженных объектов.

- Cleaned — количество очищенных объектов.

- Status — состояние процесса сканирования.

ESET_ODFileScanLogRecords

Класс ESET_ODFileScanLogRecords имеет несколько экземпляров, каждый из которых представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_ODFileScanLogs. Экземпляры этого класса содержат записи журнала о всех сканированиях по требованию или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр класса содержит следующие сведения:

- LogID — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_ODFileScanLogs).

- ID — уникальный идентификатор записи журнала сканирования.

- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).

- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

- Log — сообщение журнала.

ESET_ODServerScanLogs

Класс ESET_ODServerScanLogs имеет несколько экземпляров, каждый из которых представляет запись о сканировании сервера по требованию. Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор записи журнала сканирования.
- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).
- Targets — просканированные папки и объекты.
- TotalScanned — общее количество просканированных объектов.
- Infected — количество найденных зараженных объектов.
- Cleaned — количество очищенных объектов.
- RuleHits — общее количество совпадений по правилам.
- Status — состояние процесса сканирования.

ESET_ODServerScanLogRecords

Класс ESET_ODServerScanLogRecords имеет несколько экземпляров, каждый из которых представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_ODServerScanLogs. Экземпляры этого класса содержат записи журнала о всех сканированиях по требованию или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр класса содержит следующие сведения:

- LogID — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_ ODServerScanLogs).
- ID — уникальный идентификатор записи журнала сканирования.
- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- Log — сообщение журнала.

ESET_SmtpProtectionLog

В классе ESET_SmtpProtectionLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «Защита SMTP». Каждый экземпляр содержит следующие сведения.

- ID — уникальный идентификатор записи журнала сканирования.
- Timestamp — отметка о времени создания записи журнала (в формате даты и времени

WMI).

• LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

• HELODomain — имя домена HELO.

• IP — исходный IP-адрес.

• Sender — отправитель сообщений электронной почты.

• Recipient — получатель сообщений электронной почты.

• ProtectionType — используемый тип защиты.

• Action — выполненное действие.

• Reason — причина действия.

• TimeToAccept — количество минут, по прошествии которых сообщение электронной почты будет принято.

ESET_HIPSLog

В классе ESET_HIPSLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «HIPS». Каждый экземпляр содержит следующие сведения.

• ID — уникальный идентификатор записи журнала.

• Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).

• LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

• Application — исходное приложение.

• Target — тип операции.

• Action — действие, которое выполнил HIPS, например разрешение, запрет и т. д.

• Rule — имя правила ответственного за действие.

• AdditionalInfo

ESET_URLLog

В классе ESET_URLLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «Отфильтрованные веб-сайты». Каждый экземпляр содержит следующие сведения.

• ID — уникальный идентификатор записи журнала.

• Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).

• LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

• URL — URL-адрес.

• Status — какие действия были предприняты в отношении URL-адреса, например «Заблокировано средством контроля доступа в Интернет».

• Application — приложение, которое пыталось получить доступ к URL-адресу.

• User — учетная запись пользователя, от имени которой выполнялось приложение.

ESET_DevCtrlLog

В классе ESET_DevCtrlLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «Контроль устройств». Каждый экземпляр содержит следующие сведения.

• ID — уникальный идентификатор записи журнала.

• Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).

• LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

• Device — имя устройства.

• User — имя учетной записи пользователей.

• UserSID — идентификатор безопасности учетной записи пользователей.

• Group — имя группы пользователей.

• GroupSID — идентификатор безопасности группы пользователей.

• Status — какие действия были предприняты в отношении устройства, например «Запись заблокирована».

• DeviceDetails — дополнительная информация, которая касается устройства.

• EventDetails — дополнительная информация, которая касается события.

ESET_MailServerLog

В классе ESET_MailServerLog имеется несколько экземпляров, каждый из которых представляет

запись из журнала «Почтового сервера». Каждый экземпляр содержит следующие сведения.

- ID — уникальный идентификатор записи журнала.
- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- IPAddr — исходный IP-адрес.
- HELODomain — имя домена HELO.
- Sender — отправитель сообщений электронной почты.
- Recipient — получатель сообщений электронной почты.
- Subject — тема сообщения электронной почты.
- ProtectionType — тип защиты, выполнивший действие, описанное в текущей записи журнала, например вредоносные программы, антиспам или правила.
- Action — выполненное действие.
- Reason — причина выполнения действия над объектом, текущим ProtectionType.

ESET_HyperVScanLogs

В классе ESET_HyperVScanLogs имеется несколько экземпляров, каждый из которых представляет запуск сканирования файлов Hyper-V. Этот список идентичен показываемому в графическом интерфейсе списку журналов «Сканирование Hyper-V». Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор записи журнала.
- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).
- Targets — целевые компьютеры, диски, тома, которые были сканированы.
- TotalScanned — общее количество просканированных объектов.
- Infected — количество найденных зараженных объектов.
- Cleaned — количество очищенных объектов.
- Status — состояние процесса сканирования.

ESET_HyperVScanLogRecords

В классе ESET_HyperVScanLogRecords имеется несколько экземпляров, каждый из которых

представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_HyperVScanLogs. Экземпляры этого класса содержат записи журнала обо всех сканированиях Hyper-V или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр класса содержит следующие сведения.

- LogID — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_HyperVScanLogs).

- ID — уникальный идентификатор записи журнала.

- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).

- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

- Log — сообщение журнала.

ESET_NetworkProtectionLog

В классе ESET_NetworkProtectionLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «Защита сети». Каждый экземпляр содержит следующие сведения.

- ID — уникальный идентификатор записи журнала.

- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).

- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.

- Event — событие, вызывающее действие функции защиты сети.

- Action — действие, выполненное функцией защиты сети.

- Source — исходный адрес сетевого устройства.

- Target — адрес назначения сетевого устройства.

- Protocol — протокол сетевого подключения.

- RuleOrWormName — имя правила или червя, связанного с событием.

- Application — приложение, инициировавшее сетевое подключение.

- User — учетная запись пользователя, обусловившая создание события журнала.

ESET_SentFilesLog

В классе ESET_SentFilesLog имеется несколько экземпляров, каждый из которых представляет запись из журнала «Отправленные файлы». Каждый экземпляр содержит следующие сведения.

- ID — уникальный идентификатор записи журнала.
- Timestamp — отметка о времени создания записи журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- Sha1 — хеш Sha-1 отправленного файла.
- File — отправленный файл.
- Size — размер отправленного файла.
- Category — категория отправленного файла.
- Reason — причина отправки файла.
- SentTo — подразделение компании ESET, в которое отправлен файл.
- User — учетная запись пользователя, обусловившая создание события журнала.

ESET_OneDriveScanLogs

В классе ESET_OneDriveScanLogs имеется несколько экземпляров, каждый из которых представляет запуск сканирования OneDrive. Этот список идентичен отображаемому в графическом интерфейсе списку журналов «Сканирование OneDrive». Каждый экземпляр содержит следующие сведения:

- ID — уникальный идентификатор этого журнала OneDrive.
- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).
- Targets — просканированные папки и объекты.
- TotalScanned — общее количество просканированных объектов.
- Infected — количество найденных зараженных объектов.
- Cleaned — количество очищенных объектов.
- Status — состояние процесса сканирования.

ESET_OneDriveScanLogRecords

Класс ESET_OneDriveScanLogRecords имеет несколько экземпляров, каждый из которых

представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_OneDriveScanLogs. Экземпляры этого класса содержат записи журнала обо всех сканированиях OneDrive или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр содержит следующие сведения:

- LogID — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_OneDriveScanLogs).
- ID — уникальный идентификатор этого журнала OneDrive.
- Timestamp — отметка о времени создания журнала (в формате даты и времени WMI).
- LogLevel — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- Log — сообщение журнала.

Получение доступа к предоставляемым данным

Далее описывается несколько способов получения доступа к данным ESET WMI из командной строки Windows и PowerShell, которые подходят для любой установленной версии ОС Windows. Кроме того, существует множество других способов получения доступа к данным из других средств и языков сценария.

Командная строка без сценариев

Командной строки `wmic` может использоваться для получения доступа к различным предварительно заданным или любым настраиваемым классам инструментария WMI.

