ESET

# REMOTE ADMINISTRATOR 5

## Инструкция по установке и руководство пользователя

Щелкните здесь, чтобы загрузить самую последнюю версию этого документа

# ESET **REMOTE ADMINISTRATOR 5**



Международная служба поддержки: www.eset.eu/support
Служба поддержки в Северной Америке: www.eset.com/support

Версия 11/20/2015

# Содержание


1. Введение ..... 5
1.1 Новые возможности в ESET Remote Administrator версии 5.3 ..... 5
1.2 Архитектура программы ..... 6
1.3 Поддерживаемые продукты и языки ..... 7
2. Установка сервера ERA Server и консоли ERA Console ..... 9
2.1 Требования ..... 9
2.1.1 Требования к программному обеспечению и базе данных ..... 9
2.1.2 Требования к быстродействию ..... 10
2.1.3 Используемые порты ..... 13
2.1.4 Поиск компьютеров ..... 14
2.2 Основные рекомендации по установке ..... 15
2.2.1 Обзор среды (структура сети) ..... 15
2.2.2 Перед установкой ..... 15
2.2.3 Установка ..... 16
2.2.3.1 Установка сервера ERA Server ..... 16
2.2.3.1.1 Установка в режиме кластера ..... 17
2.2.3.2 Установка консоли ERA Console ..... 18
2.2.3.3 Зеркало ..... 19
2.2.3.4 Типы баз данных, поддерживаемые сервером ERA Server ..... 19
2.2.3.4.1 Основные требования ..... 20
2.2.3.4.2 Настройка подключения к базе данных ..... 21
2.2.3.5 Установка поверх предыдущих версий ..... 21
2.3 Сценарий: установка в корпоративной среде ..... 23
2.3.1 Обзор среды (структура сети) ..... 23
2.3.2 Установка ..... 24
2.3.2.1 Установка в головном офисе ..... 24
2.3.2.2 Филиал: установка сервера ERA Server ..... 24
2.3.2.3 Филиал: установка HTTP-сервера зеркала ..... 24
2.3.2.4 Филиал: удаленная установка на клиентах ..... 25
2.3.3 Прочие требования к корпоративным средам ..... 25
3. Работа с консолью ERA Console ..... 27
3.1 Подключение к серверу ERA Server ..... 27
3.2 Главное окно консоли ERA Console ..... 28
3.2.1 Настройка страницы ..... 29
3.3 Фильтрация данных ..... 30
3.3.1 Фильтр ..... 30
3.3.2 Контекстное меню ..... 31
3.3.3 Фильтр даты ..... 32
3.4 Вкладки в консоли ERA Console ..... 32
3.4.1 Общее описание вкладок и клиентов ..... 32
3.4.2 Репликация и данные на отдельных вкладках ..... 33
3.4.3 Вкладка «Клиенты» ..... 34
3.4.3.1 Объединение дублирующихся клиентов ..... 36
3.4.3.2 Сетевые действия ..... 37
3.4.4 Вкладка «Журнал угроз» ..... 39
3.4.5 Вкладка «Журнал файервола» ..... 39
3.4.6 Вкладка «Журнал событий» ..... 40
3.4.7 Вкладка «Журнал системы предотвращения вторжений на... 40
3.4.8 Журнал контроля устройств ..... 40
3.4.9 Журнал контроля доступа в Интернет ..... 41
3.4.10 Вкладка «Журнал защиты от спама» ..... 41
3.4.11 Вкладка «Журнал занесения в "серый" список» ..... 42
3.4.12 Вкладка «Журнал сканирования» ..... 42
3.4.13 Вкладка «Мобильный журнал» ..... 42
3.4.14 Вкладка «Карантин» ..... 43
3.4.15 Вкладка «Задачи» ..... 43
3.4.16 Вкладка «Отчеты» ..... 44
3.4.16.1 Панель мониторинга ..... 46
3.4.16.1.1 Список веб-серверов панели мониторинга ..... 49
3.4.16.2 Образец сценария отчета ..... 50
3.4.17 Вкладка «Удаленная установка» ..... 51
3.4.17.1 Мастер задачи поиска в сети ..... 52
3.4.17.2 Диспетчер пакетов ..... 54
3.4.17.2.1 Параметры командной строки ..... 56
3.4.17.2.2 Параметры пакета установки ..... 58
3.4.17.2.3 Параметры удаления ESET Endpoint Antivirus ..... 59
3.4.17.2.4 Параметры удаления ESET Endpoint Security ..... 60
3.4.17.2.5 Параметры командной строки для пользовательского ..... 61
3.4.17.3 Диагностика удаленной установки ..... 62
3.4.17.4 Журнал установки ..... 63
3.4.17.4.1 Повторный запуск задачи ..... 63
3.4.17.4.2 Просмотр содержимого файла результатов ..... 64
3.5 Настройки консоли ERA ..... 64
3.5.1 Подключение ..... 64
3.5.2 Столбцы ..... 65
3.5.3 Цвета ..... 65
3.5.4 Пути ..... 65
3.5.5 Дата/время ..... 66
3.5.6 Панели ..... 66
3.5.7 Другие настройки ..... 66
3.6 Режимы отображения ..... 67
3.7 ESET Configuration Editor ..... 67
3.7.1 Иерархическое представление конфигурации ..... 68
3.7.2 Основные элементы конфигурации ..... 69
4. Установка клиентских решений компании ESET ..... 71
4.1 Непосредственная установка ..... 71
4.2 Удаленная установка ..... 72
4.2.1 Требования и ограничения ..... 72
4.2.1.1 Требования к автоматической установке Linux/Mac ..... 73
4.2.1.2 Требования WMI ..... 74
4.2.2 Удаленная автоматическая установка ..... 74
4.2.3 Удаленная установка с использованием сценария входа ..... 76
4.2.3.1 Экспорт установщика ESET в папку или сценарий входа ..... 77
4.2.3.2 Вход по умолчанию и сведения для входа ..... 79
4.2.4 Пользовательская удаленная установка ..... 79
4.2.5 Клиент обновления Windows ..... 80
4.2.6 Как избежать повторных установок ..... 81
4.2.7 Повторный запуск задачи ..... 82
4.2.8 Новая задача установки ..... 82
4.2.8.1 Дополнительные параметры ..... 84
4.2.8.2 Настройка совместного использования установщика ..... 85
4.2.8.3 Информация WMI ..... 86
4.2.8.4 Экспорт служб WSUS ..... 86
4.2.8.5 Экспорт объекта групповой политики ..... 87
5. Управление клиентскими компьютерами ..... 88
5.1 Задачи ..... 88
5.1.1 Задача конфигурации ..... 89
5.1.2 Задача сканирования по требованию ..... 90
5.1.3 Задача «Обновить сейчас» ..... 90
5.1.4 Задача «Сценарий SysInspector» ..... 91
5.1.5 Свойства защиты ..... 91
5.1.6 Выполнить запланированную задачу ..... 91
5.1.7 Задача «Восстановить или удалить из карантина» ..... 91
5.1.8 Откат базы данных вирусов ..... 92
5.1.9 Очистка кэша обновления клиента ..... 92
5.1.10 Задача «Создать журнал аудита безопасности» ..... 93
5.1.11 Задача «Показать уведомление» ..... 93
5.1.12 Завершение задачи ..... 93
5.2 Диспетчер групп ..... 94
5.2.1 Статические группы ..... 94
5.2.2 Параметрические группы ..... 95
5.2.3 Синхронизация Active Directory/LDAP ..... 96
5.3 Политики ..... 96
5.3.1 Основные принципы применения и действия ..... 97
5.3.2 Создание политик ..... 97
5.3.3 Виртуальные политики ..... 98
5.3.4 Роль и назначение политик в древовидной структуре ..... 98
5.3.5 Просмотр политик ..... 99
5.3.6 Импорт и экспорт политик ..... 99
5.3.7 Мастер миграции политик ..... 99

5.3.8 Назначение политик клиентам ... 100
5.3.8.1 Политика по умолчанию для основных клиентов ... 100
5.3.8.2 Назначение вручную ... 100
5.3.8.3 Правила политик ... 100
5.3.8.3.1 Мастер правил политики ... 102
5.3.9 Политики для мобильных клиентов ... 102
5.3.10 Удаление политик ... 103
5.3.11 Специальные настройки ... 104
5.3.12 Сценарии развертывания политик ... 104
5.3.12.1 Каждый сервер является автономной единицей, политики ... 104
5.3.12.2 Каждый сервер обслуживается отдельно, политики управляются локально, но родительская политика по ... 106
5.3.12.3 Наследование политик с сервера верхнего уровня ... 107
5.3.12.4 Назначение политик только с сервера верхнего уровня ... 108
5.3.12.5 Использование групп ... 108
**5.4 Диспетчер уведомлений ... 110**
5.4.1 Состояние клиента ... 113
5.4.2 Состояние сервера ... 114
5.4.3 Событие «Задача завершена» ... 116
5.4.4 Событие «Новый клиент» ... 116
5.4.5 Событие вспышки ... 117
5.4.6 Событие получения журнала ... 118
5.4.7 Действие ... 118
5.4.8 Уведомления с использованием SNMP-ловушки ... 119
5.4.9 Пример создания правила ... 119
**5.5 Подробные сведения о клиентах ... 120**
**5.6 Мастер объединения правил файервола ... 121**

## 6. Параметры сервера ERA ... 122

**6.1 Общее ... 122**
6.1.1 Управление лицензиями ... 122
**6.2 Безопасность ... 123**
6.2.1 Диспетчер пользователей ... 124
6.2.2 Пароль доступа к консоли ... 124
**6.3 Обслуживание сервера ... 124**
6.3.1 Параметры сбора журналов ... 125
6.3.2 Очистка по времени ... 125
6.3.3 Расширенные параметры очистки по числу записей в журнале ... 126
**6.4 Ведение журнала ... 127**
6.4.1 Просмотр журнала аудита ... 128
**6.5 Репликация ... 129**
6.5.1 Репликация в больших сетях ... 130
**6.6 Обновления ... 132**
6.6.1 Сервер зеркала ... 133
6.6.1.1 Работа сервера зеркала ... 134
6.6.1.2 Типы обновлений ... 135
6.6.1.3 Включение и настройка зеркала ... 135
**6.7 Другие настройки ... 136**
**6.8 Дополнительно ... 137**

## 7. Консоль командной строки ERA ... 139

**7.1 Параметры команд ... 141**
**7.2 Команды ... 142**

## 8. Интерфейс API ERA ... 174

## 9. ERA Maintenance Tool ... 175

**9.1 Остановка сервера ERA Server ... 175**
**9.2 Запуск сервера ERA Server ... 175**
**9.3 Передача базы данных ... 176**
**9.4 Резервное копирование базы данных ... 176**
**9.5 Восстановление базы данных ... 177**
**9.6 Удаление таблиц ... 177**
**9.7 Резервное копирование хранилища ... 177**
**9.8 Восстановление хранилища ... 177**
**9.9 Установка нового лицензионного ключа ... 178**
**9.10 Изменение конфигурации сервера ... 178**
**9.11 Интерфейс командной строки ... 178**

## 10. Устранение неполадок ... 179

**10.1 Часто задаваемые вопросы ... 179**
10.1.1 Проблемы, связанные с установкой ESET Remote ... 179
10.1.2 Значения кода ошибки GLEerver 2000/2003 ... 179
**10.2 Часто встречающиеся коды ошибок ... 179**
10.2.1 Сообщения об ошибках, выводимые при удаленной установке ESET Smart Security или ESET NOD32 Antivirus ... 179
10.2.2 Часто встречающиеся коды ошибок в журнале era.log ... 180
**10.3 Диагностика проблем на сервере ERAS ... 181**

## 11. Советы и подсказки ... 182

**11.1 Планировщик ... 182**
**11.2 Удаление существующих профилей ... 183**
**11.3 Экспорт и прочие функции XML-конфигурации клиента ... 183**
**11.4 Комбинированное обновление для ноутбуков ... 184**
**11.5 Установка продуктов сторонних производителей с помощью программы ERA ... 186**

## 12. ESET SysInspector ... 187

**12.1 Знакомство с ESET SysInspector ... 187**
12.1.1 Запуск ESET SysInspector ... 187
**12.2 Интерфейс пользователя и работа в приложении ... 188**
12.2.1 Элементы управления программой ... 188
12.2.2 Навигация в ESET SysInspector ... 189
12.2.2.1 Сочетания клавиш ... 191
12.2.3 Сравнение ... 192
**12.3 Параметры командной строки ... 193**
**12.4 Сценарий обслуживания ... 194**
12.4.1 Создание сценария обслуживания ... 194
12.4.2 Структура сценария обслуживания ... 194
12.4.3 Выполнение сценариев обслуживания ... 197
**12.5 Часто задаваемые вопросы ... 197**

## 13. ESET SysRescue ... 199

**13.1 Минимальные требования ... 199**
**13.2 Создание компакт-диска аварийного восстановления ... 199**
**13.3 Выбор места записи ... 200**
**13.4 Параметры ... 200**
13.4.1 Папки ... 200
13.4.2 Антивирус ESET ... 201
13.4.3 Дополнительные настройки ... 201
13.4.4 Интернет-протокол ... 201
13.4.5 Загрузочное USB-устройство ... 202
13.4.6 Запись ... 202
**13.5 Работа с решением ESET SysRescue ... 202**
13.5.1 Использование решения ESET SysRescue ... 202

## 14. Приложение. Лицензия сторонних разработчиков. ... 203

# 1. Введение

ESET Remote Administrator (ERA) — это приложение, которое позволяет централизованно управлять продуктами компании ESET в сети, состоящей из рабочих станций и серверов. С помощью встроенного в ESET Remote Administrator диспетчера задач можно устанавливать продукты безопасности ESET на удаленных компьютерах и быстро реагировать на новые проблемы и угрозы.

Сам по себе ESET Remote Administrator не обеспечивает никакой другой защиты от злонамеренного кода. Работа ERA зависит от присутствия на рабочих станциях или серверах продуктов ESET для обеспечения безопасности, таких как ESET Endpoint Antivirus или ESET Endpoint Security.

Для полного развертывания пакета продуктов безопасности ESET необходимо выполнить указанные ниже действия.

- Установка сервера ERA Server (ERAS),
- Установка консоли ERA Console (ERAC),
- Установка на клиентские компьютеры (ESET Endpoint Antivirus, ESET Endpoint Security и др.).

**Примечание.** В некоторых разделах этого документа используются системные переменные, которые описывают точные размещение папок и файлов:

*%ProgramFiles%* = обычно в *C:\Program Files*
*%ALLUSERSPROFILE%* = обычно в *C:\Documents and Settings\All Users*

## 1.1 Новые возможности в ESET Remote Administrator версии 5.3

**ESET Remote Administrator версии 5.3**

- Улучшения удаленной автоматической установки и новые методы (WMI).
- Поддержка протокола IPv6.
- Улучшения интерфейса командной строки и API (появились дополнительные команды).
- 64-разрядный интерфейс API.
- Возможность объединять дублирующиеся клиенты.
- Улучшенное управление пакетами.

Щелкните здесь, если вы используете ESET Remote Administrator 6.x.

**ESET Remote Administrator версии 5.2**

- API с документируемым исходным кодом и консолью командной строки.
- Удаленное развертывание для Linux и Apple Mac.
- Отчеты в PDF-документах.
- Отчетность по двойным IP-адресам.
- Базовые сетевые действия из консоли («Пробуждение по локальной сети», «Проверка связи», «Сеанс RDP», «Сообщение», «Завершение работы», «Настраиваемое»).
- Удаленная установка пользовательского пакета с перенаправленным выводом данных.
- Упрощенная переадресация журналов.

**ESET Remote Administrator версии 5.1**

- Поддержка нового продукта — ESET File Security для Microsoft SharePoint Server.
- Поддержка нового продукта — ESET Security 4.5 для Kerio.
- Обновление для поддерживаемого продукта — ESET File Security для Microsoft Windows Server.
- Обновление для поддерживаемого продукта — ESET Mail Security для Microsoft Exchange Server.
- Обновление для поддерживаемого продукта — ESET Mail Security для IBM Lotus Domino.
- Обновление для поддерживаемого продукта — ESET Gateway Security для Microsoft Forefront TMG.
- Обновление для поддерживаемого продукта — Endpoint Security для Android.
- Для Endpoint Security для Android добавлен способ удаленной установки.
- Обновление для поддерживаемого продукта — ESET Endpoint Security.
- Обновление для поддерживаемого продукта — ESET Endpoint Antivirus.
- Улучшения панели мониторинга — внутрибраузерный режим редактирования для шаблонов панели мониторинга.
- Политики — изменен внешний вид интерфейса диспетчера политик, при этом добавлены дополнительные метаданные политик.
- Поддержка передачи оповещений и отчетов с помощью почтового SMTP-сервера.
- Схема репликации: возможность пропустить проверку сервера входящих сообщений по готовому статическому списку.
- Поддержка Apple Open Directory и OpenLDAP для поиска в сети и синхронизации групп.
- Миграция политик с целью преобразовать параметры версии 3 или 4 в конфигурацию, совместимую с версией 5.

**ESET Remote Administrator версии 5.0**

- Веб-панель мониторинга для администраторов — всесторонний обзор отчетов в веб-браузере.
- «Удаленная установка» — новый дизайн.
- «Свойства защиты» — новая задача для управления свойствами защиты на клиентах.
- «Выполнить запланированную задачу» — новая задача для немедленного запуска запланированной задачи на клиенте.
- «Диспетчер пользователей» — служебная программа для управления учетными записями и паролями для доступа в консоль.
- Вкладка «Система предотвращения вторжений на узел» — информация о событиях системы предотвращения вторжений на узел на клиентах.
- Вкладка «Контроль доступа в Интернет» — информация о событиях контроля доступа в Интернет на клиентах.
- Вкладка «Контроль устройств» — информация о событиях контроля устройств на клиентах.
- Вкладка «Защита от спама» — информация о событиях защиты от спама на клиентах.
- Вкладка «"Серый" список» — информация о сообщениях «серого» списка на клиентах.
- «Поиск компьютеров в сети» — новые задачи поиска и новый дизайн.
- Полностью поддерживает установку поверх старых версий ERA (4.x, 3.x), в том числе миграцию данных.
- «Отчеты» — новые отчеты, новый дизайн, поддержка веб-панелей мониторинга.

## 1.2 Архитектура программы

Технически программа ESET Remote Administrator состоит из двух отдельных компонентов: ERA Server (ERAS) и ERA Console (ERAC). В сети можно запускать неограниченное число экземпляров ERA Server и консолей ERA, так как в лицензионном соглашении на их использование нет никаких ограничений. Единственным ограничением является общее число клиентов, которыми может управлять установленное средство ERA.

**ERA Server (ERAS)**

Серверный компонент ERA запускается как служба в операционных системах на базе Microsoft Windows® NT, приведенных в этом разделе 9. Основная задача этой службы — сбор информации с клиентов и отправка им разных запросов. Эти запросы, к числу которых относятся задачи настройки, запросы удаленной установки и т. д., создаются с помощью консоли ERA Console (ERAC). ERAS — это промежуточная точка между ERAC и клиентскими компьютерами, место, в котором выполняется обработка, сохранение или изменение всех

сведений перед их передачей клиентам или консоли ERAC.

**ERA Console (ERAC)**

ERAC — это клиентский компонент ERA, который обычно устанавливается на рабочей станции. Администратор с помощью этой рабочей станции удаленно управляет решениями ESET, установленными на отдельных компьютерах-клиентах. С помощью консоли ERAC администратор может подключаться к серверу ERA по TCP-порту 2223. Обмен данными управляется процессом console.exe, который обычно находится в следующем каталоге:

*%ProgramFiles%\ESET\ESET Remote Administrator\Console*

При установке консоли ERAC может понадобиться ввести имя сервера ERAS. После запуска консоль будет автоматически подключаться к этому серверу. Консоль ERAC можно также настроить после установки.

## 1.3 Поддерживаемые продукты и языки

ESET Remote Administrator 5.3 может выполнять развертывание, активацию и управление для следующих продуктов ESET.

| Возможно управление с помощью ESET Remote Administrator 5 | Вплоть до указанной версии |
|---|---|
| ESET Endpoint Security для Windows | 5.x |
| ESET Endpoint Antivirus для Windows | 5.x |
| ESET File Security для Microsoft Windows Server | 4.x |
| ESET NOD32 Antivirus 4 Business Edition для Mac OS X | 4.x |
| ESET NOD32 Antivirus 4 Business Edition для Linux Desktop | 4.x |
| ESET Mail Security для Microsoft Exchange Server | 4.x |
| ESET Mail Security для IBM Lotus Domino | 4.x |
| ESET Security для Microsoft Windows Server Core | 4.x |
| ESET Security для Microsoft SharePoint Server | 4.x |
| ESET Security для Kerio | 4.x |
| ESET NOD32 Antivirus Business Edition | 4.2.76 |
| ESET Smart Security Business Edition | 4.2.76 |
| ESET Mobile Security для Symbian | 1.x |
| ESET Mobile Security для Windows Mobile | 1.x |
| ESET Mobile Security для Android | 3.x |

**Поддерживаемые языки**

| Язык | Код |
|---|---|
| Английский (США) | ENU |
| Китайский (упрощенное письмо) | CHS |
| Китайский (традиционное письмо) | CHT |
| Французский (Франция) | FRA |
| Немецкий (Германия) | DEU |
| Итальянский (Италия) | ITA |
| Японский (Япония) | JPN |
| Корейский (Корея) | KOR |

| | |
|---|---|
| Польский (Польша) | PLK |
| Португальский (Бразилия) | PTB |
| Русский (Россия) | RUS |
| Испанский (Чили) | ESL |
| Испанский (Испания) | ESN |

# 2. Установка сервера ERA Server и консоли ERA Console

## 2.1 Требования

Решение ERAS работает как услуга, и поэтому для нее требуется ОС на основе Microsoft Windows NT. Хотя для работы сервера ERAS наличие версий операционной системы Microsoft Windows Server не обязательно, для надежной работы сервер ERAS рекомендуется устанавливать на серверные операционные системы. Компьютер, на котором установлена служба ERAS, должен быть постоянно подключен к сети и доступен для:

- клиентов (обычно рабочих станций);
- компьютеров с консолью ERA Console;
- других экземпляров сервера ERAS (в случае репликации).

**Примечание.** ESET Remote Administrator 5 поддерживает установку поверх предыдущих версий 21, в том числе миграцию данных.

### 2.1.1 Требования к программному обеспечению и базе данных

**ERA Server**

| | |
|---|---|
| 32-разрядные операционные системы: | Windows 2000 и более поздние версии (см. **примечание**) |
| 64-разрядные операционные системы: | Windows XP и более поздние |
| Базы данных: | Microsoft Access (встроенная)<br>Microsoft SQL Server 2005 или более поздней версии<br>MySQL 5.0 или более поздней версии<br>ORACLE 9i или более поздней версии<br><br>Щелкните здесь, чтобы узнать подробнее 19 |
| Установщик Windows: | 2.0 или более поздней версии |
| Веб-панель мониторинга: | Internet Explorer 7.0 или более поздней версии<br>Mozilla Firefox 3.6 или более поздней версии<br>Google Chrome 9 или более поздней версии |
| HTTP-сервер: | Те же требования, что и для сервера ERA Server, но при этом необходима ОС Windows XP с пакетом обновления 2 или более поздней версии. |
| Сеть: | Полноценная поддержка протокола IPv4<br><br>Поддержка IPv6 в Windows Vista и более поздних версиях |

**ERA Console**

| | |
|---|---|
| 32-разрядные операционные системы: | Windows 2000 и более поздние версии (см. **примечание**) |
| 64-разрядные операционные системы: | Windows XP и более поздние |
| Установщик Windows: | 2.0 или более поздней версии |
| Internet Explorer: | 7.0 или более поздней версии |

**Примечание**:

- ERA Console не поддерживается в Microsoft Windows Server Core 2008 и Microsoft Windows Server Core 2012.

ERA Server поддерживается в этих операционных системах, но не поддерживает интеграцию с базой данных Microsoft Access.

- Чтобы запустить ERA Console, редактор конфигурации ESET и средство ERA Maintenance Tool в ОС Windows 2000, необходимо, чтобы в системе был файл *gdiplus.dll*. Этот файл можно загрузить здесь. Извлеките файл из пакета установки и скопируйте его в каталог *C:\WINNT\system32*.
- Роль сервера HTTPS в ОС Windows 2000 не поддерживается, поэтому в данной операционной системе функции панели мониторинга и зеркала не будут работать в режиме HTTPS. Чтобы воспользоваться функцией «Панель мониторинга» в ОС Windows 2000 Server, измените настройки таким образом, чтобы панель мониторинга не запускалась по умолчанию в режиме HTTPS.
- В Windows 2000 не поддерживается удаленная установка для продуктов безопасности для Linux и MAC, а также некоторые функции действий «RDP» и «Завершение работы» консоли.
- В некоторых операционных системах для успешной автоматической установки требуется обновление доверенных корневых сертификатов. Для обновления этих сертификатов необходимо запустить службу Центра обновления Windows или вручную импортировать последние версии.
- Если настройка SMTP-доступа в меню **Служебные программы** > **Параметры сервера** > **Другие параметры** (для IIS или Exchange) выполняется с помощью учетной записи администратора, не исключено, что отправка исходящих сообщений не будет работать.
- Некоторые **сетевые действия** 37 («RDP», «Завершение работы») недоступны в Windows 2000.

### 2.1.2 Требования к быстродействию

Производительность сервера может меняться в зависимости от указанных ниже параметров.

1. **Используемая база данных**
   - База данных MS Access устанавливается по умолчанию с сервером. Это решение рекомендуется при обслуживании сотен клиентов. Однако размер базы данных ограничен 2 гигабайтами. Следовательно, потребуется активировать очистку на сервере и задать интервал (в меню **«Служебные программы»** > **«Настройки сервера»** > **«Обслуживание сервера»**) для удаления устаревших данных.
   - Другие базы данных (MySQL, MSSQL, ORACLE) нужно устанавливать отдельно, но они могут повысить быстродействие сервера. Важно использовать подходящие оборудования для каждого ядра СУБД (в основном для ORACLE) в соответствии с техническими рекомендациями его поставщика.
   - Если в качестве базы данных выбрана ORACLE, необходимо установить количество курсоров, превышающее значение **«Максимальное количество активных подключения»** (меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Дополнительно»**; значение по умолчанию — 500). Окончательное число курсоров должно учитывать количество серверов нижнего уровня (если используется репликации) и курсоров, которые используются другими приложениями для доступа к ядру СУБД.
   - Как правило, быстродействие сервера выше при использовании внешних баз данных (то есть установленных на другом физическом компьютере).
2. **Параметры интервала подключения клиентов**
   - В ESET Endpoint Security/ESET Endpoint Antivirus интервал подключения клиента по умолчанию равняется 10 минутам. Если нужно, чтобы состояние клиента обновлялось чаще или реже по сравнению с интервалом по умолчанию, можно настроить значение этого параметра. Помните, что более краткий интервал подключения клиентов повлияет на производительность серверов.
3. **Среднее число событий, сообщаемое клиентами за одно подключение**
   - Любые данные, отправленные клиентом серверу, перечисляются в определенном событии (например, журнал угроз, журнал событий, журнал сканирования, изменение конфигурации). Этот параметр нельзя изменить напрямую, но на него его можно повлиять при изменении других связанных с ним параметров. Например в дополнительной конфигурации сервера (в меню **«Сервис»** > **«Параметры сервера»** >

**«Обслуживание сервера»**) можно настроить максимальный размер журналов, принимаемых сервером (этот параметр включает клиентов, которые подключаются напрямую, а также реплицированных клиентов). В обычном режиме работы среднее значение за долгий период можно оценить под одному событию за каждые 4 часа для каждого клиента.

**4. Оборудование**

Для **установок небольшого масштаба (к серверу ERA подключается до 1000 клиентов):**

- Процессор — совместимый с Pentium IV, частотой 2 ГГц или более мощный
- ОЗУ — 2 ГБ
- Сетевой адаптер — 1 Гбит/с

Для **установок среднего масштаба (к серверу ERA подключается 1000–4000 клиентов)** рекомендуется раздельная установка на два компьютера.

Сервер ERA:

- Процессор — совместимый с Pentium IV, частотой 2 ГГц или более мощный
- ОЗУ — 2 ГБ
- Сетевой адаптер — 1 Гбит/с

Сервер базы данных:

- Процессор — совместимый с Pentium IV, частотой 2 ГГц или более мощный
- ОЗУ — 2 ГБ
- Сетевой адаптер — 1 Гбит/с

Также можно установить сервер ERA Server и базу данных на один компьютер:

- Процессор — совместимый с Pentium IV, многоядерный, частотой 3 ГГц или более мощный
- ОЗУ — 4 ГБ
- Сетевой адаптер — 1 Гбит/с
- Жесткий диск — массив RAID0 или SSD-диск или диски обоих типов

**ПРИМЕЧАНИЕ.**: В этом случае (установка сервера ERA и базы данных на одном компьютере) не рекомендуется использовать базу данных MS Access, поскольку из-за ограничения ее размера в 2 ГБ потребуется часто проводить ее очистку. Кроме того, следует помнить, что предельный размер баз данных MS SQL Express составляет 4 ГБ.

Для **установок крупного масштаба (к серверу ERA подключается 4000–10 000 клиентов)** рекомендуется раздельная установка на 2 компьютера и использование базы данных MS SQL или Oracle.

Сервер ERA:

- Процессор — совместимый с Pentium IV, многоядерный, частотой 3 ГГц или более мощный
- ОЗУ — 4 ГБ
- Сетевой адаптер — 1 Гбит/с

Сервер базы данных:

- Процессор — совместимый с Pentium IV, многоядерный, частотой 3 ГГц или более мощный
- ОЗУ — 4 ГБ
- Сетевой адаптер — 1 Гбит/с
- Жесткий диск — массив RAID0 или SSD-диск или диски обоих типов

**Для установок сверхкрупного масштаба (10 000–20 000 клиентов на один сервер ERA Server)** рекомендуется раздельная установка на 2 компьютера и использование базы данных MS SQL или Oracle.

Сервер ERA:

- Процессор — совместимый с Pentium IV, многоядерный, частотой 3 ГГц или более мощный
- ОЗУ — 8 ГБ
- Сетевой адаптер — 1 Гбит/с
- Жесткий диск — массив RAID0 или SSD-диск или диски обоих типов

Сервер базы данных:

- Процессор — совместимый с Pentium IV, многоядерный, частотой 3 ГГц или более мощный
- ОЗУ — 8 ГБ
- Сетевой адаптер — 1 Гбит/с
- Жесткий диск — массив RAID0 или SSD-диск или диски обоих типов

**ПРИМЕЧАНИЕ.**: Все конфигурации оборудования, перечисленные выше, содержат минимальные требования для запуска ERA. Для более высокой производительности рекомендуется использовать более мощные конфигурации. Настоятельно рекомендуется использовать минимальные рекомендации к оборудованию для операционной системы сервера с учетом количества обслуживаемых клиентов. Дополнительные сведения о типах используемых баз данных и их ограничениях см. в главе Типы баз данных, поддерживаемые сервером ERA Server 19.
Чтобы управлять еще большим числом клиентов, рекомендуется распределить нагрузку между несколькими серверами с должным образом настроенной репликацией.

**Перегрузка**

Если сервер перегружен (например, 20 тыс. клиентов подключается к серверу, который способен обслуживать только 10 тыс. клиентов с интервалом через каждые 10 минут), это приведет к пропуску некоторых подключенных клиентов. Если интервал подключения клиента настроен на 20 минут вместо 10 минут, то в среднем будет обслуживаться только каждое второе подключение клиента. Для каждого отказа в обслуживании в журнал будет записываться следующая информация: "*<SERVERMGR_WARNING> ServerThread: maximum number of threads for active connections reached (500), the server will skip this connection* (достигнуто максимальное количество потоков для активных подключений (500), сервер пропустит это подключение)". Отказ в обслуживании может также возникнуть при временных перегрузках сервера.

Это значение можно изменить в поле **«Максимальное количество активных подключений»** (по умолчанию — 500) в окне дополнительных параметров сервера, однако изменять его рекомендуется только в крайних случаях (например, при решении определенных проблем). При переизбытке системных ресурсов и производительности ядра СУБД этот параметр можно использовать для настройки общей производительности сервера.

**Передача данных по сети**

В штатном режиме работы сервера подразумевается, что клиент, подключающийся каждые 10 минут, за одно подключение будет сообщать о 0,04 события, что составляет 1 сообщение о событии каждые 4 часа для каждого клиента. При этом создается примерно 2 килобайта трафика на подключение.

При появлении вируса у клиента, который сообщает о 7 событиях при каждом подключении, трафик может возрасти до 240 килобайт на подключение. Если включено сжатие (по умолчанию), размер передаваемых данных будет примерно на 50% меньше, то есть примерно 120 килобайт на подключение.

Данные включают в себя прямые подключения клиентов без учета реплицированных подключений. Репликация происходит гораздо реже и предназначена для отправки новых событий с подчиненных серверов. События автоматически реплицируются и уровень их детализации настраивается в дополнительных параметрах сервера (в меню **«Сервис»** > **«Параметры сервера»** > **«Дополнительно»** > **«Изменить дополнительные параметры»** > **«Репликация»**). В разделе обслуживания сервера можно настроить максимальный уровень детализации журналов, принимаемых сервером верхнего уровня. Этот параметр применяется как к клиентам, подключающимся напрямую, так и к реплицированных клиентам).

**Требования к объему хранилища**

Для чистой установки ESET Remote Administrator с базой данных MS Access требуется до 60 МБ места на диске.

Основная часть хранилища занята событиями клиентов, которые хранятся в базе данных и в хранилище на

диске (папка по умолчанию — *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). Для ERA требуется не менее 5% свободного места на диске. В случае превышения этого минимума сервер не будете получать некоторые из клиентских событий. Этот параметр настраивается в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Дополнительно»** > **«Максимальное использование дискового пространства»**. Для штатной работы с параметрами очистки по умолчанию (удаление событий старше 3 месяцев) требуется около 10 ГБ свободного дискового пространства на 1 000 клиентов/

**Конкретный пример**

Сервер с базой данных MS Access, к которому клиенты подключаются каждые 5 минут и сообщают о 7 событиях (например, в журнале угроз, журнале событий, журнале сканирования, об изменениях конфигурации и т. д.) за подключение, в среднем может временно обслуживать до 3 тыс. клиентов. Этот сценарий описывает временную ситуацию перегрузки, например, сообщения о вспышке вируса и т. п.

Если сервер использует внешнюю базу данных MySQL, а интервал подключения клиентов установлен в 10 минут (0,02 события на подключение), то максимальное число клиентов, которых может обслуживать сервер, увеличивается до 30 тыс. Этот сценарий демонстрирует оптимальную производительность базы данных, где клиенты сообщают об относительно небольшом числе событий.

В штатном режиме при использовании базы данных MS Access и интервале подключения клиентов в 10 минут сервер в состоянии обслуживать более 10 000 клиентов.

### 2.1.3 Используемые порты

В приведенной ниже таблице перечислены все возможные сетевые соединения, используемые при установке сервера ERAS. Процесс EHttpSrv.exe принимает данные на TCP-порту 2221, а процесс era.exe — на портах 2222, 2223, 2224 и 2846. Все остальные соединения устанавливаются встроенными процессами операционной системы (например, NetBIOS через TCP/IP).

| Протокол | Порт | Описание |
|---|---|---|
| TCP | 2221 (прием данных сервером ERAS) | Порт по умолчанию, используемый функцией зеркала, встроенной в ERAS (HTTP-версия) |
| TCP | 2222 (прием данных сервером ERAS) | Обмен данными между клиентами и сервером ERAS |
| TCP | 2223 (прием данных сервером ERAS) | Обмен данными между ERAC и ERAS |

Для правильной работы всех компонентов программы должны быть открыты следующие сетевые порты:

| Протокол | Порт | Описание |
|---|---|---|
| TCP | 2224 (прием данных сервером ERAS) | Обмен данными между агентом *einstaller.exe* и ERAS в ходе удаленной установки |
| TCP | 2225 (прием данных сервером ERAS) | Обмен информацией между HTTP-сервером панели мониторинга ESET и ERAS |
| TCP | 2846 (прием данных сервером ERAS) | Репликация ERAS. |
| TCP | 2226 (консоль командной строки ERA) | Соединение между сервером ERAS и консолью командной строки |
| TCP | 139 (целевой порт со стороны сервера ERAS) | Копирование агента *einstaller.exe* с ERAS на клиента через ресурс общего доступа admin$ |
| UDP | 137 (целевой порт со стороны сервера ERAS) | Разрешение имен в ходе удаленной установки |
| UDP | 138 (целевой порт со стороны сервера ERAS) | Обзор файлов в ходе удаленной установки |

| | | |
|---|---|---|
| TCP | 445 (целевой порт со стороны сервера ERAS) | Прямой доступ к общим ресурсам по протоколу TCP/IP в ходе удаленной установки (вместо TCP 139) |

Заранее заданные порты 2221, 2222, 2223, 2224, 2225 и 2846 можно изменить, если они уже используются другими приложениями.

Чтобы изменить используемые по умолчанию порты ERA, выберите **«Сервис»** > **«Параметры сервера»**. Чтобы изменить порт 2221, откройте вкладку **«Обновления»** и измените значение параметра «Порт HTTP-сервера». Порты 2222, 2223, 2224, 2225 и 2846 можно изменить в разделе **«Порты»** на вкладке Другие параметры 136.

Заранее заданные порты 2222, 2223, 2224 и 2846 также можно изменить в расширенном режиме установки (ERAS).

### 2.1.4 Поиск компьютеров

Чтобы управлять нужными удаленными компьютерами через ERA Server, нужно, чтобы можно было проверять с ними связь (запрос проверки связи ICMP) с сервера ERA Server. Если нужный компьютер защищен файерволом, убедитесь, что порты, используемые 13 для связи с ERA Server, включены (не заблокированы файерволом).

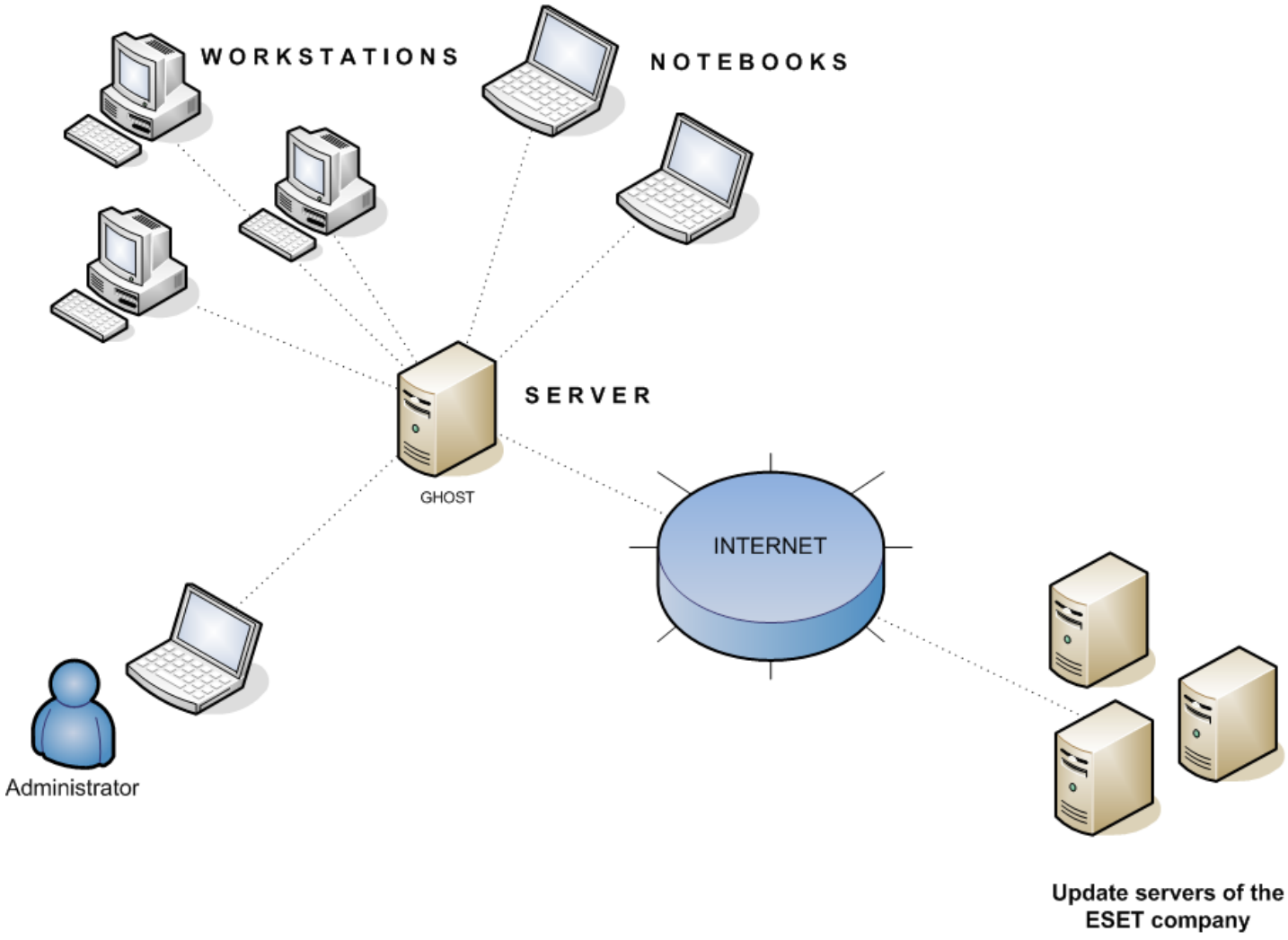
Компьютеры, видимые для сервера ERA Server, могут отображаться на вкладке **Компьютеры** вкладки **Удаленная установка** в консоли ERA Console. Список компьютеров основан на результатах выполнения **задачи поиска по умолчанию**. Вы можете изменить конфигурацию этой задачи или создать новую, щелкнув **Добавить новую** и выполнив инструкции **мастера задачи поиска в сети: способы сканирования** 52.

## 2.2 Основные рекомендации по установке

### 2.2.1 Обзор среды (структура сети)

Сеть компании обычно представляет собой одну локальную сеть (LAN), поэтому рекомендуется устанавливать сервер ERAS и сервер с зеркалом. Зеркало можно создать либо в ERAS, либо в ESET Endpoint Antivirus/ESET Endpoint Security.

Предположим, что все клиенты являются рабочими станциями и ноутбуками под управлением Microsoft Windows и находятся в одном домене. Сервер GHOST постоянно подключен к сети и может быть рабочей станцией с операционной системой Windows, Professional или Server Edition (он не обязан быть сервером Active Directory). Кроме того, предположим, что переносные компьютеры отсутствуют в сети компании во время установки клиентских решений ESET. Структура сети может быть похожей на приведенную ниже схему:




### 2.2.2 Перед установкой

Перед установкой с веб-узла компании ESET необходимо загрузить следующие установочные пакеты.

**Компоненты ESET Remote Administrator:**

ESET Remote Administrator — сервер
ESET Remote Administrator — консоль

**Клиентские и серверные решения ESET:**

См. раздел Поддерживаемые продукты и языки 7.

**ПРИМЕЧАНИЕ.**: Загружайте только те клиентские решения, которые будут использоваться на рабочих станциях-клиентах.

### 2.2.3 Установка

#### 2.2.3.1 Установка сервера ERA Server

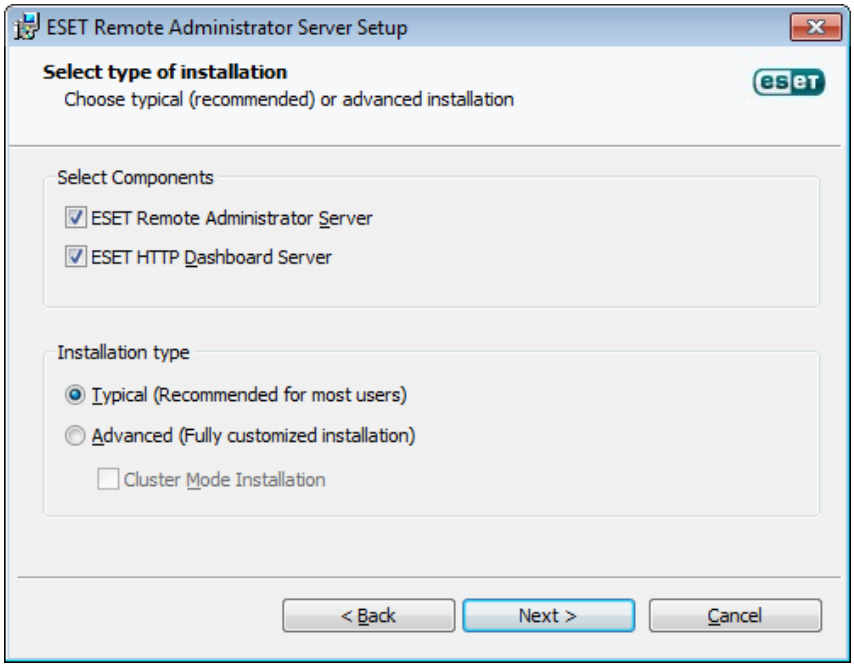
Установите сервер ERAS на сервер с именем GHOST (см. пример в разделе Обзор среды 15). Чтобы начать, выберите компоненты, которые следует установить. Есть два параметра: сервер **ESET Remote Administrator Server** и **HTTP-сервер Панели мониторинга 46 ESET**.

Для большинства приложений устанавливаются оба компонента. Можно выбрать установку двух компонентов на разные компьютеры (например, установить HTTP-сервер панели мониторинга ESET на видимый всем пользователям компьютер, а сервер ERAS установить на компьютер, который доступен только из локальной внутренней сети). Или можно отказаться от использования HTTP-сервера панели мониторинга ESET.

**ПРИМЕЧАНИЕ.**: Рекомендуется устанавливать сервер ERAS на компьютер под управлением серверной операционной системы.

**ПРИМЕЧАНИЕ.**: Сервер панели мониторинга и сервер зеркала используют один и то же HTTP-сервер (который устанавливается автоматически). Даже если вы отмените выбор сервера панели мониторинга во время установки, вы сможете позднее выбрать его снова в редакторе конфигурации ESET. (Для этого выберите **ERAC** > **Сервис** > **Параметры сервера** > **Дополнительно** > **Панели мониторинга** > **Использовать локальную панель мониторинга**).

После выбора нужных компонентов выберите **обычный** или **расширенный** режим установки.




- Если выбрать **«Обычный режим»**, потребуется указать лицензионный ключ (файл с расширением LIC или ZIP), который позволяет серверу ERAS работать в течение времени, определяемого лицензией. Затем надо будет настроить параметры обновления (имя пользователя, пароль и сервер обновления). Можно также перейти к следующему шагу и ввести параметры обновления позднее. Для этого установите флажок рядом с параметром **«Установить параметры обновления позже»** и нажмите кнопку **«Далее»**.
- Если выбрать **«Установку в расширенном режиме»**, вы сможете настроить дополнительные параметры установки. Значения этих параметров можно изменить позже в консоли ERAC, но в большинстве случаев в этом нет необходимости. Единственным исключением является имя сервера, которое должно совпадать с именем DNS, значением %COMPUTERNAME % операционной системы или же IP-адресом, присвоенным данному компьютеру. Это самый важный элемент данных при удаленной установке. Если во время установке не указать имя, программа установки автоматически воспользуется значением переменной % COMPUTERNAME%, которого в большинстве случаев будет достаточно. Также необходимо выбрать базу данных, в которой будет храниться информация ERAS. Дополнительные сведения см. в разделе Типы баз данных, поддерживаемых ERA Server 19. См. также раздел Установка в режиме кластера 17.

**ПРИМЕЧАНИЕ.**: При установке ERAS на операционную систему Windows 2000 не рекомендуется использовать DNS, используйте вместо этого полную строку соединения.

***Внимание!*** Политики безопасности ОС Microsoft Windows ограничивают разрешения учетной записи локального пользователя. Как следствие, вы не сможете выполнять связанные операции в сети. Если служба ERA работает под учетной записью локального пользователя, могут возникнуть проблемы с автоматической установкой (например, при удаленной установке из домена в рабочей группе). В системах Windows Vista, Windows Server 2008 или Windows 7 рекомендуется запускать службу ERA под учетными записями с достаточными разрешениями доступа к сети. В **Расширенном режиме установки** можно указать учетную запись, от имени которой должна выполняться служба ERA.

**Примечание**: Хотя сервер ERA Server полностью поддерживает кодировку Юникод, в некоторых ситуациях (например, при обработке сообщений электронной почты или имен компьютеров) он преобразует символы в кодировку ANSI или наоборот. В таких ситуациях необходимо использовать параметр **«Язык программ, не поддерживающих Юникод»**. Даже если используется нелокализованная версия ERA (т. е. версия на одном из вариантов английского языка), рекомендуется изменить этот параметр, чтобы он соответствовал языку среды, в которой находится сервер. Чтобы найти этот параметр, выберите **Панель управления** > **«Язык и региональные стандарты»** и откройте вкладку **«Дополнительно»**.

По умолчанию программные компоненты сервера ERAS устанавливаются в папку

*%ProgramFiles%\ESET\ESET Remote Administrator\Server*

Все остальные компоненты (такие как журналы, пакеты установки, конфигурация и др.) хранятся в папке

*%ALLUSERSPROFILE%\Application Data \ESET\ESET Remote Administrator\Server*

ERAS запускается автоматически после установки. Результаты текущей работы службы ERAS записываются в файл

*%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log*

**Установка из командной строки**

Сервер ERAS можно установить с помощью следующих параметров командной строки.

*/q* — автоматическая установка. Вмешательство пользователя невозможно. Диалоговые окна не отображаются.

*/qb* — вмешательство пользователя невозможно, но ход установки отображается на индикаторе.

Пример *era_server_nt32_ENU.msi /qb*

Параметры и конфигурация установки из командной строки могут быть дополнены конфигурационным *XML*-файлом администратора *cfg.xml*, который должен находиться в каталоге с установочным *msi*-файлом ERA. Файл конфигурации можно создать в редакторе ESET Configuration Editor. Этот файл позволяет настроить различные параметры ERA. Дополнительные сведения см. в разделе ESET Configuration Editor 67.

#### 2.2.3.1.1 Установка в режиме кластера

Сценарий **расширенной установки** позволяет активировать **установку в режиме кластера**. При установке в режиме кластера можно указать путь к папке общих данных кластера, которая полностью доступна для всех узлов кластера (то есть у всех узлов должен быть доступ на чтение и запись в эту папку). Это может быть кворумный диск кластера либо сетевой путь к общей папке. Если используется общая папка, необходимо включить общий доступ для **компьютеров** в свойствах этой папки. В группу **«Разрешения»** необходимо добавить имя узла кластера с полными правами.

**ПРИМЕЧАНИЕ.**: При указании общей папки кластера не рекомендуется использовать IP-адрес.

Необходимо установить сервер ERA Server на все узлы кластера. После каждой установки ERA Server необходимо изменить автоматический запуск службы ERA на ручной. После установки ERA Server на всех узлах создайте универсальную службу (era_server). Универсальная служба должна зависеть от ресурса сетевого имени в консоли администрирования кластера.

Если используется база данных, отличная от встроенной MS Access, необходимо убедится, что все узлы ERA Server подключены к той же базе данных. На следующих этапах также важно задать имя узла кластера, где в качестве имени сервера должно быть установлено ERA.

***Внимание!*** В консоли администратора кластера необходимо настроить службу ESET Remote Administrator Server (ERA_SERVER) как обычную службу кластера.

**Удаление**

Если планируется удаление ERA Server, кластерная группа должна быть включена, чтобы можно было выполнить процесс удаления.

1. Разделите кластер, отключив один из его узлов.

2. Дождитесь завершения отработки отказа, чтобы убедиться, что другие узлы работают.

3. Удалите ESET Remote Administrator с отключенного узла.

4. Перезапустите узел.

5. Подключите узел.

6. Повторите приведенные выше действия для всех дополнительных узлов кластера.

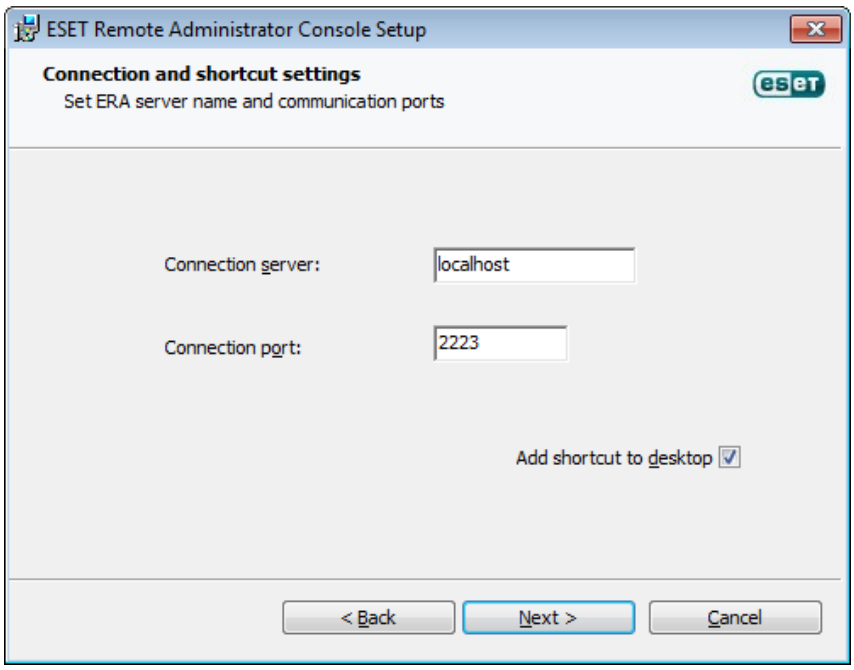
**Обновление ERA при установке в режиме кластера**

При переустановке в режиме кластера необходимо отключить кластерную группу службы ERA, выбрав команду **«Отключить»** в консоли администрирования кластера. Затем переустановите ERA на всех узлах кластера и снова переведите кластерную группу служб ERA в рабочий режим.

### 2.2.3.2 Установка консоли ERA Console

Установите ESET Remote Administrator Console на компьютер администратора или напрямую на сервер.

На завершающем этапе установки в расширенном режиме введите название сервера ERA Server (или его IP-адрес), к которому консоль ERAC будет автоматически подключаться при запуске. В нашем примере он назван GHOST.




После установки запустите консоль ERAC и проверьте соединение с сервером ERAS. По умолчанию для подключения к серверу ERA Server пароль не требуется (текстовое поле пароля пустое), однако настоятельно рекомендуется его установить. Чтобы создать пароль для подключения к серверу ERA Server, вызовите команду **«Файл»** > **«Изменить пароль...»** и изменить пароль для консоли, нажав кнопку **«Изменить...»**.

**ПРИМЕЧАНИЕ.** Администратор может указать учетную запись пользователя и пароль для доступа к ESET

Remote Administrator Console. Администратор также может указать уровень доступа. Дополнительные сведения см. в разделе Диспетчер пользователей 124. ERAC необходимо установить на компьютере, с которого вы будете заходить на ERAS под учетной записью, указанной в диспетчере пользователей.

#### 2.2.3.3 Зеркало

С помощью консоли ERA Console можно активировать сервер обновления в локальной сети — зеркало сервера ERA Server. Сервер затем можно использовать для обновления рабочих станций сети. Включение зеркала позволяет уменьшить объем данных, передаваемых через подключение к Интернету.

Выполните указанные ниже действия.

1) Подключите консоль ERA Console к серверу ERA Server, выбрав команду **Файл** > **Подключить**.
2) В консоли ERA Console выберите команду **Сервис** > **Параметры сервера** и откройте вкладку **Обновления**.
3) В раскрывающемся меню **Сервер обновлений** выберите команду **Выбирать автоматически** и установите 60-минутный интервал обновления. Укажите «Имя пользователя обновления» (EAV-***), нажмите кнопку **Установить пароль** и введите или вставьте из буфера обмена пароль, полученный с именем пользователя.
4) Выберите команду **Создать зеркало обновления**. Оставьте путь по умолчанию для дублируемых файлов и порт сервера HTTP (2221). Для параметра «Аутентификация» оставьте значение «Нет».
5) Щелкните вкладку **Дополнительно** и щелкните **Изменить дополнительные параметры**. В дереве расширенных параметров перейдите к серверу ERA Server > **Настройки** > **Зеркало** > **Создать зеркало для выбранных компонентов программы**. Нажмите кнопку **Изменить** справа и выберите компоненты программы для загрузки. Выберите все языковые версии компонентов, которые будут использоваться в данной сети.
6) На вкладке **Обновления** нажмите кнопку «Обновить сейчас», чтобы создать **Зеркало**.

Дополнительные сведения о параметрах конфигурации зеркала см. в разделе Включение и настройка зеркала 135.

#### 2.2.3.4 Типы баз данных, поддерживаемые сервером ERA Server

По умолчанию в программе используется ядро Microsoft Access (СУБД Jet). ERAS 5 также поддерживает следующие базы данных:

- Microsoft SQL Server 2005 или более поздней версии
- MySQL 5.0 или более поздней версии
- Oracle 9i или более поздней версии

Тип СУБД можно выбрать при установке сервера ERAS в расширенном режиме. После установки изменить тип СУБД непосредственно из ERA будет невозможно, однако это можно сделать с помощью средства ERA Maintenance Tool 175.

**Примечание.**

- База данных Microsoft Access не поддерживается в версиях Windows Server Core 2008 и Windows Server Core 2012.
- Для SQL Server Express максимальный размер баз данных составляет 4 Гб.
- Максимальный размер баз данных Microsoft Access составляет 2 ГБ.
- При использовании MySQL в ОС Microsoft Windows 2000 для установки подключения к базе данных рекомендуется использовать драйвер ODBC версии 5.1.8 или более поздней версии 21.
- В случае MySQL сервер ERAS по умолчанию использует ядро СУДБ MyISAM. Если вы предпочитаете InnoDB, вы можете изменить сценарий создания базы данных во время расширенной установки ERAS.

#### 2.2.3.4.1 Основные требования

Сначала необходимо создать базу данных на сервере базы данных. Программа установки сервера ERAS может создать пустую базу данных MySQL, которой автоматически присваивается имя ESETRADB.

По умолчанию программа установки автоматически создает новую базу данных. Чтобы создать базу данных вручную, нажмите кнопку **«Экспортировать сценарий»**. Флажок **«Автоматически создать таблицы в новой базе данных»** должен быть снят.

**Параметры сравнения**

Сортировка будет выполняться согласно параметрам по умолчанию в каждой базе данных. При необходимости активируйте параметра CASE INSENSIVITY (CI) (нечувствительность к регистру).

Чтобы активировать:

- для MS SQL и MySQL необходимо установить параметр COLLATE с активированным CI;
- для ORACLE необходимо установить параметр NLS_SORT с активированным CI;
- для MS Access никаких действий предпринимать не надо, поскольку CI уже активирован.

**Кодировка**

Очень важно использовать кодировку UNICODE (рекомендуется UTF-8), особенно если у клиентов настроены определенные региональные параметры или если сервер ERA работает в локализованной версии. Если репликация не планируется, и все клиенты подключены к одному серверу, можно использовать кодировку для локализованной версии ERA, которая устанавливается.

**Проверка подлинности**

Рекомендуется использовать применяемую по умолчанию проверку подлинности базы данных. При использовании проверки подлинности домена или Windows проверьте, имеет ли ваша учетная запись достаточно прав, чтобы подключаться к базе данных. При использовании сервера Microsoft SQL Server используйте формат строки DSN-подключения 21.

**MARS (несколько активных результирующих наборов)**

Если используется база данных MS SQL, для надежной работы требуется ODBC-драйвер с поддержкой MARS. В противном случае сервер будет работать менее эффективно, и в журнал сервера будет зарегистрировано следующее сообщение об ошибке:

*Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information.* (Ошибка подключения к базе данных. Настоятельно рекомендуется использовать ODBC-драйвер, который поддерживает MARS. Сервер будет продолжать работать, но может замедлиться связь с базой данных. Дополнительные сведения см. в документации или обратитесь в службу поддержки ESET.)

Если проблема возникает с другой базой данных (не MS SQL), сервер регистрирует следующее сообщение в журнале сервера и останавливается:

*Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information.* (Ошибка подключения к базе данных. Может помочь обновление ODBC-драйвера. За дополнительными сведения обращайтесь в службу поддержки ESET.)

Драйверы без поддержки MARS:

- SQLSRV32.DLL (2000.85.1117.00).
- SQLSRV32.DLL (6.0.6001.18000) — изначально есть в ОС Windows Vista и Windows Server 2008.

Драйвер с поддержкой MARS:

- SQLNCLI.DLL (2005.90.1399.00).

#### 2.2.3.4.2 Настройка подключения к базе данных

После создания новой базы данных необходимо задать параметры подключения к серверу базы данных одним из следующих способов.

1. С использованием DSN (имени источника данных).
   Чтобы вручную указать DSN, запустите
   администратор источников данных (OBDC)
   Нажмите кнопку **«Пуск» > «Выполнить»** и введите *odbcad32.exe*).

   Пример DSN-соединения:
   *DSN =ERASqlServer*

   ***Внимание!*** Для нормальной работы ERA рекомендуется использовать *System DSN*.

   ***Внимание!*** В 64-разрядной операционной системе файл *odbcad32.exe* необходимо запустить из папки *%SystemRoot%\SysWOW64*.

Для успешной установки с MS SQL с проверкой подлинности Windows или в домене необходимо использовать формат DSN при вводе строки соединения.

2. Напрямую с использованием полной строки соединения.
   Необходимо указать все обязательные параметры: драйвер, сервер и название базы данных.

   Вот пример полной строки соединения для сервера MS SQL:
   *Driver ={SQL Server}; Server =имя_сервера; Database =ESETRADB*

   Вот пример полной строки соединения для сервера Oracle:
   *Driver ={Oracle in instantclient10_1}; dbq =имя_сервера: 1521/ESETRADB*

   Вот пример полной строки соединения для сервера MySQL:
   *Driver ={MySQL ODBC 3.51 Driver}; Server =имя_сервера; Database =ESETRADB*

   Нажмите кнопку **«Установить»** и укажите **«Имя пользователя»** и **«Пароль»** для подключения. Для подключения к базам данных Oracle и MS SQL Server также требуется **Название схемы**.

   Нажмите кнопку **«Проверить соединение»**, чтобы проверить соединение с сервером базы данных.

**ПРИМЕЧАНИЕ.** Вместо проверки подлинности Windows или домена рекомендуется использовать проверку подлинности сервера базы данных.

#### 2.2.3.5 Установка поверх предыдущих версий

ESET Remote Administrator 5.3 поддерживает установку поверх предыдущих версий и миграцию данных. Не нужно выполнять миграцию с ESET Remote Administrator 5.0. Миграция данных ESET Remote Administrator 4.x возможна, но больше не поддерживается.

**ПРИМЕЧАНИЕ.**: Рекомендуется проводить переустановку только при отсутствии подключенных клиентов, поскольку при переустановке служба сервера ERA останавливается, а все подключения завершаются. Перенести базу данных можно до или после переустановки (подробнее см. в главе Передача базы данных 176).

**Установка сервера ERA Server**

1. Загрузите установочный файл на сервер. Дважды щелкните установочный файл, чтобы начать установку.
2. Выберите обычную или расширенную установку, аналогично чистой установке ERA Server 16.

- **«Обычная установка»** — потребуется указать файл лицензионного ключа (LIC-файл), пароли и данные обновления. Поддерживаются два режима миграции. В режиме **Импорт только конфигурации** в новой базе

данных создаются пустые таблицы. В режиме **Полный импорт** импортируются все данные из базы данных. Если выбрать **«Создать резервную копию текущей базы данных»** (по умолчанию), то перед любыми изменениями базы данных будет создана ее резервная копия. Для улучшения обслуживания базы данных можно выбрать параметр **Активировать автоматическую очистку по умолчанию для устаревших записей**.

- **Расширенная установка**: потребуется указать файл лицензионного ключа (*.lic), учетную запись для запуска службы сервера ERA, порты для передачи данных, пароли и данные обновления, а также параметры SMTP-сервера (не обязательно), параметры ведения журнала 127 и параметры миграции базы данных (описание см. выше в разделе **Обычная установка**). В процессе расширенной установки можно перенести данные старых политик (рабочие станции Windows версий 3 и 4) в новые (рабочие станции Windows версии 5). При миграции используются параметры по умолчанию, поэтому для настройки миграции рекомендуется использовать мастер миграции политик 99 после завершения обновления.

**ПРИМЕЧАНИЕ.** Если установщик обнаружит в текущей базе данных существующие таблицы, появится запрос. Чтобы перезаписать содержимое существующей таблицы, выберите команду **Перезаписать** (***Предупреждение.*** В результате содержимое таблиц будет удалено, а их структура перезаписана.) Чтобы оставить таблицы без изменений, выберите команду **«Пропустить»**. Выбор команды **«Пропустить»** в определенных условиях может привести к ошибкам несогласованности базы данных, особенно в ситуации, когда таблицы повреждены или несовместимы с текущей версией.

Если необходимо выполнить анализ текущей базы данных вручную, нажмите кнопку **Отмена**, чтобы прервать установку ERAS.

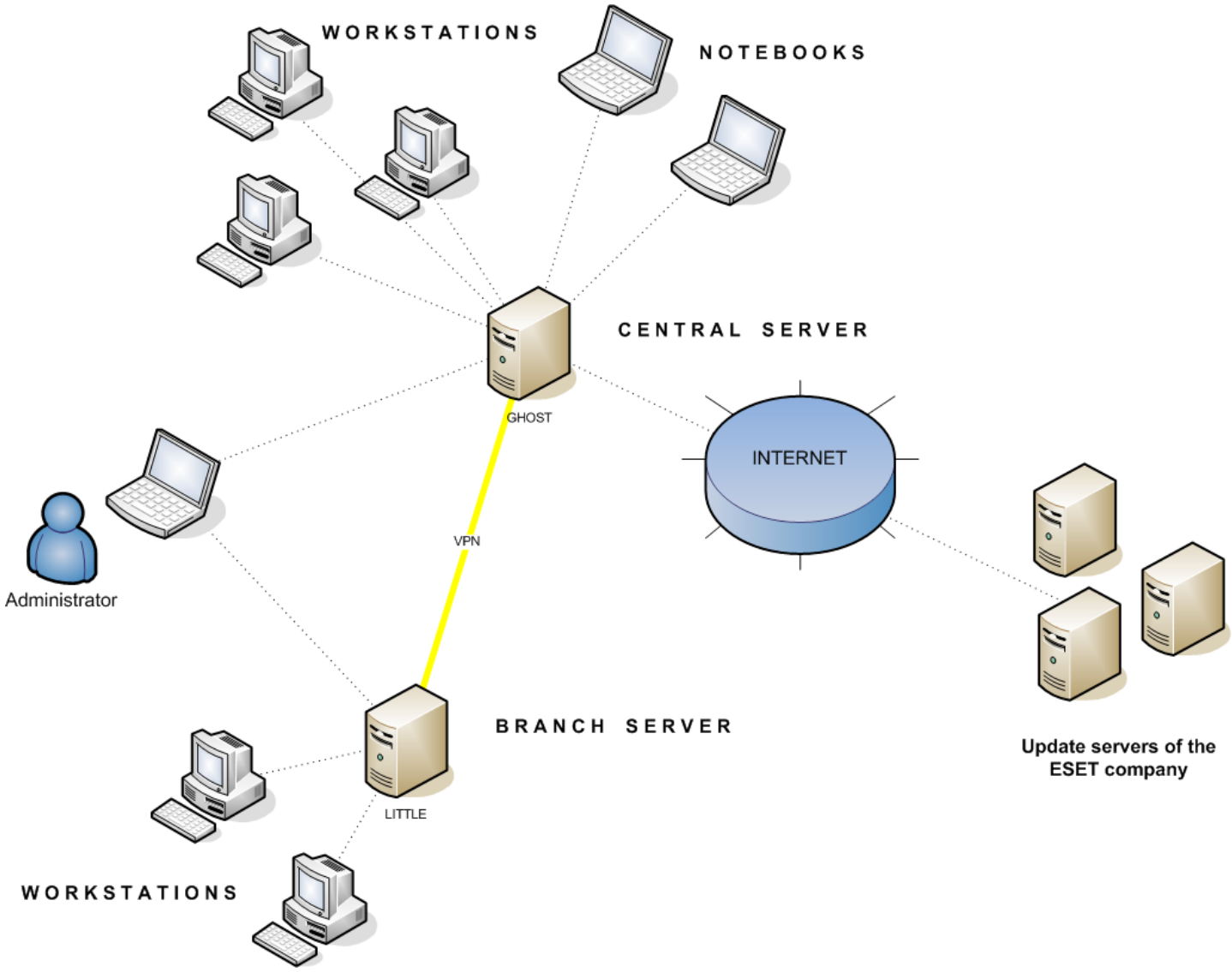
**Установка консоли ERA Console**

1. Загрузите установочный файл на сервер. Дважды щелкните установочный файл, чтобы начать установку.
2. Действуйте согласно указаниям в главе Установка ERA Console 18.

## 2.3 Сценарий: установка в корпоративной среде

### 2.3.1 Обзор среды (структура сети)

Ниже представлена копия вышеописанной сетевой структуры, в которую включен один дополнительный филиал, несколько клиентов и один сервер под именем LITTLE. Предположим, что для связи между головным офисом и филиалом используется медленное VPN-соединение. В этом сценарии зеркало следует установить на сервер LITTLE. Также установим на сервер LITTLE второй сервер ERA Server, чтобы создать более удобную для пользователя среду и свести к минимуму объем передаваемых данных.

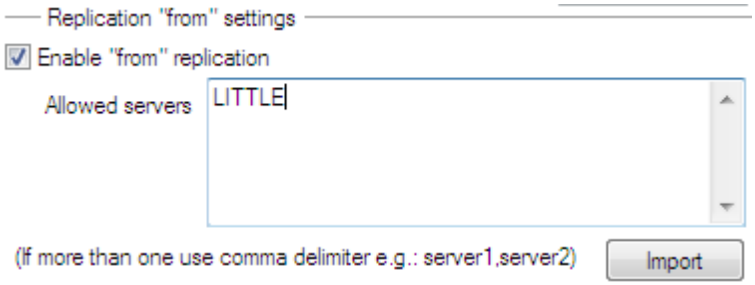


### 2.3.2 Установка

#### 2.3.2.1 Установка в головном офисе

Установка ERAS, ERAC и клиентских рабочих станций очень похожа на установку в предыдущем сценарии. Единственным отличием является конфигурация главного сервера ERAS (GHOST). В меню **«Служебные программы»** > **«Настройки сервера...»** > **«Репликация»** установите флажок **«Включить репликацию "из"»** и введите имя дополнительного сервера в группе **«Разрешенные серверы»**. В нашем случае сервер нижнего уровня называется LITTLE.

Если на сервере верхнего уровня задан пароль для репликации (**«Служебные программы»** > **«Настройки сервера...»** > **«Безопасность»** > **«Пароль для репликации»**), этот пароль нужно использовать для аутентификации на сервере нижнего уровня.




#### 2.3.2.2 Филиал: установка сервера ERA Server

Как и в примере выше, установите дополнительные сервер ERAS и консоль ERAC. Снова активируйте и настройте параметры репликации. В этот раз установите флажок **«Включить репликацию»** (**«Служебные программы»** > **«Настройки сервера...»** > **«Репликация»**) и укажите имя главного сервера ERAS. Рекомендуется указать IP-адрес основного сервера, то есть IP-адрес сервера GHOST.


#### 2.3.2.3 Филиал: установка HTTP-сервера зеркала

В этом случае также можно использовать конфигурацию установки зеркала, описанную в предыдущем сценарии. Единственные отличия заключаются в разделах, в которых определяются имя пользователя и пароль.