Чтобы отобразить полную информацию о продукте на локальном компьютере:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Чтобы отобразить номер версии продукта только для продукта на локальном компьютере:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Чтобы отобразить полную информацию о продукте на удаленном компьютере с IP-адресом 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Получить и отобразить полную информацию о продукте на локальном компьютере:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Получить и отобразить полную информацию о продукте на удаленном компьютере с IP-адресом 10.1.118.180:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
cred $cred
```

Объекты сканирования в консоли управления ESET

Эта функция позволяет решению ESET PROTECT использовать объект сканирования (сканирование базы данных почтовых ящиков по требованию и сканирование Hyper-V) при выполнении клиентской задачи Сканирование сервера на сервере, на котором установлена программа ESET Server Security. Настройка объектов сканирования в ESET PROTECT доступна, только если установлен агент ESET Management Agent, в ином случае эта настройка будет неактивной.

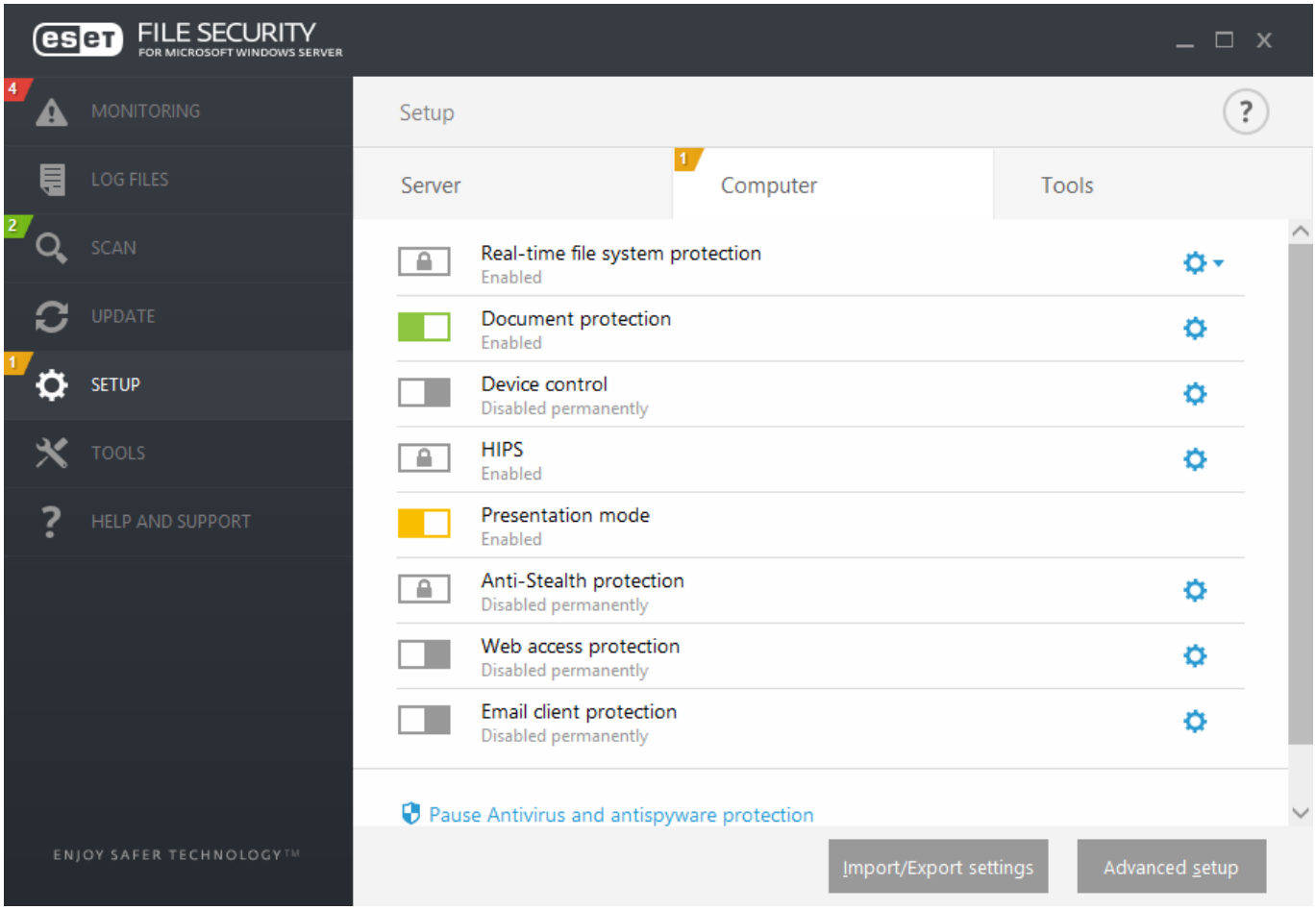
При включении функции **Создание списка объектов** ESET Server Security создает список доступных объектов сканирования. Этот список создается время от времени в соответствии с заданным **интервалом обновления**.

> При первом включении функции **Создание списка объектов** на создание списка службе ESET PROTECT требуется около половины указанного **интервала обновления**. Если **интервал обновления** составляет 60 минут, службе ESET PROTECT потребуется около 30 минут, чтобы получить список объектов сканирования. Если нужно, чтобы служба ESET PROTECT получила список быстрее, установите меньшее значение для интервала обновления. Потом его всегда можно увеличить.

При запуске клиентской задачи **Сканирование сервера** решение ESET PROTECT создает список и предлагает пользователю выбрать объекты для сканирования Hyper-V на заданном сервере.

Режим переопределения

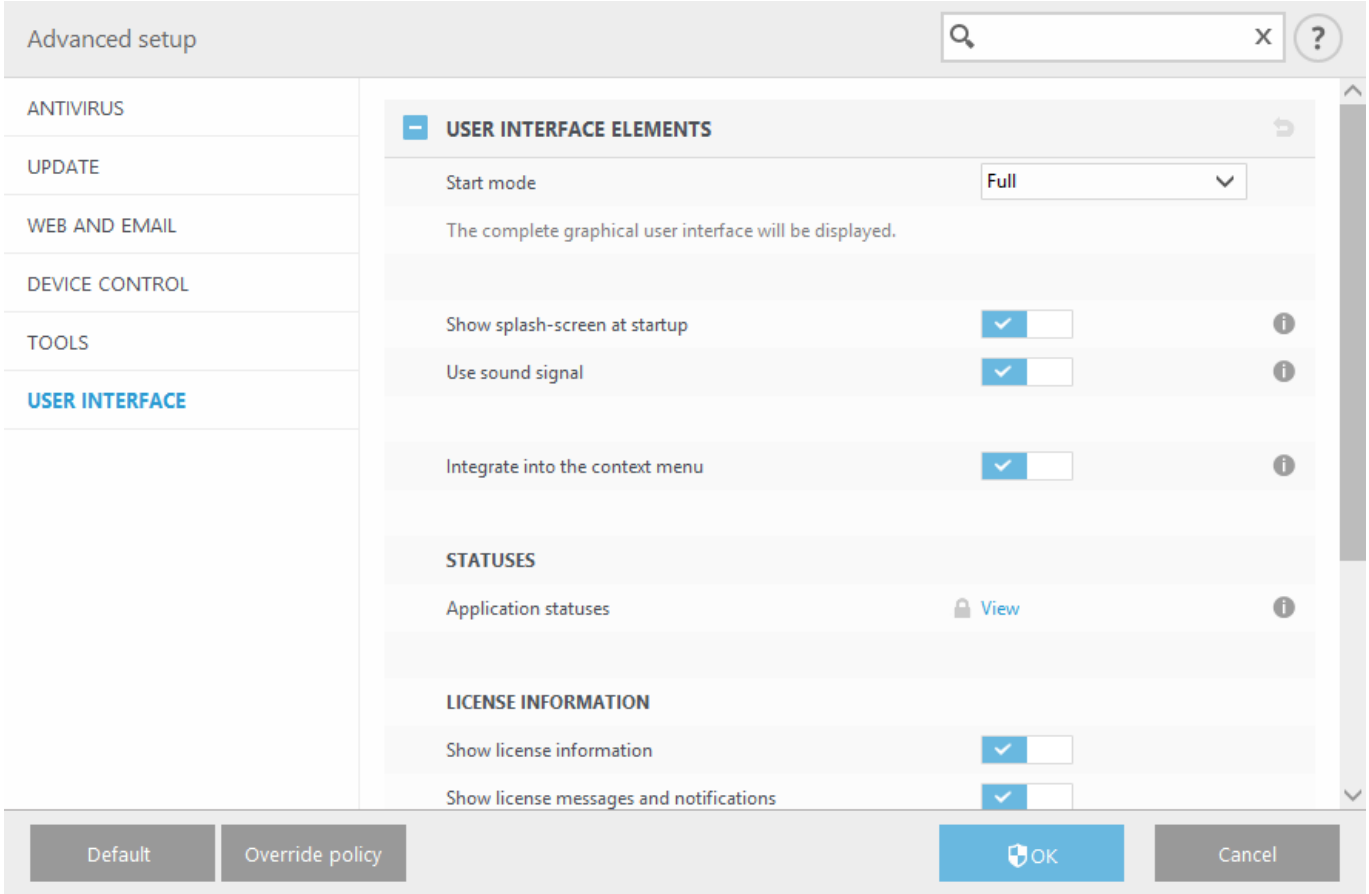
Если к ESET PROTECT применяется политика ESET Server Security, будет отображаться значок блокировки вместо переключателя «Включить/отключить» на странице с настройками и значок блокировки рядом с переключателем в окне **Дополнительные настройки**.



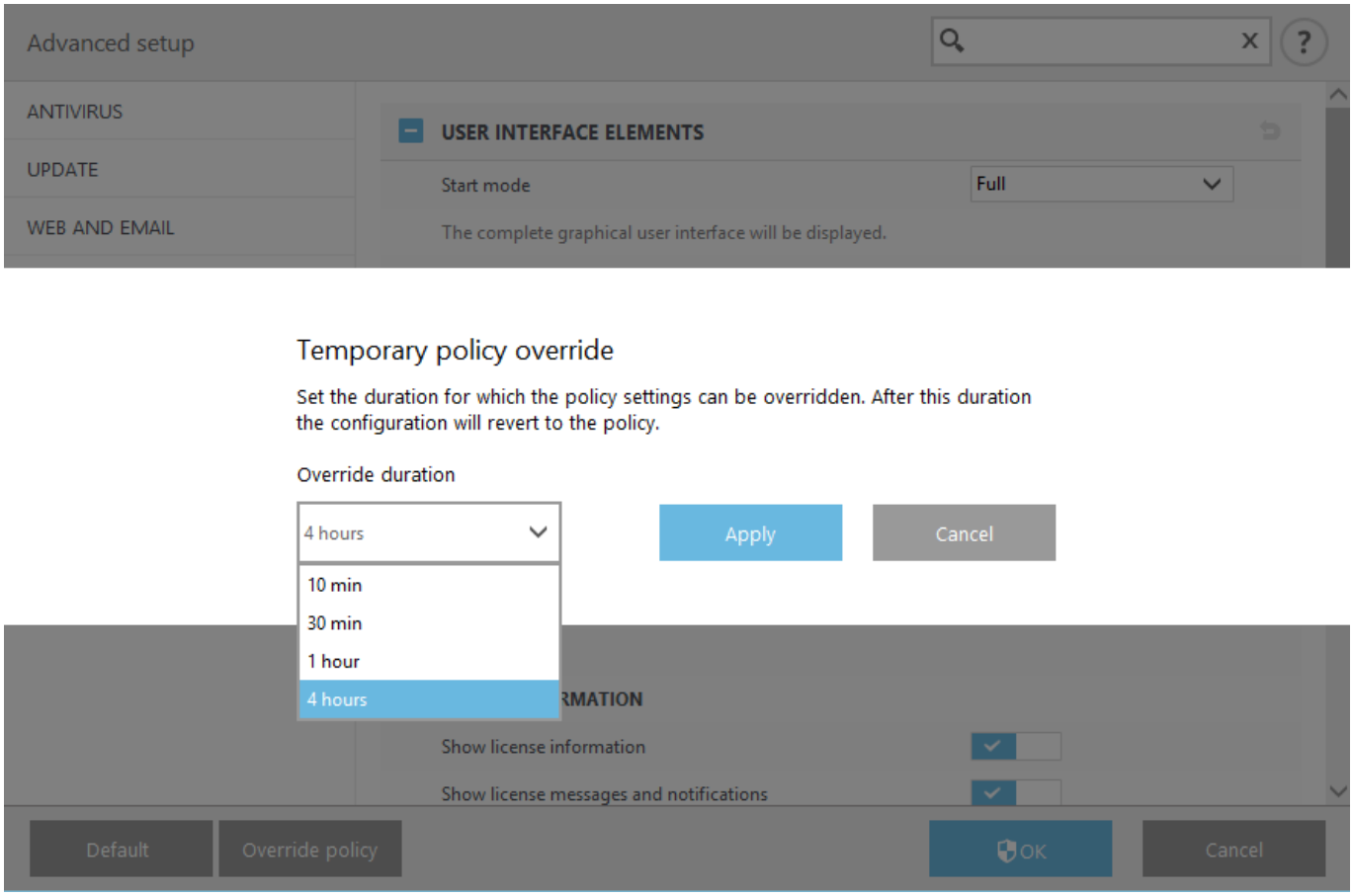
Обычно параметры, настроенные с помощью политики ESET PROTECT, изменить невозможно. Режим переопределения позволяет временно разблокировать эти параметры. Однако необходимо включить **режим переопределения** с использованием политики ESET PROTECT.

Войдите в веб-консоль ESET PROTECT , перейдите в раздел **Политики**, выберите и измените существующую политику, которая применяется к ESET Server Security, или создайте новую. В разделе **Параметры** щелкните **Режим переопределения**, включите его и настройте остальные его параметры, в том числе «Тип аутентификации» (Пользователь Active Directory или Пароль).

После изменения существующей или применения новой политики к ESET Server Security в окне Дополнительные настройки появится кнопка **Расширенные параметры**.

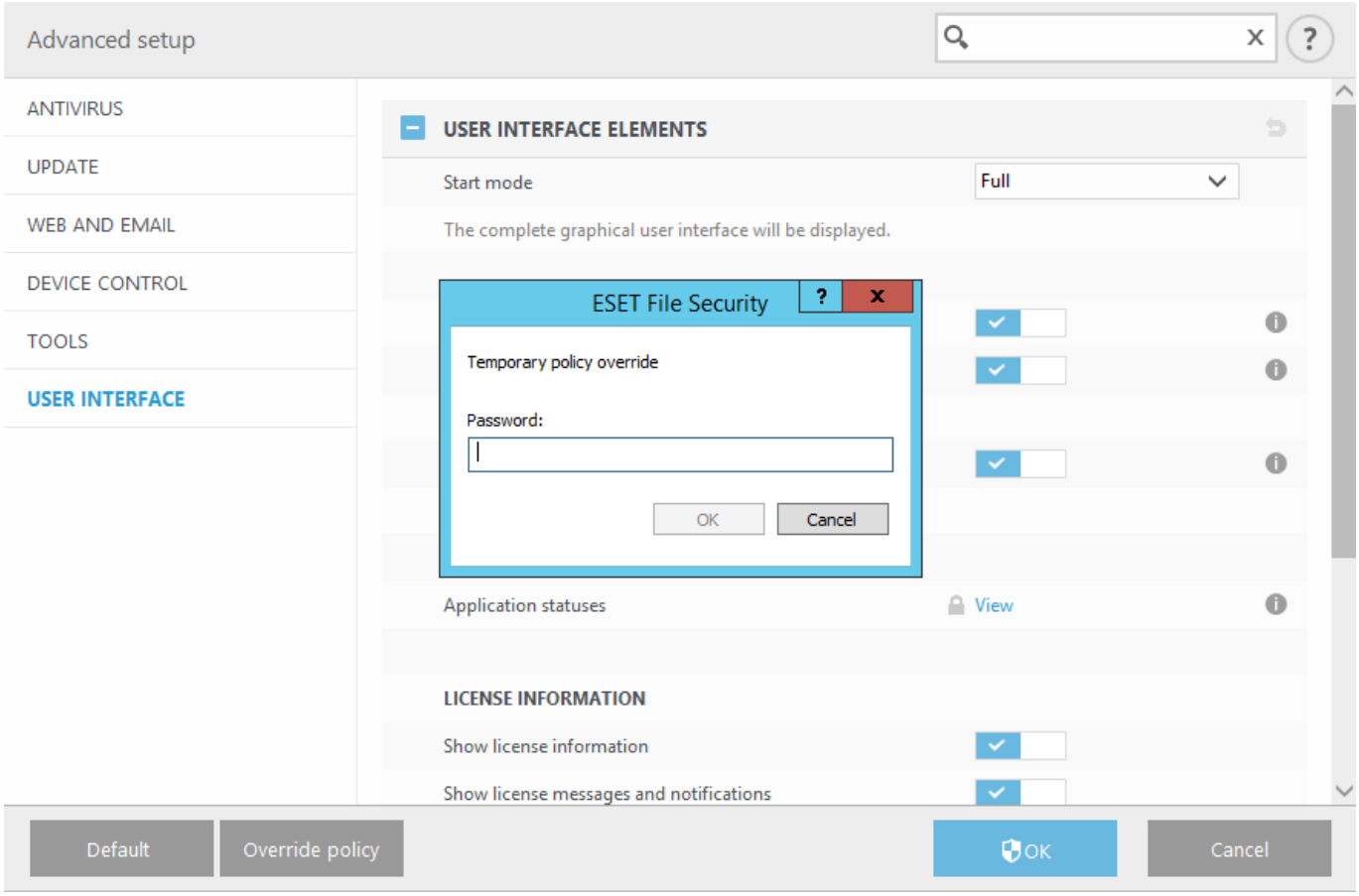


Нажмите кнопку **Переопределить политику**, задайте длительность и щелкните **Применить**.



Если в качестве типа аутентификации вы выбрали вариант **Пароль**, введите пароль для

переопределения политики.



По истечении срока действия режима переопределения настройки политики ESET PROTECT вернутся в исходное состояние, а выполненные вами изменения будут отменены. Перед окончанием действия режима переопределения отобразится соответствующее уведомление.

Завершить переопределение можно в любое время до окончания срока его действия. Это можно сделать на странице мониторинга или в окне Дополнительные настройки.

Файлы журнала

Этот раздел позволяет изменять конфигурацию ведения журналов программы ESET Server Security.

Фильтр ведения журнала

По умолчанию все параметры ведения журнала включены, поэтому производится значительный объем данных. Рекомендуется выборочно отключать ведение журнала для компонентов, которые не нужны или не связаны с проблемой.

> Чтобы запустить ведение журнала, необходимо включить ведение общего **ведения журнала диагностики** на уровне продукта, последовательно щелкнув в главном меню элементы **Настройка** > Сервис. Когда журнал будет включен, средство ESET Server Security начнет собирать подробные журналы в соответствии с тем, какие функции включены в этом разделе.

Используйте переключатели для включения или отключения определенной функции. Эти параметры также можно сочетать в зависимости от наличия отдельных компонентов в ESET Server Security.

• **Ведение журнала диагностики кластера** — ведение журнала кластера будет выполняться в рамках ведения общего журнала диагностики.

Файлы журнала

Определение способа управления журналами важно в основном для предотвращения чрезмерного использования диска. Настройки по умолчанию разрешают автоматическое удаление старых журналов для экономии дискового пространства.

Удалять записи автоматически

Записи в журнале старше указанного количества дней (ниже) будут удалены.

Удалять записи старше, чем (дн.)

Укажите количество дней.

Автоматически удалять старые записи, если превышен размер журнала

Если размер журнала превышает **максимальный размер журнала (МБ)**, удаление старых записей будет происходить до тех пор, пока не будет достигнут **уменьшенный размер журнала (МБ)**.

Создавать резервные копии автоматически удаленных записей

Резервные копии автоматически удаленных записей журнала будут создаваться в указанном каталоге и при необходимости сжиматься в ZIP-файлы.

Создавать резервные копии журналов диагностики

Будут создаваться резервные копии журналов диагностики, удаленных автоматически. Если этот параметр не включен, резервные копии записей журналов диагностики создаваться не будут.

Папка для резервных копий

Папка для хранения резервных копий журнала. Можно разрешить сжатие резервных копий журналов в ZIP-архивы.

Автоматически оптимизировать файлы журнала

Если выбрать этот параметр, файлы журнала будут автоматически дефрагментироваться при превышении значения, указанного в поле **Если количество неиспользуемых записей превышает (%)**. Чтобы начать дефрагментацию файлов журналов, щелкните элемент **Оптимизировать**. Все пустые записи журналов удаляются для улучшения производительности и скорости обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Включить текстовый протокол

Включение хранения журналов в формате, отличном от формата файлов журнала.

- **Целевой каталог** — каталог, в котором будут храниться файлы журналов (только для **текстового формата** и **формата CSV**). Каждый раздел журнала сохраняется в отдельный файл с предварительно заданным именем (например, если для хранения журналов используется текстовый формат файлов, раздел «Обнаруженные угрозы» файлов журнала сохраняется в файл *virlog.txt*).
- **Тип** — если выбрать формат файлов **Текст**, журналы будут сохраняться в текстовый файл, данные в котором будут разделены табуляцией. То же касается формата **CSV**. Если выбрать вариант **Событие**, файлы журнала будут храниться не в файле, а в журнале событий Windows (его можно просмотреть с помощью компонента «Просмотр событий» на панели управления).
- Команда **Удалить все файлы журнала** удаляет все сохраненные файлы, выбранные в раскрывающемся меню **Тип**.

> Для более быстрого решения проблем служба поддержки клиентов ESET иногда может запрашивать у пользователей журналы с их компьютеров. ESET Log Collector облегчает сбор необходимой информации. Дополнительные сведения о ESET Log Collector см. в нашей статье базы знаний.

Журнал аудита

Позволяет отслеживать изменения в конфигурации или защите. Поскольку изменение конфигурации продукта может существенно повлиять на его работу, может потребоваться отслеживание изменений в целях аудита. Записи журнала об изменениях можно посмотреть в разделе **Файлы журнала** > Журнал аудита.

Прокси-сервер

В больших локальных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. В этом случае необходимо задать описанные ниже параметры. Если не определить параметры, программа не сможет обновляться автоматически. В ESET Server Security настройку прокси-сервера можно выполнить в двух разных разделах окна **Дополнительные настройки** (**F5**).

1. **Расширенные параметры** (F5) > **Обновление** > **Профили** > **Обновления** > **Параметры подключения** > Прокси-сервер HTTP. Эта настройка применяется к конкретному профилю обновления и рекомендуется для ноутбуков, которые часто получают модули из разных мест.

2. **Дополнительные настройки** (F5) > **Служебные программы** > **Прокси-сервер**: настройка прокси-сервера на этом уровне позволяет глобально задать его параметры для программы ESET Server Security в целом. Они используются всеми модулями программы, которые подключаются к Интернету.

Для настройки параметров прокси-сервера на этом уровне используйте переключатель **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер**, а также укажите номер его **порта** в соответствующем поле.

На прокси-сервере требуется аутентификация

Если сетевая связь через прокси-сервер требует аутентификации, включите эту опцию и укажите **Имя пользователя** и **Пароль**.

Найти прокси-сервер

Нажмите кнопку **Найти**, чтобы автоматически определить параметры прокси-сервера и подставить их. Будут скопированы параметры, указанные в Internet Explorer.

> Эта функция не позволяет получить данные аутентификации (имя пользователя и пароль), пользователь должен указать их самостоятельно.

Использовать прямое подключение, если прокси-сервер недоступен

Если в программе настроено использование прокси-сервера HTTP, а он недоступен, программа будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

Уведомления

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Они отображаются в области уведомлений в правом нижнем углу экрана. Более подробные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив инструкции ниже.

Установите флажок **Не отображать уведомления при работе приложений в полноэкранном режиме**, чтобы запретить все неинтерактивные уведомления.

Показывать уведомление об успешном обновлении

После успешного обновления появится уведомление.

Отправлять уведомления о событиях по электронной почте

Включите, чтобы активировать уведомления по электронной почте.

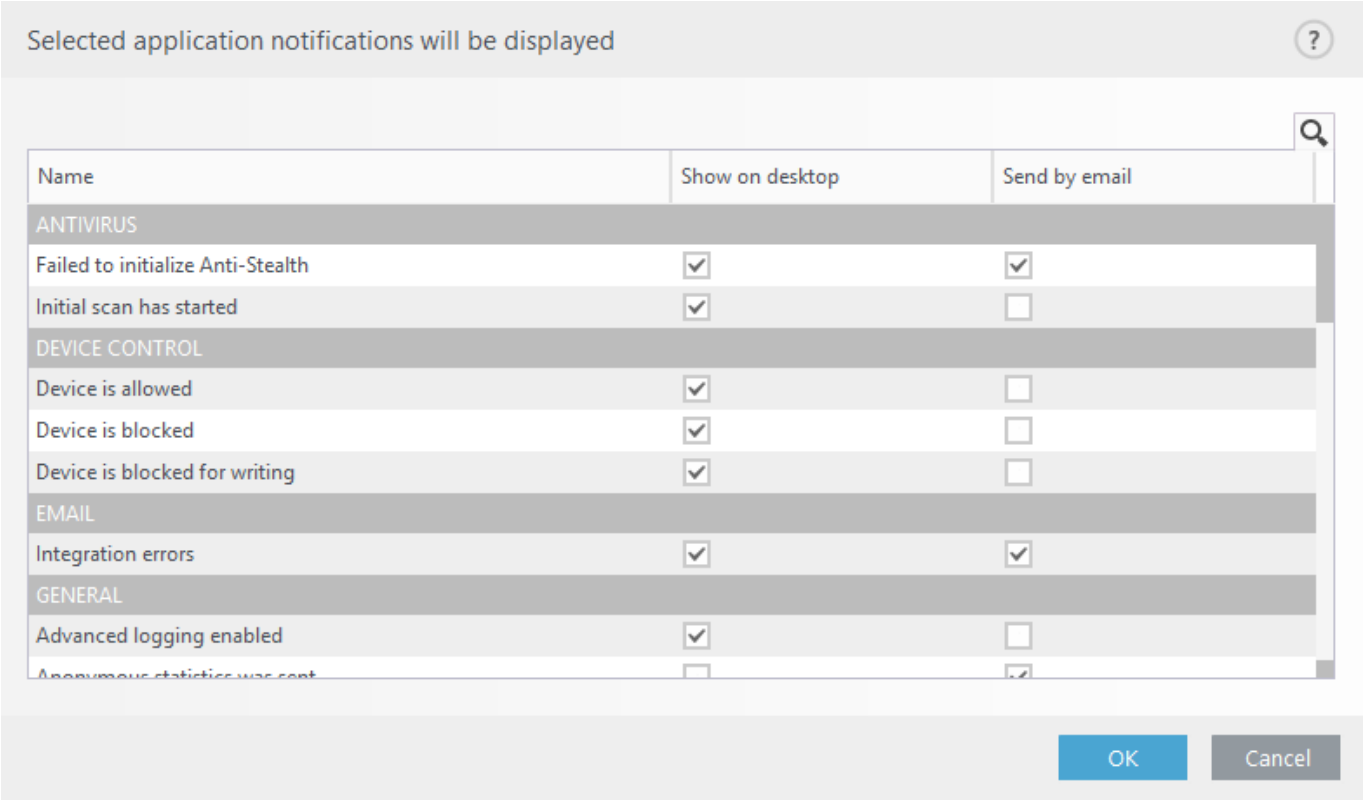
Уведомления приложения

Нажмите Изменить, чтобы включить или отключить показ уведомлений приложений.

Уведомления приложения

Вы можете настроить уведомления ESET Server Security, чтобы они отображались на рабочем столе и/или отправлялись на электронную почту.

> В случае уведомлений по электронной почте включите параметр **Отправлять уведомления о событиях по электронной почте** в разделе **Основное**, а затем при необходимости настройте SMTP-сервер и иные параметры.



Уведомления на рабочем столе

Для программы ESET Server Security можно настроить, как будут обрабатываться предупреждения об угрозах и системные уведомления (такие как сообщения об успешном обновлении). Например, можно настроить **длительность отображения** и **прозрачность** сообщений в области уведомлений Windows (применяется только к системам с поддержкой уведомлений).

В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать уровень серьезности предупреждений и уведомлений, которые следует отображать. Доступны указанные ниже варианты.

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.

- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.

- **Предупреждения** — в журнал вносится информация обо всех критических ошибках и предупреждениях.

- **Ошибки** — в журнал вносится информация об ошибках загрузки файлов и критических ошибках.

- **Критические ошибки** — в журнал вносятся только критические ошибки.

В поле **В многопользовательских системах** отображать уведомления для пользователя указывается пользователь, который будет получать системные и прочие уведомления, если одновременно может быть подключено несколько пользователей. Обычно это системный или сетевой администратор. Это особенно полезно для серверов терминалов (если все системные уведомления отправляются администратору).

Разрешить уведомлениям получать фокус экрана — уведомления будут получать фокус экрана, чтобы к ним можно было перейти с помощью сочетания Alt + Tab.

Уведомления по электронной почте

ESET Server Security поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации.

> ESET Server Security поддерживает SMTP-серверы, использующие шифрование TLS.

SMTP-сервер

Имя SMTP-сервера, используемого для отправки предупреждений и уведомлений. Как правило указывается имя сервера Microsoft Exchange Server.

Имя пользователя и пароль

Заполните эти поля, если требуется аутентификация на SMTP-сервере, для получения к нему доступа.

Адрес отправителя

Введите адрес отправителя, который будет отображаться в заголовке уведомлений, полученных по электронной почте. Это то, что увидит получатель в поле **От**.

Адрес получателя

Укажите адрес электронной почты получателя (Кому) для доставки уведомлений.

Включить шифрование TLS

Разрешить отправку предупреждений об угрозе и уведомлений с использованием протокола TLS.

Настройки электронной почты

Минимальная степень детализации уведомлений

Выбор минимальной степени детализации отправляемых уведомлений.

Интервал между отправками новых сообщений электронной почты (мин.)

Время в минутах, по истечении которого по электронной почте будут отправлены новые уведомления. Задайте для этого параметра значение 0, если нужно, чтобы уведомления отправлялись немедленно.

Отправлять уведомления в отдельных сообщениях электронной почты

Если этот параметр активирован, получатель будет получать каждое уведомление в отдельном сообщении. Это может привести к получению большого количества почты за короткий промежуток времени.

Формат сообщений

Обмен данными между программой и удаленным пользователем или системным администратором осуществляется посредством электронной почты или сообщений в локальной сети (используется служба сообщений Windows). Формат предупреждений и уведомлений, установленный по умолчанию, будет оптимален в большинстве случаев. В некоторых случаях может понадобиться изменить формат сообщений о событиях.

Формат сообщений о событиях

Формат сообщений о событиях, отображаемых на удаленных компьютерах.

Формат предупреждений об угрозах

Сообщения с предупреждениями и уведомлениями об угрозе имеют предварительно заданный формат по умолчанию. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

Ключевые слова (строки, разделенные символом %) в сообщении замещаются реальной информацией о событии. Доступны следующие ключевые слова.

- %TimeStamp% — дата и время события.
- %Scanner% — задействованный модуль.
- %ComputerName% — имя компьютера, на котором произошло предупреждение.
- %ProgramName% — программа, создавшая предупреждение.
- %InfectedObject% — имя зараженного файла, сообщения и т. п.

- %VirusName% — идентифицирующие данные заражения.
- %ErrorDescription% — описание события, не имеющего отношения к вирусам.

Ключевые слова **%InfectedObject%** и имя **%VirusName%** используются только в предупреждениях об угрозах, а описание **%ErrorDescription%** — только в сообщениях о событиях.

Кодировка

Кодировку можно выбрать в раскрывающемся меню. Сообщение электронной почты будет преобразовано в соответствии с выбранной кодировкой символов.

Использовать кодировку Quoted-printable

Сообщение будет преобразовано в формат Quoted Printable (QP), в котором используются символы ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате áéíóú).

Настройка

Этот текст отображается в нижней части всех выбранных оповещений.

Текст оповещения по умолчанию

Сообщение по умолчанию, которое будет отображаться в нижнем колонтитуле уведомления.

Угрозы

Не закрывать автоматически оповещения о вредоносных программах

Предоставляет уведомления о вредоносном ПО, которые остаются на экране, пока их не закрыть вручную.

Использовать текст по умолчанию

Сообщение по умолчанию можно отключить и указать пользовательское сообщение обработанного уведомления, которое будет отображаться при блокировке угрозы.

Текст оповещения об угрозе

Введите свое сообщение, которое следует отображать, когда блокируется угроза.

Режим презентации

Режим презентации — это функция для пользователей, которые стремятся избежать перерывов в работе программного обеспечения и появления отвлекающих всплывающих окон, а также желают свести к минимуму нагрузку на процессор. Его можно использовать также во время проведения презентаций, которые не должна прерывать деятельность модуля ESET Server Security. Если этот режим включен, появление окон уведомлений и выполнение запланированных задач блокируется. Защита системы по-прежнему работает в фоновом режиме, но не требует вмешательства со стороны пользователя.

Автоматически включать режим презентации при работе приложений в полноэкранном режиме

Когда запускается полноэкранное приложение, режим презентации активируется автоматически. При включенном режиме презентации невозможно увидеть уведомления или изменение состояния ESET Server Security.

Автоматически отключать режим презентации через

Для указания времени в минутах, по истечении которого режим презентации будет автоматически отключен.

Диагностика

Средство диагностики собирает аварийные дампы процессов ESET (например, *ekrn*). Если происходит аварийное завершение работы приложения, создается соответствующий дамп. С помощью таких дампов разработчики могут отлаживать и исправлять различные проблемы программы ESET Server Security.

Откройте раскрывающееся меню рядом с элементом **Тип дампа** и выберите один из трех доступных вариантов.

- **Отключить** — отключает эту функцию.
- **Мини** — (по умолчанию) регистрируется наименьший объем полезной информации, которая может помочь выявить причину неожиданного сбоя приложения. Этот тип файла дампа удобно использовать, если место на диске ограничено. Однако ограниченный объем включенной в него информации может не позволить при анализе такого файла обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.
- **Полный** — регистрируется все содержимое системной памяти на момент неожиданного прекращения работы программы. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

Целевой каталог

Каталог, в котором будут создаваться аварийные дампы.

Открыть папку диагностики

Нажмите кнопку '**Открыть**', чтобы открыть каталог в новом окне *Windows Explorer*.

Создать дамп диагностики

Щелкните элемент **Создать**, чтобы создать файлы дампа диагностики в целевом каталоге.

Расширенное ведение журналов

Включить расширенное ведение журналов для модуля сканирования компьютера
Запись всех событий, которые происходят при сканировании файлов и папок функцией сканирования компьютера или защиты файловой системы в реальном времени.
Включение расширенного ведения журнала контроля устройств
Запись всех событий, которые происходят в модуле "Контроль устройств", для диагностики и устранения проблем.
Включить расширенное ведение журнала Direct Cloud
Запись всех сообщений, которыми обмениваются продукт и серверы Direct Cloud.
Включить расширенное ведение журнала защиты документов
Запись всех событий, которые происходят в модуле защиты документов, для диагностики и устранения проблем.
Включить расширенное ведение журналов
Записывать все события, происходящие в службе ядра ESET (ekrn), для обеспечения возможности проведения диагностики и устранения проблем.
Включить расширенное ведение журнала для лицензирования
Записывать весь обмен данными между программой и сервером лицензий.
Включить трассировку памяти
Записывать все события, которые помогут разработчикам выявлять утечки памяти.
Включить расширенное ведение журналов для защиты сети
Запись всех сетевых данных, проходящих через защиту сети в формате PCAP. Это помогает разработчикам диагностировать и устранять проблемы с защитой сети.
Включение ведения журнала операционной системы
Будут собираться дополнительные сведения об операционной системе, например о запущенных процессах, активности ЦП и работе дисков. Они помогут разработчикам диагностировать и устранить проблемы с программами ESET в вашей ОС.
Включить расширенное ведение журнала фильтрации протоколов
Запись всех данных, проходящих через модуль фильтрации протоколов в формате PCAP. Это помогает разработчикам диагностировать и устранять проблемы с фильтрацией протоколов.
Включить расширенное ведение журналов для обмена push-сообщениями
Запись всех событий, происходящих во время обмена push-сообщениями, для обеспечения диагностики и устранения проблем.
Включение расширенного ведения журналов для защиты файловой системы в реальном времени
Запись всех событий, которые происходят при работе защиты файловой системы в реальном времени, для диагностики и устранения проблем.
Включить расширенное ведение журнала для модуля обновления
Записывать все события, которые происходили во время обновления. Это поможет разработчикам выявлять и исправлять проблемы, связанные с модулем обновления.
Расположение файлов журнала
C:\ProgramData\ESET\ESET Security\Diagnostics

Техническая поддержка

Отправить данные о конфигурации системы

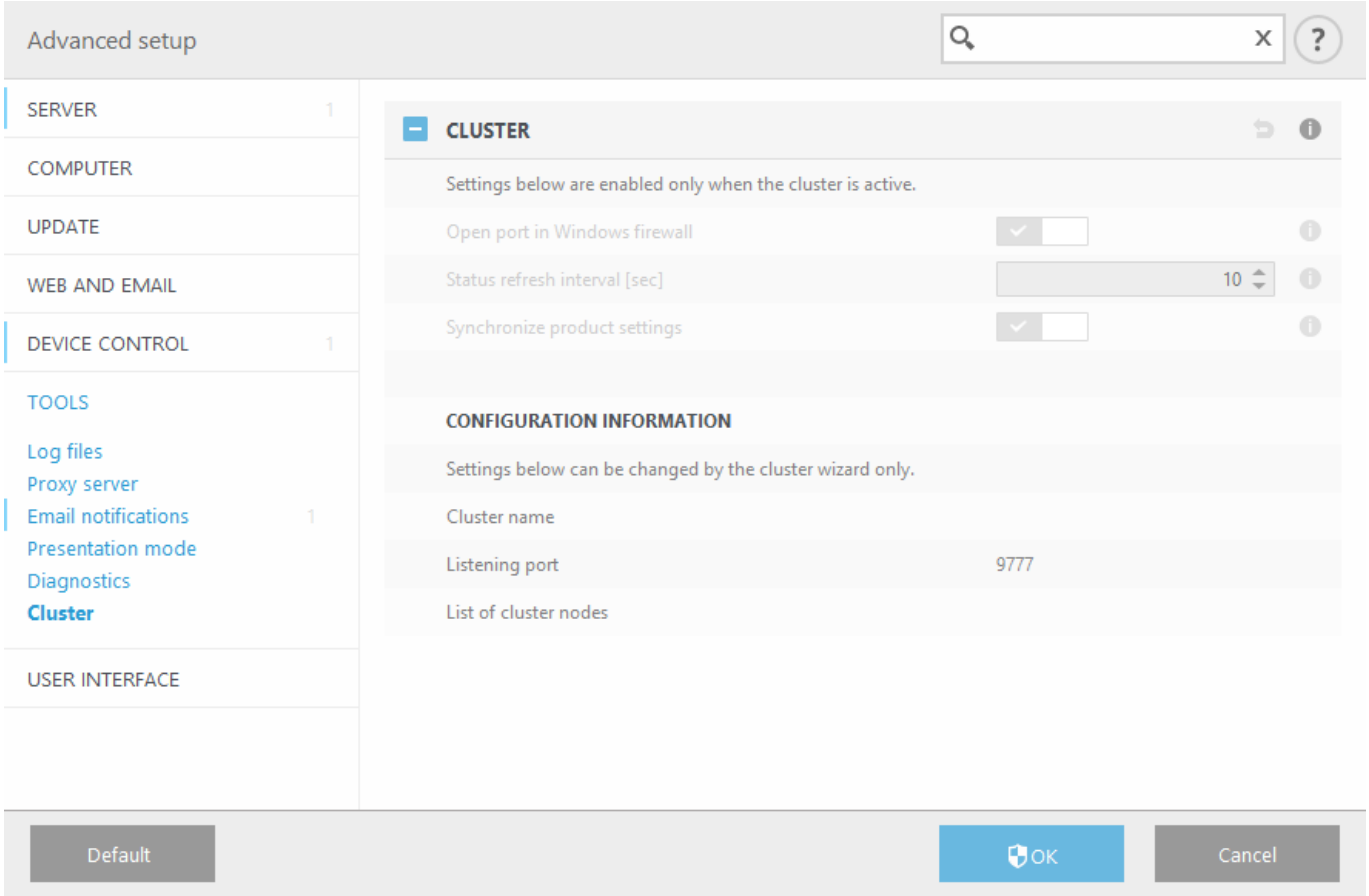
Чтобы перед отправкой данных конфигурации ESET Server Security в службу поддержки клиентов не получать или получать запрос, в раскрывающемся меню выберите элемент **Отправлять всегда** или **Запрашивать подтверждение перед отправкой**.

Кластер

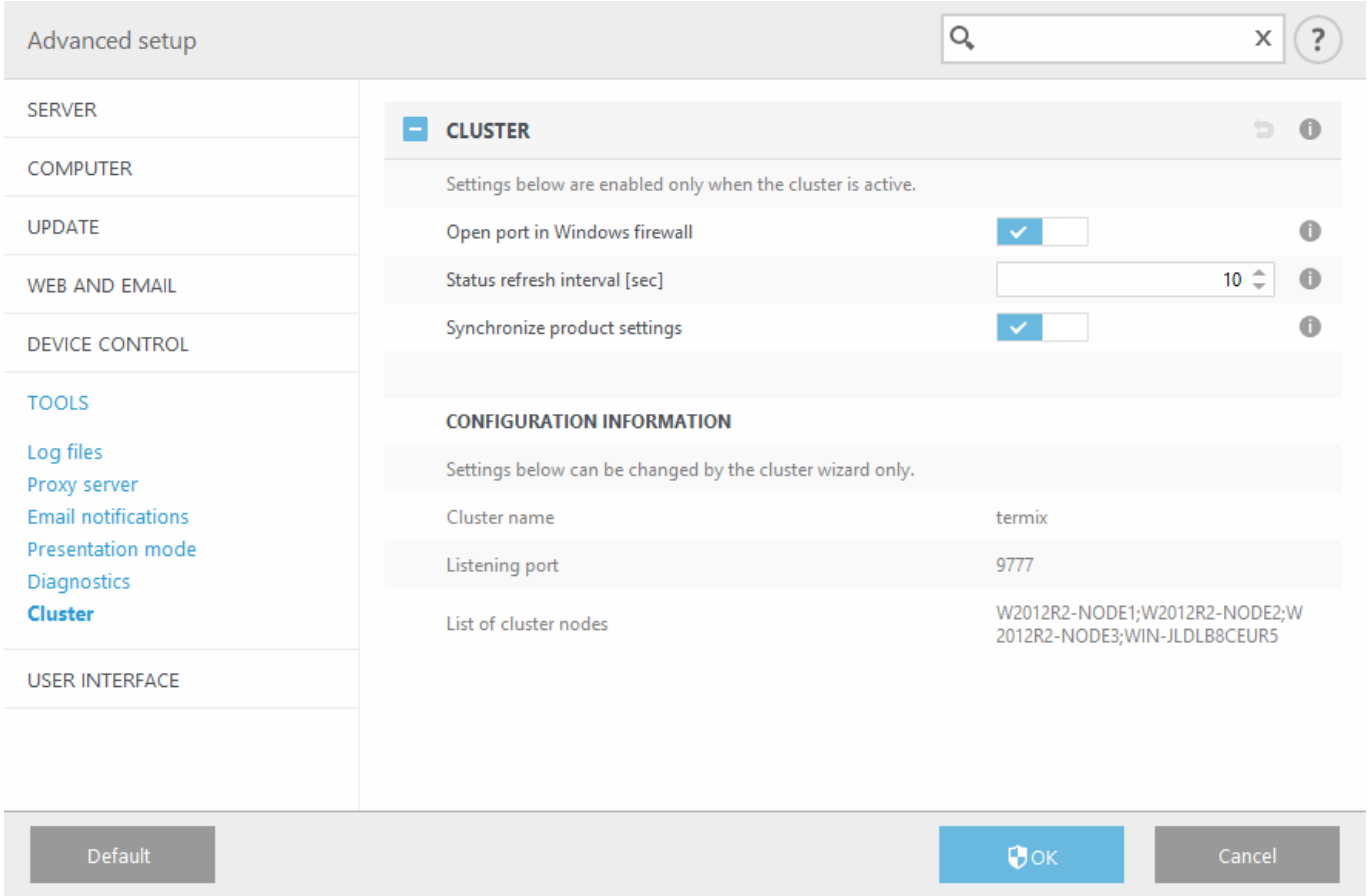
Если кластер ESET настроен, параметр «Включить кластер» включается автоматически. Его можно отключить вручную с помощью переключателя в окне **Дополнительные настройки**

или нажав клавишу F5 (это можно сделать, если необходимо изменить конфигурацию, не затрагивая другие узлы в кластере ESET). Данный переключатель только включает или отключает функцию кластера ESET. Чтобы настроить или уничтожить кластер, используйте мастер кластеров или команду **Уничтожить кластер** в разделе Сервис > Кластер главного окна программы.

Кластер ESET не настроен и выключен.



Сведения и параметры кластера ESET настроены правильно.



Интерфейс пользователя

Настройте поведение графического интерфейса программы ESET Server Security. Здесь можно изменить внешний вид программы и используемые эффекты.