Как показано на рисунке из раздела Обзор среды 23, обновления для филиала загружаются не с серверов обновления компании ESET, а с сервера в головном офисе (GHOST). Источник обновления определяется следующим URL-адресом:

*http://ghost:2221 (или http://IP_сервера_ghost:2221)*

По умолчанию не нужно указывать имя пользователя или пароль, поскольку интегрированному HTTP-серверу не требуется аутентификация.

Дополнительные сведения о настройке зеркала ERAS см. в разделе Зеркало сервера 133.

#### 2.3.2.4 Филиал: удаленная установка на клиентах

В этом случае также можно использовать предыдущую модель с тем отличием, что все действия можно выполнять в консоли ERAC, напрямую подключенной к серверу ERAS филиала (в нашем примере: LITTLE). Это делается для предотвращения передачи установочных пакетов по каналу VPN, на котором скорость обмена данными является более низкой.

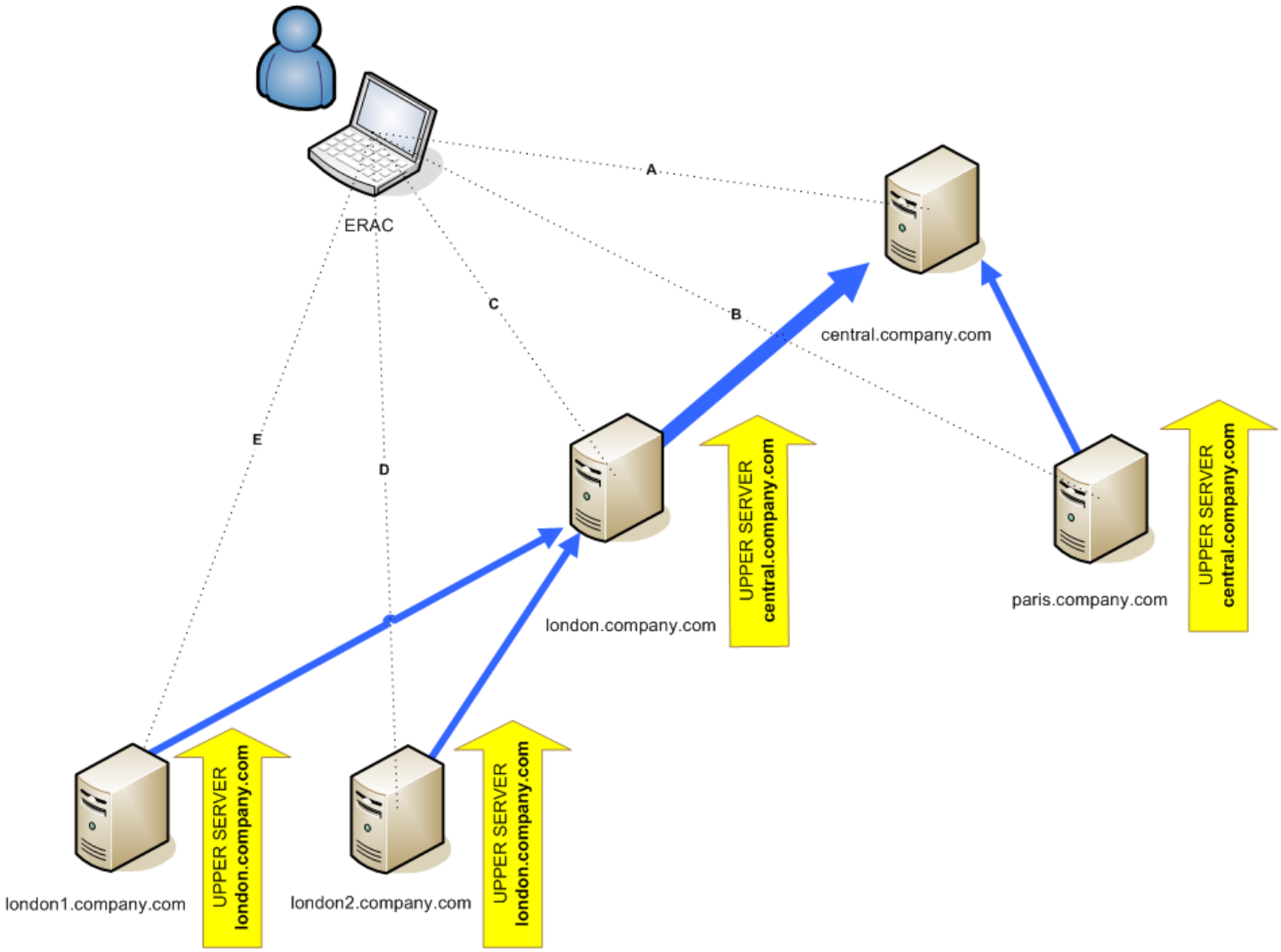
### 2.3.3 Прочие требования к корпоративным средам

В больших сетях можно устанавливать несколько серверов ERA Server для удаленной установки на клиентских компьютерах с более доступных серверов. Для этого север ERAS предлагает функцию *репликации* (см. разделы Установка в головном офисе 24 и Филиал: установка сервера ERA Server 24), которая позволяет хранить сведения, перенаправляемые родительскому серверу ERAS (*сервер верхнего уровня*). Репликацию можно настроить с помощью консоли ERAC.

Функция репликации очень полезна для компаний, в состав которых входит несколько филиалов или удаленных офисов. Сценарий развертывания данной модели описан ниже. Установите сервер ERAS в каждом офисе и реплицируйте их на центральный сервер ERAS. Преимущество этой конфигурации особенно очевидно в частных сетях, подключенных через VPN, в которых скорость передачи обычно является более низкой — администратору нужно будет подключаться только к центральному серверу ERAS (соединение, помеченное буквой A на рисунке ниже). При этом нет необходимости в использовании сети VPN для доступа к отдельным подразделениям (соединения B, C, D и E). Обход более медленного канала связи делает возможным репликация сервера ERAS.

Настройка репликации позволяет администратору определять сведения, которые будут автоматически передаваться серверам верхнего уровня через заданный интервал времени, и сведения, которые будут отправляться по запросу администратора сервера верхнего уровня. Репликация делает интерфейс ERA более удобным для пользователя, а также позволяет снизить объем сетевого трафика.

Еще одно преимущество репликации состоит в том, что несколько пользователей могут входить в систему с разными уровнями разрешений. Администратор, который через консоль обращается к серверу ERAS по адресу london2.company.com (соединение D), может управлять только теми клиентами, которые подключены к веб-узлу london2.company.com. Администратор, который обращается к центральному узлу по адресу company.com (A), может управлять всеми клиентами, размещенными в головном офисе, в отделениях и филиалах.


ERAC
A
B
C
D
E
central.company.com
london.company.com
paris.company.com
UPPER SERVER central.company.com
UPPER SERVER central.company.com
UPPER SERVER london.company.com
UPPER SERVER london.company.com
london1.company.com
london2.company.com

# 3. Работа с консолью ERA Console

## 3.1 Подключение к серверу ERA Server

Основная часть функций ERAC становится доступной только после подключения к ERAS. Перед подключением укажите имя или IP-адрес сервера следующим образом:

Откройте ERAC и выберите в меню команду **«Файл»** > **«Изменить соединения…»** (или **«Служебные программы»** > **«Настройки консоли…»**) и откройте вкладку **«Соединение»**.

Нажмите кнопку **«Добавить/удалить...»**, чтобы добавить новые серверы ERA Server или изменить перечисленные. Выберите нужный сервер в раскрывающемся меню **«Выбор соединения»**. Затем нажмите кнопку **«Подключиться»**.

**ПРИМЕЧАНИЕ.**: Консоль ERAC полностью поддерживает протокол IPv6. Адрес должен быть указан в формате *[ipv6-адрес]:порт*, например *[::1]:2223*.

Другие параметры в этом окне описаны ниже.

- **«Подключиться к выбранному серверу при запуске консоли»**. Если выбрать этот параметр, консоль автоматически подключится к выбранному серверу ERAS при запуске.
- **«Показать сообщение при ошибке соединения»**. Если при обмене данными между ERAC и ERAS возникает ошибка, на экран выводится предупреждение.

Существует два типа аутентификации.

**ERA Server**

Аутентификация пользователя с применением учетных данных ERAS. По умолчанию для подключения к серверу ERAS пароль не требуется, однако настоятельно рекомендуется его установить. Чтобы создать пароль для подключения к серверу ERAS, выполните указанные ниже действия.

Выберите в меню **«Файл»** > **«Изменить пароль»** (или **«Сервис»** > **«Параметры сервера»** > **«Безопасность»**), а затем нажмите кнопку **«Изменить»** возле параметра **«Пароль для консоли»**.

При вводе пароля можно установить флажок **«Запомнить пароль»**. Прежде чем воспользоваться им, оцените возможный риск для безопасности. Чтобы удалить все сохраненные пароли, выберите в меню **«Файл»** команду **«Удалить пароли из кэша...»**.

Чтобы установить или сменить учетные записи пользователей для аутентификации «консоль-сервер», используйте служебную программу Диспетчер пользователей 124.

**«Windows/домен»**

Аутентификация пользователей осуществляется с применением учетных данных Windows/домена. Чтобы аутентификация Windows или домена выполнялась правильно, установите ERAS с помощью учетной записи Windows или домена с достаточным уровнем доступа. Эта функция включается с помощью следующей команды: меню **«Служебные программы»** > **«Настройки сервера…»** > вкладка **«Дополнительно»** > **«Изменить дополнительные настройки…»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Безопасность»**.

Параметр **«Разрешить аутентификацию в Windows и домене»** включает или отключает аутентификацию в Windows и домене.

Параметр **«Группы администраторов»** позволяет указать группы, для которых будет включена аутентификация в Windows и домене.

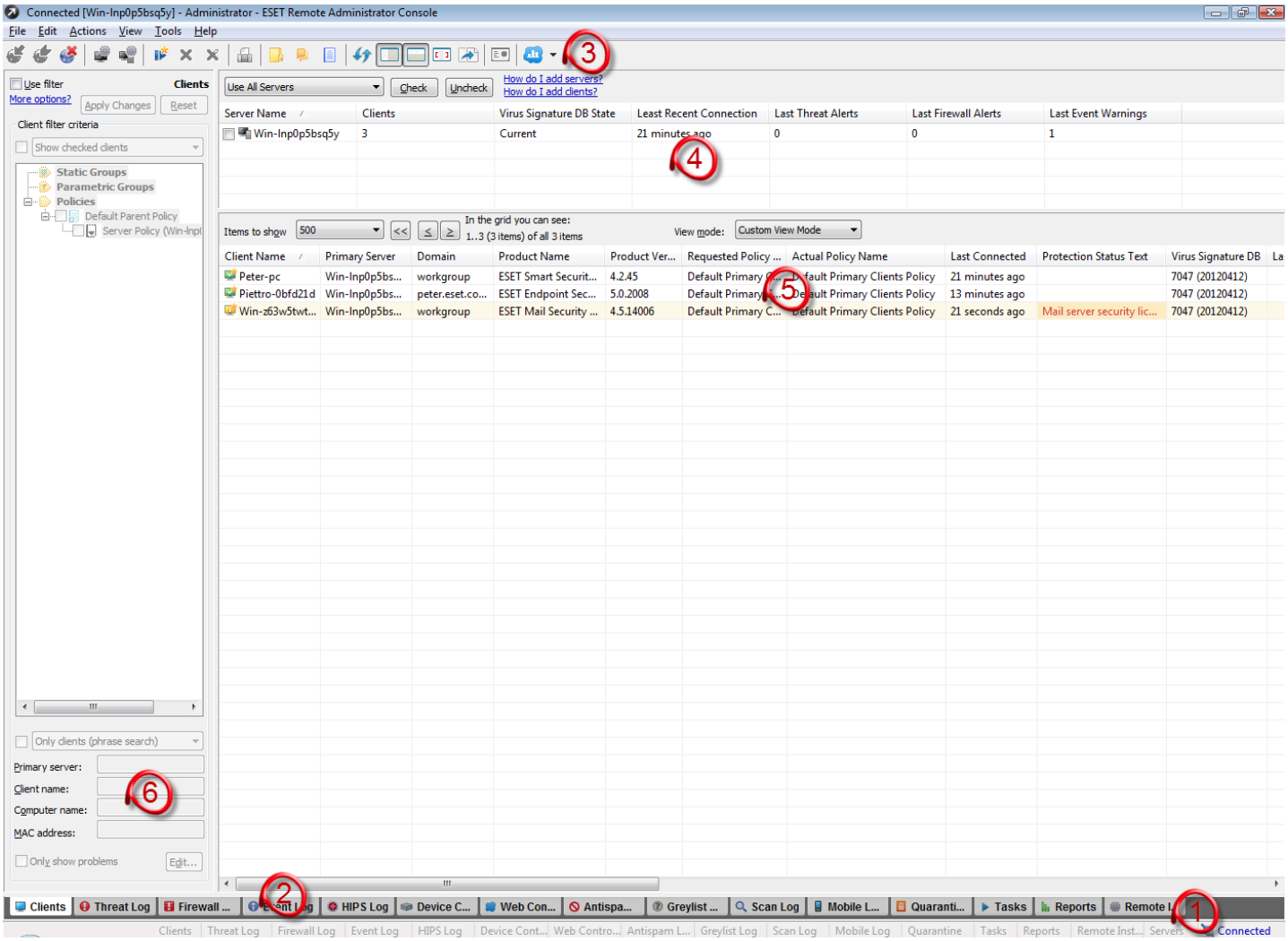
Параметр **«Группы только для чтения»** позволяет указать группы с доступом только для чтения.

После установки соединения заголовок программы изменится на строку **«Подключено к [имя_сервера]»**.

Кроме того, для подключения к серверу ERAS можно выбрать в меню **«Файл»** команду **«Подключение»**.

**Примечание.** Данные, которыми обмениваются ERAC и ERAS, шифруются по алгоритму AES-256.

## 3.2 Главное окно консоли ERA Console




Текущее состояние подключения между ERAC и ERAS отображается в строке состояния (**«1»**). Все необходимые данные регулярно обновляются с сервера ERAS (по умолчанию каждую минуту — См. **«Сервис»** > **«Настройки консоли»**> **«Другие параметры»**> **«Автообновление (мин.)»**. Ход обновления также отображается в строке состояния.

**Примечание.** Для обновления отображаемых данных нажмите клавишу F5.

Информация распределена по нескольким вкладкам 32 в порядке ее значимости (**«2»**). Большая часть данных на вкладках относится к подключенным клиентам. В большинстве случаев данные можно отсортировать в возрастающем или в убывающем порядке, щелкнув их заголовок (**«5»**), и переупорядочить с помощью операции перетаскивания. Число обрабатываемых строк данных можно ограничить с помощью раскрывающегося меню **«Элементы для отображения»** и кнопок **«Просмотр страниц одна за одной»**. Для отображения нужного набора атрибутов выберите **режим просмотра** (более подробные сведения см. в разделе Фильтрация данных 30. Если нужно распечатать какую-либо информацию с вкладок, дополнительные сведения см. в главе Настройка страницы 29.

Раздел «Сервер» (**«4»**) имеет важное значение при репликации серверов ERA Server. В этом разделе отображаются сводные данные о консоли, к которой подключен сервер ERAS, а также сведения о дочерних (или «подчиненных») серверах ERA Server. Раскрывающееся меню «Серверы» в разделе **«4»** влияет на диапазон данных, отображаемых в разделе **«5»**.

- **«Использовать все серверы»** — отображение данных со всех серверов ERA Server — раздел (**«5»**).
- **«Использовать только выбранные серверы»** — отображение данных с выбранных серверов ERA Server — раздел (**«5»**).
- **«Исключить выбранные серверы»** — исключение данных с выбранных серверов ERA Server.

Столбцы в разделе **«4»**:

- **«Имя сервера»** — отображает имя сервера.
- **«Клиенты»** — общее число подключенных клиентов или клиентов в базе данных выбранного сервера ERAS.
- **«Диапазон БД сигнатур вирусов»** — версия БД сигнатур вирусов на клиентах выбранного сервера ERAS.
- **«Самое старое подключение»** — время, прошедшее с момента последнего подключения к серверу.
- **«Последние предупреждения об угрозах»** — общее число предупреждений о вирусах (см. атрибут **«Последнее предупреждение об угрозе»** в разделе **«5»**).
- **«Последние предупреждения файервола»** — общее число предупреждений файервола.
- **«Предупреждения о последнем событии»** — Общее число текущих событий (см. атрибут **«Последнее событие»** в разделе **«5»**).

Если в данный момент подключение отсутствует соединение, щелкните правой кнопкой мыши в разделе «Сервер» (**«4»**) и выберите команду **«Соединение с этим сервером»**, чтобы подключиться к выбранному серверу ERAS. Если включена репликация, в разделе «Сервер» (**«4»**) отобразятся дополнительные сведения.

Важнейшие функции консоли ERAC доступны из главного меню или с панели инструментов консоли ERAC (**«3»**).

Последний раздел — **«Настройка фильтра компьютеров»** (**«6»**) см. раздел Фильтрация данных 30.

**ПРИМЕЧАНИЕ.** Для администрирования клиентов и фильтрации информации настоятельно рекомендуется использовать контекстное меню 31. С его помощью можно быстро запускать задачи, управлять группами и политиками, фильтровать данные и пр.

### 3.2.1 Настройка страницы

В окне **«Настройка страницы»** можно настроить параметры для печати содержимого вкладок в консоли ERA Console.

**WYSIWYG** — вкладки печатаются точно в том виде, в каком они отображаются (режим «что видите, то и получаете»).

**«Печать»** — вкладки печатаются в оттенках серого. Используются только черный и белый цвета.

**«Значки»** — также печатаются значки, которые отображаются возле имен клиентов.

**«Заголовки»** — вставляется строка, определенная в разделе **«Заголовок»** в левом верхнем углу. Используйте заголовок по умолчанию или напишите собственный заголовок в поле **«Заголовок»**.

**«Логотип»** — вставляется строка, указанная в разделе **«Путь к логотипу»** в правом верхнем углу. Логотип ESET печатается по умолчанию. Можно загрузить собственный логотип, нажав кнопку **"..."** рядом с этим параметром и выбрав логотипа с жесткого диска.

**«Номера страниц»** — внизу распечатываемых страниц вставляются номера страниц.

**«Просмотр»** — страница отображается так, как она будет выглядеть после распечатки.

## 3.3 Фильтрация данных

В консоли ERAC представлены различные возможности и средства для удобного администрирования клиентских компьютеров и событий. Наличие расширенной системы фильтрации часто может быть очень важным, особенно в системах с большим числом клиентов, когда отображаемая информация должна быть сгруппированной и простой в управлении. В ERAC есть несколько средств для эффективной сортировки и фильтрации данных о подключенных клиентах.

Фильтр 30 позволяет администраторам выводить на экран информацию только об определенных серверах или клиентских рабочих станциях. Чтобы отобразить параметры фильтра, выберите **«Вид»** > **«Показать/скрыть панель фильтров»** в меню ERAC.

**Режим просмотра**

На вкладке **«Клиенты»** число отображаемых столбцов регулируется с помощью раскрывающегося меню **«Режим просмотра»** на правой части консоли. В **режиме полного просмотра** отображаются все столбцы, в то время как в **режиме минимального просмотра** показаны только самые важные из них. Эти режимы определены заранее, изменить их невозможно. Чтобы изменить представление, выберите любой **пользовательский режим просмотра** из пяти доступных. Его можно настроить на вкладке **Сервис** > **Настройки консоли** > **Столбцы — показать/скрыть**.

**Примечание**. Изменить порядок расположения столбцов (с помощью перетаскивания) и их размер можно в любом режиме просмотра.

### 3.3.1 Фильтр

Чтобы активировать фильтрацию, установите флажок **«Использовать фильтр»** в верхней левой части консоли ERAC. При всех последующих изменениях в критериях фильтрации отображаемые данные будут обновляться автоматически, если иное не указано на вкладке **«Сервис»** > **«Настройки консоли...»** > **«Другие параметры»**.

Определите критерии фильтрации в разделе **Критерий фильтрации клиентов**. Клиенты могут принадлежать нескольким группам и политикам. Назначение клиента в статическую или параметрическую группу может эффективно использоваться не только для фильтрации, но и для таких действий, как формирование отчетов. Дополнительные сведения об управлении группами см. в разделе Диспетчер групп 94. Использование политик для разделения клиентов также может служить для нескольких задач. Дополнительные сведения о создании политик и управлении ими см. в разделе Политики 96.

Первым средством фильтрации является раздел выбора группы и политики. Доступны три перечисленных ниже варианта.

- **«Показать отмеченные клиенты»** — на панели **«Клиенты»** будут отображены клиенты в выбранных группах или политиках.
- **«Скрыть отмеченные клиенты»** — на панели **«Клиенты»** будут отображены клиенты, не выбранные в группах или политиках, и клиенты, не входящие в группы. Если клиент является членом нескольких групп и выбрана одна из этих групп, клиент не будет отображаться.
- **«Скрыть отмеченные клиенты, игнорировать множественное членство»** — будут отображены клиенты, не выбранные в группах или политиках, и клиенты, не входящие в группы. Если клиент является членом нескольких групп и выбрана одна из этих групп, клиент будет отображаться.
- **«Показать клиенты не в группах»** — будут отображены только клиенты, не принадлежащие какой-либо группе или политике.

**Примечание.** Если выбрать группу из списка, будут также выбраны все ее подгруппы.

В нижней части раздела **«Фильтр»** можно указать и другие параметры.

- **«Только клиенты (исп. целые слова)»** — в выходные данные попадают только те клиенты, имена которых совпадают с введенной строкой.
- **«Только клиенты, начинающиеся с (?,*)»** — в выходные данные попадают только те клиенты, имена

которых начинаются с указанной строки.

- **«Только клиенты типа (?,*)»** — в выходные данные попадают только те клиенты, имена которых содержат указанную строку.
- **«Исключить клиенты (исп. целые слова)», «Исключить клиенты, начинающиеся с (?,*)», «Исключить клиенты типа (?,*)»** — эти параметры позволяют получить результаты, противоположные предыдущим трем вариантам.

В полях **«Основной сервер»**, **«Имя клиента»**, **«Имя компьютера»** и **«MAC-адрес»** допустимы строки на основе критериев, указанных в раскрывающемся меню сверху. При заполнении любого из этих полей в базу данных отправляется запрос, а результаты фильтруются на основании заполненного поля (может использоваться логический оператор AND). Можно использовать целые строки или знаки подстановки (?,*).

Последний параметр фильтрует результаты на основании проблем: отображаются только клиенты с указанным видом проблемы. Чтобы отобразились выбранные проблемы, выберите **«Только показать проблемы»** и нажмите кнопку **«Изменить...»**. Выберите проблемы, которые нужно отобразить, и нажмите кнопку **«ОК»**, чтобы отобразить список клиентов с выбранными проблемами.

Все изменения, внесенные в настройки фильтрации, вступят в силу после нажатия кнопки **«Применить изменения»**. Чтобы восстановить значения по умолчанию, нажмите кнопку **«Сброс»**. Чтобы автоматически генерировать новые выходные данные при каждом изменении настроек фильтрации, щелкните **«Сервис»** > **«Настройки консоли...»** > **«Другие параметры...»**, а затем выберите **«Автоматически применять изменения»**.

**ПРИМЕЧАНИЕ.** Критерии фильтра могут отличаться в зависимости от того, какая вкладка сейчас активна. Критерии настраиваются для эффективной сортировки журналов. Например, можно сортировать журналы по уровню детализации в журнале файервола, чтобы отображались только те журналы, которые нужно просмотреть.

Можно также сортировать данные на вкладках, выбрав временной интервал, за который должны отображаться элементы. Дополнительные сведения о том, как использовать **фильтр даты**, см. в разделе Фильтр даты 32.

### 3.3.2 Контекстное меню

Правая кнопка мыши вызывает контекстное меню, с помощью которого настраиваются выходные данные в столбцах. Контекстное меню содержит перечисленные ниже команды.

- **«Выбрать все»** — выбор всех записей.
- **«Выбрать по "..."»** — эта команда позволяет щелкнуть правой кнопкой мыши любой атрибут и автоматически выбрать (выделить) все остальные рабочие станции или серверы с таким же атрибутом. Строка «...» автоматически заменяется значением текущей вкладки.
- **«Обратить выбор»** — инвертирование выбора записей в списке.
- **«Скрыть выбранное»** — скрытие выбранных записей.
- **«Скрыть невыбранное»** — скрытие всех невыбранных записей в списке.

**ПРИМЕЧАНИЕ.** Эти параметры могут быть разными в зависимости от активного окна.

- **«Показать/скрыть столбцы»** — открывает окно **«Настройки консоли»** > Столбцы — показать/скрыть 65, в котором можно указать столбцы, которые будут доступны на выбранной панели.

Команды **«Скрыть выбранное/невыбранное»** используются в ситуации, когда после фильтрации требуется дальнейшее упорядочивание. Чтобы отключить все фильтры, установленные в контекстном меню, выберите в меню **«Вид»** команду **«Ограниченный просмотр»** или щелкните по значку на панели инструментов ERAC. Также можно нажать клавишу **F5**, чтобы обновить данные и отключить фильтры.

**Пример**

- Отображение клиентов с предупреждениями об угрозе.
  На вкладке**«Клиенты»** щелкните правой кнопкой мыши по пустой панели с полем «Последнее

предупреждение о вирусе» и выберите в контекстном меню команду **«Выбрать по „...“»**. Затем выберите в контекстном меню команду **«Скрыть выбранное»**.

- Вывод предупреждений об угрозе для клиентов Joseph и Charles
  Откройте вкладку **«Журнал угроз»** и щелкните правой кнопкой мыши по любому атрибуту в столбце «Имя клиента» со значением Joseph. В контекстном меню выберите команду **«Выбрать по „Joseph“»**. Затем, нажав и удерживая клавишу CTRL, щелкните правой кнопкой мыши и выберите команду **«Выбрать по „Charles“»**. Наконец, щелкните правой кнопкой мыши, выберите в контекстном меню команду **«Скрыть невыбранное»** и отпустите клавишу CTRL.

С помощью клавиши CTRL можно выделять отдельные записи и отменять их выделение, а с помощью клавиши SHIFT — выделять и отменять выделение групп записей.

**Примечание.** Фильтрация также упрощает создание новых задач для конкретных (выделенных) клиентов. Доступны различные варианты фильтрации: просто экспериментируйте с различными их сочетаниями.

#### 3.3.3 Фильтр даты

**«Фильтр даты»** расположен в правом нижнем углу каждой вкладки ERAC. Указав **Временной промежуток**, вы сможете легко отсортировать данные за выбранный временной промежуток.

**Последние X часов/дней/недель/месяцев/лет** — выберите число и время. Это ограничит элементы на текущей вкладке: будут отображаться только элементы из этого временного интервала. Например, если выбрать *Последние 10 дней*, отобразятся все элементы за последние 10 дней.

**Последние X** — выберите из раскрывающегося меню временной интервал, элементы из которого нужно отобразить.

**До (вкл-но) / После (вкл-но)** — поставьте флажок рядом с параметром **До (вкл-но)** или **После (вкл-но)** и укажите время и дату. Отобразятся все элементы до или после этого времени и даты.

**В интервале** — выберите интервал времени и даты (от ... до). Отобразятся элементы из этого временного интервала.

**ПРИМЕЧАНИЕ.**: **Фильтр даты** можно использовать в каждом журнале для указания временного интервала, данные за который нужно отобразить на вкладке. Также можно установить степень детализации (если это возможно), чтобы отсортировать данные по релевантности. В окне **Фильтр даты** будут показаны данные, уже отобранные фильтром **Показать**. Эти фильтры взаимозависимы. Это означает, что этот фильтр можно применять только к уже отфильтрованным данным.

## 3.4 Вкладки в консоли ERA Console

#### 3.4.1 Общее описание вкладок и клиентов

Большая часть данных на вкладках относится к подключенным клиентам. Каждый компьютер, подключенный к серверу ERAS, идентифицируется следующими атрибутами:

Имя компьютера (имя клиента), MAC-адрес, Главный сервер.

Поведение сервера ERAS в связи с определенными операциями в сети (такими как переименование ПК) определяется в разделе «Дополнительные настройки сервера ERAS». Это позволяет предотвращать дублирование записей на вкладке **«Клиенты»**. Например, если один из компьютеров в сети был переименован, а его MAC-адрес не изменился, новая запись на вкладке **«Клиенты»** не будет создана.

Клиенты, которые подключаются к серверу ERAS в первый раз, отмечены значением **«Да»** в столбце **«Новый клиент»**. Они также отмечены маленькой звездочкой в правом верхнем углу на значке клиента (см. рисунок ниже). Эта функция позволяет администратору легко обнаружить новый подключившийся компьютер. Этот атрибут может иметь разное значение в зависимости от используемых администратором рабочих процедур.

На случай перенастройки и перемещения клиента в определенную группу назначение состояния «Новый клиент» можно отменить, щелкнув клиента и выбрав команду **«Задать/снять отметки»** > **«Снять отметку „Новый“»**. Значок этого клиента будет заменен значком, показанным на рисунке ниже, а значение атрибута в столбце **«Новый клиент»** будет изменено на **«Нет»**.


**Примечание.** Атрибут «Примечание» является необязательным на всех трех вкладках. Администратор может вставить сюда любое описание (например, *«Офис №129»*).

Временные значения в ERAS отображаются в относительном (*2 дня назад*), точном (20.5.2009) или системном (с учетом региональных параметров) режимах.

В большинстве случаев данные можно отсортировать в возрастающем или в убывающем порядке, щелкнув их заголовок, и переупорядочить с помощью перетаскивания.

С помощью параметра **«Показать»** можно сортировать данные, которые нужно отобразить на вкладке. Установите количество журналов, которые нужно отображать (по умолчанию это значение составляет 200 для всех журналов), и период времени, за который нужно отображать журналы (по умолчанию — 7 дней). Выбирать параметр **«Не ограничивать время»** не рекомендуется для крупных сетей, поскольку это может привести к существенной нагрузке на базу данных и к возможному снижению производительности.

**ПРИМЕЧАНИЕ.**: Можно использовать **фильтр даты** в каждом журнале, чтобы указать интервал времени, данные за который должны быть отображены на вкладке. Можно задать степень детализации на вкладках (где применимо), чтобы сортировать данные по релевантности. В окне **«Фильтр даты»** будут показаны данные, уже отобранные фильтром **«Показать»**. Эти фильтры взаимозависимы.

При выборе определенных значений активируются другие вкладки, на которых отображаются более подробные сведения. Например, если щелкнуть значение в столбце **«Последнее предупреждение об угрозе»**, программа откроет вкладку **«Журнал угроз»** и отобразит записи, относящиеся к данному клиенту. Если щелкнуть значение, информация о котором не помещается на вкладке, откроется диалоговое окно с подробными сведениями о соответствующем клиенте.

### 3.4.2 Репликация и данные на отдельных вкладках

Если консоль ERAC подключена к серверу ERAS, выполняющему роль сервера верхнего уровня, все данные от серверов нижнего уровня будут показываться автоматически, если только соответствующий подчиненный сервер не настроен иным образом. Типы реплицируемых данных настраиваются на сервере нижнего уровня в меню **«Служебные программы»** > **«Настройки сервера»** > **«Репликация»** > **«Параметры репликации "на"»**.

В таком сценарии могут отсутствовать приведенные ниже данные:

- данные журнала предупреждений (вкладка **«Журнал угроз»**);
- данные журнала сканирования по требованию (вкладка **«Журнал сканирования»**);
- подробные конфигурации текущего клиента в XML-формате (вкладка **«Клиенты»**, столбец **«Конфигурация»**, **«Состояние защиты»**, **«Свойства защиты»**, **Сведения о системе»**).

Также могут отсутствовать данные программы ESET SysInspector. Модуль ESET SysInspector встроен в продукты ESET версий 4.x и более поздних.

Если данные не удается найти в диалоговых окнах программы, нажмите кнопку **«Запрос»** (находится в разделе **«Действия»** > **«Свойства»** > **«Конфигурация»**). Нажатие этой кнопки позволяет загрузить недостающие сведения с сервера ERAS нижнего уровня. Поскольку репликация всегда инициируется сервером ERAS нижнего уровня, недостающие данные обычно передаются в пределах заданного интервала репликации.

На сервере верхнего уровня можно настроить уровень детализации журналов, которые будут получены севером (**«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные параметры...»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Обслуживание сервера»** > **«Принимаемые журналы...»**).

**Примечание.** Этот параметр применяется ко всем клиентам, подключенным к серверу (а не только к

реплицируемым).

### 3.4.3 Вкладка «Клиенты»

На этой вкладке отображаются общие сведения об отдельных клиентах. То, как эти сведения отображаются, зависит от того, как настроен режим просмотра 30 в ESET Remote Administrator.

| Атрибут | Описание |
|---|---|
| Имя клиента | Имя клиента (можно изменить в окне «Свойства клиента» на вкладке «Общие»). |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |
| Главный сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Домен | Имя домена или группы, к которым принадлежит клиент (это не группы, созданные в ERAS). |
| IP | Адрес IPv4 или IPv6 |
| Имя продукта | Название продукта ESET |
| Версия продукта | Версия продукта ESET |
| Имя запрашиваемой политики | Имя политики, запрашиваемой для клиента пользователем или сервером. Запрашиваемая политика будет синхронизирована с фактической политикой после того, как клиент подключится к ERAS (если нет правил политики, которые запрещают назначать запрашиваемую политику). |
| Имя фактической политики | Имя политики, успешно назначенной клиенту после подключения к ERAS. |
| Последнее подключение | Время последнего подключения клиента к ERAS (эта метка времени включается во все остальные данные, полученные от клиентов, за исключением некоторых данных, полученных при репликации). |
| Текст состояния защиты | Текущее состояние продукта безопасности ESET, установленного на клиенте. |
| БД сигнатур вирусов | Версия базы данных сигнатур вирусов. |
| Последнее предупреждение об угрозе | Последний инцидент с вирусом. |
| Последнее предупреждение файервола | Последнее событие, обнаруженное персональным файерволом ESET Endpoint Security (отображаются события уровня «Предупреждение» и выше). |
| Последнее предупреждение о событии | Последнее сообщение об ошибке. |
| Проверено файлов в прошлый раз | Количество файлов, проверенных во время последнего сканирования по требованию. |
| Заражено файлов в прошлый раз | Количество зараженных файлов, которые были обнаружены во время последнего сканирования по требованию. |
| Очищено файлов в прошлый раз | Количество файлов, очищенных (или удаленных) в ходе последнего сканирования по требованию. |
| Дата последнего сканирования | Дата последнего сканирования по требованию. |
| Запрос перезапуска | Запрос о необходимости перезагрузки (например, после обновления программы). |
| Дата запроса перезапуска. | Время первого запроса на перезагрузку. |
| Последний запуск продукта | Время последнего запуска клиентской программы. |
| Дата установки продукта | Дата установки продукта безопасности ESET на клиентский компьютер. |

| | |
|---|---|
| Пользователь в роуминге | Для клиентов с этим атрибутом задача «обновить сейчас» выполняется при каждом подключении к серверу ERAS (такой вариант рекомендуется для ноутбуков). Обновление производится только в том случае, если база данных сигнатур вирусов не является актуальной. Эта функция удобная для пользователей, которые долгое время не подключались к серверу ERAS, поскольку данная задача сразу же инициирует обновление (еще до того, как буде выполнена задача регулярного обновления). |
| Новый клиент | Новый подключенный компьютер (см. раздел Общее описание вкладок и клиентов 32) |
| Имя ОС | Название клиентской операционной системы. |
| Платформа ОС | Платформа операционной системы (Windows, Linux и т. п.). |
| Аппаратная платформа | 32-разрядная или 64-разрядная. |
| «Конфигурация» | Конфигурация клиента в файле current.xml (включая время и дату создания конфигурации). |
| «Состояние защиты» | Отчет об общем состоянии (смысл этого атрибута аналогичен смыслу атрибута «Конфигурация»). |
| «Свойства защиты» | Отчет об общем состоянии программных компонентов (аналогично атрибуту «Конфигурация»). |
| «Сведения о системе» | Сведения о системе, переданные клиентом на сервер ERAS (включая время отправки этих данных). |
| SysInspector | Клиенты, в состав которых входит средство ESET SysInspector, могут отправлять журналы из этого приложения. |
| Прочие сведения 1, 2, 3 | Прочие сведения, отображение которых включено администратором (настраиваются в консоли ERAC в меню «Сервис» > «Параметры сервера» > «Дополнительно» > «Изменить дополнительные параметры...» > ESET Remote Administrator > ERA Server > «Настройка» > «Другие параметры» > «Прочие данные клиента 1, 2, 3»). |
| Примечание | Краткое описание клиента (вводится администратором). |

**Примечание.** Некоторые значения выводятся только в информационных целях и могут быть неактуальны на момент их просмотра администратором в консоли. Например, информация об ошибке обновления, которая случилась в 7:00, не обязательно означает, что обновление не было успешно выполнено в 8:00 утра. **«Последнее предупреждение об угрозе»** и **«Пред. о последнем событии»** могут быть отнесены к таким значениям. Если администратор знает, что эти данные устарели, он может удалить их, щелкнув правой кнопкой мыши и выбрав в меню команду **«Удалить информацию»** > **«Удалить запись "Последнее предупреждение об угрозе"»** или **«Удалить запись "Последнее предупреждение о событии"»**. В результате информация о последнем инциденте с вирусом или последнем системном событии будет удалена.

Если дважды щелкнуть имя клиента, отобразятся следующие дополнительные параметры на вкладке **«Клиент»**.

- **«Общие»** — содержит ту же информацию, что отображается на вкладке «Клиенты». Здесь можно изменить имя клиента (имя, под которым клиент отображается в ERA), а также добавить необязательный комментарий.
- **«Член группы»** — на этой вкладке перечислены все группы, в которые входит клиент. Дополнительные сведения см. в разделе Фильтрация данных 30.
- **«Задачи»** — задачи, связанные с данным клиентом. Дополнительные сведения см. в разделе Задачи 88.
- **«Конфигурация»** — на этой вкладке можно просмотреть текущую конфигурацию клиента и экспортировать ее в XML-файл. Далее в этом руководстве будет рассказано, как с помощью *XML*-файлов создавать шаблоны конфигурации для новых и измененных конфигурационных *XML*-файлов. Дополнительные сведения см. в разделе Задачи 88.
- **«Состояние защиты»** — это сведения об общем состоянии всех программ ESET. Некоторые из отчетов являются интерактивными и позволяют немедленно выполнять нужные действия. Благодаря этой функции отпадает необходимость вручную определять новые задачи для разрешения конкретных проблем в системе защиты.
- **«Свойства защиты»** — состояние всех компонентов системы защиты ESET (модуля защиты от спама, персонального файервола и т. д.).
- **«Информация о системе»** — подробные сведения об установленной программе, версиях ее компонентов и т. п.
- **SysInspector** — подробные сведения об автоматически запускаемых процессах и процессах, выполняющихся в фоновом режиме.
- **«Карантин»** — содержит список всех файлов, помещенных в карантин. Файлы, помещенные в карантин, можно запросить у клиента и сохранить на локальном диске.

Чтобы выполнить сетевые действия для определенного клиента, щелкните клиент правой кнопкой мыши и в контекстном меню выберите пункт **Сетевое действие** 37.

Если на этой вкладке отображаются дублирующиеся клиенты, их можно легко объединить 36.

#### 3.4.3.1 Объединение дублирующихся клиентов

Например, если в компьютере, которым управляет сервер ERA Server, изменить сетевой адаптер, изменится и MAC-адрес компьютера. Если этот компьютер подключить к серверу ERA Server, то он будет дубликатом старого (ранее подключенного) компьютера. В таком случае можно удалить старый компьютер из вкладки **Клиенты** консоли ERA Console или объединить два компьютера, если журналы старого компьютера нужно оставить и связать с новым.

Чтобы объединить два компьютера, перейдите на вкладку **Клиенты** консоли ERA Console, выберите два компьютера, после этого щелкните их правой кнопкой мыши и в контекстном меню щелкните **Объединить дубликаты**. В окне **Объединение дублирующихся клиентов** выберите клиент, который нужно оставить, а затем нажмите кнопку **Объединить клиенты**. Если выбрать более плохой клиент (то есть клиент, который не подключался к серверу ERA Server дольше), отобразится предупреждение о неверном выборе.

**ПРИМЕЧАНИЕ**. При объединении двух компьютеров журналы связываются с оставленным компьютером, но задачи, карантин и назначения группы и политики удаленного компьютера удаляются.

#### 3.4.3.2 Сетевые действия

Вы можете выполнять разные сетевые действия на клиентах, управляемых сервером ERA Server. Если щелкнуть клиент правой кнопкой мыши на вкладке **Клиенты** консоли ERA Console и выбрать **Сетевые действия**, отобразится несколько пунктов: **Проверка связи**, **Пробуждение по локальной сети**, **Поделиться**, **Завершение работы или перезагрузка**, **Сообщение**, **Протокол RDP** и **Настраиваемое** . Эти действия соответствуют сетевым действиям Windows и обладают такими же функциональными возможностями.
Для каждого сетевого действия (кроме действия «Проверка связи») будет отображаться диалоговое окно с индикатором хода выполнения. В таблице ниже приведены доступные сетевые действия, выполняемые ими команды в Windows (кроме случаев, когда они выполняются по-другому через сервер ERA Server) и некоторые необходимые условия. Во многих случаях нужны не все приведенные необходимые условия или нужные совсем другие и здесь не указанные. Поэтому здесь необходимые условия приведены на всякий случай.

| Сетевое действие | Команда | Обязательные условия |
|---|---|---|
| *Проверка связи* | - | • В файерволе разрешен протокол ICMP. |
| *Пробуждение по локальной сети* | - | • Сетевая карта выбранных компьютеров должна поддерживать стандартный формат Magic Packet.<br>• «Пробуждение по локальной сети» должно быть настроено в BIOS выбранных компьютеров и в их сетевых картах.<br>• Дополнительные сведения в диалоговом окне. |
| *Поделиться* | explorer.exe \\<компьютер> | • Действие «Поделиться» включено на целевом компьютере.<br>• Исключение в файерволе для этого действия. |
| *Завершение работы* или *перезагрузка* | shutdown /s /t <время_ожидания> /c "<примечание_о_причине>" /f /m <компьютер><br>• Если выбрана перезагрузка, то вместо /s указывается /r.<br>• Если примечание о причине не введено, то элемент /c "<примечание_о_причине>" отсутствует.<br>• Если не установлен флажок «Принудительное закрытие приложений», элемент /f отсутствует.<br>• Если установлен флажок «Отменить завершение работы», то в команде остаются только элементы /a /m <компьютер>. | • Включена служба «Удаленный реестр».<br>• Включена служба инструментария управления Windows.<br>• Для инструментария управления Windows (WMI) сделано исключение в файерволе.<br>• Текущий пользователь Windows на компьютере, на котором установлена консоль, имеет права администратора на целевом компьютере (предполагается, что используется среда домена).<br>• Запуск действия с правами администратора на локальном компьютере.<br>• Нужно добавить учетные данные:<br>1. Найдите диспетчер учетных данных Windows.<br>2. Щелкните «Добавить учетные данные Windows».<br>3. На целевом компьютере введите имя целевого компьютера (или IP-адрес), имя пользователя и пароль. |
| *Сообщение* | msg.exe /SERVER:<компьютер> * "a"<br>В Windows 2000 команда принимает такой вид:<br>net send <компьютер> | • Нужно внести изменения в реестр: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server<br>Имя: AllowRemoteRPC<br>Тип: REG_DWORD<br>Значение: 1<br>• Запуск действия с правами администратора на локальном компьютере.<br>• Нужно добавить учетные данные:<br>1. Найдите диспетчер учетных данных Windows.<br>2. Щелкните «Добавить учетные данные Windows».<br>3. На целевом компьютере введите имя целевого компьютера (или IP-адрес), имя пользователя и пароль. |

Команда выполняется на компьютере, на котором запущена консоль ERA (поэтому выполнение команды с помощью **cmd.exe** на компьютере, на котором установлена консоль, должно проходить так же и может выявить проблему). Элемент <компьютер> заменяется именем узла или IP-адресом компьютера на основании значения параметра «При выполнении сетевых действий использовать имя хоста вместо IP-адреса», который находится в разделе интерфейса **Сервис > Настройки консоли > Другие настройки** в ERA Console.

Некоторые команды лучше работают в среде домена — если вы вошли как пользователь домена (у которого есть права администратора на целевом компьютере), вам не нужно добавлять учетные данные.

### 3.4.4 Вкладка «Журнал угроз»

На этой вкладке содержатся подробные сведения о конкретных вирусах и инцидентах.

| Атрибут | Описание |
|---|---|
| Имя клиента | Имя клиента, сообщившего о наличии угрозы. |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |
| Главный сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата обнаружения | Время возникновения данного события. |
| Уровень | Уровень предупреждения. |
| Сканер | Название средства безопасности, обнаружившего угрозу. |
| Объект | Тип объекта. |
| Имя | Как правило, это папка, в которой обнаружено заражение. |
| Угроза | Название обнаруженного злонамеренного кода. |
| Действие | Действие, выполненное соответствующим средством безопасности. |
| Пользователь | Имя пользователя, находившегося в системе во время инцидента. |
| Информация | Сведения об обнаруженной угрозе. |
| Детали | Состояние отправки клиентского журнала. |

### 3.4.5 Вкладка «Журнал файервола»

На этой вкладке отображаются сведения о работе клиентского файервола.

| Атрибут | Описание |
|---|---|
| Имя клиента | Имя клиента, сообщившего о событии. |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |
| Главный сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата обнаружения | Время возникновения данного события. |
| Уровень | Уровень предупреждения. |
| Событие | Описание события. |
| Источник | IP-адрес источника. |
| Объект | IP-адрес целевого объекта. |
| Протокол | Задействованный протокол. |
| Правило | Задействованное правило файервола. |
| Приложение | Задействованное приложение. |
| Пользователь | Имя пользователя, находившегося в системе во время инцидента. |

### 3.4.6 Вкладка «Журнал событий»

На этой вкладке отображаются все системные события (по компонентам программного продукта безопасности ESET).

| Атрибут | Описание |
|---|---|
| Имя клиента | Имя клиента, сообщившего о событии. |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |
| Главный сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата обнаружения | Время возникновения данного события. |
| Уровень | Уровень предупреждения. |
| Программный модуль | Название программного компонента, сообщившего о событии. |
| Событие | Описание события. |
| Пользователь | Имя пользователя, связанного с данным событием. |

### 3.4.7 Вкладка «Журнал системы предотвращения вторжений на узел»

На этой вкладке отображаются действия, связанные с системой предотвращения вторжений на узел.

| Атрибут | Описание |
|---|---|
| Идентификатор системы предотвращения вторжений на узел | Идентификатор соответствующей записи в базе данных (идентификатор имеет вид: номер системы предотвращения вторжений на узел) |
| Имя клиента | Имя клиента, отправившего сообщение системы предотвращения вторжений на узел |
| Основной сервер | Имя сервера ERA Server, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата обнаружения | Время возникновения данного события. |
| Уровень | Степень опасности события |
| Приложение | Имя приложения, которое создало журнал системы предотвращения вторжений на узел. Оно указывается в формате UNC-пути к исполняемому файлу приложения |
| Операция | Обнаруженное действие, которое влияет на целевое приложение |
| Объект | Файл приложения, который создал журнал системы предотвращения вторжений на узел. Файл указывается в формате пути к файлу в папке установки приложения |
| Действие | Действие, предпринятое системой предотвращения вторжений на узел на основе текущего режима или правила |

**ПРИМЕЧАНИЕ.**: По умолчанию ведение журнала системы предотвращения вторжений на узел отключено. Чтобы включить ведение журнала активности или изменить настройки, выберите **«Сервис»** > **«Параметры сервера»** > **«Обслуживание сервера»** > **Параметры сбора журналов** 125.

### 3.4.8 Журнал контроля устройств

На этой вкладке отображаются подробные журналы активности контроля устройств.

| Атрибут | Описание |
|---|---|
| Идентификатор контроля устройств | Идентификатор соответствующей записи в базе данных |
| Имя клиента | Имя клиента, сообщившего о событии. |
| Основной сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата события | Время возникновения данного события. |
| Уровень | Уровень предупреждения. |
| Пользователь | Имя пользователя, связанного с данным событием. |
| Группа | Группа, к которой принадлежит клиент, сообщивший об активности |
| Класс устройства | Тип съемного устройства (USB-накопитель, DVD-диск) |

| | |
|---|---|
| Устройство | Имя и серийный номер (если есть) съемного устройства |
| Событие | Событие, о котором сообщило средство контроля устройств |
| Действие | Действие, выполненное соответствующим средством безопасности. |

**ПРИМЕЧАНИЕ.**: По умолчанию ведение журнала активности контроля устройств отключено. Чтобы включить ведение журнала активности или изменить настройки, выберите **«Сервис»** > **«Параметры сервера»** > **«Обслуживание сервера»** > **Параметры сбора журналов** 125.

### 3.4.9 Журнал контроля доступа в Интернет

На этой вкладке отображаются подробные журналы контроля доступа в Интернет.

| Атрибут | Описание |
|---|---|
| Идентификатор контроля доступа в Интернет | Идентификатор соответствующей записи в базе данных |
| Имя клиента | Имя клиента, сообщившего о событии. |
| Основной сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата события | Время возникновения данного события. |
| Уровень | Уровень предупреждения. |
| Пользователь | Имя пользователя, связанного с данным событием. |
| Группа | Группа, к которой принадлежит клиент, сообщивший об активности |
| URL-адрес | URL-адрес заблокированной веб-страницы |
| Маска URL-адреса | Маска URL-адреса заблокированной веб-страницы |
| Категория URL-адреса | Категория URL-адреса заблокированной веб-страницы |
| Действие | Действие, выполненное соответствующим средством безопасности. |

**ПРИМЕЧАНИЕ.**: По умолчанию ведение журнала контроля доступа в Интернет отключено. Чтобы включить ведение журнала активности или изменить настройки, выберите **«Сервис»** > **«Параметры сервера»** > **«Обслуживание сервера»** > **Параметры сбора журналов** 125.

### 3.4.10 Вкладка «Журнал защиты от спама»

На этой вкладке отображаются все действия, связанные с защитой от спама.

| Атрибут | Описание |
|---|---|
| Идентификатор защиты от спама | Идентификатор соответствующей записи в базе данных (идентификатор имеет вид: номер защиты от спама) |
| Имя клиента | Имя клиента, отправившего сообщение системы защиты от спама |
| Основной сервер | Имя сервера ERA Server, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS |
| Дата обнаружения | Время возникновения данного события |
| Отправитель | Адрес электронной почты отправителя сообщения, помеченного как спам |
| Получатели | Получатель сообщения, помеченного как спам |
| Тема | Тема сообщения, помеченного как спам |
| Оценка | Рейтинг спама (вероятность того, что сообщение является спамом) в процентах |
| Причина | Причина, по которой сообщение помечено как спам |
| Действие | Действие, предпринятое в отношении этого сообщения |

**ПРИМЕЧАНИЕ.**: По умолчанию ведение журнала системы защиты от спама отключено. Чтобы включить ведение журнала активности или изменить настройки, выберите **«Сервис»** > **«Параметры сервера»** > **«Обслуживание сервера»** > **Параметры сбора журналов** 125.

### 3.4.11 Вкладка «Журнал занесения в "серый" список»

На этой вкладке отображаются действия, связанные с «серым» списком.

| Атрибут | Описание |
|---|---|
| Идентификатор «серого» списка | Идентификатор соответствующей записи в базе данных (идентификатор имеет вид: номер в «сером» списке) |
| Имя клиента | Имя клиента, сообщившего о событии. |
| Основной сервер | Имя сервера ERAS, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS |
| Дата обнаружения | Время возникновения данного события |
| Домен HELO | Имя домена, которое использует сервер-отправитель, чтобы его мог идентифицировать сервер-получатель |
| IP-адрес | IP-адрес отправителя сообщения |
| Отправитель | Адрес электронной почты отправителя сообщения |
| Получатель | Адрес электронной почты получателя сообщения |
| Действие | Действие, выполненное соответствующим средством безопасности. |
| Оставшееся время | Время, которое осталось до отклонения сообщения или его проверки и доставки. |

**ПРИМЕЧАНИЕ.**: По умолчанию ведение журнала занесения в «серый» список отключено. Чтобы включить ведение журнала активности или изменить настройки, выберите **«Сервис»** > **«Параметры сервера»** > **«Обслуживание сервера»** > **Параметры сбора журналов** 125.

### 3.4.12 Вкладка «Журнал сканирования»

На этой вкладке представлены результаты проверок компьютеров по требованию, которые запускались удаленно, локально на клиентских компьютерах или в качестве запланированных задач.

| Атрибут | Описание |
|---|---|
| ID сканирования | Идентификатор соответствующей записи в базе данных (идентификатор имеет вид: номер проверки) |
| Имя клиента | Имя клиентского ПК, на котором была выполнена проверка. |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |
| Главный сервер | Имя сервера ERA Server, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации события сканирования на сервере ERAS. |
| Дата об | Время выполнения проверки на клиенте. |
| Проверенные объекты | Проверенные файлы, папки и устройства. |
| Проверено | Количество проверенных файлов. |
| Заражено | Количество зараженных файлов. |
| Очищено | Количество очищенных (или удаленных) объектов. |
| Статус | Статус проверки. |
| Пользователь | Имя пользователя, находившегося в системе во время инцидента. |
| Тип | Тип пользователя. |
| Сканер | Тип сканера. |
| Детали | Состояние отправки клиентского журнала. |

### 3.4.13 Вкладка «Мобильный журнал»

На этой вкладке отображаются подробные журналы из мобильных устройств, подключенных к серверу ERA Server.

| Атрибут | Описание |
|---|---|
| ID мобильного устройства | Сетевой идентификатор мобильного устройства |
| Имя клиента | Имя клиента, на котором было выполнено действие. |
| Имя компьютера | Имя рабочей станции/сервера (имя хоста). |
| MAC-адрес | MAC-адрес (сетевой адаптер). |

| | |
|---|---|
| Главный сервер | Имя сервера ERA Server, с которым клиент ведет обмен данными. |
| Дата получения | Время регистрации данного события сервером ERAS. |
| Дата обнаружения | Время выполнения события на клиенте. |
| Уровень | Уровень предупреждения. |
| Тип журнала | Тип журнала (например, журнал аудита безопасности, журнал защиты от спама в SMS). |
| Событие | Описание события. |
| Тип объекта | Объект, к которому имеет отношение событие (например, SMS, файл и т. п.). |
| Имя объекта | Конкретный объект, к которому имеет отношение событие (например, номер телефона отправителя SMS, путь к файлу и т. п.). |
| Действие | Действие, выполненное во время события (или возникшая ошибка). |

### 3.4.14 Вкладка «Карантин»

На этой вкладке отображено все содержимое карантина в сети.

| Атрибут | Описание |
|---|---|
| ID в карантине | Идентификатор помещенного в карантин объекта (номер увеличивается в порядке возникновения). |
| Хэш | Хэш файла. |
| Дата получения | Время регистрации события сканирования на сервере ERAS. |
| Первое обнаружение | Время, которое прошло с момента первого обнаружения объекта, помещенного в карантин. |
| Последнее обнаружение | Время, которое прошло с момента последнего обнаружения объекта, помещенного в карантин. |
| Имя объекта | Как правило, это папка, в которой обнаружено заражение. |
| Имя файла | Имя файла, помещенного в карантин. |
| Расширение | Тип расширения файла, помещенного в карантин. |
| Размер | Размер файла, помещенного в карантин. |
| Причина | Причина помещения в карантин; как правило, это описание типа угрозы. |
| Количество клиентов | Количество клиентов, которые поместили объект в карантин. |
| Всего | Количество операций помещения объекта в карантин. |
| Файл | Показывает, была ли запрошена загрузка объекта на сервер. |

**ПРИМЕЧАНИЕ.** Обратите внимание, что в полях **«Имя объекта»**, **«Имя файла»** и **«Расширение»** отображаются только первые три объекта. Чтобы получить дополнительные сведения, откройте окно «Свойства», нажав клавишу **F3** или дважды щелкнув выбранный элемент.

Централизованный карантин содержит обзор изолированных файлов, которые хранятся локально на клиентах и которые можно запросить для загрузки. Если файл запрошен, он копируется на сервер ERA Server в безопасном зашифрованном виде. По соображениям безопасности расшифровка выполняется перед сохранением файла на диск. Инструкции по работе с изолированными файлами см. в разделе Задача восстановления или удаления из карантина 91.

**ПРИМЕЧАНИЕ.** Для работы централизованного карантина на клиентах должно быть установлено ПО EAV/ESS версии 4.2 или выше.

### 3.4.15 Вкладка «Задачи»

Предназначение этой вкладки описано в разделе Задачи 88. На ней доступны перечисленные ниже атрибуты.

| Атрибут | Описание |
|---|---|
| Статус | Статус задачи (активная — находится в стадии применения, завершенная — доставка на клиенты осуществлена). |
| Тип | Тип задачи. |
| Имя | Название задачи. |
| Описание | Описание задачи. |
| Дата развертывания | Дата и время выполнения задачи. |
| Дата получения | Время регистрации данного события сервером ERAS. |

| | |
|---|---|
| Детали | Состояние отправки журнала задач. |
| Примечание | Краткое описание клиента (вводится администратором). |

### 3.4.16 Вкладка «Отчеты»

Вкладка **«Отчеты»** предназначена для разделения статистической информации по графикам или диаграммам. После этого их можно сохранять и обрабатывать в формате значений, разделенных запятыми (*CSV*), с помощью средств ERA для вывода диаграмм и графиков. По умолчанию сервер ERA сохраняет выходные данные в формате HTML. Большая часть отчетов, связанных с заражением, создается в журнале угроз.

1. Панель мониторинга  **Шаблоны** — шаблоны для веб-отчетов с панели мониторинга. Панель мониторинга — это набор отчетов, которые можно просмотреть в Интернете через веб-браузер. Каждый администратор может настроить свою структуру панели мониторинга. Дважды щелкните шаблон, чтобы отобразился предварительный просмотр отчета, используемого в панели мониторинга.
2. **«Шаблоны отчетов»** — шаблоны для статических отчетов. В верхней части окна «Консоль» в разделе **«Шаблоны отчетов»** показаны названия созданных шаблонов. Рядом с именами шаблонов отображается время и интервалы, в соответствии с которыми создаются данные отчеты. Можно создавать новые шаблоны или изменять существующие готовые шаблоны (см. ниже).

- **«Обзор клиентов»** — отображает состояния защиты всех клиентов.
- **«Клиенты с активными угрозами»** — список клиентов с активными угрозами (не очищенными при сканировании) и информация об активных угрозах.
- **«Общий отчет о сетевых атаках»** — отображает общий отчет о сетевых атаках.
- **«Общий отчет об SMS»** — отображает общий отчет о SMS-спаме.
- **«Общий отчет о спаме»** — отображает общий отчет о спаме по электронной почте.
- **«Общий отчет об угрозах»** — отображает общий отчет об обнаруженных угрозах.
- **«Сводка прочих сведений»** — подробный отчет с выбранной пользователем информацией (она должна быть задана заранее).
- **«Клиенты с наибольшим количеством проблем»** — отображает клиенты с наибольшим количеством проблем (на основе предыдущих отчетов).

Щелкните **Шаблоны по умолчанию**, чтобы сбросить готовые шаблоны в исходное состояние (это не повлияет на пользовательские шаблоны).

- **Параметры**

Нажмите кнопку **«Создать сейчас»** (на вкладке **«Параметры»**), чтобы создать отчет в любой момент независимо от расписания. В раскрывающемся меню возле этого параметра выберите тип выходного файла. Это позволит определить формат создаваемого отчета (HTML, ZIP или PDF).

**Отчет**

**«Тип»** — тип отчета на базе готовых шаблонов. Это значение можно изменить для готовых шаблонов или выбрать для пользовательских шаблонов. Если нажать кнопку **...** (возле этого параметра), отобразятся отчеты, которые можно использовать для **Общего настраиваемого отчета**.

**Вид** — с помощью этого раскрывающегося меню можно изменить цвет и структуру отчета.

**Фильтр**

**Целевые клиенты** — можно собирать **все** данные, данные **только выбранных клиентов/серверов/групп** или можно **исключить выбранные клиенты/серверы/группы**. Можно указать клиенты/серверы/группы, нажав кнопку **...** рядом с раскрывающимся меню **Целевые клиенты** в диалоговом окне **Добавить/удалить**.

**Угроза** — также можно указать, должен ли отчет содержать **все** угрозы, **только выбранные угрозы**, или же можно **исключить выбранные угрозы**. Угрозы можно указать, нажав кнопку **...** рядом с этим раскрывающимся меню в диалоговом окне **Добавить/Удалить**.

Настроить другие параметры можно с помощью кнопки **Дополнительные параметры**. Эти настройки в основном относятся к данным в заголовке и в типах используемых графических диаграмм. При этом, однако, данные также можно фильтровать по состоянию выбранных атрибутов и выбирать формат для отчета (HTML, CSV).

- **Интервал**

**Текущий период** — в отчет включены только события, произошедшие в указанный период. Например, если отчет создается в среду, а в качестве интервала установлено значение Текущая неделя, то в отчет включаются все события, произошедшие в понедельник, вторник и среду.

**Завершенный период** — в отчет включаются только события, которые произошли в конкретный период (например, весь август или вся неделя с понедельника по воскресенье). Если выбрать **«Добавить также текущий период»**, в отчет будут включены события за последний завершенный период, включая момент создания.

Пример

Нужно создать отчет, включающий в себя события последней календарной недели, например с понедельника по воскресенье. Этот отчет должен быть создан в следующую среду (после воскресенья). На вкладке **Интервал** выберите параметр **Завершенный период** и **1 неделя**. Снимите флажок **«Добавить также текущий период»**. На вкладке **«Планировщик»** установите для параметра **«Частота»** значение **«Еженедельно»** и выберите пункт **«Среда»**. Остальные параметры можно настроить по своему усмотрению.

**«С/по»** — этот параметр позволяет задать период, для которого создается отчет.

- **Планировщик**

**«Частота»** — можно задавать и настраивать автоматическое создание отчетов в указанное время или в выбранные интервалы.

После занесения отчета в планировщик нажмите кнопку **«Выбрать путь…»**, чтобы указать место для сохранения отчета. Отчеты можно сохранять на сервере ERAS (по умолчанию), отправлять по электронной почте по указанному адресу или экспортировать в папку. Последний вариант необходим в том случае, если отчет отправляется в общую папку во внутренней сети организации, где может просматриваться другими работниками. Если используется этот параметр, выберите тип выходного файла (HTML, ZIP или PDF). В пути этой папки можно использовать переменные (%). В переменных не учитывается регистр. Эти переменные добавляют дополнительную информацию в созданный отчет. Если в конце пути папки добавить символ "\", отчеты записываются непосредственно в эту папку, а данные в ней перезаписываются. Поддерживаются следующие переменные.

| **Переменная** | **Описание** |
|---|---|
| %INTERVAL% | Интервал, за который создается отчет, который возвращается из ::GetIntervalString(INTERVALSTRING_FOLDER). |
| %DATE% | Текущая дата ("ГГГГ-ММ-ДД") |
| %TIME% | Текущее время ("ЧЧ-ММ-СС") |
| %DATETIME% | Текущие дата и время ("ГГГГ-ММ-ДД ЧЧ-ММ-СС") |
| %TIMESTAMP% | Текущие дата и время, формат UNIX, 8 шестнадцатеричных разрядов |
| %RND4% | Случайное значение, 4 шестнадцатеричных разряда, почти уникальное (не рекомендуется). |
| %DDATE% | Текущая дата, плотный формат ("ГГГГММДД") |
| %DTIME% | Текущее время, плотный формат ("ЧЧММСС") |
| %YEAR%, %MONTH%, %DAY%, %HOUR%, %MINUTE%, %SECOND% | Текущая дата / части времени как разряды (4 — год, 2 — остальные). |

| | |
|---|---|
| %COUNTER% | Десятичный счетчик, 5 разрядов начиная с 1. |
| %COUNTER1%, %COUNTER2%, %COUNTER3%, %COUNTER4%, %COUNTER5% | Десятичный счетчик, 1/2/3/4/5 разрядов начиная с 1. |
| %CCOUNTER% | Десятичный условный счетчик, 5 разрядов (первая итерация стерта, вторая итерация "00002") |
| %CCOUNTER1%, %CCOUNTER2%, %CCOUNTER3%, %CCOUNTER4%, %CCOUNTER5% | Десятичный условный счетчик, 1/2/3/4/5 разрядов. |
| %UCOUNTER% | Десятичный счетчик с подчеркиванием, 5 разрядов (первая итерация стерта, вторая итерация "_00002") |
| %UCOUNTER1%, %UCOUNTER2%, %UCOUNTER3%, %UCOUNTER4%, %UCOUNTER5% | Десятичный счетчик с подчеркиванием, 1/2/3/4/5 разрядов. |
| %% | Один знак %. |

Например, если ввести путь в виде *C:\Reports\%INTERVAL%_%COUNTER%"*, имена папок создаются таким образом: *C:\Reports\Day 2012-02-02_00001; C:\Reports\Day 2012-02-02_00002* и т. д.

Для отправки созданных отчетов по электронной почте необходимо ввести адрес сервера SMTP и адрес отправителя в меню **«Служебные программы»** > **«Настройки сервера»** > **«Другие настройки»**.

3. **«Созданные отчеты»** — ранее созданные отчеты можно просмотреть на вкладке **«Созданные отчеты»**. Дополнительные параметры отчетов доступны в контекстном меню соответствующих отчетов или групп отчетов, которое вызывается с помощью правой кнопки мыши. Отчеты можно сортировать по таким параметрам: **«Имя отчета»**, **«Дата»** , когда отчет был создан, **«Имя шаблона»** и **«Расположение»**. Выберите команду **Открыть** или дважды щелкните отчет в списке, чтобы открыть его. Если нажать отчет в списке, отобразится предварительный просмотр раздела ниже (если выбран этот параметр).

Шаблоны, помещенные в список **«Избранное»**, позднее можно использовать для создания новых отчетов. Чтобы переместить шаблон в «Избранное», щелкните его правой кнопкой мыши и выберите в контекстном меню команду **«Добавить в избранное»**.

#### 3.4.16.1 Панель мониторинга

**«Панель мониторинга»** — это набор отчетов, которые автоматически обновляются и предоставляют исчерпывающие сведения о состоянии системы. Каждый пользователь, имеющий доступ к консоли ERAC и имя пользователя, получает индивидуальный набор полностью настраиваемых панелей мониторинга. Эти параметры хранятся непосредственно на сервере, поэтому пользователь может получать доступ к одной и той же панели мониторинга из любого браузера.

По умолчанию панель мониторинга использует HTTP-сервер ERA и порт 443. Порты и сертификаты (для HTTPS) можно изменить в окне **расширенных параметров сервера** в консоли ERA Console. Открыть окна **«Панель мониторинга»** и **«Панель мониторинга»** можно в главном окне консоли ERAC на панели инструментов (значок с голубым облаком).

**ПРИМЕЧАНИЕ.**: Администратор должен подготовить шаблон для каждого отчета перед использованием этого отчета в панели мониторинга. В противном случае данные в отчетах могут отображаться неверно.

**ПРИМЕЧАНИЕ.**: По умолчанию **панель мониторинга** использует протокол HTTPS и самозаверяющий сертификат. Из-за этого в веб-браузере может появиться следующее предупреждение: *Сертификат безопасности этого веб-узла не был выпущен доверенным центром сертификации*. Учтите, что при использовании протокола HTTP имена пользователей и пароли будут переданы открытым текстом. Это может быть особенно небезопасно при использовании входа в систему Windows или в домен.

Установщик может создать самозаверяющий сертификат. Некоторые браузеры могут отображать предупреждение при обнаружении самозаверяющего сертификата. Также можно предоставить собственный сертификат либо в расширенном режиме установки, либо в любое время позднее с помощью редактора конфигурации ESET. Предоставленный сертификат может быть подписан доверенным центром сертификации или собственным корневым сертификатом пользователя. Поддерживаются следующие форматы сертификатов

X.509 и закрытых ключей.

- ASN — сертификат в кодировке ASN.1 DER и ключ в отдельных файлах.
- PEM — сертификат ASN в кодировке Base64 с дополнительными заголовками, сертификат и ключ в отдельных файлах.
- PFX — сертификат и закрытый ключ в одном файле-контейнере.

Невозможно использовать сертификат и ключ разного формата. Можно сменить протокол на HTTP, щелкнув **«Панель мониторинга»** (значок в виде голубого облака) в главном окне консоли ERAC и выбрав **«Настроить...»**, или же можно задать собственный сертификат (в формате PEM, кодировка X.509 base64) с помощью редактора конфигурации ESET (**«Сервис»** > **«Сервер»** > **«Параметры»** > **«Дополнительно»** > **«Изменить дополнительные параметры»** > **«Удаленный администратор»** > **«Сервер ERA»** > **«Параметры»** > **«Панели мониторинга»** > **«Ключ локального сертификата»**/**«Локальный сертификат»**).

**ПРИМЕЧАНИЕ.**: Панель мониторинга также поддерживает протокол IPv6. Например, *http://[::1]:8080*.

Можно воспользоваться набором готовых шаблонов (см. ниже) для **панели мониторинга** или создать собственные шаблоны.

- **«Сводка действий по защите от спама»** — отображает сводку по всем действиям ядра защиты от спама.
- **«Составная оценка защиты от спама»** — состав оценки защиты от спама и количество оцененных сообщений.
- **«Обзор клиентских подключений»** — отображение общих сведений о клиентских подключениях на основе их времени и состояния.
- **«Сводка по параметру ПрочиеСведения1 клиентов»** — подробный отчет с выбранной пользователем информацией (она должна быть задана заранее).
- **«Сводка по параметру ПрочиеСведения2 клиентов»** — подробный отчет с выбранной пользователем информацией (она должна быть задана заранее).
- **«Сводка по параметру ПрочиеСведения3 клиентов»** — подробный отчет с выбранной пользователем информацией (она должна быть задана заранее).
- **«Клиенты групп»** — количество клиентов в выбранных группах.
- **«Клиенты групп/все клиенты»** — процент клиентов в выбранных группах по отношению к общему количеству клиентов.
- **«Клиенты с активными угрозами»** — список клиентов с активными угрозами (не очищенными при сканировании) и информация об активных угрозах.
- **«Сводка действий с "серыми" списками»** — все сообщения из "серых" списков и предпринятые действия.
- **«Управляемые и неуправляемые компьютеры»** — компьютеры, которые на данный момент подключаются к серверу ERA (управляемые компьютеры), и компьютеры, которые не подключаются к ERA (неуправляемые). В качестве основы используется задача поиска по умолчанию.
- **«Сводка имени ОС»** — количество и тип клиентских операционных систем.
- **«Сводные сведения о продукте»** — количество и тип клиентских продуктов безопасности.
- **«Сводные сведения о состоянии защиты»** — количество клиентов и их состояние безопасности.
- **«Прогресс SMS-спама»** — вывод динамики SMS-спама.
- **«Нагрузка на серверную базу данных»** — полное время, в течение которого база данных была использована всеми потоками.
- **«Запросы серверной базы данных»** — количество SQL-запросов, выполненных в базе данных.
- **«Нагрузка на серверное оборудование»** — использование ресурсов процессора и ОЗУ на сервере.
- **«Мониторинг состояния сервера»** — состояние сервера и сведения об обновлении базы данных вирусов.
- **«Сравнительная динамика угроз»** — динамика представляющих опасность событий, связанных с указанными угрозами (которые отделяются с помощью фильтра), по сравнению с общим числом угроз.
- **«Динамика угроз»** — динамика событий, представляющих угрозу (в количественном выражении).
- **«Угрозы по объектам»** — количество предупреждений об угрозах по направлениям атаки (сообщения электронной почты, файлы, загрузочные секторы).
- **«Угрозы по сканерам»** — количество сообщений об угрозах, поступивших от отдельных программных модулей.
- **«Клиенты с наибольшим количеством разрывов подключений»** — список таких клиентов, упорядоченный до дате последнего подключения.
- **«Клиенты с наибольшим количеством сетевых атак»** — клиенты с наибольшим количеством сетевых атак.
- **«Клиенты с наибольшим количеством SMS-спама»** — список клиентов с наибольшим количеством SMS-спама.
- **«Клиенты с наибольшим количеством спама»** — список клиентов с наибольшим количеством сообщений спама.
- **«Клиенты с наибольшим количеством угроз»** — список наиболее «активных» клиентских рабочих станций (по количеству обнаруженных угроз).
- **«Основные получатели почты из "серого" списка»** — отображение адресатов, наиболее часто получающих сообщения из "серого" списка.
- **«Основные отправители почты из "серого" списка»** — отображение наиболее частых отправителей сообщений из «серого» списка.
- **«Наиболее часто встречающиеся сетевые атаки»** — список наиболее частых сетевых атак.
- **«Источники наиболее часто встречающихся сетевых атак»** — основные источники сетевых атак.
- **«Наиболее активные SMS-спамеры»** — отображение наиболее активных SMS-спамеров для указанных адресатов.
- **«Основные получатели спама»** — отображение адресатов, наиболее часто получающих спам.
- **«Основные отправители спама»** — отображение наиболее частых отправителей спама.
- **«Наиболее часто встречающиеся угрозы»** — список угроз, обнаруживаемых чаще всего.