Элементы интерфейса

В раскрывающемся меню «Режим запуска графического интерфейса пользователя» выберите один из следующих режимов запуска графического интерфейса пользователя (GUI).
• **Полный** — графический интерфейс будет отображаться полностью.
• **Терминал** — уведомления и предупреждения не отображаются. Графический интерфейс пользователя может быть запущен только администратором. Если графические элементы снижают производительность компьютера или вызывают другие проблемы, для интерфейса пользователя необходимо задать значение Терминал. Кроме того, на сервере терминалов рекомендуется отключить графический интерфейс пользователя. Дополнительные сведения о программе ESET Server Security, установленной на сервере терминалов, см. в разделе Отключение графического интерфейса пользователя на сервере терминалов.

Показывать заставку при запуске
Отключите эту опцию, если вы предпочитаете не показывать всплывающий экран при запуске GUI ESET Server Security, например, при входе в систему.

Использовать звуки
ESET Server Security воспроизводит звук, когда происходят важные события во время сканирования, например, когда обнаружена угроза или когда сканирование завершено.

Интеграция в контекстное меню
Когда включен этот режим, элементы управления ESET Server Security интегрированы в контекстное меню. Если щелкнуть объект (файл) правой кнопкой мыши, отобразится контекстное меню. В меню указаны все действия, которые можно выполнить с объектом.

Состояния приложения
Нажмите кнопку Изменить, чтобы выбрать состояния (включать их или отключать), отображаемые в окне Отслеживание. Вместо него для настройки состояний приложений можно использовать политики ESET PROTECT. Даже если ваш продукт не активирован или срок действия вашей лицензии истек, его состояние приложения также будет отображаться.

Сведения о лицензии / Показать сведения о лицензии
Когда включен этот параметр, отображаются сообщения и уведомления, касающиеся лицензии.

Окна предупреждений и сообщений

Путем настройки параметров в разделе «Предупреждения и уведомления» можно изменить поведение системных уведомлений и предупреждений об обнаруженных угрозах. Их можно настроить в соответствии со своими потребностями. Если вы отключили отображение некоторых уведомлений, они будут присутствовать в области Отключенные сообщения и состояния. Здесь можно проверить их состояние, просмотреть дополнительные сведения или удалить их из данного окна.

Настройка доступа

Для обеспечения высокого уровня безопасности можно предотвратить несанкционированные изменения с помощью средства «Настройка доступа».

ESET Shell

Настроить права доступа к параметрам, функциям и данным программы через eShell можно путем изменения политики выполнения оболочки ESET.

Значок в области уведомлений Windows

Восстановление всех параметров в разделе

Окна предупреждений и сообщений

Для программы ESET Server Security можно настроить, как будут обрабатываться предупреждения об угрозах и системные уведомления (такие как сообщения об успешном обновлении). Например, можно настроить **длительность отображения** и **прозрачность** сообщений в области уведомлений Windows (применяется только к системам с поддержкой уведомлений).

Отображать интерактивные предупреждения

Отключите эту функцию, если хотите, чтобы программа ESET Server Security не отображала предупреждения в области уведомлений Windows.

Список интерактивных предупреждений

Полезно для автоматизации. Снимите флажок **Спросить пользователя** для элементов, которые нужно автоматизировать, и выберите, какое действие будет выполнено вместо появления окна предупреждения, ожидающего отклика пользователя.

Окна сообщений предназначены для отображения коротких текстовых сообщений или вопросов.

Автоматически закрывать окна сообщений

Автоматическое закрытие окон уведомлений по истечении определенного времени. Если окно предупреждения не будет закрыто вручную, оно закрывается автоматически через указанный промежуток времени.

Подтверждения

При нажатии кнопки **Изменить** откроется всплывающее окно со списком подтверждающих сообщений, которые отображает ESET Server Security перед выполнением действия. Установите флажки, чтобы задать свои настройки для подтверждающих сообщений.

Настройка доступа

Для максимальной безопасности системы важно правильно настроить ESET Server Security. Любые неквалифицированные изменения могут привести к проблемам или даже к потере важных данных. Чтобы избежать неквалифицированных изменений, можно защитить конфигурацию ESET Server Security с помощью пароля.

> Если вы удаляете ESET Server Security при использовании защиты доступа с помощью пароля, вам будет предложено ввести пароль. В противном случае вы не сможете удалить ESET Server Security.

Защитить параметры паролем

Блокирует параметры настройки программы или снимает их блокировку. Щелкните этот элемент, чтобы открыть окно **Настройка пароля**.

Установить пароль

Чтобы установить или изменить пароль для защиты параметров настройки, нажмите **Установить**. Для защиты параметров установки ESET Server Security от несанкционированного вмешательства необходимо установить новый пароль. Для смены пароля введите старый пароль в поле **Старый пароль**, а новый пароль — в поля **Новый пароль** и **Подтвердите пароль** и затем нажмите кнопку **OK**. Этот пароль будет необходим для внесения в будущем любых изменений в ESET Server Security.

Для учетных записей администратора с ограниченными правами необходим полный набор прав администратора

Выберите этот параметр, чтобы предлагать текущему пользователю (который не имеет прав администратора) вводить учетные данные учетной записи администратора при изменении определенных параметров, например при отключении модулей защиты.

> Если пароль настройки доступа изменится и потребуется импортировать существующий файл конфигурации в формате XML (подписанный до изменения пароля) с помощью командной строки ESET CMD, не забудьте подписать его заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другом компьютере с работающей программой ESET Server Security перед импортом.

ESET Shell

Настроить права доступа к параметрам, функциям и данным продукта через eShell можно путем изменения параметра **Политика выполнения оболочки ESET**. По умолчанию задано значение **Ограниченные сценарии**, но вместо него можно задать значение «Отключено», «Только чтение» или «Полный доступ».

Отключено

eShell не может использоваться вообще. Разрешена только конфигурация самого решения eShell в контексте ui eshell. Вы можете настроить внешний вид eShell, но не можете получить доступ к настройкам или данным продукта.

Только для чтения

Решение eShell можно использовать как инструмент мониторинга. Как в интерактивном, так и в пакетном режиме все параметры можно просматривать, однако изменять параметры, свойства и данные нельзя.

Ограниченные сценарии

В интерактивном режиме можно изменять все параметры, свойства и данные. В пакетном режиме решение eShell функционирует так, как если бы был включен режим «Только чтение». Однако если используются подписанные пакетные файлы, то можно настраивать параметры и изменять данные.

Полный доступ

Неограниченный доступ ко всем параметрам как в интерактивном, так и в пакетном режиме (при выполнении пакетных файлов). Все параметры доступны для просмотра и изменения. Для

запуска eShell с полным доступом используйте учетную запись администратора. Если включен контроль учетных записей, требуется также повышение прав.

Отключение графического интерфейса пользователя на сервере терминалов

В этой главе описывается, как отключать графический интерфейс пользователя программы ESET Server Security, запущенной на сервере терминалов Windows для работы с сеансами пользователя.

Обычно графический интерфейс пользователя ESET Server Security запускается при каждом входе удаленного пользователя на сервер и создании сеанса терминала. Обычно это нежелательно на серверах терминалов. Если нужно отключить графический интерфейс пользователя в сеансах терминала, сделать это можно с помощью eShell, выполнив команду `set ui ui gui-start-mode none`. Вот два доступных режима для запуска графического интерфейса пользователя:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Если нужно узнать, какой режим сейчас используется, выполните команду `get ui ui gui-start-mode`.

> Если вы установили ESET Server Security на сервер Citrix, рекомендуется использовать параметры, описанные в нашей статье базы знаний.

Отключенные сообщения и состояния

Подтверждения

Показывает список подтверждений, отображение которых можно включить или выключить.

Параметры состояний приложения

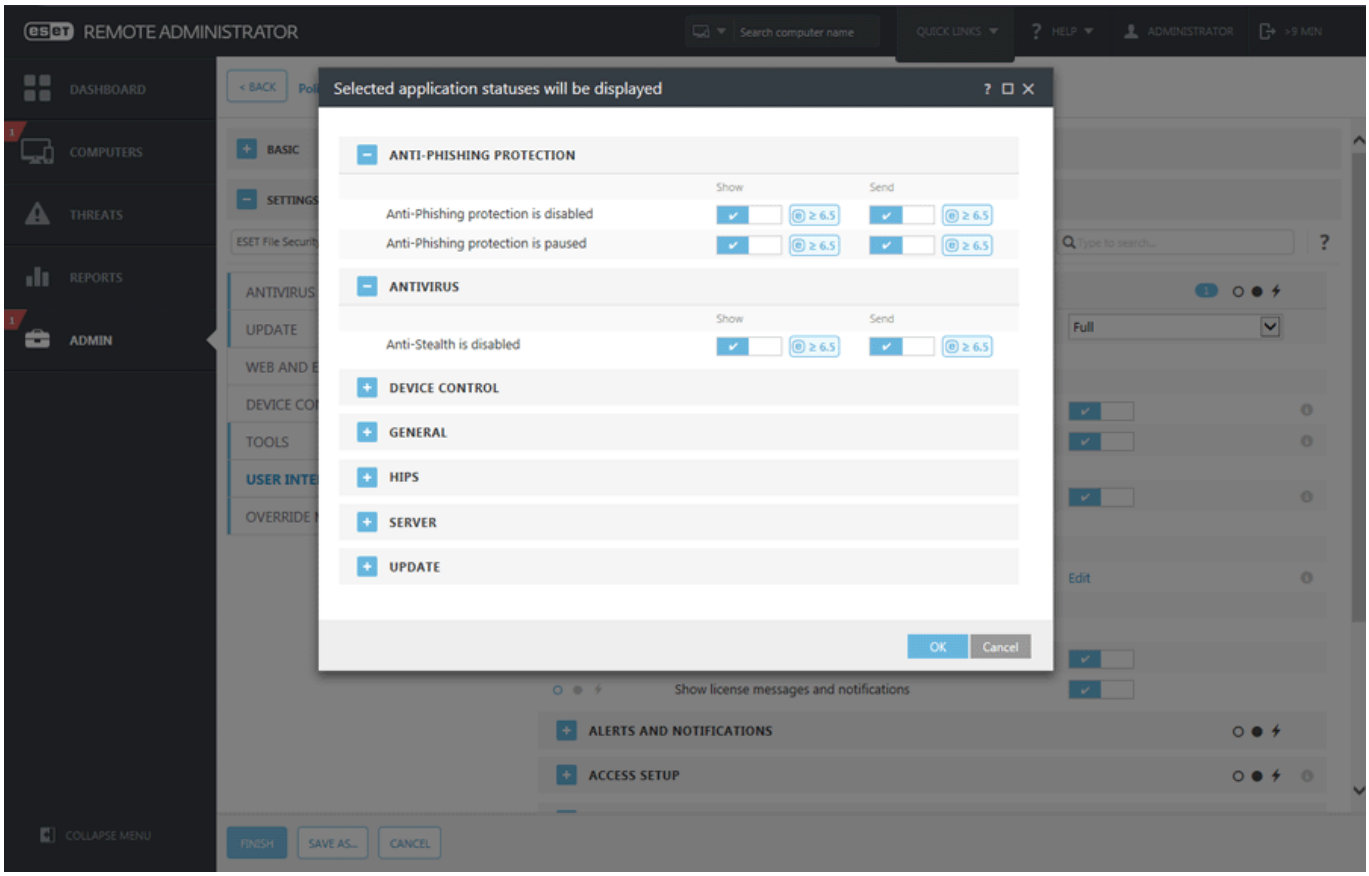
Предоставляется возможность включения и отключения отображения состояний в главном меню на странице Мониторинг.

Параметры состояний приложения

В этом диалоговом окне можно выбрать, какие состояния приложения нужно отображать, а какие — нет. Например, временное отключение защиты от вирусов и шпионских программ приведет к изменению состояния защиты, которое отображается на странице Мониторинг. Кроме того, состояние приложения отображается, если продукт не активирован или срок действия лицензии истек.

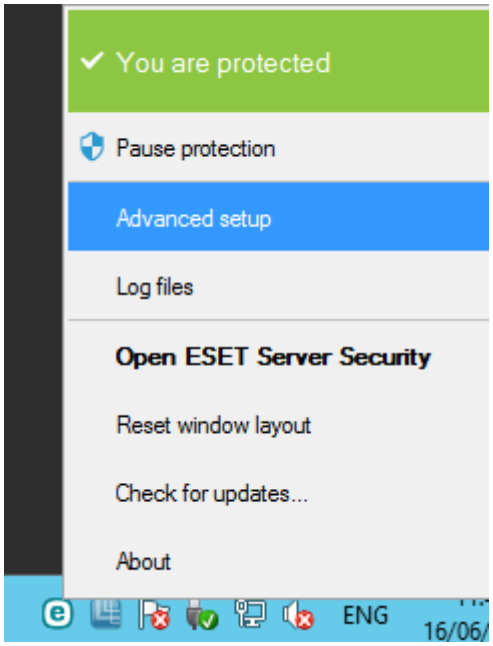
Состояниями приложения можно управлять при помощи политик ESET PROTECT. Для категорий и состояний в списке отображаются два параметра — **Показать** и **Отправить** состояние.

Столбец «Отправить» отображается для состояний приложения только в конфигурации политики ESET PROTECT. В программе ESET Server Security параметры отображаются со значком блокировки. Можно использовать режим переопределения, чтобы на некоторое время изменять состояния приложения.



Значок в области уведомлений Windows

Используется для быстрого доступа к часто используемым элементам и функциям ESET Server Security. Для этого следует щелкнуть правой кнопкой мыши значок в области уведомлений Windows.



Дополнительные сведения

Открывает страницу Мониторинг для отображения текущего состояния защиты и сообщений.

Приостановка защиты

На экран выводится диалоговое окно подтверждения. В нем можно отключить защиту от вирусов и шпионских программ, которая предотвращает атаки на компьютер, контролируя обмен файлами и данными через Интернет и электронную почту. Если щелкнуть значок в области уведомлений Windows, чтобы временно приостановить защиту от вирусов и шпионских программ, отобразится диалоговое окно **Приостановка защиты**. В этом окне можно приостановить защиту от вредоносных программ на определенный период времени. Чтобы отключить защиту насовсем, используйте раздел **Расширенные параметры**. Будьте осторожны: отключение защиты сделает систему уязвимой для угроз.

Дополнительные настройки

С помощью этого параметра можно ввести **дополнительные настройки**.

Файлы журнала

Содержат информацию обо всех важных событиях программы и предоставляют общие сведения об обнаруженных угрозах.

Скрыть ESET Server Security

Позволяет скрыть окно ESET Server Security.

Восстановить расположение окон

Восстанавливает размер окна ESET Server Security и его положение на экране по умолчанию.

Проверить наличие обновлений

Запускает обновления модулей для поддержания необходимого уровня защиты от вредоносного кода.

О программе

Отображает системную информацию, сведения об установленной версии ESET Server Security и модулях программы, а также срок действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

Восстановление параметров по умолчанию

Можно восстановить настройки до значений по умолчанию в разделе **Дополнительные настройки**. Есть два параметра. Можно вернуть все по умолчанию или вернуть настройки только для определенного раздела (параметры в других разделах останутся неизменными).

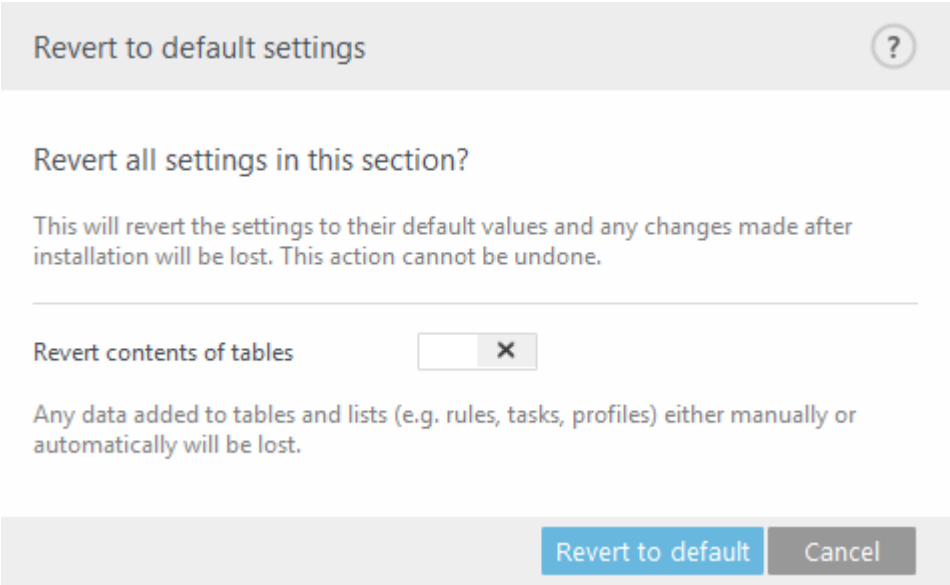
Восстановление всех параметров

Все параметры во всех разделах расширенной настройки будут восстановлены до состояния, которое было после установки ESET Server Security. Это то же самое, что Восстановить заводские настройки.

> После нажатия **Восстановить параметры по умолчанию**, все внесенные изменения будут потеряны. Это действие необратимое.

Восстановление всех параметров в разделе

Возвращает параметры модуля в выбранном разделе к предыдущим значениям. Любые изменения, внесенные в этом разделе, будут потеряны.



Восстановить содержимое таблиц

При активации этой функции правила, задачи и профили, добавленные автоматически или вручную, будут удалены.

Справка и поддержка

В ESET Server Security есть средства для устранения проблем и информация по поддержке, которые помогут решить возможные проблемы.

Установленный продукт

Информация о продукте и лицензии

- О программе ESET Server Security: на экран выводится информация о вашей копии программы ESET Server Security.

- Устранение проблем с продуктом — Выберите эту функцию, чтобы найти решения часто встречающихся проблем. Рекомендуется ознакомиться с этим разделом, прежде чем обращаться в службу технической поддержки.

- Устранение проблем с лицензией — поиск решений для проблем с активацией или изменением лицензии.

- Изменить лицензию — щелкните, чтобы открыть окно активации и активировать продукт.

Страницы справочной системы

Запускает страницы справочной системы для ESET Server Security.

База знаний

Поиск в базе знаний ESET: в базе знаний ESET содержатся ответы на наиболее часто задаваемые вопросы, а также рекомендуемые решения различных проблем. База знаний регулярно обновляется техническими специалистами ESET, что делает ее самым полезным инструментом для решения проблем.

Техническая поддержка

- Расширенное ведение журналов — Создавайте расширенные журналы для всех доступных функций, чтобы помочь разработчикам диагностировать и решать проблемы.

- Запрос в службу поддержки — если не удается найти ответ на вопрос, обратитесь в нашу службу технической поддержки.

- Информация для службы технической поддержки — Позволяет просмотреть подробные сведения (название продукта, версия продукта и т. д.) для службы технической поддержки.

- ESET Log Collector — Это приложение (ESET Log Collector), которое автоматически собирает с сервера данные (например, конфигурацию и журналы) для ускорения решения проблем.

Отправка запроса в службу поддержки клиентов

Чтобы оказать помощь максимально быстро и эффективно, компании ESET требуется информация о конфигурации программы ESET Server Security, подробные сведения о системе пользователя и выполняющихся процессах (файл журнала ESET SysInspector), а также данные реестра. Компания ESET использует эту информацию только для предоставления клиенту технической поддержки. Этот параметр также можно настроить в окне **Расширенные параметры** (F5) > **Сервис** > **Диагностика** > **Служба поддержки**.

> Если вы решили отправить данные о системе, нужно заполнить и отправить веб-форму. Иначе запрос не будет создан и данные о системе будут потеряны.

При отправке веб-формы будут отправлены и данные о конфигурации системы. Установите флажок **Всегда отправлять эти сведения**, чтобы запомнить это действие для данного процесса.

Не отправлять данные

Используйте этот параметр, если не нужно отправлять данные. Вы будете перенаправлены на веб-страницу технической поддержки ESET.

О программе ESET Server Security

В этом окне содержатся сведения об установленной версии ESET Server Security. В верхней части окна содержится информация об операционной системе и системных ресурсах, а также о текущем пользователе и полном имени компьютера.

Установленные компоненты

Содержит информацию о модулях для просмотра списка установленных компонентов и сведений о них. Чтобы скопировать список в буфер обмена, нажмите **Копировать**. Это может понадобиться при устранении неполадок или при обращении в службу технической поддержки.

Глоссарий

Посетите страницу Глоссарий, чтобы получить дополнительные сведения о технических терминах, угрозах и безопасности в Интернете.

Лицензионное соглашение с конечным пользователем

Вступает в силу с 19 октября 2021 года.

ВАЖНО! Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С ПОЛИТИКОЙ КОНФИДЕНЦИАЛЬНОСТИ.**

Лицезионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем («Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 85101 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (ESET или Поставщик) и вами, физическим или юридическим лицом (Вы или Конечный пользователь), Вы получаете право использовать Программное обеспечение, указанное в статье 1 настоящего Соглашения. Программное обеспечение, указанное в статье 1 настоящего Соглашения, может храниться на носителях данных, отправляться по электронной почте, загружаться через Интернет, загружаться с серверов Поставщика или получаться из других источников, которые удовлетворяют перечисленным ниже условиям.

ЭТО СОГЛАШЕНИЕ КАСАЕТСЯ ПРАВ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И НЕ ЯВЛЯЕТСЯ ДОГОВОРОМ ПРОДАЖИ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Конечный пользователь имеет право в соответствии с настоящим Соглашением.

Выбор варианта «Принимаю» в процессе установки, загрузки, копирования или использования этого Программного обеспечения выражает Ваше согласие с условиями настоящего Соглашения и Политики конфиденциальности. Если Вы не согласны с каким-либо из условий настоящего Соглашения или Политики конфиденциальности, немедленно выберите вариант отмены, отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате Поставщику или в организацию, в которой было приобретено Программное обеспечение.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ДАННОЕ СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ СЧИТАТЬ ИХ ОБЯЗЫВАЮЩИМИ.

1. **Программное обеспечение.** Термин "Программное обеспечение" в настоящем Соглашении означает: (i) компьютерную программу, которая сопровождается настоящим Соглашением, и все ее компоненты; (ii) все содержимое на дисках, компакт-дисках, DVD-дисках, в электронных сообщениях и каких-либо вложениях или на других носителях, которые были поставлены вместе с настоящим Соглашением, в том числе форму объектного кода Программного обеспечения, поставляемую на носителе данных, по электронной почте или загружаемую через Интернет; (iii) любые пояснительные материалы или любую другую возможную документацию, связанную с Программным обеспечением, главным образом какое-либо описание Программного обеспечения, его спецификации, какое-либо описание свойств или работы Программного обеспечения, какое-либо описание рабочей среды, в которой используется Программное обеспечение, инструкции по использованию или установке Программного обеспечения или какое-либо описание использования Программного обеспечения (Документация); (iv) копии Программного обеспечения, пакеты исправления возможных ошибок Программного обеспечения, дополнения к Программному обеспечению, расширения Программного обеспечения, измененные версии Программного обеспечения и обновления компонентов Программного обеспечения (при наличии), на которые Поставщик

предоставил Вам лицензию в соответствии со статьей 3 настоящего Соглашения. Программное обеспечение предоставляется исключительно в форме исполняемого объектного кода.

2. **Установка, компьютер и лицензионный ключ**. Программное обеспечение, поставляемое на носителе данных, по электронной почте, загруженное через Интернет или с серверов Поставщика или полученное из других источников, подлежит установке. Установка Программного обеспечения должна происходить на должным образом настроенном компьютере, который отвечает минимальным требованиям, изложенным в Документации. Способ установки описан в Документации. Компьютер, на котором выполняется установка, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на работу Программного обеспечения. Компьютер означает оборудование, в том числе, среди прочего, персональные компьютеры, ноутбуки, рабочие станции, карманные компьютеры, смартфоны, карманные или другие электронные устройства, для которых разрабатывается Программное обеспечение, на котором его будут устанавливать и/или использовать. Лицензионный ключ означает уникальную последовательность символов, букв, цифр или специальных знаков, предоставляемых конечному пользователю, чтобы разрешить законно использовать Программное обеспечение или его определенную версию либо продлить срок действия Лицензии в соответствии с настоящим Соглашением.

3. **Лицензия**. Если Вы приняли все условия, предусмотренные в настоящем Соглашении, и соблюдаете их, Поставщик предоставляет Вам следующие права (Лицензия).

a) **Установка и использование.** Вы получаете неисключительное не подлежащее передаче право установить Программное обеспечение на жесткий диск компьютера или иной носитель для хранения данных, установки и хранения Программного обеспечения в памяти компьютера, а также внедрить, хранить и отображать Программное обеспечение.

b) **Оговорка по количеству лицензий.** Право на использование Программного обеспечения ограничено определенным количеством Конечных пользователей. Под одним Конечным пользователем подразумевается (i) установка Программного обеспечения на один компьютер или (ii) в случае ограничения лицензии количеством почтовых ящиков пользователь компьютера, который принимает электронную почту через пользовательский почтовый агент («Пользовательский почтовый агент»). Если Пользовательский почтовый агент принимает электронную почту, а затем автоматически распределяет ее среди нескольких пользователей, количество Конечных пользователей должно определяться в соответствии с фактическим количеством пользователей, получающих электронную почту. Если почтовый сервер выполняет функции почтового шлюза, количество Конечных пользователей будет равняться количеству пользователей почтового сервера, которых обслуживает этот шлюз. Если один пользователь владеет несколькими адресами электронной почты (например, при использовании псевдонимов) и принимает почту по ним, а почта не распределяется автоматически клиентом другим пользователям, необходима Лицензия только для одного компьютера. Одну Лицензию нельзя использовать одновременно на нескольких компьютерах. Конечный пользователь имеет право вводить Лицензионный ключ в Программное обеспечение только в той степени, в которой Конечный пользователь имеет право использовать Программное обеспечение в соответствии с ограничением по количеству Лицензий, выданных Поставщиком. Лицензионный ключ считается конфиденциальной информацией. Вы не должны передавать Лицензию третьим сторонам или разрешать третьим сторонам использовать Лицензионный ключ, если это не разрешено настоящим Соглашением или Поставщиком. Если Ваш Лицензионный ключ взломан, немедленно сообщите об этом Поставщику.