- **«Основные угрозы по распространенности»** — список основных угроз по распространенности.
- **«Пользователи с наибольшим количеством угроз»** — список наиболее «активных» пользователей (с наибольшим числом обнаруженных угроз).
- **«Незарегистрированные компьютеры»** — отображение всех неуправляемых компьютеров, то есть компьютеров, которые не подключаются к серверу ERA. Также отображается время обнаружения нового неуправляемого компьютера.

Существующие шаблоны отчетов можно импортировать и экспортировать в *XML*-файл с помощью кнопки **«Импорт/экспорт»** . Конфликты имен при импорте (совпадение имен у существующих и импортируемых шаблонов) решаются путем добавления случайной строки после имени импортируемого шаблона.

Чтобы сохранить параметры настроенных отчетов в шаблон, нажмите кнопку **«Сохранить»** или **«Сохранить как»**. При создании нового шаблона нажмите кнопку **«Сохранить как»** и введите название шаблона. Щелкните **«Шаблоны по умолчанию»**, чтобы сбросить готовые шаблоны в исходное состояние (это не повлияет на пользовательские шаблоны).

- **«Параметры»**

**«Просмотр отчета»** — при нажатии на эту кнопку будет создана панель мониторинга и показан предварительный просмотр.

**«Отчет»**

**«Тип»** — тип отчета на базе готовых шаблонов. Это значение можно изменить для готовых шаблонов, использованных для создания пользовательских шаблонов.

**«Фильтр»**

**«Целевые клиенты»** — можно собирать **все** данные, данные **только выбранных клиентов/серверов/групп** или можно **исключить выбранные клиенты/серверы/группы**. Можно указать клиенты/серверы/группы, нажав кнопку **«...»** рядом с раскрывающимся меню **«Целевые клиенты»** в диалоговом окне **«Внести/убрать»**.

**«Угроза»** — также можно указать, должен ли отчет содержать **все** угрозы, **только выбранные угрозы**, или же можно **исключить выбранные угрозы**. Угрозы можно указать, нажав кнопку **«...»** рядом с этим раскрывающимся меню в диалоговом окне **«Внести/убрать»**.

Настроить другие параметры можно с помощью кнопки **«Дополнительные параметры»**. Эти настройки в основном относятся к данным в заголовке и в типах используемых графических диаграмм. Тем не менее, можно также фильтровать данные по состоянию выбранных атрибутов. Кроме того, можно выбрать, какой формат отчетов будет использоваться (HTML или CSV).

- **«Интервал»**

**«Время — последние X минут/часов/дней/недель/месяцев/лет»**, за которые нужно включить данные в отчет. Время основывается на времени сообщения о происшествии в ERA.

- **«Обновить»**

**«Интервал обновления браузера»** — выберите интервал обновления данных, получаемых с веб-сервера.

**«Интервал обновления сервера»** — выберите интервал отправки данных на веб-сервер.

#### 3.4.16.1.1 Список веб-серверов панели мониторинга

Щелкните стрелку рядом со значком панели мониторинга в главном меню, чтобы настроить параметры подключения в разделе **«Веб-серверы панели мониторинга»**.

- **«Веб-серверы панели мониторинга»** — список доступных веб-серверов панели мониторинга.
- **«Удалить»** — если нажать эту кнопку, выбранный веб-сервер панели мониторинга будет удален из списка.
- **«По умолчанию»** — устанавливает выбранный веб-сервер панели мониторинга веб-сервером по умолчанию. Этот параметр будет доступен первым в раскрывающемся меню (после нажатия стрелки рядом со значком панели мониторинга) и откроется первым, если щелкнуть сам значок панели мониторинга.

- **«Протокол»** — можно выбрать между протоколами HTTP и HTTPS с самозаверяющим сертификатом.
- **«Имя узла или IP-адрес»** — отображает имя узла или IP-адрес выбранного веб-сервера панели мониторинга. Кроме того, можно ввести новое имя узла или новый IP-адрес и нажать кнопку **«Добавить/сохранить»**, чтобы сохранить данные и добавить веб-сервер панели мониторинга в список.
- **«Комментарий»** — необязательный комментарий или описание для выбранного веб-сервера панели мониторинга.

**ПРИМЕЧАНИЕ.**: Панель мониторинга также поддерживает протокол IPv6. Например, *http:///[::1]:8080*.

#### 3.4.16.2 Образец сценария отчета

Чтобы добиться максимальной сетевой безопасности для клиентов, необходимо иметь хорошее представление о состоянии безопасности сети. Можно с легкостью создавать отчеты с подробным описанием угроз, обновлений, версии клиентских продуктов и т. п. (дополнительные сведения см. в разделе Отчеты 44). Как правило, всю необходимую информацию содержит еженедельный отчет. Тем не менее, могут возникнуть ситуации, в которых окажется необходима дополнительная осторожность, например при обнаружении угрозы.

В качестве примера создадим параметрическую группу с названием *«Карантин»*. Эта группа будет содержать только те компьютеры, в которых угроза была обнаружена и устранена во время последней проверки по требованию. Зададим это условие, установив флажок **При последнем сканировании обнаружена угроза**. Для создания параметрической группы следуйте инструкциям в разделе Параметрические группы 95.

**Примечание.** При создании группы *«Карантин»* убедитесь в том, что параметр **«Закрепить»** отключен. При этом компьютер будет назначен динамически и удален, как только условия перестанут выполняться.

Создайте отчет *«Компьютеры в карантине»*. Для создания отчета следуйте инструкциям в разделе Отчеты 44.

Ниже указаны конкретные параметры для данного примера.

- Параметры в разделе **«Параметры»**:

Тип: «Подробный отчет по карантину»
«Вид»: «Голубая схема»
«Целевые клиенты»: «Только выбранные группы»
«Угроза»: «н/д»

- Параметры шаблона **«Интервал»**:

«Данный»: «День»

- Параметры шаблона **«Планировщик»**:

«Частота»: «Ежедневно»
«Кажд.»: «1 день»

**Совет.** Результаты можно сохранить в базы данных отчетов или указать папку, в которой будут сохранены копии отчетов. Отчеты также можно отправить по электронной почте. Все эти параметры вызываются с помощью кнопки **«Выбрать путь...»**.

Созданные отчеты можно просматривать в разделе **«Отчеты»** в шаблоне **«Созданные отчеты»**.

**Выводы.** Была создана параметрическая группа *Карантин* с компьютерами, на которых была обнаружена угроза в ходе последней проверки по требованию. Затем был создан автоматизированный отчет, который будет ежедневно информировать нас о том, какие компьютеры принадлежат группе *«Карантин»*, что дает хорошее представление о состоянии сетевых клиентов, позволяя держать потенциальную угрозу под контролем.

**Совет.** Чтобы отобразить данные журнала последней проверки, можете воспользоваться отчетом типа **«Подробный отчет по сканеру»**.

### 3.4.17 Вкладка «Удаленная установка»

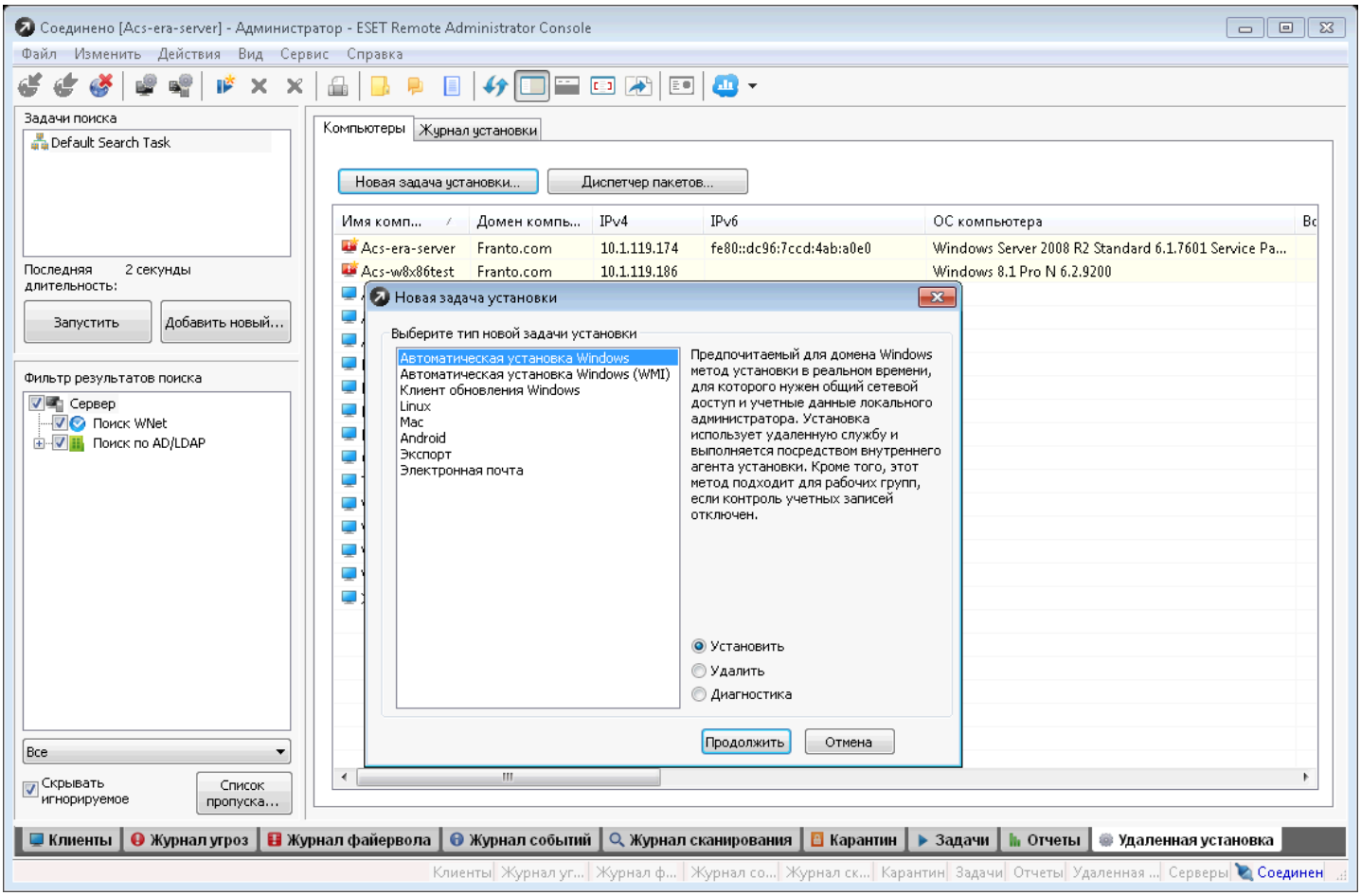
На этой вкладке представлены параметры различных способов удаленной установки приложений ESET Endpoint Security или ESET Endpoint Antivirus на клиентские компьютеры. Дополнительные сведения см. в разделе Удаленная установка 72.

1. Чтобы найти компьютер, можно воспользоваться задачей поиска по умолчанию или создать новую. Чтобы создать новую задачу, выберите **Добавить новую**. Будет запущен мастер задачи поиска в сети 52. Чтобы запустить задачу поиска, нажмите кнопку **«Запуск»**. Чтобы изменить выбранную задачу поиска, щелкните задачу правой кнопкой мыши и выберите **Изменить**.

2. Результаты поиска будут отфильтрованы с помощью служебной программы **Фильтр результатов поиска** в разделе ниже. Фильтрация результатов не влияет на текущую задачу поиска. Дополнительные условия поиска в раскрывающемся меню приведены ниже.

- **Все**: отображает все компьютеры, видимые решению ERAS.
- **Неуправляемые и новые**: отображает компьютеры, которые не отображены на вкладке **Клиенты** в ERA Console.
- **Управляемые с предупреждением о последнем подключении**: отображает компьютеры, которые приведены на вкладке **Клиенты** в ERA Console и которые некоторое время не подключались (по умолчанию — 3 дня). Период настраивается в меню **Сервис** > **Настройки консоли** > **Цвета** > **Клиенты: Соединение** > **Укажите промежуток времени для цвета предупреждения последнего соединения**.
- **Скрывать пропускаемые** — по умолчанию этот параметр включен. Он скрывает компьютеры из списка пропуска, созданного администратором. Чтобы добавить любой компьютер в список пропуска, просто щелкните нужный компьютер правой кнопкой мыши и в контекстном меню выберите пункт **Добавить к списку игнорирования**. . Кроме того, чтобы редактировать список пропуска, вы можете нажать кнопку **Список пропуска** и применить нужные изменения в окне **Список пропуска для удаленной установки**.

3. Результаты поиска для текущей задачи поиска отображаются в основном разделе **Компьютеры**. В нем вы можете управлять пакетами установки 54 (для этого нужно нажать кнопку **Диспетчер пакетов**) и запускать удаленную автоматическую установку 74 (для этого нужно нажать кнопку **Новая задача установки**).




Кроме стандартных пунктов, которые есть в контекстных меню решения ERA Console, контекстное меню вкладки **Компьютеры** содержит еще приведенные ниже уникальные пункты.

- **Добавить к списку игнорирования...** — добавление выбранных компьютеров в **список пропуска**.
- **Информация WMI** — указание сведений для входа выбранного компьютера в WMI.
- **Свойства** — открывает окно **Свойства**, содержащее важные сведения о выбранном компьютере.

Описание других параметров контекстного меню см. в разделе Контекстное меню 31.

### 3.4.17.1 Мастер задачи поиска в сети

Задача поиска — это набор параметров, используемых для поиска компьютеров в сети. Созданные задачи поиска хранятся непосредственно на сервере, и они доступны для всех администраторов.

Вы можете использовать стандартные задачи поиска по умолчанию, которые периодически запускаются (их также можно запустить вручную), а также задачи поиска по всей сети. Результаты поиска этой задачи хранятся на сервере. Эту задачу можно изменить, но как если она запущена, ее нельзя остановить до ее завершения.

Пользовательские параметры задачи хранятся на сервере, но результаты поиска отправляются только на консоль, из которой они были запущены. Эти поисковые задачи можно запускать только вручную.

Чтобы создать новую задачу, нажмите кнопку **Добавить новую**. Появится окно **Мастер задачи поиска в сети: способы сканирования**, в котором можно выбрать способы поиска в сети (можно выбрать сразу несколько).

- **Active Directory или LDAP** — этот параметр позволяет выбрать филиалы Active Directory, в которых нужно искать компьютеры. С его помощью можно также **добавить отключенные компьютеры**.
- **Сеть Windows (WNet)** — поиск компьютеров в сети Windows.
- **Оболочка** — поиск всех компьютеров в расположениях сети (Сетевое окружение Windows).
- **IP-адрес** — позволяет выбрать **диапазон IP-адресов** или **маску IP-адреса**, которые нужно использовать во время поиска, или можно указать **настраиваемый список IP-адресов**. Компьютеры ищутся с помощью

доступа к их портам (который может быть настроен). Можно также использовать проверку связи (особенно рекомендуется при поиске компьютеров с ОС Linux).

- **Настраиваемый список компьютеров** — настройка списка компьютеров или импорт настраиваемого списка из текстового файла с помощью кнопки **Импорт из файла**.

Кроме того, можно выбрать параметр **Использовать WMI для получения дополнительной информации о найденных компьютерах**.

Щелкните **Далее**. На следующем экране вы можете решить, нужно ли выбранную задачу поиска сохранять временно (для этого снимите флажок **Сохранять на панели задач поиска**) или навсегда в **панели задач поиска** (это вариант по умолчанию). Вы сможете указать также то, нужно ли задачу запускать сразу после нажатия кнопки **Готово** (это вариант по умолчанию) или нет (для этого снимите флажок **Запустить сейчас**).

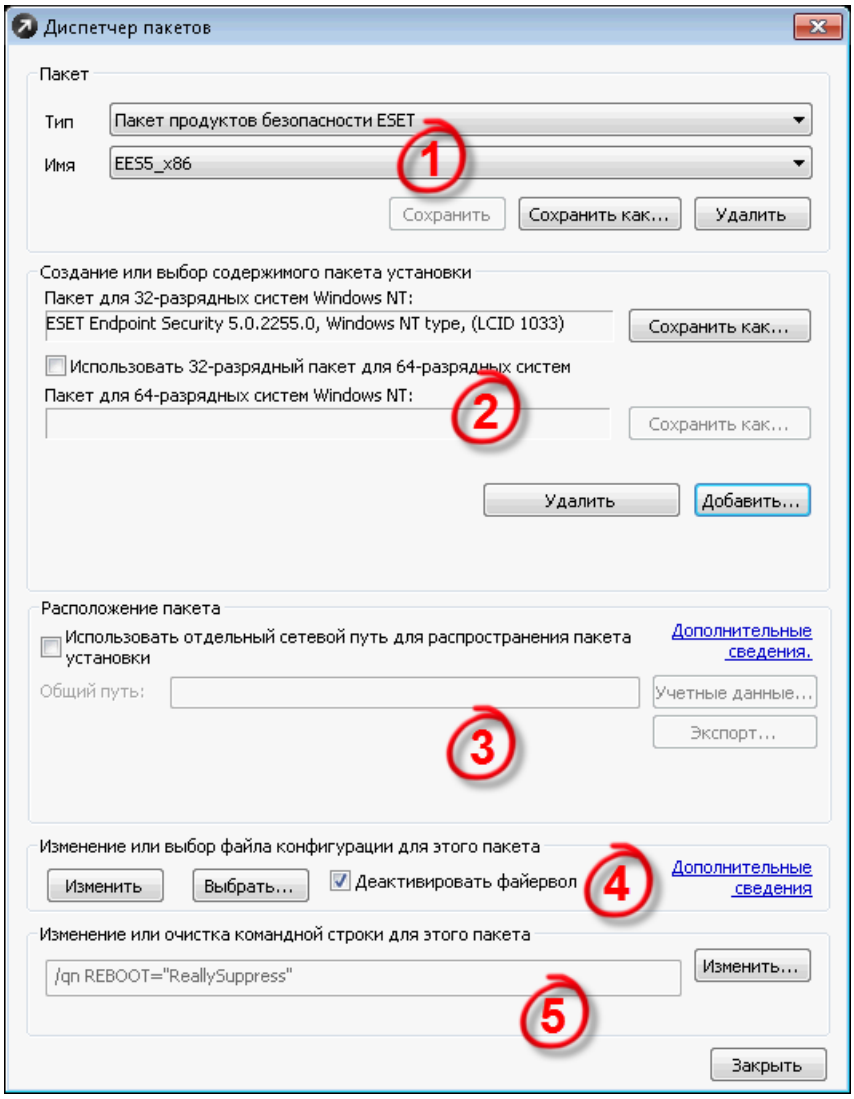
Чтобы запустить задачу, нажмите кнопку **Запустить** на вкладке **Удаленная установка**.

**ПРИМЕЧАНИЕ.**: Если служба работает под локальной системной учетной записью, компьютеры не могут быть найдены с помощью поиска в оболочке и поиска Wnet, поскольку локальная системная учетная запись не имеет разрешений на выполнение такого поиска. Для решения этой проблемы измените пользователей или используйте другой метод поиска.

**ПРИМЕЧАНИЕ**. Если нужно повысить скорость выполнения задачи поиска при оценке диапазонов IP-адресов и информации WMI, укажите более высокое значение для параметра **Максимальное количество потоков поиска** (*Сервис* > ESET Configuration Editor > *Remote Administrator* > ERA Server > *Параметры* > *Удаленная установка*).

### 3.4.17.2 Диспетчер пакетов

Удаленная установка запускается через консоль ERAC. Для запуска установочных пакетов из консоли ERAC перейдите на вкладку **Удаленная установка** и выберите вкладку **Компьютеры**. Нажмите кнопку **Диспетчер пакетов**, чтобы открыть окно **Диспетчер пакетов**.




Каждый пакет установки имеет свое **имя** (см. (1) на рисунке выше). Остальные разделы диалогового окна связаны с содержимым пакета, которое применяется после его успешной доставки на целевую рабочую станцию.

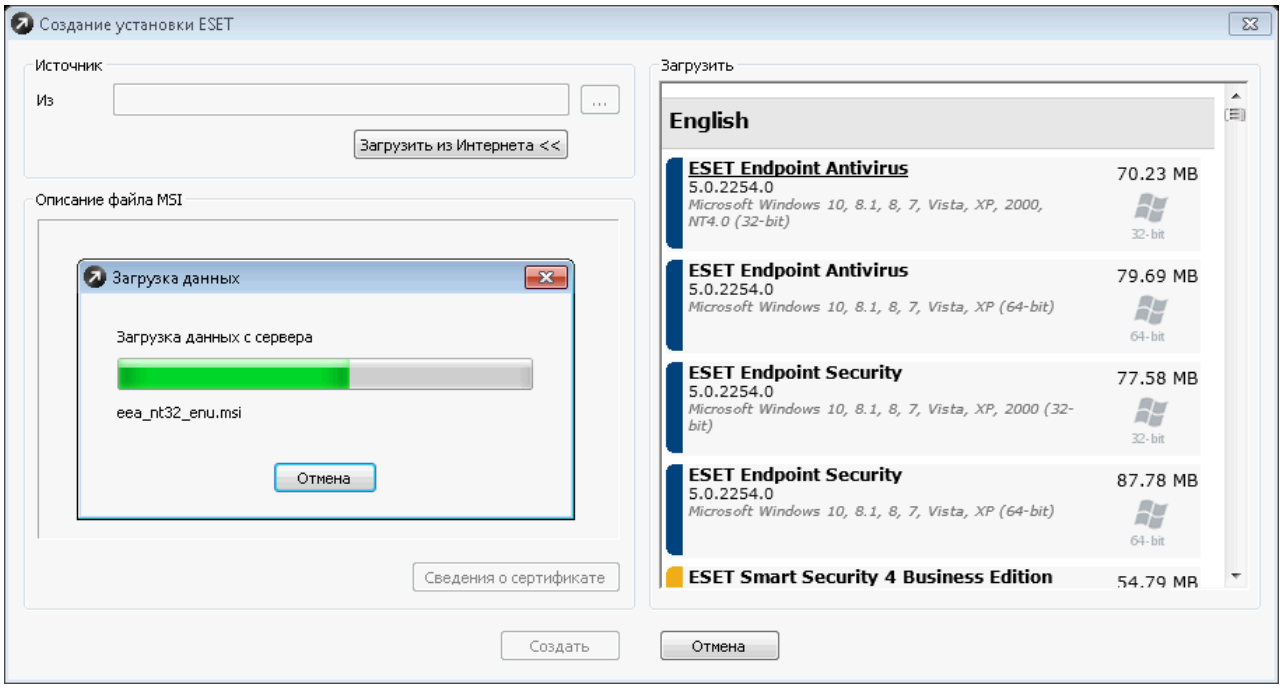
Раскрывающееся меню **«Тип»** в разделе (1) предоставляет доступ к дополнительным функциям ERA. Продукты ESET для безопасности поддерживают не только удаленную установку, но и удаленное удаление с помощью функции **Удаление продуктов безопасности ESET для Windows и NOD32 версии 2**. Можно также удаленно установить внешнее приложение, выбрав пункт **Пользовательский пакет**. Это особенно удобно, если нужно запускать различные сценарии и исполняемые файлы на клиентском компьютере, в том числе средства для удаления сторонних продуктов безопасности или автономные средства очистки. С помощью меню **Входной файл пакета** можно указать пользовательские параметры командой строки. Дополнительные сведения см. в разделе Установка продуктов сторонних производителей с помощью программы ERA 186.

Каждому пакету автоматически присваивается удаленный установщик ESET — агент, который облегчает установку и обмен данными между целевыми рабочими станциями и сервером ERAS. Файл агента удаленной установки ESET называется *einstaller.exe*. Он содержит имя сервера ERAS, а также имя и тип пакета, к которому относится. В следующем разделе дано подробное описание агента установки.

**Установочные файлы клиентского решения ESET (2)**

Чтобы выбрать источник пакета установки, нажмите кнопку **Добавить**. У вас есть два варианта:

1. Вы можете выбрать пакет установки локально, нажав кнопку «...».
2. Или же воспользуйтесь параметром **Загрузить из Интернета** (рекомендуется). В разделе **Загрузка** должен отобразиться список пакетов. Чтобы запустить загрузку, выберите язык, щелкните нужный пакет и выберите папку назначения.




**Примечание.** Для типа пакетов **Продукты ESET для безопасности для ОС Windows** рекомендуется устанавливать флажок **Использовать 32-разрядный пакет для 64-разрядных систем** только при установке решения ESET, например сервера или консоли ESET Remote Administrator. Его не следует устанавливать при установке «настоящего» продукта безопасности ESET (например, ESET Endpoint Security или ESET Endpoint Antivirus), так как на 64-системе нужна 64-разрядная версия продукта (попытка установить 32-разрядную версию будет неуспешной).

**Расположение пакета (3)**

Пакеты установки размещены на сервере ERAS в следующей папке:

*%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\packages*

Для пакетов удаленной установки здесь можно выбрать другое сетевое расположение.

**Конфигурационный XML-файл для клиентских решений ESET (4)**

При создании нового пакета установки пароль основного сервера для подключения к серверу ERA останется пустым. Нажмите кнопку **Изменить**, чтобы изменить XML-конфигурацию этого пакета, и (при необходимости) задайте пароль в разделе **Удаленное администрирование** соответствующего продукта.

Параметр **Отключить файервол** по умолчанию включен, чтобы файервол решения ESET Endpoint Security был отключен. Это позволяет избежать блокировки подключения сервера ERA Server к клиенту. Включить файервол можно позже, отправив задачу конфигурации 89 клиенту. В этой задаче конфигурации нужно найти элемент "*Защита рабочих станций Windows, версия 5 > Персональный файервол > Параметры > Интеграция файервола в систему: персональный файервол неактивен*" и выбрать значение **Все функции активны**.

**Примечание**: При отключении или включении параметра «Отключить файервол» изменяются два свойства параметра. Одно из них отображается в ESET Configuration Editor, а другое — только в XML-файле конфигурации. Если любое из этих свойств параметра не задано (например, одно задано, а другое — нет) или не имеет значение в диапазоне от 1 до 10, то в поле **Значение** нужно выбрать параметр **Сканировать только протоколы уровня приложений**. В этом случае поле флажка **Отключить файервол** полностью заполняется синим цветом.

Если вы настроили пароль для сервера ERA (**Сервис** > **Параметры сервера** > **Безопасность** > **Пароль для**

**клиентов (продукты ESET для обеспечения безопасности)**), то он будет автоматически использоваться в создаваемом пакете. Вследствие этого им будут пользоваться клиентские компьютеры для подключения к серверу ERA. Если пароль к серверу ERA был недавно изменен, то управляемые клиенты не смогут подключаться к серверу, даже если в сервере ERA включен параметр **Включить доступ без аутентификации для клиентов (продукты ESET для обеспечения безопасности)**. В таком случае нужно запустить задачу конфигурации 89 для управляемых клиентов.

**Параметры командной строки, назначенные пакету (5)**

На процесс установки могут влиять несколько параметров 56. Их можно использовать как при выполнении администратором непосредственной установки на рабочей станции, так и для удаленной установки.

#### 3.4.17.2.1 Параметры командной строки

При удаленной установке значения параметров выбираются в процессе формирования установочных пакетов, а затем автоматически применяются на целевых клиентах.

Дополнительные параметры для ESET Endpoint Security и ESET Endpoint Antivirus можно ввести также после имени *MSI*-установщика (например, *eea_nt64_ENU.msi /qn*), если удаленная установка выполняется с помощью интерфейса командной строки в операционной системе компьютера.

- **/qn** — режим установки без вывода информации на экран (диалоговые окна не показываются).
- **/qb!** — вмешательство пользователя невозможно, но ход установки отображается на индикаторе в процентах.
- **REBOOT ="ReallySuppress"** — подавление перезагрузки после установки программы.
- **REBOOT ="Force"** — автоматическая перезагрузка после установки.
- **REMOVE=...** — выключает установку выбранного компонента. Параметры команд для каждого компонента перечислены ниже.

  **Emon** — защита почтового клиента
  **Antispam** — защита от спама
  **Dmon** — защита документов
  **ProtocolScan** — фильтрация протоколов
  **Firewall** — персональный файервол
  **eHttpServer** — обновление зеркала сервера
  **eDevmon** — контроль устройств
  **MSNap** — Microsoft NAP
  **eParental** — контроль доступа в Интернет

- **REBOOTPROMPT =""** — после установки открывается диалоговое окно, предлагающее перезагрузить компьютер (этот параметр нельзя использовать вместе с параметром */qn*).
- **ADMINCFG ="path_to_xml_file"** — во время установки к продуктам безопасности ESET применяются параметры, заданные в указанных XML-файлах. Этот параметр не требуется при удаленной установке. В установочных пакетах содержится собственная *XML*-конфигурация, применяемая автоматически.
- **PASSWORD="password"** — этот параметр необходимо добавить, если настройки клиентского продукта ESET защищены паролем.
- **/SILENTMODE** — режим автоматической установки — диалоговые окна не показываются.
- **/FORCEOLD** — установка старой версии поверх уже установленной новой.
- **/CFG ="path_to_xml_file"** — во время установки к клиентским решениям ESET применяются параметры, заданные в указанных *XML*-файлах. Этот параметр не требуется при удаленной установке. В установочных пакетах содержится собственная *XML*-конфигурация, применяемая автоматически.
- **/REBOOT** — автоматическая перезагрузка после установки.

- **/SHOWRESTART** — после установки открывается диалоговое окно, предлагающее перезагрузить компьютер. Этот параметр можно использовать только вместе с параметром *SILENTMODE*.
- **/INSTMFC** — установка библиотек MFC для операционной системы Microsoft Windows версии 9x, необходимых для правильной работы программы ERA. Этот параметр можно использовать всегда, даже если библиотеки MFC доступны.

**ПРИМЕЧАНИЕ.** Если UAC включен на клиентском решении, настройки безопасности UAC по умолчанию для Windows Vista/7/2008 требуют перед выполнением любой программы подтверждения пользователя. Попытка удаленно установить клиентские решения и использование любого из вышеперечисленных параметров приведет к открытию на клиенте всплывающего окна, которое будет требовать вмешательства пользователя. Чтобы избежать вмешательства пользователя, запустите установку с помощью следующей команды: *C:\Windows\System32\msiExec.exe -i path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"* где *C:\Windows\System32\msiExec.exe -i* — это исполняемый файл компонента установщика Windows и параметр установки и *path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"* — это путь файла установки и файла настроек продукта безопасности, за которым следует параметр подавления вмешательства пользователя.

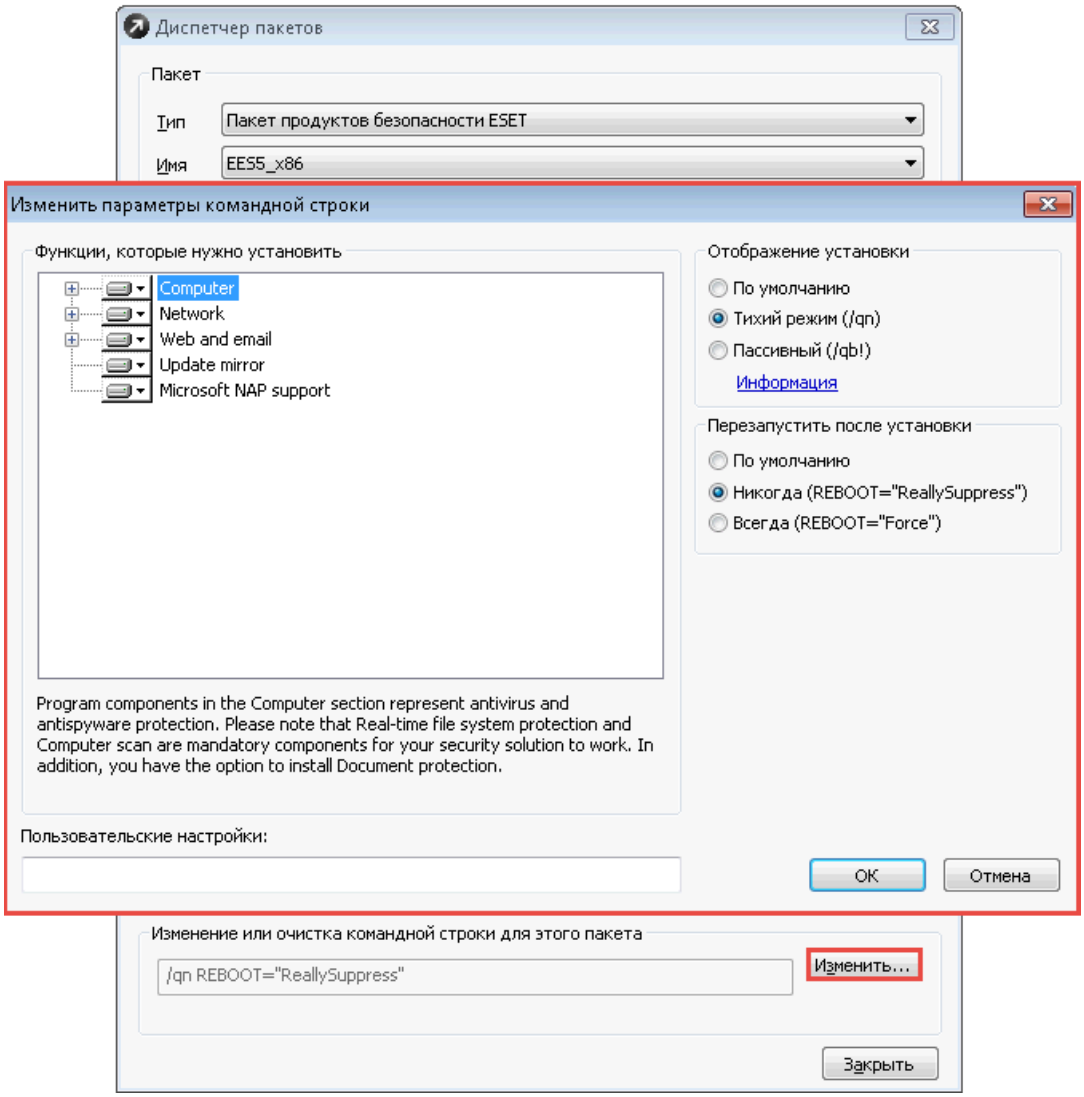
В разделе **Создание или выбор содержимого пакета установки** (2) администратор может создать автономный установочный пакет с предопределенной конфигурацией из уже существующего установочного пакета (кнопка **Сохранить как**). Такие установочные пакеты запускаются на клиентской рабочей станции, на которую нужно установить программу. Пользователю необходимо только запустить пакет, после чего продукт устанавливается автоматически без подключения к серверу ERAS во время установки.

**ПРИМЕЧАНИЕ.** При добавлении конфигурации в установочный *MSI*-файл цифровая подпись этого файла становится недействительной.

***Внимание!*** В системах Microsoft Windows Vista и старше настоятельно рекомендуется выполнять автоматическую удаленную установку (с параметром */qn*, */qb*). В противном случае взаимодействие с пользователем может привести к сбою удаленной установки из-за превышения интервала ожидания.

### 3.4.17.2.2 Параметры пакета установки

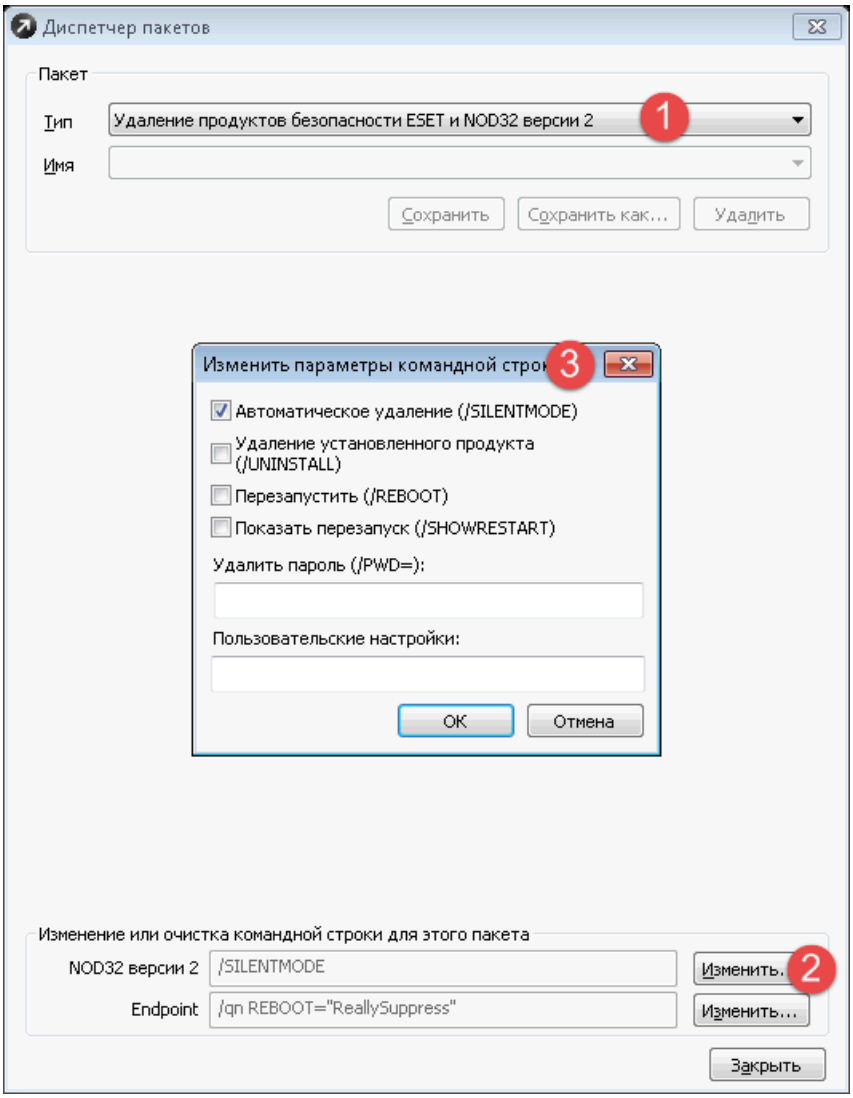
При удаленной установке значения параметров выбираются в процессе формирования установочных пакетов, а затем автоматически применяются на целевых клиентах.




Как показано на рисунке выше, у вас есть возможность выбрать, какие части пакета не нужно устанавливать. Кроме того, вы можете использовать дополнительные параметры 56 для ESET Endpoint Security и ESET Endpoint Antivirus в поле ввода **Пользовательские параметры**.

### 3.4.17.2.3 Параметры удаления ESET Endpoint Antivirus

В случае удаленного удаления программы ESET Endpoint Antivirus (или, если точнее, NOD 32) используемую по умолчанию конфигурацию можно с легкостью изменить, нажав кнопку **Изменить** возле поля **NOD32 версии 2** в окне **Диспетчер пакетов** после выбора параметра **Удаление продуктов ESET для безопасности для ОС Windows и NOD32 версии 2**.

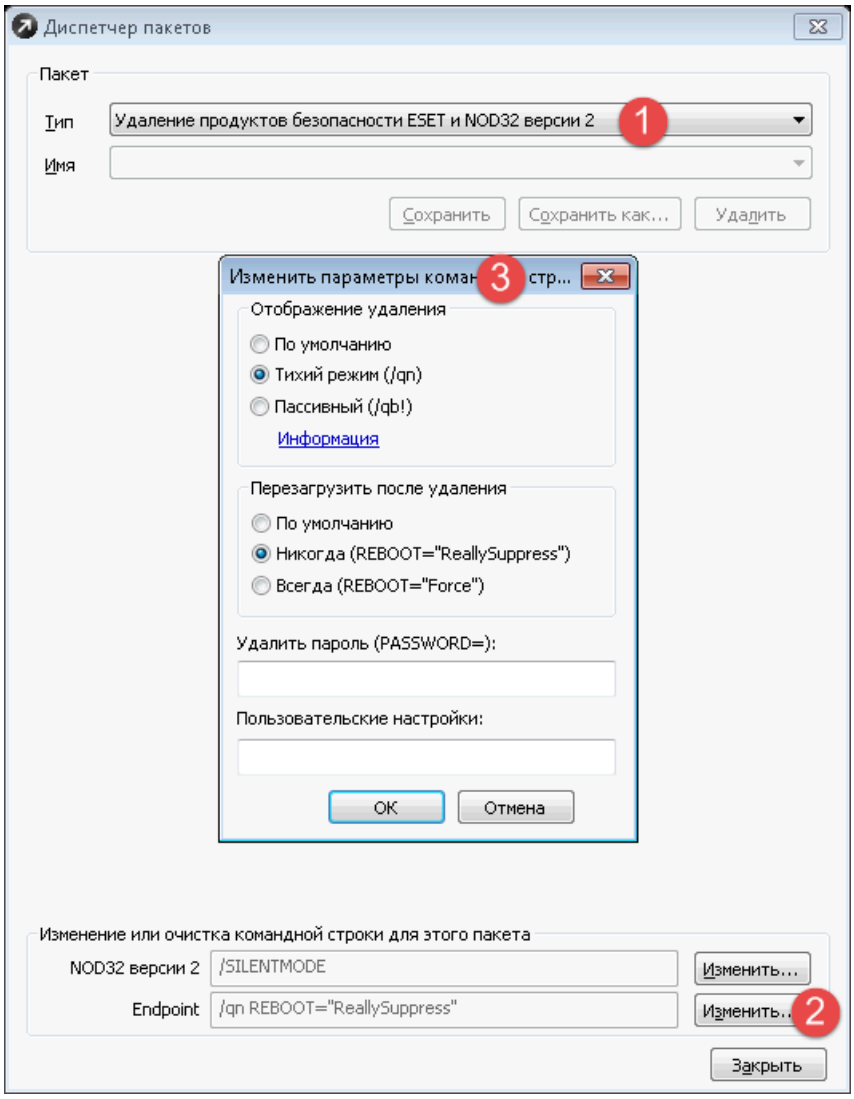



Окно **Изменение параметров командной строки** позволяет применять разные параметры, например **Автоматическое удаление** (от пользователя целевого компьютера не требуется подтверждение), **Перезапуск** (после удаления целевой компьютер перезапускается) и некоторые другие. Если вы выберите какие-нибудь из них, они будут переданы в качестве параметров в поле **NOD32 версии 2** окна **Диспетчер пакетов** после закрытия окна **Изменение параметров командной строки** с помощью кнопки **ОК**.

В поле **Пользовательские параметры** окна **Изменение параметров командной строки** вы можете ввести дополнительные параметры командной строки 56. Например, вы можете использовать */L*v "my_log.log"*, чтобы записывать журналы удаления в файл *my_log.log*. Потом этот файл журнала можно искать с помощью функции поиска в операционной системе Windows. Или же вы можете использовать абсолютный путь для файла *my_log.log* в поле **Пользовательские параметры**.

### 3.4.17.2.4 Параметры удаления ESET Endpoint Security

В случае удаленного удаления программы ESET Endpoint Security используемую по умолчанию конфигурацию можно с легкостью изменить, нажав кнопку **Изменить** возле поля **Конечная точка** окна **Диспетчер пакетов** после выбора параметра **Удаление продуктов ESET для безопасности для ОС Windows и NOD32 версии 2**.



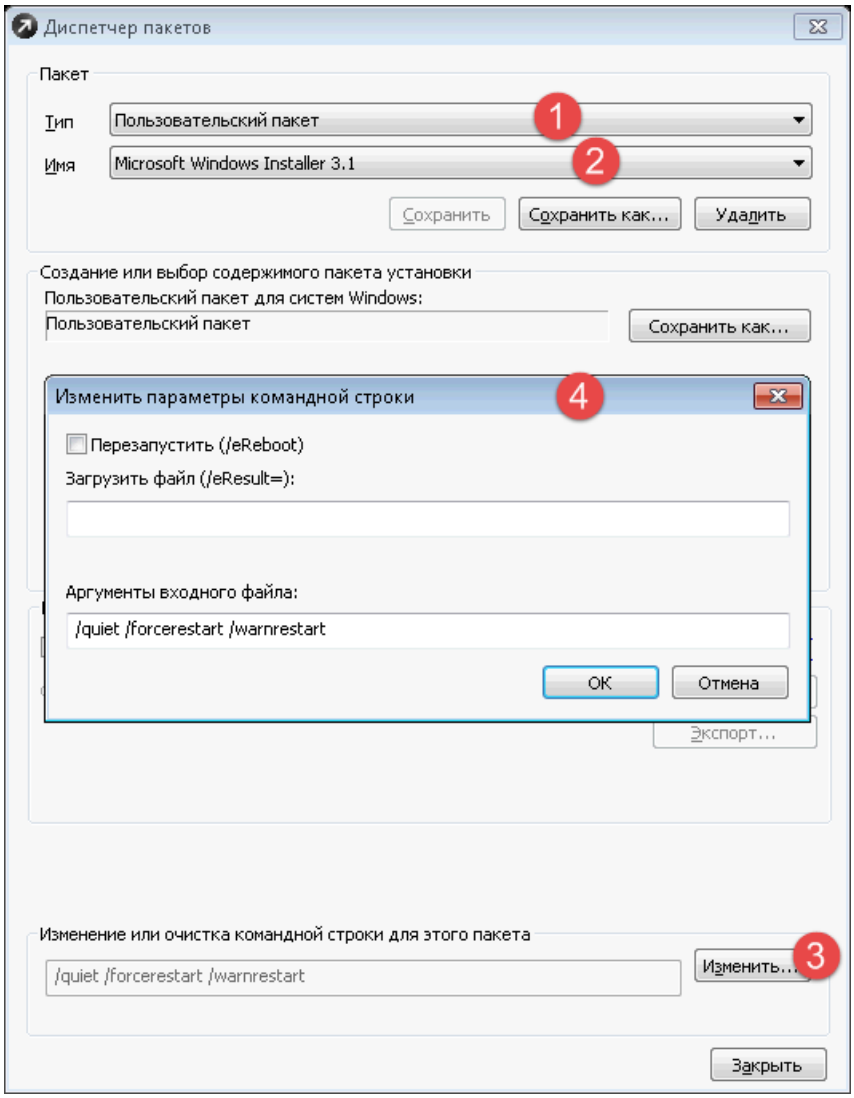

Когда открывается окно **Изменение параметров командной строки**, можно изменять выбранные параметры, например можно выбрать **пассивный** тип установки (в таком случае пользователь целевого компьютеры будет видеть процесс удаления), или можно выбрать принудительный перезапуск целевого компьютера после завершения процесса удаления.

В поле **Пользовательские параметры** окна **Изменение параметров командной строки** вы можете ввести дополнительные параметры командной строки 56. Например, вы можете использовать */L*v "my_log.log"*, чтобы записывать журналы удаления в файл *my_log.log*. Потом этот файл журнала можно искать с помощью функции поиска в операционной системе Windows. Или же вы можете использовать абсолютный путь для файла *my_log.log* в поле **Пользовательские параметры**.

**ПРИМЕЧАНИЕ**. Если для какой-либо настройки выбрать значение «По умолчанию», к ней не будут применяться параметры.

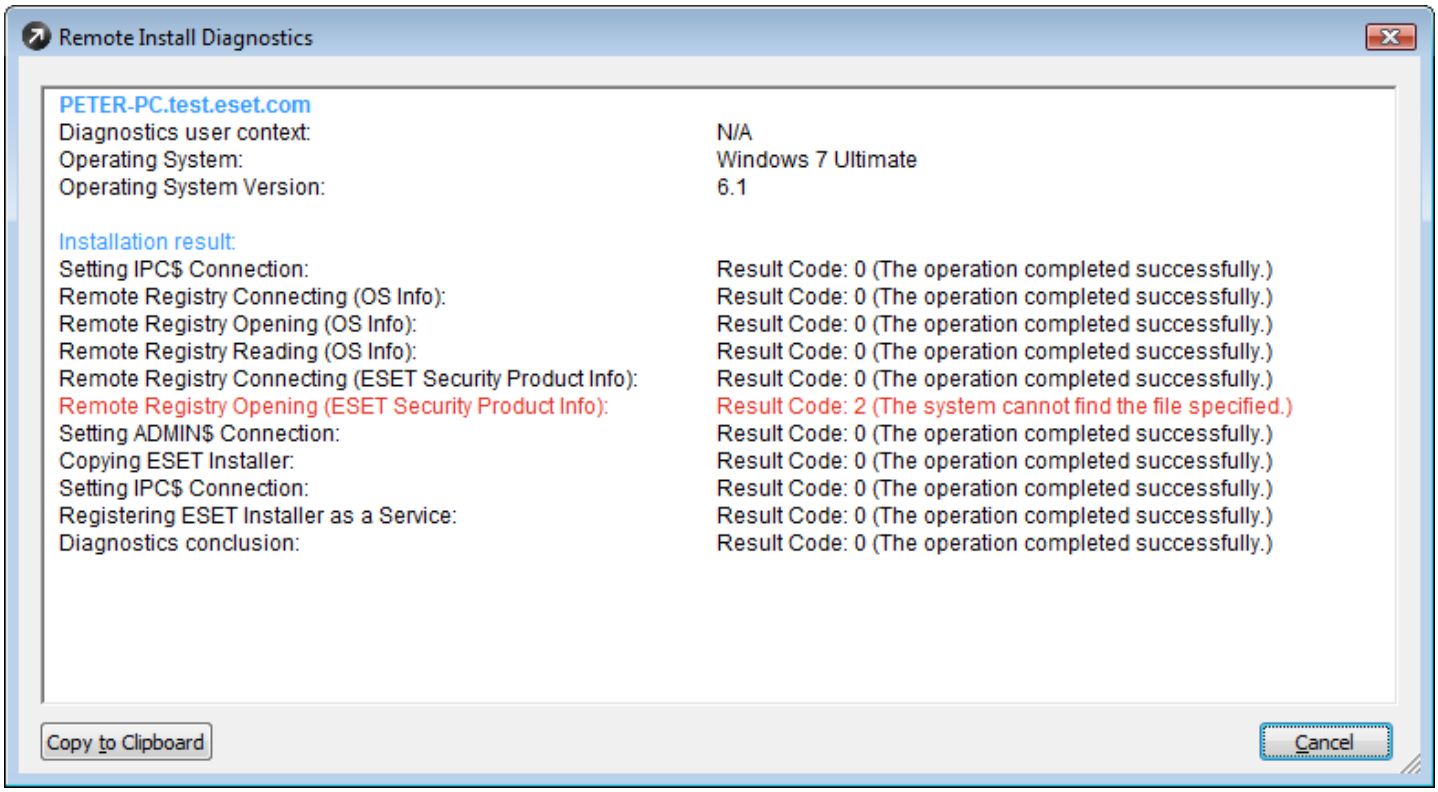
### 3.4.17.2.5 Параметры командной строки для пользовательского пакета

Когда вы настраиваете **пользовательский пакет** в **диспетчере пакетов**, то, если пользовательский пакет поддерживает некоторые пользовательские параметры, вы можете определить любой поддерживаемый параметр в поле **Аргументы входного файла** окна **Изменение параметров командной строки**. Нажмите кнопку **Изменить** возле поля **Изменение или очистка командной строки для этого пакета**, чтобы получить доступ к окну **Изменение параметров командной строки**.




Если пользовательский сценарий должен записать результаты в файл на целевом компьютере, вы можете задать имя файла в поле **Загрузка файла (/eResult=)** окна **Изменение параметров командной строки**, чтобы сервер ERA Server мог загружать файл после установки пользовательского пакета и чтобы содержимое файла можно было просматривать через внутреннюю программу для просмотра 64 решения ERA Console.

### 3.4.17.3 Диагностика удаленной установки




- **Установка подключения IPC$**:

  У администратора должны быть права локального администратора для всех клиентских компьютеров.

  Общие ресурсы необходимо устанавливать и включать на клиентах.

  На сетевом файерволе должны быть включены общие ресурсы (порты 445 и 135–139).

  Пароль администратора Windows Administrator не может быть пустым.

  Параметр «Простой общий доступ к файлам» должен быть активирован в смешанной среде рабочих групп и доменов.

  Убедитесь, что служба сервера выполняется на клиентском компьютере.

- **Подключение к удаленному реестру (данные об ОС)**:

  На клиенте должна быть включена и запущена служба удаленного реестра.

- **Открытие удаленного реестра (данные об ОС)**:

  То же + администратор должен иметь права на управление клиентским регистром.

- **Чтение удаленного реестра (данные об ОС)**:

  Администратор должен иметь права на чтение клиентского регистра. Если предыдущая операция выполнена успешно, эта тоже будет выполнена успешно.

- **Подключение к удаленному реестру (данные о продукте безопасности ESET)**:

  администратор должен иметь права на управление HKEY_LOCAL_MACHINE/SOFTWARE/ESET (или всего филиала HKEY_LOCAL_MACHINE/SOFTWARE).

- **Открытие удаленного реестра (данные о продукте безопасности ESET)**:

  Убедитесь, что служба удаленного реестра запущена на клиентском компьютере.

- **Установка подключения ADMIN$**:

  административный общий ресурс ADMIN$ должен быть включен;

- **Копирование установщика ESET**:

На сервере должны быть открыты порты 2222, 2223 и/или 2224, эти же порты должны быть разрешены в файерволе сети.

- **Установка подключения IPC$**:

Если эта операция успешна выполнена в диагностике запроса данных, она должна быть успешно выполнена и здесь.

- **Регистрация службы установщика ESET**:

Убедитесь, что у вас достаточно прав для запуска файла einstaller.exe на целевом компьютере(ах).

**ПРИМЕЧАНИЕ.**: Если во время диагностики возникла ошибка, можно начать устранение неполадок на основе этой информации. См. раздел Требования 72 перед инсталляцией и раздел Часто встречающиеся коды ошибок 179, чтобы проанализировать коды ошибок.

#### 3.4.17.4 Журнал установки

На вкладке **Журнал установки** вкладки **Удаленная установка** перечислены задачи и их атрибуты. Отображаются также выполняемые, ожидающие и завершенные задачи. Здесь можно изменить количество элементов, которые будут отображаться, а также щелкнуть правой кнопкой мыши задачи в списке для вызова команд управления и обслуживания. Раскрывающееся меню **«Элементы для отображения»** используется для увеличения или уменьшения количества элементов на странице, прилегающие кнопки навигации — для переключения между доступными страницами.

Информацию, которая отображается на вкладке «Журнал установки», можно также фильтровать. Установите флажок возле параметра **Использовать фильтр** в левой части окна, чтобы активировать фильтр. Затем задайте критерии фильтрации задач: **Только компьютеры типа (?,*)/Исключать компьютеры типа (?,*)**. Введите имя компьютера в поле **Имя компьютера**.. Вы можете использовать также знаки подстановки, например *Ком* вместо целого слова «Компьютер». Если нажать кнопку **Сброс**, критерии фильтрации будут удалены, а фильтр выключен.

- **«Имя задачи»** — имя задачи, для предопределенных задач оно совпадает с типом задачи.
- **«Тип задачи»** — тип задачи. Дополнительную информацию см. в разделе Задачи 88.
- **«Состояние»** — текущее состояние задачи.
- **«Описание»** — краткое описание параметра задачи.
- **Дата развертывания** — время, прошедшее с момента выполнения задачи.
- **«Дата получения»** — время до/прошедшее с момента получения задачи до момента ее выполнения.
- **«Комментарий»** — примечание, присвоенное задаче установки.

Если дважды щелкнуть задачу установки, откроется окно **«Свойства»** .

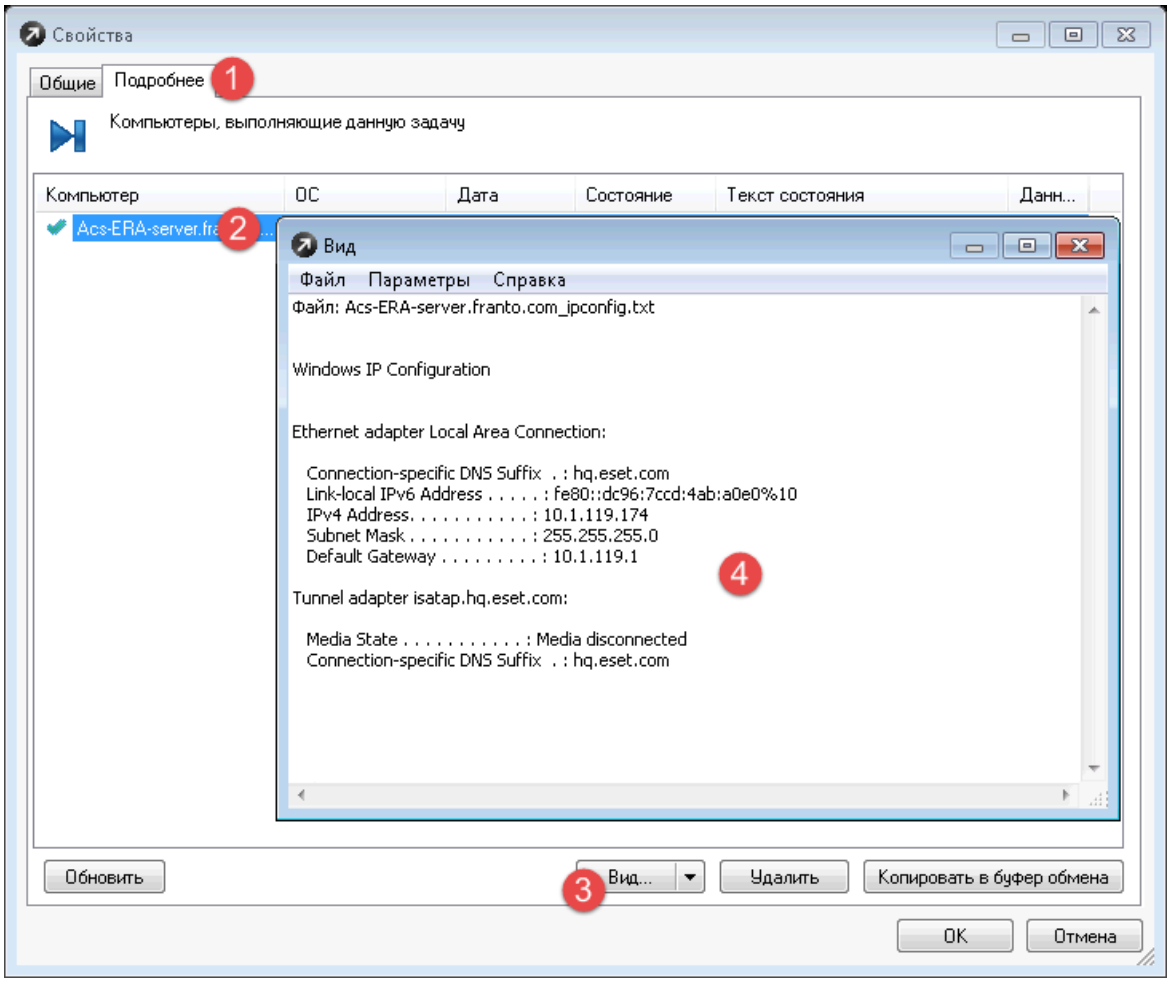
##### 3.4.17.4.1 Повторный запуск задачи

Если нужно запустить задачу, отображаемую на вкладке **Журнал установки** вкладки **Удаленная установка**, щелкните нужную задачу (или несколько выбранных задач) правой кнопкой мыши и в контекстном меню выберите **Повторный запуск задачи**. . Запущенный мастер **Повторный запуск задачи** похож на мастер Новая задача установки 51. Вы можете щелкнуть **Продолжить**, чтобы перейти к экрану **Параметры входа компьютеров**, или, прежде чем нажимать кнопку **Продолжить**, можно изменить задачу, которую нужно запустить.

Повторный запуск любой задачи приводит к созданию новой записи (строки) во вкладке **Журнал установки**. Если при завершении задача имеет статус ***Завершено с предупреждением***, щелкните задачу дважды, в окне **Свойства** откройте вкладку **Сведения** и, чтобы ознакомиться с дополнительными сведениями, просмотрите **сообщение о состоянии**. Если отображается только часть **сообщения о состоянии**, подведите к нему указатель мыши, и отобразится весь текст.

#### 3.4.17.4.2 Просмотр содержимого файла результатов

Если после установки пользовательского пакета появляется файл результатов на целевом компьютере и если при настройке пользовательского пакета 61 задано имя этого файла, вы сможете просматривать содержимое этого файла в ERA Console. Для этого нужно дважды щелкнуть выполненную задачу на вкладке **Подробности** вкладки **Журнал установки** 63, выбрать компьютер и нажать кнопку **Просмотр**.




## 3.5 Настройки консоли ERA

Консоль ERA Console настраивается в меню **«Служебные программы»** > **«Настройки консоли...»**.

### 3.5.1 Подключение

Доступ к параметрам ERA Console можно получить из главного меню консоли ERAC, выбрав **Служебные программы** > **Настройки консоли...** или **Файл** > **Настройка соединений...**. Эта вкладка предназначена для настройки подключения консоли ERAC к серверу ERAS. Дополнительные сведения см. в разделе Подключение к серверу ERAS 27.

На вкладке **«Параметры соединения»** можно выбрать сервер для подключения и настроить автоматическое подключение к этому серверу при запуске консоли ERA Console. В каждый момент времени консоль может быть подключена только к одному серверу. Для того чтобы добавить реплицированные серверы, настройте репликацию в меню «Служебные программы» > «Настройки сервера» > «Настройки репликации...» 130.

**Примечание.** Порт для подключения к серверу ERA Server можно задать в меню **«Служебные программы»** > **«Настройки сервера»** > **«Другие настройки»** (см. раздел Другие настройки 136).

**«Внести/убрать...»** — **используется, чтобы** добавить новые серверы ERA Server или изменить существующие. Если выбрать этот параметр, откроется окно **«Редактор соединения»**. Чтобы добавить новое подключение, введите IP-адрес или имя узла сервера, порт, который будет использоваться для подключения, и комментарий (необязательно). Нажмите кнопку **«Добавить/сохранить»**, чтобы добавить подключение в список серверов в

верхней части окна. Выберите конкретный сервер для таких действий: вы можете выбрать команду **«Удалить»** или **«Удалить все»** либо изменить соединение (выполняется так же, как и создание нового).

- **«Подключиться к выбранному серверу при запуске консоли»** — консоль автоматически подключится к указанному серверу ERA Server.
- **«Показать сообщение при ошибке соединения»** — если при обмене данными возникает ошибка, на экран выводится предупреждение.

### 3.5.2 Столбцы

На этой вкладке можно задать список атрибутов (столбцов), отображаемых на других вкладках. Изменения отражаются в пользовательском режиме просмотра (вкладка «Клиенты» 34). Внести изменения в других режимах просмотра нельзя.

Чтобы отобразить столбец на определенной вкладке, щелкните имя вкладки в списке вкладок и выберите столбцы, которые нужно отобразить.

- **«Выбрать»** — выберите панель, в которой вы хотите изменить выбор отображаемых столбцов.
- **«Отобразить столбцы»** — выберите столбцы для отображения в панели. Выбирайте внимательно, чтобы включить всю необходимую вам в панели информацию и в то же время сохранить представление данных прозрачным.
- **«Очистить все»** — снимает все флажки в окне **«Отобразить столбцы»** для выбранной панели.
- **«Задать все»** — устанавливает все флажки окне **«Отобразить столбцы»** для выбранной панели.
- **«По умолчанию»** — восстанавливает все флажки по умолчанию в окне **«Отобразить столбцы»** для выбранной панели.
- **«По умолчанию»** — восстанавливает все флажки по умолчанию в окне **«Отобразить столбцы»** для всех панелей.

### 3.5.3 Цвета

На этой вкладке можно назначать разные цвета конкретным системным событиям, что позволяет обращать внимание на проблемные клиенты (т. н. условное выделение). Например, клиенты с несколько устаревшей базой данных сигнатур вирусов **«Клиенты: Предыдущая версия»**) могут отличаться от клиентов с полностью устаревшей базой данных (**«Клиенты: устаревшая версия или н/д»**).

Чтобы назначить определенный цвет панелям и столбцам, выберите их в списке **«Панели и столбцы»**. Затем выберите нужный цвет.

**Примечание.** Цвет столбца **Клиенты: устаревшая версия или н/д** используется в ситуации, когда версия базы данных сигнатур вирусов ESET Endpoint Security на клиенте старше, чем на сервере, или не добавлена. Он также используется в случае, если версия продукта безопасности ESET на сервере старше, чем на клиенте, или не добавлена.

В столбце **«Клиенты: последнее соединение»** можно задать временной интервал использования цвета.

### 3.5.4 Пути

Доступ к параметрам ERA Console можно получить из главного меню консоли ERAC с помощью команды **«Служебные программы»** > **«Настройки консоли...»**.

На вкладке **«Пути»** выбираются пути, по которым будут сохраняться отчеты, создаваемые консолью ERA Console. Дополнительные сведения о создании и просмотре отчетов см. в главе Создание и просмотр отчетов 44 этого справочного файла.

### 3.5.5 Дата/время

На вкладке **«Дата/время»** настраиваются дополнительные параметры консоли ERA Console. Кроме того, здесь можно задать предпочитаемый формат времени для отображения записей в окне консоли ERA Console.

- **«Точное»** — в консоли отображается точное время (например, *«14:30:00»*).
- **«Относительное»** — в консоли отображается относительное время (например, *«2 недели назад»*).
- **«Местное»** — в консоли отображается время в соответствии с региональными настройками Windows.
- **«Пересчет времени в UTC (введите местное время)»** — если установить этот флажок, будет выполняться пересчет на местное время. В противном случае отображаются значения времени в формате GMT – UTC.

### 3.5.6 Панели

На вкладке **Панели** можно выбрать, какие вкладки и панели 32 должны отображаться в ERA Console.

В разделе **Видимые панели** выберите панели и вкладки, которые нужно отобразить в нижней части консоли ERA Console, и нажмите кнопку **ОК**.

**Примечания.**

- Отобразятся и скрытые вкладки, если щелкнуть связанный элемент в меню «Вид» консоли ERA Console.
- Вкладку можно скрыть с помощью контекстного меню любой вкладки или панели. Для этого в меню нужно щелкнуть **Скрыть вкладку**.
- Невозможно скрыть все вкладки, так как по крайней мере одна должна оставаться видимой.

### 3.5.7 Другие настройки

На вкладке **«Другие настройки»** устанавливаются расширенные параметры консоли ERA Console.

**1. «Настройки фильтра»**

**«Автоматически применять изменения»** — если эта функция включена, фильтры на различных вкладках формируют новые выходные данные после каждого изменения своих параметров. В противном случае фильтрация будет выполняться только после нажатия кнопки **«Применить изменения»**.

**Примечание.** Если консоль ERA Console будет постоянно подключена к серверу ERA Server с компьютера администратора, рекомендуется выбрать параметр **Показывать на панели задач** и оставить консоль свернутой в неактивном режиме. При возникновении проблемы значок в системном лотке станет красным, что является сигналом для вмешательства администратора. Рекомендуется также настроить параметр **Изменять вид значка в области уведомлений при наличии проблем на клиентах** и задать события, вызывающие изменение цвета значка в лотке.

**«Обновления удаленного администрирования»** — в этом разделе можно включить проверку наличия новых версий программы ESET Remote Administrator. Рекомендуется использовать значение по умолчанию («Ежемесячно»). Если доступна новая версия, при запуске программы в консоли ERA Console появится уведомление.

**2. Другие настройки**

- **«Автообновление»** — автоматическое обновление данных на отдельных вкладках через выбранные интервалы времени.
- **«Показать сетку»** — этот параметр включает отображение сетки, разделяющей рабочее пространство на всех вкладках на отдельные ячейки.
- **«Отображать клиент как "Сервер/Имя", а не как "Сервер/Компьютер/MAC"»** — определяет режим отображения клиентов в некоторых диалоговых окнах (например, в окне **«Новая задача»**). Это влияет только на внешний вид.
- **«Показывать значок в области уведомлений»** — консоли ERA Console будет соответствовать значок в области

уведомлений Windows.

- **«Показывать на панели задач»** — окно консоли ERA Console в свернутом виде будет доступно в панели задач Windows.
- **Изменять вид значка в области уведомлений при наличии проблем на клиентах** — выбрав этот параметр и нажав кнопку **Изменить**, можно настроить события, вызывающие изменение цвета значка в области уведомлений.

**Примечание**. Значок области уведомлений изменяется также тогда, когда обновляется список пропуска, завершается выполнение задачи поиска по умолчанию, добавляется или удаляется клиент. Изменение не происходит мгновенно, возможна задержка длительностью 5–15 секунд, и нужно еще ждать, пока выполняется объединение (хотя, как правило, объединение происходит сразу).

- **При выполнении сетевых действий использовать имя хоста вместо IP-адреса** — при выполнении сетевых действий на клиентах (см. раздел Вкладка «Клиенты» 34) вместо IP-адреса можно использовать имя хоста.
- **«Необязательное информационное сообщение»** — отключает (**«Выкл. все»**) или включает (**«Вкл. все»**) все информационные сообщения. Если этот параметр включен, в консоли ERA Console будут отображаться подчеркнутые сообщения синего цвета. Если щелкнуть эти сообщения, откроются окна с подсказками и рекомендациями по использованию продукта.

## 3.6 Режимы отображения

В консоли ERAC доступно два режима отображения:

- **«Режим администратора»**. В режиме администратора в консоли ERAC пользователю предоставляется полный контроль над всеми функциями и параметрами, а также возможность администрировать все подключенные клиентские рабочие станции.
- **«Режим только для чтения»**. Режим только для чтения предназначен для просмотра состояния решений ESET на клиентских машинах, подключенных к серверу ERAS; создание задач для клиентских рабочих станций, создание пакетов установки и удаленная установка запрещены. Диспетчеры лицензий, политик и уведомлений также недоступны. В режиме только для чтения администратору не разрешено менять настройки консоли ERAC и создавать отчеты.

Режим отображения выбирается при каждом запуске консоли в раскрывающемся меню **«Доступ»**, а пароль для подключения к серверу ERAS можно установить в любом режиме отображения. Возможность настройки пароля особенно полезна в ситуации, когда необходимо, чтобы часть пользователей имела полный доступ к серверу ERAS, а остальные — доступ только для чтения. Для установки пароля выберите команду **«Служебные программы»** > **«Настройки сервера...»** > **«Безопасность»** и нажмите кнопку **«Изменить»** напротив параметра «Пароль для консоли (доступ с правами администратора)» или «Пароль для консоли (доступ только для чтения» или используйте инструмент Диспетчер пользователей 124.