c) **Выпуск для дома или для бизнеса.** Версия Программного обеспечения для дома должна использоваться исключительно в личной и/или некоммерческой средах и предназначена

только для домашнего и семейного использования. Для использования Программного обеспечения в коммерческих средах, а также на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходимо приобрести версию Программного обеспечения для бизнеса.

d) **Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

e) **Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, классифицированное как OEM (распространяется через изготовителей комплектного оборудования), можно использовать только на том компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

f) **Не предназначенные для продажи и пробные версии Программного обеспечения.** Программное обеспечение, классифицированное как не предназначенная для продажи или пробная версия, не может быть связано с каким-либо платежом и должно использоваться исключительно для демонстрации или тестирования функций Программного обеспечения.

g) **Прекращение действия Лицензии.** Действие Лицензии прекращается автоматически по окончании периода, на который она была выдана. Если Вы нарушаете любое положение настоящего Соглашения, Поставщик получает право выйти из него, что никак не повлияет на его возможности воспользоваться любыми правами и средствами судебной защиты, доступными ему в таких обстоятельствах. В случае отмены Лицензии Вы обязаны незамедлительно за собственный счет удалить, уничтожить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в точку продажи, в которой оно было приобретено. В случае прекращения действия Лицензии Поставщик также имеет право запретить Конечному пользователю использовать функции Программного обеспечения, которые требуют подключения к серверам Поставщика или серверам третьих лиц.

4. **Функции, для которых необходим сбор данных и подключение к Интернету.** Для корректной работы Программного обеспечения необходимо подключение к Интернету, поскольку Программное обеспечение должно регулярно подключаться к серверам Поставщика или третьих лиц, а также собирать соответствующие данные в соответствии с документом Политика конфиденциальности. Подключение к Интернету необходимо для использования перечисленных далее функций Программного обеспечения.

a) **Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения (далее — «Обновления»), но не обязан их предоставлять. Эта функция включена при использовании стандартных параметров Программного обеспечения. Это значит, что Обновления устанавливаются автоматически, если Конечный пользователь не отключит их автоматическую установку. Для предоставления обновлений необходима проверка подлинности лицензии, включая информацию о компьютере и/или платформе, на которой установлено Программное обеспечение, в соответствии с Политикой конфиденциальности.

Предоставление любых Обновлений может регулироваться политикой в отношении окончания срока службы (далее — «Политика ОСС»), которая доступна по адресу https://go.eset.com/eol. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, Обновления предоставляться не будут.

b) **Отправка зараженных файлов и информации Поставщику.** Программное обеспечение оснащено функциями, которые собирают образцы компьютерных вирусов и других вредоносных программ, а также подозрительные, проблемные, потенциально нежелательные или потенциально опасные объекты, такие как файлы, URL-адреса, IP-пакеты и кадры Ethernet («Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о Компьютере и/или платформе, на которых установлено Программное обеспечение, а также информацию об операциях и функциональности Программного обеспечения («Информация»). Информация и Заражения могут содержать данные (в том числе случайно или непредумышленно полученные персональные данные) о Конечном пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, и о файлах, пораженных Заражениями с соответствующими метаданными.

Информацию и Заражения могут собирать следующие функции Программного обеспечения:

i. Функция LiveGrid Reputation System отвечает за сбор и отправку Поставщику в одном направлении хэшей, связанных с Заражениями. Эта функция включена при использовании стандартных параметров Программного обеспечения.

ii. Система обратной связи LiveGrid отвечает за сбор и отправку Поставщику Заражений со связанными метаданными и Информации. Конечный пользователь может активировать эту функцию в процессе установки Программного обеспечения.

Поставщик обязуется использовать полученные Заражения и Информацию только для анализа и исследования Заражений, улучшения Программного обеспечения и усовершенствования проверки подлинности Лицензии, а также принять необходимые меры предосторожности по сохранению конфиденциальности Информации и Заражений. Активируя эту функцию Программного обеспечения, Вы соглашаетесь на отправку Заражений и Информации Поставщику, а также даете ему необходимое разрешение, регулируемое соответствующими правовыми нормами, на обработку полученной Информации. Данную функцию можно отключить в любой момент.

Для целей настоящего Соглашения необходимо собирать, обрабатывать и хранить данные, позволяющие Поставщику идентифицировать Вас в соответствии с документом Политика конфиденциальности. Настоящим Вы подтверждаете, что Поставщик с помощью своих средств может проверять, используете ли Вы Программное обеспечение в соответствии с положениями настоящего Соглашения. Вы соглашаетесь на передачу информации в процессе обмена данными между Программным обеспечением и компьютерными системами Поставщика или его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, с целью обеспечения работы и проверки возможности использования Программного обеспечения и защиты прав Поставщика.

После заключения этого Соглашения Поставщик или любой из его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, получат право передавать, обрабатывать и хранить важные данные, позволяющие идентифицировать Вашу личность, в целях оплаты и исполнения настоящего Соглашения, а также для отправки уведомлений на Ваш компьютер.

Сведения о конфиденциальности, защите персональных данных и Ваших правах как субъекта персональных данных приведены в Политике конфиденциальности, которая доступна на веб-сайте Поставщика, а также непосредственно в процессе установки. Вы также можете открыть ее из справки Программного обеспечения.

5. **Использование прав Конечного пользователя**. Права Конечного пользователя необходимо использовать лично, либо их могут использовать Ваши сотрудники. Вы имеете право на использование Программного обеспечения только для защиты своих действий и компьютеров или компьютерных систем, на которые приобретена Лицензия.

6. **Ограничения прав.** Не разрешается копировать, распространять Программное обеспечение, извлекать его компоненты и создавать производные работы на его основе. При использовании Программного обеспечения Вы обязаны соблюдать перечисленные далее ограничения.

a) Вы можете создать одну резервную копию Программного обеспечения на носителе постоянного хранения данных при условии, что эта резервная копия не установлена и не используется ни на каком компьютере. Создание любых иных копий Программного обеспечения является нарушением этого Соглашения.

b) Вы не должны использовать, изменять, переводить или воспроизводить Программное обеспечение и передавать права на использование Программного обеспечения или копии Программного обеспечения любым способом, отличным от описанного в настоящем Соглашении.

c) Вы не должны продавать, передавать на условиях сублицензии, сдавать в аренду или передавать во временное пользование Программное обеспечение, а также использовать Программное обеспечение для предоставления коммерческих услуг.

d) Запрещается вскрывать технологию, декомпилировать или разбирать код Программного обеспечения и иными способами пытаться получить исходный код Программного обеспечения за исключением того, в чем данное ограничение противоречит действующему законодательству.

e) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем действующим законодательным нормам страны, в которой используется Программное обеспечение, в том числе применимым ограничениям относительно авторского права, других прав на интеллектуальную собственность и так далее.

f) Вы соглашаетесь использовать Программное обеспечение и его функции только способом, который не ограничивает возможности доступа к этим услугам других Конечных пользователей. Поставщик оставляет за собой право ограничить объем услуг, предоставляемых отдельным Конечным пользователям, чтобы обеспечить использование услуг максимально возможным числом Конечных пользователей. Ограничение объема услуг должно также означать полное прекращение возможности использовать любую из функций Программного обеспечения, а также удаление Данных и информации на серверах Поставщика или сторонних серверах, относящихся к определенной функции Программного обеспечения.

g) Вы обязуетесь не предпринимать действий, связанных с использованием Лицензионного ключа, которые противоречат условиям настоящего Соглашения или приводят к предоставлению Лицензионного ключа лицу, не имеющему права использовать Программное обеспечение, например передачу использованного или неиспользованного Лицензионного ключа в любой форме, а также несанкционированное воспроизведение или распространение дублированных или сгенерированных лицензионных ключей или использование Программного обеспечения с помощью Лицензионного ключа, полученного не от Поставщика.

7. **Авторское право**. Программное обеспечение и все права на него, в том числе, среди прочего, право собственности и права на объекты интеллектуальной собственности,

принадлежат компании ESET и/или ее лицензиарам. Эти права защищены международными соглашениями и всеми прочими применимыми законодательными нормами страны, в которой используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются ценной коммерческой тайной и конфиденциальной информацией, принадлежащими компании ESET и/или ее лицензиарам. Запрещается копировать Программное обеспечение кроме случаев, описанных в статье 6(a). Любые копии, которые разрешено создать в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и другие уведомления о правах интеллектуальной собственности, которые присутствуют в самом Программном обеспечении. Если Вы вскрываете технологию, декомпилируете, разбираете исходный код Программного обеспечения или иным способом пытаетесь получить исходный код Программного обеспечения в нарушение положений этого Соглашения, любая полученная таким образом информация автоматически и безоговорочно должна считаться подлежащей передаче Поставщику и принадлежащей ему полностью с момента создания вне зависимости от прав Поставщика в отношении нарушения этого Соглашения.

8. **Сохранение прав**. Настоящим Поставщик сохраняет за собой все права на Программное обеспечение, за исключением прав, явно предоставленных Вам как Конечному пользователю Программного обеспечения в соответствии с условиями настоящего Соглашения.

9. **Несколько языковых версий, программное обеспечение на носителях двух типов, несколько копий**. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько экземпляров программного обеспечения, разрешается использовать Программное обеспечение только на том количестве компьютеров и в тех версиях, на которые была приобретена Лицензия. Запрещается продавать, передавать на условиях сублицензии, сдавать в аренду, передавать во временное или постоянное пользование версии или копии Программного обеспечения, которые не используются Вами.

10. **Момент вступления в силу и прекращение действия Соглашения.** Настоящее Соглашение вступает в законную силу с дня, когда Вы согласились с его условиями. Завершить действие Соглашения можно в любой момент, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии и любые относящиеся к нему материалы, предоставленные Поставщиком или одним из его коммерческих партнеров. Ваше право на использование Программного обеспечения и любых его функций может регулироваться политикой в отношении окончания срока службы. После наступления даты окончания срока службы, которая устанавливается политикой в отношении окончания срока службы для Программного обеспечения или какой-либо из его функций, ваше право на использование Программного обеспечения прекратится. Независимо от способа прекращения действия этого Соглашения положения статей 7, 8, 11, 13, 19 и 21 остаются действительными без ограничения по времени.

11. **ГАРАНТИИ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ**. ВЫСТУПАЯ В КАЧЕСТВЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ГАРАНТИЙ ЛЮБОГО ТИПА, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ. НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ, НИ ПРАВООБЛАДАТЕЛИ НЕ ДЕЛАЮТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО ИСПОЛЬЗОВАНИЯ, А ТАКЖЕ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ ЗНАКИ

И ДРУГИХ ПРАВ ТРЕТЬИХ ЛИЦ. ПОСТАВЩИК И ЛЮБЫЕ ДРУГИЕ ЛИЦА НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫХ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС.

12. **Отказ от других обязательств**. Настоящее Соглашение не предусматривает никаких обязательств для Поставщика и его лицензиаров за исключением тех, которые изложены в настоящем Соглашении.

13. **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**. В ТОЙ СТЕПЕНИ, В КОТОРОЙ ЭТО РАЗРЕШЕНО ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПОСТАВЩИК, ЕГО СОТРУДНИКИ ИЛИ ЛИЦЕНЗИАРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКУЮ-ЛИБО УПУЩЕННУЮ ПРИБЫЛЬ, ВЫРУЧКУ, ПРОДАЖИ, ДАННЫЕ ИЛИ РАСХОДЫ НА ЗАКУПКУ ВЗАИМОЗАМЕНЯЕМЫХ ТОВАРОВ ИЛИ УСЛУГ, ПОВРЕЖДЕНИЕ ИМУЩЕСТВА, ТЕЛЕСНЫЕ ПОВРЕЖДЕНИЯ, ПРИОСТАНОВКУ РАБОТЫ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ЗА КАКИЕ-ЛИБО ФАКТИЧЕСКИЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, ЭКОНОМИЧЕСКИЕ, КОМПЕНСИРУЕМЫЕ, ШТРАФНЫЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, НАНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ВЫПОЛНЕНИЯ СОГЛАШЕНИЯ, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ ИЛИ НЕБРЕЖНОСТИ, НЕЗАВИСИМО ОТ ПРИЧИНЫ И ВИДА ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ УСТАНОВКИ, ИСПОЛЬЗОВАНИЯ ИЛИ ОТСУТСТВИЯ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК, ЕГО ЛИЦЕНЗИАРЫ ИЛИ АФФИЛИРОВАННЫЕ ЛИЦА ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ТАКОГО УЩЕРБА. ПОСКОЛЬКУ ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ РАЗРЕШАЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО ПОЗВОЛЯЮТ ОГРАНИЧИВАТЬ ЕЕ, В ТАКИХ СЛУЧАЯХ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ ОГРАНИЧИВАЕТСЯ СУММОЙ, ВЫПЛАЧЕННОЙ ВАМИ ЗА ЛИЦЕНЗИЮ.

14. Ни одно из положений настоящего Соглашения не затрагивает законные права любой стороны, выступающей в качестве потребителя, даже если они противоречат таким правам.

15. **Техническая поддержка**. ESET или привлеченные компанией ESET третьи лица предоставляют техническую поддержку по собственному усмотрению без каких-либо гарантий или заявлений. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, техническая поддержка предоставляться не будет. Конечный пользователь обязан создать резервную копию всех существующих данных, программного обеспечения или программных средств, прежде чем обратиться за технической поддержкой. ESET и (или) третьи лица, привлеченные ESET, не могут принять на себя ответственность за повреждение или потерю данных, собственности, программного обеспечения или оборудования, а также за упущенную прибыль, которые связаны с предоставлением технической поддержки. ESET и (или) привлеченные ESET третьи лица оставляют за собой право принять решение о том, что устранить конкретную проблему невозможно в рамках технической поддержки. ESET оставляет за собой право отказать в предоставлении технической поддержки, приостановить или прекратить ее оказание по своему собственному усмотрению. Сведения о лицензии, Информация и другие данные в соответствии с Политикой конфиденциальности могут потребоваться для предоставления технической поддержки.

16. **Передача лицензии**. Программное обеспечение может быть перенесено с одного компьютера на другой, если это не противоречит условиям настоящего Соглашения. Если это не противоречит условиям Соглашения, Конечный пользователь может только перманентно

передать Лицензию и все права по настоящему Соглашению другому Конечному пользователю с согласия Поставщика, если соблюдаются следующие условия: (i) у первого Конечного пользователя не остается никаких экземпляров Программного обеспечения; (ii) передача прав должна быть непосредственной, т. е. от исходного Конечного пользователя к новому; (iii) новый Конечный пользователь должен принять все права и обязательства исходного Конечного пользователя по настоящему Соглашению; (iv) исходный Конечный пользователь должен предоставить новому Конечному пользователю документацию, позволяющую проверить подлинность Программного обеспечения в соответствии со статьей 17.

17. **Проверка подлинности Программного обеспечения.** Конечный пользователь может продемонстрировать наличие у него прав на использование Программного обеспечения одним из следующих способов: (i) с помощью лицензионного сертификата, выданного Поставщиком или третьим лицом, которое назначено Поставщиком; (ii) письменным лицензионным соглашением, если таковое было заключено; (iii) путем предоставления отправленного Поставщиком сообщения электронной почты, в котором содержатся сведения о лицензии (имя пользователя и пароль). Сведения о лицензии и идентификационные данные Конечного пользователя в соответствии с Политикой конфиденциальности могут потребоваться для проверки подлинности программного обеспечения.

18. **Предоставление лицензии органам власти и правительству США**. Программное обеспечение будет предоставлено органам власти, в том числе правительству Соединенных Штатов Америки, в соответствии с правами и ограничениями, описанными в настоящем Соглашении.

19. **Соответствие нормам регулирования внешней торговли**.

a) Вы не будете прямо или косвенно экспортировать, реэкспортировать, передавать или иным образом предоставлять Программное обеспечение кому-либо, а также не будете использовать его каким-либо образом либо иметь отношение к каким-либо действиям, в результате чего компания ESET или ее холдинговые компании, ее филиалы, филиалы ее холдинговых компаний, прочие субъекты, находящиеся под управлением ее холдинговых компаний («Аффилированные лица»), может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением. К законодательству по регулированию внешней торговли относится:

i. Любое законодательство, которое предназначено для регулирования, ограничения или введения лицензионных требований в сфере экспорта, реэкспорта или передачи товаров, программного обеспечения, технологий, услуг и которое принимается любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица

ii. Любые экономические, финансовые, торговые и прочие санкции, ограничения, эмбарго, запреты на импорт или экспорт, запреты на перевод денежных средств или активов либо на предоставление услуг, а также эквивалентные меры, которые вводятся в действие любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица.

(Законодательные акты, упомянутые в пунктах i и ii выше, совместно именуются «Законодательство по регулированию внешней торговли».)

b) Компания ESET имеет право приостановить выполнение своих обязательств согласно настоящим Условиям либо незамедлительно прекратить действие настоящих Условий в следующих случаях:

i. В случае, если компания ESET устанавливает, что по ее обоснованному мнению Пользователь нарушил или может нарушить положения Статьи 19 a) настоящего Соглашения.

ii. В случае, если Конечный пользователь и/или Программное обеспечение попадут под действие Законодательства по регулированию внешней торговли, и, как результат, компания ESET установит, что по ее обоснованному мнению продолжение выполнения своих обязательств согласно настоящему Соглашению может привести к тому, что компания ESET или ее Аффилированные лица может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением.

c) Ни одна часть настоящего Соглашения не предназначена, не может интерпретироваться или истолковываться так, чтобы побуждать либо обязывать любую его сторону действовать или воздерживаться от действий (или согласиться действовать или воздерживаться от действий) каким-либо образом, который противоречит любому применимому Законодательству по регулированию внешней торговли, преследуется или запрещается им.

20. **Уведомления**. Все уведомления, возвращаемые Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, что не ограничивает право ESET сообщать Вам о любых изменениях в настоящем Соглашении, политиках конфиденциальности, политике в отношении окончания срока службы и документации в соответствии со статьей 22 настоящего Соглашения. ESET может отправлять Вам письма по электронной почте и уведомления в Программном обеспечении, а также публиковать сообщения на нашем веб-сайте. Вы соглашаетесь получать юридически значимые сообщения от компании ESET в электронной форме, в том числе любые сообщения об изменении Условий, Специальных условий или Политик конфиденциальности, любые предложения и принятие условий договоров, приглашения вести переговоры о заключении договора, уведомления или другие юридически значимые сообщения. Такие электронные сообщения считаются полученными в письменной форме, если только действующее законодательство не требует другого формата коммуникации.

21. **Применимое законодательство**. Данное Соглашение регулируется и толкуется в соответствии с законодательством Словацкой Республики. Конечный пользователь и Поставщик согласны, что принципы коллизионного права и Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров не применяются. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду I в Братиславе.

22. **Общие положения**. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения, которые по-прежнему будут действительными и выполнимыми в соответствии с указанными здесь условиями. Настоящее Соглашение составлено на английском языке. В случае подготовки перевода настоящего Соглашения для удобства или любой иной цели либо при наличии любых расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке.