## 3.7 ESET Configuration Editor

ESET Configuration Editor является важным компонентом консоли ERAC и служит для выполнения нескольких задач. Вот некоторые наиболее важные из них:

- создание предопределенных конфигураций установочных пакетов;
- создание конфигураций или политики, отправляемых на клиенты в виде задач;
- создание общего конфигурационного XML-файла.

Configuration Editor является частью консоли ERAC и представлен в основном файлами *cfgedit.**.

Configuration Editor позволяет администратору удаленно настраивать множество параметров продуктов безопасности компании ESET (в частности, продукты, установленные на клиентских рабочих станциях). Он также позволяет администратору экспортировать конфигурации в XML-файлы, которые затем можно будет использовать в различных целях (например, для создания задач в консоли ERAC, локального импортирования

конфигураций в ESET Endpoint Security и т. п.).

В Configuration Editor используется структура *XML*-шаблона, в котором конфигурация хранится в виде древовидной структуры. Этот шаблон находится в файле *cfgedit.exe*. Именно поэтому рекомендуется регулярно обновлять сервер ERAS и консоль ERAC.

***Предупреждение.*** Configuration Editor позволяет изменять *XML*-файлы. Не изменяйте и не перезаписывайте исходный файл *cfgedit.xml*.

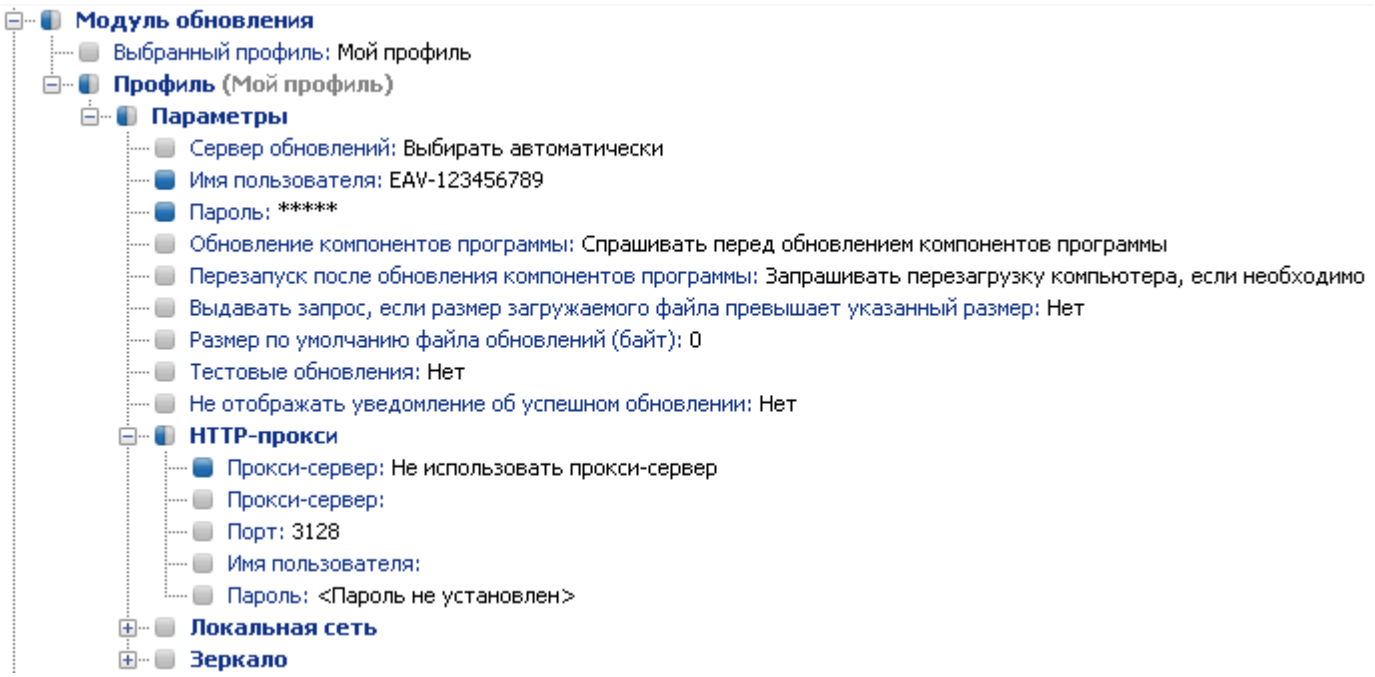
Для работы Configuration Editor необходимы следующие файлы: *eguiHipsRa.dll, eguiHipsRaLang.dll, eguiRuleManagerRa.dll* и *eset.chm*.

### 3.7.1 Иерархическое представление конфигурации

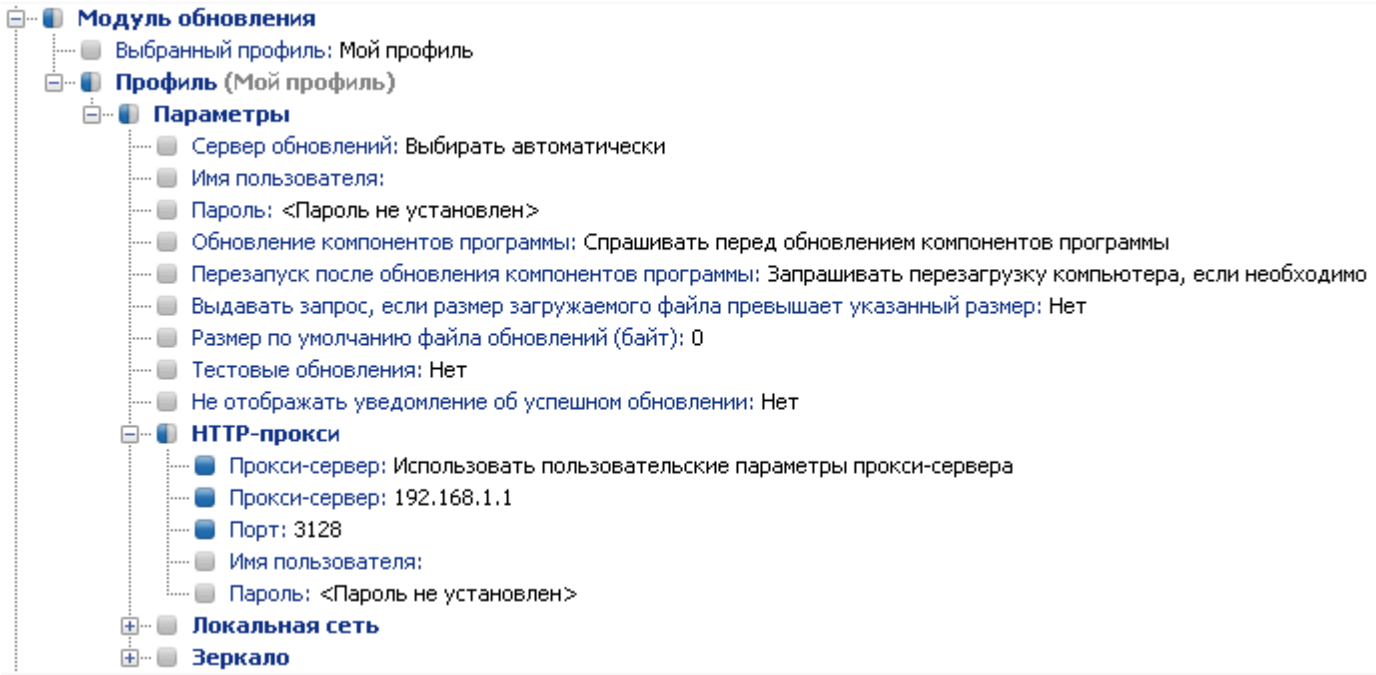
При изменении значения в Configuration Editor это значение отмечается синим символом. Запись, обозначенная серым значком, не менялась и не будет записана в выходную конфигурацию в формате *XML*.

При применении конфигурации к клиентам применяются только те изменения, которые были сохранены в выходном *XML*файле конфигурации (), а все остальные элементы () останутся в прежнем состоянии. Такой подход позволяет последовательно применить несколько разных конфигураций без отмены предыдущих изменений.

На рисунке ниже показан пример. В этой конфигурации вставляются имя пользователя *EAV-12345678* и пароль и запрещается использование прокси-сервера.



Вторая отправляемая клиентам конфигурация (рис. 3—8) гарантирует сохранение предыдущих изменений, включая имя пользователя *EAV-12345678* и пароль. В этой конфигурации также разрешается использование прокси-сервера и задается его адрес и порт.




### 3.7.2 Основные элементы конфигурации

В этом разделе описано несколько основных элементов конфигурации программ для Windows версий 3 и 4.

- **«Программы для Windows, версии 3 и 4»** > **«Ядро ESET»** > **«Параметры»** > **«Удаленное администрирование»**
  Здесь можно активировать обмен данными между клиентскими компьютерами и сервером ERAS (**«Подключиться к ESET Remote Administrator Server»**). Введите имя или IP-адрес сервера ERAS (**«Адрес основного/дополнительного сервера»**). Значение параметра **«Интервал между подключениями к серверу»** оставьте значение по умолчанию (5 мин.). При выполнении проверок это значение можно уменьшать до 0, в каковом случае соединение будет устанавливаться каждые десять секунд. Если установлен пароль, воспользуйтесь паролем, заданным на сервере ERAS. Дополнительные сведения см. в статье о параметре **«Пароль для клиентов»** в разделе Вкладка «Безопасность». В данном разделе также доступны дополнительные сведения о настройке пароля.

- **«Ядро ESET»** > **«Параметры»** > **«Лицензионные ключи»**
  На клиентских компьютерах не требуется ни добавлять лицензионные ключи, ни управлять ими. Лицензионные ключи необходимы только для серверных продуктов.

- **«Ядро ESET»** > **«Параметры»** > **«ESET Live Grid»**
  В этом разделе задается режим работы системы быстрого оповещения ESET Live Grid, позволяющей отправлять подозрительные файлы на анализ в лаборатории компании ESET. При развертывании решений ESET в большой сети параметры **«Передача подозрительных файлов»** и **«Разрешить передачу анонимной статистической информации»** играют особую роль: если для них установлено значение **«Не отправлять»** или **«Нет»** соответственно, система ESET Live Grid полностью отключается. Для автоматической отправки файлов без вмешательства пользователя выберите значения **«Передавать, не спрашивая»** и **«Да»** соответственно. При использовании для подключения к Интернету прокси-сервера задайте параметры соединения в меню **«Ядро ESET» > «Настройка» > «Прокси-сервер»**.
  По умолчанию клиентские продукты отправляют подозрительные файлы на сервер ERAS, который передает их на серверы компании ESET. Поэтому необходимо правильно настроить прокси-сервер на сервере ERAS (**«Служебные программы» > «Настройки сервера...» > «Дополнительно» > «Изменить дополнительные параметры» > ERA Server > «Настройка» > «Прокси-сервер»**).

- **«Ядро ESET» > «Параметры» > «Защита установочных параметров»**
  Позволяет администратору защитить параметры настройки паролем. Если пароль установлен, он будет запрашиваться при доступе к параметрам настройки на клиентских рабочих станциях. Однако он не используется при внесении изменений в конфигурацию из консоли ERAC.

- **«Ядро ESET» > «Параметры» > «Планировщик»**
  В этом разделе представлены параметры планировщика, с помощью которых администратор может планировать регулярные проверки на вирусы и т. п.

**Примечание.** По умолчанию в состав всех решений по обеспечению безопасности ESET входит ряд предопределенных задач (в том числе регулярное автоматическое обновление и автоматическая проверка важных файлов при запуске). В большинстве случаев изменять эти задачи или добавлять новые не требуется.

- **«Ядро ESET» > «Параметры» > «Значения интерфейса пользователя по умолчанию»**
  Параметры в разделе «Значения интерфейса пользователя по умолчанию» (например, **«Показывать заставку при запуске»**/**«Не показывать заставку при запуске»**) применимы только к параметрам по умолчанию клиента. Параметрами клиента можно управлять на основе каждого пользователя и их нельзя изменить удаленно. Чтобы можно было удаленно изменить параметра, для параметра **«Переопределить параметры пользователя»** необходимо установить значение **«Да»**. Параметр **«Переопределить параметры пользователя»** доступен только для клиентов с продуктами безопасности ESET версии 4.0 и старше.

- **«Модуль»**
  В этом разделе Configuration Editor задаются способы применения профилей обновления в обычном режиме. Для этого нужно только внести изменения в предопределенный профиль **«Мой профиль»** и изменить параметры **«Сервер обновлений»**, **«Имя пользователя»** и **«Пароль»**. Если для параметра «Сервер обновлений» задано значение **«Выбирать автоматически»**, все обновления будут загружаться с серверов обновлений компании ESET. В этом случае укажите для параметров **«Имя пользователя»** и **«Пароль»** значения, предоставленные вам при покупке продукта. Дополнительные сведения о настройке получения обновлений от локального сервера (зеркало) на клиентских рабочих станциях см. в разделе Сервер зеркала 133. Дополнительные сведения об использовании планировщика см. в разделе Планировщик 182.

**Примечание.** На портативных устройствах, таких как ноутбуки, можно настроить два профиля, один из которых будет предназначен для загрузки обновлений с сервера зеркала, а другой — непосредственно с серверов ESET. Дополнительные сведения см. в разделе Комбинированное обновление для ноутбуков 184 в конце этого документа.

# 4. Установка клиентских решений компании ESET

Эта глава посвящена установке клиентских решений ESET в операционных системах Microsoft Windows. Установку можно выполнять непосредственно 71 на рабочих станциях или удаленно 54 с сервера ERAS. В этой главе также кратко описаны альтернативные способы удаленной установки.

**Примечание.** Хотя это и возможно чисто технически, не рекомендуется выполнять удаленную установку продуктов ESET на серверы (используйте этот способ только для рабочих станций).

***Внимание!*** Администраторы, использующие подключение удаленного рабочего стола Microsoft для доступа к удаленным клиентским компьютерам, должны ознакомиться со следующей статьей перед удаленной установкой ESET Smart Security.

## 4.1 Непосредственная установка

При непосредственной установке администратор заходит на компьютер, на который нужно установить продукт безопасности ESET. Этот способ не требует никакой дополнительной подготовки и предназначен для небольших компьютерных сетей или сценариев, в которых средства ERA не используются.

Эту задачу можно существенно упростить с помощью предопределенной конфигурации в формате XML. После установки нет необходимости указывать сервера обновлений (имя пользователя, пароль, путь к серверу зеркала и т. п.), настраивать автоматический режим, расписание проверок и т. п.

Отличия в применении конфигурации в формате XML к клиентским решениям ESET версий 5.x, 4.x, 3.x и 2.x заключаются в следующем.

- Версия 5.x: Выполните такие же действия, как для версии 4.x.

**ПРИМЕЧАНИЕ.**: Установить продукты ESET Security для Linux и Mac можно с помощью клиентов версии 5.

- Версия 4.x: загрузите установочный файл (например *ess_nt32_enu.msi*) с веб-сайта *eset.com* и создайте свой собственный установочный пакет в **редакторе установочных пакетов**. Измените или выберите конфигурацию, которую нужно связать с эти пакетом, нажмите кнопку **«Копировать...»** рядом с полем **«Пакет для XX-разрядных систем Windows NT»** и сохраните пакет как **«MSI-файл установки ESET с конфигурацией (*.msi)»**.

  **Примечание.** При добавлении конфигурации в установочный *MSI*-файл цифровая подпись этого файла больше не будет действительной. Кроме того, шаги для версии 3.x применимы также для версии 4.x.

- Версия 3.x: Загрузите установочный файл (например, *ess_nt32_enu.msi*) с веб-сайта *eset.com*. Скопируйте файл конфигурации (*cfg.xml*) в каталог, в котором находится установочный файл. При запуске программа установки автоматически воспользуется конфигурацией из *XML*-файла конфигурации. Если *XML*-файла конфигурации имеет другое имя или он находится в другом месте, можно использовать параметр *ADMINCFG ="genm_r_xml-файлу"* (например, *ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* для применения конфигурации, которая хранится на сетевом диске).

**ПРИМЕЧАНИЕ.** Если выполняется установка ESET Smart Security (включая персональный файервол), необходимо разрешить общий доступ и удаленное администрирование. В противном случае сетевые подключения между такими клиентами и сервером ERA будут заблокированы.

## 4.2 Удаленная установка

При удаленной установке не требуется предустанавливать или физически устанавливать продукты безопасности на клиентские компьютеры. ERA поддерживает несколько способов удаленной установки.

Удаленная установка с помощью ERA состоит из следующих этапов:

- Создание установочных пакетов.

  Сначала проверьте требования 72 к удаленной установке.

  Затем создайте установочные пакеты 54, которые будут распространены на клиенты.

- Рассылка пакетов на клиентские рабочие станции (посредством автоматической установки, с помощью сценария входа, электронной почты, обновления, стороннего решения):

  Проверьте и настройте сетевую среду для удаленной установки.

  Распространите установочные пакеты на клиенты. Существует несколько способов удаленной установки.

  Удаленная автоматическая установка 74. Это наиболее эффективный способ распространения продуктов безопасности на клиентах.

  Также возможна удаленная установка с использованием сценария входа или электронной почты 76.

  Если нежелательно использовать описанные выше методы, можно выполнить пользовательскую удаленную установку 79.

Если на некоторых клиентах установлены устаревшие продукты безопасности ESET, их можно обновить до последней версии. См. главу Обновление клиента 80. Если у них уже есть последняя версия, см. главу Как избежать повторных установок 81. Сведения об установки пакетов в крупной корпоративной среде см. здесь 87.

### 4.2.1 Требования и ограничения

Основным требованием для удаленной установки является правильно настроенная сеть TCP/IP, которая обеспечивает надежную связь между клиентом и сервером. При установке клиентского решения с помощью программы ERA к клиентской рабочей станции предъявляются более строгие требования, чем при непосредственной установке. Для удаленной установки должны выполняться следующие требования:

**Windows**

- включен клиент сети Microsoft;
- включена служба «Общий доступ к файлам и принтерам»;
- открыты порты общего доступа к файлам (445, 135–139);
- включен административный общий ресурс ADMIN$;
- для клиентских рабочих станций существуют имя пользователя и пароль учетной записи администратора (имя пользователя не может быть пустым);
- отключена служба «Простой общий доступ к файлам»;
- включена служба «Сервер»;

**ПРИМЕЧАНИЕ.**: В последних версиях ОС Microsoft Windows (Windows Vista, Windows Server 2008 и Windows 7) используются политики безопасности, ограничивающие разрешения учетной записи локального пользователя, то есть пользователь может быть не в состоянии выполнять определенные сетевые действия. Если служба ERA работает в учетной записи локального пользователя, при некоторых конфигурациях сети могут возникнуть проблемы с автоматической установкой (например, при удаленной установке из домена в рабочую группу). В

системах Windows Vista, Windows Server 2008 или Windows 7 рекомендуется запускать службу ERA с достаточными разрешениями доступа к сети. Чтобы указать учетную запись пользователя, от имени которой будет выполняться служба ERA, выберите **Пуск** > **Панель управления** > **Администрирование** > **Службы**. Выберите службу ESET Remote Administrator Server в списке и щелкните элемент **Вход**. ESET Remote Administrator 5 встраивает этот параметр в сценарий расширенной установки, поэтому во время установки необходимо выбрать **Расширенная** > **Полностью настраиваемая установка**.

***Внимание!*** Если вы используете метод установки **Автоматическая установка Windows** на целевых рабочих станциях под управлением Windows Vista, Windows Server 2008 или Windows 7, убедитесь, что сервер ERA Server и целевые рабочие станции находятся в домене. Если сервер ERA Server и целевой компьютер находятся не в домене, нужно отключить UAC (контроль учетных записей) на целевом компьютере. Это можно сделать, щелкнув **Пуск** > **Панель управления** > **Учетные записи пользователей** > **Включение или отключение контроля учетных записей**. Или же можно нажать кнопку **Пуск**, ввести в поле поиска **Msconfig**, нажать клавишу **ВВОД** а затем выбрать **Сервис** > **Отключить контроль учетных записей (UAC) (потребуется перезагрузка)**.

Перед установкой настоятельно рекомендуется проверить все требования, особенно если в сети есть несколько рабочих станций.
На вкладке **Удаленная установка** выберите вкладку **Компьютеры**, выберите нужные клиенты, нажмите кнопку **Новая задача установки**, выберите **Автоматическая установка Windows**, затем — **Диагностика**, нажмите кнопку **Продолжить**, задайте сведения для входа 79 выбранных клиентов, щелкнув **Задать для всех** или **Задать учетные данные** (после выбора указанного клиента в окне **Параметры входа компьютеров**), нажмите кнопку **Далее**, а затем — кнопку **Готово**.

Удаленная установка продуктов безопасности для систем Linux и Mac в Windows 2000 не поддерживается.

***Внимание!*** Администраторы, использующие подключение удаленного рабочего стола Microsoft для доступа к удаленным клиентским компьютерам, должны ознакомиться со следующей статьей перед удаленной установкой ESET Smart Security.

#### 4.2.1.1 Требования к автоматической установке Linux/Mac

Прежде чем выполнять удаленную установку, убедитесь, что все клиентские рабочие станции настроены правильно.

**Linux**

1. Компьютер должен иметь функцию подключения к серверу через SSH.
2. Учетная запись SSH должна иметь права администратора. Это означает, что установку необходимо выполнять под учетной записью привилегированного пользователя (UID=0) или пользователя с правами sudo.

**Mac**

1. Компьютер должен иметь функцию подключения к серверу через SSH.
2. Учетная запись SSH должна иметь права администратора. Это означает, что установку необходимо выполнять под учетной записью администратора.

**Примечание.**: Эта функция поддерживается решением ESET NOD32 Antivirus Business Edition для Mac OS X 4.1.94 и ESET NOD32 Antivirus Business Edition для Linux Desktop 4.0.79 и всеми более поздними версиями для обеих платформ.

#### 4.2.1.2 Требования WMI

Чтобы использовать метод удаленной установки WMI, нужно выполнить следующие условия:

- На целевом компьютере инструментарий WMI нужно включить и запустить. По умолчанию он включен.
- Учетная запись пользователя, используемая для удаленного подключения, должна иметь права администратора.
- Подключение WMI должно быть разрешено в файерволе целевого компьютера. Чтобы подключение состоялось, порт 135 должен быть включен для DCOM (распределенной компонентной модели объектов) для входящих подключений. Кроме того, нужно включить любой порт с номером выше 1024 (обычно 1026–1029).

  Вы можете настроить файервол Windows по умолчанию, выполнив на целевом компьютере следующую команду:

  ```
  netsh firewall set service RemoteAdmin enable
  ```

- Учетная запись для подключения к удаленному компьютеру должна быть учетной записью домена и должна иметь права локального администратора.

  Инструментарий WMI может функционировать также тогда, когда учетная запись является локальной, но на удаленной системе компонент UAC нужно отключить.

Дополнительные сведения см. в статье http://msdn.microsoft.com/en-us/library/aa826699%28v=vs.85%29.aspx.

### 4.2.2 Удаленная автоматическая установка

При использовании этого способа удаленной установки клиентские решения ESET автоматически устанавливаются на удаленные компьютеры. Автоматическая установка — самый эффективный метод установки, при использовании которого необходимо, чтобы целевые рабочие станции были в режиме онлайн. Перед началом автоматической установки необходимо загрузить с веб-сайта ESET установочные MSI-файлы для ESET Endpoint Security или ESET Endpoint Antivirus и создать пакет установки. Можно создать XML-файл конфигурации, который будет применяться автоматически при запуске данного пакета. Перед установкой прочтите раздел Требования 72.

Чтобы начать автоматическую установку на вкладке **Удаленная установка**, выполните указанные ниже действия.

1) Когда компьютеры, подходящие для удаленной установки, отображены на вкладке **Компьютеры**, вы можете выбрать все или некоторые из них, нажав кнопку **Новая задача установки**. Откроется окно Новая задача установки 82, в котором по умолчанию выбраны параметры **Автоматическая установка Windows** и **Установка** и в котором нужно нажать кнопку **Продолжить**.

2) Задайте сведения для входа для компьютеров, внесенных в список (используйте элемент **Задать учетные данные**, чтобы задать учетные данные для выделенного или выбранного компьютера, или элемент **Задать для всех**, чтобы применить учетные данные ко всем компьютерам в списке). Это должно быть сделано с использованием учетной записи с правами администратора. На этом этапе можно еще добавить клиенты в список с помощью функции **Специальное добавление клиентов**.

3) Выберите пакет установки 54, который нужно отправить на рабочие станции.

4) Укажите время запуска задачи и нажмите кнопку **«Готово»**.

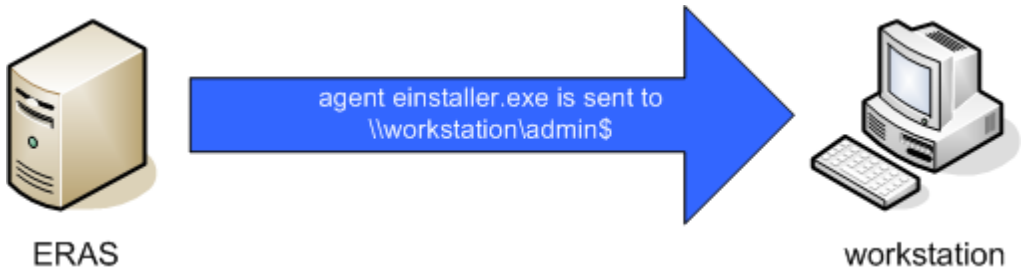
Состояние задачи автоматической установки отображается на вкладке Журнал установки 63. Для просмотра более подробных результатов диагностики выберите нужное задание и нажмите клавишу F4. В окне **«Свойства»** есть вкладка **«Детали»**, в которой можно просмотреть результаты диагностики удаленной установки, нажав кнопку **«Просмотреть выбранные журналы/Просмотреть все журналы»**.

**Примечание.** Максимальное количество одновременных потоков автоустановки по умолчанию равно 20. При отправке задачи автоматической установки на несколько компьютеров, превышающих этот предел,

дополнительные компьютеры будут поставлены в очередь, ожидая освобождения потока. Не рекомендуется увеличивать это значение, чтобы не снизить продуктивность. Однако при необходимости это ограничение можно изменить в редакторе конфигураций (**ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Удаленная установка»**).

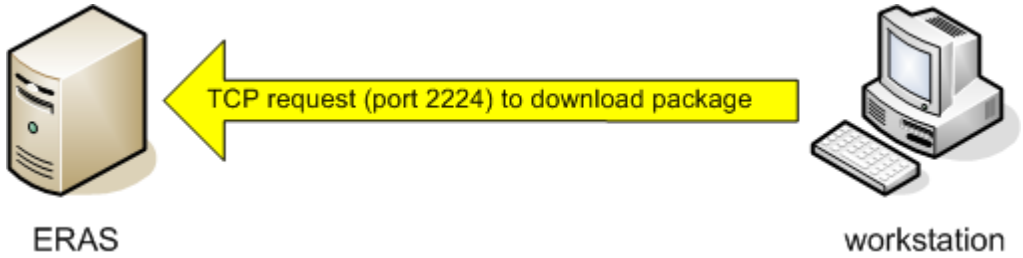
Ниже подробно описан процесс удаленной установки.

5) Сервер ERAS отправляет агент *einstaller.exe* на рабочую станцию с использованием административного общего ресурса admin$.

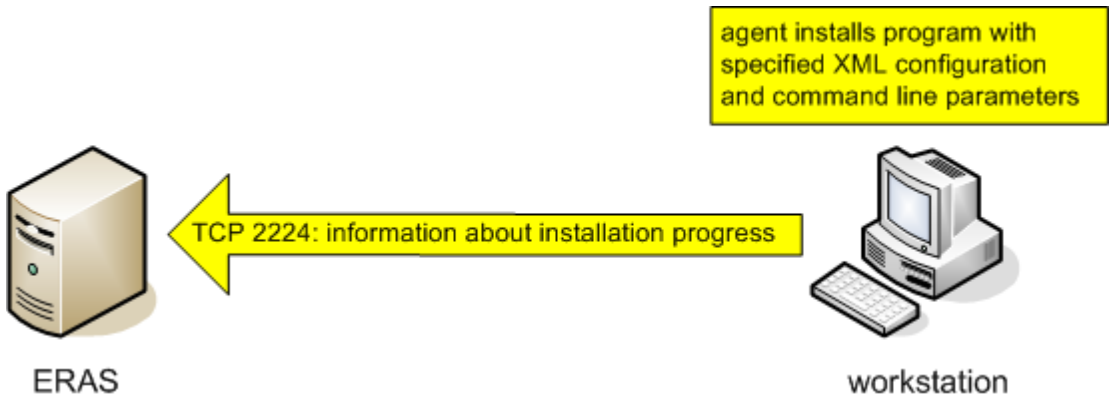



6) Агент запускается как служба с правами учетной записи системы.

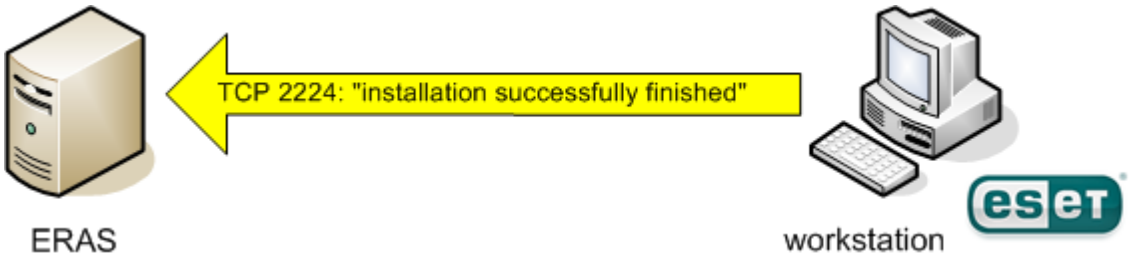

7) Агент устанавливает соединение с «родительским» сервером ERAS и загружает соответствующий установочный пакет по TCP-порту 2224.




Агент устанавливает пакет с учетной записью администратора, выбранной на шаге 2. При этом также применяется соответствующая *XML*-конфигурация и параметры командной строки.



9) Завершив установку, агент немедленно отправит сообщение на сервер ERAS. Некоторые продукты безопасности ESET предлагают в случае необходимости перезагрузить компьютер.




### 4.2.3 Удаленная установка с использованием сценария входа или электронной почты

Методы удаленной установки с использованием сценария входа или электронной почты очень похожи. Единственным отличием является способ отправки агента *einstaller.exe* на клиентские рабочие станции. Программа ERA позволяет запускать агент с помощью сценария входа или по электронной почте. Агент *einstaller.exe* также можно использовать отдельно и запускать другими способами (дополнительные сведения см. в разделе Пользовательская удаленная установка 79).

Установка с использованием сценария входа хорошо подходит для ноутбуков, которые часто находятся за пределами локальной сети. Установка происходит после их входа в домен.

Сценарий входа выполняется автоматически при входе в систему, а для удаленной установки с помощью электронной почты требуется вмешательство пользователя, который должен запустить агент einstaller.exe, содержащийся во вложении сообщения электронной почты. При повторном запуске агент einstaller.exe не инициирует повторную установку клиентского решения ESET. Дополнительные сведения см. в разделе Как избежать повторных установок 81.

Пошаговую инструкцию по экспорту установщика ESET в папку или сценарий входа либо по отправке его по электронной почте см. в этом разделе 77.

#### Удаленная установка продуктов безопасности ESET для Android

***Внимание***: Прежде чем продолжить, прочтите сначала этот раздел 102.

1. Нажмите кнопку **Новая задача установки** на вкладке «Удаленная установка» решения ERA Console, выберите **Android** и щелкните **Продолжить**.
2. Нажмите кнопку **...** возле поля **Вложение**, найдите расположение, в которое вы сохранили продукт безопасности ESET для Android (*APK*-файл), выберите приложение и нажмите кнопку **ОК**.
3. Введите электронную почту пользователя, проверьте или измените сведения в полях **Тема** и **Описание** и нажмите кнопку **...** рядом со ссылкой для настройки конфигурации (находится прямо под полем описания). Откроется окно **Настройки конфигурационной ссылки**, в котором можно настроить подключение продукта к средству ERA.

**Примечание**: Эта ссылка позволяет настроить необходимый продукт ESET для безопасности для платформы Android (можно отправить ссылку пользователю вместе с установочным файлом или отправить приложение непосредственно, как указано в описании этапа 1).

4. Поля **Сервер** и **Порт** задаются автоматически в соответствии с текущим сервером ERA. Если для подключения пользователей к серверу необходим пароль, введите его в поле **Пароль**. В противном случае можно оставить это поле пустым. Если используется пароль, необходимо выбрать параметр **Добавить текущую SIM-карту как доверенную**. Он устанавливается по умолчанию, чтобы предотвратить блокирование мобильного телефона при попытке подключения к серверу ERA. Эти основные настройки будут отправлены на клиент. Чтобы задать дополнительные настройки (такие как обновленное **Имя пользователя** и **Пароль**), клиент должен быть подключен к серверу ERA, тогда эти настройки можно распространять с помощью Политики 96.

#### 4.2.3.1 Экспорт установщика ESET в папку или сценарий входа

С помощью текстового редактора или другого инструмента строку, вызывающую файл *einstaller.exe* можно вставить в сценарий входа. Также агент *einstaller.exe* можно отправлять в виде вложения в сообщении электронной почты с помощью почтового клиента. Независимо от используемого способа убедитесь в том, что используется правильный файл *einstaller.exe*.

Для запуска агента *einstaller.exe* вошедшему в систему пользователю не обязательно иметь права администратора. Агент получает требуемые имя пользователя, пароль и домен учетной записи администратора с сервера ERAS. Дополнительные сведения см. в конце этого раздела.

**Указание в сценарии входа пути к файлу einstaller.exe**

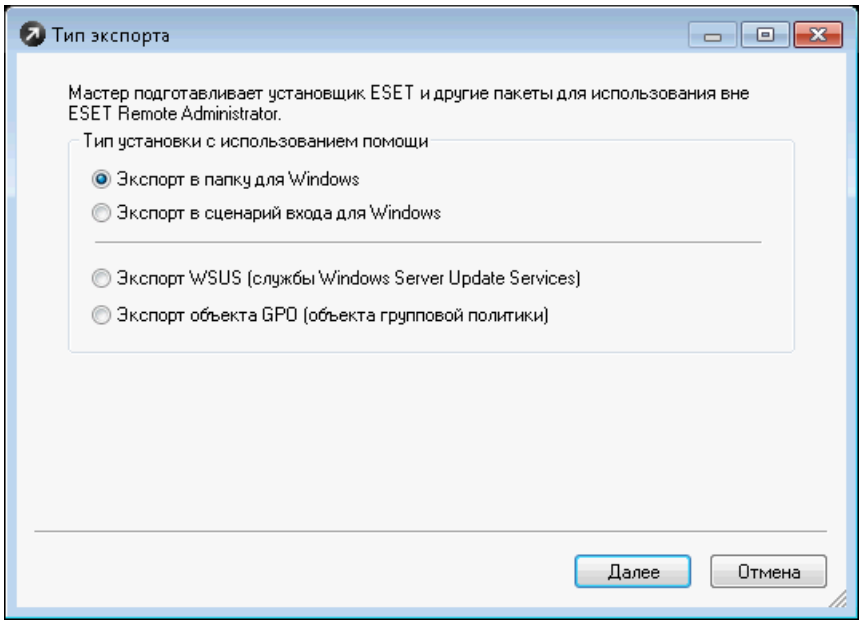
1) Выберите во вкладке **Удаленная установка** запись, нажмите кнопку **Новая задача установки**, выберите **Экспорт** и щелкните **Продолжить**, чтобы перейти к экрану **Тип экспорта**.

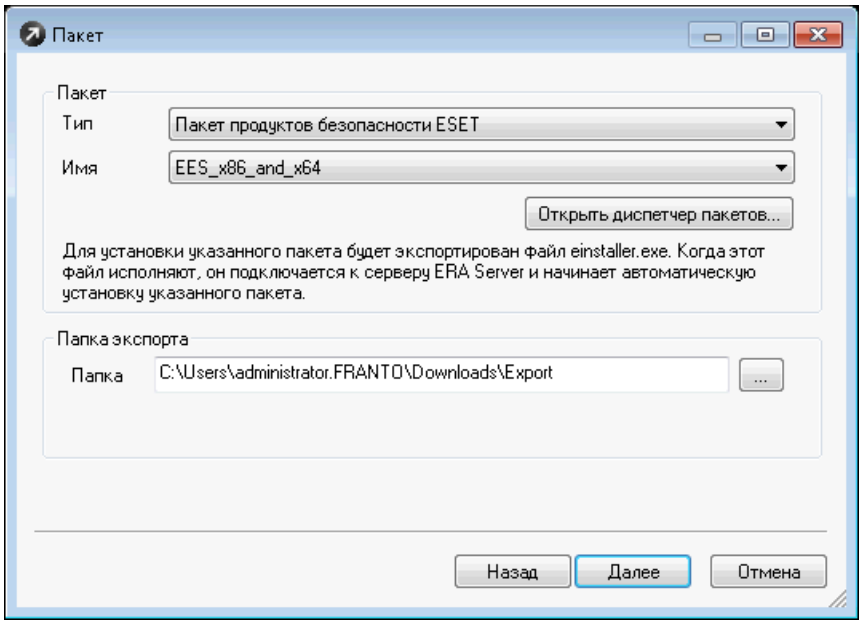
2) На экране **Тип экспорта** отображены следующие параметры:

- **Экспорт в папку для Windows**: этот параметр полезен, если нужно разослать файл *einstaller.exe* на компьютеры пользователей, у которых нет прав администратора. Учетные данные для входа с правами администратора нужно получить с сервера ERA, когда установщик подключается к нему (кроме случаев, когда файл *einstaller.exe* запускается с правами администратора).
- **Экспорт в сценарий входа для Windows**: параметр, аналогичный параметру **Экспорт в папку для Windows**. Есть одно отличие: на экране **Готово** нужно получить ссылку на папку экспорта, чтобы использовать эту ссылку в сценарии входа компьютеров, которыми нужно управлять.
- **Экспорт служб WSUS (Windows Server Update Services)**: этот параметр загружает весь пакет установки, который затем нужно выбрать в качестве исполняемого файла установки в формате *MSI*. Пакет установки можно разослать на нужные компьютеры как часть служб WSUS.
- **GPO (объект групповой политики)**: этот параметр загружает весь пакет установки, который затем нужно выбрать. Пакет установки можно разослать на нужные компьютеры через GPO.

3) Щелкните **...** возле элемента **Папка** в разделе **Папка экспорта**, чтобы выбрать каталог, куда файл *einstaller.exe* (или *.msi installer) будет экспортирован и где он будет доступен в рамках сети (если выбран параметр **Экспорт в сценарий входа для Windows**), а затем нажмите кнопку **Далее**.

4) После этого отображается экран «Готово».






**Вложение агента (einstaller.exe) в сообщение электронной почты**

1) Щелкните **Новая задача установки** на вкладке **Удаленная установка**, выберите **Эл. почта**, нажмите кнопку **Продолжить**.

2) Выберите тип и имя пакета, который нужно установить, и нажмите кнопку **Далее**.

**Примечание**. Если нужно удалить продукты безопасности ESET с компьютера пользователя, то в списке **Тип** выберите параметр **Удаление продуктов ESET для безопасности для ОС Windows и NOD32 версии 2**.

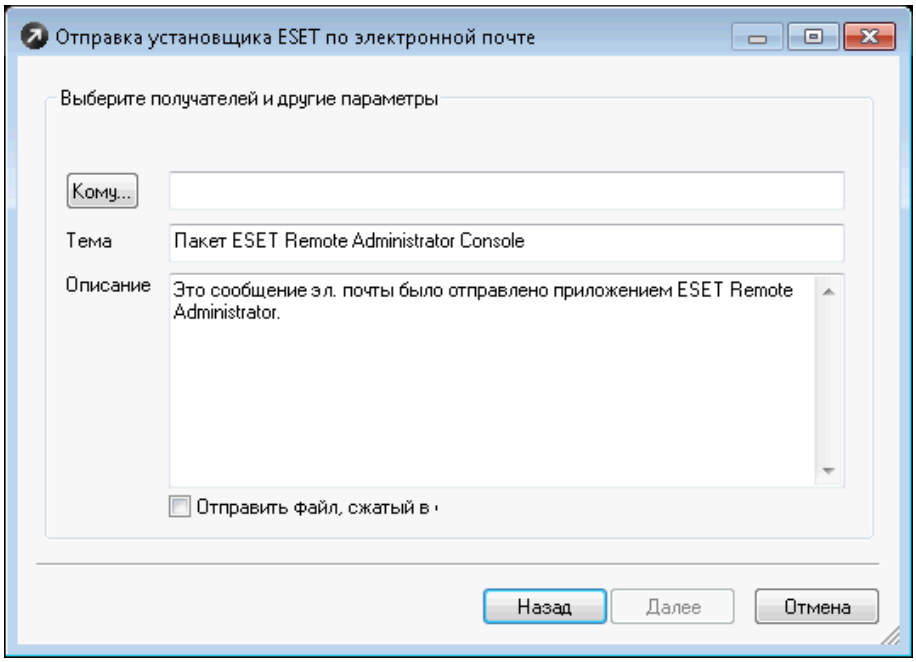
3) Нажмите кнопку **Кому**, чтобы выбрать адреса из адресной книги (или введите адреса вручную).

4) Введите **тему** в соответствующее поле.

5) Введите текст сообщения в поле **«Тело»**.

6) Установите флажок **«Отправить файл, сжатый в формате .zip»**, чтобы отправить агент в сжатом ZIP-архиве.

7) Нажмите кнопку **«Отправить»**, чтобы отправить сообщение.




Во время удаленной установки выполняется обратное подключение к решению ERAS, а параметры агента (*einstaller.exe*) задаются согласно сведениям для входа по умолчанию 79, указанным в окне **Параметры** 84

(чтобы отобразилось это окно, нужно нажать кнопку **Параметры** в окне **Новая задача установки**, если выбран параметр **Эл. почта**).

Учетная запись, под которой будет установлен пакет, должна быть учетной записью с правами администратора локального компьютера или домена. После каждой перезагрузки службы сервера ERAS значения, введенные в диалоговое окно **«Вход по умолчанию...»**, теряются.

#### 4.2.3.2 Вход по умолчанию и сведения для входа

В окне **Вход по умолчанию** и **Сведения для входа** можно указать учетные данные пользователя и сведения о домене, необходимые для доступа к клиентскому компьютеру по сети и управления установленным продукт ESET.

Необходимые данные клиента:

- **«Имя пользователя»**
- **«Пароль»**
- **«Домен/рабочая группа»**

Введя данные, нажмите кнопку **Настроить вход** (в окне **Вход по умолчанию**) или **ОК** (в окне **Сведения для входа**), чтобы сохранить сведения на сервере.

**Примечание.** Эта информация хранится на сервере только до его перезапуска.

**Примечание.** Если в окне **«Вход по умолчанию»** отображается сообщение *Параметры для входа уже хранятся на сервере*, это означает, что параметры уже были сохранены на сервере. Если нужно изменить сохраненные параметры, нажмите кнопку **«Перезаписать»** и настройте новые параметры входа.

### 4.2.4 Пользовательская удаленная установка

Для удаленной установки клиентских решений ESET не обязательно использовать средства ERA. В конечном итоге самым важным аспектом является доставка и запуск файла *einstaller.exe* на клиентских рабочих станциях.

Для запуска агента *einstaller.exe* вошедшему в систему пользователю не обязательно иметь права администратора. Агент получает требуемые имя пользователя, пароль и домен учетной записи администратора с сервера ERAS. Дополнительные сведения см. в конце этой главы.

Файл *einstaller.exe* можно получить следующим образом.

- На вкладке **Компьютеры** (на вкладке **Удаленная установка**) нажмите кнопку **Новая задача установки**, выберите **Экспорт** и щелкните **Продолжить**.
- Выберите **Экспорт в папку для Windows**, а затем — **Далее**. Выберите **тип** и **имя пакета**, который нужно установить.
- Нажмите кнопку **...** рядом с полем **Папка**, выберите каталог, в который будет экспортирован файл *einstaller.exe*, и щелкните **Выбрать папку**.
- Щелкните **Далее**, чтобы перейти на следующий экран, связанный с экспортом файла *einstaller.exe*. Отобразится экран **Готово**, на котором нужно щелкнуть **Готово**.
- Используйте распакованный файл *einstaller.exe*.

**Примечание.** *Прямая установка* 71 *с предопределенной XML-конфигурацией* используется в ситуациях, когда для установки можно получить права администратора. *MSI*-пакет запускается с параметром */qn* (версии 5.x, 4.x, 3.x). Эти параметры позволяют выполнять установку без соответствующего интерфейса пользователя.

Имя пользователя и пароль учетной записи, с использованием которой будет установлен пакет, должны принадлежать учетной записи администратора локального компьютера или домена.

В ходе удаленной установки устанавливается обратное подключение к серверу ERAS и агент (*einstaller.exe*) использует параметры, заданные в разделе **Вход по умолчанию** 79.

Если агент *einstaller.exe* запускается на целевой рабочей станции вручную, удаленная установка выполняется следующим образом.

- Агент *einstaller.exe* отправляет запрос на сервер ERAS (TCP-порт 2224).
- Сервер ERAS запускает новый сеанс автоматической установки (с новым агентом) соответствующего пакета (отправляемого через общий ресурс *admin$*). Агент ожидает ответа от сервера ERAS (отправки пакета в общий ресурс *admin$*). При отсутствии ответа агент попытается загрузить установочный пакет (через TCP/IP-порт 2224). В этом случае имя пользователя и пароль учетной записи администратора, указанные в разделе **Вход по умолчанию** 79 на сервере ERAS, не передаются, поэтому агент пытается установить пакет с использованием учетной записи текущего пользователя. В операционных системах Microsoft Windows 9x/Me нельзя использовать общий административный ресурс, поэтому агент автоматически устанавливает прямое подключение к серверу по протоколу TCP/IP. Затем новый агент начинает загрузку пакета с сервера ERAS по протоколу TCP/IP.

При запуске установки пакета применяются параметры из XML-файла под учетной записью, указанной на сервере ERAS (кнопка **Вход по умолчанию** 79).

### 4.2.5 Клиент обновления Windows

Этот тип установки предназначен для клиентов с ESS/EAV версии 4.2 и выше. Начиная с версии 4.2 в ERA был реализован новый механизм обновления, который позволяет запускать процесс обновления на стороне клиента без агента *einstaller.exe*. Этот механизм работает по аналогии с обновлением компонентов программы (PCU), при котором клиенты обновляются до более новой версии программы. Для клиентов ESS/EAV версии 4.2 и старше настоятельно рекомендуется использовать этот тип обновления.

**ПРИМЕЧАНИЕ.** Если для установочного пакета был определен пользовательский файл конфигурации, он будет игнорироваться во время обновления.

Параметр **Клиент обновления Windows** команды **Новая задача установки** позволяет удаленно обновлять клиент или группу клиентов.

1) Если нужно использовать инструмент выделения для выбора клиентов для обновления, нажмите кнопку **«Специальное добавление клиентов»** в первом шаге. После выбора нажмите кнопку **«Далее»** для продолжения.

**Примечание.** Кнопка **«Специальное добавление клиентов»** открывает новое окно, в котором можно добавлять клиентов по серверам (в разделе **«Серверы»**) или по группам (в разделе **«Группы»**).

2) В окне **Параметры задачи** вы можете:

- использовать соответствующие раскрывающиеся меню, чтобы выбрать **имя** пакета продукта ESET, с помощью которого нужно обновить клиент, или открыть диспетчер пакетов 54, чтобы изменить существующие пакеты;
- изменить стандартные имя и описание задачи обновления. Нажмите кнопку **Применить задачу**, если нужно немедленно выполнить задачу, или кнопку **Применить задачу позже**, если нужно указать время для выполнения задачи позже.

3) Нажмите кнопку **«Готово»**, чтобы завершить настройку задачи обновления клиента.

**ПРИМЕЧАНИЕ.**: Эта задача работает только на клиентах, которые подключены непосредственно к основному серверу. Клиенты с реплицированных серверов будут игнорироваться.

### 4.2.6 Как избежать повторных установок

Сразу после завершения удаленной установки агент помечает удаленный клиент флажком, запрещающим повторно использовать тот же самый установочный пакет. Этот флажок записывается в следующий ключ реестра:

*HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer*

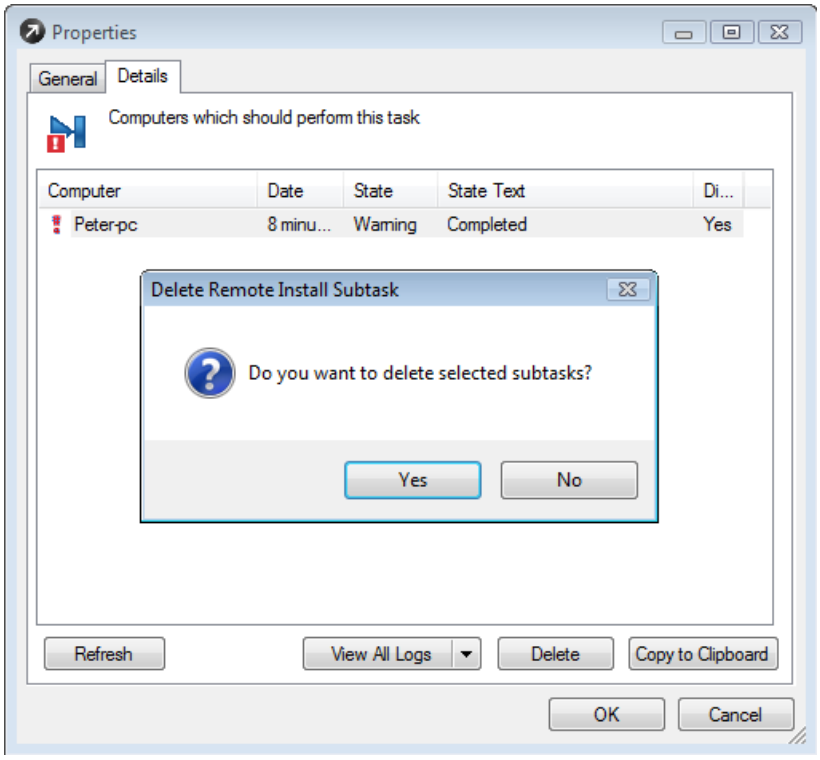
Если тип и название пакета, заданные в агенте *einstaller.exe*, совпадают с данными в реестре, установка не выполняется. Это предотвратит повторные установки на целевых рабочих станциях.

**Примечание.** При удаленной автоматической установке содержимое этого раздела реестра не принимается во внимание.

Сервер ERAS обеспечивает дополнительный уровень защиты от повторных установок, реализуемый в момент установки программой обратного соединения с сервером ERAS (TCP 2224). Если установка успешно завершена, дополнительные попытки установки отклоняются.

Агент записывает следующую ошибку в журнал установщика *%TEMP%\einstaller.log*:

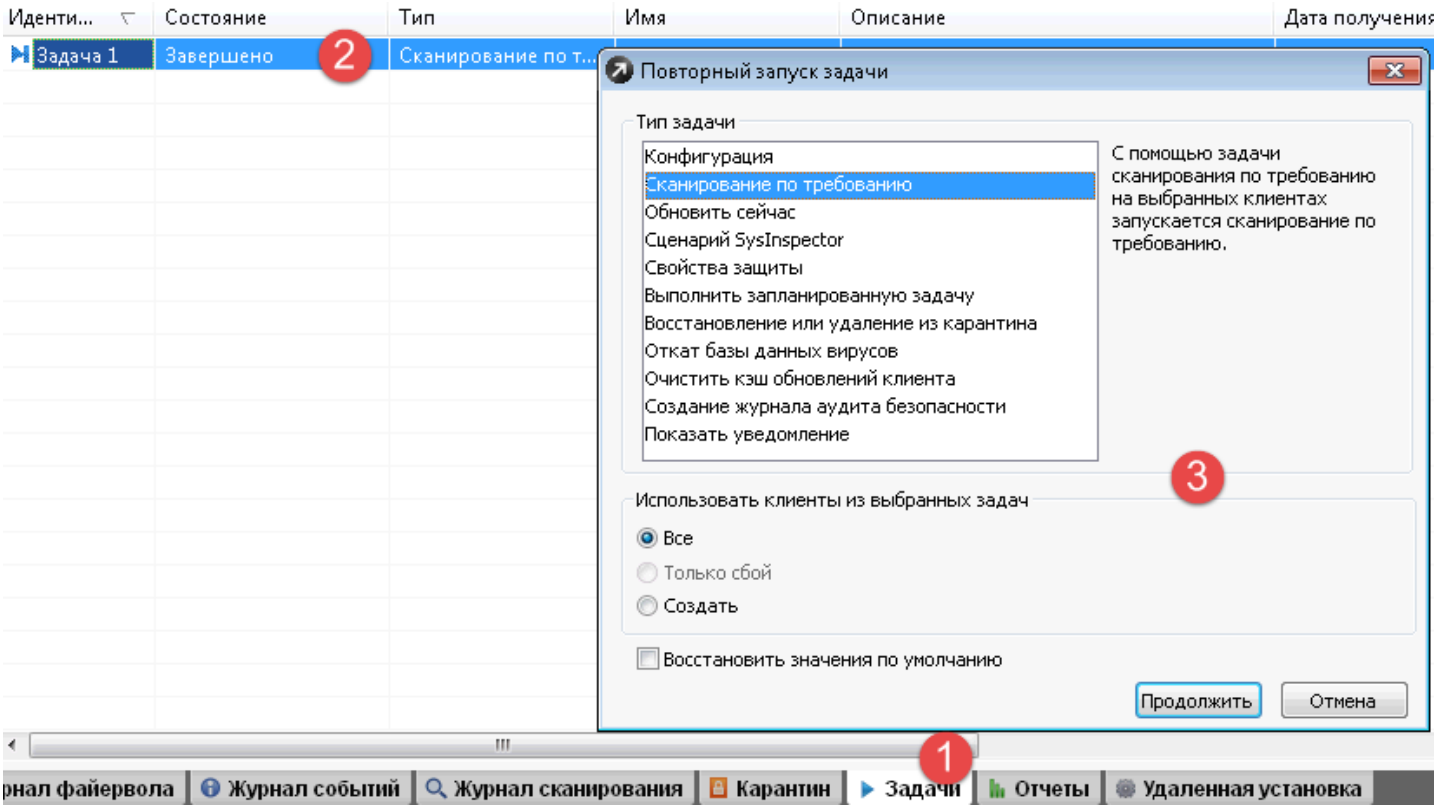
*Программа установки ESET получила сообщение от сервера „X:2224" о выходе;*




чтобы предотвратить отклонение повторных установок сервером ERAS, необходимо удалить соответствующие записи на вкладке **«Данные задачи удаленной установки»**. Чтобы удалить запись, выделите ее, нажмите кнопку **«Удалить»** и подтвердите действие, нажав кнопку **«Да»**.

### 4.2.7 Повторный запуск задачи

Любую задачу, запущенную во вкладке **Клиенты** (через щелчок клиента правой кнопкой мыши и выбора элемента **Новая задача** в контекстном меню), можно найти во вкладке **Задачи**. Любую из этих задач можно запустить повторно. Для этого нужно щелкнуть задачу правой кнопкой мыши и в контекстном меню выбрать пункт **Повторный запуск задачи**.




Если вы открыли окно **Повторный запуск задачи**, значит, у вас несколько вариантов действий:

- перейти к диалоговому окну задачи, которую нужно запустить, нажатием кнопки **Продолжить**;
- выбрать клиенты, к которым нужно применить запускаемую задачу (**Все** — все клиенты, имевшие отношение к задаче; **Только неудавшиеся** — клиенты, выполнение задачи на которых завершилось неудачно; **Создать** — клиенты, которые нужно выбрать в одном из последующих окон диалога);
- выбрать другую задачу для запуска;
- **Восстановить параметры по умолчанию**: если вы изменили используемые по умолчанию параметры ранее запускавшейся задачи, то выбор параметра **Восстановить параметры по умолчанию** приведет к повторному запуску задачи с параметрами по умолчанию.

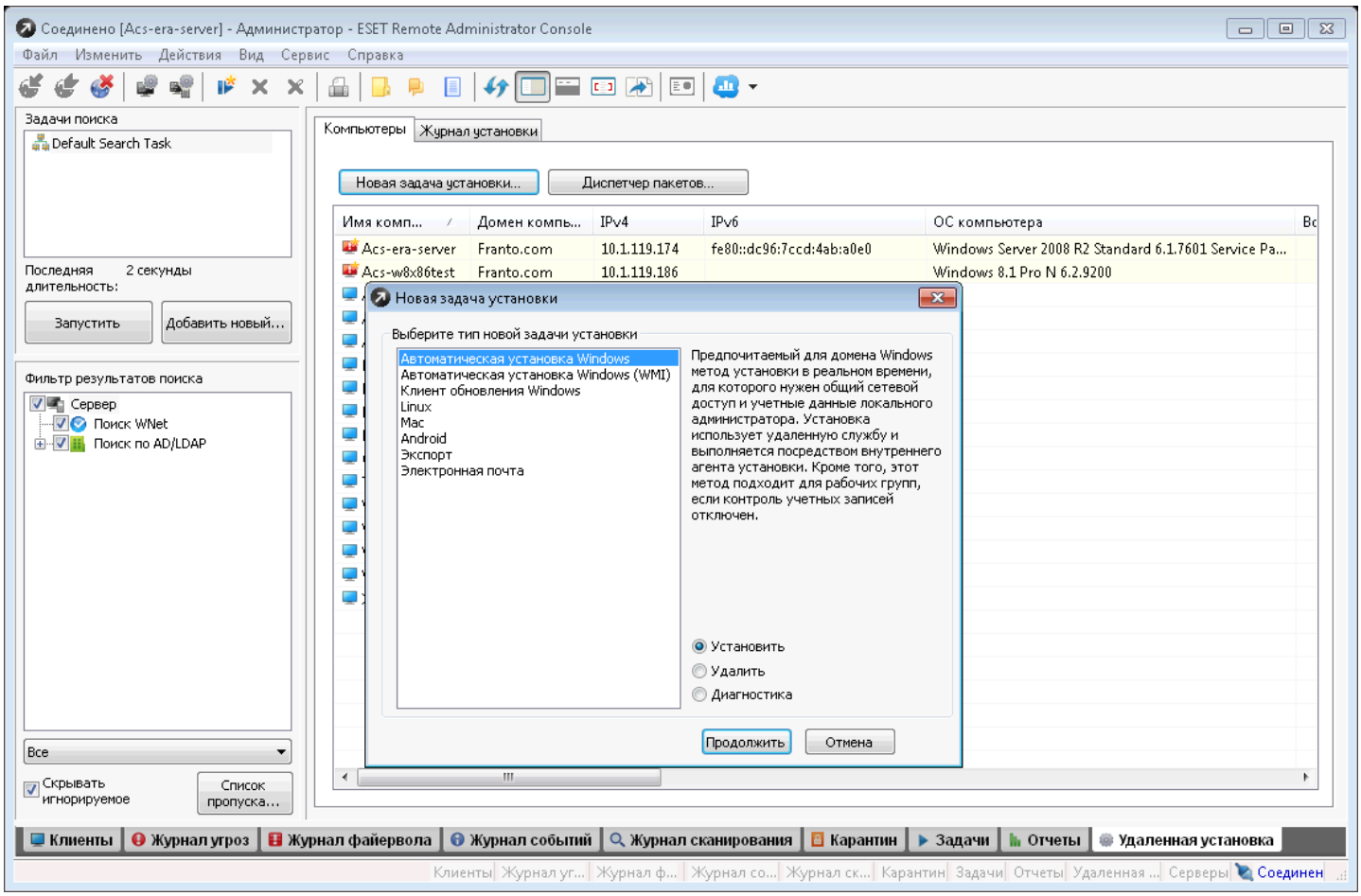
### 4.2.8 Новая задача установки

Щелкнув **Новая задача установки** на вкладке **Удаленная установка**, вы можете выбрать тип Удаленная установка 74, относящийся к следующим вариантам:

- **Автоматическая установка Windows**: выполняет удаленную установку клиентских решений ESET на выбранных удаленных компьютерах в качестве службы. Этому способу установки нужны учетные данные локального администратора, чтобы запускать агент установки на целевом компьютере. При этом на целевых компьютерах должен быть включен общий сетевой доступ и они должны быть в сети.
- **Автоматическая установка Windows (WMI)**: новая функция в ESET Remote Administrator 5.3, которая находит и выполняет пакеты установки в указанной вами 85 сетевой папке.
  Сведения об инструментарии WMI (руководство по инструментарию управления Windows на сайте MSDN)
- **Клиента обновления Windows**: самый надежный способ обновить антивирусное решение ESET (версия 4.2 и более поздние) на управляемых рабочих станциях. Учетные данные администратора не требуются, но на

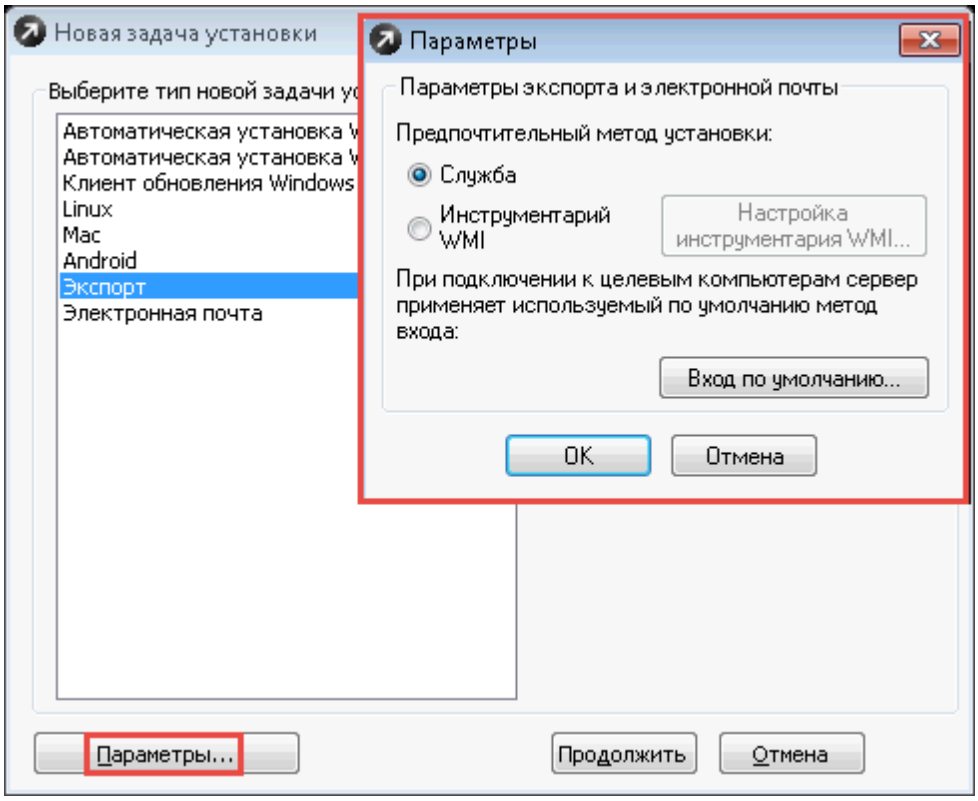
удаленном компьютере нужно включить общий сетевой доступ.

- **Linux**: тип установки клиентских решений ESET из командной строки на большинстве дистрибутивов Linux со включенным доступом SSH.
- **Mac**: тип установки клиентских решений ESET из командной строки на компьютерах под управлением Mac OS X со включенным доступом SSH, который позволяет выполнять пакет установки.
- **Android**: отправка простых в выполнении инструкций по загрузке на устройства под управлением Android и включение процесса регистрации одним щелчком.
- **Экспорт**: экспорт 77 нужного пакета в качестве выполняемого установщика (*einstaller.exe*), чтобы развернуть клиентские решения ESET на компьютеры вне решения ESET Remote Administrator. Если нужно, чтобы экспортированный установщик использовал инструментарий WMI, то, прежде чем выполнять экспорт 77, измените **параметры** способа **Экспорт**.
- **Эл. почта**: доставка небольшого агента установки и инструкций по его применению целевым пользователям по электронной почте 78.



#### 4.2.8.1 Дополнительные параметры

Выбирая один из способов установки клиентских решений ESET (**Экспорт** 77 или **Эл. почта** 77) при запуске **новой задачи установки** 82, помните, что доступны дополнительные **параметры**. Получить к ним доступ можно, нажав кнопку **Параметры**.




**Предпочитаемый способ установки**

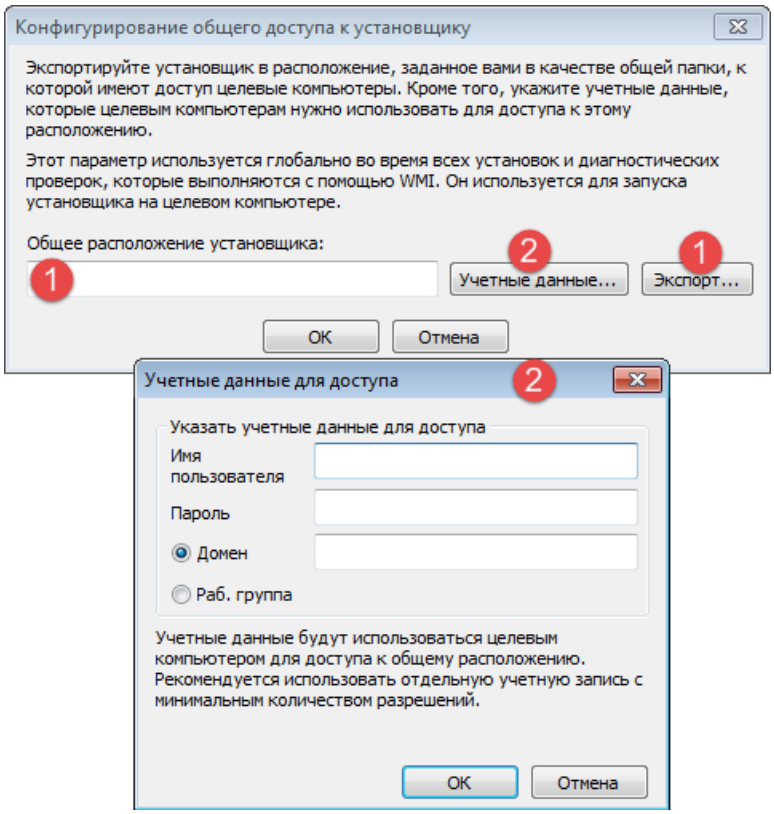
- **Служба**: этот способ задан по умолчанию, даже если вы не открыли диалоговое окно **Параметры**.
- **WMI**: выберите этот способ, если нужно, чтобы целевые компьютеры имели доступ к установщику через инструментарий WMI, и щелкните **Настройка WMI**, чтобы перейти к разделу **Настройка совместного использования установщика** 85.

**Вход по умолчанию** 79: настройка имени пользователя и пароля для системы на основе Windows NT.

#### 4.2.8.2 Настройка совместного использования установщика

Если нужно выполнить автоматическую установку Windows [82] или если выбрать параметр **Эл. почта** или **Экспорт** в окне **Новая задача установки**, а в качестве **предпочитаемого способа установки** выбрать **WMI**, тогда нужно задать сведения о доступе к общему расположению. Это можно сделать с помощью кнопки **Настройка WMI**.

Если нажать кнопку **Настройка WMI**, отобразится окно **Настройка совместного использования установщика**, в котором с помощью кнопки **Экспорт** можно найти нужную папку экспорта (общее расположение), а с помощью кнопки **Учетные данные** — задать учетные данные доступа. Нажатие этой кнопки открывает окно **Учетные данные доступа**.



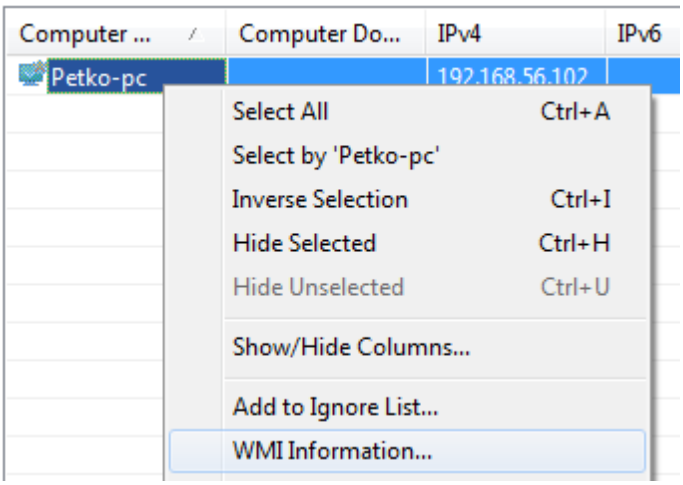

Если в операционной системе настроены переменные среды, то, когда выбран локальный файл, их можно добавлять в путь к общему расположению.

**Примечание**. Даже если для распространения пакета установки используется общее расположение, целевой компьютер должен быть видим для сервера ERA Server по протоколу TCP/IP.

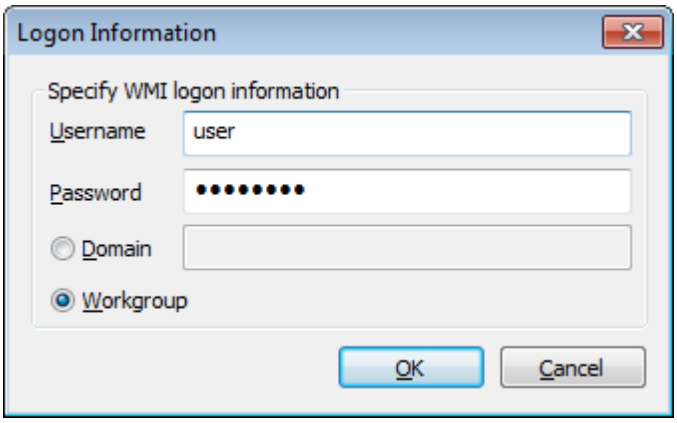
#### 4.2.8.3 Информация WMI

Если нужно отобразить и редактировать информацию WMI управляемого компьютера, выполните следующие действия:

1. В контекстном меню выбранного компьютера щелкните **Информация WMI**.




2. Введите **сведения для входа WMI** и нажмите кнопку **ОК**.




3. Подождите, пока информация не загрузится с компьютера в консоль ERA Console.
4. Информация WMI должна отобразиться через несколько секунд.

#### 4.2.8.4 Экспорт служб WSUS

Если вы хотите установить клиентские решения ESET в качестве **служб WSUS (служб Windows Server Update)**, нужно экспортировать 77 пакет установки из ERA Server 5.3, выбрав при этом параметр **Экспорт служб WSUS (служб Windows Server Update Services)**.

Подробное поэтапное руководство по установке и настройке **служб WSUS** доступно по адресу https://technet.microsoft.com/en-us/library/dd939822(v=ws.10).aspx.

Службы WSUS рассылают только те пакеты, что подписаны сертификатом, установленным на сервере служб WSUS. Вы можете создать такой сертификат с помощью издателя локального обновления (*LUP*). Чтобы установить его на сервере служб WSUS, используйте оснастку MMC для сертификатов.

Добавьте экспортированный 77 *MSI*-установщик и *XML*-файл конфигурации в пакет, созданный издателем *LUP*, и утвердите этот пакет в *LUP*. С этого времени утвержденный пакет будет доставляться в комплекте с обновлениями, приходящими из Центра обновления Windows.

#### 4.2.8.5 Экспорт объекта групповой политики

Если нужно развернуть клиентские решения ESET в рамках установки ПО групповой политики в Active Directory в среде домена, вы можете экспортировать 77 пакет установки из ERA Server 5.3, выбрав при этом параметр **Экспорт объекта групповой политики**. Скопируйте экспортированный *MSI*-установщик и *XML*-файл конфигурации в общую папку (с доступом для чтения), доступную для целевых компьютеров, которыми будет управлять общий объект групповой политики.

Создайте новый объект групповой политики или свяжите существующий объект с нужным подразделением Active Directory в консоли управления групповыми политиками.

Щелкните правой кнопкой мыши объект групповой политики, щелкните **Изменить**, затем в окне **Редактор управления групповыми политиками** в разделе *Конфигурация компьютера* (или «Конфигурация пользователя») *> Политики > Параметры программного обеспечения > Установка программного обеспечения* щелкните пустую область правой кнопкой мыши, выберите **Создать**, **Пакет** и затем найдите *MSI*-установщик, скопированный в общую папку.

- Укажите сетевой путь к *MSI*-установщику, скопированному в общую папку.
- Выберите способ развертывания.

a) назначение — установка программного обеспечения;

b) публикация — предложение ПО в разделе интерфейса «Установка и удаление программ» (только если используется назначенный пользователем объект групповой политики);

c) дополнительно — настройка параметров «Назначенный» и «Опубликованный» и применение изменений к пакету.

ПО автоматически устанавливается после применения групповой политики и перезапуска целевых компьютеров (или входа в систему и выхода из нее, если используется назначенный пользователем объект групповой политики).

# 5. Управление клиентскими компьютерами

## 5.1 Задачи

Для настройки и администрирования клиентских рабочих станций, которые надлежащим образом подключены к серверу ERAS и отображаются на консоли ERAC, можно использовать различные типы задач.

Этап I. **«Новая задача»**

1) Чтобы применить задачу к одной или нескольким клиентским рабочим станциям, щелкните их правой кнопкой мыши на панели **«Клиенты»**, после чего откроется контекстное меню 31.

2) Нажмите кнопку **«Новая задача»** и выберите вид задачи, которую нужно выполнить.

**Примечание.** Кроме того, мастер задач можно запустить с помощью команды главного меню консоли ERAC **«Действия» > «Новая задача»**.

Этап II. Выберите одну из следующих задач:


- Задача конфигурации 89
- Сканирование по требованию (очистка отключена/очистка включена) 90
- Обновить сейчас 90
- Задача «Сценарий SysInspector» 91
- Свойства защиты 91
- Выполнить запланированную задачу 91
- Задача «Восстановить или удалить из карантина» 91
- Откат базы данных вирусов 92
- Очистка кэша обновления клиента 92
- Создать журнал аудита безопасности 93
- Показать уведомление 93


3) После выбора нужной задачи необходимо выполнить действия, описанные в каждом из разделов (см. по ссылкам выше).

Этап III. **«Выбор клиентов»**

4) После настройки задачи в появившемся окне **«Выбор клиентов»** можно изменить выбор клиентов. Выбор клиентов можно изменить путем добавления клиентов из дерева **«Все элементы»** (в левой половине окна) в список **«Выбранные элементы»** (в правой половине окна) или путем удаления клиентов, которые уже есть в списке.

   **Примечание.** Нажмите кнопку **«Добавить специальное...»**, чтобы открыть новое окно, в котором можно добавить клиентов с панели **«Клиенты»** или **«Сервер»** и/или **«Группы»**.

Этап IV. «Завершение задачи» 93

В следующих подразделах дается краткое описание отдельных типов задач для клиентских рабочих станций, каждый из которых сопровождается образцом сценария.

**ПРИМЕЧАНИЕ.**: Окно **проверки обновлений ERA** появляется по истечении заданного интервала времени или при появлении новой версии продукта. Для загрузки последнего обновления продукта с веб-сайта ESET нажмите кнопку **Перейти на веб-сайт обновлений**.

Каждую задачу, которую можно найти на вкладке **Задачи**, можно запустить повторно. Для этого нужно щелкнуть нужную задачу (или несколько выделенных задач) правой кнопкой мыши и выбрать в контекстном

меню пункт **Повторный запуск задачи**. Запущенный мастер **Повторный запуск задачи** похож на мастер **Новая задача**. Вы можете щелкнуть **Продолжить**, чтобы перейти к следующему экрану, или, прежде чем нажимать кнопку **Продолжить**, можно изменить задачу, которую нужно запустить.

Повторный запуск любой задачи приводит к созданию новой записи (строки) во вкладке **Задачи**.

### 5.1.1 Задача конфигурации

Задачи конфигурации используются для изменения настроек защиты на клиентских рабочих станциях. Эти задачи доставляются на клиентские рабочие станции в конфигурационных пакетах, содержащих параметры изменений. *XML*-файлы, созданные в ESET Configuration Editor или экспортированные из клиентов, также совместимы с задачами конфигурации. Ниже приведен пример создания задачи конфигурации, изменяющей имя пользователя и пароль на целевых компьютерах. Все переключатели и параметры, не использующиеся в этом примере, будут описаны в конце этой главы.

Сначала выберите рабочие станции, на которые необходимо доставить задачу. Отметьте эти рабочие станции на панели **«Клиенты»** в консоли ERAC.

1) Щелкните правой кнопкой мыши по любой из выделенных рабочих станций и выберите в контекстном меню пункт **«Новая задача»** > **«Задача конфигурации»**.

2) Откроется окно **«Конфигурация для клиентов»**, которое является мастером задачи конфигурации. Чтобы указать источник конфигурации, нажмите кнопку **«Создать»**, **«Выбрать»** или **«Создать из шаблона...»**.

3) Нажмите кнопку **«Создать**, чтобы открыть ESET Configuration Editor, и выберите применяемую конфигурацию. Выберите **Программы для Windows, версии 3 и 4** > **Модуль обновления** > **Профиль** > **Настройки** > **Имя пользователя** и **Пароль**.

4) Введите предоставленные компанией ESET имя пользователя и пароль и нажмите находящуюся справа кнопку **«Консоль»** для возврата в мастер задачи. В поле **«Создать/Выбрать конфигурацию»** отобразится путь к пакету.

5) Если уже имеется файл с необходимыми изменениями, нажмите кнопку **«Выбрать»**, найдите файл и назначьте его задаче конфигурации.

6) Также можно нажать кнопку **«Создать из шаблона»**, выбрать *XML*-файл и внести необходимые изменения.

7) Нажмите кнопку **«Просмотр»** или **«Изменить»** для просмотра или изменения только что созданного или измененного файла конфигурации.

8) Нажмите кнопку **«Далее»** для перехода в окно **«Выбор клиентов»**, содержащем список рабочих станций, на которые будет доставлена задача. На этом этапе можно добавить клиенты из выбранных серверов или групп. Нажмите кнопку **«Далее»** для перехода к следующему этапу.

9) Последнее диалоговое окно (**«Отчет по задаче»**) предназначено для предварительного просмотра задачи конфигурации. Введите название или описание задачи (необязательно). Параметр **«Применить в»** позволяет назначить запуск задачи на указанное время или дату. Параметр **«Очищать задачи автоматически при успешном выполнении»** удаляет все задачи, которые были успешно доставлены на конечные рабочие станции.

10) Нажмите кнопку **«Готово»**, чтобы поместить задачу на исполнение.

### 5.1.2 Задача сканирования по требованию

В контекстном меню **Новая задача** есть два варианта сканирования по требованию. Первым вариантом является **сканирование по требованию** — по умолчанию выполняется тщательное сканирование и очистка зараженных файлов в **памяти**, **при загрузке жестких дисков** и в **локальных дисках**. Второй вариант — **Сканирование по требованию (очистка отключена)**. После сканирования только создается журнал, и никакие действия не выполняются по отношению к зараженным файлам.

В окне **Сканирование по требованию** для обоих вариантов доступны одни и те же настройки по умолчанию, за исключением параметра **Сканировать без очистки**. Этот параметр включает или отключает очистку зараженных файлов при сканировании. Ниже приведен пример создания задачи «Сканирование по требованию».

1) В раскрывающемся меню **Раздел конфигурации** можно выбрать тип продукта ESET, для которого назначается задача сканирования по требованию. Следует выбирать только продукты, установленные на целевых рабочих станциях.

   **Примечание.** Параметр **Исключить этот раздел из сканирования по требованию** отключает все настройки в окне для выбранного типа продуктов — они не будут применяться на рабочих станциях с продуктом, указанным в разделе **Конфигурация**. Таким образом, все клиенты с указанным продуктом исключаются из списка получателей задачи. Если администратор отмечает клиентов как получателей и исключает продукт с помощью этого параметра, задача завершается неудачей с уведомлением о том, что ее не удалось применить. Во избежание этого администратору всегда следует указывать клиенты, которым назначается соответствующая задача.

2) В поле **Название профиля** можно выбрать профиль сканирования, который нужно применить к задаче.

3) В разделе **Диски** выбираются типы дисков, проверяемых на клиентских компьютерах. Если предлагаемый выбор слишком общий, можно указать точный путь к проверяемым объектам. Для этого используется поле **Путь** или кнопка **Добавить путь**. Параметр **Очистить историю** позволяет восстановить исходный список проверяемых дисков.

4) Нажмите кнопку **Далее**, чтобы перейти к окнам **Выбор клиентов** и **Отчет по задаче**, которые подробно описаны в разделе Задачи 88.

5) После выполнения задачи на клиентских рабочих станциях результаты отправляются обратно серверу ERAS и отображаются в ERAC на панели **Журнал сканирования**.

### 5.1.3 Задача «Обновить сейчас»

Предназначением этой задачи является принудительное обновление рабочих станций (обновляется база данных сигнатур вирусов и программные компоненты).

1) На вкладке **Клиенты** щелкните правой кнопкой мыши по любой рабочей станции и выберите команду **Новая задача** > **Обновить сейчас**.

2) Если нужно исключить из задачи определенные виды продуктов безопасности ESET, выберите их в раскрывающемся меню **Раздел конфигурации** и установите параметр **Исключить данный раздел из задачи обновления**.

3) Чтобы использовать для задачи **Обновить сейчас** определенный профиль обновления, установите флажок **Выбрать название профиля** и выберите необходимый профиль. Также можно установить флажок **Пользовательское имя профиля** и ввести название профиля. Кнопка **Очистить историю** возвращает значение поля по умолчанию.

4) Нажмите кнопку **Далее**, чтобы перейти к диалоговым окнам **Выбор клиентов** и **Отчет по задаче**. Описание этих окон см. в разделе Задачи 88.

### 5.1.4 Задача «Сценарий SysInspector»

Задача «Сценарий SysInspector» позволяет запускать сценарии на конечных компьютерах. Он предназначен для удаления из системы нежелательных объектов. Дополнительную информацию см. в справке по ESET SysInspector 187.

1) После выполнения первого и второго этапов, описанных в разделе Задачи 88, нажмите кнопку **«Выбрать»**, чтобы выбрать сценарий для запуска на целевой рабочей станции.

2) Чтобы настроить сценарий, нажмите кнопку **«Просмотреть и изменить»**.

3) Нажмите кнопку **«Далее»**, чтобы перейти к окнам **«Выбор клиентов»** и **«Отчет по задаче»**, которые подробно описаны в разделе Задачи 88.

4) По окончании выполнения задачи на рабочей станции данные отобразятся в столбце **«Состояние»** на панели **«Задачи»**.

**Примечание.** Задачи сценариев SysInspector поддерживаются в продуктах ESET Endpoint Security/ESET Endpoint Antivirus версии 4.0 и выше.

### 5.1.5 Свойства защиты

Эта задача позволяет администратору изменить состояние свойств защиты продукта безопасности (продукты безопасности ESET версии 5 и выше для Windows ).

1. Каждое свойство защиты имеет три стадии: **Не изменять**, **Временная деактивация** и **Активировать**. Эти стадии можно переключать, устанавливая флажок рядом с каждым свойством. Если свойство защиты было деактивировано (временная деактивация), можно выбрать **Интервал временной деактивации**. Этот интервал может быть от 10 минут до **следующей перезагрузки** (полностью выключает свойство до следующей перезагрузки компьютера).
2. Затем выберите клиенты, для которых нужно изменить свойства защиты и завершите задачу 93.

**ПРИМЕЧАНИЕ.**: Будьте осторожны, когда отключаете свойства защиты, так как это несет потенциальную угрозу безопасности. Клиент получает уведомление каждый раз после отключения свойства защиты.

### 5.1.6 Выполнить запланированную задачу

Эта задача запустит запланированную задачу, которая немедленно запустится на клиенте. Можно выбрать **предопределенную** задачу в планировщике клиента или выбрать задачу **«По идентификатору»**. У каждой запланированной задачи есть идентификатор, чтобы можно было выбрать задачу из раскрывающегося меню или ввести идентификатор. Чтобы просмотреть каждую задачу в планировщике конкретного клиента, запустите задачу из контекстного меню на вкладке **Клиент**.

Выберите задачу, которую нужно запустить на клиенте(ах), затем выберите клиенты для которых нужно изменить функции защиты и завершите задачу 93.

### 5.1.7 Задача «Восстановить или удалить из карантина»

С помощью этой задачи можно восстанавливать или удалять помещенные в карантин объекты с помощью клиента.

1) Когда откроется окно **Восстановление или удаление из карантина** (см. раздел Задачи 88), выберите действие, которое нужно выполнить с изолированным объектом: **Восстановить** или **Удалить**.

   **Примечание.** При восстановлении из карантина объекта, который по-прежнему идентифицируется как угроза, рекомендуем исключить этот объект из дальнейшей проверки, воспользовавшись параметром **Добавить исключение**, чтобы предотвратить повторную проверку объекта и помещение его в карантин. Обратите внимание, что некоторые объекты, например троянские кони и вирусы, исключить нельзя. Попытка исключить такие файлы приведет к ошибке. Если вы хотите исключить чистые файлы (не идентифицированные как угроза), сделайте это непосредственно на клиента или с помощью редактора конфигурации ESET (политика, задачи и т. п.).

2) Выберите условие, в соответствии с которым изолированные объекты должны быть восстановлены или удалены и нажмите кнопку **Далее**.

**ПРИМЕЧАНИЕ.** Если диалоговое окно «Восстановление или удаление из карантина» открыто из окна карантина щелчком правой кнопкой мыши непосредственно на вкладке **Карантин** (и выбран параметр **Задача восстановления или удаления из карантина**), вам не нужно указывать условия (параметр **По хэшу** будет выбран автоматически, а в качестве идентификатора будет использован хэш изолированного файла).

3) Выберите клиентов для операции восстановления или удаления (см. раздел. Задачи 88) и нажмите кнопку **Далее**.

4) Проверьте параметры в окне **Отчет по задаче**, введите имя задачи, укажите время применения задачи, затем, если необходимо, задайте параметры очистки и нажмите кнопку **Готово** для подтверждения. Дополнительные сведения см. в разделе Задачи 88.

### 5.1.8 Откат базы данных вирусов

Если вы подозреваете, что новые обновления антивирусных баз могут быть нестабильными или поврежденными, вы можете откатить ее до предыдущей версии и отключить обновления для выбранного периода времени. Кроме того, вы можете включить ранее отключенные обновления.

1) Отключить/включить обновления базы данных сигнатур вирусов

**Выключить на X часов** — будет выполнен откат базы данных клиентов до предыдущей версии (на основе созданного на клиенте снимка) и любые обновления для выбранных клиентов будут отключены на выбранный период времени. Можно также выбрать **Навсегда** и полностью отключить обновления. Будьте осторожны, когда отключаете обновления базы данных, так как это несет потенциальную угрозу безопасности.

***Предупреждение***: Параметр **Навсегда** остается активным даже после перезагрузки клиентского компьютера.

**Включить ранее отключенные обновления** — обновление базы данных вирусов будет снова включено.

2) Выберите клиенты для этой задачи и нажмите кнопку **Далее**.

3) Проверьте параметры в окне **Отчет по задаче**, введите имя задачи, укажите время применения задачи, затем, если необходимо, задайте параметры очистки и нажмите кнопку **Готово** для подтверждения. Дополнительные сведения см. в разделе Задачи 88.

### 5.1.9 Очистка кэша обновления клиента

Эта задача предназначена для продуктов безопасности ESET версии 5 и выше. Если есть основания думать, что обновление вирусной базы не удалось, можно очистить кэш обновления клиента, и тогда последние обновления будут загружены снова.

1) Запустите задачу и нажмите кнопку **Далее**.

2) Выберите клиенты для этой задачи и нажмите кнопку **Далее**.

3) Проверьте параметры в окне **Отчет по задаче**, введите имя задачи, укажите время применения задачи, затем, если необходимо, задайте параметры очистки и нажмите кнопку **Готово** для подтверждения. Дополнительные сведения см. в разделе Задачи 88.

### 5.1.10 Задача «Создать журнал аудита безопасности»

Данная задача применима только к ESET Mobile Security.

Проверки безопасности: заряд аккумулятора, состояние Bluetooth, свободное место на диске, видимость устройства, домашняя сеть и выполняемые процессы. Будет создан подробный отчет, показывающий, не опустилось ли значение элемента ниже установленного порога или может ли это представлять потенциальную угрозу безопасности (например, устройство стало видимым и т.д.).

Включение аудита безопасности на телефоне

1) Щелкните правой кнопкой мыши имя клиента на панели **«Клиенты»** и выберите в контекстном меню команду **«Новая задача»** > **«Создать журнал аудита безопасности»**.

2) Затем нажмите кнопку **«Далее»**, чтобы перейти к диалоговым окнам **«Выбор клиентов»** и **«Отчет по задаче»**. Описание этих окон см. в разделе Задачи 88.

### 5.1.11 Задача «Показать уведомление»

Данная задача применима только к ESET Mobile Security.

Отправка уведомления (например, предупреждения) на телефон:

1) Щелкните правой кнопкой мыши имя клиента на панели **«Клиенты»** и выберите в контекстном меню команду **«Новая задача»** > **«Показать уведомление»**.

2) Введите **заголовок** уведомления и **текст** сообщения в соответствующих полях и установите уровень **детализации** уведомления.

3) Затем нажмите кнопку **«Далее»**, чтобы перейти к диалоговым окнам **«Выбор клиентов»** и **«Отчет по задаче»**. Описание этих окон см. в разделе Задачи 88.

### 5.1.12 Завершение задачи

В последнем диалоговом окне можно еще раз просмотреть сводку параметров задачи. В нем отображаются все параметры задачи и есть кнопка **Назад**, которая позволяет вернуться к изменению параметров.

Во второй части доступны есть следующие параметры:

- **Название** — название задачи;
- **Описание** — описание задачи;
- **Применить задачу после** — время запуска задачи на клиентских компьютерах;
- **Удалять задачи автоматически при успешном выполнении** — задачи автоматически удаляются после их успешного выполнения.
- **Произвольная задержка начала до X мин** — будет выполнена произвольная задержка задачи для выбранных компьютеров. Поэтому если выбрано несколько компьютеров, то задача будет отправлена на каждый из них в разное время, а не одновременно.

**Примечание**. Произвольная задержка доступна только для продуктов ESET версии 5 и выше.

## 5.2 Диспетчер групп

Диспетчер группы представляет собой функциональный инструмент для управления клиентами, позволяющий разделить их на отдельные группы и применить к ним различные параметры, задачи, ограничения и т. д. Диспетчер легко вызывается из меню **«Служебные программы» > «Диспетчер групп»** или клавишами **CTRL+G**. Группы независимы для каждого сервера ERAS и не реплицируются.

Можно создавать собственные группы с учетом текущий потребностей сети компании или просто синхронизировать группы клиентов ERAC с каталогом Microsoft Active Directory с помощью шаблона **«Синхронизация Active Directory»** прямо в главном окне диспетчера групп.

Группы клиентов могут быть двух типов:

- Статические группы 94
- Параметрические группы 95

Статические и параметрические группы можно использовать в различных частях ERA, что существенно расширяет возможности в области управления клиентами.

### 5.2.1 Статические группы

Статические группы создаются для объединения клиентов в сети в именованные группы и подгруппы. Например, можно создать группу «Маркетинг», в которой будут собраны всю клиенты маркетинга, а также создать специализированные подгруппы — «Местные продажи», «Руководство EMEA» и т. п.

Главное окно статических групп разделено на две части. В левой части отображается иерархия существующих группы и подгрупп. Клиенты, являющиеся членами выбранной группы, отображаются в правой части окна. По умолчанию отображаются только клиенты из выбранной группы. Чтобы отображались клиенты, входящие в подгруппы выбранной группы, установите флажок **«Показывать клиенты в подгруппах»** справа от окна.

Чтобы создать новую группу, нажмите кнопку **«Создать»** и введите название группы. Новая группа будет создана как подгруппа выбранной в данный момент родительской группы. Если нужно создать основную группу, выделите корень иерархического дерева — **«Статические группы»**. Поле **«Родительская группа»** содержит имя родительской группы для новой созданной группы (например, "/" для корневой группы). Рекомендуется использовать названия, обозначающие местонахождение компьютеров (например, *Бухгалтерия, Технический отдел* и т. п.). В поле «Описание» можно задавать дополнительное описание группы (например, *«Компьютеры в центральном офисе», «Компьютеры дизайнеров»* и т. п.). Кроме того, свойства созданных и настроенных групп можно изменить позже.

**Примечание.** Если задача отправлена в родительскую группу, все рабочие станции, принадлежащие ее подгруппе, также примут эту задачу.

Кроме того, можно создать пустую группы для последующего использования.

Нажмите кнопку **ОК**, чтобы создать группу. Слева появится название и описание группы. Кроме того, станет активной кнопка **«Добавить/удалить»**. Эта кнопка предназначена для добавления клиентов в группу (дважды щелкните по клиенту или перетащите его из левой части в правую). Чтобы найти и добавить клиента, полностью или частично введите его имя в поле **«Быстрый поиск»**: в результате появится список всех клиентов, в названии которых есть введенная строка. Чтобы отметить всех клиентов, нажмите кнопку **«Выбрать все»**. Для проверки наличия новых клиентов, подключившихся к серверу, нажмите кнопку **«Обновить»**.

Если выбор клиентов вручную не подходит, нажмите кнопку **«Добавить специальные...»**, чтобы открыть окно с дополнительными параметрами.

Параметр **«Добавить клиенты»** на панели клиентов позволяет добавить все клиенты, отображенные в разделе клиентов; кроме того, доступен параметр **«Только выбранные»**. Чтобы добавить клиенты, уже относящиеся к другому серверу или группе, выделите их в списках слева и справа и нажмите кнопку **«Добавить»**.

Для возврата в главное окно редактора статических групп нажмите в окне **«Добавить/удалить»** кнопку **ОК**. В

результате отобразится новая группа с соответствующими клиентами.

Для добавления или удаления клиентов из групп предназначена кнопка **«Внести/убрать»**, а для удаления целых групп — кнопка **«Удалить»**. Для копирования списков клиентов и групп используется кнопка **«Копировать в буфер обмена»**. Для обновления клиентов группы нажмите кнопку **«Обновить»**.

Клиентов выбранной группы можно также **импортировать/экспортировать** в *XML*.

### 5.2.2 Параметрические группы

В дополнение к статическим группам доступны параметрические группы. Клиентские станции динамически присваиваются определенной параметрической группе при соответствии условиям данной группы. Преимущество параметрических групп заключается в том, что их можно использовать в различных местах: в фильтрах, в политиках, в отчетах и уведомлениях.

Главное окно параметрический группы состоит из четырех частей. В разделе **«Параметрические группы»** перечислены созданные родительские группы и подгруппы. После выбора определенной группы из **Списка «Параметрические группы»** принадлежащие этой группе клиенты отображаются в разделе **«Выбранная группа»**.

**Примечание.** Если выбрана родительская группа, список будет также содержать членов подгруппы.

Параметры, установленные для выбранной группы, отображаются в разделе **«Параметры»** данного окна. Чтобы изменить или добавить параметры, нажмите кнопку **«Изменить...»**.

В разделе **«Состояние синхронизации»** отображается ход выполнения синхронизации.

1. Чтобы создать новую группу, нажмите кнопку **«Создать...»**. Новая группа будет создана как подгруппа выбранной в данный момент родительской группы. Если нужно создать основную группу, выделите корень иерархического дерева — **«Параметрические группы»**. Поле **«Родительская группа»** содержит имя родительской группы для новой созданной группы (например, "/" для корневой группы). Введите **имя** и краткое **описание** новой группы.
2. Следующим шагом является создание **параметров фильтрации клиентов**. Это можно сделать в **Редакторе правил**, выбрав параметры после нажатия кнопки **«Изменить...»**. Здесь можно указать условия, необходимые для запуска и применения правила. Выберите условие и укажите его, нажав кнопку **«Указать»** возле правила в окне **«Параметры»**. Также можно указать, в каких случаях должно применяться правило: только если **соблюдены все условия** или если **соблюдены некоторые условия**.
3. Если установлен флажок **«Закрепить»**, клиенты будут автоматически добавляться в эту группу, если отвечают ее условиям (при этом автоматическое удаление не выполняется). Содержимое закрепленной группы можно сбросить вручную на уровне корневого каталога.

**Примечание.** Этот параметр можно установить только при создании новой группы.

Чтобы изменить существующую группу, выберите ее из **Списка параметрических групп** и нажмите кнопку **«Изменить...»** в нижней части окна. Чтобы удалить группу, выберите нужную группу и нажмите кнопку **«Удалить»**.

Список групп можно обновить вручную с помощью кнопки **«Обновить»**. Чтобы импортировать группу из файла, выберите в разделе **«Параметрические группы»** группу, в которую нужно импортировать новую группу, и нажмите кнопку **«Импорт...»**. Подтвердите выбор, нажав кнопку **«Да»**. Найдите файл для импорта и нажмите кнопку **«Открыть»**. Группы (и все ее подгруппы) будут импортированы в выбранное место. Чтобы экспортировать группу (и ее подгруппы), выберите ее в разделе **«Параметрические группы»**, щелкните стрелку кнопки **«Импорт...»** и выберите команду **«Экспорт...»**. Подтвердите действие, нажав кнопку **«Да»**, выберите имя экспортируемого файла, укажите для него расположение и нажмите кнопку **«Сохранить»**.

**Примечание.** Группы в разделе **«Параметрические группы»** можно перетаскивать с помощью мыши.

**ПРИМЕЧАНИЕ.**: Параметрические группы можно использовать для фильтрации данных или клиентов. Например, можно создать отчеты только для компьютеров с ОС Windows XP. Создавайте параметрическую группу только для компьютеров с конкретной операционной системой и используйте эту группу для фильтрации. Также можно настроить собственные **«Клиентские данные»** во время создания пакета установки

54 — (**«Редактор конфигурации»** > **«Ядро»** > **«Настройки»** > **«Удаленное администрирование»**). Установите этот параметр (Клиентские данные) в качестве параметра для параметрической группы. Таким образом, каждый пользователь, который установит этот пакет, станет членом этой группы.

### 5.2.3 Синхронизация Active Directory/LDAP

При синхронизации Active Directory группы (с соответствующими клиентами) создаются автоматически на базе структуры Active Directory. Это позволяет администратору сортировать клиенты по группам (при условии, что имя клиента соответствует типу объекта *компьютер* на стороне Active Directory (AD) и входит в группы AD).

Есть два основных параметра, которые определяют порядок синхронизации.

- С помощью параметра **Синхронизировать группы** можно выбрать группы AD для синхронизации. Параметр **Все группы** используется для синхронизации всей структуры дерева AD независимо от того, есть ли в группах AD клиенты ERA. Следующие два параметра (**Только группы с клиентами сервера ERA Server** и **Только группы с клиентами главного сервера ERA**) обеспечивают только синхронизацию групп с уже существующими клиентами ERA.
- Параметр **Тип синхронизации** определяет, будут ли синхронизируемые группы AD добавлены в существующие группы AD/LDAP (значение **Импорт групп AD/LDAP**) или существующие группы AD/LDAP будут полностью заменены синхронизируемыми (значение **Синхронизация групп AD**).
- Параметр **Синхронизированные филиалы** позволяет выбрать конкретные филиалы **Active Directory/LDAP** для синхронизации. Щелкните **Настроить** и выберите филиалы Active Directory/LDAP, которые необходимо синхронизировать с группами. По умолчанию отмечены/выбраны все филиалы.

**Примечание**: щелкните **Дополнительные сведения**, чтобы отобразить дополнительные сведения о параметрах и правилах синхронизации Active Directory/LDAP.

- Чтобы настроить интервал синхронизации между AD/LDAP и сервером ERA, щелкните **Изменить** рядом с параметром «Синхронизировать». В диалоговом окне **Запланированный интервал синхронизации AD/LDAP (по локальному времени сервера)** выберите необходимую частоту синхронизации. Выбранная частота будет отображаться возле параметра **Синхронизировать**.

Подробная настройка синхронизации Active Directory выполняется в **редакторе конфигурации** (**Remote Administrator** > **ERA Server** > **Параметры** > **Группы** и **Active Directory/LDAP**). Можно добавить и другие объекты Active Directory/LDAP, установив соответствующие флажки.

Нажатие кнопки **Синхронизировать** запускает процесс синхронизации (в соответствии с выполненной выше настройкой параметров).

**Примечание.** Для синхронизации ERAS с Active Directory сервер ERAS не требуется устанавливать на контроллер домена. Достаточно того, чтобы контроллер домена был доступен с компьютера, на котором находится сервер ERAS. Чтобы настроить аутентификацию для контроллера домена, выберите **Служебные программы** > **Параметры сервера** > **Дополнительно** > **Изменить дополнительные параметры** > **Remote Administrator** > **ERA Server** > **Параметры** > **Active directory/LDAP**.

## 5.3 Политики

Политики напоминают **«Задачи конфигурирования»**, с тем отличием, что не являются разовыми задачами, отправляемыми на одну или несколько рабочих станций. Вместо этого политики предназначены для постоянного обслуживания конфигурационных настроек продуктов безопасности ESET. Другими словами, **«Политика»** политика — это конфигурация, которая принудительно устанавливается для клиента.

### 5.3.1 Основные принципы применения и действия

Диспетчер политик вызывается с помощью команды меню **«Служебные программы»** > **«Диспетчер политик»**. В дереве политик слева перечислены политики, присутствующие на отдельных серверах. Правая часть состоит из четырех областей — **«Параметры политики»**, **«Конфигурация политики»**, **«Действие политики»** и **«Глобальные настройки политики»**, — параметры в которых позволяют администратору управлять политиками и настраивать их.

Основными функциями диспетчера политик являются создание, изменение и удаление политик. Клиенты получают политики с сервера ERAS. На сервере ERAS может использоваться несколько политик, которые наследуют настройки друг от друга или с сервера верхнего уровня.

Система копирования политик с сервера верхнего уровня называется *наследованием*; политики, созданные в результате наследования, называются *объединенными политиками*. Наследование основано на принципе «Родитель — ребенок», то есть дочерняя политика наследует настройки родительской политики.

### 5.3.2 Создание политик

При установке по умолчанию реализована только одна политика — «Политика сервера». Сама политика настраивается в редакторе ESET Configuration Editor: нажмите кнопку **Изменить политику...** и задайте параметры для выбранного продукта ESET для безопасности (или клиента). Все параметры упорядочены в обширную структуру, а все элементы в редакторе обозначены значками. Для клиентов можно применять только активные параметры (они отмечены голубым значком). Все неактивные параметры (серого цвета) остаются на целевых компьютерах без изменений. Тот же принцип действует для унаследованных и объединенных политик: дочерняя политика наследует из родительской политики только активные параметры.

На серверах ERA Server можно использовать несколько политик (**Новая дочерняя политика...**). Для новых политик доступны следующие параметры: **Название политики**, связанное с параметрами **Родительская политика** и **Конфигурация политики** (можно использовать пустую конфигурацию, скопировать объединенную конфигурацию из плотики в раскрывающемся меню, скопировать ее из *XML*-файла конфигурации или использовать **мастер объединения правил файервола**). Политики можно создавать только на сервере, к которому подключена консоль ERAC. Для создания политик на подчиненном сервере необходимо подключиться к этому серверу.

У каждой политики есть два основных атрибута. **«Переопределять все дочерние политики»** и **«Реплицируемая вниз политика»**. Эти атрибуты определяют наследование дочерними клиентами активных параметров конфигурации.

- **«Переопределить все дочерние политики»** — принудительно изменяет все активные параметры в унаследованных политиках. Если в дочерней политике имеются отличия, объединенная политика будет содержать все активные параметры из родительской политики (даже если для дочерней политики включен параметр **«Переопределить все дочерние политики»**). Все неактивные параметры из родительской политики будут приведены в соответствие с дочерней политикой. Если параметр **Переопределить все дочерние политики** не включен, в объединенной политике настройки дочерней политики будут иметь более высокий приоритет, чем настройки родительской политики. Такие объединенные политики применяются ко всем остальным дочерним политикам той политики, в которую вносятся изменения.
- **Реплицируемая вниз политика** — включает репликацию политики на подчиненные серверы, например, политика может служить политикой по умолчанию для подчиненных серверов, а также назначаться клиентам, подключенным к подчиненным серверам.

Политики также можно импортировать из *XML*-файла и экспортировать в него, а также импортировать из групп. Дополнительные сведения см. в разделе Импорт и экспорт политик 99.

### 5.3.3 Виртуальные политики

В дополнение к созданным и реплицированным с других серверов политикам (см. раздел Вкладка «Репликация» 130) в дереве политик также есть родительская политика по умолчанию, которая называется виртуальной политикой.

Родительская политика по умолчанию находится на сервере более высокого уровня в **глобальных** настройках политик и выбирается как **Политика по умолчанию для подчиненных серверов**. Если сервер не реплицируется, политика является пустой (этот момент подробнее разъясняется далее).

Политика по умолчанию для основных клиентов находится на выбранном сервере (не на сервере более высокого уровня) в глобальных настройках политик и выбирается как «Политика по умолчанию для основных клиентов». Она автоматически применяется к новым (основным) клиентам, подключившимся к данному серверу ERAS, независимо от того, применялась ли к ним другая политика из правил политик (дополнительные сведения см. в разделе Назначение политик клиентам 100. Виртуальные политики являются ссылками на другие политики, находящиеся на том же сервере.

### 5.3.4 Роль и назначение политик в древовидной структуре политик

Каждая политика в **дереве политик** обозначается значком слева. Значение этих значков описано ниже.

1) Политики, обозначенные синими значками, используются на данном сервере. Существует три разновидности синих значков.

Значки с белой серединой — политика создана на данном сервере. Кроме того, она не реплицируется вниз, т. е. не назначается клиентам серверами нижнего уровня, а также не является родительской политикой для дочерних серверов. Такие политики можно использовать только на данном сервере — для клиентов, подключенных к этому серверу. Она также может быть родительской политикой для другой политики на том же самом сервере.

Значки с синей серединой — политика также создана на данном сервере, но при этом выбран параметр **«Переопределять все дочерние политики»** (дополнительные сведения см. в главе Создание политик 97).

Значки со стрелкой вниз — эти политики реплицируются, т. е. включен параметр **Реплицируемая вниз политика** включен. Эти политики можно использовать на данном сервере или на его дочерних серверах.

Значки для **политик сервера** по умолчанию.

2) Политики, обозначенные неактивными значками, созданы на других серверах.

Значки со стрелкой «Вверх» — эти политики реплицированы с дочерних серверов. Их можно только просмотреть или удалить с помощью функции **«Удалить ветвь политики»**. Сама политика при этом не удаляется, она будет удалена только из дерева политик. Поэтому такие политики могут снова появляться после репликации. Чтобы не отображать политики с подчиненных серверов, воспользуйтесь параметром **«Скрыть неиспользуемые политики чужого сервера в дереве политик»**.

Значки со стрелкой «Вниз» — эти политики реплицированы с серверов верхнего уровня. Их можно использовать в качестве родительских для других назначенных политик, назначать клиентам (**«Добавить клиенты»**) или удалять (**«Удалить политику»**). В этом случае удаляется только сама эта политика — она снова появится после репликации с сервера верхнего уровня (если на сервере верхнего уровня для нее не отключен атрибут **«Реплицируемая вниз политика»**).

**Примечание.** Чтобы переместить или назначить политику в рамках структуры, можно либо выбрать ей родительскую политику, либо перетащить ее с помощью мыши.

Существующие правила политики можно импортировать и экспортировать в *XML*-файл с помощью кнопки **Импорт/экспорт**. Если имена существующей и импортированной политики совпадают, после названия импортируемой политики добавляется случайная строка.

### 5.3.5 Просмотр политик

Политики в структуре **дерева политик** можно просматривать прямо в **редакторе конфигураций**, выбрав **Просмотр политики** > **Вид...** или **Показать объединенные...**.

**«Показать объединенные»** — отображение объединенной политики, созданной в результате наследования (в ходе наследования применяются настройки родительской политики). Этот параметр отображается по умолчанию, поскольку действующая политика уже является объединенной.

**«Просмотр»** — отображение исходной политики до ее слияния с родительской.

На серверах нижнего уровня политикам, унаследованным от серверов верхнего уровня, доступны следующие параметры.

**«Показать объединенные»** — см. выше.

**Просмотреть обязательную часть** — эта кнопка применяется только к политикам с атрибутом **Переопределить все дочерние политики**. Этот параметр позволяет просматривать только принудительно заданную часть политики, т. е. ту ее часть, которая имеет приоритет над другими настройками дочерних политик.

**«Просмотреть необязательную часть»** — имеет значение, противоположное параметру «Просмотреть обязательную часть», т. е. отображает только активные элементы, к которым параметр «Переопределить...» не применяется.

**ПРИМЕЧАНИЕ.**: Для просмотра объединенных элементов дважды щелкните элемент в дереве политики.

### 5.3.6 Импорт и экспорт политик

Диспетчер политик позволяет импортировать и экспортировать политики и правила политик. Существующие политики можно импортировать и экспортировать в *XML*-файл с помощью кнопки **Импорт и экспорт политик**. Кроме того, политики можно импортировать из групп с помощью кнопки **«Импорт из групп...»**. Правила политик можно импортировать и экспортировать с помощью кнопки **Импорт...** или **Экспорт...**. Их также можно создавать в **мастере правил политик**.

Конфликты имен при импорте (существующая и импортированная политика с одинаковыми названиями) решаются путем добавления случайной строки после названия импортируемой политики. Если конфликт не может быть решен таким образом (как правило, из-за того, что новое имя слишком длинное) импорт заканчивается с предупреждением *Конфликт неразрешенного имени политики*. Решением является переименование или удаление конфликтующей политики или правил политики.

### 5.3.7 Мастер миграции политик

**Мастер миграции политик** поможет создать новую **политику рабочей станции Windows версии 5** или обновить существующую политику **рабочей станции Windows версии 5** с помощью параметров из существующих политик программ для Windows версий 3 и 4. Можно выполнить миграцию всех политик в процессе установки поверх предыдущей версии, но для настройки всех необходимых для миграции параметров рекомендуется использовать **мастер миграции политик**.

Для миграции политик выполните следующие действия.

1. Установите флажки для политик, параметры которых подлежат миграции.
2. Если политика Endpoint уже существует, выберите один из следующих параметров.

- **Заменить существующую политику Endpoint и использовать только исходные настройки**: полная замена существующей политики на новую (**рабочие станции Windows версии 5**), при этом используются настройки исходной политики (**программы для Windows версий 3 и 4**).
- **Объединить политики и не заменять конфликтующие настройки Endpoint**: существующие политики будут объединены с перенесенными, а существующие настройки политики рабочей станции Windows версии 5 не будут перезаписаны настройками политики программ для Windows версий 3 и 4.
- **Объединить политики и заменить конфликтующие настройки Endpoint**: существующие политики будут

объединены с перенесенными, а конфликтующие настройки будут заменены исходными (версий 3 и 4).

3. Дождитесь завершения процесса. Его продолжительность может быть разной и зависит от количества переносимых политик. Нажмите кнопку **Готово**, когда отобразится сообщение **Миграция политик завершена**.

### 5.3.8 Назначение политик клиентам

Ниже описаны два основных правила назначения политик клиентам.

1. Локальным (основным) клиентам можно назначить любую локальную политику или любую политику, реплицированную с серверов более высокого уровня.
2. Клиентам, реплицированным с серверов более низкого уровня, можно назначить любую локальную политику с атрибутом **«Реплицируется вниз»** или любую политику, реплицированную с серверов более высокого уровня. Этим клиентам нельзя принудительно назначить политику с их собственного главного сервера (для этого необходимо подключиться к этому серверу с помощью консоли ERAC).

Важным моментом является то, что каждому из клиентов назначается какая-нибудь политика (клиентов без политики не существует). Кроме того, политику клиента нельзя удалить — ее можно только заменить другой. Чтобы не применять к клиенту конфигурацию ни из одной политики, создайте пустую политику.

#### 5.3.8.1 Политика по умолчанию для основных клиентов

Одним из методов назначения политик является автоматическое применение **Политики сервера** — виртуальной политики, которая настраивается в **глобальных** настройках политики. Эта политика применяется к основным клиентам — к клиентам, которые напрямую подключены к серверу ERAS. Дополнительную информацию см. в разделе Виртуальные политики 98.

#### 5.3.8.2 Назначение вручную

Назначить политику вручную можно двумя способами: Щелкните правой кнопкой мыши панель **«Клиенты»** и выберите в контекстном меню команду **«Задать политику»** или щелкните в диспетчере политик **«Добавить клиенты»** > **«Внести/убрать»**.

После выбора команды **«Добавить клиенты»** в диспетчере политик откроется диалоговое окно **«Установить/удалить»**. Список клиентов находится слева в виде «Сервер/Клиент». Если выбран параметр **«Реплицируется вниз»**, в окне также будут перечислены клиенты, реплицированные с подчиненных серверов. Выберите клиенты для политики посредством перетаскивания или с помощью кнопки **>>**, перемещающей их в список **выбранных**. Новые выбранные клиенты помечаются желтой звездочкой; их можно удалить из списка **выбранных** с помощью кнопки **<<** или клавиши **С**. Нажмите кнопку **ОК**, чтобы подтвердить выбор.

**Примечание.** Если после подтверждения повторно открыть окно **«Установить/удалить»**, клиентов уже нельзя будет удалить из списка **«Выбранные элементы»**. Можно будет только заменить политику для них.

Клиенты также можно добавлять с помощью функции **«Добавить специальное»**, которая добавляет все клиенты сразу, только выбранные клиенты или клиенты из выбранных серверов или групп.

#### 5.3.8.3 Правила политик

Инструмент **«Правила политик»** позволяет администратору автоматически назначать политики клиентским рабочим станциям более удобным способом. Правила применяются сразу после подключения клиента к серверу. Они имеют более высокий приоритет, чем у **Политика сервера** или назначения, заданные вручную. **Политика сервера** применяется только в случае, если клиент не подпадает под текущие правила. Аналогичным образом, если применяется вручную назначенная политика, конфликтующая с правилами политик, приоритет будет иметь конфигурация, принудительно примененная правилами политик.

Если все серверы обслуживаются локальными администраторами, каждый администратор может создавать для своих клиентов отдельные правила политик. В этом сценарии важно, чтобы правила политик не конфликтовали. Например, сервер верхнего уровня назначает клиентам политику, основанную на правилах

политик, а подчиненный сервер в то же время назначает отдельные политики, основанные на правилах локальных политик.

Для создания правил политик и управления в диспетчере политик есть отдельная вкладка **Правила политики**. Процесс создания и применения правил очень похож на аналогичный процесс в почтовых клиентах: каждое правило содержит один или несколько критериев; чем выше правило в списке, тем оно важнее (их можно перемещать вверх и вниз).

Чтобы создать новое правило, нажмите кнопку **Создать правило** и выберите один из вариантов: **Создать новое** или использовать Мастер правил политики 102. Затем укажите значения параметров **«Название»**, **«Описание»**, **«Фильтр клиентов»** и **«Политика»** (политика, которая применяется ко всем клиентам, удовлетворяющим указанному критерию).

Для настройки критерия фильтрации нажмите кнопку **Изменить**.

**«(NOT) FROM основного сервера»** — клиент (не) находится на основном сервере.
**«(НЕ) ЯВЛЯЕТСЯ новым клиентом»** — клиент (не) является новым.
**«HAS (NOT) новый флаг»** — применяется к клиентам с флагом «Новый клиент» или без него.
**«Основной сервер (НЕ) содержит (указать)»** — имя основного сервера (не) содержит указанную строку.
**«ГРУППЫ ERA IN (указать)»** — клиент относится к указанным группам.
**«НЕ В ГРУППАХ ERA (указать)»** — клиент не относится к указанным группам.
**«ДОМЕН/РАБОЧАЯ ГРУППА (NOT) IN (указать)»** — клиент относится/не относится к указанному домену.
**«Маска имени компьютера (указать)»** — имя компьютера соответствует указанному значению.
**«HAS маска IPv4 (указать)»** — клиент относится к группе, определяемой указанными адресом IPv4 и маской.
**«HAS диапазон IPv4 (указать)»** — клиент относится к группе, определяемой указанными диапазоном адресов IPv4.
**«HAS маска IPv6 (указать)»** — клиент относится к группе, определяемой указанными адресом IPv6 и маской.
**«HAS диапазон IPv6 (указать)»** — клиент относится к группе, определяемой указанными диапазоном адресов IPv6.
**«HAS (NOT) определенная политика (указать)»** — клиент (не) наследует указанную политику.
**«Название продукта (НЕ) содержит»** — название продукта содержит указанную строку.
**«Версия продукта (НЕ)»** — версия продукта соответствует указанной.
**«Маска прочих данных клиента 1, 2, 3 (НЕ) содержит»** — прочие данные клиента содержат указанное значение.
**Маска комментария клиента (НЕ) содержит** —
**«HAS (NOT) состояние защиты (указать)»** — для клиента установлено указанное состояние защиты.
**«Версия БД сигнатур вирусов (НЕ)»** — версия БД сигнатур вирусов соответствует указанной.
**«Последнее подключение (НЕ) старше чем (указать)»** — последнее подключение старше указанного времени.
**«Ожидание перезапуска (НЕТ)»** — клиент ожидает перезапуска.

Правила политики можно импортировать в *XML*-файл и экспортировать из него. Правила политики можно также создать автоматически с помощью мастера правил политики 102, который позволяет создать структуру политики но основе структуры существующей группы и сопоставлять созданные политики группам путем создания соответствующих правил политики. Дополнительные сведения об импорте и экспорте правил политики см. в разделе Импорт и экспорт политик 99.

Для удаления правила политики нажмите кнопку **Удалить правило...**.

Чтобы немедленно применить активное правило, нажмите кнопку **Применить сейчас правило политики...**.

#### 5.3.8.3.1 Мастер правил политики

Мастер правил политики позволяет создать структуру политики на основе структуры существующей группы и сопоставлять созданные политики с группами путем создания соответствующих правил политики.

1. Сначала будет предложено организовать собственные группы. Если нужная структура групп отсутствует, выберите Диспетчер групп 94, чтобы сначала настроить группы, а затем нажмите кнопку **Далее**.
2. На втором этапе будет предложено указать категории групп клиентов, на которые будет влиять новое правило политики. После установки нужных флажков нажмите кнопку **«Далее»**.
3. Выберите **«Родительскую политику»**.
4. На этом последнем этапе будет показано простое сообщение о состоянии процесса. Чтобы закрыть окно **мастера правил политики**, нажмите кнопку **«Готово»**.

Новое правило политики появится в списке на вкладке **«Правила политики»**. Установите флажок рядом с именем правила, чтобы активировать его.

Дополнительные сведения об импорте и экспорте правил политики, а также о конфликтах имен см. в разделе Импорт и экспорт политик 99.

### 5.3.9 Политики для мобильных клиентов

У пользователя, у которого продукт ESET установлен на мобильном устройстве, больше возможностей для управления параметрами и поведением программного обеспечения, чем у пользователя, у которого продукт ESET установлен на ноутбуке или настольном ПК. Поэтому нет необходимости постоянно применять политики для мобильных пользователей, так как пользователь может, при желании, изменить или настроить некоторые параметры. Чтобы создать политику для мобильных клиентов, рекомендуем использовать методику, продемонстрированную ниже.

**Создание пустой политики (политики по умолчанию для клиентов)**

1. Выберите **Служебные программы > Диспетчер политик**.
2. Выберите **Добавить новую политику**, чтобы создать пустую политику без измененных настроек. В разделе «Конфигурация политики», выберите пункт **Создать пустую конфигурацию политики**.
3. Нажмите кнопку **Добавить клиенты** и выберите мобильных пользователей, которыми нужно управлять с помощью этой политики.
4. Перейдите на вкладку Правила политики 100 и нажмите кнопку **Создать**.
5. Выберите эту политику в раскрывающемся меню **Политика** и нажмите кнопку **Изменить**.
6. Выберите условие правила **ЭТО новый клиент** , а затем в поле «Параметры» выберите «ЭТО», чтобы изменить условие правила на «ЭТО НЕ новый клиент», и нажмите кнопку «ОК» два раза.
7. Нажмите кнопку «ОК», а затем — кнопку «Да», когда отобразится вопрос о том, нужно ли сохранить настройки.
8. Эта политика будет применяться к клиенту при каждом подключении к решению ERA.

**Создание одноразовой политики (политика запуска для клиентов)**

1. Выберите **Служебные программы > Диспетчер политик**.
2. Выберите **Добавить новую политику**, чтобы создать пустую политику без измененных настроек. В разделе «Конфигурация политики», выберите пункт **Создать пустую конфигурацию политики**.
3. Настройте параметры, которые необходимо применить для мобильных клиентов, и сохраните конфигурацию.
4. Нажмите кнопку **Добавить клиенты** и назначьте мобильных пользователей, которыми нужно управлять с помощью этой политики.

5. Перейдите на вкладку Правила политики [100] и нажмите кнопку **Создать**.
6. Выберите эту политику в раскрывающемся меню **Политика** и нажмите кнопку **Изменить**.
7. Выберите условие правила **ЭТО новый клиент** и нажмите кнопку «ОК» два раза.
8. Нажмите кнопку «ОК», а затем — кнопку «Да», когда отобразится вопрос о том, нужно ли сохранить настройки.

Когда мобильные клиенты подключаются к решению ERA в первый раз, они получают настройки из **одноразовой политики**. При следующем подключении к решению ERA, они получают **пустую политику**, и она никак не повлияет на их настройки.

### 5.3.10 Удаление политик

Как и создание правил, их удаление возможно только для политик, находящихся на сервере, с которым установлено соединение. Для удаления политик на других серверах к ним необходимо подключиться с помощью консоли ERAC.

**Примечание.** Политика может быть связана с другими серверами или политиками (как родительская политика, как политика по умолчанию для подчиненных серверов, как политика по умолчанию для основных клиентов и т. п.), поэтому в некоторых случаях ее придется заменить, а не удалить. Для просмотра параметров удаления и замены нажмите кнопку **Удалить политику**. Описанные ниже параметры могут быть доступны или недоступны в зависимости от положения заданной политики в иерархии политик.

- **«Новая политика для главных клиентов с удаленной политикой»**: позволяет выбрать новую политику для основных клиентов в качестве замены для удаляемых. Основные клиенты могут принимать **политику по умолчанию для основных клиентов**, а также другие политики с того же сервера (назначенные вручную с помощью кнопки **«Добавить клиенты»** или принудительно **правилами политик**). В качестве замены можно использовать любую политику с заданного сервера или реплицированную политику.
- **«Новая родительская политика для дочерних политик удаленной политики»** — если удаляемая политика является родительской для других дочерних политик, ее также необходимо заменить. Заменить ее можно политикой с того же сервера, политикой, реплицированной с серверов более высокого уровня, или флагом «н/д», который означает, что дочерним политикам будет назначена незаменяемая политика. Настоятельно рекомендуется назначать замену, даже если дочерних политик не существует. Назначение другим пользователем дочерней политики этой политике в процессе удаления приведет к конфликту.
- **«Новая политика для реплицированных клиентов с удаленной или измененной политикой»**: здесь можно выбрать новую политику для клиентов, реплицированных с серверов более низкого уровня, которые были связаны с удаляемой политикой. В качестве замены можно использовать любую политику с заданного сервера или реплицированную политику.
- **«Новая политика по умолчанию для подчиненных серверов»**: если удаленная политика является виртуальной (см. раздел **«Глобальные настройки политики»**), ее необходимо заменить другой политикой (дополнительную информацию см. в разделе Виртуальные политики [98]). В качестве замены можно использовать любую политику с заданного сервера или флаг «н/д».
- **«Новая политика по умолчанию для главных клиентов»**: если удаленная политика является виртуальной (см. раздел **«Глобальные настройки политики»**), ее необходимо заменить другой политикой (дополнительную информацию см. в разделе Виртуальные политики [98]). Для замены можно использовать политику с того же сервера.

Если отключить параметр политики **«Реплицируется вниз»** и нажать кнопку **«ОК, Применить»** или выбрать в дереве политик другую политику, появится такое же диалоговое окно. При этом будут включены параметры **«Новая политика для реплицированных клиентов с удаленной или измененной политикой»** или **«Новая политика по умолчанию для подчиненных серверов»**.

### 5.3.11 Специальные настройки

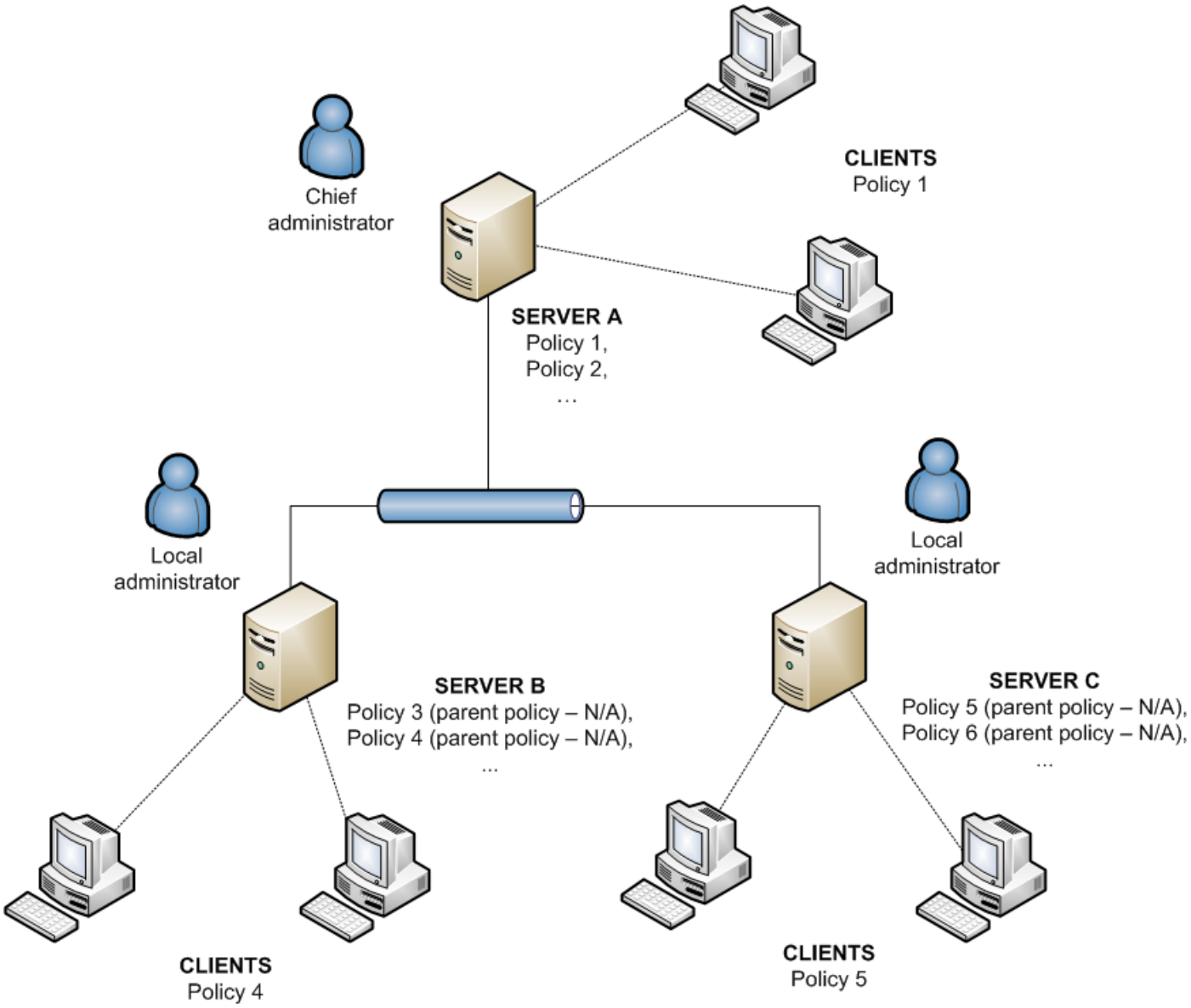
Еще две политики находятся не в диспетчере политик, а в разделе **Служебные программы** > **Параметры сервера** > **Дополнительно** > **Изменить дополнительные настройки** > **ESET Remote Administrator** > **ERA Server** > **Параметры > Политики**.

- **Интервал принудительного применения политики (мин)** — эта функция применяется к политикам через указанный промежуток времени. Рекомендуется оставлять значение по умолчанию.
- **Отключить использование политики** — включите этот параметр, чтобы отменить применение политики к серверам. Рекомендуется использовать этот параметр в случае возникновения проблем с политикой. Если к некоторым клиентам не нужно применять политику, лучше назначить им пустую политику.

### 5.3.12 Сценарии развертывания политик

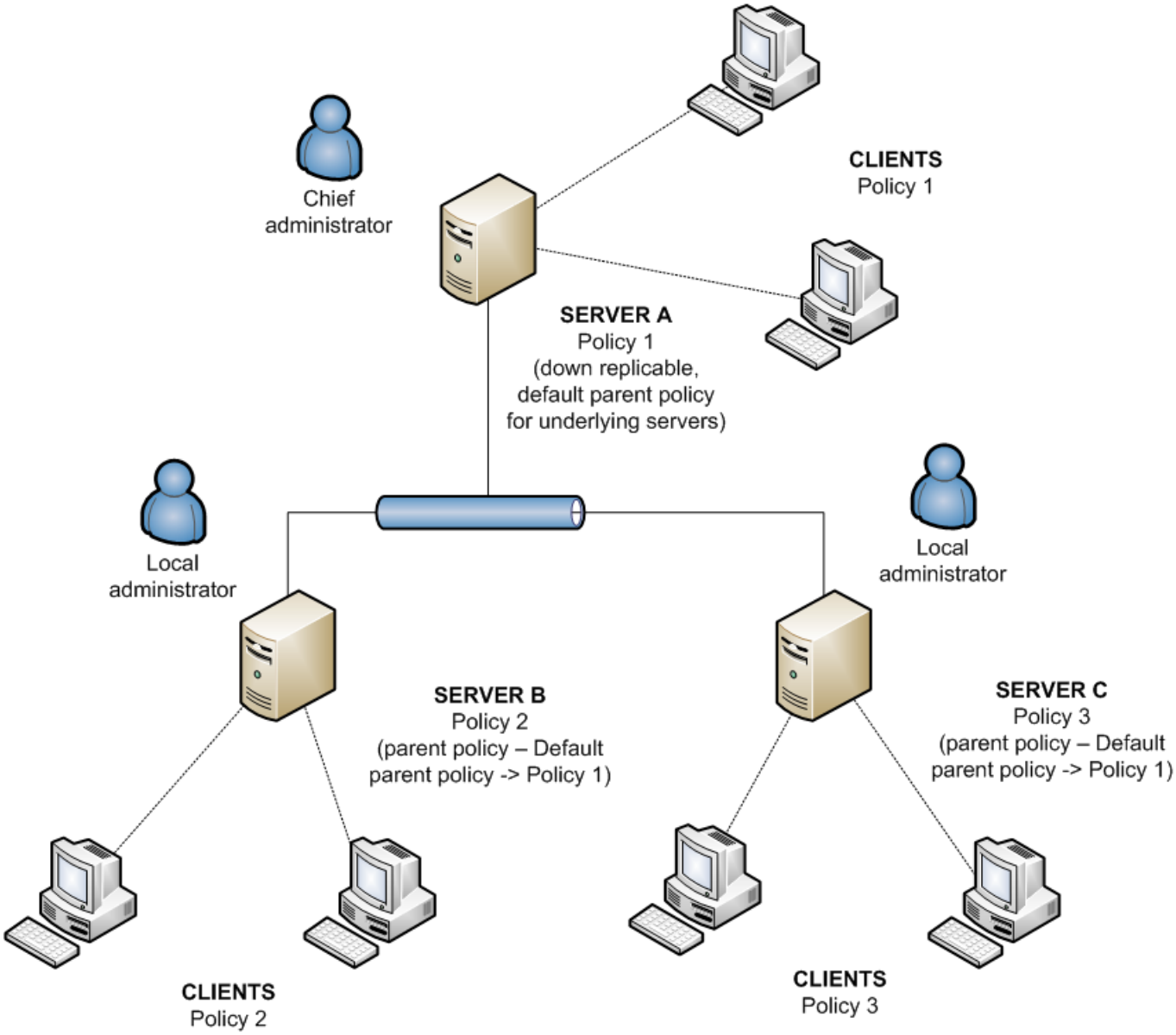
#### 5.3.12.1 Каждый сервер является автономной единицей, политики определяются локально

Этот сценарий предназначен для небольших сетей с одним главным и двумя подчиненными серверами. У каждого сервера есть несколько клиентов. На каждом из серверов создано не менее одной политики. Подчиненные серверы находятся в филиалах; оба сервера обслуживаются локальными администраторами. Каждый из администраторов сам решает, какие политики применяются к различным клиентам его сервера. Главный администратор не изменяет конфигурации, созданные локальными администраторами, и не назначает политики клиентам подчиненных серверов. С точки зрения политики сервера это означает, что у сервера А отсутствует **политика по умолчанию для подчиненных серверов**. Это также означает, что у сервера Б и сервера В для родительской политики установлен флаг «н/д» или другая локальная политика (отдельно от **родительской политики по умолчанию**). (Например, у серверов Б и В отсутствуют родительские политики, назначенные с главного сервера.)


Chief
administrator
CLIENTS
Policy 1
SERVER A
Policy 1,
Policy 2,
…
Local
administrator
Local
administrator
SERVER B
Policy 3 (parent policy – N/A),
Policy 4 (parent policy – N/A),
…
SERVER C
Policy 5 (parent policy – N/A),
Policy 6 (parent policy – N/A),
…
CLIENTS
Policy 4
CLIENTS
Policy 5

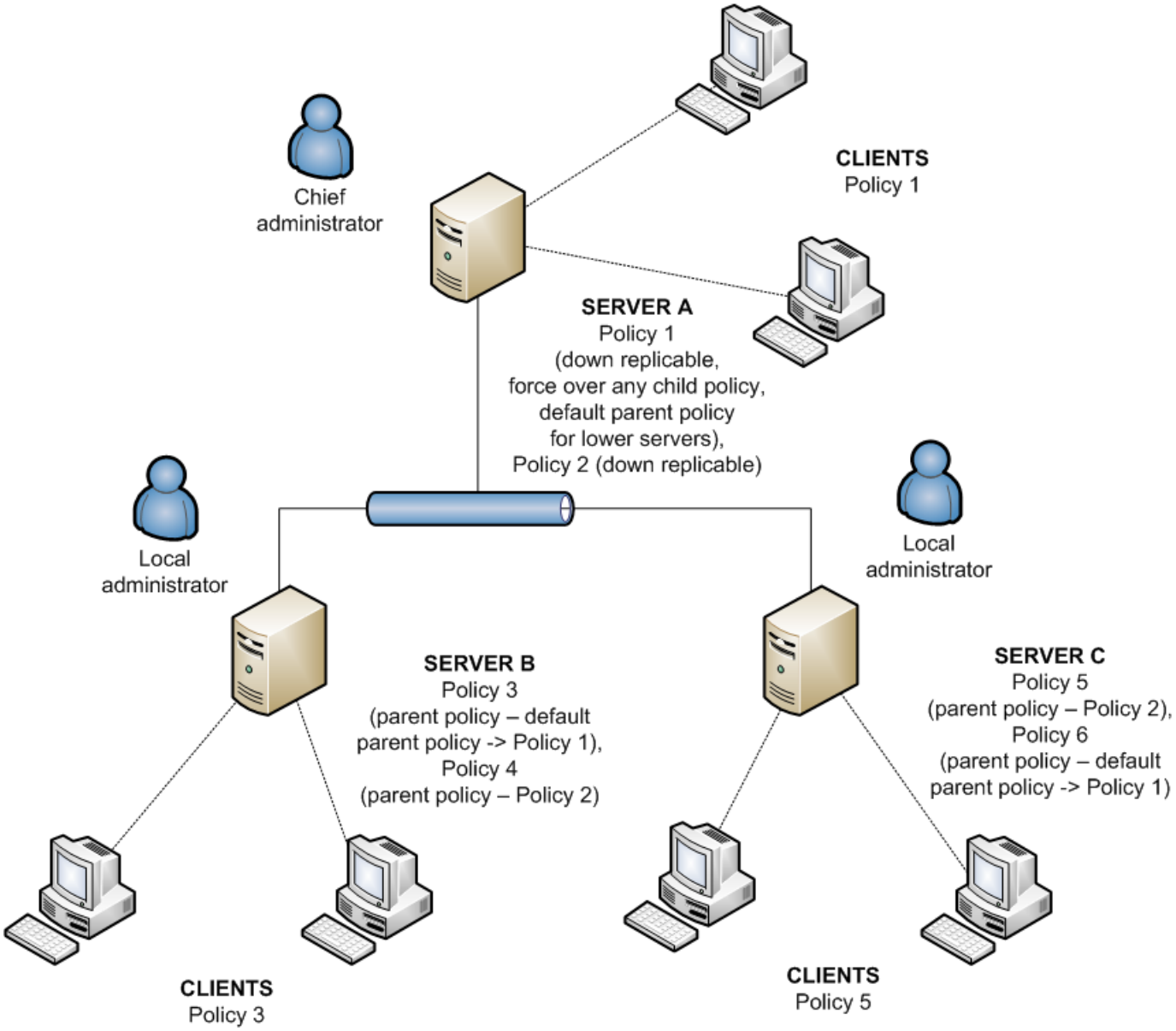
**5.3.12.2 Каждый сервер обслуживается отдельно, политики управляются локально, но родительская политика по умолчанию наследуется с сервера верхнего уровня.**

Конфигурация из предыдущего сценария применима также и к этому сценарию. Однако при этом для сервера А включен параметр «Политика по умолчанию для подчиненных серверов», а политики на подчиненных серверах наследуют с основного сервера конфигурацию родительской политики по умолчанию. В этом сценарии локальные администраторы имеют достаточно прав для настройки политик. Хотя дочерние политики на подчиненных серверах могут наследовать родительскую политику по умолчанию, локальные администраторы все-таки могут изменять ее своими собственными политиками.



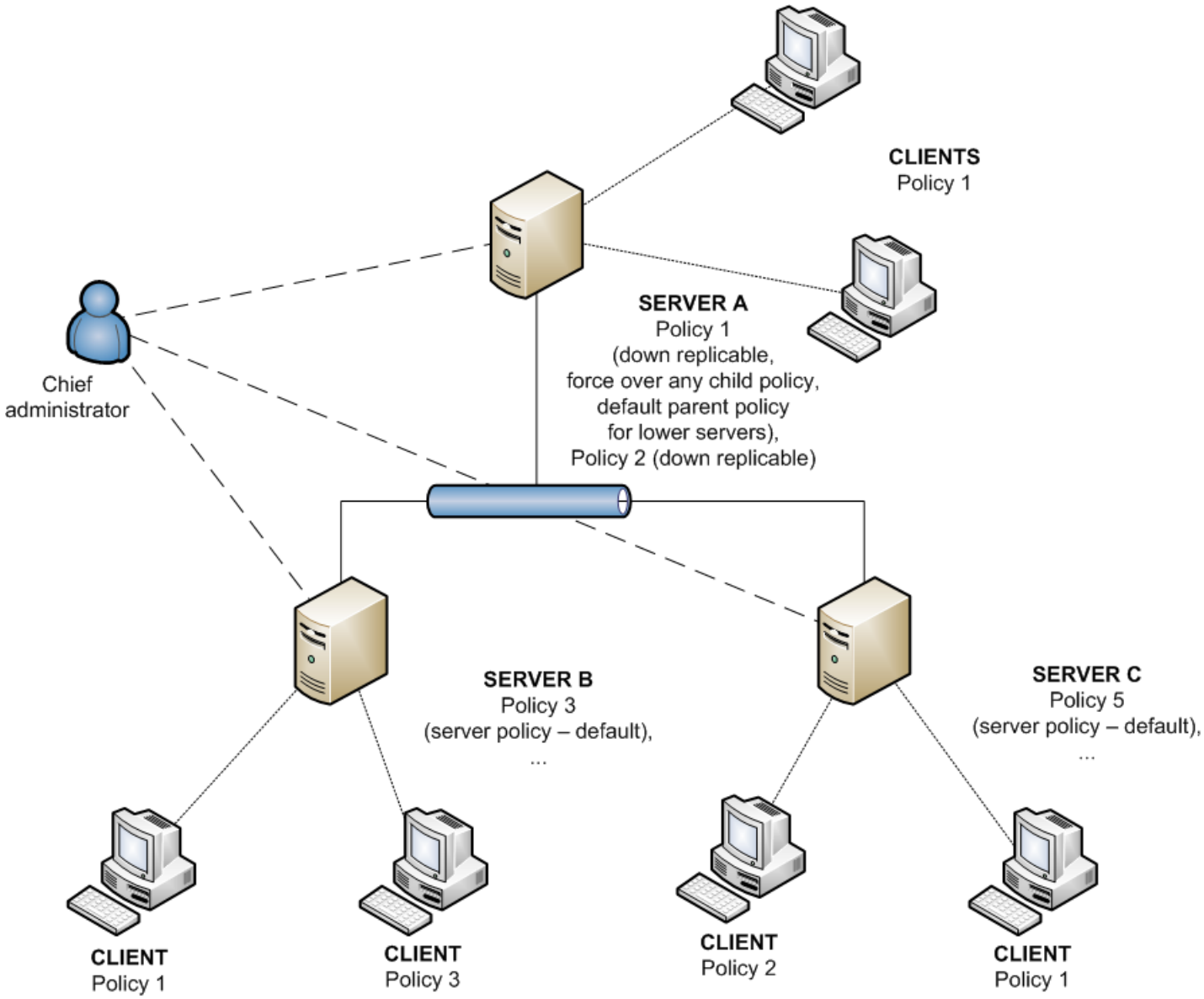
### 5.3.12.3 Наследование политик с сервера верхнего уровня

Сетевая модель этого сценария та же самая, что и в предыдущих двух сценариях. Кроме того, основной сервер с родительской политикой по умолчанию содержит другие политики, которые реплицируются на уровень ниже и служат родительскими политиками для подчиненных серверов. Для политики 1 (см. рисунок ниже) активирован атрибут **«Применить поверх любых дочерних политик»**. У локального администратора остается достаточно прав, но главный администратор определяет, как и какие политики реплицируются вниз и какие из них служат родительскими для локальных политик. Атрибут **«Переопределить…»** означает, что конфигурации, установленные в выбранных политиках, переопределяют эти настройки на локальных серверах.



### 5.3.12.4 Назначение политик только с сервера верхнего уровня

Данный сценарий соответствует централизованной системе управления политиками. Политики для клиентов создаются, изменяются и назначаются только на главном сервере, а у локальных администраторов нет прав на их изменение. У всех подчиненных серверов есть только одна базовая политика, которая является пустой (по умолчанию она называется «Политика сервера»). Эта политика служит родительской политикой по умолчанию для основных клиентов.




### 5.3.12.5 Использование групп

В некоторых ситуациях назначение политик группам клиентов служит дополнением к ранее использовавшимся сценариям. Группы можно создавать вручную или с помощью параметра **«Синхронизация Active Directory»**.

Клиентов можно добавлять в группы вручную (**«Статические группы»**) или автоматически — по свойствам группы (**«Параметрические группы»**). Дополнительные сведения см. в разделе Диспетчер групп 94.

Чтобы назначить политику для группы клиентов, можно использовать параметр разового назначения **«Диспетчер групп»** (**«Добавить клиентов» > «Добавить специальное»**), или доставить политики напрямую через **правила политик**.

Ниже показан один из возможных сценариев.

**Администратору нужно назначить различные политики для клиентов, принадлежащих различным группам AD, и автоматически изменять политики клиента, когда клиент перемещается в другую группу AD.**

1) Сначала необходимо настроить **синхронизацию Active Directory** в **диспетчере групп** согласно своим потребностям. Здесь важно правильно запланировать синхронизацию AD (возможные варианты: каждый час, ежедневно, каждую неделю, каждый месяц).

2) После первой удачной синхронизации группы AD появятся в разделе **«Статические группы»**.

3) Создайте новое правило политики и установите **«Группы ERA В»** и/или **«Группы ERA НЕ В»** как условие правила.

4) Укажите группы AD, которые нужно добавить в условие.

5) В следующем шаге определите политику, которая будет применяться к клиентам, соответствующим условиям правил(а) и нажмите кнопку **ОК**, чтобы сохранить правило.

**ПРИМЕЧАНИЕ.**: Шаги 3–5 можно заменить, используя **мастер правил политики**, который позволяет создать структуру политики но основе структуры существующей группы и сопоставлять созданные политики группам путем создания соответствующих правил политики.

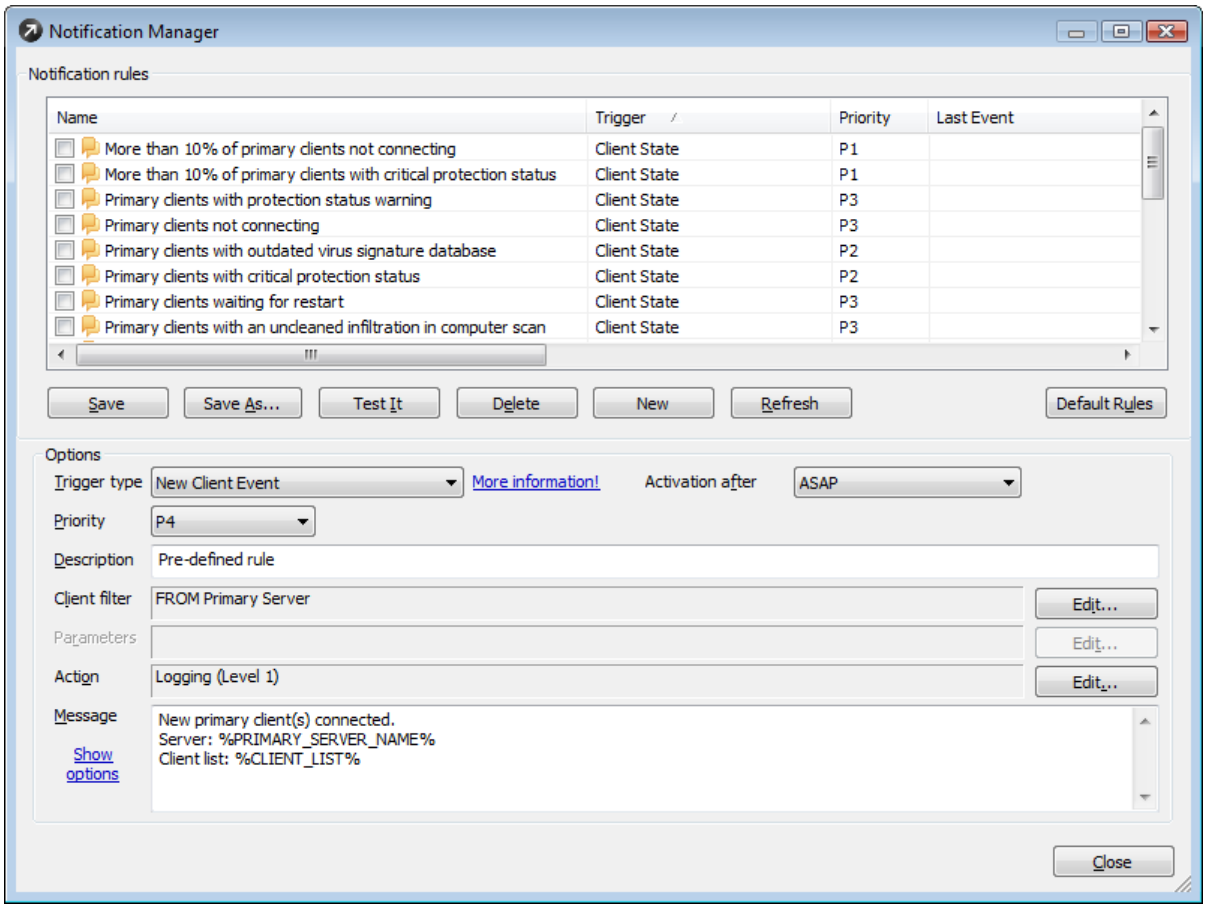
Таким образом можно определить конкретное правило политики для каждой группы AD. Присвоение конкретной политики определенным клиентам теперь зависит от членства клиента в определенной группе AD. Поскольку синхронизация AD выполняется регулярно, все изменения членства клиента в группах AD обновляются и учитываются при применении правила политики. Другими словами, политики применяются к клиентам автоматически в зависимости от их группы AD. После полного определения правил и политик администратору больше не нужно заниматься применением политик.

Основным преимуществом такого подхода является прямое автоматическое связывание членства в группах AD с присвоением политики.

## 5.4 Диспетчер уведомлений

Возможность уведомлять системных и сетевых администраторов о важных событиях является важной составляющей системы защиты и обеспечения целостности сети. Своевременное предупреждение об ошибке или вредоносной программе может предотвратить потерю огромного количества времени и денег для устранения проблемы на более поздней стадии. В следующих трех разделах описаны возможности функции уведомлений, реализованной в программе удаленного администрирования ESET.

Чтобы открыть главное окно **«Диспетчера уведомлений»**, выберите **«Сервис»** > **«Диспетчер уведомлений»**.




Главное окно разделено на две области.

1. В верхней части окна в разделе **«Правила уведомлений»**перечислены существующие (предварительно определенные или определенные пользователем) правила. Для создания уведомлений необходимо выбрать правило из списка. По умолчанию уведомления включены. Поэтому рекомендуется проверить, включены ли правила. Функциональные кнопки в списке правил: **«Сохранить»** (сохранение изменений в правиле), **«Сохранить как...»** (сохранение изменений в правиле с новым именем), **Удалить**, **Проверить** (при нажатии этой кнопки будет незамедлительно запущено правило и отправлено уведомление), **Создать** (эта кнопка используется для создания новых правил), **Обновить** и **Правила по умолчанию** (обновление списка правил по умолчанию).

По умолчанию в окне **«Диспетчера уведомлений»** содержится список предопределенных правил. Чтобы активировать правило, установите напротив него флажок. Ниже перечислены доступные правила уведомлений. Если они включены, при соблюдении условий конкретного правила в журнале создается запись.

- **«Нет соединения с более чем 10 % основных клиентов»** — к серверу в течение более одной недели не подключалось более 10 % основных клиентов. Правило выполняется в режиме «как можно скорее».
- **«Более 10 % клиентов с критическим состоянием защиты»** — для более чем 10 % клиентов было выдано предупреждение о критическом состоянии защиты, причем ни один из этих клиентов не подключался к серверу более одной недели. Правило выполняется в режиме «как можно скорее».
- **«Основные клиенты с предупреждением о состоянии защиты»** — есть хотя бы один клиент с предупреждением о состоянии защиты, который не подключался к серверу в течение одной и более недель.
- **«Нет соединения с основными клиентами»** — есть хотя бы один клиент, который не подключался к серверу в течение одной и более недель.
- **«Основные клиенты с устаревшей базой данных сигнатур вирусов»** — есть клиент с базой данных сигнатур вирусов на две или более версий младше, чем текущая, который не отключался от сервера в течение более чем одной недели.
- **«Основные клиенты с критическим состоянием защиты»** — есть клиент с предупреждением о критическом состоянии защиты, который не отключался от сервера в течение более чем одной недели.
- **«На основных клиентах более новая база данных сигнатур вирусов, чем на сервере»** — есть клиент с более новой базой данных сигнатур вирусов, чем на сервере, который при этом не отключался от сервера в течение более чем одной недели.
- **«Основные клиенты, ожидающие перезапуска»** — есть ожидающий перезагрузки клиент, который не отключался от сервера в течение более чем одной недели.
- **«На основных клиентах остались неочищенные после сканирования вирусы»** — есть клиент, который во время сканирования не удалось очистить от не менее одного вируса; клиент при этом не отключался от сервера в течение более чем одной недели.
- **«Выполненная задача»** — на клиенте была завершена задача. Правило выполняется в режиме «как можно скорее».
- **«Новые основные клиенты»** — к серверу подключился новый клиент. Правило выполняется в режиме «как можно скорее».
- **«Новые реплицируемые клиенты»** — в списке клиентов появился новый реплицированный клиент. Правило выполняется через час после события.
- **«Возможно проникновение вируса»** — частота записей в журнале угроз на клиенте превысила 1000 критических предупреждений в час на более чем 10 % всех клиентов.
- **«Возможна сетевая атака»** — частота записей в журнале персонального файервола ESET на клиенте превысила 1000 критических предупреждений в час на более чем 10 % всех клиентов.
- **«Сервер обновлен»** — сервер был обновлен.
- **«Сервер не обновлен»** — сервер не обновлялся в течение пяти дней или более. Правило выполняется в режиме «как можно скорее».
- **«Ошибка в текстовом журнале сервера»** — в журнале сервера есть запись с ошибкой.
- **«Истечение срока действия лицензии»** — срок действия текущей лицензии истекает через 20 дней, после чего максимальное количество слотов для клиентов станет меньше текущего числа клиентов. Правило выполняется в режиме «как можно скорее».
- **«Ограничение лицензии»** — количество свободных слотов клиентов снижается до 10 % от числа всех доступных слотов клиентов.

Если не указано иное, все правила выполняются и повторяются через 24 часа и применяются к основному серверу и основным клиентам.

2. В разделе **«Параметры»** в нижней части окна отображается информация о выбранном в данный момент правиле. Все поля и параметры из этого раздела описаны в демонстрационном правиле в разделе Создание правила 119.

Для каждого правила можно указать критерий, который называется **«Триггером»** и активирует данное правило. Доступны следующие триггеры.

- «Состояние клиента» 113 — правило применяется при возникновении проблем на клиентах.
- «Состояние сервера» 114 — правило применяется при возникновении проблем на серверах.
- «Событие завершенной задачи» 116 — правило запускается после завершения указанной задачи.

- «Новое событие клиента» 116 — правило выполняется при подключении к серверу нового клиента (в том числе реплицированного).
- Событие вспышки 117 — правило выполняется при вспышке инцидентов на определенном количестве клиентов.
- «Событие получения журнала» 118 — правило выполняется, если администратор хочет получать уведомления о журналах через определенные временные интервалы.

В зависимости от типа триггера активируются или деактивируются и другие параметры правил, поэтому при создании новых правил 119 рекомендуется сначала создавать триггеры.

В раскрывающемся меню **«Приоритет»** можно выбрать приоритет правила. **P1** означает самый высокий приоритет, а **P5** — самый низкий. Приоритет никак не влияет на функциональность правил. Для назначения приоритета уведомлениям можно использовать переменную *%PRIORITY%*. Под раскрывающимся меню **«Приоритет»** находится поле **«Описание»**. Рекомендуется давать каждому правилу осмысленное описание, например *«правило, предупреждающее об обнаружении вируса»*.

Формат уведомлений настраивается в поле **«Сообщение»** в нижней части окна диспетчера уведомлений. В тексте можно использовать специальные переменные вида *%ИМЯ_ПЕРЕМЕННОЙ%*. Чтобы просмотреть список доступных переменных, нажмите кнопку **«Показать параметры»**.

- **Rule_Name — имя правила уведомления.**
- **Rule_Description — описание правила уведомления.**
- **Priority** — приоритет правила уведомления (P1 означает самый высокий приоритет).
- **Triggered** — дата последнего отправленного уведомления (без учета повторений).
- **Triggered_Last** — дата последнего отправленного уведомления (с учетом повторений).
- **Client_Filter** — параметры фильтрации клиентов.
- **Client_Filter_Short** — параметры фильтрации клиентов (краткая форма).
- **Client_List** — список клиентов.
- **Parameters** — параметры правила.
- **Primary_Server_Name — имя главного сервера.**
- **Server_Last_Updated** — последнее обновление сервера.
- **Virus_Signature_DB_Version** — последняя версия базы данных сигнатур вирусов.
- **Pcu_List** — последний список всех устройств управления.
- **Pcu_List_New_Eula** — последний список всех устройств управления с новым лицензионным соглашением.
- **Last_Log_Date** — дата последнего журнала.
- **Task_Result_List** — список завершенных задач.
- **Log_Text_Truncated** — текст записи в журнале, которая активировала уведомление (усеченный вид).
- **License_Info_Merged** — информация о лицензии (сводка).
- **License_Info_Full** — информация о лицензии (полностью).
- **License_Days_To_Expiry** — количество дней, оставшихся до истечения срока действия лицензии.
- **License_Expiration_Date** — ближайшая дата срока истечения лицензии.
- **License_Clients_Left** — количество свободных слотов для подключения клиентов к серверу согласно текущей лицензии.
- **Actual_License_Count** — количество клиентов, подключенных к серверу в данный момент.

### 5.4.1 Состояние клиента

Определите параметры фильтрации клиентов в диалоговом окне **«Фильтр клиентов»**. При применении правила учитываются только те клиенты, которые отвечают критериям фильтрации клиентов. Критерии фильтрации.

- **«FROM основного сервера»** — только клиенты с основного сервера; кроме того, можно использовать отрицание этого условия (т. е. «NOT FROM»).
- **«ВКЛЮЧИТЬ основной сервер»** — включить в выходные данные основной сервер.
- **«HAS новый флаг»** — клиенты с флагом *«Новый»* (можно использовать отрицание «HAS NOT»).
- **«Группы ERA IN»** — клиенты, относящиеся к указанной группе.
- **«Домен/рабочая группа IN»** — клиенты, относящиеся к указанному домену.
- **«Маска имени компьютера»** — клиенты с указанным именем компьютера.
- **«HAS маска IPv4»** — клиенты, соответствующие указанной маске IPv4.
- **«HAS диапазон IPv4»** — клиенты, относящиеся к указанному диапазону адресов IPv4.
- **«HAS IPv6 префикс сети»** — клиенты с указанным префиксом сети IPv6.
- **«HAS диапазон IPv6»** — клиенты, с указанным диапазоном адресов IPv6.
- **«HAS определенная политика»** — клиенты с назначенной им указанной политикой (можно использовать отрицание «HAS NOT»).

Указав для правила уведомлений фильтр клиентов, нажмите кнопку **«ОК»** и переходите к параметрам правила. Параметры клиента определяют, какому условию должен отвечать клиент или группа клиентов для запуска действия уведомления. Чтобы просмотреть доступные параметры, нажмите кнопку **«Изменить...»** в разделе **«Параметры»**.

Доступность параметров зависит от выбранного типа триггера. Для триггеров типа «Состояние клиента» доступны следующие параметры.

- **«Состояние защиты: любые предупреждения»** — в элементе «Состояние защиты» обнаружено предупреждение.
- **«Состояние защиты: критические предупреждения»** — в элементе «Состояние защиты» обнаружено критическое предупреждение.
- **«Версия БД сигнатур вирусов»** — проблема с базой данных сигнатур вирусов (этот параметр может принимать 6 значений).

  - **«Предыдущая»** — базы данных сигнатур вирусов на одну версию старше текущей.
  - **«Более старая или н/д»** — базы данных сигнатур вирусов на одну версию старше текущей.
  - **«Устарела на 5 версий или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 5 версий.
  - **«Устарела на 10 версий или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 10 версий.
  - **«Старше 7 дней или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 7 версий.
  - **«Устарела на 14 дней или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 14 дней.

- **«Предупреждение о последнем подключении»** — последнее подключение было установлено до указанного периода времени.
- **«Имеется запись об угрозе»** — в столбце «Угроза» есть предупреждение об угрозе.
- **«Имеется запись о событии»** — в столбце «Последнее событие» есть запись.
- **«Имеется запись о последнем событии файервола»** — в столбце «Событие файервола» есть запись о событии файервола.
- **«HAS новый флаг»** — для клиента установлен флаг «Новый».
- **«Ожидание перезапуска»** — клиент ожидает перезапуска.
- **«При последнем сканировании обнаружена угроза»** — на клиенте при последнем сканировании обнаружены угрозы в указанном количестве.
- **«При последнем сканировании угроза не была устранена»** — на клиенте при последнем сканировании обнаружены неустраненные угрозы в указанном количестве.

Для всех параметров можно использовать отрицание, но не все отрицания имеет смысл использовать. Отрицание имеет смысл только для параметров с двумя логическими значениями: истина и не истина. Например, параметр **«HAS новый флаг»** охватывает только клиенты, отмеченные флагом *«Новый»*. Обратный параметр будет охватывать все клиенты без этого флага.

Все вышеперечисленные условия можно логически комбинировать и инвертировать. Раскрывающееся меню **«Правило применяется, когда»** содержит два пункта:

- **«все параметры совпадают»** — правило применяется в случае, если соблюдены **все** указанные условия;
- **«любой из параметров совпадает»** — правило применяется в случае, если соблюдено хотя бы **одно** условие.

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий нажмите кнопку **«Изменить...»** в разделе «Действия» 118.

Активацию правила можно отложить на период от одного часа до трех месяцев. Если нужно активировать правило как можно скорее, выберите пункт **«Как можно скорее»** в раскрывающемся меню **«Активация после»**. По умолчанию диспетчер уведомлений активируется каждые 10 минут, поэтому если выбрать пункт **«Как можно скорее»**, задача будет запущена в течение 10 минут. Если в меню выбрать конкретный период, действие будет автоматически выполнено по истечении этого времени (в том случае, если будет соблюдено условие правила).

В меню **«Повторять каждые...»** можно выбрать интервал повторения действия. Однако для активации правила все равно должно быть соблюдено его условие. В меню **«Сервер»** > **«Дополнительно»** > **«Изменить дополнительные параметры»** > **ESET Remote Administrator** > **«Сервер** > **«Настройка»** > **«Уведомления»** > **«Интервал обработки уведомлений (мин.)»** можно задать интервал времени, по истечении которого сервер будет проверять и выполнять активные правила.

Значение по умолчанию — 10 минут. Не рекомендуется уменьшать это значение, поскольку это может привести к замедлению работы сервера.

### 5.4.2 Состояние сервера

В окне **«Параметры правил сервера»** можно настроить параметры для вызова правила, связанного с конкретным состоянием сервера, которое затем используется для отправки уведомлений. Чтобы настроить параметр, щелкните переключатель рядом с определенным условием. При этом будут активированы соседние активные элементы интерфейса, чтобы можно было изменить параметры состояния.

- **«Сервер обновлен»** — сервер находится в актуальном состоянии.
- **«Сервер не обновлен»** — сервер не обновлялся дольше, чем предусмотрено значением параметра.
- **«Журнал аудита»** — в **«Журнале аудита»** отслеживаются и регистрируются все изменения в конфигурации и все действия, которые выполняют пользователи ERAC. Можно отфильтровать записи журнала по типу. См. **«Журнал сервера»**.
- **«Журнал сервера»** — ниже перечислены различные виды записей в журнале сервера.

  - **«Ошибки»** — сообщения об ошибках.

  - **«Ошибки и предупреждения»** — сообщения об ошибках и предупреждениях.

  - **«Ошибки, предупреждения и информация»** — сообщения об ошибках, предупреждениях и информационные сообщения.

- **«Фильтровать записи в журнале по типу»** — включив этот параметр, можно указать, какие записи об ошибках и предупреждениях в журнале нужно отслеживать. Обратите внимание на то, что для правильной работы функции уведомлений необходимо установить соответствующий уровень детализации журнала (**«Сервис» > «Параметры сервера» > «Ведение журнала»**). В противном случае для правила уведомления в журнале сервера не обнаружится соответствующий ему триггер. В журнал заносятся следующие записи.

- **ADSI_SYNCHRONIZE** — синхронизация групп Active Directory.
- **CLEANUP** — задачи очистки сервера.
- **CREATEREPORT** — создание отчета по запросу.
- **DEINIT** — завершение работы сервера.
- **INIT** — Запуск сервера.
- **INTERNAL 1** — внутреннее сообщение сервера.
- **INTERNAL 2** — внутреннее сообщение сервера.
- **LICENSE** — управление лицензиями.
- **MAINTENANCE** — задачи обслуживания сервера.
- **NOTIFICATION** — управление уведомлениями.
- **PUSHINST** — автоматическая установка.
- **RENAME** — переименование внутренней структуры.
- **REPLICATION** — репликация сервера.
- **POLICY** — управление политиками.
- **POLICYRULES** — правила политик.
- **SCHEDREPORT** — автоматически созданные отчеты.
- **SERVERMGR**— управление внутренними потоками сервера.
- **SESSION** — сетевые подключения сервера.
- **SESSION_USERACTION** — различные действия пользователя.
- **THREATSENSE** — отправка статистической информации ESET Live Grid.
- **UPDATER** — обновление сервера и создание зеркала.

К примеру, параметр UPDATER предписывает отправлять уведомления, когда диспетчер уведомлений находит в журнале сервера проблему, связанную с обновлением и созданием зеркала.

- **«Истечение срока действия лицензии»** — срок действия лицензии истекает через указанное число дней либо уже истек. Выберите параметр **«Предупреждать, только если это приведет к падению числа клиентов в лицензии ниже фактического числа клиентов на сервере базы данных»**, чтобы отправлять уведомления только в случае, если истечение срока действия лицензии приведет к падению разрешенного количества клиентов ниже числа клиентов, подключенных в данный момент.

- **«Ограничить лицензию»** — процентная доля свободных слотов клиентов опускается ниже указанного значения.

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий нажмите кнопку **«Изменить...»** в разделе «Действия» 118.

Активацию правила можно отложить на период от одного часа до трех месяцев. Если нужно активировать правило как можно скорее, выберите пункт **«Как можно скорее»** в раскрывающемся меню **«Активация после»**. По умолчанию диспетчер уведомлений активируется каждые 10 минут, поэтому если выбрать пункт **«Как можно скорее»**, задача будет запущена в течение 10 минут. Если в меню выбрать конкретный период, действие будет автоматически выполнено по истечении этого времени (в том случае, если будет соблюдено условие правила).

В меню **«Повторять каждые...»** можно выбрать интервал повторения действия. Однако для активации правила все равно должно быть соблюдено его условие. В меню **«Сервер»** > **«Дополнительно»** > **«Изменить дополнительные параметры»** > **ESET Remote Administrator** > **«Сервер** > **«Настройка»** > **«Уведомления»** > **«Интервал обработки уведомлений (мин.)»** можно задать интервал времени, по истечении которого сервер будет проверять и выполнять активные правила.

Значение по умолчанию — 10 минут. Не рекомендуется уменьшать это значение, поскольку это может привести к замедлению работы сервера.

### 5.4.3 Событие «Задача завершена»

Правило будет запущено после выполнения выбранных задач. В параметрах **По умолчанию** выбираются все типы задач 88.

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий нажмите кнопку **«Изменить...»** в разделе «Действия» 118.

Активацию правила можно отложить на период от одного часа до трех месяцев. Если нужно активировать правило как можно скорее, выберите в раскрывающемся меню **«Активация после»** пункт «Как можно скорее». По умолчанию диспетчер уведомлений активируется каждые 10 минут, поэтому если выбрать пункт **«Как можно скорее»**, задача будет запущена в течение 10 минут. Если в меню выбрать конкретный период, действие будет автоматически выполнено по истечении этого времени (в том случае, если будет соблюдено условие правила).

### 5.4.4 Событие «Новый клиент»

Определите новые параметры фильтрации клиентов в диалоговом окне **«Фильтр клиентов»**. При применении правила учитываются только те клиенты, которые отвечают критериям фильтрации клиентов. Критерии фильтрации.

- **«FROM основного сервера»** — только клиенты с основного сервера; кроме того, можно использовать отрицание этого условия (т. е. «NOT FROM»).
- **«ВКЛЮЧИТЬ основной сервер»** — включить в выходные данные основной сервер.
- **«HAS новый флаг»** — клиенты с флагом *«Новый»* (можно использовать отрицание «HAS NOT»).
- **«Группы ERA IN»** — клиенты, относящиеся к указанной группе.
- **«Домен/рабочая группа IN»** — клиенты, относящиеся к указанному домену.
- **«Маска имени компьютера»** — клиенты с указанным именем компьютера.
- **«HAS маска IPv4»** — клиенты, соответствующие указанной маске IPv4.
- **«HAS диапазон IPv4»** — клиенты, относящиеся к указанному диапазону адресов IPv4.
- **«HAS IPv6 префикс сети»** — клиенты с указанным префиксом сети IPv6.
- **«HAS диапазон IPv6»** — клиенты с указанным диапазоном адресов IPv6.
- **«HAS определенная политика»** — клиенты с назначенной им указанной политикой (можно использовать отрицание «HAS NOT»).

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий нажмите кнопку **«Изменить...»** в разделе «Действия» 118.

Активацию правила можно отложить на период от одного часа до трех месяцев. Если нужно активировать правило как можно скорее, выберите пункт **«Как можно скорее»** в раскрывающемся меню **«Активация после»**. По умолчанию диспетчер уведомлений активируется каждые 10 минут, поэтому если выбрать пункт **«Как можно скорее»**, задача будет запущена в течение 10 минут. Если в меню выбрать конкретный период, действие будет автоматически выполнено по истечении этого времени (в том случае, если будет соблюдено условие правила).

### 5.4.5 Событие вспышки

Это уведомление запускается, как только соблюдаются определенные условия для вспышки инцидентов, оно не сообщает о каждом отдельном инциденте или об инцидентах, возникающих после выполнения таких условий.

Параметры фильтрации события вспышки можно настроить в окне **«Фильтр клиентов»**. При применении правила учитываются только те клиенты, которые отвечают критериям фильтрации клиентов. Критерии фильтрации.

- **«FROM основного сервера»** — только клиенты с основного сервера; кроме того, можно использовать отрицание этого условия (т. е. «NOT FROM»).
- **«ВКЛЮЧИТЬ основной сервер»** — включить в выходные данные основной сервер.
- **«HAS новый флаг»** — клиенты с флагом *«Новый»* (можно использовать отрицание «HAS NOT»).
- **«Группы ERA IN»** — клиенты, относящиеся к указанной группе.
- **«Домен/рабочая группа IN»** — клиенты, относящиеся к указанному домену.
- **«Маска имени компьютера»** — клиенты с указанным именем компьютера.
- **«HAS маска IPv4»** — клиенты, соответствующие указанной маске IPv4.
- **«HAS диапазон IPv4»** — клиенты, относящиеся к указанному диапазону адресов IPv4.
- **«HAS IPv6 префикс сети»** — клиенты с указанным префиксом сети IPv6.
- **«HAS диапазон IPv6»** — клиенты с указанным диапазоном адресов IPv6.
- **«HAS определенная политика»** — клиенты с назначенной им указанной политикой (можно использовать отрицание «HAS NOT»).

Указав для правила уведомлений фильтр клиентов, нажмите кнопку **«ОК»** и переходите к параметрам правила. Параметры клиента определяют, какому условию должен отвечать клиент или группа клиентов для запуска действия уведомления. Чтобы просмотреть доступные параметры, нажмите кнопку **«Изменить...»** в разделе **«Параметры»**.

- **«Тип журнала»** — выберите тип журнала, который вы хотите отслеживать.
- **«Уровень детализации журнала»** — уровень детализации записей в выбранном журнале.
  **«Уровень 1 — критические предупреждения»** — только критические ошибки.
  **«Уровень 2 — То же + предупреждения»** — то же, что и уровень 1, плюс предупреждения.
  **«Уровень 3 — То же + норма»** — то же, что и уровень 2, плюс информационные сообщения.
  **«Уровень 4 — То же + диагностика»** — то же, что и уровень 3, плюс сообщения диагностики.
- **«1000 событий за 60 минут»**: введите количество событий и выберите период времени, чтобы установить частоту событий, необходимую для отправки уведомления. По умолчанию частота составляет 1000 событий в час.
- **«Количество»** — количество клиентов (абсолютное или в процентах).

**«Интервал регулирования»** — это временной интервал для отправки уведомлений. Например, если интервал регулирования установлен на 1 час, данные собираются в фоновом режиме, и вы получаете уведомления каждый час (если вспышка еще существует и триггер еще активен).

### 5.4.6 Событие получения журнала

Используйте этот параметр, если хотите получать уведомление о каждом журнале в определенное время.

Определите параметры фильтрации клиентов в диалоговом окне **«Фильтр клиентов»**. При применении правила учитываются только те клиенты, которые отвечают критериям фильтрации клиентов. Критерии фильтрации.

- **«FROM основного сервера»** — только клиенты с основного сервера; кроме того, можно использовать отрицание этого условия (т. е. «NOT FROM»).
- **«ВКЛЮЧИТЬ основной сервер»** — включить в выходные данные основной сервер.
- **«HAS новый флаг»** — клиенты с флагом *«Новый»* (можно использовать отрицание «HAS NOT»).
- **«Группы ERA IN»** — клиенты, относящиеся к указанной группе.
- **«Домен/рабочая группа IN»** — клиенты, относящиеся к указанному домену.
- **«Маска имени компьютера»** — клиенты с указанным именем компьютера.
- **«HAS маска IPv4»** — клиенты, соответствующие указанной маске IPv4.
- **«HAS диапазон IPv4»** — клиенты, относящиеся к указанному диапазону адресов IPv4.
- **«HAS IPv6 префикс сети»** — клиенты с указанным префиксом сети IPv6.
- **«HAS диапазон IPv6»** — клиенты с указанным диапазоном адресов IPv6.
- **«HAS определенная политика»** — клиенты с назначенной им указанной политикой (можно использовать отрицание «HAS NOT»).

Указав для правила уведомлений фильтр клиентов, нажмите кнопку **«ОК»** и переходите к параметрам правила. Параметры клиента определяют, какому условию должен отвечать клиент или группа клиентов для запуска действия уведомления. Чтобы просмотреть доступные параметры, нажмите кнопку **«Изменить...»** в разделе **«Параметры»**.

- **«Тип журнала»** — выберите тип журнала, который вы хотите отслеживать.
- **«Уровень детализации журнала»** — уровень детализации записей в выбранном журнале.
  **«Уровень 1 — критические предупреждения»** — только критические ошибки.
  **«Уровень 2 — То же + предупреждения»** — то же, что и уровень 1, плюс предупреждения.
  **«Уровень 3 — То же + норма»** — то же, что и уровень 2, плюс информационные сообщения.
  **«Уровень 4 — То же + диагностика»** — то же, что и уровень 3, плюс сообщения диагностики.

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий нажмите кнопку **«Изменить...»** в разделе «Действия» 118.

**«Интервал регулирования»** — это временной интервал для отправки уведомлений. Например, если интервал регулирования установлен на 1 час, данные собираются в фоном режиме и вы получаете уведомления каждый час (если триггер еще активен).

### 5.4.7 Действие

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий предназначена кнопка **«Изменить»** в разделе **«Действия»**. Ниже описаны варианты, доступные в редакторе действий.

- **«Электронная почта»** — отправка текста уведомления для данного правила на указанный адрес электронной почты; в поле **«Тема»** можно указать тему сообщения. Кнопка **«Кому»** открывает адресную книгу.
- **«SNMP-ловушка»** — создание и отправка SNMP-уведомления.
- **«Выполнить на сервере»** — выбрав этот вариант, укажите приложение для запуска на сервере. Введите полный путь к приложению.

- **«Записывать в файл»** — в указанном файле журнала создаются записи. Введите полный путь к приложению; необходимо настроить **степень детализации**.
- **«Записывать в системный журнал»** — включает запись уведомлений в журнал сервера; также можно настроить **степень детализации**уведомлений.
- **«Ведение журнала»** — включение записи уведомлений в журнал сервера; также можно настроить **степень детализации** уведомлений.
- **«Запустить отчет»** — после выбора этого параметра раскрывающееся меню **«Имя шаблона»** становится активным. Выберите шаблона для отчета. Дополнительную информацию о шаблонах см. в разделе Отчеты 44.

Для правильной работы этой функции необходимо включить ведение журнала на сервере ERA Server (**«Служебные программы»** > **«Настройки сервера»** > **«Ведение журнала»**).

### 5.4.8 Уведомления с использованием SNMP-ловушки

Протокол SNMP (простой протокол управления сетью) — это простой и широко распространенный протокол управления, предназначенный для отслеживания и идентификации сетевых проблем. Одним из действий этого протокола является «Ловушка», отправляющая отправляются определенные данные. В ERA функция «Ловушка» используется для отправки уведомлений для SNMP.

Уведомления можно просматривать в диспетчере протокола SNMP, подключенному к серверу SNMP, на который импортирован файл конфигурации *eset_ras.mib*. Этот файл является стандартным компонентом установочного пакета ERA и обычно находится в папке *C:\Program Files\ESET\ESET Remote Administrator\Server*.

**ПРИМЕЧАНИЕ.** Чтобы оповещения заработали, в ОС Windows, в которой размещен сервер ERA Server, должны работать как служба SNMP, так и служба SNMP-ловушки. Кроме того, вам понадобится программное обеспечение, которое может считывать и отображать сведения SNMP-ловушки.

**Для Windows 2000**

Для эффективной работы функции «Ловушка» необходимо надлежащим образом установить и настроить протокол SNMP на компьютере с сервером ERAS (**«Пуск»** > **«Панель управления»** > **«Установка и удаление программ»** > **«Установка и удаление компонентов Windows»**). Службу SNMP необходимо настроить так, как описано в статье по адресу http://support.microsoft.com/kb/315154. На сервере ERAS необходимо активировать правило уведомлений протокола SNMP.

### 5.4.9 Пример создания правила

В следующих пунктах показано создание правила для отправки администратору уведомлений по электронной почте в случае возникновения проблем с состоянием защиты на какой-либо клиентской рабочей станции. Это уведомление также сохраняется в файл *log.txt*.

1) В раскрывающемся меню **«Тип триггера»** выберите пункт **«Состояние клиента»**.
2) Оставьте для параметров **«Приоритет, Активация через»** и **«Повторять через»** имеющиеся значения. Правилу будет автоматически назначен приоритет 3, и оно будет активировано через 24 часа.
3) В поле **«Описание»** введите **уведомление о состоянии защиты для клиентов головного офиса**.
4) В разделе **«Фильтр клиентов»** выберите команду **«Изменить…»** и активируйте только условие **«Группы ERA B»**. В нижней части окна щелкните ссылку **«указать»** и введите *Центральный офис* в новом окне. Нажмите кнопку **«Добавить»** и дважды нажмите **ОК** для подтверждения. Это означает, что правило применяется только к клиентам, входящим в группу головного офиса.
5) В меню **«Параметры» > «Изменить…»** укажите другие параметры для правила. Снимите все флажки кроме **«Состояние защиты: любые предупреждения»**.
6) Перейдите в раздел **«Действие** и нажмите кнопку **«Изменить…»**. В окне **«Действие»** выберите параметр **«Электронная почта»**, укажите получателя (поле **«Кому…»**) и **тему** письма. Затем установите флажок **«Журнал в файл»** и введите имя и путь к создаваемому журналу. Дополнительно для файла журнала можно

указать уровень **детализации**. Для сохранения действия нажмите кнопку **ОК**.

7) В поле **«Сообщение»** введите текст сообщения, отправляемого при срабатывании данного правила. Пример *«Клиент %CLIENT_LIST% сообщает о проблеме с состоянием защиты»*.

8) Нажмите кнопку **«Сохранить как…»**, укажите имя правила (например, *«проблемы с состоянием защиты»*) и выберите правило в списке правил уведомлений.

Теперь правило активно. Оно применяется при обнаружении проблемы с защитой на клиенте из группы головного офиса. Администратор получит уведомление по электронной почте с вложением, содержащим название проблемного клиента. Нажмите кнопку **«Закрыть»**, чтобы выйти из диспетчера уведомлений.

## 5.5 Подробные сведения о клиентах

Приложение ERA позволяет получать сведения о выполняемых процессах и программах, запущенных на клиентских рабочих станциях. Эти сведения можно получать с помощью средства ESET SysInspector, которое встроено в сервер ERAS. Помимо других своих полезных функций, средство ESET SysInspector тщательно анализирует операционную систему и создает системные журналы. Чтобы открыть эту программу, выберите команду **«Служебные программы»** > **ESET SysInspector** в главном меню ERAC.
Если на определенном клиенте есть проблемы, можно запросить журнал ESET SysInspector с данного клиента. Для этого щелкните правой кнопкой мыши область **«Клиенты»** и выберите **«Запросить данные»** — **«Запрос данных SysInspector»**. Журналы можно получать только с продуктов поколения 4.x; более ранние версии не поддерживают эту функцию. Откроется окно со следующими параметрами:

- **«Создать снимок (с записью результатов в журнал на клиенте)»** — копия журнала сохраняется на клиентском компьютере.
- **«Включить сравнение в последний снимок до указанного времени»** — отображается журнал сравнения. Журналы сравнения создаются путем слияния текущего журнала с доступным предыдущим журналом. Приложение ERA выберет первый из журналов, созданных до указанной даты.

Нажмите кнопку **ОК**, чтобы получить выбранные журналы и сохранить их на сервере. Чтобы открыть и просмотреть журналы, выполните указанные ниже действия.

Параметры ESET SysInspector для отдельных клиентских рабочих станций находятся на вкладке **«Свойства клиента»** — **SysInspector**. Это окно разделено на три области; в верхней области отображается список последних журналов данного клиента. Чтобы загрузить последние сведения, нажмите кнопку **«Обновить»**.

Средний раздел окна **«Запрос параметров»** практически идентичен окну, появляющемуся при запросе требуемых журналов на клиентских рабочих станциях. Кнопка **Запрос** предназначена для получения с клиента журнала ESET SysInspector.

В нижней части окна есть следующие три кнопки.

- **«Вид»** — открытие журнала, указанного в верхнем разделе, в ESET SysInspector.
- **«Сохранить как…»** — сохранение текущего журнала в файл. Если включен параметр **«С последующим просмотром файла в приложении ESET SysInspector»** содержимое журнала автоматически отобразится после его сохранения (как при нажатии кнопки **«Вид»**).

Создание и просмотр новых журналов иногда может замедляться локальным клиентом из-за размера журнала и скорости передачи данных. Дата и время, назначенные журналу в разделе **«Свойства клиента»** > **SysInspector** отображают дату и время доставки на сервер.

## 5.6 Мастер объединения правил файервола

Мастер объединения правил файервола позволяет объединять правила для выбранных клиентов. Это особенно полезно, если необходимо создать единую конфигурацию со всеми правилами файервола, которые были собраны клиентами в режиме обучения. Полученную конфигурацию затем модно отправить клиентам посредством задачи конфигурации или применить как политику.

Мастер доступен в раскрывающемся меню **«Служебные программы»** и в контекстном меню на вкладке **«Клиенты»**, если щелкнуть правой кнопкой мыши выбранного клиента (выбранные клиенты затем автоматически добавляются в список выбранных элементов первого этапа).

**Примечание.** Для успешного выполнения этой операции для всех выбранных клиентов необходимо сохранить (отправить или реплицировать) последние конфигурации на сервере. Сначала необходимо выбрать клиенты или группу клиентов, из которых будут собираться правила файервола для объединения. На следующем этапе будет показан список выбранных клиентов и их состояния конфигурации. Если конфигурация клиента отсутствует на сервере, запросите ее с помощью кнопки **«Запрос»**. На последнем этапе можно выбрать объединенные правила для использования в конфигурации и сохранить их в *XML*-файл.

# 6. Параметры сервера ERA

Сервер ERA Server легко настраивается непосредственно из консоли ERA Console, подключенной к серверу ERA Server с помощью меню **«Сервис»** > **«Параметры сервера...»**.

## 6.1 Общее

На вкладке **«Общие»** отображается основная информация о сервере ERA Server.

- **«Сведения о сервере»** — в этом разделе отображается основная информация о сервере ERA. Нажмите кнопку «Изменить пароль...», чтобы открыть вкладку Безопасность 123 в параметрах сервера ERA.
- **Информация о лицензии** — отображается количество приобретенных клиентских лицензий на продукты безопасности ESET и текущая версия антивирусной системы NOD32 или системы ESET Endpoint Security на сервере. Если срок действия лицензии истек, и была получена новая лицензия, нажмите кнопку «Диспетчер лицензий» 122, чтобы открыть диалоговое окно, в котором можно указать путь к новой лицензии для активации ERA.
- **«Версия БД сигнатур вирусов»** — отображает текущую версию БД сигнатур вирусов (на основании предоставленной информации об обновлениях и используемых продуктов безопасности).
- **«Быстродействие»** — отображает подключение «сервер-клиент» и общую информацию о быстродействии.

### 6.1.1 Управление лицензиями

Для нормальной работы ERA необходимо загрузить на сервер ключ лицензии. При покупке вместе с ключами лицензий на адрес электронной почты отправляется имя пользователя и пароль. Для управления лицензий предназначен **Диспетчер лицензий**.

В ERA версии 3.x и старше была добавлена поддержка нескольких ключей лицензий. Благодаря этой функции управлять ключами стало гораздо удобнее.

Главное окно диспетчера лицензий вызывается с помощью команды **«Служебные программы»** > **«Диспетчер лицензий»**.

Для добавления нового ключа лицензии выполните указанные ниже действия.

1) Выберите команду **«Служебные программы»** > **«Диспетчер лицензий»** или нажмите сочетание клавиши **CTRL+L**.
2) Нажмите кнопку **«Обзор»** и найдите нужны файл ключа лицензии (это файлы с расширением *LIC*).
3) Нажмите кнопку **«Открыть»**, чтобы подтвердить выбор.
4) Проверьте правильность лицензионного ключа и нажмите кнопку **«Загрузить на сервер»**.
5) Нажмите кнопку **«ОК»** для подтверждения.

Кнопка **«Загрузить на сервер»** станет активна только после выбора файла лицензии с помощью кнопки **«Обзор»**. В этой части окна отображаются сведения о ключе лицензии. Это позволяет еще раз проверить данные, прежде чем копировать ключ на сервер.

В центральной части окна отображается информация о ключе лицензии, который сейчас используется на сервере. Для просмотра подробных сведений о доступных на сервере ключах лицензии нажмите кнопку **«Детали...»**.

Сервер ERAS может выбрать из нескольких ключей лицензии самый подходящий и объединить несколько ключей в один. Если загружено несколько ключей лицензии, сервер ERAS будет всегда искать ключ с наибольшим числом клиентов и самой поздней датой истечения срока действия.

Функция объединения нескольких ключей работает только в том случае, если эти ключи принадлежат одному пользователю. Объединение лицензий — это простой процесс, при котором создается новый ключ с количеством клиентов, равным общему числу клиентов на всех объединяемых серверах. Дата истечения

срока действия нового ключа лицензии берется из ключа, срок действия которого истекает первым.

В нижней части окна диспетчера лицензий отображаются уведомления о проблемах с лицензиями. Доступны перечисленные ниже варианты.

- **«Предупредить, если срок действия лицензии сервера истекает через 20 дней»** — за X дней до истечения срока действия лицензии выводится предупреждение.
- **«Предупреждать, только если это приведет к падению числа клиентов в лицензии ниже фактического числа клиентов на сервере базы данных»** — этот вариант предписывает выводить предупреждение только в случае, если истечение срока действия лицензии или ее части приведет к падению числа клиентов ниже числа подключенных в данный момент клиентов или клиентов в базе данных сервера ERAS.
- **«Предупреждать, если в лицензии сервера осталось только 10% свободных клиентов»** — сервер выведет предупреждение в случае, если число свободных клиентов упадет ниже указанного значения (в процентах).

Сервер ERAS может объединить несколько ключей разных владельцев. Эта функция активируется с помощью специального ключа. Для получения такого ключа необходимо отметить это в заказе или связаться с местным распространителем компании ESET.

## 6.2 Безопасность

Продукты безопасности ESET версии 3.x (ESET Endpoint Security и т. п.) поддерживают защиту паролей для зашифрованного обмена данными между клиентом и сервером ERAS (связь по протоколу TCP через порт 2222). В более старых версиях (2.x) эта функциональная возможность отсутствует. Для обратной совместимости со старыми версиями должен быть активирован режим **Включить доступ без аутентификации для клиентов**. На вкладке **Безопасность** представлены параметры, позволяющие администратору использовать версии 2.x и 3.x в одной сети.

Защита соединения с сервером ERA Server.

**Примечание.** Если аутентификация включена на сервере ERAS и на всех клиентах поколения 3.x, параметр **«Включить доступ без аутентификации для клиентов»** можно отключить.

**Параметры безопасности консоли**

- **Использовать аутентификацию Windows или домена** — разрешает аутентификацию Windows или домена и позволяет задать группы администраторов (с полным доступом к серверу ERA Server), а также группы с доступом только для чтения (выберите параметр **Для всех остальных пользователей доступ только для чтения**). Если установлен этот флажок, параметр **Разрешить доступ только для чтения пользователям Windows/домена, которые не являются назначенными пользователями сервера ERA** становится активным, и его можно выбрать. Этот параметр защищает ERAC от изменений со стороны таких пользователей. Если вы хотите назначить пользователей сервера ERA, щелкните элемент **Диспетчер пользователей**.
- Доступом пользователей к консоли можно управлять в служебной программе Диспетчер пользователей 124.

**Параметры безопасности сервера**

- **Пароль для клиентов** — устанавливает пароль для доступа клиентов к серверу ERAS.
- **«Пароль для репликации»** —устанавливает пароль для ERA Server нижнего уровня для репликации на данный сервер ERAS.
- **Пароль для удаленного установщика ESET (агент)** — устанавливает пароль для доступа агента программы установки к серверу ERAS (в том числе и для удаленных установок).
- **Включить доступ без аутентификации для клиентов (продукты ESET для обеспечения безопасности)** — разрешает доступ к серверу ERAS для клиентов с отсутствующим или недействительным паролем (если текущий пароль отличается от пароля в поле **Пароль для клиентов**).
- **Включить доступ без аутентификации для репликации** — разрешает доступ к серверу ERAS для клиентов серверов ERA Server нижнего уровня, у которых отсутствует или недействителен пароль для репликации.

- **Включить доступ без аутентификации для удаленного установщика ESET (агент)** — разрешает доступ к серверу ERAS удаленному установщику ESET, для которого не задан действительный пароль.

**ПРИМЕЧАНИЕ.**: **По умолчанию** — позволяет только восстановить предустановленные настройки (отличается от процедуры сброса паролей).

**ПРИМЕЧАНИЕ.**: Если вы хотите повысить уровень безопасности, можно использовать сложные пароли. Перейдите на вкладку **«Сервис»** > **«Редактор конфигурации ESET»** > **«Удаленное администрирование»** > **«Сервер ERA»** > **«Настройки»** > **«Безопасность»** > **«Требуется сложный пароль»** и установите для этого параметра значение **«Да»**. Если этот параметр включен, все новые пароли должны содержать не менее 8 символов, в том числе букву в верхнем и нижнем регистре, а также небуквенный символ.

### 6.2.1 Диспетчер пользователей

Инструменты **Диспетчера пользователей** позволяют управлять учетными записями пользователей для аутентификации Консоль-Сервер. Учетные записи «Администратор» (полный доступ) и «Только чтение» являются стандартными.

Нажмите кнопку **Создать**, чтобы добавить новую учетную запись пользователя для аутентификации Консоль-Сервер. Укажите **Имя пользователя**, **Пароль** и конкретные **Разрешения**.

В поле **Описание** можно ввести необязательное описание пользователя.

В поле **Разрешения** укажите уровень доступа для пользователя и задачи, которые он может выполнять. Можно изменить Пароль доступа к консоли 124 для каждого пользователя, который заходит в консоль. Для этого выберите конкретного пользователя и нажмите кнопку **Изменить...** возле параметра **Пароль для аутентификации консоли**.

**ПРИМЕЧАНИЕ.**: Разрешения стандартных учетных записей (Администратор и Только чтение) изменить нельзя.

К выбранному пользователю сервера ERA можно добавить одну или несколько **Групп аутентификации Windows или домена**. Если группа Windows/домен назначена нескольким пользователям, она будет применена к первому пользователю из списка. Стрелки вверх и вниз возле списка пользователей определяют порядок расположения пользователей.

### 6.2.2 Пароль доступа к консоли

Чтобы изменить пароль доступа к консоли, выберите **«Файл»** > **«Изменить пароль»** или измените пароль с помощью диспетчера пользователей 124. Введите старый пароль, затем дважды введите новый (для подтверждения). Если установить флажок возле параметра **«Также изменить пароль в кэше»**, пароль в кэше, который использовался при запуске приложения (чтобы пользователю не нужно было каждый раз вводить пароль для доступа к ERAC), будет изменен.

**ПРИМЕЧАНИЕ.** Пароли, установленные в данном диалоговом окне, отправляются непосредственно на сервер. Это означает, что сразу же после нажатия кнопки **«ОК»** изменение вступает в силу и не может быть отменено.

## 6.3 Обслуживание сервера

Если на вкладке **«Обслуживание сервера»** настроены нужные параметры, база данных ERA Server будет автоматически обслуживаться и оптимизироваться. Можно задать следующие параметры очистки.

- **«Параметры сбора журналов...»** — определяет уровень журналов, получаемых сервером.
- **«Параметры очистки...»** — удаляет журналы по времени.
- **«Дополнительные параметры очистки...»** — удаляет журналы по количество записей.

Укажите, сколько записей журнала должно остаться после очистки, а также уровень журналов, получаемых сервером. Например, если выбрано **«Удалять содержимое журналов угроз, кроме последних 600 000 записей»** в Расширенных параметрах очистки по числу записей в журнале 126 и уровень Параметров сбора журналов 125 для **«Угроз»** определен как **«Уровень 3 —То же + нормальный»**, последние 600 000 записей, которые содержат информацию о критических ошибках, предупреждения и информационные сообщения,

будут сохранены в базе данных. Также можно ограничить количество записей журнала с помощью параметра Очистка по времени 125.

**«Планировщик очистки»** — работает с учетом всех выбранных выше параметров через определенный интервал времени. Нажмите кнопку **«Изменить...»** возле этого параметра, чтобы установить параметры времени. Нажмите кнопку **«Очистить»**, чтобы немедленно начать очистку.

**«Планировщик сжатия и восстановления» —** сжимает базу данных с указанным интервалом в заданное время. При сжатии и восстановлении удаляются несогласованности и ошибки, что ускоряет обмен данными с базой данных. Нажмите кнопку **«Изменить...»** возле этого параметра, чтобы установить параметры времени. Нажмите кнопку **«Сжать сейчас»**, чтобы немедленно начать сжатие и восстановление.

**ПРИМЕЧАНИЕ.** Служебные программы **«Очистка»** и **«Сжатие и восстановление»** требуют много времени и ресурсов, поэтому рекомендуется планировать их работу на время минимальной нагрузки на сервер (например, чистку на ночь, а сжатие и восстановление на выходные).

По умолчанию записи и журналы старше трех/шести месяцев удаляются, а каждые пятнадцать дней выполняется задача **«Сжатие и восстановление»**.

### 6.3.1 Параметры сбора журналов

Определите уровень журналов, отправляемых на сервер. Выберите степень детализации для каждого типа журнала, используя соответствующие раскрывающиеся меню.

**Нет**: журналы не будут отправлены на сервер. Клиент ничего не регистрирует при помощи этого параметра, поэтому сервер ERA не будет получать журналы.

**«Уровень 1 — критические предупреждения»** — только критические ошибки. Критические ошибки не регистрируются на вкладках **Контроль доступа в Интернет** или **Контроль устройств**, потому что клиент не может создавать такие журналы.

**Уровень 2 — вышеперечисленное + предупреждения**: то же, что и уровень 1, плюс предупреждения.

**Уровень 3 — вышеперечисленное + обычное**: то же, что и уровень 2, плюс информационные сообщения. Эта степень детализации называется **Информационная**, а не **Обычная** на стороне клиента.

**Уровень 4 — вышеперечисленное + диагностика**: то же, что и уровень 3, плюс сообщения диагностики. Данную степень детализации также необходимо задать и на стороне клиента. Параметр по умолчанию клиента — **Информационная** степень ведения журнала.

**«Все»** — будет осуществляться получение всех журналов.

### 6.3.2 Очистка по времени

Основные параметры очистки по времени.

- **«Удалять клиенты, не подключавшиеся в течение последних X месяцев (дней)»** — удаляет клиенты, которые не подключались к ERAS больше указанного количества месяцев (или дней).
- **«Удалять журналы угроз старше X месяцев (дней)»** — удаляет все инциденты с вирусами (обнаруженные угрозы) старше указанного числа месяцев (дней).
- **«Удалять журналы файервола старше X месяцев (дней)»** — удаляет все журналы файервола старше указанного числа месяцев (дней).
- **«Удалять журналы событий старше X месяцев (дней)»** — удаляет все журналы событий старше указанного числа месяцев (дней).
- **«Удалять журналы системы предотвращения вторжений на узел старше X месяцев (дней)»** — удаляет все журналы системы предотвращения вторжений на узел старше указанного числа месяцев (дней).
- **«Удалять журналы контроля устройств старше X месяцев (дней)»** — удаляет все журналы контроля устройств старше указанного числа месяцев (дней).

- **«Удалять журналы контроля доступа в Интернет старше X месяцев (дней)»** — удаляет все журналы контроля доступа в Интернет старше указанного числа месяцев (дней).
- **«Удалять журналы защиты от спама старше X месяцев (дней)»** — удаляет все журналы защиты от спама старше указанного числа месяцев (дней).
- **«Удалять журналы занесения в "серый" список старше X месяцев (дней)»** — удаляет все журналы занесения в "серый" список старше указанного числа месяцев (дней).
- **«Удалять журналы проверки старше X месяцев (дней)»** — удаляет все журналы проверки старше указанного числа месяцев (дней).
- **«Удалять мобильные журналы старше X месяцев (дней)»** — удаляет все мобильные журналы старше указанного числа месяцев (дней).
- **«Удалять записи в карантине без клиентов старше X месяцев (дней)»**— удаляет все записи в карантине, которые не присвоены ни одному из клиентов и которые старше указанного числа месяцев (или дней).
- **«Удалять записи незарегистрированных компьютеров старше X месяцев (дней)»** — удаляет записи незарегистрированных компьютеров (компьютеры, которые не управляются ERA) старше указанного числа месяцев (или дней).
- **«Удалять записи выполненных задач старше X месяцев (дней)** — удаляет все записи выполненных задач старше указанного числа месяцев (или дней).
- **«Удалять записи задач старше X месяцев (дней)** — удаляет все записи задач старше указанного числа месяцев (или дней).

### 6.3.3 Расширенные параметры очистки по числу записей в журнале

Расширенные параметры очистки по числу записей в журнале.

- **«Удалить журналы угроз, кроме последних X записей»** — удаление всех инцидентов с вирусами (обнаруженных угроз), кроме указанного количества записей.
- **«Удалить журналы файервола, кроме последних X записей»** — удаление всех журналов файервола, кроме указанного количества записей.
- **«Удалить журналы событий, кроме последних X записей»** — удаление всех журналов событий, кроме указанного количества записей.
- **«Удалить журналы системы предотвращения вторжений на узел, кроме последних X записей»** — удаление всех журналов системы предотвращения вторжений на узел, кроме указанного количества записей.
- **«Удалить журналы контроля устройств, кроме последних X записей»** — удаление всех журналов контроля устройств, кроме указанного количества записей.
- **«Удалить журналы контроля доступа в Интернет, кроме последних X записей»** — удаление всех журналов контроля доступа в Интернет, кроме указанного количества записей.
- **«Удалить журналы защиты от спама, кроме последних X записей»** — удаление всех журналов защиты от спама, кроме указанного количества записей.
- **«Удалить журналы занесения в "серый" список, кроме последних X записей»** — удаление всех журналов занесения в "серый" список, кроме указанного количества записей.
- **«Удалить журналы сканирования, кроме последних X записей»** — удаление всех журналов сканирования, кроме указанного количества записей.
- **«Удалить мобильные журналы, кроме последних X записей»** — удаление всех мобильных журналов, кроме указанного количества записей.

## 6.4 Ведение журнала

Чтобы настроить параметры обслуживания базы данных, выберите в главном меню консоли ERA Console пункт **«Служебные программы» > «Настройки сервера»**.
При обслуживании базы данных доступны различные параметры, позволяющие обеспечивать прозрачность журналов, а также выполнять регулярное сжатие главной базы данных ERA с целью экономии пространства.

**1. Журнал аудита**

В «Журнале аудита» отслеживаются и регистрируются все изменения в конфигурации и все действия, которые выполняют пользователи ERAC.

- Если выбран параметр **«Записывать в текстовый файл»**, новые файлы журнала будут создаваться (**«Ротация, если более X МБ»**) и удаляться (**«Удалять журналы с ротацией старше X дн.»**) ежедневно. Также можно изменить степень детализации журнала в раскрывающемся меню слева.

Щелкните ссылку Просмотр журнала, чтобы просмотреть текущий журнал аудита.

- Параметр **«Записывать в журнал приложений ОС»** разрешает копирование информации в журнал системных событий (**«Панель управления Windows»** > **«Администрирование»** > **«Просмотр событий»**). Также можно изменить степень детализации журнала в раскрывающемся меню слева.

- Параметр **«Записывать в системный журнал»** отправляет сообщение системного журнала на указанный порт указанного сервера системного журнала (сервером по умолчанию является localhost, портом по умолчанию является 514). Чтобы просмотреть дополнительные настройки системного журнала, перейдите на вкладку **«Сервис»** > **«Параметры сервера»** > **«Дополнительно»** >**«Изменить дополнительные параметры»** > **«Настройка»** > **«Ведение журнала»**. Здесь можно изменить параметры системного журнала: имя сервера системного журнала, порт сервера системного журнала, средство формирования системного журнала и степень детализации системного журнала.

**ПРИМЕЧАНИЕ.**: Серьезность системного журнала должна быть настроена для каждого типа журнала. Для журнала сервера это настройка **«Средство формирования системного журнала для журнала сервера»**, для журнала отладки это настройка **«Средство формирования системного журнала для журнала отладки»**. Для этих журналов серьезность системного журнала должна быть настроена, как указано ниже.

| **Степень детализации ERA** | **Серьезность системного журнала** |
|---|---|
| Уровень 1 (информация) | LOG_INFO //6 |
| Уровень 2 (ошибка) | LOG_INFO //3 |
| Уровень 3 (предупреждение) | LOG_INFO //4 |
| Уровень 4, 5 (отладка) | LOG_INFO //7 |

**Степень детализации** журнала означает уровень детализации журнала и информации, которую он включает.

- **«Уровень 1 — Пользователи и группы»** — регистрируются действия, связанные с пользователями и группами (статические группы, параметрические группы, добавление или удаление клиента из группы и пр.).
- **«Уровень 2 — Вышеперечисленное + действия клиента»** — вышеперечисленное и все действия, связанные с клиентом ERA (установка или удаление нового флага, настройка клиентской политики, запрос данных и пр.).
- **«Уровень 3 — Вышеперечисленное + задачи и уведомления»** — вышеперечисленное и все действия, связанные с задачами (создание и удаление задач, создание и удаление уведомлений и пр.).
- **«Уровень 4 — Вышеперечисленное + отчеты»** — вышеперечисленное и все действия, связанные с отчетами (создание и удаление отчетов, создание и удаление шаблонов отчетов и пр.).
- **«Уровень 5 — Все события»** — все действия, связанные с журналом (очистка журнала системы предотвращения вторжений на узел, очистка журнала угроз и пр.).

**2. Журнал сервера**

Во время работы сервер ERA Server создает журнал сервера (**«Имя файла журнала»**) о своих действиях, и его можно настроить (**«Детализация журнала»**).

**Примечание.** По умолчанию выходные текстовые данные сохраняются в файл *%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\logs\era.log*

- Если выбран параметр **«Записывать в текстовый файл»**, новые файлы журнала будут создаваться (**«Ротация, если более X МБ»**) и удаляться (**«Удалять журналы с ротацией старше X дн.»**) ежедневно.

**Примечание.** В разделе **«Записывать в текстовый файл»** рекомендуется оставить для параметра **«Детализация журнала»** значение *«Уровень 2 — То же + Ошибки сессии»* и повышать его только в случае возникновения проблем или согласно рекомендациям службы поддержки клиентов ESET.

- Параметр **«Записывать в журнал приложений ОС»** разрешает копирование информации в журнал системных событий (**«Панель управления Windows»** > **«Администрирование»** > **«Просмотр событий»**).

- Параметр **«Записывать в системный журнал»** отправляет сообщение системного журнала на указанный порт указанного сервера системного журнала (сервером по умолчанию является localhost, портом по умолчанию является 514). Чтобы просмотреть дополнительные настройки системного журнала, перейдите на вкладку **«Сервис»** > **«Параметры сервера»** > **«Дополнительно»** >**«Изменить дополнительные параметры»** > **«Настройка»** > **«Ведение журнала».** Здесь можно изменить параметры системного журнала: имя сервера системного журнала, порт сервера системного журнала, средство формирования системного журнала и степень детализации системного журнала.

**Степень детализации** журнала означает уровень детализации журнала и информации, которую он включает.

- **Уровень 1 — Критическая информация** — неустойчивое поведение (в этом случае обратитесь в службу поддержки клиентов ESET).
- **Уровень 2 — То же + Важная информация о сеансе** — информация об обмене данными с сервером (кто заходил на сервер ERA Server, когда и зачем).
- **Уровень 3 — То же + различные данные** — информация о внутренних процессах на сервере ERA.
- **Уровень 4 — То же + установщик** — информация об агенте einstaller.exe (информация о сервере ERA — подключение или отключение агента и результаты).
- **Уровень 5 — То же + клиенты** — информация о клиенте (информация о сервере ERA, подключении или отключении клиента и результатах).

**ПРИМЕЧАНИЕ.** Рекомендуется оставить уровень детализации «Уровень 2 - То же + Ошибки сессии». Менять уровень детализации журнала следует только при возникновении проблем или после получения соответствующей рекомендации от службы поддержки клиентов ESET.

3. При обычных условиях параметр базы данных **«Журнал отладки»** следует отключить — он используется для устранения проблем в базе данных. Для настройки степени сжатия для отдельных журналов с ротацией выберите **«Сервис»** > **«Параметры сервера»** > **«Дополнительно»** > **«Изменить дополнительные параметры»** > **«Настройка»** > **«Ведение журнала»** > **«Сжатие журнала отладки с ротацией»**.

### 6.4.1 Просмотр журнала аудита

В **журнале аудита** отслеживаются и регистрируются все изменения в конфигурации и все действия, которые выполняют пользователи ERAC. Это помогает администратору отслеживать все действия, связанные с ERAC, в том числе возможный несанкционированный доступ.

**ПРИМЕЧАНИЕ.**: Средство просмотра журнала аудита отображает изменения, внесенные в базу данных. Журнал аудита не включает другие журналы (например, журнал файла и другие).

Слева находится **фильтр**, который используется для фильтрации записей в **журнале аудита**. В этом модуле в верхней правой части под списком записей **журнала аудита** в раскрывающемся меню можно также выбрать количество элементов для отображения с помощью параметра **«Показать»**.

**«Фильтр»**

- **«С»**/**«До»**. Выберите конкретное время, для которого будет выполнена фильтрация журналов. Если выбрать оба параметра и указать время, будет создан временной интервал.

- **«Пользователь»**. Введите имена пользователей, для которых будут отображаться журналы.

- **«Имя для входа в домен»**. Введите имена пользователей для входа в домен, для которых будут отображаться журналы.
- **«IP адрес»**. Выберите нужный параметр (**«Адрес»**, **«Диапазон»** или **«Маска»**) и введите адреса в соответствующие поля. Эти параметры являются общими для адресов IPv4 и IPv6.
- **«Типы действий»**. Выберите действия, которые должны отображаться в журналах аудита. По умолчанию для отображения выбраны все действия.
- **«Применить фильтр»**. Если нажать эту кнопку, параметры фильтра немедленно применяются к **журналу аудита**.
- **«По умолчанию»**. Если нажать эту кнопку, параметры фильтра будут сброшены до значений по умолчанию.

**«Список записей журнала аудита»**

- **«Дата»** — дата выполнения действия. Дата и время совпадают с настройками времени на компьютере сервера.
- **«Пользователь»** — пользователь консоли ERAC, который выполнил действие.
- **«Имя для входа»** — имя пользователя для входа в домен Windows, который выполнил действие. Отображается только в случае использования типа входа «Windows/домен».
- **«IP-адрес консоли»** — IP-адрес консоли, из которой пользователь ERAC выполнил действие.
- **«Действие»** — действие, выполненное пользователем.
- **«Объект»** — количество объектов, затронутых действием.

**ПРИМЕЧАНИЕ.**: Чтобы отобразилась дополнительная информация (если она есть), щелкните дважды строку в журнале.

## 6.5 Репликация

Чтобы настроить параметры сервера ERA Server выберите **«Сервис»** > **«Параметры сервера»** в главном окне программы ERA Console.

Репликация используется в больших сетях с несколькими серверами ERA Server, например в компании с нескольким подразделениями. На вкладке **«Репликация»** настраиваются параметры репликации данных между несколькими серверами ERA Server, работающими в сети. Сведения о настройке нескольких серверов ERA Server в организации см. в разделе Настройка серверов ERA в больших сетях 130.

Для настройки репликации используются перечисленные ниже параметры.

**«Параметры репликации „на“»**

- **Включить репликацию «на»** — включает репликацию в большой сети, как описано в разделе Репликация 130.
- **Главный сервер** — IP-адрес или имя главного сервера ERA, который собирает данные с локального сервера ERA.
- **Порт** — порт, используемый для репликации.
- **Выполнять репликацию каждые XX минут** — интервал репликации.
- **«Реплицировать:» «Журнал угроз»**, **«Журнал файервола»**, **«Журнал событий»**, **«Журнал сканирования»**, **«Мобильный журнал»**, **«Журнал карантина»** — если выбраны эти параметры, все данные, отображаемые на вкладках «Клиенты», «Журнал угроз», «Журнал файервола», «Журнал событий», «Журнал сканирования» и «Задачи», реплицируются в отдельные столбцы и строки. Информация, хранящаяся не в базе данных, а в отдельных файлах (например, в *текстовом* или *XML*-формате), может не реплицироваться. Включение этих параметров позволит реплицировать записи в таких файлах.
- **«Автоматически реплицировать:» «Данные клиента»**, **«Данные журнала угроз»**, **«Данные журнала**

**сканирования»**, **«Подробности мобильного журнала»**, **«Файлы в карантине»** — эти параметры позволяют автоматически реплицировать дополнительные сведения, хранящиеся в отдельных файлах. Их также можно загрузить по требованию, нажав кнопку **«Запрос»**.

- **Тип журнала** — тип реплицируемых на главный сервер ERA событий (предупреждение, событие, проверка).
- **Автоматическая репликация...** — включение периодической репликации. Если этот параметр не выбран, репликацию можно запускать вручную.

**«Состояние репликации „на“»**

- **Реплицировать** — запуск процесса репликации.
- **Выделить все клиенты для репликации** — если этот флажок установлен, будут реплицированы все клиенты, включая те, на которых не было изменений.

**«Параметры репликации „из“»**

- **Включить репликацию «от»** — этот параметр позволяет локальному серверу ERA собирать данные с других серверов, указанных в поле **Разрешенные серверы**. Для разделения нескольких серверов RA используются запятые.
- **Разрешить репликацию с любого сервера** — если этот флажок установлен, репликацию можно выполнить с любого сервера. При установке этого флажка поле **Разрешенные серверы** отключается.

### 6.5.1 Репликация в больших сетях

Репликация используется в больших сетях с несколькими серверами ERA Server, например в компании с нескольким подразделениями. Дополнительные сведения см. в разделе Установка 24.

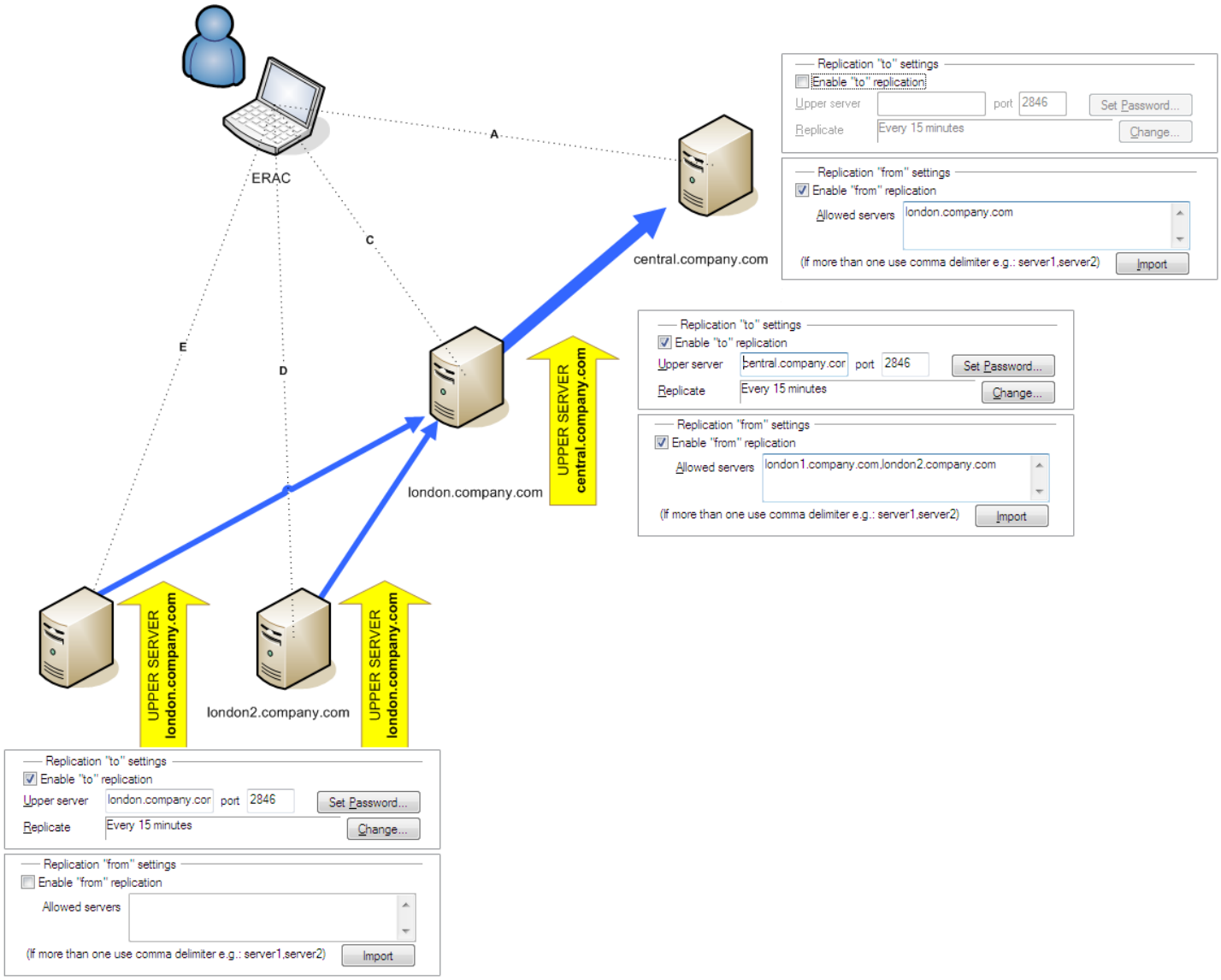
Параметры на вкладке «Репликация» (**«Служебные программы» > «Настройки сервера...»**) разделены на две части:

- «Параметры репликации „на“»
- «Параметры репликации „из“»

Раздел **«Параметры репликации "на"»** предназначен для настройки подчиненных серверов ERA Server. Необходимо активировать параметр **«Включить репликацию "на"»** и указать IP-адрес или имя главного сервера ERAS (верхнего уровня). После этого данные с подчиненного сервера реплицируются на основной сервер. **«Параметры репликации "из"»** позволяют основным серверам ERA Server (верхнего уровня) принимать данные от подчиненных серверов ERA Server или передавать их своим вышестоящим серверам. Необходимо активировать параметр **«Включить репликацию "из"»** и ввести названия подчиненных серверов, разделенные запятыми.

Для серверов ERA Server, находящихся внутри иерархии репликации (например, имеющих и подчиненный сервер, и сервер верхнего уровня), оба эти параметра должны быть включены.

Все вышеперечисленные сценарии показаны на рисунке ниже. Отдельные серверы ERA Server выделены бежевым цветом. Каждый из серверов ERAS представлен в окне репликации своим именем (которое во избежание путаницы должно совпадать со значением переменной *%Computer Name%*) и соответствующими параметрами.




Другие параметры, влияющие на репликацию серверов.

- **«Реплицировать журнал угроз»**, **«Реплицировать журнал файервола»**, **«Реплицировать журнал событий»**, **«Реплицировать журнал сканирования»**, **«Реплицировать мобильный журнал»**, **«Реплицировать журнал карантина»**
  Если выбраны эти параметры, все данные, отображаемые на вкладках **«Клиенты»**, **«Журнал угроз»**, **«Журнал файервола»**, **«Журнал событий»**, **«Журнал сканирования»**, **«Мобильный журнал»**, **«Журнал карантина»** и **«Задачи»**, реплицируются в отдельные строки и столбцы. Информация, хранящаяся не в базе данных, а в отдельных файлах (например, в текстовом (*TXT*) или *XML*-формате), может не реплицироваться. Включение этих параметров позволит реплицировать записи в таких файлах.

- **«Автоматически реплицировать данные журнала угроз»**, **«Автоматически реплицировать данные журнала сканирования»**, **«Автоматически реплицировать данные клиента»**, **«Автоматически реплицировать данные мобильного журнала»**, **«Автоматически реплицировать файлы карантина»**
  Эти параметры позволяют автоматически реплицировать подробные данные, хранящиеся в отдельных файлах. Их также можно загрузить по требованию, нажав кнопку **«Запрос»**.

**Примечание.** Некоторые журналы реплицируются автоматически, в то время как подробные журналы и журналы настройки клиента реплицируются только по запросу. Это связано с тем, что некоторые журналы содержат большие объемы данных, которые могут являться несущественными. Например, журнал сканирования с включенным параметром «Регистрировать все файлы» будет занимать много места на диске. Такая информация обычно не нужна и запрашивается вручную. Дочерние серверы не отправляют данные об удаленных клиентах автоматически. В связи с этим серверы верхнего уровня могут продолжать хранить сведения о клиентах, удаленных с подчиненных серверов. Чтобы удалить клиента с вкладки «Клиенты» на серверах верхнего уровня, выберите в меню **«Настройки сервера»** > **«Дополнительно»** > **«Изменить**

**дополнительные настройки»** > **«Настройка»** > **«Репликация»** для подчиненных серверов параметр «Включить удаление реплицированных клиентов».

Чтобы установить уровень обслуживания в ERAS, выберите меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки…»** > **«Настройка»** > **«Обслуживание сервера»**.

Если необходимо реплицировать только клиенты с изменением состояния, выберите команду **«Служебные программы»** > **«Настройки сервера»** > **«Репликация»** > **«Отметить все клиенты для репликации как "Начать репликацию"»**.

## 6.6 Обновления

Окно **«Обновления»** в модуле **«Параметры сервера»** предназначена для настройки параметров обновления ESET Remote Administrator Server. Окно разделено на две области. В верхней части перечислены параметры обновления сервера, а нижняя часть предназначена для настройки зеркала обновлений. В ESET Remote Administrator Server версии 2.0 доступна функция Сервер зеркала 133, которая создает локальный сервер обновлений для клиентских рабочих станций.

Описание всех элементов и функций приведено внизу.

- **«Сервер обновления»** — сервер обновлений ESET. Рекомендуется оставлять значение по умолчанию («Автоматический выбор»).
- **«Интервал обновлений»** — определяет максимальный интервал времени между проверками доступности новых файлов обновления.
- **«Имя пользователя для обновления»** — имя пользователя, применяемое ESET Remote Administrator для аутентификации на серверах обновлений.
- **«Обновить пароль»** — пароль, связанный с данным именем пользователя.

Регулярная база данных сигнатур вирусов и обновления компонентов программы являются ключевыми элементами для своевременного обнаружения угроз. Однако, сетевые администраторы, которые управляют большими сетями, могут иногда сталкиваться с проблемами обновления, например с ложными оповещениями или проблемами, связанными с модулем. Есть три варианта подключения к серверу обновлений.

- **«Регулярное обновление»** — база данных сигнатур вирусов обновляется за счет регулярных обновлений серверов к моменту их выпуска.
- **«Тестовое обновление»** — если этот параметр включен, бета-модули будут загружены во время обновления. Этот вариант не рекомендуется для рабочей среды, он подходит только для тестирования.
- **«Отложенное обновление»** — включите этот параметр, чтобы получать обновления с задержкой в 12 часов, т. е. после того, как обновления будут протестированы в рабочей среде и будут считаться стабильными.

Для запуска задачи обновления и загрузки обновленных компонентов программы ESET Remote Administrator нажмите кнопку **«Обновить сейчас»**. Обновления могут содержать важные компоненты или функции, поэтому крайне важно убедиться в том, что обновление работает правильно и в автоматическом режиме. Если возникают проблемы с обновлениями, выберите **«Очистить кэш обновлений»** , чтобы очистить папку с временными файлами обновления. Параметр **«Зеркальное отображение загруженного устройства управления»** становится активным, когда обновление PCU (*PCU — обновление компонентов программы*) загружено и ожидает подтверждения вручную. Нажмите кнопку, чтобы просмотреть доступные обновления PCU Updates и лицензионное соглашение. Чтобы настроить зеркала для обновлений программных компонентов, выберите **Дополнительно** > **Изменить дополнительные параметры** и настройте параметры в **ESET Remote Administrator** > **ERA Server** > **Настройка** > **Зеркало**.
Конфигурация зеркала в ESET Remote Administrator Server такая же, как и в версиях ESET Endpoint Antivirus Business Edition и ESET Endpoint Security Business Edition. Описания важных элементов зеркала указаны ниже.

- **«Создать зеркало обновления»** — включение функции зеркала. Если этот параметр отключен, копии обновления не создаются.

- **«Создать зеркало для выбранных компонентов программы»** — выбор языковых версий и типов программных компонентов, которые нужно создать на зеркале.
- **«Создавать зеркало для выбранных обновлений программных компонентов только по требованию»** — если включен этот параметр, зеркала для обновлений программных компонентов не создаются автоматически. Если нужно включить зеркала для обновлений программных компонентов, установите флажок **«Зеркальное отображение загруженного устройства управления»** в меню **«Сервис»** > **«Параметры сервера»** > **«Обновления»**
- **«Зеркальное отображение папки»** — локальная или сетевая папка, предназначенная для хранения файлов обновлений.
- **«Включить рассылку обновлений через HTTP»** — включение доступа к обновлениям через внутренний HTTP-сервер.
- **«Порт HTTP-сервера»** — порт, на котором ESET Remote Administrator Server будет предоставлять службу обновления.
- **«Аутентификация HTTP-сервера»** — способ аутентификации, используемый для доступа к файлам обновления. Доступны следующие варианты: **«Отсутствует»**, **«Обычная»**, **NTLM**. Вариант **«Обычная»** предписывает использовать обычную аутентификацию с использованием шифрования base64. Вариант **NTLM** предписывает использовать безопасный способ шифрования. Для аутентификации используются учетные записи, созданные на рабочих станциях с файлами обновлений для общего пользования.

Кнопка **«По умолчанию»** позволяет восстановить для всех параметров в этом окне их стандартные значения.

**Примечание.** В режиме HTTP-сервера рекомендуется использовать не более 400 клиентов для одного зеркала. В крупных сетях с большим количеством клиентов рекомендуется разнести зеркала обновлений на дополнительные серверы ERA (или ESS/EAV). Если зеркало должно быть централизовано на одном сервере, рекомендуется использовать HTTP-сервера другого типа, например Apache. В ERA также поддерживаются дополнительные способы аутентификации (например, на веб-сервере Apache используется способ .htaccess).

Администратор должен указать лицензионный ключ купленного продукта и ввести имя пользователя и пароль для активации функции зеркала на сервере ERAS. Если администратор использует лицензионный ключ, имя пользователя и пароль для ESET Endpoint Antivirus Business Edition, то при дальнейших обновлениях ESET Endpoint Security Business Edition исходный лицензионный ключ, имя пользователя и пароль также нужно заменить.

**Примечание.** Клиенты ESET Endpoint Antivirus могут также обновляться с помощью лицензии ESET Endpoint Security, но не наоборот.

### 6.6.1 Сервер зеркала

Функция зеркала позволяет создавать локальный сервер обновления. Клиентские компьютеры не загружают обновления сигнатур вирусов с сервера ESET в Интернете, а подключаются к локальному серверу-зеркалу в своей сети. Основным преимуществом этого решения является сокращение нагрузки на внешний канал и уменьшение трафика, поскольку для обновления к Интернету подключается только зеркало, а не сотни клиентских компьютеров. В такой конфигурации важно, чтобы зеркало было постоянно подключено к Интернету.

***Предупреждение.*** В работе зеркала, выполнившего обновление компонентов программы, но еще не перезагруженного, возможны отказы. В этом случае сервер не сможет загружать обновления и рассылать их на клиентские рабочие станции. НЕ ВКЛЮЧАЙТЕ АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ПРОГРАММНЫХ КОМПОНЕНТОВ ДЛЯ СЕРВЕРНЫХ ПРОДУКТОВ КОМПАНИИ ESET!

Работать с зеркалом можно из двух мест:

- ESET Remote Administrator (зеркало физически работает на сервере ERAS и управляется из консоли ERAC);
- ESET Endpoint Security Business Edition или ESET Endpoint Antivirus Business Edition (при условии, что пакет Business Edition был активирован с использованием лицензионного ключа).
- Зеркало также доступно в ESET Endpoint Security и ESET Endpoint Antivirus. Дополнительную информацию см.

в документации соответствующего клиентского продукта.

Администратор выбирает способ активации функции зеркала.

В больших сетях можно создавать несколько зеркал (например, для различных отделений компании) и устанавливать одно из них в качестве центрального (в головном офисе) в каскадной конфигурации — аналогично конфигурации сервера ERAS с несколькими клиентами.

Администратор должен указать лицензионный ключ купленного продукта и ввести имя пользователя и пароль для активации функции зеркала на сервере ERAS. Если администратор использует лицензионный ключ, имя пользователя и пароль для ESET Endpoint Antivirus Business Edition, то при дальнейших обновлениях ESET Endpoint Security Business Edition исходный лицензионный ключ, имя пользователя и пароль также нужно заменить.

**Примечание.** Клиенты ESET Endpoint Antivirus могут также обновляться с помощью лицензии ESET Endpoint Security, но не наоборот. Этот принцип также применим к ESET Endpoint Antivirus и ESET Endpoint Security.

#### 6.6.1.1 Работа сервера зеркала

Компьютер, на котором находится сервер зеркала, должен быть постоянно включен и подключен к Интернету или зеркалу верхнего уровня для репликации. Пакеты обновления зеркала можно загружать двумя способами:

1. По протоколу HTTP (рекомендуется).
2. С помощью общего сетевого диска (SMB).

Сервер обновления ESET использует протокол HTTP с аутентификацией. Центральное зеркало должно иметь доступ к серверам обновления по имени пользователя (которое обычно имеет вид *EAV-XXXXXXX*) и пароль.

В сервер зеркала, который является частью ESET Endpoint Security и ESET Endpoint Antivirus, встроен HTTP-сервер (вариант 1).

**Примечание.** При использовании встроенного HTTP-сервера (без аутентификации) обеспечьте его недоступность за пределами своей сети (т. е. для клиентов, не охватываемых лицензией). Сервер не должен быть открыть для доступа из Интернета.

По умолчанию встроенный HTTP-сервер подключается через TCP-порт 2221. Не используйте этот порт для других приложений.

**Примечание.** Если используется HTTP-сервер, рекомендуется использовать не более 400 клиентов для одного зеркала. В крупных сетях с большим количеством клиентов рекомендуется разнести зеркала обновлений на дополнительные серверы ERA (или ESS/EAV). Если зеркало должно быть центральным на одном сервере, рекомендуется использовать HTTP-сервера другого типа, например Apache. В ERA также поддерживаются дополнительные способы аутентификации (например, на веб-сервере Apache используется способ .htaccess).

Второй способ (общая сетевая папка) требует совместного использования (с правами для чтения) папки, в которой содержатся пакеты обновления. В этом сценарии имя пользователя и пароль с правами на чтение папки обновления необходимо вводить на клиентской рабочей станции.

**Примечание.** Клиентские решения ESET используют учетную запись SYSTEM, поэтому их права доступа отличаются от прав доступа пользователя, находящегося в системе. Аутентификация требуется даже в том случае, если сетевой диск доступен группе пользователей «Все» (Everyone), в том числе текущему пользователю. Кроме того, для задания сетевого пути к локальному серверу следует использовать формат UNC. Не рекомендуется использовать формат *ДИСК:*\.

При использовании общей сетевой папки (вариант 2) рекомендуется создать уникальное имя пользователя (например, NODUSER). Эта учетная запись будет использоваться на всех клиентских компьютерах только для загрузки обновлений. Учетная запись NODUSER должна иметь права для чтения на общую сетевую папку, в которой находятся пакеты обновления.

Для получения доступа к сетевому диску введите полные данные аутентификации: *РАБОЧАЯ ГРУППА* *Пользователь* или *ДОМЕН**Пользователь*..

Помимо данных для аутентификации, необходимо также задать источник обновлений для клиентских

решений ESET. Источником обновления может быть URL-адрес локального сервера (*http://имя_сервера_зеркала:порт*) либо UNC-путь к сетевому диску: (*имя_сервера_зеркала**имя_общего_ресурса*).

#### 6.6.1.2 Типы обновлений

Помимо обновлений БД сигнатур вирусов (которые могут включать обновления ядра программного обеспечения ESET), выполняются также обновления программных компонентов. Обновления программных компонентов добавляют новые функции в продукты безопасности ESET и требуют перезагрузки компьютера.

Сервер зеркала позволяет администратору отключать автоматическую загрузку обновлений программы с серверов обновления ESET (или с зеркала верхнего уровня) и их рассылку на клиенты. Позднее администратор сможет активировать рассылку вручную (например, когда он будет уверен, что это не приведет к конфликту между новой версией и существующими приложениями).

Эта функция особенно необходима, если администратору нужно загружать обновления БД сигнатур вирусов вместе с новой версией программы. При использовании более старой версии программы вместе с последней версией БД сигнатур вирусов программа будет продолжать обеспечивать наилучшую защиту. Однако для получения доступа к новым функциям рекомендуется загружать и устанавливать последние версии программы.

По умолчанию программные компоненты не загружаются автоматически и их загрузку нужно настраивать вручную на сервере ERAS. Дополнительные сведения см. в разделе Включение и настройка зеркала 135.

#### 6.6.1.3 Включение и настройка зеркала

Если зеркало встроено непосредственно в ERA, подключитесь к серверу ERAS с помощью ERAC и выполните следующие действия.

- В консоли ERAC выберите команду **«Служебные программы»** > **«Настройки сервера...»** > **«Обновления»**.
- В раскрывающемся меню **«Сервер обновлений»** выберите пункт **«Выбирать автоматически»** (обновления будут загружаться с серверов ESET) или введите URL-адрес или путь к зеркалу в формате *URL/UNC*.
- Установите интервал обновления (рекомендуется 60 минут).
- Если в предыдущем шаге было выбрано **«Выбирать автоматически»**, введите имя пользователя (имя пользователя для обновления) и пароль (пароль для обновления), полученные после приобретения продукта. При доступе к серверу верхнего уровня введите правильное имя пользователя домена и пароль для данного сервера.
- Выберите пункт **«Создать зеркало обновления»** и введите путь к папке, в которой будут храниться файлы обновления. По умолчанию используется относительный путь к папке зеркального отображения. Если выбран параметр **«Передавать файлы обновления с помощью внутреннего HTTP-сервера»**, обновления доступны по порту HTTP, заданному в поле **«Порт HTTP-сервера»** (по умолчанию — 2221). Установите для параметра **«Аутентификация»** значение **«НЕТ»** (дополнительные сведения см. в разделе Работа сервера зеркала 134).

**Примечание.** При возникновении проблем с обновлением нажмите кнопку **«Очистить кэш обновлений»**, чтобы удалить содержимое папки с временными файлами.

- Параметр **«Зеркало загруженных обновлений программных компонентов»** позволяет активировать зеркала для программных компонентов. Чтобы настроить зеркала для обновлений программных компонентов, выберите **«Дополнительно» > «Изменить дополнительные параметры»** и настройте параметры в разделе **ESET Remote Administrator** > **ERA Server** > **«Настройка» > «Зеркало»**.
- Выберите компоненты, которые должны загружаться, в меню **«Дополнительно»** > **«Изменить дополнительные настройки...»** в разделе **ERA Server** > **«Настройка»** > **«Зеркало»** > **«Создать зеркало для выбранных компонентов программы»**. Выберите все языковые версии компонентов, которые будут использоваться в данной сети. Учтите, что загрузка языковой версии, которая не установлена в сети, будет увеличивать объем сетевого трафика.

Функция зеркала также доступна непосредственно из интерфейса программ ESET Endpoint Security Business

Edition, ESET Endpoint Antivirus Business Edition, ESET Endpoint Security и ESET Endpoint Antivirus. Администратор сам решает, с помощью какой из них будет создан сервер зеркала.

Чтобы активировать и запустить зеркало в ESET Endpoint Security Business Edition или ESET Endpoint Antivirus Business Edition, выполните указанные ниже действия.

1) Установите ESET Endpoint Security Business Edition, ESET Endpoint Antivirus Business Edition (версия клиента 4.X), ESET Endpoint Security или ESET Endpoint Antivirus.

2) В окне **«Дополнительные настройки»** (F5) выберите команду **«Разное»** > **«Лицензии»**. Нажмите кнопку **«Добавить…»**, укажите путь к файлу **.lic* и нажмите кнопку **«Открыть»**. Это позволит выбрать лицензию и настроить функцию зеркала.

3) В разделе **«Обновление»** нажмите кнопку **«Настройка»** и щелкните вкладку **«Зеркало»**.

4) Установите флажки **«Создать зеркало обновления»** и **«Передавать файлы обновления с помощью внутреннего HTTP-сервера»**.

5) Введите полный путь к папке (**«Папка для дублируемых файлов»**), где будут храниться файлы обновления.

6) Параметры **«Имя пользователя»** и **«Пароль»** служат для аутентификации клиентских рабочих станций, пытающихся получить доступ к папке зеркального отображения. В большинстве случаев заполнять эти поля не требуется.

7) Установите для параметра «Аутентификация» значение **«НЕТ»**.

8) Выберите компоненты для загрузки (компоненты всех языковых версий, которые будут использоваться в данной сети). Компоненты отображаются только в случае, если они доступны на серверах обновления ESET.

**Примечание.** Для обеспечения оптимальной работы рекомендуется включать загрузку и зеркалирование программных компонентов. Если этот параметр отключен, обновляются только БД сигнатур вирусов, а программные компоненты не обновляются. Если зеркало является частью ERA, этот параметр можно настроить в консоли ERAC в меню **«Сервис»** > **«Параметры сервера»** > вкладка **«Дополнительно»** > **«Изменить дополнительные параметры»** > **«ESET Remote Administrator»** > **«ERA Server»** > **«Настройка»** > **«Зеркало»**. Включите все языковые версии программы, присутствующие в сети.

**ПРИМЕЧАНИЕ.**: Если необходимо настроить зеркало таким образом, чтобы для обновления клиентов использовался протокол HTTPS, выберите **ERAC** > **Служебные программы** > **Параметры сервера…** > вкладка **Дополнительно** > **Изменить дополнительные параметры…** > **ESET Remote Administrator** > **ERA Server** > **Настройка** > **Зеркало** > **Протокол** > **HTTPS**.

## 6.7 Другие настройки

На вкладке **Другие параметры** можно настроить адрес сервера **SMTP**, чтобы использовать его при отправке пакетов установки по электронной почте, и адрес электронной почты администратора, который администратор может использовать для отправки электронных писем. Если сервер требует аутентификацию, укажите соответствующие имя пользователя и пароль.

**Примечание**: Подключение можно защитить, выбрав протокол безопасности в раскрывающемся меню **Безопасное соединение**. Доступны протоколы **TLS** и **SSL**, а также вариант **Автоматически**, когда доступный протокол выбирается автоматически.

**Новые клиенты**

- **«Включать новые ПК»** — если установлен этот флажок, новые клиенты автоматически добавляются в список клиентов при их первом подключении к серверу ERA Server. Клиенты, импортированные посредством репликации с других серверов ERA, добавляются в список клиентов автоматически во время репликации.
- **Автоматически сбрасывать флаг «Новый» для новых клиентов** — если выбран этот параметр, флаг нового клиента не устанавливается автоматически для клиентов при их первом подключении к серверу ERAS. Дополнительную информацию см. в описании вкладки **«Клиенты»**.

**«Порты»** — позволяет настраивать порты.

- **«Консоль»**: порт, используемый консолью ERA Console для подключения к серверу ERA Server (по умолчанию — 2223).
- **«Клиент»**: порт, используемый клиентом ESET для подключения к серверу ERA Server (по умолчанию — 2222).
- **«Порт репликации сервера»**: используется сервером ERA для репликации на вышестоящий сервер ERA Server (по умолчанию — 2846).
- **«Программа удаленной установки ESET (агент)»**: порт, используемый агентом удаленной установки для удаленной установки (Удаленный установщик ESET, по умолчанию — 2224).
- **«Веб-сервер»**: порт, используемый для подключения к веб-серверу, (по умолчанию — 2225).

**Примечание.** Чтобы изменения конфигурации порта вступили в силу, необходимо перезапустить службу NOD32 сервера ERA Server.

**ESET Live Grid**

- **Сбор** — сервер ERAS будет отправлять подозрительные файлы и статистические данные клиентов на серверы ESET. В некоторых случаях передача этих данных непосредственно от клиентов невозможна.

**Панели мониторинга**

- **Настроить список веб-серверов...** — нажмите здесь, чтобы получить доступ к Списку веб-серверов панели мониторинга 49.

## 6.8 Дополнительно

На вкладке **«Дополнительно»** окна **«Настройки сервера»** можно просматривать и настраивать дополнительные параметры сервера с помощью редактора ESET Configuration Editor. Configuration Editor можно открыть с помощью кнопки **«Изменить дополнительные настройки...»** на данной вкладке. Прочтите предупреждение и действуйте с осторожностью.

В число дополнительных параметров входят следующие.

- **«Максимальное использование дискового пространства (%)»** — при превышении данного значения некоторые функции сервера могут быть недоступны. При подключении к серверу ERAS в консоли ERAC выводится уведомление при превышении указанного значения.
- **«Предпочтительный метод кодирования обмена данными по протоколу»** — определяет тип шифрования. Рекомендуется оставлять значение по умолчанию.
- **Включить переименование MAC-адреса (с неизвестного на действительный)** — после перехода с клиентского решения ESET, не поддерживающего отправку MAC-адреса (например, ESET Endpoint Antivirus 2.x), на клиентское решение, которое ее поддерживает (например, клиенты версии 3.x), запись старого клиента будет преобразована в новую. Рекомендуется оставлять значение по умолчанию («Да»).
- **Включить переименование MAC-адреса (с действительного на неизвестный)** — после перехода с клиентского решения ESET, поддерживающего отправку MAC-адреса (например, ESET Endpoint Antivirus 3.x), на клиентское решение, которое ее не поддерживает (например, клиенты версии 2.x), запись старого клиента будет преобразована в новую. Рекомендуется оставлять значение по умолчанию («Нет»).
- **«Включить переименование MAC-адреса (с действительного на другой действительный)»** — включает переименование действительных MAC-адресов. Значение по умолчанию не позволяет выполнять переименование, что означает, что MAC-адрес участвует в уникальной идентификации клиентов. Отключите этот параметр, если для одного ПК имеется несколько записей. Рекомендуется также отключать этот параметр, если после изменения MAC-адреса клиент идентифицируется как тот же клиент.
- **«Включить переименование компьютера»** — позволяет переименовывать клиентские компьютеры. Если этот параметр отключен, имя компьютера будет участвовать в уникальной идентификации клиентов.

- **«Использовать вход на сервер по умолчанию во время автоматической установки»** — ERAS позволяет задавать имя пользователя и пароль только для сценария входа и удаленной установки по электронной почте. Включение этого параметра позволяет использовать предопределенные значения и для автоматической удаленной установки.

# 7. Консоль командной строки ERA

Консоль командной строки ERA представляет собой инструмент, предназначенный для выполнения задач и управления клиентами непосредственно из командной строки. Для этого необходимо запустить консоль командной строки ERA из папки расположения консоли ERA или ввести в командной строке *eracmd.exe*.

Консоль командной строки ERA использует интерфейс API ERA 174 для обмена данными с сервером ERA Server.

При запуске консоли командной строки ERA потребуется ввести учетные данные для входа. Если оставить эти поля пустыми, будут использованы значения по умолчанию.

**Примечание.**: Консоль командной строки ERA поддерживает функцию автозаполнения. Начните вводить команду в консоли и нажмите клавишу TAB для завершения команды. Нажимая клавишу TAB несколько раз подряд, можно просмотреть все возможные варианты. Для просмотра истории введенных команд используйте клавиши со стрелками ВВЕРХ/ВНИЗ. Чтобы вернуться к предыдущему тексту, нажмите клавишу ESC, а чтобы полностью удалить текст, нажмите клавишу ESC дважды.

**Синтаксис в командной строке**.

```
eracmd.exe --connectionparameters [command arguments [-commandflags]] [;command arguments -commandflags]
```

**Пример**:

```
eracmd.exe --s 127.0.0.1 version server -format csv
eracmd.exe --aa
```

После запуска консоль командной строки ERA автоматически пытается подключиться к серверу. Если подключение установлено, eracmd начинает обработку команд. Если команда не указана, eracmd запускается в режиме оболочки, и пользователь сможет вводить команды и просматривать результаты напрямую. Чтобы просмотреть список доступных команд, введите команду `HELP COMMANDS`.

**Синтаксис в режиме оболочки**.

```
[command arguments [-commandflags]] [;command arguments -commandflags]
```

Если аргумент содержит пробелы, все слова аргумента необходимо поместить в кавычки. Если текст аргумента содержит кавычки, используйте двойные кавычки. Например, текст "Сказать ""привет"" всем" будет интерпретирован как 'Сказать "привет" всем'.

Два связанных между собой слова (одно из них выделено кавычками) будут связаны. Например, текст "Сказать "привет будет интерпретирован как 'Сказать привет'.

В ключевых словах и командах Eracmd не учитывается регистр. Регистр учитывается только в аргументах, используемых при отправке запроса в базу данных.

**Замена @**.

Любую часть команды можно взять из файла. Путь к файлу необходимо выделить символом @. При использовании такого синтаксиса содержимое указанного файла используется вместо него. Если файл содержит другие строки, они объединяются запятыми и используются в качестве одной строки. Таким образом, в файле можно сохранить список аргументов, которые будут использованы в следующей команде. Пустые строки пропускаются. Чтобы отменить эту функцию, символ @ необходимо поместить в кавычки.

**Примеры**:

Файл *myconnection.txt* содержит текст *--s 192.168.0.1*, а затем команду

*eracmd.exe @myconnection@ show clients id* с именем *-like "*@*"*:

*eracmd.exe --s 192.168.0.1 show clients id where name -like *@**.

В данном примере создается задача конфигурации для клиентов, в имени которых содержится слово «notebook»:

show client id where client_name -like *Notebook* -out notebookID.txt -format csv -header none

task config c:\task_config_01.xml @notebookID.txt@

**Команды** 142.

Введите в терминале команду HELP COMMANDS, чтобы просмотреть список доступных команд. Введите HELP <команда>, чтобы просмотреть инструкции для конкретной команды. Команды могут иметь обязательные параметры, а также дополнительные параметры, которые можно указать с помощью ключевого слова. Дополнительные параметры, вызываемые с помощью ключевого слова, могут использоваться в любом порядке после обязательных параметров. Команда начинается сразу после параметров подключения. Префикс не требуется. Если командная строка не содержит команд, eracmd запускается в режиме оболочки. В одной строке можно указать несколько команд через точку с запятой (;). Для исполнения файла сценария, содержащего несколько команд, используйте команду SCRIPT <имя_файла_сценария>. В файле сценария команды разделяются разрывом строки.

**Параметры команд**.

Параметры команд определяют общее действие команды, например формат вывода данных, или механизм обработки ошибок. Для правильной работы параметры команды следует указывать после команды и ее аргументов. Перед каждым ключевым словом параметра необходимо вставлять дефис (-). Чтобы просмотреть список параметров, введите команду HELP FLAGS.

**Комментарии.**

В режиме оболочки в сценариях или аргументах командной строки можно использовать комментарии. Комментарий начинается символом # и продолжается до конца текущей строки. Разделитель команды не является окончанием комментария. Если символ # используется внутри помещенной в кавычки последовательности, он не является началом комментария, а является обычной частью текста в кавычках.

**Режим оболочки**.

В режиме оболочки нажмите клавишу TAB для активации функции автозаполнения с учетом регистра. Чтобы включить, отключить или удалить историю команд, используйте команду `HISTORY`. Чтобы выбрать команду из истории, используйте клавиши со стрелками ВВЕРХ и ВНИЗ. Чтобы отменить изменения, внесенные с помощью клавиши TAB и клавиш со стрелками ВВЕРХ и ВНИЗ, нажмите клавишу ESC.

**Сценарий запуска.**

Сценарий запуска — это файл с командами, которые автоматически выполняются при запуске режима оболочки.

Файл сценария запуска по умолчанию расположен в папке ProgramData (All Users\Application Data), в файле ESET\ESET Remote Administrator\Console\eracmd_startup.txt. Альтернативный путь можно указать с помощью аргумента --startup eracmd.exe (например, eracmd.exe --startup startup_script.txt).

Сценарий не выполняется как отдельный подсценарий (как выполнение с использованием команды script), но выполняется так, как если бы команды вводились непосредственно в консоль в режиме оболочки (поэтому параметры, заданные в сценарии запуска с помощью команды set, остаются заданными в режиме оболочки).

Команду set save можно использовать для сохранения текущих значений параметров в сценарии запуска с перезаписью файла сценария запуска, если он существует.

Если в сценарии запуска используется команда выхода, следующие за ней команды не будут выполняться, но при этом eracmd.exe не выйдет из режима оболочки.

**Стили форматирования**

Параметры заголовка и полей можно использовать для указания стилей форматирования:

- keyword - используется неизменный текст (подходящий для автоматического выполнения последующей обработки);

- pretty - используется понятный текст (подходящий для отображения пользователям).

Параметр заголовка влияет на заголовки таблицы (имена столбцов). Параметр поля влияет на значения полей таблицы.

**Параметры подключения**

Параметры, связанные с подключением к серверу ERA, необходимо указывать в качестве параметров командной строки. Eracmd.exe выполняет обработку команд только при условии успешного подключения. Перед каждым используемым параметром подключения указывается двойной дефис (--).

*--s сервер:порт*: сервер, к которому необходимо подключиться. Значение по умолчанию: `localhost:2226`
*--u имя пользователя*: имя пользователя на сервере Era. Если имя пользователя начинается с префикса домена, оно будет использоваться в качестве имени пользователя для проверки подлинности домена. Эту команду нельзя использовать в сочетании с параметром --ud или --uc. Значение по умолчанию: `Administrator`
*--ud имя пользователя*: имя пользователя для проверки подлинности домена. Нельзя использовать в сочетании с параметром --u или --uc.
*--uc*: использование учетных данных текущего сеанса Windows. Нельзя использовать в сочетании с параметром --u или --ud.
*--p пароль*: пароль для проверки подлинности домена или сервера Era. Нельзя использовать в сочетании с параметром --pa. Значение по умолчанию: "" (пустой пароль).
*--pa*: подсказка пароля. После запуска консоли можно будет ввести пароль только с отображением символов «*». Нельзя использовать в сочетании с параметром --p.
*--aa*: запрос всех параметров подключения. Если указан этот параметр, никакие другие параметры подключения указать нельзя.
*--startup*: альтернативный путь к сценарию запуска. Сценарий запуска выполняется автоматически в начале работы режима оболочки.

## 7.1 Параметры команд

Параметры используются для определения метода работы команды или задания выходного файла. Чтобы задать для параметра значение по умолчанию, используйте команду SET. Параметры указываются после команды и ее аргументов. Ниже приведен список доступных параметров.

| | |
|---|---|
| `-format` | формат выходного файла. Возможные значения: *csv, table*. Значение по умолчанию: *csv* (в режиме командной строки), *table* (в режиме оболочки). |
| `-delim` | выбор разделителя для файла CSV. Если указан аргумент "", будет использоваться системный разделитель (также является значением по умолчанию). Если системный разделитель не задан, будет использоваться запятая (,). Точка с запятой используется в качестве разделителя команд. Чтобы задать точку с запятой как разделитель в выходном файле, используйте кавычки. Значение по умолчанию: "" (системный разделитель; если значение не указано, используется запятая). |
| `-out` | перенаправление выходных данных в файл. См. также сведения о параметрах -mode и -enc. Если данный параметр используется с аргументом "", перенаправление будет отключено (поведение по умолчанию). Значение по умолчанию: "" (перенаправление отключено). |
| `-mode` | Режим выходного файла. Возможные значения: o (перезапись файла), a (добавление данных в конец файла). Значение по умолчанию: o (перезапись файла). |
| `-enc` | кодировка выходного файла. Возможные значения: *ansi, utf8, utf16*. Значение по умолчанию: *utf8*. |
| `-header` | тип заголовка таблицы. Возможные значения: *keyword* (использовать в качестве заголовков аргументы команд, например client_name), *pretty* (использовать более удобные и понятные названия столбцов, например «Имя клиента»), *none* (не показывать заголовки). Значение по умолчанию: *keyword*. |
| `-paged` | разбивка выходных данных на страницы. Если этот параметр включен, после каждой страницы нужно нажимать определенную клавишу. Возможные значения: *true, false*. Значение по умолчанию: *false*. |
| `-tableclip` | обрезка таблиц по размеру экрана. Применяется только при выводе таблицы в окно |

консоли. Возможные значения: *true, false*. Значение по умолчанию: *true*.

`-color` использование разных цветов при отображении содержимого в окне консоли. Возможные значения: *true, false*. Значение по умолчанию: *true*.

`-field` стиль форматирования полей таблицы. Возможные значения: *keyword* (использовать константные ключевые слова, например finished_with_warning), *pretty* (использовать более удобный и понятный текст, например «Завершено с предупреждением»). Значение по умолчанию: *keyword*.

`-onerror` реакция на возникновение ошибки при выполнении команды. Если задать stop, выполнение последовательности команд будет немедленно остановлено. Если задать continue, продолжится выполнение следующих команд. Если во время выполнения какой-то команды возникла ошибка, завершение всей последовательности команд завершится сообщением об ошибке. Возможные значения: *stop, continue*. Значение по умолчанию: *stop*.

## 7.2 Команды

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *clearinfo* | Удаляет указанную информацию из клиента. Вы можете удалить предупреждение о последней угрозе, последнее предупреждение файервола, предупреждение о последнем событии и прочие сведения. | clearinfo <data type> <clients> | **data type** Разделенный запятыми список типов информации, которую нужно удалить. Возможные значения: threat,firewall,event,scan,custom<br><br>**clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов). Чтобы отобразился список клиентов, введите show client *. | clearinfo firewall * |
| *client comment* | Задание комментария клиента. | client comment <client ID> <comment> | **client ID** Идентификатор клиента, для которого будет задан комментарий. Чтобы отобразилась информация о существующих клиентах, в том числе о типе их идентификаторов, введите show client *.<br><br>**comment** Комментарий для клиента. | client comment 1 Problematic |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *client delete* | Удаляет клиенты с сервера. | client delete <client ID> [<nowait>] | **client ID** Разделенный запятыми список идентификаторов клиентов, которые нужно удалить.<br>**nowait** Не нужно ждать результата обработки запроса на сервере. Возможное значение: nowait | client delete 1,5,9 nowait |
| *client new* | Установка или сброс флага «Новый» для клиента на сервере. | client new <client ID> <action> | **client ID** Разделенный запятыми список идентификаторов клиентов для установки или сброса флага «Новый».<br>**action** Выбор установки или сброса флага «Новый». Возможные значения: set, reset | client new 1 reset |
| *client rename* | Переименование клиента на сервере. | client rename <client ID> <name> | **client ID** Идентификатор клиента для переименования.<br>**name** Новое имя для клиента. | client rename 1 new_client_name |
| *client roaming* | Установка или сброс флага «Пользователь в роуминге» для клиента на сервере. | client roaming <client ID> <action> | **client ID** Разделенный запятыми список идентификаторов клиентов для установки или сброса флага «Пользователь в роуминге».<br>**action** Выбор установки или сброса флага «Пользователь в роуминге». Возможные значения: set, reset | client roaming 1 set |
| *cls* | Очистка выводимых данных консоли. | cls | | cls |
| *echo* | Отображение аргумента в виде сообщения. При отсутствии аргумента в выводимые данные добавляется только | echo [<message>] | **message** Сообщение для отображения. Может содержать несколько объединенных значений. | echo "hello world"<br>echo "Report created with ID: ",@reportId.csv@<br>echo |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | новая строка. | | | |
| *encrypt* | Шифрование пароля для использования в конфигурации. Используется два типа шифрования: server — используется для паролей, определяемых сервером ERA (репликация, клиент, установщик, пользователи), и other — используется для паролей, определяемых другими службами (SMTP, обновление и т. д.). В результате данная команда обеспечивает отображение зашифрованного пароля, который можно использовать для создания файлов конфигурации. Если пароль не указан, пользователю будет предложено ввести его, при этом символы в поле пароля будут отображаться в виде звездочек. | encrypt <encryptionType> [<password>] | **encryptionType** Тип шифрования. Возможные значения: server, other, hash, int64<br>**password** Пароль для шифрования. | encrypt server MyReplicationPassword6578<br>encrypt other MySmnpPwdBfx5<br>encrypt hash MyLockPass2<br>encrypt int64 580076500 |
| *errmsg* | Отображение сообщения об ошибке по коду ошибки. | errmsg <code> | **code** Код ошибки для поиска сообщения об ошибке. | errmsg 2001 |
| *exit* | Прекращение работы консоли командной строки в случае использования в режиме оболочки. Остановка выполнения текущего файла сценария в случае использования в файле сценария. | exit | | |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *getdata* | Получение определенного набора сведений с конкретного клиента или о конкретной политике для локального файла. Некоторые сведения могут быть недоступны на сервере. Чтобы обновить информацию, используйте команду REQUEST.<br><br>Сведения о конфигурации, функциях защиты, состоянии защиты и системе автоматически обновляются для клиентов на основном сервере. | getdata <data type> <data ID> <file> | **data type** Тип данных, которые необходимо получить. Возможные значения: клиент: sysinspector (журнал SysInspector), configuration (XML-конфигурация), protection_status (состояние защиты), protection_features (функции защиты), system_information (сведения о системе); политика: policy (XML-политика, только для политик, которые не реплицируются с сервера верхнего уровня), policy_merged (XML объединенной политики, созданной в результате наследования применяемых настроек от политики верхнего уровня), policy_override (XML обязательной части политики, только для политик, реплицированных с сервера верхнего уровня), policy_nonoverride (XML необязательной части политики)<br><br>**data ID** Идентификатор информационного объекта (клиента или политики), из которого загружаются данные.<br><br>**file** Путь к локальному файлу назначения. | getdata configuration 1 c:\file.xml |
| *group* | Отображение определенных групп и сведений о группах. | group [<tree>] | **tree** Используйте режим дерева для отображения групп с наследованием | group |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | группы. | |
| *group assign* | Назначает клиенты статической группе. | group assign <group ID> <clients> | **group ID** Идентификатор группы, для которой нужно назначить клиенты.<br><br>**clients** Разделенные запятыми идентификаторы клиентов, которые нужно назначить указанной группе. Или используйте «*» для всех клиентов. Чтобы отобразился список клиентов и сведения о них (в том числе идентификаторы), введите «show client *». | group assign 1 3,4 |
| *group create* | Создает статическую или параметрическую группу. | group create <type> <name> [description <description>] [parentID <parent ID>] [paramsXML <params XML>] [sticky <sticky>] | **type** Тип новой группы (возможные значения: static, parametric)<br><br>**name**, **description**, **parent ID**, **params XML**, **sticky** — для типа справки `help group create` в eracmd.exe | group create static new_group |
| *group delete* | Удаляет статическую или параметрическую группу со всеми ее подгруппами. | group delete <group ID> | **group ID** Идентификатор группы, которую нужно удалить. Чтобы отобразились существующие группы и их идентификаторы, введите group. | group delete 2 |
| *group export* | Экспортирует статические или параметрические группы в локальный XML-файл. | group export <type> <group ID> <filename> [<tree>] | **type** Тип групп, которые нужно экспортировать. Возможные значения: static, parametric<br><br>**group ID** Идентификатор группы или идентификатор корневой группы | group export static * gr_static.xml<br><br>group export parametric 2 gr_parametric.xml false |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | поддерева, которое нужно экспортировать. Если используется знак «*» и дерево имеет значение TRUE, экспортировано будет все дерево групп.<br><br>**filename** Путь к XML-файлу, из которого нужно импортировать группы.<br><br>**tree** По умолчанию экспортируется все поддерево (с группой в качестве корня). Чтобы не экспортировать поддерево, используйте значение `false`. | |
| *group import* | Импортирует статические и параметрические группы в локальный XML-файл. Если уже существует группа с таким путем, она будет изменена (то есть к существующей группе будут добавлены связи клиента). | group import <type> <parent ID> <filename> [<relations>] | **type** Тип групп, которые нужно импортировать. Возможные значения: `static`, `parametric`<br><br>**parent ID** Идентификатор родительской группы. Группы будут импортированы в эту группу дерева. Если используется знак «*», поддерево будет импортировано в корень дерева групп.<br><br>**filename** Путь к XML-файлу, из которого нужно импортировать группы.<br><br>**relations** Импортирует связи клиентов указанной статической группы, если используется значение `true`. Значение по умолчанию — `false`. | group import static * gr_static.xml true<br><br>group import parametric 2 gr_parametric.xml |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *group remove* | Удаляет клиенты из статической группы. | group remove <group ID> <clients> | **group ID** , **clients** То же, что и для команды group assign. | group remove 1 3,4 |
| *group update* | Обновляет статическую или параметрическую группу с указанными параметрами. | group update <group ID> [name <name>] [description <description>] [parentID <parent ID>] [paramsXML <params XML>] | **group ID** Идентификатор группы, которую нужно обновить.<br>**name**, **description**, **parent ID**, **params XML**, **sticky** — для типа справки `help group update` в eracmd.exe | group update 2 newname |
| *help* | Отображаются сведения об использовании консоли командной строки ERA. Используйте аргумент, чтобы выбрать более конкретный раздел справки. | help [<command 1>] [<command 2>] | **command 1** Команда, для которой необходимо отобразить справку (первое слово имени команды). Возможные значения: <имя команды>, flags, commands<br>**command 2** Команда, для которой необходимо отобразить справку (второе слово имени команды). | help version<br>help commands<br>help help |
| *history* | Включение и отключение функции постоянного сохранения истории команд в режиме оболочки после закрытия консоли. По умолчанию эта функция отключена. | history [<action>] | **action** Если это действие пропущено, будет отображаться текущее состояние сохранения истории после закрытия консоли. Возможные значения: true (включить), false (отключить), clear (удалить историю команд), list (показать содержимое текущей сохраненной истории) | history true |
| *license* | Отображение сведений о лицензии сервера. | license | | license |
| *license add* | Загрузка указанного файла или файлов с лицензионным ключом на сервер | license add <filename> | **filename** Разделенный запятыми список путей к файлам | license add c:\era.lic |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | ERA. | | лицензионных ключей для загрузки. | |
| *license details* | Отображение сведений о частичных лицензионных ключах, загруженных на сервер ERA. | license details | | license details |
| *license replace* | Загрузка одного или нескольких файлов лицензионного ключа на сервер ERA и замена всех старых файлов лицензии загруженными лицензионными ключами. | license replace <filename> | **filename** Разделенный запятыми список путей к файлам лицензионных ключей для загрузки. | license replace c:\era.lic |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *logforward* | Отображение или настройка текущих параметров пересылки журналов. Эту команду можно использовать двумя способами.<br><br>1. Для отображения состояния конкретного параметра пересылки журналов используйте первый параметр <type> или используйте команду без параметров, чтобы отобразились текущие параметры пересылки для всех журналов.<br><br>2. Для настройки параметров пересылки журналов параметры <type> и <enable> являются обязательными. Другие параметры ([level <уровень>], [severity <серьезность>] и [facility <объект>]) являются необязательными. Если необязательный параметр пропущен, значение остается неизменным. | logforward [<type>] [<enable>] [level <level>] [severity <severity>] [facility <facility>] | **type** Тип журнала, который необходимо отобразить или обновить. Возможные значения: event, threat, firewall, hips, antispam, greylist, scan, mobile, device_control, web_control<br><br>**enable** Выбор включения или отключения пересылки. Возможные значения: true, false<br><br>**level** Уровень журнала, который обрабатывается при пересылке журнала. Возможные значения: critical, warning, normal, diagnostics<br><br>**severity** Значение важности системного журнала. Возможные значения: informational, error, warning, debug<br><br>**facility** Объект системного журнала. Возможные значения: от 0 до 23 | logforward<br><br>logforward scan<br><br>logforward eventlog true level warning<br><br>logforward threat false |
| *password* | Изменение пароля безопасности для сервера ERA. Если пароль пустой, используйте "". Если старый и новый пароли не указаны, система предложит пользователю ввести пароли. При вводе символы паролей будут отображаться в виде звездочек. Эта команда не обеспечивает | password <passwordType> [<oldPassword> <newPassword>] | **passwordType** Тип пароля, который необходимо установить. Возможные значения: replication, client, installer, currentuser<br><br>**oldPassword** Старый пароль. Можно использовать пароль администратора сервера ERA.<br><br>**newPassword** Новый пароль. | password currentuser<br><br>password replication oldPass1 newPass2 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | настройку паролей, которые являются частью конфигурации сервера. Для таких паролей используйте команду SERVERCFG SET или SERVERCFG SETPWD. | | | |
| *path* | Отображение или настройка текущего рабочего каталога, используемого в качестве основы для всех относительных путей (в случае указания пути к сценарию или путей к файлам данных). | path [<action>] [<path>] | **action** Действие. Возможные значения: get (показать текущий рабочий каталог), set (установить путь, указанный с помощью следующего аргумента), script (установить путь к текущему сценарию). Значение по умолчанию: get<br>**path** Новый рабочий каталог. Если используется относительный путь, он считается относительным для предыдущего рабочего каталога. | path<br>path set d:\scripts<br>path script |
| *policy* | Отображение определенных политик и сведений о политиках. Если имеется «дерево» аргументов, отображается дерево иерархии политик. | policy [<tree>] | **tree** Используйте режим дерева для отображения политик с наследованием политик. | policy<br>policy tree |
| *policy assign* | Назначение определенной политики определенным клиентам. Обратите внимание, что нельзя назначить любую политику любому клиенту. Если список клиентов содержит реплицированные клиенты, необходимо использовать реплицируемую вниз политику. Нельзя | policy assign <policy ID> <clients> | **policy ID** Назначенная политика. Возможные значения: <policy ID>, !DefaultClientsPolicy<br>**clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов). | policy assign 10 1,2,5,9<br>policy assign !DefaultClientsPolicy * |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | назначать политику с подчиненных серверов. | | | |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *policy create* | Создание политики с указанными параметрами на сервере. Если она успешно создана, отображается идентификатор новой политики. | policy create <name> <config XML> [parentID <parent ID>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>] | **name** Имя новой политики.<br><br>**config XML** XML-файл, содержащий конфигурацию новой политики.<br><br>**parent ID** Идентификатор родительского элемента новой политики.<br><br>**description** Описание новой политики.<br><br>**override any child** Установка флага «Переопределить все дочерние политики» для новой политики. Возможные значения: true, false. Значение по умолчанию: false<br><br>**down replicable** Установка флага «Реплицируемая вниз политика» для новой политики. Возможные значения: true, false. Значение по умолчанию: false<br><br>**default for clients** Установка политики в качестве политики по умолчанию для клиентов. Возможные значения: true, false. Значение по умолчанию: false<br><br>**default for lower servers** Установка политики в качестве политики по умолчанию для подчиненных серверов. Возможные значения: true, false. Значение по умолчанию: false | policy create new_policy policy.xml |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *policy delete* | Удаление политики и разрешение настройки замены для удаленной политики. Ненужные замены игнорируются. | policy delete <policy ID> [child_policies <child policies parent replacement>] [primary_clients <primary clients policy replacement>] [replicated_clients <replicated clients policy replacement>] [primary_clients_default <primary clients default policy replacement>] [lower_servers_default <lower servers default policy replacement>] [whole_branch <delete whole branch>] | **policy ID** Идентификатор политики, которую необходимо удалить.<br><br>**child policies parent replacement** Новая родительская политика для дочерних политик удаляемой политики. Возможные значения: <policy ID>, !DefaultUpperServerPolicy, !Not Available<br><br>**primary clients policy replacement** Новая политика для основных клиентов с удаляемой политикой. Возможные значения: <policy ID>, !DefaultClientsPolicy<br><br>**replicated clients policy replacement** Идентификатор новой политики для реплицированных клиентов с удаляемой политикой.<br><br>**primary clients default policy** Идентификатор замены новой политики по умолчанию для основных клиентов.<br><br>**lower servers default policy** Новая политика по умолчанию для подчиненных серверов. Возможные значения: <policy ID>, !NotAvailable | policy delete 2 primary_clients 4 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | **delete whole branch** При необходимости удаления всего раздела (указанной политики вместе с дочерними политиками). Возможные значения: true, false. Значение по умолчанию: false | |
| *policy export* | Экспортирует указанные политики из локального сервера в XML-файл. Экспортировать можно все политики, одну политику или дерево политик с указанным корнем. | policy export <policy ID> <filename> [<tree>] | **policy ID** Идентификатор политики, которую нужно экспортировать. Чтобы экспортировать все политики, используйте знак «*».<br><br>**filename** Путь к XML-файлу, в который будет экспортирована политика.<br><br>**tree** Задано значение по умолчанию true, и это значит, что указанная политика будет экспортирована вместе со своим целым поддеревом. Если вы используете значение false, поддерево указанной политики не будет экспортировано. | policy export * all_policies.xml<br><br>policy export 3 policy3.xml true |
| *policy import* | Импорт всех политик из XML-файла. Ранее определенные политики изменены не будут. Если имя политики уже существует, новая (импортированная) политика будет переименована. | policy import <filename> | **filename** Путь к XML-файлу, из которого нужно импортировать политики. | policy import policyBackup.xml |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *policy update* | Обновление конфигурации политики с помощью указанных параметров. | policy update <ID> [name <name>] [parentID <parent ID>] [configXML <config XML>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>] [replicated_clients <replicated clients policy replacement>] [lower_servers_default <lower servers default policy replacement>] [primary_clients_default <primary clients default policy replacement>] | **ID** Идентификатор обновленной политики.<br><br>**name** Новое имя обновленной политики.<br><br>**parent ID** Новый идентификатор родительского элемента обновленной политики. Возможные значения: <идентификатор политики>, !NoPolicy (у обновленной политики не будет родительской политики)<br><br>**config XML** XML-файл, содержащий новую конфигурацию обновленной политики.<br><br>**description** Новое описание обновленной политики.<br><br>**override any child** Новое значение флага «Переопределить все дочерние политики» для обновленной политики. Возможные значения: true, false<br><br>**down replicable** Новое значение флага «Реплицируемая вниз политика» для обновленной политики. Возможные значения: true, false<br><br>**default for clients** Установка политики в качестве политики по умолчанию для клиентов. Возможные значения: true, false | policy update 123 name policy1 parentID 1 configXML policy.xml overrideAnyChild TRUE defaultForLowerServers FALSE |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | **default for lower servers** Установка политики в качестве политики по умолчанию для подчиненных серверов. Возможные значения: true, false<br><br>**replicated clients policy replacement** Новая политика для реплицированных клиентов с обновляемой политикой. Возможные значения: <идентификатор политики>, !DefaultClientsPolicy, !NotAvailable<br><br>**lower servers default policy replacement** Новая политика по умолчанию для подчиненных серверов. Возможные значения: <идентификатор политики>, !DefaultClientsPolicy, !NotAvailable<br><br>**primary clients default policy replacement** Идентификатор новой политики по умолчанию для основных клиентов. | |
| *report* | Отображение шаблонов статических отчетов, шаблонов отчетов панели мониторинга или созданных отчетов. В случае с созданными отчетами отображаются только те отчеты, которые хранятся на сервере. | report <type> | **type** Тип отчета. Возможные значения: static, dashboard, generated | report static |
| *report create* | Создает шаблон статического отчета или шаблон отчета | report create <type> <name> <config XML> [active <active>] | **type** Тип новосозданного шаблона отчета. | report create static new_template C:\config.xml |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | панели мониторинга. | [description <description>] | Возможные значения: static, dashboard<br><br>**name** Имя созданного шаблона отчета.<br><br>**config XML** Путь к XML-файлу с конфигурацией для созданного шаблона отчета. Первый объект <INFO>, найденный в файле, применяется к новосозданному шаблону отчета. Вместо имени, описания и типа шаблона отчета, которые можно найти в XML-файле, используются аналогичные значения из командной строки.<br><br>**active** Активное состояние созданного шаблона отчета. Неприменимо к шаблонам панели мониторинга (игнорируется, если указано). Возможные значения: true, false. Значение по умолчанию: false.<br><br>**description** Описание нового шаблона отчета. | |
| *report delete* | Удаляет шаблон статического отчета или шаблон отчета панели мониторинга. | report delete <report ID> | **report ID** Идентификатор шаблона отчета, который нужно удалить. Чтобы отобразились доступные идентификаторы, выполните следующие команды: 'report static', 'report dashboard'. | report delete 2 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *report export* | Экспортирует шаблон отчетов в локальный XML-файл. Шаблоны с несовместимым типом пропускаются. | report export <type> <templates> <filename> | **type** Тип отчета. Возможные значения: static, dashboard<br>**templates** Разделенный запятыми список идентификаторов шаблонов отчетов (для всех шаблонов этого типа используйте «*»). Чтобы отобразились доступные идентификаторы, выполните команду API report generated.<br>**filename** Путь к XML-файлу, в который нужно экспортировать шаблоны. | report export static * c:\reports_static.xml<br>report export dashboard 2,3 c:\reports_dashboard.xml |
| *report generate* | Используется, чтобы создавать статические отчеты на основе заданного шаблона, то есть выполняет ту же функцию, что и кнопка «Создать статический» в консоли ERA. | report generate <template ID> <directory> | **template ID** Идентификатор нужного шаблона. Чтобы отобразились идентификаторы шаблона, выполните команду API report statistic.<br>**directory** Путь к нужному каталогу, где будут создаваться файлы отчетов. | report generate 3 C:\era_statistics |
| *report import* | Импортирует шаблоны отчетов из локального XML-файла. Шаблоны, указанные в XML-файле и имеющие несовместимый тип, пропускаются. | report import <type> <filename> | **type** Тип отчета. Возможные значения: static, dashboard<br>**filename** Путь к XML-файлу, из которого нужно импортировать шаблоны. | report import static c:\reports_static.xml<br>report import dashboard c:\reports_dashboard.xml |
| *report server* | Функция, аналогичная функции загрузки отчета, который хранится на сервере, с помощью вкладки «Созданные отчеты» на консоли ERA. | report server <generated template ID> <directory> | **generated template ID** Идентификатор созданного шаблона отчетов, хранящегося на сервере. Чтобы отобразить идентификаторы имеющихся | report server 1 C:\era_reports |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | шаблонов отчетов, выполните команду report generated.<br><br>**directory** Путь к нужному каталогу, куда будет загружен файл отчета. | |
| *report update* | Изменение параметров или конфигураций шаблона отчета. | report update <report ID> [configXML <config XML>] [active <active>] [description <description>] | **report ID**Идентификатор шаблона отчетов, который нужно обновить.<br><br>**config XML** Путь к XML-файлу с новой конфигурацией для обновляемого шаблона отчета. Первый объект <INFO>, найденный в файле, применяется к обновляемому шаблону отчета. Если он задан, то вместо значения, которое есть в XML-файле, используется описание из командной строки. В противном случае значение остается неизменным. Указанный в XML-файле тип шаблона отчета игнорируется. Тип шаблона отчета нельзя изменить с помощью обновления.<br><br>**active** Активное состояние обновленного шаблона отчета. Неприменимо к шаблонам панели мониторинга (игнорируется, если указано). Возможные значения: true, false<br><br>**description** Описание обновленного шаблона отчета. | report update 1 configXML C:\new_config.xml |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *request* | Запрос на передачу текущей версии данных с клиента на сервер ERA. Передавать можно такие сведения: данные SysInspector, конфигурация, состояние защиты, функции защиты и информация о системе. Запрошенные данные будут получены, когда требуемая информация станет доступной и клиент подключится к основному серверу. На реплицированных клиентах запрос должен сначала реплицироваться. На клиентах основного сервера конфигурация, функции защиты, состояние защиты и информация о системе обновляются автоматически. | request <data type> <clients> [si_compare <compare date>] [<si_snapshot>] | **data type** Разделенный запятыми список типов запрашиваемых данных. Возможные значения: sysinspector, configuration, protection_status, protection_features, system_information<br><br>**clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов).<br><br>**compare date** Сравнивает запрашиваемый журнал с его предыдущей версией. Предыдущая версия определяется по времени UTC, указанном в формате ГГГГ-ММ-ДД чч:мм:сс (например, 2014-01-21 10:43:00). Используется только при запросе данных SysInspector.<br><br>**si_snapshot** Сохранение журнала локально на клиентской рабочей станции. Используется только при запросе данных SysInspector. | request protection_features *<br><br>request sysinspector,config 1,2,8 si_compare "2014-01-01 01:02:03" si_snapshot |
| *restart* | Перезапускает сервер ERA. Консоль (командная строка) отключается сразу после перезапуска. | restart [<full>] | **full** С помощью этого параметра можно выполнить полную перезагрузку сервера ERA. Действие вносится в журнал аудита. | restart<br><br>restart full |
| *rule* | Отображение правил политики. | rule | | rule |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *rule create* | Создание нового правила политики | rule create <xml> <name> <policy ID> [desc <description>] [priority <priority>] [enabled <enable>] | **xml** Исходный XML-файл, созданный в результате экспорта существующего правила.<br><br>**name** Имя правила политики.<br><br>**policy ID** Идентификатор связанной политики. Можно использовать только следующие типы: политика по умолчанию на клиентах, локальные политики, реплицируемая вниз политика с сервера верхнего уровня. Возможные значения: , !DefaultClientsPolicy<br><br>**description** Описание правила политики.<br><br>**priority** Приоритет правила политики. Возможные значения: top, bottom. Значение по умолчанию: bottom<br><br>**enable** Исходное состояние созданного правила политики. Возможные значения: true, false. Значение по умолчанию: true | rule create "c:\my data \exportedPolicy.xml" myNewPolicy 3 desc "New policy rule" priority top enabled false |
| *rule delete* | Удаление правила политики | rule delete <policy rule ID> | **policy rule ID** Идентификатор правила политики, которое необходимо удалить. | rule delete 3 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *rule import* | Импорт правил политики из XML-файла. Ранее определенные правила изменены не будут. Если имя правила уже существует, новое (импортированное) правило будет переименовано. | rule import <file path> | **file path** Путь к XML-файлу, из которого нужно импортировать правила. | rule import d:\rule.xml |
| *rule export* | Экспорт правил политики в XML-файл. | rule export <rules> <file path> | **rules** Разделенный запятыми список идентификаторов правил (или символ «*» для всех правил).<br>**file path** Путь к XML-файлу, в который нужно импортировать правила. | rule export 1,2 d:\rule.xml |
| *rule update* | Изменение параметров или конфигураций правила политики. Неуказанные параметры не будут изменены. | rule update <policy rule ID> [xml <config xml>] [desc <description>] [policy <policy ID>] [priority <priority>] [enabled <enable>] | **policy rule** Идентификатор правила политики, которое необходимо обновить.<br>**config xml** XML-файл конфигурации, созданный в результате экспорта существующего правила.<br>**description** Новое описание правила политики.<br>**policy ID** Идентификатор новой связанной политики. Возможные значения: , !DefaultClientsPolicy<br>**priority** Изменение приоритетов правила политики. Возможные значения: up, down, top, bottom<br>**enable** Новое состояние правила политики. Возможные значения: true, false | rule update 2 xml d:\rule.xml enabled true |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *runnow* | Незамедлительно запускает указанное действие сервера. | runnow <actions> | **actions** Действия, которые нужно запустить. Возможные значения: cleanup, compact, replicate, replicate_with_mark_all_clients, update, update_with_clear_cache, apply_policy_rules, synchronize_parametric_groups | runnow update<br>runnow cleanup,compact |
| *scanlog* | Отображение содержимого указанного журнала сканирования. | scanlog <ID> | **ID** Идентификатор требуемого журнала сканирования. | scanlog 1 |
| *script* | Выполнение набора команд во внешнем файле. | script <filename> | **filename** Путь к файлу с командами. Команды разделяются точкой с запятой или переходом на новую строку. | script c:\eraGetClientsInfo.txt |
| *servercfg get* | Загрузка текущей серверной конфигурации в указанный локальный файл. | servercfg get <filename> | **filename** Путь к локальному файлу, в который будет сохранена загруженная конфигурация. | servercfg get d:\era_config.xml |
| *servercfg list* | Отображение доступных параметров конфигурации, которые можно изменять непосредственно командами SERVERCFG SET и SERVERCFG SETPWD. | servercfg list | | servercfg list |
| *servercfg put* | Выгрузка серверной конфигурации из локального XML-файла. | servercfg put <filename> | **filename** Путь к выгружаемому локальному XML-файлу. | servercfg put d:<br>ew_config.xml |
| servercfg set | Установка значения для определенного параметра конфигурации. Чтобы показать все доступные параметры, | servercfg set <name=value> | **name=value** Имя параметра и устанавливаемое значение. | servercfg set port_con=2223<br>servercfg set mirror_enabled=1 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | используйте команду SERVERCFG LIST. | | | |
| servercfg setpwd | Установка значения для определенного параметра конфигурации с вводом пароля. Вместо вводимых значений отображаются звездочки, что делает такой метод пригодным для ввода паролей. Чтобы показать все доступные параметры, используйте команду SERVERCFG LIST. Эта команда не может использоваться для установки паролей безопасности на сервере. Вместо нее следует использовать команду PASSWORD. | servercfg setpwd <name> | **name** Имя настраиваемого параметра. | servercfg setpwd ps_password_smtp |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *set* | Получение, установка и сохранение значений параметров команд. Параметры используются для определения выходного файла команд и задания других настроек. Чтобы просмотреть список доступных флагов, используйте команду HELP FLAGS. Установка параметра влияет на все последующие команды в текущем файле сценария или на все последующие команды в режиме оболочки (если используется непосредственно в режиме оболочки). Для одной команды параметр можно переопределить. Это делается путем указания нового параметра после команды. | set [<flag name>] [<flag value>] | **flag name** Использование имени параметра команды без начального дефиса. Чтобы просмотреть список доступных параметров, введите команду HELP FLAGS. Если значение не указано, на экран выводятся текущие значения всех параметров. Также можно использовать аргумент save — текущее состояние параметров будет сохранено в файл запуска (вторым аргументом можно определить путь к другому файлу запуска).<br><br>**flag value** Чтобы просмотреть список доступных значений, введите команду HELP FLAGS. Если значение не указано, на экран выводится текущее значение параметра. | set<br>set enc<br>set enc utf8<br>set format table<br>set paged true<br>set save<br>set save startup.txt |
| *show* | Отображение данных из указанной таблицы. Чтобы узнать только количество строк (вместо списка столбцов), используйте аргумент count. | show <table name> <list of columns> [where <where>] [group by <group by>] [order by <order by>] [skip <skip>] [limit <limit>] | **table name** Чтобы просмотреть список доступных таблиц, введите команду SHOW TABLES.<br><br>**list of columns** Разделенный запятыми список. Чтобы просмотреть список столбцов в определенной таблице, введите команду SHOW COLUMNS. Символ «*» используется для всех столбцов. Чтобы узнать только количество строк, используйте аргумент count. Возможные | show client *<br>show client client_name<br>show client ID, client_name WHERE ID>4, configuration -IN (ready, requested) ORDER BY client_name LIMIT 5<br>show client * WHERE product_name -LIKE *endpoint*<br>show client count WHERE ID>4<br>show client * where group_ID=4<br>show client * where requested_policy_ID -IN (2,3)<br>show event * where client_group_ID=4<br>show event * where client_requested_policy_ID |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | значения: <имя столбца>, *, count, где список разделенных запятыми условий указан в формате <столбец><оператор сравнения><значение> (например, id>3) или <столбец> <IN-оператор> (<список_разделенных_запятыми_значений>). Можно использовать такие операторы сравнения: = (или -EQ), != (или -NE), <= (или -LE), >= (или -GE), < (или -LT), > (или -GT). Можно использовать такие IN-операторы: -IN или -NOTIN. Для текстовых столбцов вместо операторов сравнения можно использовать операторы -LIKE и -NOTLIKE со знаками подстановки («*» — ноль или больше символов, «?» — ровно один символ).<br><br>**group by** Разделенный запятыми список столбцов, по которым требуется группировать данные. Строки с соответствующими значениями во всех таких столбцах будут отображаться одной строкой.<br><br>**order by** Разделенный запятыми список столбцов, за которыми требуется упорядочить данные. После каждого имени столбца можно указать способ | -IN (2,3) |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | упорядочивания: по возрастанию (-ASC) или убыванию (-DESC). По умолчанию данные упорядочиваются по возрастанию.<br><br>**skip** Количество строк, которые нужно пропустить в начале.<br><br>**limit** Максимальное количество строк для отображения. | |
| *show columns* | Отображение доступных столбцов из указанной таблицы. | show columns [for] <table name> | **table name** Таблица, для которой требуется отобразить столбцы. Чтобы просмотреть список доступных имен таблиц, введите команду SHOW TABLES. | show columns for client |
| *show tables* | Отображение доступных таблиц, которые можно использовать в команде SHOW. | show tables | | show tables |
| *task config* | Создание задачи конфигурации с помощью файла конфигурации. Если она успешно создана, отображается идентификатор новой задачи. | task config <configuration file> <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] | **configuration file** XML-файл из редактора конфигураций.<br><br>**clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов).<br><br>**name** Название задачи.<br><br>**description** Описание задачи.<br><br>**apply after** Время UTC, когда задача должна применяться, в одном из следующих форматов: ГГГГ-ММ-ДД чч:мм:сс, ГГГГ-ММ-ДД чч:мм, ГГГГ-ММ-ДД чч, ГГГГ-ММ-ДД. Например (дата и | task config d:\task_config_01.xml 1,4,5 name "Config01" description "email client protection config" |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | время): "2014-01-21 10:43". Например (дата без времени): "2014-01-21".<br><br>**delete if completed** Используется в тех случаях, когда задачу необходимо удалить после успешного выполнения. Возможные значения: true, false. Значение по умолчанию: false. | |
| *task scan* | Создается задача сканирования. Если она успешно создана, отображается идентификатор новой задачи. | task scan <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <profile>] [windows_targets <windows targets>] [windows_no_cleaning <no cleaning>] [windows_shutdown_after_scan <shutdown>] [windows_allow_shutdown_cancel <allow cancel>] [linux3_targets <linux3 targets>] [linux3_no_cleaning <no cleaning>] [linux_profile <profile>] [linux_targets <linux targets>] [linux_no_cleaning <no cleaning>] [mobile_targets <mobile targets>] [mobile_no_cleaning <no cleaning>] [max_delay <max delay>] | **clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов).<br><br>**name** Название задачи.<br><br>**description** Описание задачи.<br><br>**apply after** Время UTC, когда задача должна применяться, в одном из следующих форматов: ГГГГ-ММ-ДД чч:мм:сс, ГГГГ-ММ-ДД чч:мм, ГГГГ-ММ-ДД чч, ГГГГ-ММ-ДД. Например (дата и время): "2014-01-21 10:43". Например (дата без времени): "2014-01-21".<br><br>**delete if completed** Если задачу необходимо удалить после успешного выполнения. Возможные значения: true, false. Значение по умолчанию: false.<br><br>**exclude** Разделенный запятыми список разделов, которые необходимо исключить из задачи сканирования. | task scan 1,3 |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | Возможные значения: windows, linux3, linux, mobile.<br><br>**profile** Сканирование имени профиля. Возможные значения: !InDepthScan, !MyProfile, !SmartScan, !ContextMenuScan, <определенное пользователем имя профиля>. Значение по умолчанию: !InDepthScan<br><br>**windows targets** Разделенный запятыми список объектов Windows, которые требуется просканировать. Возможные значения: !Memory, !RemovableDrivesBoot, !RemovableDrives, !LocalDrivesBoot, !LocalDrives, !RemoteDrives, !AllDrivesBoot, !AllDrives, <заданный путь>.<br><br>Значение по умолчанию: !Memory, !LocalDrivesBoot, !LocalDrives.<br><br>**no cleaning** Сканирование без очистки. Возможные значения: true, false. Значение по умолчанию: false<br><br>**shutdown** Завершение работы компьютера после сканирования. Возможные значения: true, false. Значение по умолчанию: false<br><br>**allow cancel** Разрешить пользователю отменить завершение работы. Возможные | |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| | | | значения: true, false. Значение по умолчанию: false<br><br>**linux3 targets**<br>Разделенный запятыми список путей linux3, которые требуется просканировать. Значение по умолчанию: /<br><br>**linux targets**<br>Разделенный запятыми список путей linux, которые требуется просканировать. Значение по умолчанию: /<br><br>**mobile targets**<br>Разделенный запятыми список объектов на мобильном устройстве, которые требуется просканировать. Возможные значения: !All, <заданный путь>. Значение по умолчанию: !All.<br><br>**max delay**<br>Максимальная продолжительность произвольной задержки в минутах. | |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *task update* | Создание задачи обновления. Если она успешно создана, отображается идентификатор новой задачи. | task update <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <windows profile>] [max_delay <max delay>] | **clients** Разделенный запятыми список идентификаторов клиентов (или символ «*» для всех клиентов).<br><br>**name** Название задачи.<br><br>**description** Описание задачи.<br><br>**apply after** Время UTC, когда задача должна применяться, в одном из следующих форматов: ГГГГ-ММ-ДД чч:мм:сс, ГГГГ-ММ-ДД чч:мм, ГГГГ-ММ-ДД чч, ГГГГ-ММ-ДД. Например (дата и время): "2014-01-21 10:43". Например (дата без времени): "2014-01-21".<br><br>**delete if completed** Используется в тех случаях, когда задачу необходимо удалить после успешного выполнения. Возможные значения: true, false. Значение по умолчанию: false<br><br>**exclude** Список указанных через запятую разделов, которые необходимо исключить из задачи обновления. Возможные значения: windows, linux3, linux, mobile.<br><br>**windows profile** Имя профиля для раздела Windows.<br><br>**max delay** Максимальная продолжительность произвольной задержки в минутах. | task update 2,4,6 name "Update01" exclude windows<br><br>task update * |

| КОМАНДА | ОПИСАНИЕ | СИНТАКСИС | ПАРАМЕТРЫ | ПРИМЕР |
|---|---|---|---|---|
| *version* | Отображение текущей версии консоли командной строки, API и сервера ERA. | version [<component>] | **component** Версия компонента, которую нужно отобразить. Если значение не указано, показываются все версии. Возможные значения: cmd, api, server. | version<br>version cmd |

# 8. Интерфейс API ERA

Взаимодействовать с сервером ERA Server можно также через его API. Интерфейс API использует те же команды 142, что и консоль командной строки ERA 139. Фактически консоль командной строки взаимодействует с сервером ERA Server с помощью API.

Файлы API можно загрузить с сайта http://www.eset.com/int/download/business/detail/family/241/.

Документация по API в Интернете: http://help.eset.com/era/5/en-US/api/

# 9. ERA Maintenance Tool

Средство ESET Remote Administrator Maintenance Tool предназначено для выполнения конкретных задач по обслуживанию сервера. Нажмите кнопку **«Пуск»** > **«Программы»** > **«ESET»** > **«ESET Remote Administrator Server»** > **«ESET Remote Administrator» Maintenance Tool**. При запуске средства ERA Maintenance появится интерактивный мастер, который поможет в выполнении необходимых задач.

Если запустить ESET Remote Administrator Maintenance Tool и нажать кнопку **«Далее»**, появится информационное окно ERA Server. Средство отображает сводку данных об установленном сервере ERA Server. Показанные сведения можно рассмотреть более подробно в отдельном окне, выбрав команду **«Дополнительные сведения»**. Их можно скопировать в буфер обмена командой **«Копировать в буфер»** и обновить с помощью команды **«Обновить»**. После просмотра сведений перейдите к следующему шагу, нажав кнопку **«Далее»** и выберите задачу:

- Остановка ERA Server 175
- Запуск ERA Server 175
- Передача базы данных 176
- Резервное копирование базы данных 176
- Восстановление базы данных 177
- Удаление таблиц 177
- Резервное копирование хранилища 177
- Восстановление хранилища 177
- Установка нового лицензионного ключа 178
- Изменение конфигурации сервера 178

В конце каждой задачи настройки можно сохранить параметры текущей задачи, нажав кнопку **«Сохранить все параметры в файл»**. Эти параметры затем можно использовать в любое время с помощью кнопки **«Загрузить все параметры из файла»**. В каждом шаге задачи настройки также есть функция **«Сохранить все параметры в файл»** или **«Загрузить все параметры из файла»**.

## 9.1 Остановка сервера ERA Server

Данная задача останавливает службу ESET Remote Administrator Server.

**ПРИМЕЧАНИЕ.**: Имя службы — ERA_SERVER. Исполняемый файл этой службы — *C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*.

## 9.2 Запуск сервера ERA Server

Данная задача запускает службу ESET Remote Administrator Server.

**ПРИМЕЧАНИЕ.**: Имя службы — ERA_SERVER. Исполняемый файл этой службы — *C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*.

## 9.3 Передача базы данных

Данная задача позволяет преобразовать формат базы данных. Это средство может выполнять преобразование между следующими типами баз данных:

- MS Access
- MS SQL Server
- Oracle
- MySQL

Прежде всего следует проверить подключение к базе данных. Этот шаг является общим для всех задач кроме отправки нового лицензионного ключа и изменения конфигурации сервера.

Если базой данных является MS Access, укажите путь к *MDB*-файлу. По умолчанию используется путь, указанный во время установки ERA Server.

Для всех остальных форматов БД необходимо указать дополнительные параметры.

- Строка соединения: специальная строка, используемая для идентификации исходной базы данных.
- Имя пользователя: имя пользователя для доступа к базе данных.
- Пароль: пароль для доступа к базе данных.
- Название схемы: название схемы (только для Oracle и MS SQL).

Выберите пункт **«Загрузить текущую конфигурацию сервера»**, чтобы использовать текущие параметры ERA Server. Нажмите кнопку **«Проверить соединение»**, чтобы проверить соединение с сервером базы данных. Если соединение не удается установить, проверьте правильность параметров. После успешной проверки связи с БД переходите к следующему шагу, нажав кнопку **«Далее»**.

Затем выберите целевую базу данных. Выберите пункт **«Заменить параметры подключения к серверу»**, чтобы подключиться к серверу и использовать новую базу данных после успешного преобразования. Если не выбрать этот параметр, новая база данных будет создана без обновления сервера до новой версии базы данных.

Для всех типов баз данных (кроме MS Access) решите, нужно ли автоматически создавать таблицы базы данных (**«Автоматически создать таблицы в новой базе данных»**) или вставьте таблицы в базу данных позже (**«Просмотреть сценарий»** > **«Сохранить в файл»**) в следующем шаге. Для базы данных MySQL параметр **Автоматически создать базу данных (ESETRADB)** автоматически создает новую базу данных MS SQL с именем ESETRADB. Последним шагом является подтверждение преобразования базы данных.

## 9.4 Резервное копирование базы данных

Это средство позволяет создавать файл резервной копии базы данных. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 176). В этом окне выбрана исходная база данных. Исходная база данных будет скопирована в файл резервной копии, указанный в следующем шаге.

Необязательные параметры в нижней части окна позволяют перезаписать существующий файл (**«Перезаписать, если существует»**), а также остановить ESET Remote Administrator Server во время резервного копирования (**«Остановить сервер во время обработки»**). Чтобы подтвердить выполнение задачи, нажмите кнопку далее **«Далее»**.

## 9.5 Восстановление базы данных

Данная задача позволяет восстановить базу данных из файла резервной копии. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 176). В этом окне выбран тип база данных.

Для всех типов баз данных (кроме MS Access) решите, нужно ли автоматически создавать таблицы базы данных (**«Автоматически создать таблицы в новой базе данных»**) или вставьте таблицы в базу данных позже (**«Просмотреть сценарий»** > **«Сохранить в файл»**) в следующем шаге. Для базы данных MS SQL параметр **«Автоматически создать базу данных (ESETRADB)»** автоматически создает новую базу данных MS SQL с именем ESETRADB. Последним шагом является подтверждение восстановления базы данных.

Выберите файл, из которого будет восстановлена БД в следующем шаге. Необязательные параметры в нижней части окна позволяют импортировать файлы из баз данных различных типов, выбранных в предыдущем шаге (**«Разрешить импорт баз данных различных типов»**), а также останавливать ESET Remote Administrator Server во время восстановления базы данных (**«Остановить сервер во время обработки»**). Нажмите кнопку далее **«Далее»** для подтверждения выполнения задачи.

## 9.6 Удаление таблиц

Данная задача удаляет содержимое текущих таблиц в базе данных. В результате база данных будет возвращена в состояние, которое было сразу после установки ERA Server. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 176). В этом окне выбран тип база данных. В следующем шаге будет выведен запрос на подтверждение действия. выберите **«Да, принимаю»** и нажмите кнопку **«Далее»** для подтверждения действия.

**Примечание.** Если используется база данных MS SQL, MySQL или Oracle, перед удалением этих таблиц рекомендуется остановить ERA Server.

Если используется СУБД MS Access, она будет заменена пустой базой данных по умолчанию.

## 9.7 Резервное копирование хранилища

Эта задача выполняет резервное копирование хранилища. Все данные из папки хранилища (по умолчанию — *C:\ProgramData\ESET\ESET Remote Administrator\Server\storage*)будут сохранены во внешний файл дампа (DMP-файл). В этой папке хранятся важные журналы и конфигурации сервера. Щелкните значок конверта в нижней части окна, чтобы перейти в папку, в которой нужно создать резервную копию хранилища, и введите имя файла. Также можно установить флажок **«Перезаписывать существующие объекты»**, чтобы перезаписать существующие DMP-файлы. Рекомендуется не снимать флажок **«Останавливать сервер на время обработки»**, поскольку задача резервного копирования хранилища может привести к снижению производительности сервера. Нажмите кнопку **«Далее»**, а затем **«Пуск»**, чтобы запустить задачу.

## 9.8 Восстановление хранилища

Эта задача выполняет восстановление хранилища из сохраненного ранее файла дампа (DMP-файла). Дополнительные сведения см. в описании задачи резервного копирования хранилища. Щелкните значок конверта в нижней части окна, чтобы перейти в папку, в которой находится файл дампа. Рекомендуется не снимать флажок **«Останавливать сервер на время обработки»**, поскольку задача восстановления хранилища может привести к снижению производительности сервера. Нажмите кнопку **«Далее»**, а затем **«Пуск»**, чтобы запустить задачу.

## 9.9 Установка нового лицензионного ключа

Чтобы добавить новый лицензионный ключ для использования на сервере, укажите путь к новому лицензионному ключу.

Замените существующий ключ лицензии в случае необходимости (**«Перезаписать, если существует»**) и перезапустить сервер при необходимости (**«Принудительно запустить сервер (если он не запущен)»**). Нажмите кнопку далее **«Далее»** для подтверждения и выполнения задачи.

## 9.10 Изменение конфигурации сервера

Эта задача запускает Configuration Editor (если он установлен). По окончании задачи открывается окно редактора конфигураций, в котором можно изменять дополнительные параметры ERA Server. Эти параметры также доступны в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»**.

**Примечание.** Для работы этой функции должен быть установлен ERA Console. Также можно сохранить параметры сервера в XML-файле и затем использовать их с помощью параметра **«Загрузить все настройки из файла»**.

## 9.11 Интерфейс командной строки

ESET Remote Administrator Maintenance Tool (ERAtool.exe) также может работать как средство командной строки, которое можно встраивать в сценарии. При запуске этой программы она обрабатывает указанные параметры и выполняет все действия в заданной последовательности. Если не указан ни один аргумент, запускается интерактивный мастер.

Поддерживаются следующие команды:

- */startserver* или */startservice* — запуск службы ESET Remote Administrator Server;
- */stopserver* или */stopservice* — остановка службы ESET Remote Administrator Server;
- */gui* — запуск интерактивного мастера после завершения всех задач.

Любой параметр, не начинающийся с символа косой черты (/), считается именем файла сценария конфигурации, который должен быть выполнен. Сценарии конфигурации создаются путем сохранения параметров в интерактивном мастере.

**ПРИМЕЧАНИЕ.**: Для запуска программы ERAtool.exe требуется повышенный уровень прав администратора. Если у сценария, вызывающего ERAtool.exe, недостаточно прав, в Windows может появиться запрос повышения прав или запуска программы в отдельном консольном процессе (при этом выходные данные будут потеряны).

# 10. Устранение неполадок

## 10.1 Часто задаваемые вопросы

В этой главе даны ответы на наиболее часто задаваемые вопросы и решения для проблем, связанных с установкой и функционированием ERA.

### 10.1.1 Проблемы, связанные с установкой ESET Remote Administrator на Windows Server 2000/2003

**Причина**

Одной из возможных причин может быть работа сервера терминалов в режиме *выполнения*.

**Решение**

Корпорация Microsoft рекомендует устанавливать сервер терминалов в режим *установки*, если он запущен при установке в системе программ. Это можно сделать в оснастке **«Панель управления»** > **«Установка или удаление программ»** или с помощью команды *change user /install* в командной строке. После установки введите *change user /execute* для возврата сервера терминалов в режим выполнения. Описание пошаговых инструкций этого процесса см. в следующей статье: http://support.microsoft.com/kb/320185.

### 10.1.2 Значения кода ошибки GLE

При установке ESET Endpoint Security или ESET Endpoint Antivirus в консоли ESET Remote Administrator Console может возникать ошибка GLE. Чтобы определить номер ошибки GLE, выполните следующие действия.

1) Откройте окно командной строки, выбрав в меню пункт **«Пуск»** > **«Выполнить»**. Введите *cmd* и нажмите кнопку **ОК**.
2) В командной строке введите *net helpmsg номер_ошибки.*

**Пример** *net helpmsg 55*

**Пример результата:** The specified network resource or device is no longer available («Указанный сетевой ресурс или устройство больше не доступны»).

## 10.2 Часто встречающиеся коды ошибок

Во время работы ERA могут выводиться сообщения об ошибках, коды которых указывают на проблему с некоторой функцией или действием. В разделах ниже дано краткое описание кодов ошибок, которые возникают при автоматической установке, а также ошибок, которые содержатся в журнале сервера ERAS.

### 10.2.1 Сообщения об ошибках, выводимые при удаленной установке ESET Smart Security или ESET NOD32 Antivirus с использованием ESET Remote Administrator

**«Код ошибки SC 6, код ошибки GLE 53. Не удалось установить подключение IPC к целевому компьютеру.»**
Для установки подключения IPC должны выполняться следующие требования.

1. На компьютере с сервером ERAS и на целевом компьютере должен быть установлен стек TCP/IP.
2. Должна быть установлена служба «Общий доступ к файлам и принтерам Microsoft».
3. Должны быть открыты порты общего доступа к файлам (135–139, 445).
4. Целевой компьютер должен отвечать на PING-запросы.

**«Код ошибки SC 6, код ошибки GLE 67. Не удается разместить установщик ESET на целевом компьютере.»**
На системном диске клиента должен быть доступен административный общий ресурс *ADMIN$*.

**«Код ошибки SC 6, код ошибки GLE 1326. Не удалось установить подключение IPC к целевому компьютеру, вероятно, из-за неправильного имени пользователя или пароля.»**
Введено неправильное имя пользователя учетной записи администратора (либо оно не вводилось вообще).

**«Код ошибки SC 6, код ошибки GLE 1327. Не удалось установить подключение IPC к целевому компьютеру.»**
Поле пароля администратора не заполнено. Удаленная установка не запускается с пустым полем пароля.

**«Код ошибки SC 11, код ошибки GLE 5. Не удается разместить установщик ESET на целевом компьютере.»**
Установщику не удается получить доступ к клиентскому компьютеру из-за отсутствия достаточных прав (нет доступа).

**Код ошибки SC 11, код ошибки GLE 1726. Не удается разместить установщик ESET на целевом компьютере.**
Эта ошибка выводится после попытки повторной установки, если окно «Автоматическая установка» не было закрыто после первой попытки.

**Ошибка установки пакета — код выхода 1603. Описание: неустранимая ошибка**
Код выхода 1603 является универсальным и может иметь разные причины. В случае автоматической установки есть две самые частые причины, и они указаны ниже.

1. Целевого компьютера нет в домене. Решение: нужно отключить UAC (контроль учетных записей) на целевом компьютере. Применимо на компьютерах под управлением Windows Vista, Windows 7 и Windows 8 (8.1).
2. Клиентское решение ESET было удалено перед установкой, но целевой компьютер не был перезагружен. Решение: перезагрузить целевой компьютер.

### 10.2.2 Часто встречающиеся коды ошибок в журнале era.log

**0x1203 - UPD_RETVAL_BAD_URL**
Ошибка модуля обновления — неправильно введенное имя сервера обновления.

**0x1204 - UPD_RETVAL_CANT_DOWNLOAD**
Эта ошибка может возникать в следующих случаях.

- При обновлении по протоколу HTTP:
  - сервер обновления выводит код ошибки HTTP в интервале 400— 500 кроме 401, 403, 404 и 407;
  - Если обновления загружаются с сервера CISCO, при этом изменился формат ответа проверки подлинности HTTP.
- При обновлении из общей папки:
  выводимые ошибки не относятся к категориям «неправильная аутентификация» или «файл не найден» (например, *прерывание соединения*, *несуществующий сервер* и т. п.).
- При использовании обоих способов обновления:
  не удается найти ни один из серверов, указанных в файле *upd.ver* (файл находится в каталоге *%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\updfiles*)
  - не удалось подключиться к надежному серверу (вероятно, из-за удаления соответствующих записей ESET в реестре);
- неправильная настройка прокси-сервера на сервере ERAS
  - Администратор должен указать адрес прокси-сервера в правильном формате.

**0x2001 - UPD_RETVAL_AUTHORIZATION_FAILED**
Не удалось пройти аутентификацию на сервере обновления, введены неправильное имя пользователя или пароль.

**0x2102 - UPD_RETVAL_BAD_REPLY**
Эта ошибка модуля обновления возникает при подключении к Интернету с использованием прокси-сервера Webwasher.

**0x2104 - UPD_RETVAL_SERVER_ERROR**
Ошибка модуля обновления, указывающая на то, что код ошибки HTTP превышает значение 500. При работе с HTTP-сервером ESET значение ошибки 500 означает проблему с распределением памяти.

**0x2105 - UPD_RETVAL_INTERRUPTED**

Эта ошибка модуля обновления возникает при подключении к Интернету с использованием прокси-сервера Webwasher.

## 10.3 Диагностика проблем на сервере ERAS

Если возникли подозрения, что на сервере ERAS есть проблемы или он работает неправильно, рекомендуется выполнить указанные ниже действия.

1) Проверьте журнал ERAS: в главном меню консоли ERAC выберите **«Служебные программы»** > **«Настройки сервера»**. В окне **«Настройки сервера»** щелкните вкладку **«Ведение журнала»** и нажмите кнопку **«Просмотр журнала»**.

2) Если сообщения об ошибках отсутствуют, увеличьте уровень **«Детализации журнала»** в окне **«Настройки сервера»** до уровня 5. После выявления проблемы рекомендуется вернуть значение по умолчанию.

3) Проблемы также можно обнаруживать посредством включения журнала отладки базы данных на той же самой вкладке (см. раздел **«Журнал отладки»**). **«Журнал отладки»** рекомендуется активировать только при попытке воспроизведения проблемы.

4) В случае появления кодов ошибок, не указанных в данном документе, обращайтесь в службу поддержки клиентов ESET. Опишите работу программы, способ репликации или способ избежать возникновения проблемы. Очень важно указать версии всех используемых продуктов безопасности ESET (т. е. сервера ERAS, консоли ERAC, ESET Endpoint Security, ESET Endpoint Antivirus).

# 11. Советы и подсказки

## 11.1 Планировщик

В ESET Endpoint Antivirus и ESET Endpoint Security встроен планировщик задач, который позволяет планировать регулярные проверки, обновления и т. п. В планировщике перечислены все возможные задачи.

С помощью ERA можно настроить следующие четыре типа задач:

- Запуск внешнего приложения
- Обслуживание журнала
- Сканирование компьютера
- Создать снимок состояния компьютера
- Обновление
- Автоматически проверять файлы при запуске системы

В большинстве случаев настраивать задачу **«Запуск внешнего приложения»** нет необходимости. Задача **«Автоматическая проверка файлов, исполняемых при запуске системы»** является задачей по умолчанию, поэтому не рекомендуется изменять ее параметры. Если после установки не делались никакие изменения, ESET NOD32 и ESET Endpoint Security содержат две предопределенные задачи этого вида. Первая задача выполняет проверку файловой системы при каждом входе в систему, а вторая задача выполняет ту же самую задачу после обновления БД сигнатур вирусов. С точки зрения администратора задачи **«Сканирование компьютера»** и **«Обновление»** возможно, представляются самыми необходимыми.

- **«Сканирование ПК»** — обеспечивает регулярную проверку на наличие вирусов (обычно на локальных дисках) на клиентах.
- **«Обновить»** — эта задача отвечает за обновление клиентских решений ESET. Она является предопределенной и выполняется каждый час. Обычно изменять ее параметры не требуется. Единственным исключением являются ноутбуки, поскольку их владельцы часто подключаются к Интернету за пределами локальных сетей. В таком случае для этой задачи можно настроить использование двух профилей обновления. Это позволит ноутбукам обновляться с локального зеркала, а также с серверов обновления компании ESET.

Планировщик можно настроить в **ESET Configuration Editor** с помощью меню **«Программы для Windows, версии 3 и 4»** > **«Ядро ESET»** > **«Параметры»** > **«Планировщик»** > **«Изменить»**.

Дополнительные сведения см. в разделе ESET Configuration Editor 67.

В диалоговом окне могут быть перечислены существующие задачи (нажмите кнопку **«Изменить»** чтобы изменить их параметры), или оно может быть пустым. Это зависит от того, открыта ли конфигурация на клиенте (например, на ранее настроенном и работающем компьютере) или новый файл с шаблоном по умолчанию, в котором отсутствуют задачи.

Каждой новой задаче присваивается идентификатор: задачам по умолчанию — десятичные (1, 2, 3...), а пользовательским — шестнадцатеричные (например, *4AE13D6C*), которые автоматически создаются для каждой новой задачи.

Если для задачи установлен флажок, это значит, что она активна и будет выполнена на указанном клиентском ПК.

Кнопки в окне запланированных задач выполняют следующие функции:

- **«Добавить»** — добавляет новую задачу;
- **«Изменить»** — изменяет выбранные задачи;
- **«Изменить идентификатор»** — изменяет идентификаторы выбранных задач;

- **Подробности** — выводит сводные данные о выбранной задаче;
- **«Выбрать для удаления»** — приложение для работы с *XML*-файлами удаляет выбранные задачи на целевых клиентах;
- **«Удалить из списка»** — удаляет выбранные задачи из списка. Обратите внимание, что задачи, удаленные из списка в XML-конфигурации, не удаляются на целевых рабочих станциях.

При создании новой задачи (кнопка **«Добавить»**) или изменении параметров существующей задачи (кнопка **«Изменить»**) необходимо указывать время ее запуска. Выполнение задачи может повторяться через определенные периоды времени (ежедневно в 12 часов, каждую пятницу и т. п.) или активироваться событием (после успешного обновления, ежедневно при первом запуске компьютера и т. п.).

На последнем этапе задачи **«Сканирование компьютера по требованию»** появляется окно специальных настроек, в котором можно задавать конфигурацию проверки,т. е. профиль и целевые объекты сканирования.

На последнем этапе задачи **«Обновление»** указываются профили обновления, которые будут запускаться в рамках данной задачи. Эта задача является предопределенной и по умолчанию выполняется каждый час. Обычно изменять ее параметры не требуется. Единственным исключением являются ноутбуки, поскольку их владельцы подключаются к Интернету и за пределами локальных сетей. В последнем диалоговом окне можно указать два разных профиля обновления для обновлений с локального сервера и с серверов обновления ESET.

## 11.2 Удаление существующих профилей

Иногда встречаются одинаковые профили обновления или проверки, которые были созданы по ошибке. Чтобы удаленно удалить эти профили, не затрагивая другие настройки «Планировщика», выполните указанные ниже действия.

- В консоли ERAC откройте вкладку **«Клиенты»** и щелкните дважды клиента с проблемой.
- В окне **«Свойства клиента»** откройте вкладку **«Конфигурация»**. Выберите параметры **«С последующим запуском ESET Configuration Editor для редактирования файла»** и **«Использовать загруженную конфигурацию в новой задаче»** и нажмите кнопку **«Новая задача»**.
- В мастере создания новой задачи нажмите кнопку **«Изменить»**.
- В Configuration Editor нажмите сочетание клавиш **CTRL + D** для отмены выбора (затенения) всех параметров. Это позволяет предотвратить внесение случайных изменений, поскольку новые изменения выделяются синим цветом.
- Щелкните правой кнопкой мыши профиль, который нужно удалить, и выберите в контекстном меню команду **«Отметить профиль для удаления»**. Профиль будет удален после доставки задачи на клиенты.

Нажмите кнопку **«Консоль»** в ESET Configuration Editor и сохраните параметры.

- Убедитесь в том, что выбранный клиент находится в столбце **выбранных** справа. Нажмите кнопку **«Далее»**, а затем — **«Готово»**.

## 11.3 Экспорт и прочие функции XML-конфигурации клиента

В консоли ERAC выберите любой клиент на вкладке **«Клиенты»**. Щелкните по клиенту правой кнопкой мыши и выберите в контекстном меню команду **«Конфигурация...»**. Выберите команду **Сохранить как…**, чтобы экспортировать конфигурацию указанного клиента в *XML*-файл (*XML*-файлы конфигурации можно также извлечь непосредственно в программе ESET Endpoint Security). Этот *XML*-файл затем можно будет использовать в следующих операциях.

- При удаленной установке *XML*-файл можно использовать как шаблон предопределенной конфигурации. Это означает, что новый *XML*-файл не создается, а новому пакету установки назначается существующий *XML*-файл (кнопка **«Выбрать…»**). *XML*-файл конфигурации также можно получить непосредственно из интерфейса программы ESET Endpoint Security.

- При настройке нескольких клиентов они получают ранее загруженный *XML*-файл и используют определенные в нем настройки (новая конфигурация не создается, а просто назначается с помощью кнопки **«Выбрать...»**).

**Пример**

Продукт безопасности ESET устанавливается только на одной рабочей станции. Настройте параметры программы непосредственно в интерфейсе пользователя программы. Сделав это, экспортируйте настройки в *XML*-файл. *XML*-файл также впоследствии можно использовать для удаленной установки на других рабочих станциях. Данный метод очень удобен для решения таких задач как точная настройка правил файервола, если используется режим *«На основе политики»*.

## 11.4 Комбинированное обновление для ноутбуков

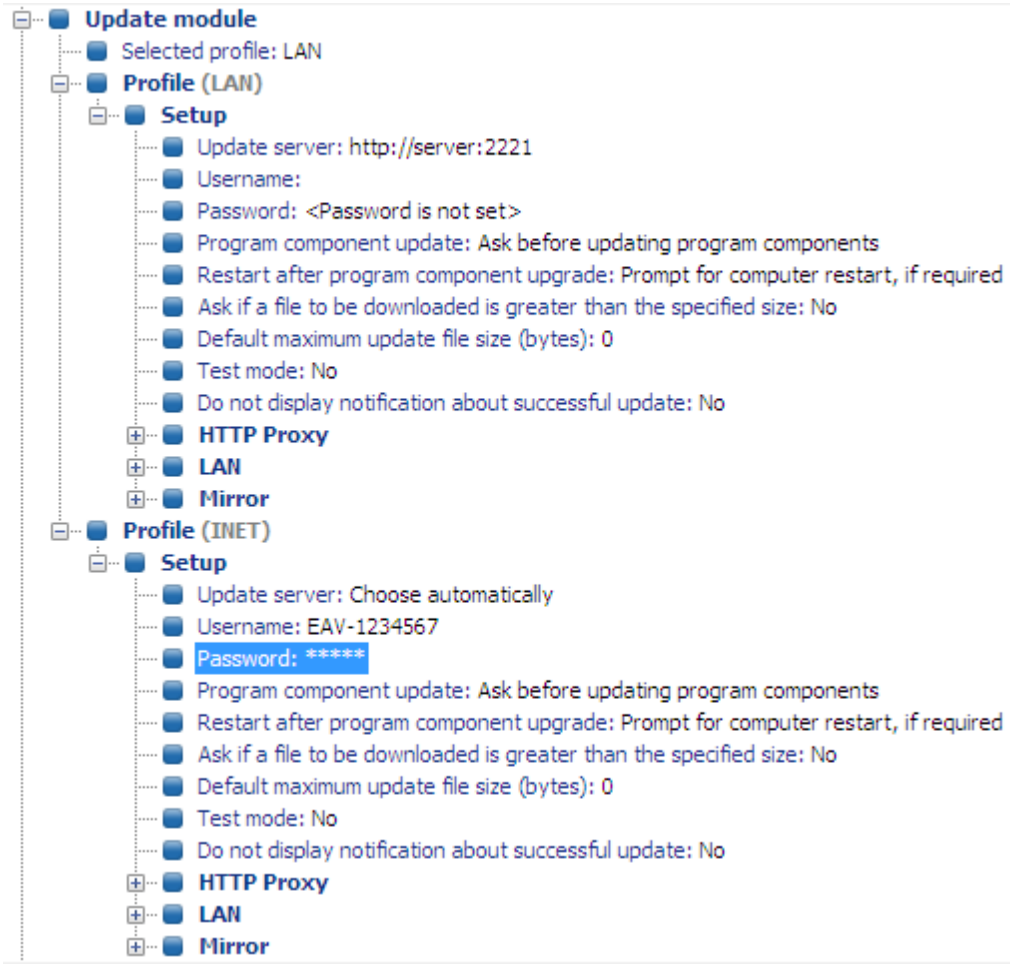
Если в локальной сети есть мобильные устройства (например, ноутбуки), рекомендуется настроить комбинированное обновление из двух источников: с серверов обновления ESET и с локального сервера обновления (зеркала). Сначала ноутбуки обращаются к зеркальному серверу, и если не удается установить соединение (они находятся вне офиса), обновления загружаются непосредственно с серверов ESET. Чтобы этот метод работал, необходимо выполнить такие действия.

- Создайте два профиля обновления: один (Экспорт и прочие функции XML-конфигурации клиента 183) с подключением к серверу зеркала (с названием LAN в примере ниже), а второй — к серверам обновления ESET (INET)
- Создайте задачу обновления или измените существующую с помощью планировщика (меню **Сервис** > **Планировщик** в главном окне программы ESET Endpoint Security или ESET Endpoint Antivirus).

Настройку можно выполнять непосредственно на ноутбуках или удаленно с помощью ESET Configuration Editor. Созданную конфигурацию можно применять во время установки или позже в виде задачи конфигурации.

Чтобы создать новый профиль в ESET Configuration Editor, щелкните правой кнопкой мыши по ветке **«Обновление»** и выберите в контекстном меню пункт **«Новый профиль»**.

Результат изменений будет примерно соответствовать приведенному ниже примеру.




Профиль LAN загружает обновления с локального зеркала компании (*http://server:2221*), а профиль INET подключается к серверам ESET (**«Выбирать автоматически»**). Затем нужно указать задачу обновления, которая последовательно запускает каждый из профилей обновления. Для этого выберите **«Программы для Windows, версии 3 и 4»** > **«Ядро ESET»** > **«Параметры»** > **«Планировщик»** в ESET Configuration Editor. Нажмите кнопку **«Изменить»**, чтобы открыть окно **«Запланированные задачи»**.

Для создания новой задачи нажмите кнопку **«Добавить»**. В раскрывающемся меню **«Запланированная задача»** выберите пункт **«Обновить»** и нажмите кнопку **«Далее»**. Введите **название задачи** (например, *«Комбинированное обновление»*), установите флажок **«Многократно каждые 60 минут»** и перейдите к выбору основного и дополнительного профилей.

Если рабочие станции на ноутбуках должны сначала обращаться к серверу зеркала, главным должен быть профиль LAN, а дополнительным — профиль INET. Профиль INET должен использоваться только при сбое обновления по профилю LAN.

**Рекомендация.** Экспортируйте текущую *XML*-конфигурацию с клиента (дополнительные сведения см. в разделе Диагностика проблем на сервере ERAS? 181) и внесите указанные изменения в экспортированный *XML*-файл. Это позволит избежать дублирования в расписании и неиспользуемых профилях.

## 11.5 Установка продуктов сторонних производителей с помощью программы ERA

Помимо удаленной установки продуктов ESET, программа ESET Remote Administrator может устанавливать и другие программы. Единственным требованием является то, чтобы пользовательский пакет был в формате *MSI*. Удаленную установку пользовательских пакетов можно выполнить с использованием процесса, аналогичного тому, который описан в разделе Удаленная автоматическая установка 74.

Основное отличие заключается в процессе создания пакета, который описан ниже.

1) В консоли ERA откройте вкладку ERAC **«Удаленная установка»**.
2) Выберите вкладку **Компьютеры** и нажмите кнопку **Диспетчер пакетов**.
3) В раскрывающемся меню «Тип пакета» выберите пункт **«Пользовательский пакет»**.
4) Нажмите кнопку **Создать**, выберите команду **Добавить файл** и выберите нужный *MSI*-пакет.
5) Выберите файл в раскрывающемся меню **Входной файл пакета** и нажмите кнопку **Создать**.
6) Чтобы сохранить пакет, нажмите **Сохранить как** по возвращении в исходное окно.
7) Кроме того, задайте для *MSI*-файла параметры командной строки, если это необходимо. Эти параметры будут такими же, как и при локальной установке этого пакета. После этого обязательно щелкните **Сохранить** в разделе пакетов окна **Диспетчер пакетов**.
8) Нажмите кнопку **«Закрыть»**, чтобы закрыть редактор пакета установки.

Созданный пользовательский пакет можно разослать по клиентским рабочим станциям так же, как и при удаленной установке, описанной в предыдущих главах. При удаленной автоматической установке, установке через сценарий входа или отправке по электронной почте пакет отправляется на целевые рабочие станции. После открытия пакета управление установкой переходит к службе установки Microsoft Windows. После выполнения выборочной установки программа ERAS может загрузить с клиента файл, содержащий сведения о результатах установки. Чтобы указать файл с результатами, после сохранения пользовательского пакета добавьте параметр **/eResult** в командную строку, связанную с пакетом. После запуска задачи выборочной установки можно загрузить файлы с результатами из программы ERAS в окне **Подробности задачи**.

**ПРИМЕЧАНИЕ.** Для пользовательских сторонних пакетов установки действует ограничение размера в 100 МБ.

# 12. ESET SysInspector

## 12.1 Знакомство с ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в обобщенном виде. Такая информация, как данные об установленных драйверах и приложениях, сетевых соединениях и важных записях в реестре, позволяет определить причину подозрительного поведения системы, которое могло иметь место, например, вследствие несовместимости программного или аппаратного обеспечения или заражения вредоносными программами.

Доступ к программе ESET SysInspector можно получить двумя способами: воспользовавшись ее интегрированной версией в решениях ESET Security или бесплатно загрузив автономную версию (SysInspector.exe) с веб-сайта ESET. Обе версии работают одинаково и имеют одинаковое управление. Единственная разница состоит в способе управления полученными данными. И автономная, и интегрированная версии дают возможность экспортировать снимки системы в *XML*-файлы и сохранять их на диске. Однако интегрированная версия позволяет также сохранять снимки системы непосредственно в меню **Служебные программы** > **ESET SysInspector** (за исключением программы ESET Remote Administrator).

Подождите некоторое время, пока программа ESET SysInspector сканирует компьютер. Это может занять от 10 секунд до нескольких минут в зависимости от конфигурации оборудования, операционной системы и количества установленных на компьютере приложений.

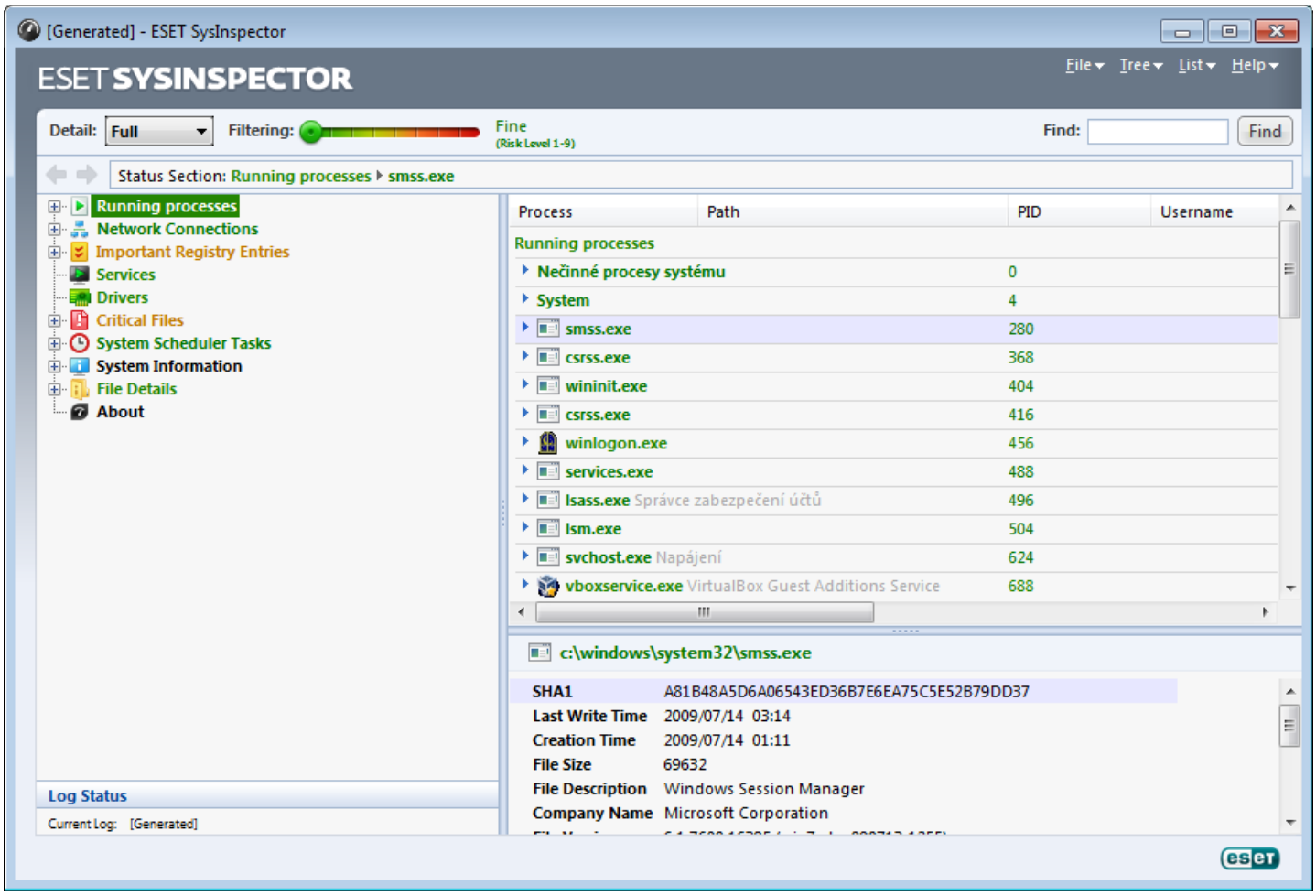
### 12.1.1 Запуск ESET SysInspector

Чтобы запустить ESET SysInspector, достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET.

Подождите, пока программа проверяет систему — это может занять несколько минут в зависимости от оборудования и собираемых данных.

## 12.2 Интерфейс пользователя и работа в приложении

Для удобства главное окно разделено на четыре основных раздела: вверху находятся элементы управления программой, слева — окно навигации, справа по центру — окно описания, а справа внизу — окно подробных сведений. В разделе «Состояние журнала» отображаются основные параметры журнала (используемый фильтр, тип фильтра, является ли журнал результатом сравнения и т. д.).




### 12.2.1 Элементы управления программой

В этом разделе описаны все элементы управления приложением ESET SysInspector.

#### Файл

Щелкнув элемент **Файл**, можно сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, при его создании рекомендуется использовать параметр **Подходит для отправки**. В этом случае из него исключается конфиденциальная информация (например, имя текущего пользователя, имя компьютера и домена, права текущего пользователя, переменные среды и т. п.).

**ПРИМЕЧАНИЕ.** Чтобы открыть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно программы.

#### Дерево

Позволяет развернуть или закрыть все узлы, а также экспортировать выбранные разделы в сценарий обслуживания.

#### Список

Содержит функции, облегчающие навигацию в программе, а также прочие функции, например средства поиска информации в Интернете.

**Справка**

Содержит сведения о приложении и его функциях.

**Подробнее**

Этот параметр облегчает работу с информацией, отображаемой в главном окне программы. В базовом режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В среднем режиме отображаются расширенные данные. В полном режиме программа ESET SysInspector отображает всю информацию, необходимую для решения самых нестандартных проблем.

**Фильтрация элементов**

Используется для поиска подозрительных файлов или записей в реестре системы. С помощью ползунка можно фильтровать элементы по их уровню риска. Если ползунок установлен в крайнее левое положение (уровень риска 1), отображаются все элементы. При перемещении ползунка вправо программа отфильтровывает все элементы с уровнем риска, меньшим текущего уровня, и выводит только те элементы, уровень подозрительности которых выше выбранного уровня. Если ползунок находится в крайнем правом положении, программа отображает только известные вредоносные элементы.

Все элементы с уровнем риска от 6 до 9 могут быть опасными для системы. Если вы не используете решение компании ESET для обеспечения безопасности, после нахождения программой ESET SysInspector такого элемента рекомендуется проверить систему с помощью ESET Online Scanner. ESET Online Scanner является бесплатной службой.

**ПРИМЕЧАНИЕ.** Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.

**Поиск**

Служит для быстрого нахождения определенного элемента по его названию или части названия. Результаты поиска отображаются в окне описания.

**Возврат**

С помощью стрелок назад и вперед в окне описания можно возвращаться к ранее отображенной информации. Вместо стрелок назад и вперед можно использовать соответственно клавишу BACKSPACE и пробел.

**Раздел состояния**

Отображает текущий узел в окне навигации.

***Внимание!*** Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как потенциально опасные. Если элемент выделен красным, это не означает, что его можно удалить. Перед удалением убедитесь в том, что эти файлы действительно опасны и не являются необходимыми.

### 12.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разного типа по нескольким базовым разделам, называемым узлами. Чтобы получить дополнительные сведения, разверните подузлы соответствующего узла. Чтобы открыть или свернуть узел, дважды щелкните название узла либо значок ⊞ или ⊟ рядом с именем узла. При перемещении по древовидной структуре узлов и подузлов в окне навигации о каждом узле доступны различные сведения, отображаемые в окне описания. При переходе в окне описания к конкретному элементу в окне подробной информации появляются дополнительные сведения о нем.

Ниже описаны главные узлы в окне навигации и относящиеся к ним сведения в окнах описания и подробной информации.

**Запущенные процессы**

Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия

динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения и уровень риска файла.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

**ПРИМЕЧАНИЕ.** Любая операционная система состоит из нескольких важных компонентов ядра, которые постоянно запущены и обеспечивают работу базовых и жизненно важных функций для других пользовательских приложений. В определенных случаях путь к файлам таких процессов начинается в программе ESET SysInspector с символов «\??\». Эти символы обеспечивают таким процессам оптимизацию до запуска и с точки зрения системы являются безопасными.

**Сетевые подключения**

В окне описания перечислены процессы и приложения, которые обмениваются данными через сеть по протоколу, выбранному в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Также в нем можно найти IP-адреса DNS-серверов.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

**Важные записи реестра**

Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе: например, записи с указанием автоматически загружаемых программ, вспомогательных объектов браузера и т. п.

В окне описания можно узнать, какие файлы связаны с определенными записями реестра. Дополнительная информация отображается в окне подробных сведений.

**Службы**

В окне описания перечислены файлы, зарегистрированные как службы Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть некоторую дополнительную информацию.

**Драйверы**

Список драйверов, установленных в системе.

**Критические файлы**

В окне описания отображается содержимое критически важных файлов операционной системы Microsoft Windows.

**Задачи системного планировщика**

Отображается список задач, инициируемых планировщиком заданий Windows в определенное время/период времени.

**Информация о системе**

Содержит подробные сведения об оборудовании и программном обеспечении, а также сведения о заданных переменных среды, правах пользователей и журналах системных событий.

**Сведения о файле**

Список важных системных файлов и файлов из папки Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о них.

**О программе**

Сведения о версии программы ESET SysInspector и список программных модулей.

#### 12.2.2.1 Сочетания клавиш

Ниже перечислены сочетания клавиш, которые можно использовать при работе с программой ESET SysInspector.

**Файл**

| | |
|---|---|
| Ctrl+O | открывает существующий журнал |
| Ctrl+S | сохраняет созданные журналы |

**Создание**

| | |
|---|---|
| Ctrl+G | создает стандартный снимок состояния компьютера |
| Ctrl+H | создает снимок состояния компьютера, который также может содержать конфиденциальную информацию |

**Фильтрация элементов**

| | |
|---|---|
| 1, O | безопасно, отображаются элементы с уровнем риска 1–9 |
| 2 | безопасно, отображаются элементы с уровнем риска 2–9 |
| 3 | безопасно, отображаются элементы с уровнем риска 3–9 |
| 4, U | неизвестно, отображаются элементы с уровнем риска 4–9 |
| 5 | неизвестно, отображаются элементы с уровнем риска 5–9 |
| 6 | неизвестно, отображаются элементы с уровнем риска 6–9 |
| 7, B | опасно, отображаются элементы с уровнем риска 7–9 |
| 8 | опасно, отображаются элементы с уровнем риска 8–9 |
| 9 | опасно, отображаются элементы с уровнем риска 9 |
| - | понижает уровень риска |
| + | повышает уровень риска |
| Ctrl+9 | режим фильтрации, равный или более высокий уровень |
| Ctrl+0 | режим фильтрации, только равный уровень |

**Вид**

| | |
|---|---|
| Ctrl+5 | просмотр по производителям, все производители |
| Ctrl+6 | просмотр по производителям, только Майкрософт |
| Ctrl+7 | просмотр по производителям, все другие производители |
| Ctrl+3 | отображение полных сведений |
| Ctrl+2 | отображение сведений средней степени подробности |
| Ctrl+1 | основной вид |
| BACKSPACE | переход на один шаг назад |
| Пробел | переход на один шаг вперед |
| Ctrl+W | развертывание дерева |
| Ctrl+Q | свертывание дерева |

**Прочие элементы управления**

| | |
|---|---|
| Ctrl+T | переход к исходному расположению элемента после его выбора в результатах поиска |
| Ctrl+P | отображение базовых сведений об объекте |
| Ctrl+A | отображение полных сведений об объекте |
| Ctrl+C | копирование дерева текущего элемента |
| Ctrl+X | копирование элементов |
| Ctrl+B | поиск сведений о выбранных файлах в Интернете |
| Ctrl+L | открытие папки, в которой находится выбранный файл |
| Ctrl+R | открытие соответствующей записи в редакторе реестра |
| Ctrl+Z | копирование пути к файлу (если элемент связан с файлом) |
| Ctrl+F | переход в поле поиска |
| Ctrl+D | закрытие результатов поиска |
| Ctrl+E | запуск сценария обслуживания |

**Сравнение**

| | |
|---|---|
| Ctrl+Alt+O | открытие исходного или сравнительного журнала |
| Ctrl+Alt+R | отмена сравнения |
| Ctrl+Alt+1 | отображение всех элементов |
| Ctrl+Alt+2 | отображение только добавленных элементов (отображаются только элементы из текущего журнала) |
| Ctrl+Alt+3 | отображение только удаленных элементов (отображаются элементы из предыдущей версии журнала) |
| Ctrl+Alt+4 | отображение только замененных элементов (включая файлы) |
| Ctrl+Alt+5 | отображение только различий между журналами |
| Ctrl+Alt+C | отображение результатов сравнения |
| Ctrl+Alt+N | отображение текущего журнала |
| Ctrl+Alt+P | отображение предыдущей версии журнала |

**Разное**

| | |
|---|---|
| F1 | вызов справки |
| Alt+F4 | закрытие программы |
| Alt+Shift+F4 | закрытие программы без вывода запроса |
| Ctrl+I | статистика журнала |

### 12.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом работы этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе — полезное средство для обнаружения деятельности вредоносных программ.

После запуска приложение создает новый журнал, который открывается в новом окне. Чтобы сохранить журнал в файл, выберите **Файл** > **Сохранить журнал**. Сохраненные файлы журналов можно впоследствии открывать и просматривать. Чтобы открыть существующий журнал, выберите **Файл** > **Открыть журнал**. В главном окне программы ESET SysInspector всегда отображается только один журнал.

Преимуществом функции сравнения двух журналов является то, что она позволяет просматривать активный на данный момент журнал и журнал, сохраненный в файле. Чтобы сравнить журналы, выберите **Файл** > **Сравнить журналы**, а затем выполните команду **Выбрать файл**. Выбранный журнал сравнивается с активным журналом в главном окне программы. Сравнительный журнал будет содержать только различия между двумя сравниваемыми журналами.

**ПРИМЕЧАНИЕ.** Если выполняется сравнение двух файлов журнала, выберите **Файл** > **Сохранить журнал**, чтобы сохранить журнал как ZIP-файл. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

Рядом с отображенными элементами ESET SysInspector добавляет символы, указывающие на различия между журналами.

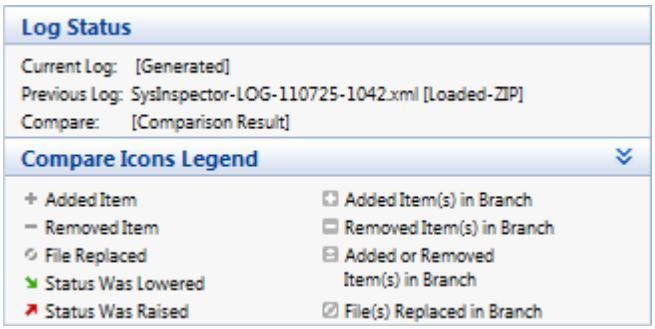
Элементы, отмеченные знаком –, есть только в активном журнале и отсутствуют в открытом сравниваемом журнале. Элементы, отмеченные знаком +, есть только в открытом журнале и отсутствуют в активном.

Ниже описаны все символы, которые могут отображаться рядом с элементами.

- + новое значение, отсутствует в предыдущем журнале
- раздел древовидной структуры содержит новые значения
- – удаленное значение, присутствует только в предыдущей версии журнала
- раздел древовидной структуры содержит удаленные значения
- значение или файл были изменены
- раздел древовидной структуры содержит измененные значения или файлы
- уровень риска снизился или был выше в предыдущей версии журнала
- уровень риска повысился или был ниже в предыдущей версии журнала

В разделе пояснений в левом нижнем углу отображается описание всех символов, а также названия

сравниваемых журналов.




Любой сравниваемый журнал можно сохранить в файл и открыть позже.

**Пример**

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». Внеся в систему изменения, откройте ESET SysInspector и создайте новый журнал. Сохраните его в файл с названием *текущий.xml*.

Чтобы отследить различия между этими двумя журналами, выберите **Файл** > **Сравнить журналы**. Программа создаст сравнительный журнал с перечнем различий между исходными журналами.

Тот же результат можно получить с помощью следующей команды, вызываемой из командной строки:

*SysIsnpector.exe текущий.xml предыдущий.xml*

## 12.3 Параметры командной строки

В ESET SysInspector можно формировать отчеты из командной строки. Для этого используются перечисленные ниже параметры.

| | |
|---|---|
| **/gen** | создание журнала непосредственно из командной строки без запуска графического интерфейса пользователя |
| **/privacy** | создание журнала без включения в него конфиденциальной информации |
| **/zip** | сохранение журнала непосредственно на диск в сжатом файле |
| **/silent** | скрытие индикатора выполнения при создании журнала |
| **/help, /?** | отображение сведений о параметрах командной строки |

**Примеры**

Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe "c:\клиентский_журнал.xml"*
Чтобы создать журнал в текущей папке, воспользуйтесь следующей командой: *SysInspector.exe /gen*
Чтобы создать журнал в определенной папке, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\"*
Чтобы создать журнал в определенной папке и в определенном файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\новый_журнал.xml"*
Чтобы создать журнал, из которого исключена конфиденциальная информация, в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\новый_журнал.zip" /privacy /zip*
Чтобы сравнить два журнала, воспользуйтесь следующей командой: *SysInspector.exe "текущий.xml" "исходный.xml"*

**ПРИМЕЧАНИЕ.** Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

## 12.4 Сценарий обслуживания

Сценарий обслуживания является средством для пользователей программы ESET SysInspector, с помощью которого можно легко удалить из системы нежелательные объекты.

Сценарий обслуживания позволяет целиком или частично экспортировать журнал ESET SysInspector. После экспорта можно отметить нежелательные объекты для удаления. Затем можно запустить отредактированный журнал для удаления отмеченных объектов.

Сценарий обслуживания предназначен для пользователей, имеющих определенный опыт в диагностике компьютерных систем. Неквалифицированное использование данного средства может привести к неисправности операционной системы.

**Пример**

При наличии подозрений на заражение компьютера вирусом, который не определяется антивирусной программой, можно воспользоваться описанной ниже пошаговой процедурой.

- Запустите ESET SysInspector и создайте новый снимок системы.
- Выберите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу SHIFT, а затем выберите последний объект, чтобы отметить все элементы в списке.
- Щелкните выделенные объекты правой кнопкой мыши и выберите в контекстном меню команду **Экспортировать выбранные разделы в сценарий обслуживания**.
- Выбранные объекты будут экспортированы в новый журнал.
- Далее следует наиболее важный шаг всей процедуры: откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, подлежащих удалению. Убедитесь, что не отмечены какие-либо важные для операционной системы файлы или объекты.
- Откройте ESET SysInspector, выберите **Файл** > **Запустить сценарий обслуживания** и укажите путь к своему сценарию.
- Нажмите кнопку **ОК**, чтобы запустить сценарий.

### 12.4.1 Создание сценария обслуживания

Чтобы создать сценарий, щелкните правой кнопкой мыши любой элемент в древовидном меню (на левой панели) в главном окне ESET SysInspector. В контекстном меню выберите команду **Экспортировать все разделы в сценарий обслуживания** или **Экспортировать выбранные разделы в сценарий обслуживания**.

**ПРИМЕЧАНИЕ.** Сценарий обслуживания нельзя экспортировать в ходе сравнения двух журналов.

### 12.4.2 Структура сценария обслуживания

Первая строка заголовка сценария содержит данные о версии ядра (ev), версии интерфейса (gv) и версии журнала (lv). Эти данные позволяют отслеживать изменения в XML-файле, используемом для создания сценария. Они гарантируют согласованность на этапе выполнения. Эту часть сценария изменять не следует.

Остальное содержимое файла разбито на разделы, объекты в которых можно редактировать. Те из них, которые должны быть обработаны сценарием, следует пометить. Для этого символ «-» перед объектом надо заменить на символ «+». Разделы отделены друг от друга пустой строкой. Каждый раздел имеет собственный номер и название.

**01) Запущенные процессы**

Этот раздел содержит список всех процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэшу CRC16, заключенному в символы звездочки (*).

Пример

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

В данном примере выбран (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

**02) Загруженные модули**

В этом разделе перечислены используемые в данный момент системные модули.

Пример

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

В данном примере модуль khbekhb.dll помечен символом «+». При выполнении сценария процессы, использующие данный модуль, распознаются и прерываются.

**03) TCP-соединения**

Этот раздел содержит данные о существующих TCP-соединениях.

Пример

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

При запуске этого сценария обнаруживается владелец сокета помеченного TCP-соединения, после чего сокет останавливается, высвобождая системные ресурсы.

**04) Конечные точки UDP**

Этот раздел содержит информацию о существующих конечных точках UDP.

Пример

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

При выполнении сценария определяется владелец сокета помеченных конечных точек UDP, после чего сокет останавливается.

**05) Записи DNS-сервера**

Этот раздел содержит информацию о текущей конфигурации DNS-сервера.

Пример

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

При выполнении сценария помеченные записи DNS-сервера удаляются.

**06) Важные записи реестра**

Этот раздел содержит информацию о важных записях реестра.

Пример

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

При выполнении сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или сброшены к значениям по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения раздела в определенной записи реестра.

**07) Службы**

Этот раздел содержит список служб, зарегистрированных в системе.

Пример

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

При выполнении сценария помеченные службы, а также все зависящие от них службы будут остановлены и удалены.

**08) Драйверы**

В этом разделе перечислены установленные драйверы.

Пример

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

При выполнении сценария выбранные драйверы останавливаются. Следует учесть, что некоторые драйверы не позволяют остановить свою работу.

**09) Важные файлы**

Этот раздел содержит информацию о файлах, критически важных с точки зрения правильной работы операционной системы.

Пример

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Выбранные объекты будут удалены или возвращены к исходным значениям.

### 12.4.3 Выполнение сценариев обслуживания

Отметьте все нужные объекты, а затем сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна программы ESET SysInspector с помощью команды **Запустить сценарий обслуживания** в меню «Файл». При открытии сценария появится следующее сообщение: **Выполнить сценарий обслуживания «%Scriptname%»?** После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Чтобы запустить сценарий, нажмите кнопку **Запуск**.

В диалоговом окне появится подтверждение успешного выполнения сценария.

Если сценарий может быть обработан только частично, отобразится следующее сообщение: **Сценарий обслуживания выполнен частично. Показать отчет об ошибке?** Чтобы просмотреть полный отчет об ошибках, в котором перечислены невыполненные действия, нажмите кнопку **Да**.

Если сценарий не был признан действительным, отобразится следующее сообщение: **Выбранный сценарий обслуживания не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?** Это может быть вызвано несоответствиями в сценарии (поврежден заголовок, искажено название раздела, пропущена пустая строка между разделами и т. д.). В этом случае откройте файл сценария и исправьте ошибки либо создайте новый сценарий обслуживания.

## 12.5 Часто задаваемые вопросы

**Требуются ли для запуска ESET SysInspector права администратора?**

Хотя для запуска ESET SysInspector права администратора не требуются, некоторые из собираемых этим приложением данных доступны только для учетной записи администратора. Запуск с правами обычного пользователя или с ограниченными правами приведет к сбору меньшего объема данных о системе.

**Создает ли ESET SysInspector файл журнала?**

ESET SysInspector может создать файл журнала с конфигурацией системы. Чтобы сохранить такой файл, в главном меню выберите **Файл** > **Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке *%USERPROFILE%\Мои документы* и получают название типа «SysInpsector-%COMPUTERNAME%-ГГММДД-ЧЧММ.XML». Перед сохранением файла журнала можно изменить его расположение и имя.

**Как просмотреть файл журнала ESET SysInspector?**

Чтобы просмотреть файл журнала, созданный с помощью ESET SysInspector, запустите программу и в главном меню выберите **Файл** > **Открыть журнал**. Кроме того, файлы журнала можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, создайте на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого файлы для просмотра можно просто

перетаскивать на этот ярлык. По соображениям безопасности в ОС Windows Vista/7 может быть запрещено перетаскивать элементы между окнами с разными настройками безопасности.

**Доступна ли спецификация для формата файлов журнала? Существует ли пакет SDK?**

В настоящее время ни спецификация файла журнала, ни пакет SDK недоступны, поскольку программа все еще находится на стадии разработки. После выхода окончательной версии программы мы можем предоставить эти данные по просьбам клиентов.

**Как ESET SysInspector оценивает риск определенного объекта?**

В большинстве случаев ESET SysInspector присваивает объектам (файлам, процессам, разделам в реестре и т. п.) уровни риска, используя наборы эвристических правил, которые изучают характеристики каждого объекта и затем оценивают угрозу их вредоносного действия. По результатам этого эвристического анализа объектам присваивается уровень риска от 1 — хорошо (зеленый) до 9 — опасно (красный). В окне навигации слева разделы окрашиваются в разные цвета в зависимости от уровня риска объекта внутри них.

**Означает ли уровень риска «6 — неизвестно (красный)», что объект является опасным?**

Анализ ESET SysInspector не гарантирует, что данный объект является вредоносным — эта оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует проверить в связи с их необычным поведением.

**Зачем ESET SysInspector в ходе работы подключается к Интернету?**

Как и многие приложения, программа ESET SysInspector подписана цифровым сертификатом, гарантирующим, что издателем программы является компания ESET и что программа не была изменена. Для проверки сертификата и подлинности издателя программы операционная система связывается с центром сертификации. Это нормальное поведение программ с цифровой подписью в Microsoft Windows.

**Что такое технология Anti-Stealth?**

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система атакована вредоносной программой, которая ведет себя как руткит, пользователь может подвергнуться риску потери или кражи данных. Без специального инструмента для борьбы с руткитами такие программы практически невозможно обнаружить.

**Почему иногда в файлах, помеченных как «Подписано MS», в записи «Название компании» стоит название другой компании?**

В ходе идентификации цифровой подписи исполняемого файла программа ESET SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. Если цифровая подпись найдена, файл будет проверен с использованием этих данных. Если цифровая подпись не найдена, программа ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности *%systemroot%\system32\catroot*), содержащего сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, его цифровая подпись применяется при проверке исполняемого файла.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется запись с названием другой компании.

Пример

В системе Windows 2000 есть приложение HyperTerminal, которое находится в папке *C:\Program Files\Windows NT*. Главный исполняемый файл приложения не имеет цифровой подписи, однако программа ESET SysInspector помечает его как подписанный корпорацией Майкрософт. Причиной этому служит ссылка в файле *C:\WINNT \system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat*, которая указывает на файл *C:\Program Files\Windows NT\hypertrm.exe* (главный исполняемый файл приложения HyperTerminal), а файл *sp4.cat* имеет цифровую подпись Майкрософт.

# 13. ESET SysRescue

ESET SysRescue — это служебная программа, которая позволяет создавать загрузочный диск с одним из решений ESET Security (это может быть ESET NOD32 Antivirus, ESET Smart Security или даже некоторые из серверных продуктов). Главным преимуществом ESET SysRescue является то, что решение ESET Security запускается независимо от операционной системы компьютера, имея при этом доступ к жесткому диску и всей файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

## 13.1 Минимальные требования

Средство ESET SysRescue работает в среде предустановки Microsoft Windows (Windows PE) версии 2.x, созданной на базе системы Windows Vista.

Windows PE является частью свободно распространяемого пакета автоматической установки Windows (Windows AIK), поэтому перед созданием необходимо установить Windows AIK ESET SysRescue (http://go.eset.eu/AIK). Поскольку поддерживается 32-разрядная версия Windows PE, при создании решения ESET Security в 64-разрядных системах необходимо использовать 32-разрядную версию пакета решения ESET SysRescue. Решение ESET SysRescue поддерживает пакет Windows AIK 1.1 и более поздней версии.

**ПРИМЕЧАНИЕ.** Поскольку размер пакета Windows AIK превышает 1 ГБ, для беспрепятственной загрузки необходимо высокоскоростное подключение к Интернету.

Средство ESET SysRescue доступно в решении ESET Security версии 4.0 и выше.

**Поддерживаемые операционные системы**

- Windows 7
- Windows Vista
- Windows Vista с пакетом обновления 1
- Windows Vista с пакетом обновления 2
- Windows Server 2008
- Windows Server 2003 с пакетом обновления 1 с KB926044
- Windows Server 2003 с пакетом обновления 2
- Windows XP с пакетом обновления 2 с KB926044
- Windows Vista XP с пакетом обновления 3

## 13.2 Создание компакт-диска аварийного восстановления

Чтобы запустить мастер ESET SysRescue, выберите в меню **Пуск** > **Программы** > **ESET** > **ESET Remote Administrator** > **ESET SysRescue**.

На первом этапе мастер определяет наличие в системе установленного пакета Windows AIK и подключенного к компьютеру устройства, подходящего для создания загрузочного носителя. Если пакет Windows AIK не установлен, установлен некорректно или поврежден, мастер предложит установить его или указать путь к папке с Windows AIK (http://go.eset.eu/AIK).

**ПРИМЕЧАНИЕ.** Поскольку размер пакета Windows AIK превышает 1 ГБ, для беспрепятственной загрузки необходимо высокоскоростное подключение к Интернету.

На следующем этапе 200 предлагается выбрать носитель для размещения на нем файлов ESET SysRescue.

## 13.3 Выбор места записи

Помимо компакт-диска, DVD-диска и USB-устройства, образ диска ESET SysRescue можно сохранить в файл ISO. Впоследствии этот файл с ISO-образом можно записать на компакт- или DVD-диск или использовать его другим способом (например, в виртуальной среде VMware или VirtualBox).

Если в качестве целевого носителя выбрано USB-устройство, загрузка может не выполняться на некоторых компьютерах. Некоторые версии BIOS сообщают о наличии проблем при обмене данными между BIOS и диспетчером загрузки (например, в Windows Vista), поэтому загрузка завершается следующим сообщением об ошибке:

```
файл: \boot\bcd
состояние: 0xc000000e
информация: ошибка при попытке чтения конфигурационных данных загрузки.
```

При появлении этого сообщения рекомендуется выбрать в качестве носителя вместо USB-устройства компакт-диск.

## 13.4 Параметры

Перед началом создания ESET SysRescue в мастере установки отображаются параметры компиляции, используемые на последнем этапе работы мастера ESET SysRescue. Их можно изменить, нажав кнопку **Изменить...**. Доступные параметры перечислены ниже.

- Папки 200
- Антивирус ESET 201
- Дополнительно 201
- Интернет-протокол 201
- Загрузочное USB-устройство 202 (если выбрано целевое USB-устройство)
- Запись 202 (если для записи выбран DVD- или компакт-диск)

Если не указан пакет установки MSI или на компьютере не установлено решение ESET Security, кнопка **Создать** будет неактивна. Чтобы выбрать пакет установки, нажмите кнопку **Изменить** и откройте вкладку **Антивирус ESET**. Если не ввести имя пользователя и пароль (**Изменить** > **Антивирус ESET**), кнопка **Создать** будет неактивна (затенена серым цветом).

### 13.4.1 Папки

**«Временная папка»** — это рабочий каталог для файлов, необходимый при создании диска ESET SysRescue.

**«Папка с ISO»** — это папка, в которую сохраняется полученный ISO-файл.

В списке на этой вкладке перечислены все локальные и сетевые диски с указанием свободного места на них. Если какие-то из папок располагаются на диске, где недостаточно свободного места, рекомендуется выбрать другой диск, на котором места достаточно. В противном случае недостаток свободного места не позволит создать образ диска.

**Внешние приложения** — позволяет указать дополнительные программы, которые будут выполняться или устанавливаться после загрузки с носителя ESET SysRescue.

**Включить внешние приложения** — позволяет добавлять внешние программы в компиляцию ESET SysRescue.

**Выбранная папка** — папка, где расположены программы, которые будут добавлены на диск ESET SysRescue.

### 13.4.2 Антивирус ESET

При создании компакт-диска ESET SysRescue можно выбрать один из двух источников файлов ESET для компилятора:

**Папка ESS/EAV** — файлы, уже содержащиеся в папке, в которую установлено решение ESET Security;

**MSI-файл** — файлы, которые содержатся в установщике MSI.

Далее, при необходимости можно обновить расположения файлов (NUP). Как правило, по умолчанию должен быть установлен параметр **ESS/Папка EAV/MSI-файл**. В некоторых случаях можно выбрать пользовательскую **папку обновления**, например, чтобы воспользоваться старой или новой версией базы данных сигнатур вирусов.

Источником имени пользователя и пароля может послужить один из двух следующих вариантов:

**Установленное решение ESS/EAV** — имя пользователя и пароль будут скопированы из установленного решения ESET Security.

**От пользователя** — имя пользователя и пароль вводятся в соответствующие текстовые поля.

**ПРИМЕЧАНИЕ.** Решение ESET Security на компакт-диске ESET SysRescue обновляется либо из Интернета, либо из решения ESET Security, установленного на компьютере, на котором используется компакт-диск ESET SysRescue.

### 13.4.3 Дополнительные настройки

На вкладке **Дополнительно** можно настроить параметры компакт-диска ESET SysRescue в соответствии с объемом оперативной памяти компьютера. Чтобы записать содержимое компакт-диска в оперативную память (ОЗУ), выберите вариант **576 МБ и больше**. Если выбрать вариант **Меньше 576 МБ**, при работе WinPE будет постоянно происходить обращение к компакт-диску восстановления.

В разделе **Внешние драйверы** можно добавить драйверы для конкретных аппаратных устройств (обычно для сетевой карты). Хотя среда WinPE основана на ОС Windows Vista с пакетом обновления 1 (SP1), поддерживающей широкий спектр оборудования, иногда оборудование не распознается. В этом случае необходимо добавить драйвер вручную. Есть два способа внедрения драйвера в компиляцию ESET SysRescue: вручную (кнопка **Добавить**) и автоматически (кнопка **Автопоиск** ). При включении драйвера вручную необходимо указать путь к соответствующему INF-файлу (в той же папке должен находиться и SYS-файл). В режиме автоматического добавления поиск драйвера в операционной системе данного компьютера выполняется автоматически. Режим автоматического включения рекомендуется использовать только в том случае, если средство ESET SysRescue установлено на компьютере с такой же сетевой картой, как и на компьютере, на котором был создан компакт-диск ESET SysRescue. При создании диска ESET SysRescue драйвер добавляется в сборку, поэтому его не придется искать позже.

### 13.4.4 Интернет-протокол

В этом разделе можно задать основные сведения о сети и создать готовые подключения после использования ESET SysRescue.

Выберите пункт **Автоматический частный IP-адрес**, чтобы получить IP-адрес автоматически от DHCP-сервера.

Кроме того, для этого подключения к сети можно использовать IP-адрес, указанный вручную (его также называют статическим IP-адресом). Выберите значение **Пользовательская**, чтобы настроить соответствующие параметры IP. При выборе этого параметра необходимо указать значения параметров **IP-адрес** и, для локальной сети и высокоскоростного подключения к Интернету, **Маска подсети**. В полях **Основной DNS-сервер** и **Дополнительный DNS-сервер** введите адреса основного и дополнительного DNS-сервера.

### 13.4.5 Загрузочное USB-устройство

Если в качестве целевого носителя было выбрано USB-устройство, на вкладке **Загрузочное USB-устройство** можно указать одно из доступных USB-устройств (если доступно несколько USB-устройств).

Выберите соответствующее целевое **Устройство**, на которое будет установлено решение ESET SysRescue.

***Предупреждение***: Выбранное USB-устройство будет отформатировано в процессе создания решения ESET SysRescue. Все данные на устройстве будут удалены.

Если выбрать вариант **Быстрое форматирование**, в процессе форматирования будут удалены все файлы из раздела без проверки диска на наличие поврежденных секторов. Воспользуйтесь этим вариантом, если USB-устройство было отформатировано ранее, и вы уверены, что оно не повреждено.

### 13.4.6 Запись

Если в качестве целевого носителя выбран компакт-диск или DVD-диск, на вкладке **Запись** можно задать дополнительные параметры записи.

**Удалить ISO-файл** — установите этот флажок, чтобы удалить временный ISO-файл после создания компакт-диска ESET SysRescue.

**Включить удаление** — этот параметр позволяет сделать выбор между быстрой и полной очисткой диска.

**Устройство записи** — выберите диск, который будет использоваться для записи.

***Предупреждение.*** Этот параметр установлен по умолчанию. При использовании перезаписываемого компакт- или DVD-диска все данные на нем будут стерты.

В разделе «Носитель» указаны сведения о компакт- или DVD-диске в дисководе.

**Скорость записи** — выберите нужную скорость в раскрывающемся меню. При выборе скорости необходимо учитывать возможности записывающего устройства и тип компакт- или DVD-диска.

## 13.5 Работа с решением ESET SysRescue

Для эффективного использования функции аварийного восстановления с USB-носителя, DVD- или компакт-диска необходимо загрузить компьютер с загрузочного носителя, на котором установлено средство ESET SysRescue. Порядок загрузки настраивается в параметрах BIOS. Кроме того, на этапе загрузки компьютера можно воспользоваться меню загрузки; обычно оно вызывается с помощью клавиш F9–F12 (в зависимости от версии системной платы и BIOS).

После загрузки с загрузочного носителя решение ESET Security запустится автоматически. Поскольку решение ESET SysRescue используется только в определенных ситуациях, некоторые модули защиты и функции программы, присутствующие в стандартной версии решения ESET Security, не нужны. Их список сужен до функций **Сканирование компьютера**, **Обновление** и некоторых разделов в окне **Настройка**. Возможность обновления базы данных сигнатур вирусов — это самая важная функция ESET SysRescue. Рекомендуем обновить программу перед началом сканирования компьютера.

### 13.5.1 Использование решения ESET SysRescue

Представим себе ситуацию, когда компьютеры в сети заражены вирусами, изменяющими исполняемые файлы (EXE). Решение ESET Security способно очистить все инфицированные файлы, кроме файла проводника *explorer.exe*, который нельзя очистить даже в безопасном режиме. Это является следствием того, что файл *explorer.exe*, как один из основных компонентов системы Windows, загружается и используется даже в безопасном режиме. ESET Security не сможет выполнять какие-либо действия с файлом и он останется инфицированным.

В сценарии этого типа для решения проблемы можно использовать средство ESET SysRescue. Для решения ESET SysRescue не нужны какие-либо компоненты операционной системы, в которой оно установлено, и поэтому оно может обрабатывать (очищать, удалять) любые файлы на диске.

# 14. Приложение. Лицензия сторонних разработчиков.

Компания ESET признает, что настоящее программное обеспечение включает код третьих сторон, подпадающий под действие лицензий сторонних разработчиков.

---

3-clause BSD License ("New BSD License")

---

Copyright (c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
• Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
Copyright (c) 2006-2007 The Written Word, Inc.
Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
Copyright (c) 2009 Daniel Stenberg
Copyright (C) 2008, 2009 Simon Josefsson
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
• Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

---