Компания ESET оставляет за собой право вносить изменения в Программное обеспечение и пересматривать условия настоящего Соглашения, приложений и дополнений к нему, Политики конфиденциальности, Политики ОСС и документации или какой-либо их части в любое время путем обновления соответствующего документа (а) для отображения изменений в Программном обеспечении либо в способе осуществления деятельности компанией ESET, (б) для соблюдения нормативно-правовых норм или из соображений безопасности либо (в) для недопущения нарушений или нанесения вреда. В случае изменения настоящего Соглашения Вы будете уведомлены с помощью электронной почты, уведомления в приложении или другими электронными средствами. Если Вы не согласны с предлагаемыми изменениями к настоящему Соглашению, Вы можете расторгнуть его в соответствии со статьей 10 в течение 30 дней после получения уведомления об изменении. Если Вы не расторгнете настоящее Соглашение в течение этого срока, предлагаемые изменения будут считаться принятыми и вступят в силу в отношении Вас с даты получения Вами уведомления об изменении.

Это полное Соглашение между Поставщиком и Вами относительно использования Программного обеспечения, которое заменяет все предыдущие заверения, обсуждения, гарантии или уведомления или рекламные материалы в отношении Программного обеспечения.

EULAID: EULA-PRODUCT-LG; 3537.0

Политика конфиденциальности

Компания ESET, spol. s r. o., зарегистрированная по адресу Einsteinova 24, 851 01 Bratislava, Slovak Republic, внесенная в реестр юридических лиц окружного суда I в Братиславе, раздел Sro, запись 3586/B, регистрационный номер предприятия 31333532, как контролер данных (далее — «ESET» или «Мы») уделяет особое внимание защите персональных данных. Мы стремимся соблюдать требования к прозрачности, устанавливаемые Общим регламентом ЕС по защите данных (GDPR). Поэтому Мы публикуем эту Политику конфиденциальности, исключительно чтобы уведомить клиента, который является субъектом данных (далее — «Конечный пользователь» или «Вы»), о следующих аспектах защиты персональных данных:

- Правовые основания для обработки персональных данных.
- Передача данных третьим лицам и конфиденциальность.
- Защита данных.
- Ваши права как субъекта данных.
- Обработка персональных данных.
- Контактная информация.

Обработка персональных данных

Услуги, предоставляемые ESET и реализованные в нашем продукте, предоставляются в соответствии с договором, именуемым ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, некоторые условия которого заслуживают особого внимания. Мы хотим рассказать Вам подробнее о сборе данных, связанных с предоставлением наших служб. Мы предоставляем различные услуги, перечисленные в Лицензионном соглашении и описании возможностей продукта, именуемом документация. Чтобы все это работало, нам необходимо собирать следующую информацию.

- обновления и другую статистику, содержащую данные о процессе установки и Вашем компьютере, в том числе тип платформы, операции и функции Наших программ,

например версию ОС, характеристики оборудования, идентификаторы инсталляций и лицензий, IP- и MAC-адреса, конфигурации программ;
- Однонаправленные хеш-функции, связанные с заражениями и входящие в систему репутации ESET LiveGrid®, которая повышает эффективность решений для защиты от вредоносных программ и благодаря которой сканируемые файлы сопоставляются с элементами белого и черного списков в облаке.
- Подозрительные образцы метаданных из внешних источников в рамках системы обратной связи ESET LiveGrid®, благодаря которой ESET может мгновенно реагировать на нужды пользователей и своевременно адаптироваться под новейшие угрозы. Мы рассчитываем на то, что вы будете присылать нам:
    - зараженные элементы, такие как потенциальные образцы вирусов и прочих вредоносных программ; подозрительные, проблемные, потенциально нежелательные и небезопасные объекты, такие как исполняемые файлы, сообщения электронной почты, про которые сообщили вы как про спам или которые выявил наш продукт;
    - информацию об устройствах в локальной сети, например тип, производитель, модель и/или название;
    - сведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;
    - файлы аварийных дампов и их содержимое.

Мы не стремимся собирать какие-либо данные, кроме обозначенных выше, но иногда этого невозможно избежать. Случайно собранные данные могут входить в состав вредоносных программ (будучи собранными без вашего ведома и одобрения) либо входить в имена файлов и URL-адреса, и Мы не намерены делать их частью наших систем или обрабатывать их для целей, указанных в настоящей Политике конфиденциальности.

- Сведения о лицензиях, например идентификаторы лицензий, и личные данные, например имя, фамилия, адрес, электронная почта, необходимые для выставления счетов, проверки подлинности лицензий и предоставления наших услуг.
- Для обслуживания и предоставления поддержки может потребоваться контактная информация и данные, указанные в Ваших запросах на поддержку. Исходя из выбранного способа общения, Мы можем фиксировать Ваш электронный адрес, номер телефона, информацию о лицензии, сведения о программах и описание Вашего инцидента. Возможно, служба поддержки попросит Вас предоставить дополнительную информацию, чтобы упростить решение проблемы.

Передача данных третьим лицам и конфиденциальность

Мы не передаем Ваши данные третьим лицам. Однако ESET — это компания, ведущая деятельность в глобальных масштабах через сеть распространения, обслуживания и поддержки, которая состоит из аффилированных компаний и партнеров. В целях выполнения Лицензионного соглашения, например для предоставления услуг или поддержки, Мы можем обмениваться с аффилированными компаниями и партнерами информацией о лицензиях, оплате и технической поддержке, которую обрабатывает компания ESET.

Компания ESET обрабатывает данные преимущественно в странах Европейского Союза (ЕС). Однако в зависимости от Вашего местонахождения (при использовании наших продуктов и/или служб за пределами ЕС) и/или выбранной Вами службы нам может понадобиться передать Ваши данные в страну за пределами ЕС. Например, мы используем сторонние службы

облачных вычислений. В таких случаях мы тщательно выбираем поставщиков таких служб и обеспечиваем надлежащий уровень защиты данных с помощью договорных, а также технических и организационных мер. Как правило, мы применяем стандартные договорные условия, действующие в ЕС. При необходимости они могут дополняться другими условиями.

В некоторых странах за пределами ЕС, таких как Великобритания и Швейцария, сопоставимый уровень защиты данных уже определен законодательством ЕС. В связи с этим передача данных в эти страны не требует специального разрешения или соглашения.

Права субъекта данных

Права каждого Конечного пользователя важны, поэтому Мы хотели бы рассказать Вам о правах, которые ESET гарантирует всем Конечным пользователям независимо от того, находятся ли они в странах ЕС или нет. Эти права описаны ниже. Чтобы воспользоваться своими правами субъекта данных, Вы можете обратиться к нам через форму для связи со службой поддержки или по адресу электронной почты dpo@eset.sk. В целях идентификации просим Вас предоставить следующую информацию: имя, адрес электронной почты и лицензионный ключ (если есть) или номер клиента и название компании. Не отправляйте другие персональные данные, такие как дата рождения. Чтобы рассмотреть Ваше обращение, а также в целях идентификации Мы обработаем Ваши персональные данные.

Право отозвать согласие. Право отозвать согласие действует только в том случае, если данные обрабатываются исключительно по согласию. Если Мы обрабатываем Ваши персональные данные на основании Вашего согласия, Вы имеете право в любое время отозвать его без указания причин. Отзыв согласия касается только обработки данных в будущем и не влияет на законность их обработки, выполнявшейся до этого.

Право на возражение. Право возразить против обработки данных действует в том случае, если данные обрабатываются на основании законного интереса ESET или третьей стороны. Если Мы обрабатываем Ваши персональные данные в своих законных интересах, Вы как субъект данных можете в любое время возразить против этого. Ваше возражение касается только обработки данных в будущем и не влияет на законность их обработки, выполнявшейся до этого. Если Мы обрабатываем Ваши персональные данные в целях прямого маркетинга, Вам не нужно указывать причину возражения. Это также относится к составлению профиля в той мере, насколько это связано с прямым маркетингом. Во всех остальных случаях Мы просим Вас кратко описать, почему Вы возражаете против законных интересов компании ESET обрабатывать Ваши персональные данные.

Обратите внимание, что в некоторых случаях, несмотря на Ваш отзыв согласия, Мы можем продолжить обрабатывать Ваши персональные данные на другом правовом основании, например для выполнения договора.

Право доступа. Как субъект данных Вы имеете право в любое время бесплатно получить информацию о своих данных, которые хранятся в ESET.

Право на исправление. Если Мы непреднамеренно обрабатываем неверные персональные данные о Вас, Вы имеете право требовать их исправления.

Право на удаление и право на ограничение обработки. Как субъект данных Вы имеете право требовать удаления или ограничения обработки Ваших персональных данных. Если персональные данные обрабатываются с Вашего согласия, вы можете отозвать его и, если нет иных правовых оснований для обработки данных, например в целях выполнения договора, Мы

немедленно их удалим. Ваши персональные данные также будут удалены по окончании нашего периода хранения, если они больше не требуются для указанных в их отношении целей.

Если Мы используем Ваши персональные данные исключительно в целях прямого маркетинга, а Вы отозвали свое согласие или выдвинули возражение против законных интересов ESET на сбор таких данных, Мы ограничим их обработку следующим образом: Ваши контактные данные будут внесены в наш внутренний черный список, чтобы не допускать нежелательных контактов. В противном случае Ваши персональные данные будут удалены.

Обратите внимание, что по закону или предписанию надзорного органа от нас может требоваться хранить персональные данные в течение определенного периода. Обязательства по хранению и периоды хранения могут также регулироваться законодательством Словакии. По окончании такого периода персональные данные удаляются.

Запросить переносимость данных. Как субъект данных Вы можете получить персональные данные, которые обрабатывает ESET, в файле формата XLS.

Право на подачу жалобы. Как субъект данных Вы имеете право в любое время подать жалобу в надзорный орган. ESET действует согласно словацким законам и законам о защите данных ЕС. Надзорным органом является Офис по защите персональных данных Словацкой Республики, расположенный по адресу Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Контактная информация

Если Вы хотите воспользоваться своими правами субъекта данных или у Вас возникнет вопрос или проблема, отправьте нам письмо по адресу:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk