

ESET **Remote** **Administrator**

**Руководство по установке
и руководство пользователя**



we protect your digital world

Содержание

ESET Remote Administrator

© ESET spol. s r. o., 2007

Программный продукт ESET Remote Administrator разработан компанией © ESET spol. s r. o. Дополнительные сведения можно получить на сайте компании www.esetnod32.ru

Все права защищены. Никакая часть настоящего документа не может быть воспроизведена, сохранена или представлена в какой-либо системе хранения данных, передана в какой бы то ни было форме какими бы то ни было средствами (электронными, фотокопировальными, записывающими, сканирующими или другими) в каких бы то ни было целях без специального письменного разрешения автора.

Компания ESET, spol. s r. o. оставляет за собой право вносить любые изменения в описанное программное обеспечение без предварительного уведомления.

Международная техническая поддержка:

www.eset.eu/support

Техническая поддержка в России:

[http://esetnod32.ru/support/index.php](http:// esetnod32.ru/support/index.php)

REV.20071205-002

1.	Введение	8
2.	ERA – архитектура клиент-сервер	9
2.1	Сервер ERA (ERAS)	9
2.1.1	Требования	9
2.1.2	Иерархия ERAS в больших сетях	10
2.1.3	Установка	11
2.1.4	Журналы	11
2.1.5	Конфигурация	11
2.1.6	Ключи лицензии	11
2.1.7	База данных и хранение информации	12
2.2	Консоль ERA (ERAC)	12
3.	Другие компоненты ESET в сетевой среде	13
3.1	Клиентские решения ESET	13
3.2	Редактор конфигурации ESET	13
3.2.1	Наложение конфигураций	14
3.2.2	Важнейшие элементы конфигурации	14
3.3	LAN Update Server – зеркало	15
3.3.1	Функционирование сервера-зеркала	16
3.3.2	Типы обновлений	16
3.3.3	Как создать и настроить зеркало	17
4.	Подробные сведения о консоли удаленного администрирования ESET	19
4.1	Подключение к ERAS	19
4.2	ERAC – главный экран	19
4.3	Фильтрация данных	20
4.3.1	Группы	20
4.3.2	Фильтр	20
4.3.3	Контекстные меню	21
4.3.4	Представления	22
4.4	Вкладки ERAC	22
4.4.1	Общее описание вкладок и клиентов	22
4.4.2	Репликация и сведения на отдельных вкладках	22
4.4.3	Вкладка Клиенты	23
4.4.4	Вкладка Журнал угроз	26
4.4.5	Вкладка Журнал файервола	26
4.4.6	Вкладка Журнал событий	26
4.4.7	Вкладка Журнал сканирования	27
4.4.8	Вкладка Задачи	27
4.4.9	Вкладка Отчеты	27
4.4.10	Вкладка Удаленная установка	29
4.5	Настройка Консоли ERA	29
4.5.1	Вкладка Подключения	29
4.5.2	Вкладка Столбцы – отображение/скрытие	29
4.5.3	Вкладка Цвета	29
4.5.4	Вкладка Пути	29
4.5.5	Вкладка Дата/время	29
4.5.6	Вкладка Другие параметры	29
4.6	Конфигурирование сервера ERA с использованием консоли	30
4.6.1	Вкладка Общие	30
4.6.2	Вкладка Безопасность	30
4.6.3	Вкладка Обслуживание сервера	31
4.6.4	Вкладка Протоколирование	31
4.6.5	Вкладка Репликация	31
4.6.6	Обновления	33
4.6.7	Вкладка Другие параметры	33
5.	Задания	34
5.1	Задание Конфигурация	34
5.2	Задание Сканирование по запросу	35
5.3	Задание Немедленное обновление	35
6.	Установка клиентских решений ESET	36
6.1	Параметры командной строки для непосредственной установки клиентских решений	36
6.2	Способы установки	36
6.2.1	Непосредственная установка с предварительно определенной XML-конфигурацией	36
6.2.2	Удаленная установка – обзор	37
6.2.3	Активная удаленная установка	38
6.2.4	Удаленная установка по электронной почте	41
6.2.5	Выборочная удаленная установка	43

6.3	Подробные сведения об агенте installer.exe	43
6.4	Как избежать повторной установки	44
6.5	Процесс установки – сообщения об ошибках	44
6.5.1	Диагностика удаленной установки	45
7.	Сценарии развертывания для ESET NOD32	
	Remote Administrator, сервера-зеркала	
	и клиентских решений ESET	46
7.1	Малая сеть – 1х ERAS, сервер-зеркало	46
7.1.1	Установка зеркального HTTP-сервера	46
7.1.2	Установка сервера ERA	47
7.1.3	Установка Консоли ERA	47
7.1.4	Удаленная установка на подключенные к сети рабочие	47
	станции	47
7.1.5	Удаленная установка на ноутбуки, в данный момент	48
	не подключенные к сети	48
7.2	Компания с удаленным филиалом – 2х ERAS,	
	2х сервера-зеркала	50
7.2.1	Установка программного обеспечения в основном офисе ...	50
7.2.2	Филиал: установка сервера ERA	51
7.2.3	Филиал: установка зеркального HTTP-сервера	51
7.2.4	Филиал: Удаленная установка на клиенты	51
8.	Советы и рекомендации	52
8.1	Экспорт и другие функции клиентской	
	XML-конфигурации	52
8.2	Комбинированное обновление для ноутбуков	
	и мобильных устройств	52
8.3	Удаление существующих профилей	53
8.4	Настройка планировщика	54
8.5	Пакеты для выборочной установки	55

ВАЖНО: Перед загрузкой, установкой, копированием или использованием продукта прочитайте изложенные ниже положения о применении этого программного продукта. **ЗАГРУЖАЯ, УСТАНОВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТОТ ПРОДУКТ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И ПОЛОЖЕНИЯМИ.**

Лицензионное соглашение об использовании программного обеспечения конечными пользователями

Это соглашение об использовании программного обеспечения («Соглашение») заключено и исполняется: компанией ESET, spol. s r. o., зарегистрированной по адресу Pionierska 9/A, 831 02 Bratislava в коммерческом регистре окружного суда Bratislava I. Section Sro, Insertion No 3586/B, BIN: 31 333 535 («Поставщик») и Вами, физическим или юридическим лицом, выступающим в качестве конечного пользователя (далее просто «Пользователь»), и подтверждает предоставленное Вам право на использование Программного обеспечения, определенного в статье 1 настоящего Соглашения. Экземпляр Программного обеспечения, определенного в статье 1 настоящего Соглашения, может храниться на носителях формата CD-ROM или DVD, быть отправлен по электронной почте, загружен через Интернет, загружен с серверов Поставщика или получен из других источников, которые удовлетворяют положениям и условиям, перечисленным ниже.

ЭТОТ ДОКУМЕНТ НЕ ЯВЛЯЕТСЯ КОНТРАКТОМ НА ЗАКУПКУ, НО ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ НА ПРАВО ИСПОЛЬЗОВАНИЯ КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, если таковой присутствует, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Пользователь имеет право в соответствии с настоящим Соглашением.

Нажатие кнопки «Я согласен» в процессе загрузки, установки, копирования или использования этого Программного обеспечения выражает Ваше согласие с положениями и нормами, утвержденными в Соглашении. Если Вы не согласны с каким-либо из положений этого Соглашения, нажмите кнопку «Не согласен» или «Отклонить», прекратите процесс загрузки или установки.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ЭТО СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ ПРИНЯТЬ ОПИСАННЫЕ В НЕМ ОБЯЗАТЕЛЬСТВА.

1. Программное обеспечение. Программное обеспечение, относительно которого заключено настоящее Соглашение, включает в себя (а) экземпляр компьютерной программы компании ESET и все её части, (б) содержимое материального носителя: дисков, компакт-дисков, DVD-дисков, отчетов по электронной почте и их вложений, если таковые существуют, а также других носителей, с которыми поставляется это Соглашение, включая Программное обеспечение, поставляемое в виде объектного кода на компакт-дисках, DVD-дисках или посредством электронной почты через Интернет, (в) любые руководства и документации, которые относятся к Программному обеспечению, что включает в себя следующий список (но не ограничивается им): любое описание Программного обеспечения, его спецификации, описания параметров, руководства по использованию, описание интерфейса Программного обеспечения, инструкции по эксплуатации и установке и любые другие описания по использованию Программного обеспечения («Документация»), (г) копии Программного обеспечения, исправления ошибок в коде Программного обеспечения, если таковые существуют, дополнения Программного обеспечения, расширения Программного обеспечения, усовершенствованные версии Программного обеспечения, новые версии Программного обеспечения, а также все обновления любых частей Программного обеспечения, если таковые поставляются, в отношении которых Поставщик дает вам право на использование этой Лицензии в соответствии со статьей 4 настоящего документа. Поставщик предоставляет Программное обеспечение только в форме исполняемого кода.

2. Отправка зараженных файлов и информации Поставщику. Программное обеспечение содержит функции для сбора образцов новых компьютерных вирусов и других вредоносных программ (далее просто «Вирусы») и последующей отправки их Поставщику, совместно с информацией о компьютере и/или платформе, на которой установлено Программное обеспечение («Информация»). Информация может содержать данные, в том числе регистрационные данные о пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, данные о самом компьютере и операционной системе, информацию о файлах компьютера, на котором установлено Программное обеспечение и о файлах, подвергшихся заражению, а также подробную информацию о зараженных файлах. Поставщик обязуется использовать полученную Информацию и Вирусы только для изучения Вирусов и принимает все разумные меры для сохранения Информации в тайне от третьих лиц. Если Вы принимаете положения этого Соглашения и включаете описанную выше функцию Программного обеспечения, Вы согласны передавать Вирусы и Информацию Поставщику. В то же время Вы даете право Поставщику обрабатывать полученную информацию в рамках соответствующих законодательных норм.

3. Установка. Программное обеспечение поставляется на материальном носителе: компакт-дисках, DVD-дисках; отправляется посредством электронной почты, загружается через Интернет, загружается с серверов Поставщика или из других источников. Перед использованием Программного обеспечения необходимо провести установку. Установка Программного обеспечения должна происходить на настроенном компьютере, конфигурация которого соответствует минимальным требованиям, изложенным в комплекте Документации. Способ установки описан в Документации. Компьютер, на который устанавливается Программное обеспечение, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на его работу.

4. Лицензия. Получив настоящий документ, тем самым Вы соглашаетесь с пунктами Соглашения и оплачиваете, при необходимости, Лицензионный сбор, описанный в статье 1б, при предоставлении Поставщиком неисключительного и не подлежащего передаче права на установку Программного обеспечения на жесткий диск компьютера или на аналогичный носитель постоянного хранения данных, на установку и хранение Программного обеспечения в памяти компьютера и на исполнение, хранение и отображение данных Программного обеспечения на компьютерах, число которых не превышает число, указанное Пользователем в заказе и оплаченное в соответствующем объеме Лицензионного сбора («Лицензия»). Под одним пользователем подразумевается: (1) установка Программного обеспечения на один компьютер, (2) в случае распределенной лицензии с привязкой к количеству почтовых ящиков, означает одного пользователя компьютера, получающего электронную почту посредством Пользовательского почтового агента. Если Пользовательский почтовый агент принимает электронную почту и распределяет ее автоматически среди нескольких пользователей, количество пользователей должно быть определено из расчета количества реальных пользователей, получающих электронную почту. Если почтовый сервер функционирует в режиме почтового шлюза, количество пользователей приравнивается количеству почтовых серверов, к которым предоставляется доступ через этот шлюз. Если какое-либо количество электронных адресов (например, вследствие использования псевдонимов) принадлежит одному пользователю и один пользователь принимает почту по ним, а почта не распределяется автоматически на стороне клиента по другим пользователям, Лицензия необходима только для одного компьютера.

5. Использование прав Пользователя. Как Пользователь Вы можете использовать Программное обеспечение только для защиты своих действий и компьютеров, на которые получена и оплачена соответствующая Лицензия.

6. Ограничения прав Пользователя. Не разрешается копировать, распространять, разделять на части или создавать дочерние версии Программного обеспечения за исключением следующих оговоренных случаев:

- (а) Вы можете создавать одну резервную копию Программного обеспечения на носителе данных, не используя эту архивную резервную копию для установки и использования Программного обеспечения на других компьютерах. Создание копий Программного обеспечения в других целях является нарушением этого Соглашения.
- (б) Вы не должны использовать, изменять, толковать, воспроизводить или передавать права на использование Программного обеспечения или копий Программного обеспечения иным образом, отличным от описанного в настоящем Соглашении.
- (в) Вы не должны продавать, сдавать в аренду или передавать во временное пользование другим лицам Программное обеспечение или права на его использование.
- (г) Запрещается анализировать, декомпилировать или разбирать код приложения, а также искать пути получения исходного кода Программного обеспечения способами, противоречащими действующему законодательству.
- (е) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем существующим законодательным нормам и правилам, которые применимы к случаям использования этого Программного обеспечения, в том числе нормам, установленным международным законом об авторском праве, внутренними нормативными актами Российской Федерации об авторском праве и смежных правах, а также другими законами по защите интеллектуальной собственности.
- (ж) Запрещается использование Программного обеспечения, полученного в виде пробной версии или версии категории «Не для продажи» в целях избежания уплаты Лицензионного сбора (статья 16).

7. Авторское право. Программное обеспечение и все права, включая (без ограничений) право собственности и право интеллектуальной собственности принадлежат компании ESET. Права компании ESET защищены международными соглашениями и прочими соответствующими законодательными нормами стран, в которых используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются коммерческой тайной и конфиденциальной информацией, принадлежащей компании ESET. Запрещается копирование Программного обеспечения, кроме случаев, описанных в статье 6 (а). Любые копии, создаваемые в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и наименование оригинального Программного обеспечения. Если Вы анализируете, декомпилируете или разбираете код Программного обеспечения или ищете пути получения исходного кода способами, нарушающими положения этого Соглашения, любая информация, полученная таким образом, автоматически и безоговорочно должна быть передана Поставщику, так как принадлежит Поставщику изначально.

8. Сохранение прав. Все права на Программное обеспечение закреплены за Поставщиком, кроме тех прав, которые в явной форме передаются Вам, как Пользователю, этим Соглашением.

9. Несколько языковых версий, версии для разных операционных систем, несколько копий. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько копий программного обеспечения, запрещается установка большего количества копий или версий Программного обеспечения, чем было указано в заказе и чем было оплачено соответствующими Лицензионными сборами в соответствии со статьей 16 настоящего Соглашения. Запрещается продавать, сдавать в аренду или напрокат, выдавать сублицензии, передавать во временное или постоянное пользование другим лицам любые версии или копии Программного обеспечения, даже если оно не используется вами.

10. Момент вступления в силу и продолжительность действия Соглашения. Настоящее Соглашение вступает в законную силу и действует с момента установки Программного обеспечения, принятия условия настоящего Соглашения и подтверждения Поставщиком правильности ключа. Завершить действие Соглашения можно, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии (если таковые делались) и все дополнительные материалы, которые были получены от Поставщика или от одного из его коммерческих партнеров. Ваши права как Пользователя автоматически и немедленно аннулируются, без предупреждений со стороны Поставщика, если любое из положений настоящего Соглашения будет нарушено Вами. В этом случае Вы обязаны без промедления удалить, разрушить или вернуть за свой счет Программное обеспечение, все резервные копии (если таковые делались) и все дополнительные материалы, которые были получены от компании ESET или от одного из ее коммерческих партнеров.

Настоящее Соглашение заключается на срок один или два года (или иной согласованный срок), как указано в вашем заказе на Программное обеспечение в качестве периода использования, и его действие может быть продлено на период продолжительностью один или два года (или иной согласованный срок) в случае оплаты вами соответствующих Лицензионных сборов, как описано в статье 16 настоящего Соглашения.

Независимо от способа окончания действия текущего Соглашения, положения статей 7, 8, 11, 13 и 19 остаются действительными без ограничения по времени

11. ПРЕДОСТАВЛЕНИЕ ГАРАНТИИ. ВЫСТУПАЯ В КАЧЕСТВЕ ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ ПРЯМОЙ ИЛИ ВМЕНЕННОЙ ГАРАНТИИ ЛЮБОГО ТИПА, И, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ, НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ПОСТАВЩИКОВ ЛИЦЕНЗИЙ, НИ ПРАВООБЛАДАТЕЛИ НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ СООТВЕТСТВИЯ КАКОМУ-ЛИБО НАЗНАЧЕНИЮ, ИЛИ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ МАРКИ ИЛИ ДРУГИХ ПРАВ ТРЕТЬИХ СТОРОН. ПОСТАВЩИК И ЕГО ПАРТНЕРЫ НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ ПОЛНОСТЬЮ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. ВСЯ ОТВЕТСТВЕННОСТЬ И РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ ОПРЕДЕЛЕННЫХ РЕЗУЛЬТАТОВ, КОТОРЫЕ НЕОБХОДИМЫ ВАМ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ

И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫЕ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС. ВЫ ДОЛЖНЫ БЫТЬ ОСВЕДОМЛЕННЫ О МИНИМАЛЬНЫХ СИСТЕМНЫХ ТРЕБОВАНИЯХ ВАШЕГО КОМПЬЮТЕРА, КОТОРЫЕ ПОЗВОЛЯТ ФУНКЦИОНИРОВАТЬ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.

12. Отказ от дальнейших обязательств. Настоящее Соглашение не накладывает никаких обязательств на Поставщика, за исключением тех, что изложены в настоящем Соглашении.

13. ОГРАНИЧЕННАЯ ГАРАНТИЯ. В ТОЙ СТЕПЕНИ, НАСКОЛЬКО ЭТО ДОПУСКАЕТСЯ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСТАВЩИК, ЕГО СОТРУДНИКИ И ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ПОСТАВЩИКОВ ЛИЦЕНЗИЙ, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПОТЕРИ ПРИБЫЛИ, ДОХОДОВ ИЛИ ОБОРОТА С ПРОДАЖ, ИЛИ ЗА УTRATУ ДАННЫХ, ИЛИ ПО ЗАТРАТАМ НА ДОПОЛНИТЕЛЬНЫЕ ЗАПАСНЫЕ ЧАСТИ И ОБСЛУЖИВАНИЕ, ЗА ПОРЧУ ИМУЩЕСТВА, ВРЕД ЗДОРОВЬЮ, ПЕРЕРЫВЫ В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ДРУГИЕ СЛУЧАИ УЩЕРБА, В ТОМ ЧИСЛЕ СПЕЦИАЛЬНОГО, НАМЕРЕННОГО, НЕНАМЕРЕННОГО, СЛУЧАЙНОГО, ЭКОНОМИЧЕСКОГО, ПОКРЫВАЕМОГО, ПРЕСТУПНОГО, ПРЯМОГО ИЛИ ОПОСРЕДОВАННОГО, ПРОИЗОШЕДШЕГО КАКИМ-ЛИБО ЕЩЕ СПОСОБОМ, НЕЗАВИСИМО ОТ ДЕЙСТВИЯ ДОПОЛНИТЕЛЬНЫХ КОНТРАКТОВ, УМЫШЛЕННЫХ ДЕЙСТВИЙ, НЕБРЕЖНОСТИ ИЛИ ДРУГИХ ФАКТОРОВ, КОТОРЫЕ МОГУТ ВЫЗВАТЬ ОТВЕТСТВЕННОСТЬ, ВКЛЮЧАЯ ПОВРЕЖДЕНИЯ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ НЕВОЗМОЖНОСТИ ЕГО ИСПОЛЬЗОВАНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ЕГО ПАРТНЕР, ПОСТАВЛЯЮЩИЙ ЛИЦЕНЗИЮ, БЫЛ ПРЕДУПРЕЖДЕН О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА. ТАК КАК ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ ПОЗВОЛЯЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО РАЗРЕШАЮТ ОГРАНИЧИВАТЬ ЕЕ, ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ ИЛИ ЕГО ПАРТНЕРОВ, ПОСТАВЛЯЮЩИХ ЛИЦЕНЗИИ, ОГРАНИЧИВАЕТСЯ РАЗМЕРОМ СУММЫ, ВЫПЛАЧЕННОЙ ВАМИ ПРИ ПРИОБРЕТЕНИИ ЛИЦЕНЗИИ.

ВАЖНОЕ ЗАМЕЧАНИЕ ДЛЯ ПОЛЬЗОВАТЕЛЯ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ОТКАЗООУСТОЙЧИВО И НЕ ПРЕДНАЗНАЧЕНО ДЛЯ РАБОТЫ В ОПАСНЫХ УСЛОВИЯХ, ТРЕБУЮЩИХ БЕСПЕРЕБОЙНОЙ РАБОТЫ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ПРЕДНАЗНАЧЕНО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ НАВИГАЦИИ САМОЛЕТОВ, В ЯДЕРНЫХ ЦЕНТРАХ ИЛИ СИСТЕМАХ СВЯЗИ, В СИСТЕМАХ ВООРУЖЕНИЙ, В СИСТЕМАХ ПРЯМОГО ИЛИ НЕПРЯМОГО ЖИЗНЕОБЕСПЕЧЕНИЯ, В УПРАВЛЕНИИ ПОЛЕТАМИ ИЛИ В ЛЮБЫХ ДРУГИХ ВИДАХ ДЕЯТЕЛЬНОСТИ, ГДЕ ОШИБКА МОЖЕТ ПОВЛЕЧЬ ЗА СОБОЙ СМЕРТЬ, СЕРЬЕЗНЫЕ ПОВРЕЖДЕНИЯ ИЛИ БОЛЬШОЙ УЩЕРБ.

14. Ни одно из положений настоящего Соглашения не затрагивает права той стороны, для которой закон обозначает права и положение в качестве потребителя. Поставщик со своей стороны, стороны своих сотрудников и со стороны поставщиков лицензий, выступает с позиции отказа, исключения или ограничения любых обязательств, ответственности и гарантий, как указано в статье 13, что исключает любую другую позицию и не преследует иных причин.

15. Поддержка. Поставщик обязан оказывать техническую поддержку для наиболее свежих версий Программного обеспечения. В соответствии с положениями Лицензии, Пользователь имеет право использовать следующие службы:

- (а) **Помощь по техническим вопросам.** Поставщик обязан обеспечивать помощь и поддержку во время поиска неисправностей и отладке в случае использования наиболее свежих версий Программного обеспечения в заранее объявленное рабочее время. Любые запросы помощи и поддержки, полученные в нерабочее время, рассматриваются как полученные в начале следующего рабочего дня. Запросы помощи и поддержки могут быть доставлены Поставщику посредством телефонной связи, факса или электронной почты с использованием отдельных телефонных линий или адресов электронной почты, указанных в Документации или на веб-сайтах Поставщика. Запросы помощи и поддержки должны быть достаточно осмысленными и обязаны содержать достаточно данных для воспроизведения возникшей проблемы. При необходимости Пользователь обязан предоставить необходимую помощь в решении описываемой проблемы.
- (б) **Обновление.** Обновления включают в себя все новые версии или изменения Программного обеспечения или отдельных его частей, о выпуске которых объявлено на сайтах Поставщика или сайтах его коммерческих партнеров. Поставщик обязуется предоставить Пользователю доступ к Обновлению в защищенной области своего веб-сайта посредством сети Интернет. Доступ к обновлениям предоставляется при указании имени пользователя и пароля («Идентификация»). Данные Идентификации Пользователя содержат случайную комбинацию алфавитно-цифровых символов и автоматически генерируются системой Поставщика. Данные Идентификации должны быть предоставлены Пользователю в форме электронного письма, или вложены в торговую упаковку Лицензированного продукта или доставлены любым другим подходящим способом. Пользователь обязан принять меры для сохранения данных Идентификации и защитить их от повреждения, потери или неверного использования. Вы признаете, что Программное обеспечение и связанные с ним серийный номер, регистрационный ключ и код активации являются производственной тайной и важной конфиденциальной информацией компании ESET («Конфиденциальная информация»). Вы соглашаетесь не предоставлять третьим лицам и не раскрывать перед ними эту конфиденциальную информацию, за исключением (если Вы представляете Компанию) собственных работников и независимых консультантов, давших стандартные для отрасли подписки о неразглашении. При обнаружении первого случая неверного использования данных Идентификации Пользователя Поставщик имеет право отменить действие данных Идентификации и предоставить новые данные Идентификации для пользователя («Замена идентификации»). Пользователь обязан предоставить Поставщику все данные, необходимые для расследования случаев неверного использования данных Идентификации, в том числе записи действий компьютерных систем, записи доступа к файлам и другие необходимые данные. В случаях, когда обнаружено неверное использование данных Идентификации, поставщик по своему усмотрению и в результате своего решения может предоставить новую Замену идентификации для Пользователя, или прекратить действие Лицензии немедленно без какой-либо компенсации Пользователю. Право Поставщика компенсировать ущерб не противоречит немедленной отмене действия Лицензии. Пользователь обязуется получать обновления только с веб-сайтов Поставщика или его официальных партнеров («Авторизованные источники»). Пользователь согласен устанавливать каждую новую версию или изменение Лицензированного продукта сразу же после получения или не позже, чем указано Поставщиком в Программном обеспечении, Документации к нему или на веб-сайте Поставщика или его коммерческих партнеров. Поставщик не может нести ответственность за ущерб, произошедший вследствие нарушения Пользователем последовательности получения новых версий Программного обеспечения и/или установки обновлений из Авторизованных источников.

- (в) **Отказ в поддержке.** Поставщик не обязан обеспечивать поддержку в следующих случаях:
- I. ошибка произошла вследствие постороннего вмешательства в структуру Программного обеспечения, его исходный код или при использовании неверных параметров или установок Программного обеспечения;
 - II. ошибка произошла по вине обслуживающего персонала Пользователя, или при использовании Программного обеспечения в условиях, не соответствующих описанным в Документации;
 - III. ошибка устраняется путем установки Обновления, которое Пользователь не может установить;
 - IV. Лицензионный сбор не оплачен Пользователем, как того требует статья 16 настоящего Соглашения;
 - V. другие случаи, описанные в настоящем Соглашении.
- (г) **Обучение.** Настоящее Соглашение не влечет за собой обязательств по предоставлению услуг обучения или практики по эксплуатации и установке Программного обеспечения.

16. Лицензионный сбор и порядок оплаты. Размер Лицензионного сбора за полноценную версию Программного обеспечения определяется на основе текущего прейскуранта Поставщика в соответствии с количеством компьютеров, для которых предназначено Программное обеспечение («Лицензионный сбор»). Перед оплатой Лицензионного сбора Вы можете ознакомиться с положениями и условиями Соглашения и сроком, на который передается право на использование этого Программного обеспечения. Если на счете или другом документе, предоставленном Поставщиком или его коммерческим партнером, не указано иной даты погашения, Лицензионный сбор уплачивается в момент доставки Программного обеспечения. Вы обязаны оплатить все налоги и иные пошлины, начисленных в отношении оплаты Лицензионного сбора вследствие действия текущего законодательства, исключая налоги на доход Поставщика. Если Вы не оплачиваете Лицензионный сбор до указанной даты, Ваша Лицензия на использование Программного обеспечения отменяется, и Вы обязаны компенсировать все операционные расходы, включая расходы на юридические услуги и судебные пошлины. Под обязательство оплаты Лицензионного сбора не попадают случаи использования Программного обеспечения, поставленного под категорией «Не для продажи» и пробных версий. Факт оплаты Лицензионного сбора является подтверждением Пользователем принятия данного лицензионного соглашения.

17. Пробные версии и версии не для продажи. Вы можете использовать Программное обеспечение, поставляемое не для продажи или поставляемое в качестве пробных версий, которые предназначены для проверки и тестирования функций Программного обеспечения. Кроме того, Вы можете использовать Программное обеспечение категории «Не для продажи» в демонстрационных целях.

18. Данные пользователя и защита прав. Вы, как Пользователь, разрешаете Поставщику передавать, обрабатывать и сохранять данные, позволяющие Поставщику устанавливать Вашу личность. Вы согласны с тем, что поставщик может своими средствами проверить правильность использования Программного обеспечения в соответствии с настоящим Соглашением. Вы согласны, что посредством обмена данными между Программным обеспечением и компьютерами Поставщика или его коммерческих партнеров будут передаваться данные, которые удостоверяют право на использование Программного обеспечения и обеспечивают защиту прав Поставщика.

19. Экспортная и реэкспортная проверка. Программное обеспечение, Документация или ее часть, включая информацию о Программном обеспечении и его частях, являются объектом, попадающим под действие надзорных правил по импорту и экспорту в соответствии с действующим законодательством. Вы согласны строго следовать всем действующим нормам и правилам по экспорту и импорту и подтверждаете, что Вы ответственны за получение лицензий на экспорт, реэкспорт, перевозку и импорт Программного обеспечения.

20. Примечания. Все замечания, возвращаемое Программное обеспечение и Документация должны быть доставлены по адресу: ESET, spol. s r. o., Svoradova 1, 811 03 Bratislava, Slovak Republic.

21. Регулирующее законодательство. Пользователь и Поставщик согласны, что решение конфликтов производится в соответствии с государственным законодательством Российской Федерации, а Конвенция ООН о контрактах по международной торговле товарами (United Nations Convention on Contracts for the International Sale of Goods) неприменима. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду в Братиславе (District Court Bratislava I., Slovakia), и Вы выражаете персональное согласие в настоящем и будущем и явным образом подчиняетесь юридическим процедурам этого суда (District Court Bratislava I., Slovakia) в связи с любым спором или конфликтом такого рода.

22. Общие положения. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения. Они остаются в силе в соответствии с условиями и сроками, изложенными в этом документе. Любые поправки к этому документу могут иметь место только в письменной форме и должны быть подписаны действующим на основе закона компетентным и уполномоченным представителем Поставщика.

Настоящее Соглашение между Вами и Поставщиком является единым и неделимым Соглашением, применимым к Программному обеспечению, и полностью отменяющим любые предыдущие изложения фактов, результаты переговоров, обязательства, отчеты или объявления относительно Программного обеспечения.

1. Введение

ESET Remote Administrator (ERA) является решением, предназначенным для централизованного администрирования продуктов ESET, в том числе на рабочих станциях и серверах. Благодаря наличию в составе ESET Remote Administrator встроенной системы управления заданиями можно быстро реагировать на возникающие проблемы и угрозы, а также, что немаловажно, устанавливать решения ESET на удаленных компьютерах.

Само по себе приложение ESET Remote Administrator не осуществляет защиту от вредоносного кода, в частности вирусов и червей. Для обеспечения полноценной антивирусной защиты рекомендуется использовать ESET NOD32 Antivirus for Windows или ESET NOD32 Smart Security.

Для полного развертывания комплекса решений ESET необходимо выполнить следующие действия:

- установить сервер ERA (ERA Server, ERAS);
- установить Консоль ERA (ERA Console, ERAC);
- установить сервер-зеркало;
- установить программное обеспечение для клиентских компьютеров (антивирус ESET NOD32, ESET NOD32 Smart Security, ESET NOD32 BusinessEdition и т.д.).

ПРИМЕЧАНИЕ. В некоторых местах этого документа используются системные переменные, содержащие пути к файлам и папкам:

%ProgramFiles% обычно = C:\Program Files

%ALLUSERSPROFILE% обычно = C:\Documents and Settings\All Users

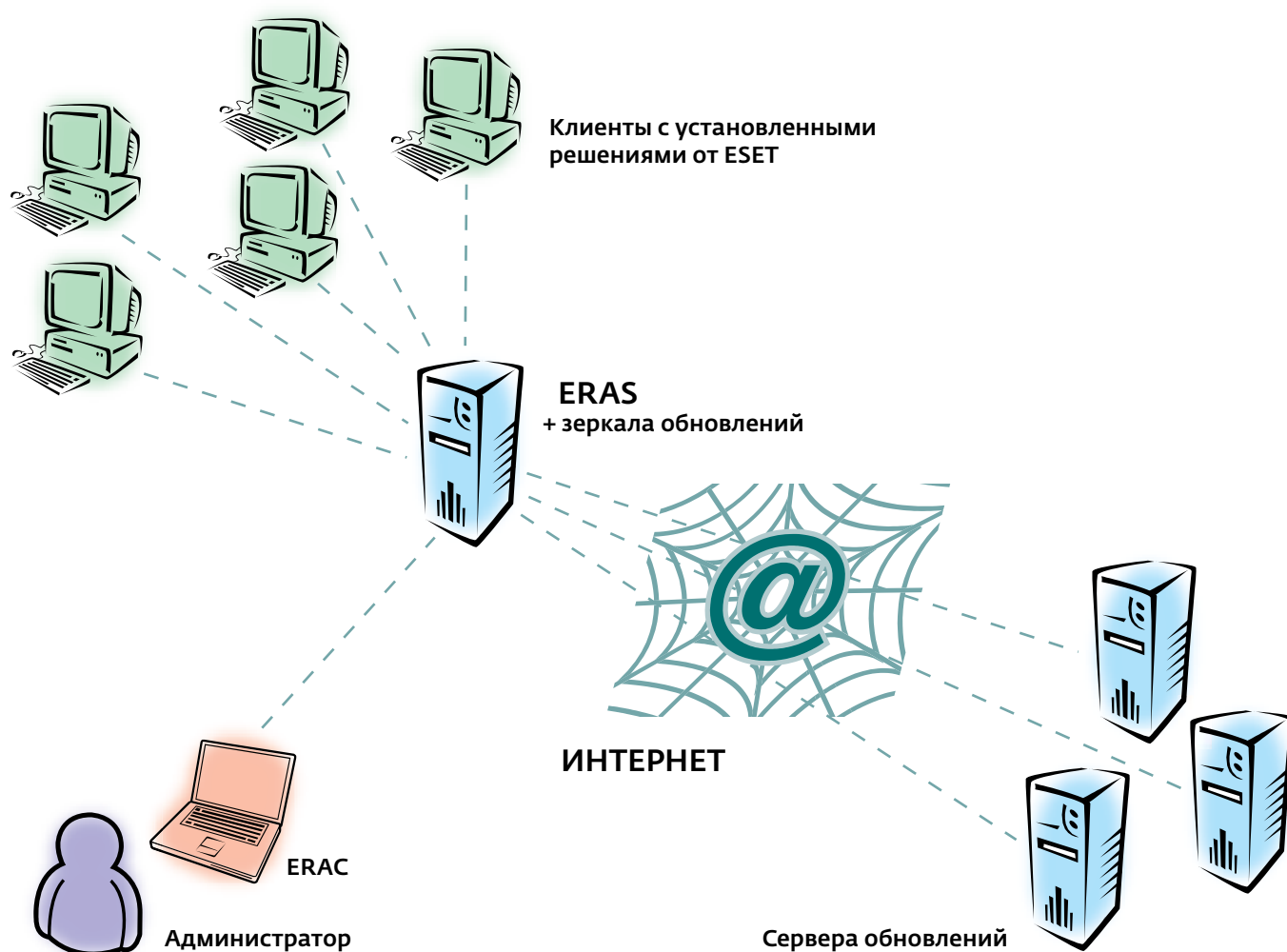


Рис. 1 Упрощенная модель развертывания: ESET для Windows-клиентов, ESET Remote Administrator. ERAS и MIRROR SERVER могут, но не обязательно должны быть установлены в той же системе.

2. ERA – архитектура клиент-сервер

С технической точки зрения ESET Remote Administrator состоит из двух отдельных компонентов: сервера ERA (ERA Server – ERAS) и Консоли ERA (ERA Console – ERAC). В вашей сети может функционировать неограниченное количество серверов и клиентов ERA, поскольку лицензионное соглашение не накладывает на этот счет никаких ограничений. Единственным ограничением является общее число клиентов, которые можно администрировать в вашей системе ERA (см. раздел 2.1.6 «Ключи лицензии»).

2.1 Сервер ERA (ERAS)

Серверный компонент архитектуры ERA выполняется как служба, функционирующая в одной из следующих операционных систем семейства Microsoft Windows® NT: NT4, 2000, XP или 2003, Vista. Основной задачей этой службы является сбор информации от клиентов и отправка им различных запросов. Запросы, в том числе на выполнение конфигурационных задач и удаленную установку, создаются с использованием Консоли ERA.

ERAS является связующим звеном между ERAC и клиентскими компьютерами – именно здесь вся информация обрабатывается, хранится и модифицируется перед передачей клиентам или ERAC.

2.1.1 Требования

ERAS функционирует как служба, а потому должен быть установлен в операционной системе семейства Microsoft Windows NT (NT4, 2000, XP, 2003). Наличие Microsoft Windows Server Edition не является обязательным для работы ERAS. Компьютер, на котором установлен ERAS, должен быть постоянно (24 часа в сутки 7 дней в неделю), включенным и доступным через компьютерную сеть для:

- клиентов (обычно рабочих станций);
- ПК с Консолью ERA;
- других экземпляров ERAS (если он реплицирован).

В приведенной ниже таблице представлен список возможных вариантов сетевого взаимодействия, которое может осуществляться, когда ERAS установлен. Процесс ega.exe слушает TCP-порты 2222, 2223, 2224 и 2846. Другие виды взаимодействия связаны также с собственными процессами операционной системы (например, «NetBIOS через TCP/IP»).

Протокол	Порт	Описание
TCP	2222 (ERAS прослушивает)	Взаимодействие между клиентами и ERAS
TCP	2223 (ERAS прослушивает)	Взаимодействие между ERAC и ERAS
TCP	2221 (ERAS прослушивает)	По умолчанию через этот порт предлагаются пакеты обновлений с использованием интегрированной в ERAS функции зеркала (взаимодействие посредством HTTP)

При использовании всех функций программы необходимо открытие дополнительных сеансов сетевого взаимодействия

Протокол	Порт	Описание
TCP	2224 (ERAS прослушивает)	Взаимодействие между агентом einstaller.exe и ERAS с ходе удаленной установки
TCP	2846 (ERAS прослушивает)	Репликация ERAS
TCP	139 (целевой порт с точки зрения ERAS)	Копирование агента einstaller.exe с ERAS на клиент в ходе активной установки с использованием общей папки admin\$
UDP	137 (целевой порт с точки зрения ERAS)	«Разрешение имен» в ходе удаленной установки
UDP	138 (целевой порт с точки зрения ERAS)	«Браузинг» во время удаленной установки
TCP	445 (целевой порт с точки зрения ERAS)	Прямой доступ к общим ресурсам с использованием TCP/IP в ходе удаленной установки (альтернатива TCP 139)

Минимальная аппаратная конфигурация, необходимая для развертывания ERAS, является также рекомендуемой минимальной конфигурацией для используемой на том же компьютере операционной системы Microsoft Windows.

2.1.2 Иерархия ERAS в больших сетях

В большой сети можно установить дополнительные серверы ERA и в дальнейшем выполнять удаленную установку программного обеспечения клиентских компьютеров с тех серверов, которые наиболее легко доступны. Для этой цели предлагается использовать технологию репликации, позволяющую перенаправлять сохраняемую информацию серверу ERA, расположенному уровнем выше по иерархии («родительскому серверу»). Настройку репликации можно осуществлять посредством ERAC.

Функция репликации является эффективным решением для компаний, имеющих разветвленную структуру или удаленные подразделения. Сценарий развертывания для такой модели может быть следующим: серверы ERA устанавливаются в каждом подразделении, а затем реплицируются на центральный сервер ERA, находящийся в основном офисе компании. Преимущества такой конфигурации наиболее очевидны для частных сетей на базе VPN, которые обычно не отличаются быстродействием, – администратору достаточно подключиться к центральному ERAS (ниже на иллюстрации это соединение обозначено буквой А). Ему не нужно использовать VPN-туннели, являющиеся относительно медленнодействующими коммуникационными каналами, для доступа к отдельным подразделениям (соединения В, С, D и Е), – вся необходимая работа осуществляется посредством репликации сервера ERA.

Настраивая систему репликации, администратор определяет, какая информация будет автоматически с заданной периодичностью передаваться на родительские серверы, и какая информация будет отправляться с дочерних серверов по запросам администратора родительского сервера. Репликация облегчает пользователям работу с ERA и минимизирует сетевую нагрузку.

Еще одним преимуществом репликации является то, что она позволяет входить в систему разным пользователям с разными уровнями полномочий. Администратор, осуществляющий доступ к ERAS london1.company.com с консоли (соединение Е), может администрировать только клиентов, подключенные к london1.company.com, london2.company.com и paris.company.com. Если же он подключится к central.company.com (соединение А), то сможет управлять всеми клиентами, находящимися в основном офисе компании и ее подразделениях либо филиалах.

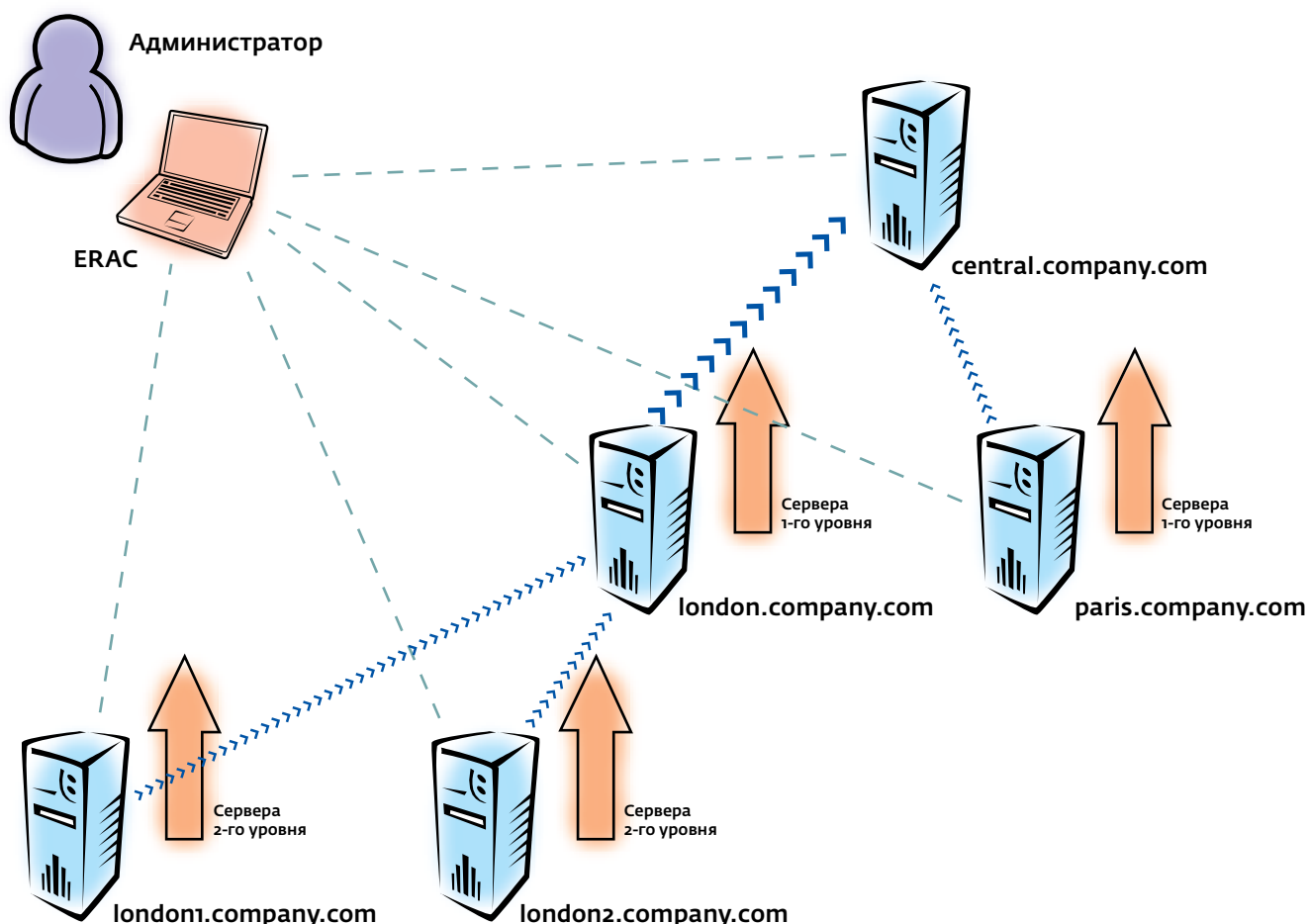


Рис. 2 Репликация в сети, состоящей из сети основного офиса и сетей подразделений либо филиалов.

2.1.3 Установка

Процесс установки инициируется путем запуска пакета установки. В ходе этого процесса вас попросят предоставить ключ лицензии, представляющий собой файл с расширением LIC. Если выбран режим установки Expert (Экспертная), будет определено еще несколько параметров. Впоследствии вы сможете модифицировать их в ERAC, но, как правило, необходимости в этом не возникает. Единственным исключением является имя сервера. Оно должно быть таким же, как в DNS, или совпадать со значением параметра Имя компьютера (Computer name) в вашей операционной системе, задаваемого на вкладке **Имя компьютера** (Computer name) в окне, открываемом командой **Мой компьютер – Свойства** (My Computer – Properties). Также может использоваться IP-адрес компьютера. Это наиболее важная информация, необходимая для удаленной установки. Если не задать при установке имя сервера, программа установки автоматически использует значение системной переменной `%COMPUTERNAME%`, которое в большинстве случаев является вполне подходящим.

По умолчанию программные компоненты ERAS устанавливаются в следующую папку:

`%ProgramFiles%\Eset\Eset Remote Administrator\Server`

Другие «переменные» компоненты (журналы, пакеты установки, конфигурация и т. п.) записываются в папку:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server`

ПРИМЕЧАНИЕ. На серверах с ERAS необходимо устанавливать и клиентское программное обеспечение. ERAS принимает номер текущей версии базы данных вирусных сигнатур и использует его в качестве ссылочного значения для клиентов. Предлагается установка решения с LAN Update Server (зеркало).

2.1.4 Журналы

ERAS не генерирует выходных данных для файла журнала. Этот файл находится в папке:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs`

В файле журнала `era.log` содержатся записи обо всех событиях, которые произошли во время работы ERAS, включая сообщения об ошибках, связанных с запуском службы ERAS (например, о повреждении базы данных или ключа лицензии). Используя этот журнал, можно быстро выявить точную причину, по которой ERAS не был успешно запущен.

ПРИМЕЧАНИЕ. В программе настройки ERAS (доступной через ERAC) можно определить несколько уровней протоколирования, включая ротацию журналов, позволяющую значительно уменьшить размер файла и темп увеличения его размера. Можно также настроить ERAS таким образом, чтобы для протоколирования его событий использовался стандартный журнал приложений операционной системы.

2.1.5 Конфигурация

Основную работу по конфигурированию ERAS можно выполнить прямо в процессе установки, особенно, если она осуществляется в расширенном режиме, или позднее, используя Консоль ERA, подключенную к серверу ERA. При необходимости можно модифицировать находящиеся на сервере конфигурационные XML-файлы. Эти файлы находятся в следующей папке:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\configuration`

ПРИМЕЧАНИЕ. По соображениям, связанным с безопасностью, параметры настройки паролей отделены от других параметров (они находятся в отдельных XML-файлах). В случае утраты паролей (тех, что необходимы для доступа к серверу ERA) удалите файл `era_private.xml`, находящийся в папке Configuration.

2.1.6 Ключи лицензии

Ключ лицензии – это защищенный электронной подписью файл с расширением LIC, структура которого напоминает XML-формат. Наличие этого файла является важнейшим фактором успешного конфигурирования ERAS. Файл ключа лицензии содержит следующую информацию:

- владелец лицензии;
- количество клиентских компьютеров (количество лицензий);
- дата устаревания лицензии.

Вот четыре типичные проблемы, связанные с файлами ключей лицензии:

- **.LIC-файл отсутствует**
ERAS запустится в пробном режиме, в котором поддерживается администрирование не более 2 клиентов (рабочих станций) в течение неограниченного времени.
- **.LIC-файл поврежден**
Служба ERAS не запустится вовсе. В файл `era.log` будет записано соответствующее сообщение.
- **.LIC-файл устарел**
Если указанная в LIC-файле дата устаревания больше текущей даты, установка соединения между ERAC и ERAS невозможна. ERAS по-прежнему будет принимать информацию от клиентов, но не позволит осуществлять их администрирование.

■ Превышено количество клиентов, определенное в LIC-файле

Об этом факте вы узнаете из выводимых ERAC сообщений об ошибках. Администрирование дополнительных клиентов, взаимодействующих с ERA Server, будет невозможно.

Ключи лицензии должны храниться в следующей папке:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\license`

В процессе установки ERAS ключи лицензии автоматически копируются в указанную выше папку. При изменении или обновлении лицензии необходимо обновить ключ лицензии вручную. Данная папка может содержать несколько файлов ключей лицензии, но ERAS всегда выбирает наиболее подходящий файл с расширением LIC. Каждый раз, когда потребуется использовать новую лицензию, необходимо будет перезапустить службу ERAS.

Существует несколько способов передачи ключей лицензии ERAS:

- скопировать их в упомянутую выше папку, куда установлен сервер ERA, после чего перезапустить службу ERAS;
- воспользоваться входящим в состав ERAC Редактором конфигурации ESET и удаленно импортировать ключи лицензии в ERAS;
- импортировать ключи лицензии с помощью функции **Лицензии** (Licenses) продукта ESET Smart Security/ESET NOD32 Antivirus.

2.1.7 База данных и хранение информации

Для хранения данных ERAS использует MDAC (Microsoft Data Access Components – компоненты Microsoft для доступа к данным), а более крупные информационные элементы сохраняет в отдельных файлах (в папке Storage).

В состав ERAS входят средства, позволяющие администраторам автоматически выполнять операции по обслуживанию базы данных и хранящейся информации. Соответствующую настройку можно произвести во время установки (в экспертном режиме) или позднее посредством ERAC. Операции по обслуживанию базы данных направлены на ускорение обработки запросов к ней от ERAS и на обеспечение экономии дискового пространства.

Мы рекомендуем использовать стандартную конфигурацию, согласно которой удаляются все элементы, хранящиеся более 6 месяцев. Уменьшать это значение целесообразно лишь в случаях, когда система перегружена записями от тысяч клиентов.

База данных хранится в следующей папке:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\database`

Файлы, связанные с записями в базе данных, хранятся в папке:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\storage`

Информация о взаимодействии клиентов с ERAS хранится в отдельных файлах. Эти файлы находятся в папке Storage и содержат следующую информацию:

- подробные сведения о клиенте (XML-конфигурация, состояние защиты, функции защиты, системная информация);
- подробные сведения из журналов (журнала угроз и журнала сканирования);
- подробные сведения о заданиях;
- подробные сведения из генерируемых по расписанию отчетов (они не имеют прямого отношения к взаимодействию клиента и ERAS).

ПРИМЕЧАНИЕ. Если папка **Storage** находится на компьютере с файловой системой NTFS и содержит большой объем информации, можно значительно уменьшить размер этой папки с помощью имеющейся в NTFS функции сжатия.

2.2 Консоль ERA (ERAC)

Консоль ERA, или ERAC, является клиентским компонентом ERA, обычно устанавливаемым на рабочую станцию. Эта рабочая станция используется администратором для удаленного управления решениями ESET на отдельных клиентах. С помощью ERAC администратор может подключиться к серверному компоненту ERA – используя целевой TCP-порт 2223. Взаимодействием управляет процесс console.exe, исполняемый файл которого обычно находится в папке:

`%ProgramFiles%\Eset\Eset Remote Administrator\Console` (Можно также открыть Консоль ERA, выбрав в меню **Пуск – Все программы** (Start – All Programs) команду **ESET – ESET NOD32 Remote Administrator Console**).

При установке ERAC от вас может потребоваться ввод имени сервера ERA. После запуска консоль будет автоматически подключаться к указанному вами серверу. Настройка Консоли ERA может быть выполнена и после установки продукта.

HTML-вывод ERAC (графические журналы) сохраняется локально. Всю остальную информацию ERAS отправляет в составе данных, пересылаемых через TCP-порт 2223. 3.1 Клиентские решения ESET

Клиентские решения – это программные продукты, предназначенные для обнаружения и блокирования вредоносного кода на рабочих станциях и серверах. Главнейшими из клиентских решений являются ESET NOD32 Antivirus 3.0 и ESET Smart Security.

Клиенты устанавливают взаимодействие по двум главным каналам:

3. Другие компоненты ESET в сетевой среде

3.1 Клиентские решения ESET

Клиентские решения – это программные продукты, предназначенные для обнаружения и блокирования вредоносного кода на рабочих станциях и серверах. Главнейшими из клиентских решений являются ESET NOD32 Antivirus 3.0 и ESET Smart Security.

Клиенты устанавливают взаимодействие по двум главным каналам:

- с сервером ERA через TCP-порт 2222 для передачи текущих данных (журналы, используемая конфигурация, сообщения об угрозах и т. п.) и выполнения поступающих от ERAS заданий и запросов (изменение конфигурации, выполнение сканирования и т. д.);
- со своим сервером обновлений через определенный порт (используя протокол HTTP или SMB), далее в этом руководстве будет описан метод, позволяющий администратору создать локальный сервер обновлений, или «зеркало» серверов обновлений ESET.

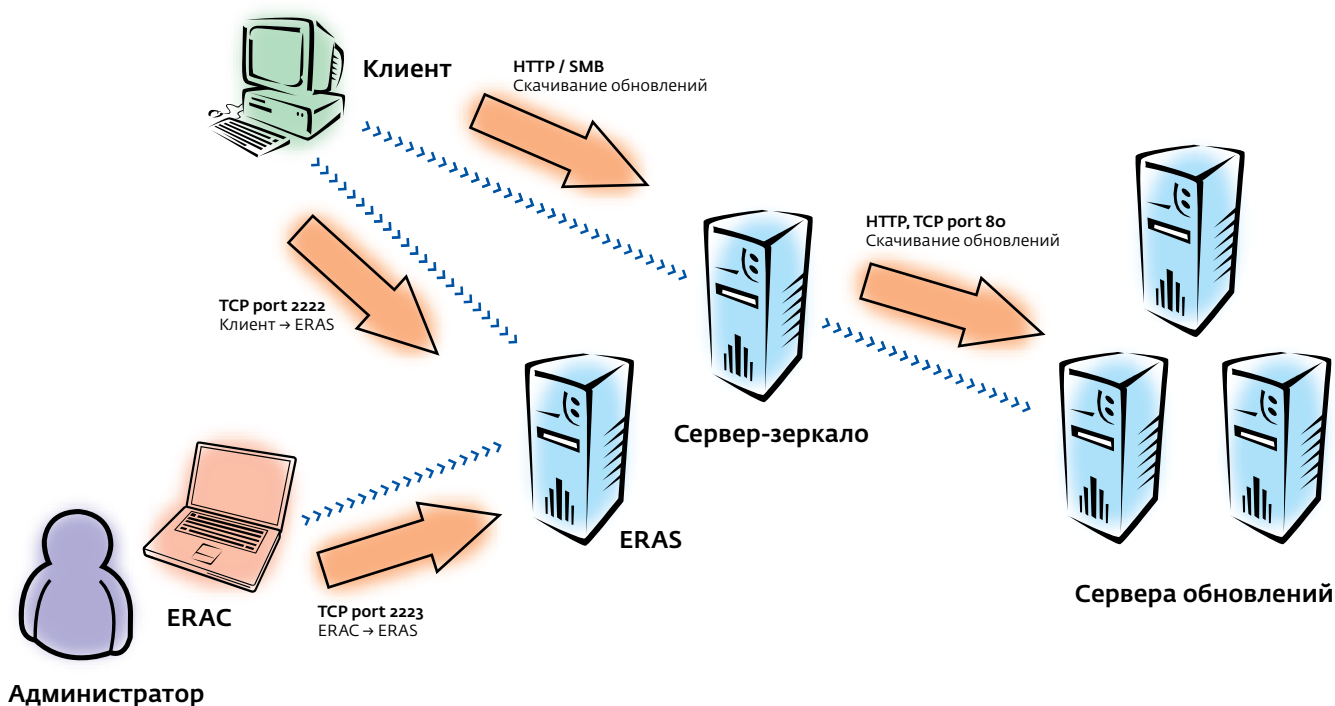


Рис. 3 Наиболее важные коммуникационные каналы, связывающие ERAS, ERAC и серверы обновлений. ERAS и сервер-зеркало могут функционировать на одном компьютере

3.2 Редактор конфигурации ESET

Редактор конфигурации ESET – важный компонент ERAC, используемый для нескольких целей. Одной из важнейших среди них является создание следующих элементов:

- предварительно определенных конфигураций для пакетов установки;
- конфигураций, которые отправляются клиентам как задания;
- глобального конфигурационного XML-файла.

Редактор конфигурации позволяет администратору удаленно конфигурировать практически каждый параметр любого из решений ESET. Кроме того, он дает администратору возможность экспортировать конфигурации в XML-файлы, которые позднее могут использоваться для разных целей (например, для создания заданий в ERAC, импорта конфигурации локально в ESET Smart Security и т. д.).

Редактор конфигурации сохраняет информацию о конфигурации в древовидной структуре, формируемой на основе шаблона. Этот шаблон хранится в файле `cfgedit.exe`.

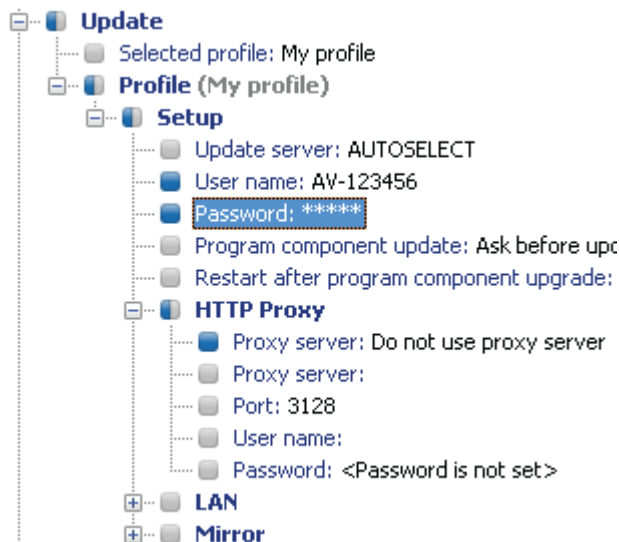
Редактор конфигурации позволяет модифицировать любой XML-файл. Ни в коем случае не изменяйте и не перезаписывайте файл `cfgedit.xml`! Правильная работа Редактором конфигурации зависит также от следующих файлов: `guiEpfw.dll`, `cfgeditLang.dll` и `eguiEpfwLang.dll`.

Для доступа к Редактору конфигурации выберите в Консоли ERA команду **Инструменты – Редактор конфигурации ESET (Tools – ESET Configuration Editor)**.

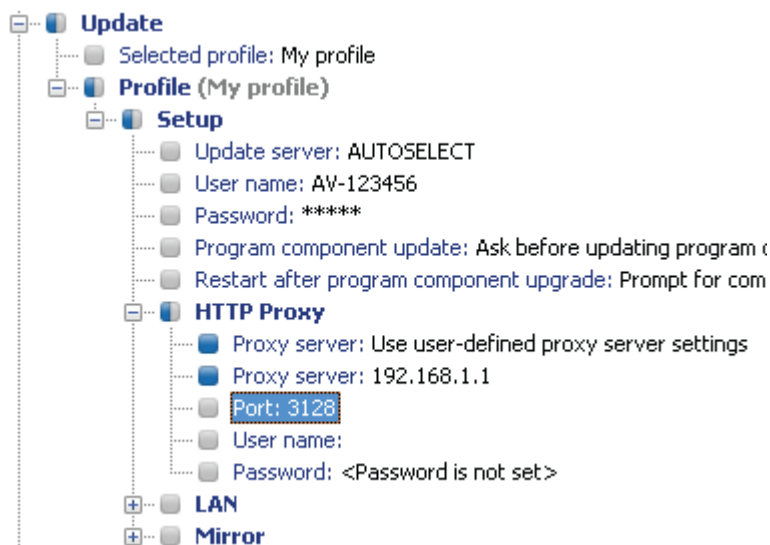
3.2.1 Наложение конфигураций

Если в Редакторе конфигурации изменяется значение того или иного параметра, он помечается синим значком. Если значок параметра серый, значит, его значение еще не менялось и не будет записано в выходной конфигурационный XML-файл. При конфигурировании клиентов к ним применяются только те установки, которые сохранены в XML-файле.

Ниже продемонстрирован пример описанной ситуации. В данной конфигурации определены имя и пароль пользователя и запрещено использование прокси-сервера.



В другой конфигурации, представленной ниже, определены те же имя (AV-123456) и пароль пользователя, чтобы при ее применении не изменились предшествующие установки этих параметров, но использование прокси-сервера разрешено и определены его адрес и порт.



3.2.2 Важнейшие элементы конфигурации

В этом разделе перечислены и описаны важнейшие конфигурационные элементы ESET Smart Security, доступные посредством Редактора конфигурации ESET (Инструменты – Редактор конфигурации ESET (Tools – ESET Configuration Editor)). Для изменения той или иной установки выберите в древовидном представлении конфигурации требуемый элемент (слева) и измените его значение (справа).

- **Ядро – Настройка – Удаленный администратор (Kernel – Setup – Remote administrator)**
Здесь можно разрешить взаимодействие клиентских компьютеров с сервером ERA, включив параметр **Подключаться к серверу Remote Administrator (Connect to Remote Administrator server)**. Задайте имя сервера ERA или его IP-адрес в параметре **Адрес сервера (Server address)**. Для параметра **Интервал между подключениями к серверу (Interval between connections to server)** следует оставить заданное по умолчанию значение 5 минут. Для целей тестирования это значение можно уменьшить до 0, чтобы подключение устанавливалось каждые 10 секунд. Если будете менять значение параметра **Пароль (Password)**, задайте тот же пароль, который задан в ERAS (см. главу о конфигурировании ERAS — параметр **Пароль для клиентов (Password for Clients)**). Тогда взаимодействие между клиентами и ERAS будет шифроваться.

■ **Ядро – Настройка – Ключи лицензии** (Kernel – Setup – License keys)

Клиентским компьютерам добавление лицензионных ключей и управление ими не требуется. Ключи лицензии используются лишь некоторыми серверными решениями.

■ **Ядро – Настройка – ThreatSense.Net** (Kernel – Setup – ThreatSense.Net)

Эта ветвь определяет поведение Системы раннего обнаружения ThreatSense.Net, позволяющей отправлять подозрительные файлы в лабораторию ESET на анализ. При развертывании решений ESET в крупных сетях особенно важны параметры **Предоставлять подозрительные файлы** (Submit suspicious files) и **Разрешить предоставление анонимной статистической информации** (Enable submission of anonymous statistical information). Если для них установлены значения **Не предоставлять** (Do not submit) и **Нет** (No) соответственно, ThreatSense.Net System полностью отключена. Для того чтобы предоставление файлов осуществлялось автоматически, без участия пользователя, выберите для указанных параметров значения **Предоставлять, не спрашивая** (Submit without asking) и **Да** (Yes). Если соединение с интернетом устанавливается через прокси-сервер, задайте параметры подключения к этому серверу в разделе **Ядро – Настройка – Прокси-сервер** (Kernel – Setup – Proxy server).

■ **Ядро – Настройка – Защитить параметры настройки** (Kernel – Setup – Protect setup parameters)

Позволяет администратору защитить параметры настройки паролем. Если пароль задан, система будет запрашивать его перед предоставлением доступа к параметрам настройки с клиентских рабочих станций. Однако установка пароля не повлияет на возможность внесения изменений в конфигурацию из ERAC.

■ **Ядро – Настройка – Планировщик** (Kernel – Setup – Scheduler/Planner)

В этом разделе содержатся параметры планировщика, позволяющего администратору задавать расписания для регулярного выполнения антивирусного сканирования, обновления сигнатур вирусов и т. д.

ПРИМЕЧАНИЕ. По умолчанию все решения ESET, связанные с защитой, содержат несколько предварительно определенных заданий. В большинстве случаев редактировать их или добавлять новые задания не обязательно.

■ **Обновление** (Update)

Эта ветвь Редактора конфигураций позволяет определять способ обновления вирусных сигнатур и программных компонентов на клиентских рабочих станциях. В большинстве случаев необходимо лишь модифицировать готовый профиль **Мой профиль** (My profile) и задать значения параметров **Сервер обновлений** (Update server), **Имя пользователя** (User name) и **Пароль** (Password). Если для параметра **Сервер обновлений** (Update server) выбрано значение **Автоматический выбор** (Choose Automatically), все обновления будут загружаться с серверов обновлений ESET. В таком случае задайте в параметрах **Имя пользователя** (User name) и **Пароль** (Password) имя и пароль пользователя, присланные вам при покупке продукта. За информацией о настройке клиентских рабочих станций для получения обновлений от локального сервера (зеркала) обратитесь к разделу 3.3, «LAN Update Server – зеркало».

ПРИМЕЧАНИЕ. На мобильных устройствах могут быть сконфигурированы два профиля – один для обновления с сервера-зеркала, а другой для загрузки обновлений прямо с серверов ESET.

Дополнительные сведения см. в разделе 8.2 «Комбинированное обновление для ноутбуков и мобильных устройств».

3.3 LAN Update Server – зеркало

Функция зеркала позволяет пользователю создать локальный сервер обновлений. При наличии такого сервера-зеркала клиентские компьютеры будут загружать обновления вирусных сигнатур с него (через локальную или связанную с ней сеть), не обращаясь к серверам обновлений ESET через интернет. Главным преимуществом такого решения является экономия полосы пропускания сети компании и минимизация сетевого трафика (к интернету) вместо сотен клиентских компьютеров подключается за обновлениями только сервер-зеркало). Единственным недостатком является то, что в случае выхода из строя сервера-зеркала (если он является единственным) клиентские компьютеры перестанут получать обновления.

Внимание!

Если после обновления программных компонентов сервера-зеркала не выполнить его перезагрузку, он может перестать работать. Этот сервер не сможет более загружать обновления и передавать их на клиентские компьютеры. **НЕ ЗАДАВАЙТЕ АВТОМАТИЧЕСКИЙ РЕЖИМ ОБНОВЛЕНИЯ ПРОГРАММНЫХ КОМПОНЕНТОВ ДЛЯ СЕРВЕРНЫХ РЕШЕНИЙ ESET!** (Дополнительную информацию об обновлении программных компонентов см. в разделе 3.3.1.)

Функция зеркала поддерживается для:

- ESET Remote Administrator (зеркало физически функционирует в ERAS, а управление им осуществляется из ERAC);
- ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition (при условии, что версия Business Edition продукта активирована с использованием ключа лицензии).

Метод активации функции зеркала выбирает администратор (имейте в виду, что при одновременном использовании обеих версий возможен конфликт в отношении TCP-порта 2221).

В больших сетях возможно создание дополнительных зеркал (например, для разных подразделений компании) и определение их иерархии с выделением одного из них как центрального (в основном офисе компании) – подобно конфигурации ERAS со многими клиентами.

3.3.1 Функционирование сервера-зеркала

Любой сервер (или рабочая станция), выполняющий роль зеркала, должен работать постоянно (24 часа в сутки 7 дней в неделю) и быть подключенным к интернету или к центральному зеркалу (в конфигурации с репликацией). Пакеты обновлений сервера-зеркала могут загружаться двумя способами:

- с использованием протокола HTTP (рекомендуется).
- с использованием общего сетевого диска (по протоколу SMB).

Серверы обновлений ESET используют для аутентификации протокол HTTP. Центральный зеркальный сервер должен осуществлять доступ к серверам обновлений, указывая имя пользователя (обычно в форме: EAV-XXXXXXX) и пароль.

Сервер-зеркало, входящий в состав системы ESET Smart Security либо ESET NOD32 Antivirus, имеет интегрированный веб-сервер, доступ к которому осуществляется по протоколу HTTP, не требующий аутентификации. Это означает, что клиентам, которые обращаются к этому интегрированному HTTP-серверу, имя пользователя и пароль для аутентификации не требуются.

ПРИМЕЧАНИЕ. Если используется интегрированный HTTP-сервер, он должен быть недоступен извне вашей сети (то есть для клиентов, не включенных в лицензию). Этот сервер должен быть недоступен из Интернета.

ПРИМЕЧАНИЕ. По умолчанию интегрированный HTTP-сервер слушает TCP-порт 8081. Убедитесь, что этот порт не занят другим приложением!

Может также использоваться HTTP-сервер любого другого типа. ESET поддерживает дополнительные методы аутентификации (доступ с указанием имени и пароля – в Apache Web Server используется метод доступа с использованием файла .htaccess).

Второй метод (общая сетевая папка) требует открытия общего доступа (для чтения) к папке, в которой хранятся пакеты обновлений (папка Mirror). При его использовании имя и пароль пользователя, имеющего право чтения из папки обновлений, должны вводиться на клиентской рабочей станции.

ПРИМЕЧАНИЕ. Клиентские решения ESET используют учетную запись пользователя SYSTEM, и поэтому их права на доступ к сетевым ресурсам отличаются от прав текущего вошедшего в систему пользователя. Аутентификация необходима даже в случае, если сетевой диск доступен всем и текущий пользователь также имеет к нему доступ. Сетевой путь к локальному серверу следует задавать в формате UNC. Использовать формат `DISK:\` не рекомендуется!

При осуществлении доступа к обновлениям через общую папку рекомендуется определить для этой цели отдельное имя пользователя (например, `NODUSER`). Данную учетную запись следует использовать на всех клиентских компьютерах с единственной целью загрузки обновлений. Учетная запись `NODUSER` должна иметь разрешение на чтение из общей сетевой папки, содержащей пакеты обновлений.

ПРИМЕЧАНИЕ. Аутентификационные данные для доступа к сетевому диску следует вводить в полной форме: `РАБОЧАЯ_ГРУППА\Пользователь` или `ДОМЕН\Пользователь`.

Помимо аутентификационных данных для клиентских решений ESET следует определить источник обновлений. Его задают либо как URL-адрес локального сервера:

`http://имя_сервера_зеркала:порт`

либо как UNC-путь к сетевому диску:

`\\имя_сервера_зеркала\имя_общей_папки`

3.3.2 Типы обновлений

Помимо регулярных обновлений базы данных вирусных сигнатур, включающих и обновления ядра ESET, время от времени могут загружаться обновления программных компонентов. Как правило, программные обновления добавляют новые возможности в решения ESET, связанные с защитой, и поэтому требуют перезагрузки компьютера. Если в сети установлен сервер-зеркало, программные обновления загружаются с этого зеркала.

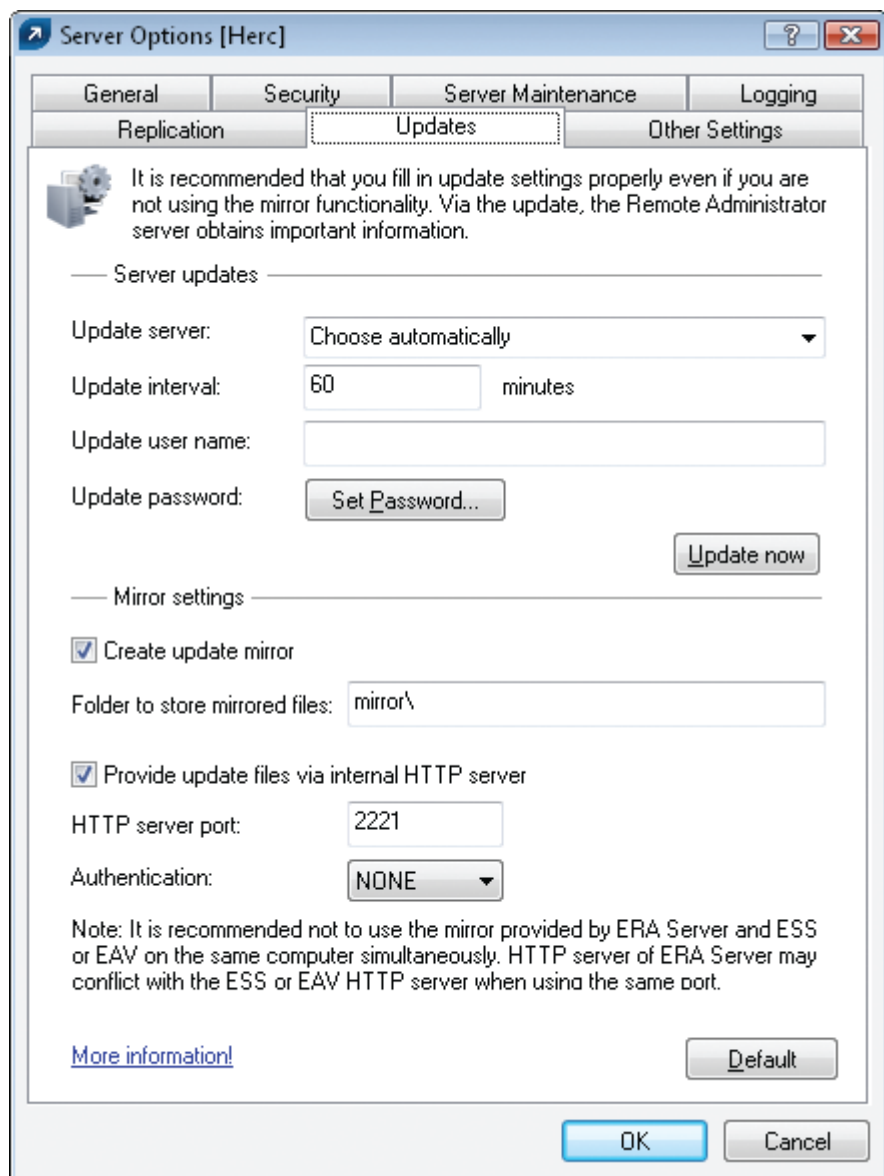
Наличие сервера-зеркала позволяет администратору отключить автоматическую загрузку программных обновлений с серверов обновлений ESET (или с родительского сервера-зеркала) и отключить их рассылку клиентам. Позднее администратор может вручную инициировать рассылку обновлений с зеркала (например, когда будет уверен, что между новой версией и прочими приложениями не возникнет конфликтов).

Данная возможность особенно полезна в случае, когда администратор желает загрузить и использовать обновления базы данных вирусных сигнатур, но не хочет устанавливать имеющиеся на серверах обновлений ESET новые версии программных компонентов. Администратор может вначале протестировать новую версию программного обеспечения в тестовой среде, и лишь затем ввести ее в эксплуатацию. Если старая версия программы используется совместно с последней версией вирусной базы данных, программа по-прежнему будет обеспечивать наилучшую возможную защиту. Однако рекомендуется не затягивать с загрузкой и установкой новейших версий программы.

3.3.3 Как создать и настроить зеркало

Если зеркало интегрировано прямо в используемый продукт ESET Remote Administrator (версия Business Edition), подключитесь к ERAS посредством Консоли ERA и выполните указанные ниже действия:

- В Консоли ERA выберите команду **Инструменты – Параметры сервера** (Tools – Server Options) и в открывшемся окне перейдите на вкладку **Обновления** (Updates).
- В раскрывающемся списке **Сервер обновлений** (Update server) выберите установку **Автоматический выбор** (Choose Automatically), чтобы обновления загружались с серверов ESET, или выберите путь **URL/UNC** к серверу-зеркалу.
- Задайте в поле **Интервал обновления** (Update interval) подходящее значение (рекомендуется загружать обновления каждые 60 минут).
- Если выше выбрана установка **Автоматический выбор** (Choose Automatically), введите в поле **Имя пользователя обновлений** (Update user name) имя пользователя, присланное вам при покупке продукта (если осуществляется доступ к серверу, расположенному выше по иерархии, введите доменное имя пользователя и пароль к этому серверу).
- Установите флажок **Создать зеркало обновлений** (Create update mirror) и введите путь к папке, в которой будут храниться файлы обновлений. По умолчанию это относительный путь к папке **Mirror**, если выбрана установка **Предоставлять файлы обновлений через внутренний сервер HTTP** (Provide update files via internal HTTP server) (и папка доступна через HTTP-порт, указанный в поле **Порт сервера HTTP** (HTTP server port), по умолчанию – 2221).
- Для параметра **Аутентификация** (Authentication) выберите значение **НЕТ** (NONE).
- В режиме расширенной настройки выберите компоненты, которые подлежат загрузке (необходимо выбрать компоненты для всех языковых версий, которые будут использоваться в сети).



Функция зеркала непосредственно доступна из интерфейса программ ESET Smart Security Business Edition и ESET NOD32 Antivirus Business Edition. Какой интерфейс использовать для реализации сервера-зеркала, администратор выбирает по своему усмотрению.

Для активации и загрузки сервера зеркала из ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition выполните следующие действия.

- Установите ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition.
- В режиме расширенной настройки (F5) выберите **Разное – Ключи лицензии** (Miscellaneous – License keys). Нажмите кнопку **Добавить** (Add), найдите файл [nod32.lic](#) и нажмите кнопку **Открыть** (Open). В результате лицензия будет установлена, и вы сможете сконфигурировать функцию зеркала.
- В разделе **Обновление** (Update) нажмите кнопку **Настройка** (Setup) и выберите вкладку **Зеркало** (Mirror).
- Выберите установки **Создать зеркало обновлений** (Create update mirror) и **Предоставлять файлы обновлений через внутренний сервер HTTP** (Provide update files via internal HTTP server).

Введите полный путь к папке (Mirror), где будут храниться файлы обновлений (не указывайте путь к сетевому ресурсу do not reference a mapped network drive).

- Значения параметров **Имя пользователя** (User name) и **Пароль** (Password) используются для аутентификации клиентских рабочих станций, пытающихся получить доступ к папке Mirror. В большинстве случаев заполнять эти поля не обязательно, поскольку аутентификационные данные будут вводиться на уровне клиента.
- Нажмите кнопку **Расширенная настройка** (Advanced Setup) и выберите для параметра **Аутентификация** (Authentication) значение **НЕТ** (NONE).
- В режиме расширенной настройки выберите компоненты, которые подлежат загрузке (необходимо выбрать компоненты для всех языковых версий, которые будут использоваться в сети).

Для достижения оптимальной функциональности рекомендуется разрешить загрузку и зеркалирование программных компонентов. Если данная функция отключена, будут обновляться только сигнатуры вирусов, но не программные компоненты. Если используется зеркало в составе ESET Remote Administrator, указанную функцию можно настроить в ERA. Для этого нужно выбрать команду **Инструменты – Параметры сервера** (Tools – Server Options), затем перейти на вкладку **Другие параметры** (Other Settings), нажать кнопку **Редактировать дополнительные параметры** (Edit Advanced Settings) и выбрать **ESET NOD32 Remote Administrator – Сервер ERA – Настройка – Зеркало** (ESET Remote Administrator – ERA Server – Setup – Mirror). Выберите все языковые версии программы, используемые в вашей сети.

* Дополнительную информацию см. в разделе 2.1.5, посвященном конфигурированию сервера ERA.

4. Подробное описание консоли удаленного администратора ESET NOD32 Remote Administrator

4.1 отключение к серверу ERA

Практически все компоненты консоли ERA становятся доступными только после подключения к серверу ERA. Перед первым подключением следует определить сервер, задав ему имя или IP-адрес:

Откройте раздел Консоль ERA (ERA Console), выберите **Файл – Редактировать соединения...** (File – Edit Connections...) и щелкните вкладку **Соединение** (Connection).

Нажмите кнопку **Добавить/Удалить...** (Add/Remove...), чтобы добавить новые или изменить имеющиеся в списке серверы ERA. Нажмите кнопку **ОК** (OK) после добавления или изменения серверов и выберите нужный сервер в списке **Выбрать соединение** (Select connection). Нажмите кнопку **Подключиться** (Connect).

Другие параметры данного окна:

- **Подключаться к выбранному серверу при запуске консоли** (Connect to selected server on the console startup) При выборе данного параметра консоль автоматически подключится к выбранному серверу ERA при запуске.
- **Показывать сообщение при неудачном соединении** (Show message when connection fails) При наличии сбоя связи между консолью ERA и сервером ERA появляется соответствующее предупреждение.

Соединения можно защитить паролем. По умолчанию для защиты подключения к серверу ERA пароль не задается, но его использование настоятельно рекомендуется. Чтобы создать пароль подключения к серверу ERA:

Выберите **Файл – Изменить пароль...** (File – Change Password...), затем нажмите кнопку **Изменить...** (Change...) справа параметра **Пароль для консоли** (Password for Console).

При вводе пароля можно воспользоваться флажком **Запомнить пароль** (Remember password) (при этом следует учесть возможный риск для безопасности). Чтобы удалить все сохраненные пароли, выберите **Файл – Удалить пароли из кэша...** (File – Clear Cached Passwords...).

В момент установления связи заголовок программы изменится на **Подключено [имя_сервера]** (Connected [server_name])

4.2 Консоль ERA – главный экран

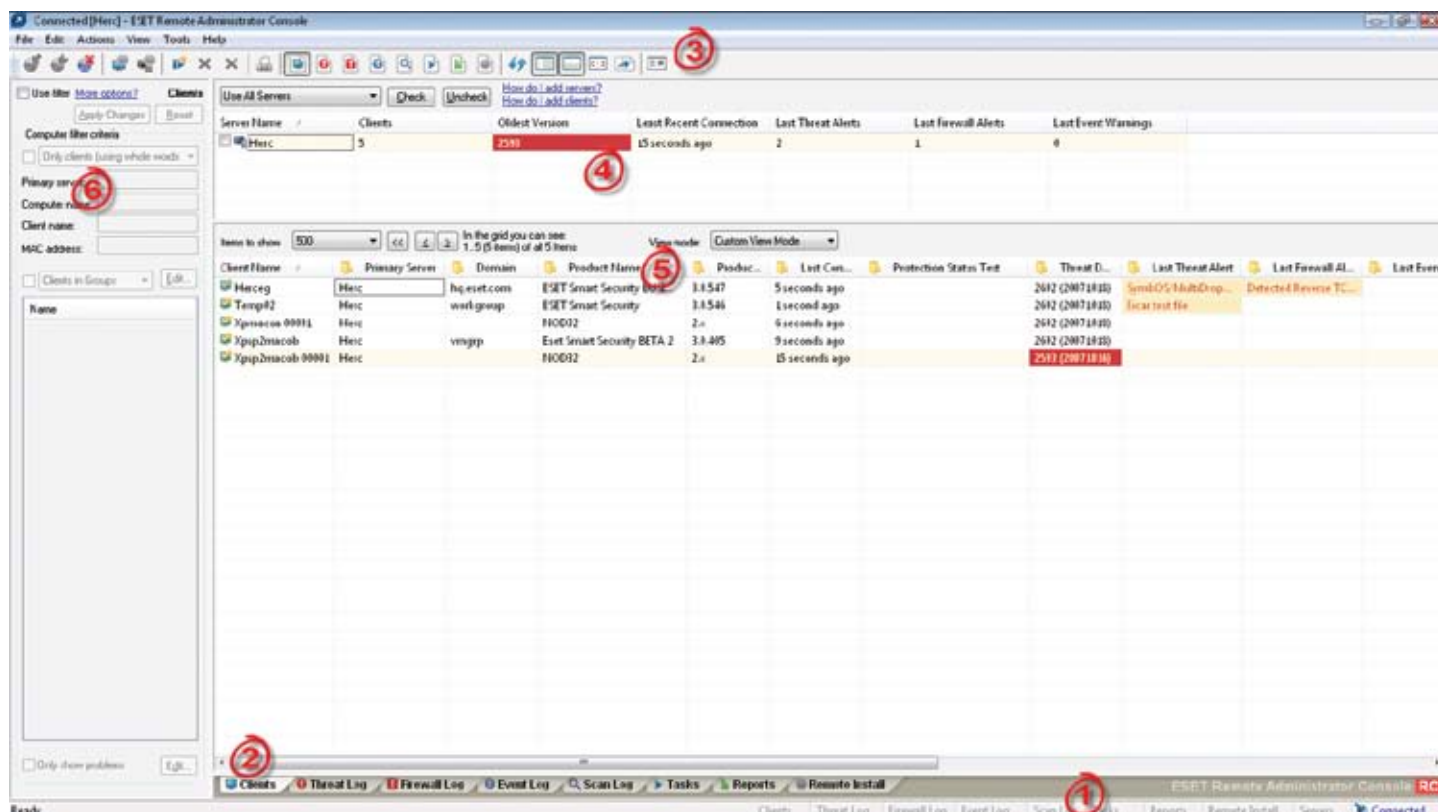


Рис. 4 Главный экран консоли удаленного администратора ESET Remote Administrator

В статусной строке отображается текущее состояние соединения между консолью ERA и сервером ERA (1). Все важные данные от сервера ERA регулярно обновляются (по умолчанию – каждую минуту. См. **Инструменты – Параметры консоли...** (Tools – Console Options...)). Процесс обновления также отображается в статусной строке.

ПРИМЕЧАНИЕ. Для обновления отображаемых данных нажмите F5.

Информация сосредоточена на нескольких вкладках (2) в порядке значимости. В большинстве случаев данные можно (5) отсортировать в восходящем или нисходящем порядке, щелкнув атрибут. Изменение порядка следования элементов достигается простым перетаскиванием. При необходимости обработки нескольких строк данных имеется возможность ограничения их количества с помощью пункта **Элементы** (Items) для отображения раскрывающегося списка и просмотра страниц с помощью кнопок пролистывания страниц. Выберите нужный режим просмотра атрибутов (View). Дополнительную информацию см. в разделе 4.3, «Фильтрация информации».

Раздел **Сервер** (Server) (4) необходим при репликации серверов ERA. В нем сосредоточена информация о консоли, к которой подключен ваш сервер ERA, а также данные о дочерних серверах ERA или серверах ERA более низкого уровня. Выпадающий список **Серверы** (Servers) в разделе 4 оказывает влияние на объем информации, отображаемой в разделе 5. Параметры меню **Сервер** (Server):

- **Использовать все серверы** (Use All Servers)
Отображает информацию от всех серверов ERA
- **Использовать только выбранные серверы** (Use Only Checked Servers)
Отображает информацию от выбранных серверов ERA
- **Исключить выбранные серверы** (Exclude Checked Servers)
Отображает информацию от всех невыбранных серверов ERA

Столбцы в разделе 4:

- **Имя сервера** (Server Name)
Отображает имя сервера
- **Клиенты** (Clients)
Общее число клиентов, подключающихся к данному серверу ERA
- **Самая старая версия** (Oldest Version)
Самая старая версия базы данных вирусных сигнатур клиентов данного сервера ERA
- **Последнее подключение** (Least Recent Connection)
Указывает самый длинный период неактивности (интервал от последнего соединения) среди клиентов данного сервера ERA
- **Последние предупреждения об угрозе** (Last Threat Alerts)
Общее число предупреждений о вирусах (см. атрибут Последнее предупреждение (Last Threat Alert) в разделе 5 рис. 4)
- **Последние предупреждения файервола** (Last Firewall Alerts)
Общее число предупреждений файервола (см. атрибут Последнее предупреждение файервола (Last Firewall Alert) в разделе 5 рис. 4)
- **Последние предупреждения о событиях** (Last Event Warnings)
Общее число предупреждений о системных событиях (см. атрибут Последнее предупреждение о событии (Last Event Warning) в разделе 5 рис. 4)

Если в настоящий момент соединение не установлено, вы можете щелкнуть правой кнопкой мыши раздел **Сервер** (Server) (4) и выбрать пункт **Подключиться к данному серверу** (Connect to This Server), чтобы подключиться к выбранному серверу ERA.

ПРИМЕЧАНИЕ. Если включена репликация, серверы нижнего уровня автоматически отображаются в разделе **Сервер** (Server) (4).

Самые важные компоненты консоли ERA доступны из меню или панели инструментов консоли ERA (3). **Последний раздел – Критерий фильтрации компьютера** (Computer filter criteria) (6) – см. следующий раздел, «Фильтрация информации».

4.3 Фильтрация информации

Консоль ERA предоставляет несколько инструментов и компонентов, которые обеспечивают удобное администрирование клиентов и событий.

4.3.1 Группы

Отдельных клиентов можно разделить на группы, выбрав команду **Редактировать – Группы...** (Edit – Groups...) на консоли ERA. Группы в дальнейшем можно использовать при применении фильтров или создании задач, поскольку данные действия можно применить ко всей группе клиентов одновременно. Группы независимы для каждого сервера ERA и не реплицируются. Функция **Синхронизировать с активным каталогом** (Synchronize with Active Directory) позволяет администратору выполнять сортировку клиентов и групп, если имя клиента соответствует типу объекта **«компьютер»** ("computer") на стороне **Активного каталога** (Active Directory – AD) и принадлежит группам, входящим в активный каталог.

4.3.2 Фильтр

Фильтр позволяет администратору отображать только ту информацию, которая относится к определенным серверам или клиентским рабочим станциям. Чтобы отобразить параметры фильтра, выберите в меню консоли ERA команду **Вид – Отобразить/Скрыть панель фильтров** (View > Show/Hide Filter Pane).

Чтобы включить фильтрацию, установите флажок **Использовать фильтр** (Use Filter) в верхнем левом углу консоли ERA и нажмите кнопку **Применить изменения** (Apply Changes). При любом последующем изменении критерия фильтрации отображаемые данные будут автоматически обновляться, при условии, что иные установки не заданы на вкладке **Инструменты – Параметры консоли...** – **Прочие параметры** (Tools > Console Options... > Other Settings).

В разделе **Критерии фильтрации компьютеров** (Computer filter criteria) имеется возможность фильтрации серверов ERA / клиентов на основе следующих критериев:

- **Только клиенты (используя полное слово)** (Only clients (using whole word))
Выборка включает только тех клиентов, имена которых совпадают с введенной строкой.
- **Только клиенты, начинающиеся с** (Only clients beginning like)
Выборка включает только клиентов с именами, начинающимися с определенной строки.
- **Только клиенты с** (Only clients like)
Выборка включает только клиентов с именами, содержащими определенную строку.
- **Исключить клиентов (используя полное слово)** (Exclude clients (using whole word)), **Исключить клиентов, начинающихся с** (Exclude clients beginning like), **Исключить клиентов с** (Exclude clients like)
Данные параметры обеспечивают результаты, противоположные результатам трех предыдущих фильтраций

В полях **Первичный сервер** (Primary server), **Имя компьютера** (Computer name), **Имя клиента** (Client name) и **MAC-адрес** (MAC Address) допускается ввод полных строк. При заполнении любого из этих полей выполняется запрос к базе данных, и результаты фильтруются на основе заполненных полей.

Следующий раздел выполнить Фильтрация по группам позволяет раздлить клиентов следующим образом:

- **Клиенты в группах** (Clients in Groups)
Отображает только клиентов, входящих в определенную группу (группы)
- **Клиенты в других группах или недоступно** (Clients in other Groups or N/A)
Выборка будет содержать только клиентов, входящих в другие группы, или клиентов, не являющихся членами какой-либо группы. Если клиент принадлежит и к определенной, и к неопределенной группе, он будет здесь отображен.
- **Клиенты, не входящие ни в какую группу** (Clients in no Groups)
Отображает только клиентов, не входящих ни в какую группу

Параметры фильтрации незначительно меняются в соответствии с активной вкладкой (**Клиенты** (Clients), **Журнал угроз** (Threat Log) и т.д.)

4.3.3 Контекстное меню

Для вызова контекстного меню и изменения выходных значений в столбцах используйте правую кнопку мыши.

- **Выбрать по «...»** (Select by '...')
Данный параметр позволяет щелкнуть правой кнопкой атрибут и автоматически выбрать (выделить) все другие рабочие станции или серверы с аналогичным атрибутом.
- **Инверсное выделение** (Inverse selection)
Выполняет инверсное выделение записей
- **Скрыть выделенные** (Hide selected)
Скрывает выделенные записи
- **Скрыть невыделенные** (Hide unselected)
Скрывает все невыделенные записи в списке

Последние два параметра эффективны, если после использования предыдущих методов фильтрации необходима дополнительная организация. Чтобы отключить все фильтры, заданные с помощью контекстного меню, выберите команду **Вид – Усеченный вид** (View > Stopped View) или щелкните значок на панели инструментов консоли ERA. Для обновления отображаемой информации также можно воспользоваться клавишей F5.

Пример:

- Чтобы отобразить только клиентов с предупреждениями об угрозах:

На вкладке **Клиенты** (Clients) щелкните правой кнопкой любую пустую панель с атрибутом **Последнее предупреждение о вирусе** (Last Virus Alert) и выберите команду **Выбрать по «...»** (Select by '...') контекстного меню. Затем выберите команду **Скрыть выделенные** (Hide selected) контекстного меню.

- Чтобы отобразить предупреждения об угрозах для клиентов «Джозеф» ("Joseph") и «Чарльз» ("Charles"):

Выберите вкладку **Журнал угроз** (Threat Log) и щелкните правой кнопкой любую ячейку с атрибутом в столбце **Имя клиента** (Client Name) со значением **Джозеф** (Joseph). Затем выберите команду **Выбрать по «Джозеф»** (Select by 'Joseph') контекстного меню. Далее, удерживая нажатой клавишу **CTRL**, щелкните правой кнопкой и выберите команду **Выбрать по «Чарльз»** (Select by 'Charles') контекстного меню. Щелкните правой кнопкой и выберите команду **Скрыть невыделенные** (Hide unselected) контекстного меню. Клавишу **CTRL** можно отпустить.

Клавиша **CTRL** может использоваться для выделения/снятия выделения определенных записей, клавиша **SHIFT** используется для маркировки/отмены маркировки группы записей.

ПРИМЕЧАНИЕ. Фильтрация также может использоваться для обеспечения создания новых задач для определенных (выделенных цветом) клиентов. Существует множество способов эффективной фильтрации, вы можете свободно использовать различные комбинации.

4.3.4 Режимы отображения

На вкладке **Клиенты** (Clients) число отображаемых столбцов можно изменить с помощью **режима отображения** (View mode): (см. выпадающее меню справа с краю консоли). Если включен **режим полноэкранного отображения** (Full View Mode), отображаются все столбцы, в то время как в **режиме минимального экрана** (Minimal View Mode) отображаются лишь самые важные столбцы. Эти режимы заданы в настройках и не могут быть изменены. Чтобы переключиться в пользовательский режим, выберите **Пользовательский режим отображения** (Custom View Mode). Пользовательский режим можно сконфигурировать в разделе **Инструменты – Параметры консоли...** (Tools > Console Options...), щелкнув вкладку **Столбцы – Отобразить/Скрыть** (Columns – Show/Hide).

4.4 Вкладки консоли ERA

4.4.1 Общее описание вкладок и клиентов

Большинство сведений на вкладках определенным образом относится к подключенным клиентам. Каждый клиент, подключенный к серверу ERA, идентифицируется следующими атрибутами:

Имя компьютера (имя клиента) (Computer Name (client name)) + **MAC-адрес** (MAC Address) + **Первичный сервер** (Primary Server)*

Поведение сервера ERA, имеющее отношение к определенным сетевым операциям (например, переименование ПК) можно задать в разделе **Расширенная настройка сервера ERA** (ERAS Advanced Setup) (Дополнительные сведения см. в разделе «Другие настройки» главы 4). Например, если один из компьютеров в сети был переименован, но MAC-адрес остался прежним, можно избежать необходимости создания новой записи на вкладке **Клиенты** (Clients).

Клиенты (рабочие станции и серверы с установленным программным решением по безопасности от ESET), которые подключаются к серверу ERA впервые, определяются значением **Да** (Yes) в столбце **Новый пользователь** (New User) и помечаются небольшой звездочкой в верхнем правом углу значка клиента. Эта функция используется исключительно в целях администрирования и облегчает администратору задачу обнаружения компьютера, подключенного впервые. Этот атрибут имеет различные значения в зависимости от рабочих процедур администратора.



После настройки такого клиента (и перемещения в определенную группу) статус **Новый** (New) можно отключить, щелкнув правой кнопкой на клиенте и выбрав команду **Сбросить флаг «Новый»** (Reset "New" Flag). Значок соответствующего клиента примет вид, указанный в примере ниже (а значение атрибута **Новый пользователь** (New User) изменится на **Нет** (No)).



ПРИМЕЧАНИЕ. Атрибут **Комментарий** (Comment) является необязательным на всех трех вкладках. Администратор может указать здесь любое описание (например, "№ офиса 129").

ПРИМЕЧАНИЕ. Значения времени в сервере ERA могут отображаться в относительном режиме («2 дня назад» ("2 days ago")) или в абсолютном режиме (20. 5. 2007).

В большинстве случаев данные на вкладках можно сортировать в восходящем или нисходящем порядке, щелкнув атрибут. Для изменения порядка столбцов может использоваться метод перетаскивания.

Щелчки на определенных значениях вызывают другие вкладки для отображения дополнительных сведений. Например, при щелчке на столбце **Последнее предупреждение об угрозе** (Last Threat Alert) программа перейдет на вкладку **Журнал угроз** (Threat Log) и отобразит записи журнала, имеющие отношение к данному клиенту. При щелчке на значении, содержащем слишком много информации, которая не умещается на вкладке, откроется диалоговое окно с подробной информацией о соответствующем клиенте.

4.4.2 Репликация и информация на отдельных вкладках

Если консоль ERA подключена к серверу ERA, который функционирует как сервер верхнего уровня, вся информация от серверов нижнего уровня будет отображаться автоматически, при условии, что в конфигурации сервера задано разрешение на это.

В таком случае может отсутствовать следующая информация:

- **Подробные журналы угроз** (вкладка **Журнал угроз** (Threat Log))
- **Подробные журналы сканирования по запросу** (вкладка **Журнал сканирования** (Scan Log))
- **Подробные конфигурации клиента в формате XML** (вкладка **Клиенты** (Clients), столбец **Конфигурация** (Configuration), **Состояние защиты** (Protection status), **Функции защиты** (Protection Features), **Системная информация** (System Information))

В диалоговых окнах, в которых такая информация может присутствовать, доступна кнопка **Запросить** (Request). Нажмите эту кнопку для загрузки недостающей информации с сервера ERA нижнего уровня. Поскольку репликацию всегда инициирует сервер ERA нижнего уровня, недостающая информация должна быть доставлена в рамках заданного интервала репликации.

* В двух предыдущих версиях удаленного администратора ESET Remote Administrator идентификация основывалась на атрибутах Имя компьютера + Первичный сервер (Computer Name + Primary Server)

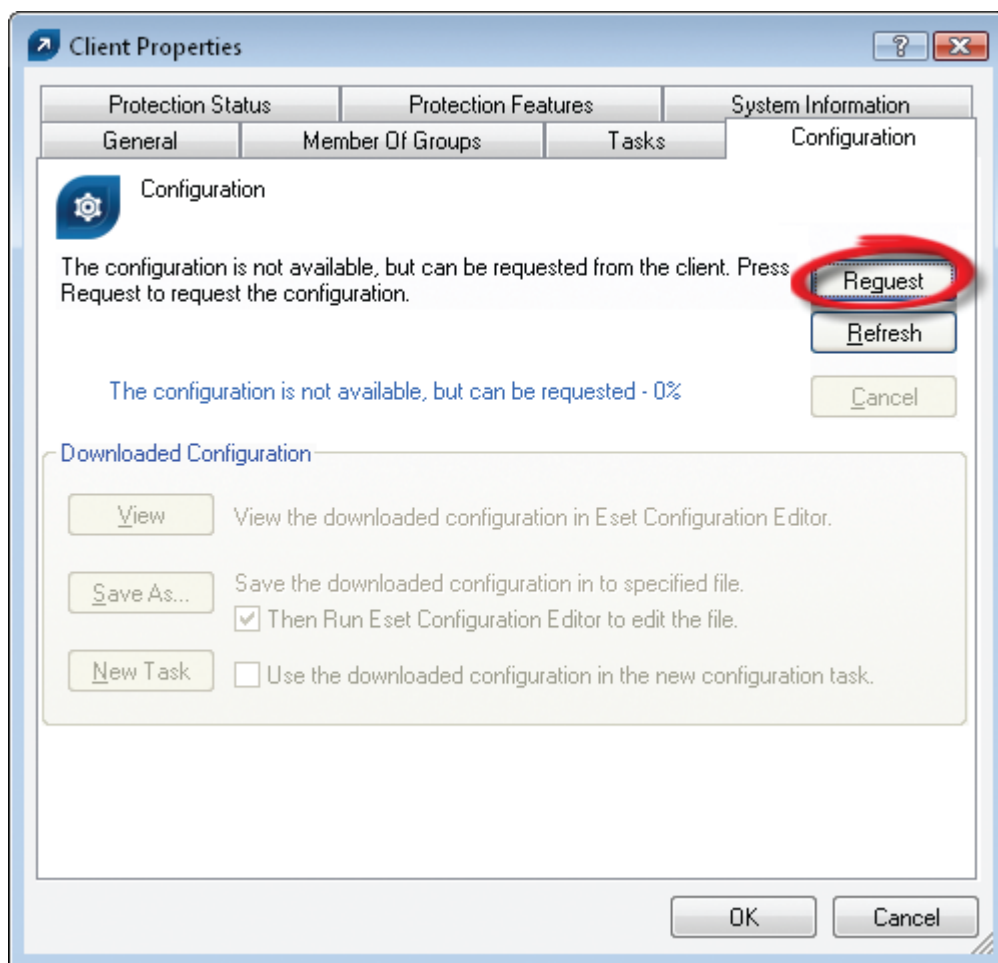


Рис. 5 Нажмите кнопку Запросить (Request) для загрузки недостающей информации с серверов ERA нижнего уровня.

4.4.3 Вкладка Клиенты (Clients)

На этой вкладке отображаются общие сведения об отдельных клиентах.

Атрибут	Описание
Имя клиента (Client Name)	Имя, идентифицирующее клиента в ERA. Новые клиенты пользуются значением «Имя компьютера» ("Computer Name"). Имя компьютера можно изменять, не боясь побочных эффектов.
Имя компьютера (Computer Name)	Имя рабочей станции / сервера (имя узла)
MAC-адрес (MAC Address)	MAC-адрес (сетевой адаптер)
Первичный сервер (Primary Server)	Имя сервера ERA, к которому подключен клиент.
Домен (Domain)	Домен / имя группы, к которой принадлежит клиент (эти группы не создаются в сервере ERA)
IP-адрес (IP)	IP-адрес
Имя продукта (Product Name)	Название продукта компании ESET
Версия продукта (Product Version)	Версия вышеуказанного продукта
Последнее подключение (Last Connected)	Последнее подключение клиента к своему серверу ERA. Все остальные данные от клиента имеют эту временную метку, за исключением некоторых данных, полученных в ходе репликации.
Описание статуса защиты (Protection Status Text)	Текущий статус программного решения ESET, установленного на клиенте
Версия БД угроз (Threat DB Version)	Версия базы данных вирусных сигнатур
Последнее предупреждение об угрозе (Last Threat Alert)	Последний инцидент с вирусом
Последнее предупреждение файервола (Last Firewall Alert)	Последнее событие, обнаруженное файерволом
Последнее предупреждение о событии (Last Event Warning)	Последнее сообщение об ошибке
Последние отсканированные файлы (Last Files Scanned)	Число файлов, отсканированных в ходе последнего сканирования по запросу

Последние зараженные файлы (Last Files Infected)	Число зараженных файлов, выявленных в ходе последнего сканирования по запросу
Последние очищенные файлы (Last Files Cleaned)	Число файлов, очищенных (или удаленных) в ходе последнего сканирования по запросу
Дата последнего сканирования (Last Scan Date)	Время последнего сканирования по запросу
Запрос на перезагрузку (Restart Request)	Запрос на перезагрузку (например, после обновления программы)
Дата запроса на перезагрузку (Restart Request Date)	Время первого запроса на перезагрузку
Последний запуск продукта (Product Last Started)	Время последнего запуска клиентской программы
Дата установки продукта (Product Install Date)	Дата установки программы
Мобильный пользователь (Mobile User)	Клиенты с этим атрибутом выполняют задачу «обновить сейчас» (“update now”) при каждом подключении к серверу ERA (подходит для портативных ПК)
Новый пользователь (New User)	Более подробно см. в общем описании клиентов
Имя ОС (OS Name)	Имя операционной системы
Платформа ОС (OS Platform)	Платформа операционной системы (Windows / Linux...)
Платформа аппаратных средств (HW Platform)	32-разрядный / 64-разрядный процессор
Конфигурация (Configuration)	Клиент также передает текущую конфигурацию в формате XML. Этот атрибут включает время конфигурации (если не включена репликация, оно соответствует времени последнего изменения конфигурации)
Статус защиты (Protection Status)	Общее описание статуса. По характеру соответствует атрибуту Конфигурация (Configuration)
Функции защиты (Protection Features)	Общее описание статуса программных компонентов. Соответствует атрибуту Конфигурация (Configuration).
Системная информация (System Information)	Информация о версиях программных компонентов. По характеру соответствует атрибуту Конфигурация (Configuration)

ПРИМЕЧАНИЕ. Некоторые значения носят информационный характер и могут не являться текущими в тот момент, когда администратор видит их на консоли. Например, в 7:00 могла произойти ошибка обновления, но в 8:00 обновление прошло успешно. Если администратор знает, что информация не является актуальной, он может щелкнуть правой кнопкой значение и выбрать команду **Стереть информацию о последнем предупреждении об угрозе** (Clear “Last Threat Alert” Info) или **Стереть информацию о последнем событии** (Clear “Last Event” Info). Информация о последнем предупреждении о вирусе или последнем системном событии будет удалена. Это относится к значениям в столбцах **Последнее предупреждение об угрозе** (Last Threat Alert) и **Последнее событие** (Last Event).

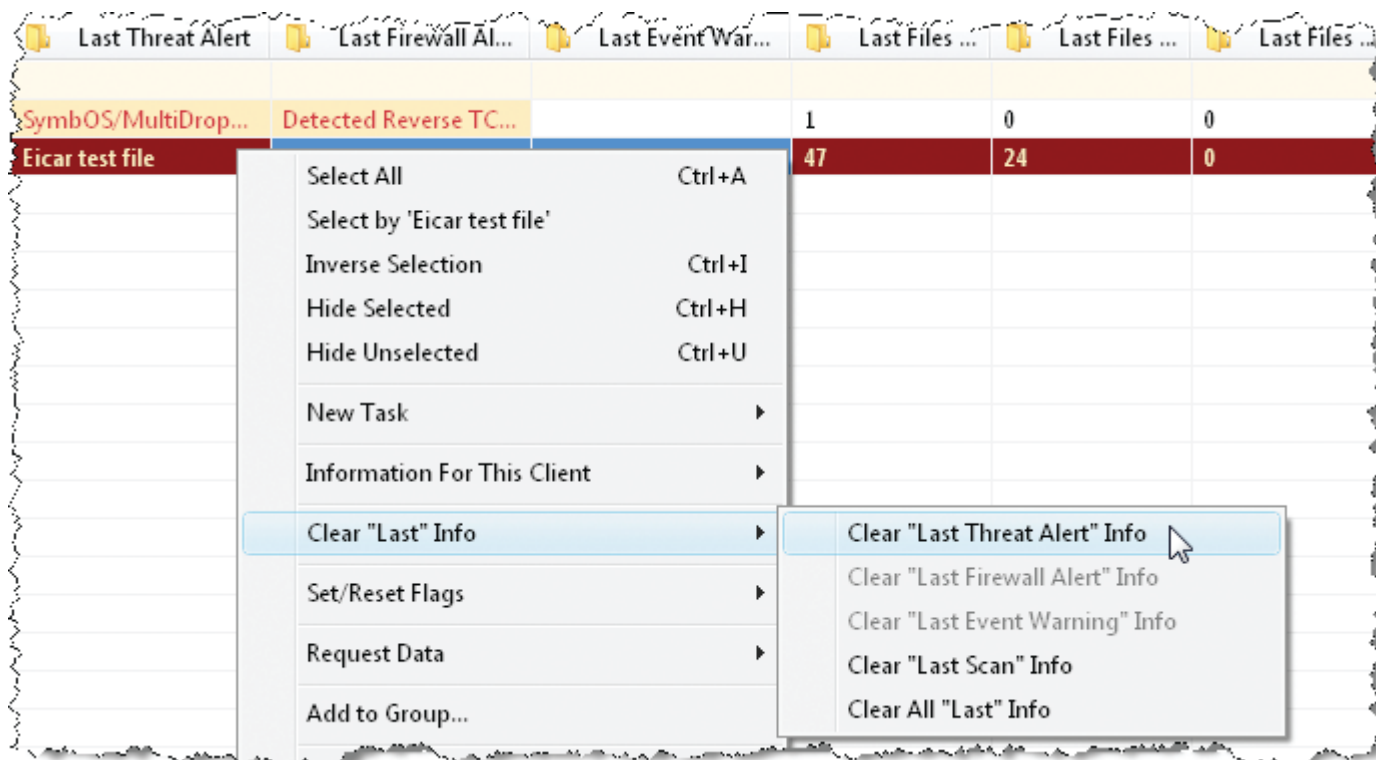


Рис. 6 Неактуальные события можно легко удалить из столбцов Последнее предупреждение об угрозе (Last Threat Alert) и Последнее событие (Last Event).

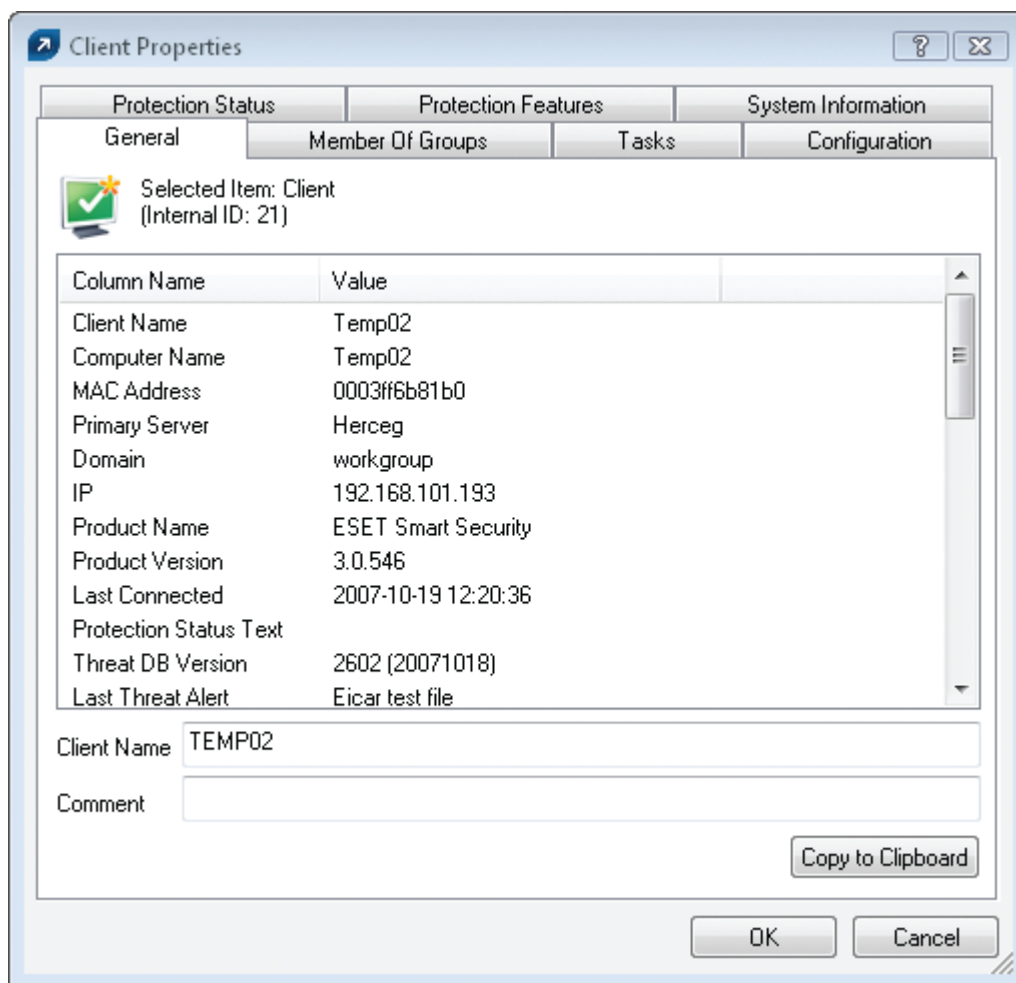


Рис. 7 Подробная информация о клиентской рабочей станции.

На вкладке **Клиенты** (Clients) сосредоточены несколько параметров, которые становятся доступными после щелчка на клиенте:

- Вкладка **Общие параметры** (General)
Содержит информацию, аналогичную информации, отображаемой на вкладке **Клиенты** (Clients). Здесь можно указать **Имя клиента** (Client Name) – имя, под которым клиент отображается в ERA, включая необязательный комментарий.
- Вкладка **Член групп** (Member Of Groups)
На данной вкладке перечисляются все группы, к которым принадлежит клиент. Дополнительную информацию см. в разделе 4.3, "Фильтрация информации".
- Вкладка **Задачи** (Tasks)
Задачи относятся к данному клиенту. Дополнительную информацию см. в главе 5, "Задачи".
- Вкладка **Конфигурация** (Configuration)
На данной вкладке можно просмотреть текущую конфигурацию клиента или экспортировать ее в XML-файл. В дальнейшем XML-файлы могут быть использованы для создания шаблона конфигурации для новых/измененных XML-файлов конфигурации. Дополнительную информацию см. в главе 5, "Задачи".
- Вкладка **Статус защиты** (Protection Status)
Общее описание статуса в отношении всех программ ESET. Некоторые описания носят интерактивный характер, имеется возможность немедленного вмешательства. Данная функция полезна тем, что она устраняет необходимость вручную определять новые задачи для решения проблем.
- Вкладка **Компоненты защиты** (Protection Features)
Статус всех защитных компонентов ESET (защита от спама, персональный файрвол и т.д.)
- Вкладка **Системная информация** (System Information)
Подробная информация об установленной программе, версии ее программных компонентов и т.д.

4.4.4 Вкладка Журнал угроз (Threat Log)

Атрибут	Описание
Идентификатор угрозы (Threat Id)	Идентификатор соответствующей записи на вкладке базы данных
Имя клиента (Client Name)	Имя клиента, сообщившего об угрозе
Имя компьютера (Computer Name)	Имя клиентского компьютера, сообщившего об угрозе
MAC-адрес (MAC Address)	MAC-адрес клиента, сообщившего об угрозе
Первичный сервер (Primary Server)	Имя сервера ERA, к которому подключен клиент.
Дата получения (Date Received)	Время записи события в журнал сервером ERA
Дата возникновения (Date Occurred)	Время возникновения инцидента на клиенте
Уровень (Level)	Уровень предупреждения
Сканер (Scanner)	Имя защитного компонента, обнаружившего угрозу
Объект (Object)	Тип объекта
Имя (Name)	Как правило, папка, в которую проник вирус
Угроза (Threat)	Как правило, имя обнаруженного вредоносного кода
Действие (Action)	Действие, выполненное данным защитным компонентом
Пользователь (User)	Имя пользователя, зарегистрированного в системе в момент возникновения инцидента
Информация (Information)	Задается пользователем

4.4.5 Вкладка Журнал файрвола (Firewall Log)

На данной вкладке отображаются общие сведения о деятельности клиентского файрвола.

Атрибут	Описание
Идентификатор файрвола (Firewall Id)	Идентификатор соответствующей записи на вкладке базы данных
Имя клиента (Client Name)	Имя клиента, сообщившего о событии
Имя компьютера (Computer Name)	Имя клиентского компьютера, сообщившего о событии
MAC-адрес (MAC Address)	MAC-адрес клиента, сообщившего о событии
Первичный сервер (Primary Server)	Имя сервера ERA, к которому подключен клиент.
Дата получения (Date Received)	Время записи события в журнал сервером ERA
Дата возникновения (Date Occurred)	Время возникновения инцидента на клиенте
Уровень (Level)	Уровень предупреждения
Событие (Event)	Описание события
Источник (Source)	IP-адрес источника
Объект назначения (Target)	IP-адрес объекта назначения
Протокол (Protocol)	Соответствующий протокол
Правило (Rule)	Соответствующее правило
Приложение (Application)	Соответствующее приложение
Пользователь (User)	Имя пользователя, зарегистрированного в системе в момент возникновения инцидента

4.4.6 Вкладка Журнал событий (Event Log)

На данной вкладке перечисляются системные события.

Атрибут	Описание
Идентификатор события (Event Id)	Идентификатор соответствующей записи на вкладке базы данных
Имя клиента (Client Name)	Имя клиента, сообщившего о событии
Имя компьютера (Computer Name)	Имя клиентского компьютера, сообщившего о событии
MAC-адрес (MAC Address)	MAC-адрес клиента, сообщившего о событии
Первичный сервер (Primary Server)	Имя сервера ERA, к которому подключен клиент.
Дата получения (Date Received)	Время записи события в журнал сервером ERA
Дата возникновения (Date Occurred)	Время возникновения инцидента на клиенте
Уровень (Level)	Уровень события.

Модуль (Plugin)	Имя программного компонента, сообщившего о событии
Событие (Event)	Описание события
Пользователь (User)	Имя пользователя, зарегистрированного в системе в момент возникновения события

4.4.7 Вкладка Журнал сканирования (Scan Log)

На данной вкладке перечисляются результаты сканирования компьютеров по запросу, выполненного удаленно, локально на клиентских компьютерах или в ходе запланированных задач.

Атрибут	Описание
Идентификатор сканирования (Scan Id)	Идентификатор соответствующей записи на вкладке базы данных
Имя клиента (Client Name)	Имя клиента, на котором было выполнено сканирование
Имя компьютера (Computer Name)	Имя клиентского компьютера, на котором было выполнено сканирование
MAC-адрес (MAC Address)	MAC-адрес клиентского компьютера, на котором было выполнено сканирование
Первичный сервер (Primary Server)	Имя сервера ERA, к которому подключен клиент.
Дата получения (Date Received)	Время записи в журнал сервером ERA
Дата возникновения (Date Occurred)	Время возникновения инцидента на клиенте
Отсканированные объекты назначения (Scanned Targets)	Отсканированные файлы, папки и устройства
Отсканировано (Scanned)	Число проверенных файлов
Инфицировано (Infected)	Число инфицированных файлов
Очищено (Cleaned)	Число очищенных файлов
Статус (Status)	Статус сканирования
Пользователь (User)	Имя пользователя, зарегистрированного в системе в момент сканирования
Тип (Type)	Кто запустил задачу
Сканер (Scanner)	Сканер, выполнивший сканирование
Подробнее (Details)	Доступность подробной информации

4.4.8 Вкладка Задачи (Tasks)

Значение данной вкладки описано в главе 5, "Задачи". Доступны следующие атрибуты:

Атрибут	Описание
Идентификатор задачи (Task Id)	Идентификатор соответствующей записи на вкладке базы данных
Состояние (State)	Состояние задачи (Активная (Active) = задача применяется, Finished (Завершено) = задача была выполнена у клиента)
Тип (Type)	Тип задачи
Имя (Name)	Имя задачи
Описание (Description)	Описание задачи
Дата получения (Date Received)	Время записи события в журнал сервером ERA
Комментарий (Comment)	Необязательное описание

4.4.9 Вкладка Отчеты (Reports):

Вкладка **Отчеты (Reports)** используется для сбора статистической информации – отчетов – в виде графиков или диаграмм. Эти данные в дальнейшем могут обрабатываться (в формате CSV) с помощью инструментов ERA для создания графиков и графических данных. По умолчанию ERA сохраняет значения в формате HTML (изображения сохраняются в формате PNG).

ERA предоставляет несколько predefined шаблонов для отчетов. Чтобы выбрать отчет, воспользуйтесь раскрывающимся списком **Тип отчета (Report Type)** в центральной части окна под кнопкой **Создать сейчас (Generate Now)**.

- **Основные угрозы (Top Threats)**
Перечень наиболее часто встречающихся угроз
- **Топ клиентов с наибольшим числом угроз (Top Clients with most Threats)**
Перечень наиболее «активных» клиентских рабочих станций (по числу обнаруженных угроз)
- **Развитие угроз (Threats Progress)**
Накапливание событий с вредоносными кодами (число)
- **Сравнительное развитие угроз (Threats Comparative Progress)**
Накапливание событий по выборочным угрозам (с помощью фильтра) в сравнении с общим числом вредоносных программ

- **Угрозы по сканеру** (Threats By Scanner)
Число предупреждений об угрозах от отдельных программных модулей
- **Угрозы по объектам** (Threats By Object)
Число предупреждений об угрозах в соответствии со способом проникновения (электронная почта, файлы, загрузочные секторы)
- **Комбинация основных клиентов/основных угроз** (Combined Top Clients / Top Threats)
Комбинация вышеуказанных типов
- **Комбинация основных угроз/ развития угроз** (Combined Top Threats / Threats Progress)
Комбинация вышеуказанных типов
- **Комбинация основных угроз/ сравнительного развития угроз** (Combined Top Threats / Threats Comparative Progress)
Комбинация вышеуказанных типов
- **Отчет о клиентах** (Clients Report), **Отчет об угрозах** (Threats Report), **Отчет о событиях** (Events Report), **Отчет о сканировании** (Scans Report), **Отчет о задачах** (Tasks Report)
Стандартные отчеты, отображаемые на вкладке **Клиенты** (Clients), **Журнал угроз** (Threat Log), **Журнал событий** (Event Log), **Журнал сканирования** (Scan Log) или **Задачи** (Tasks).
- **Комплексный отчет** (Comprehensive Report)

Резюме

- **Комбинации основных клиентов/основных угроз** (Combined Top Clients / Top Threats)
- **Комбинации основных угроз/ сравнительного развития угроз** (Combined Top Threats / Threats Comparative Progress)
- **Развитие угроз** (Threats Progress)

В разделе **Фильтр** (Filter) можно использовать раскрывающиеся списки **Клиенты** (Target clients) или **Угрозы** (Threat) для выбора клиентов или вирусов, которые должны быть включены в отчет.

Другие настройки можно выполнить, нажав кнопку **Дополнительные настройки...** (Additional Settings...). Данные настройки в основном применяются к данным в заголовке и в используемых графических диаграммах. Тем не менее, можно выполнить фильтрацию данных в соответствии со статусом выбранного атрибута (отображать только клиентов с проблемой с «Состоянием защиты» ("Protection State"), а также выбрать формат отчета (HTML, CSV).

Вкладка **Интервал** (Interval) – На данной вкладке можно задать интервал создаваемого отчета:

- **Текущий** (Current)
В отчет включаются события, возникшие в выбранный период, – например, если отчет создается в среду, а интервал установлен в значение **Текущая неделя** (Current Week), в отчет будут включены события воскресенья, понедельника, вторника и среды.
- **Завершенный** (Completed)
В отчет включаются события, возникшие в выбранный период, ограниченный рамками, (например, весь месяц август или целая неделя – от воскресенья до следующей субботы). Если установлен флажок **Добавить также текущий период** (Add also the current period), отчет будет включать события последнего завершенного периода до момента создания отчета.

Пример:

Нужно создать отчет, включающий события последней календарной недели, т.е. от воскресенья до следующей субботы. Данный отчет должен быть создан в следующую среду (после субботы).

На вкладке **Интервал** (Interval) выберите параметры **Завершенный** (Completed) и **1 неделя** (1 Weeks). На вкладке **Планировщик** (Scheduler) установите параметр **Частота** (Frequency) в значение **Еженедельно** (Weekly) и выберите **Среда** (Wednesday). Все другие настройки выполняются по усмотрению администратора.

- **От/До** (From/To)

Данная настройка используется для задания периода, для которого создается отчет.

Вкладка **Планировщик** (Scheduler) – На данной вкладке осуществляется определение и настройка автоматического создания отчета в выбранное время или с выбранным интервалом (с помощью раздела **Частота** (Frequency)).

С помощью окошка счетчика **Запустить в** (Run at) и раскрывающегося списка **Старт** (Start) введите время и дату создания отчета. Нажмите кнопку **Выбрать назначение..** (Select Target..), чтобы указать место сохранения отчета. Отчеты могут сохраняться на сервер ERA (по умолчанию), отправляться по электронной почте на выбранный адрес или экспортироваться в папку. Последний вариант используется в том случае, когда отчет отправляется в папку с совместным доступом во внутренней сети организации, которую могут просматривать другие сотрудники.

Для отправки созданных отчетов по электронной почте необходимо ввести информацию о сервере SMTP и адрес отправителя согласно описанию в главе 4.6, «Конфигурирование сервера ERA с помощью консоли».

Чтобы задать фиксированный временной диапазон для процесса генерации отчетов, воспользуйтесь параметрами в разделе **Диапазон** (Range). Имеется возможность определения числа сгенерированных отчетов (**Завершить после** ((End after)) или даты, до которой выполняется процесс создания отчета (**Завершить до** (End by)).

Для сохранения настроек заданных отчетов в шаблон нажмите кнопку **Сохранить** (Save) или **Сохранить как...** (Save as...). При создании нового шаблона нажмите кнопку **Сохранить как...** (Save as...) и задайте шаблону имя.

На верхней части окна консоли в разделе **Шаблоны отчетов** (Report templates) можно увидеть имена уже созданных шаблонов. Рядом с именами шаблонов имеются сведения о времени/интервалах создания отчеты в соответствии с предварительно заданными шаблонами. Нажмите кнопку **Создать сейчас** (Generate Now) (вкладка **Параметры** (Options) должна быть выбрана) для создания отчета а любой момент, независимо от плана.

Ранее созданные отчеты можно просмотреть на вкладке **Сгенерированные отчеты** (Generated Reports). Для вызова дополнительных параметров выберите отчет или несколько отчетов и с помощью контекстного меню (щелкните правой кнопкой) скопируйте отчеты в другие папки, добавьте в список фаворитов и т.д.

Шаблоны, помещенные в **Список фаворитов** (Favorites List), могут впоследствии использоваться для немедленного создания новых отчетов. Чтобы переместить шаблон в список **Фавориты** (Favorites), щелкните отчет правой кнопкой мыши и выберите в контекстном меню команду **Добавить к фаворитам** (Add to Favorites).

4.4.10 Вкладка Удаленная установка (Remote Install)

На данной вкладке имеются параметры нескольких методов удаленной установки антивирусной системы ESET NOD32 на клиентах. Подробные сведения см. в разделе «Удаленная установка» в главе 6, «Установка клиентских программных решений ESET».

4.5 Настройка консоли ERA

Настройка консоли ERA выполняется в меню **Инструменты/Параметры консоли...** (Tools/Console Options...).

4.5.1 Вкладка Соединение (Connection)

Данная вкладка относится к связи между консолью ERA и сервером ERA. Подробные сведения см. в начале главы 4, «Подробное описание консоли удаленного администратора ESET Remote Administrator».

4.5.2 Вкладка Столбцы – Отобразить/Скрыть (Columns – Show / Hide)

На данной вкладке можно указать, какие атрибуты (столбцы) должны отображаться на отдельных вкладках. Изменения отражаются в **пользовательском режиме отображения** (Custom View Mode). Другие режимы изменить нельзя.

4.5.3 Вкладка Цвета (Colors)

Здесь определяется цветовая маркировка событий. Например, клиентов с несколько устаревшей базой данных вирусных сигнатур (**Клиенты: Предыдущая версия** (Clients: Previous Version) можно отличать по цвету от клиентов с значительно устаревшей базой данных (**Клиенты: Более старые версии или неприменимо** (Clients: Older Versions or N/A).

4.5.4 Вкладка Пути (Paths)

Здесь можно указать каталог, в который консоль ERA будет сохранять отчеты, загруженные с сервера ERA. По умолчанию все отчеты сохраняются в следующий каталог:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Console\reports`

4.5.5 Вкладка Дата/Время (Date/Time)

Вид столбцов вкладки **Дата/Время** (Date/Time)

- **Абсолютное** (Absolute)
Консоль отобразит абсолютное время (например, 14:30:00).
- **Относительное** (Relative)
Консоль отобразит относительное время (например, 2 недели назад).
- **Региональное** (Regional)
Консоль отобразит время с учетом региональных настроек (заимствуются настройки Windows).
- **Перевести всеобщее скоординированное время в локальное время** (использовать локальное время)(Recalculate UTC time to your local time (use local time))
Установите данный флажок для перевода времени в локальное. В противном случае будет отображаться Гринвичское – всеобщее скоординированное время.

4.5.6 Вкладка Другие настройки (Other Settings)

- **Автоматически применять изменения** (Auto Apply Changes)
При установке данного флажка фильтры в отдельных столбцах будут генерировать новые выборки после каждого изменения настроек фильтров. В противном случае фильтрация произойдет только после нажатия кнопки **Применить изменения** (Apply Changes).
- **Обновления удаленного администратора** (Remote Administrator updates)
Данный раздел позволяет задать проверку наличия новых версий удаленного администратора ESET Remote Administrator. Рекомендуется оставить настройку по умолчанию **Ежемесячно** (Monthly). При наличии новой версии консоль ERA отобразит соответствующее уведомление при запуске программы.

- **Использовать автоматическое обновление** (Use automatic refresh)
При установке данного флажка отдельные вкладки автоматически обновляются в соответствии с указанным интервалом.
- **Опустошать мусорные корзины консоли при выходе из приложения** (Empty console recycle bins at application exit)
Установка данного флажка позволяет автоматически удалять элементы из внутренней мусорной корзины консоли после завершения работы с ней. Элементы также можно удалять вручную, щелкнув правой кнопкой мыши значок **Мусорная корзина** (Recycle Bin) на вкладке **Отчеты** (Reports).
- **Отображать сетку** (Show gridlines)
Установка данного флажка позволяет разделять отдельные ячейки на всех вкладках с помощью сетки.
- **Предпочтение отображению клиента в виде «Сервер/Имя», а не в виде «Сервер/Компьютер/МАС-адрес»** (Prefer showing Client as «Server/Name» instead of «Server/Computer/MAC»)
Влияет на режим отображения клиентов в некоторых диалоговых окнах (например, **Новая задача** (New task)).
- **Использовать значок системного лотка** (Use systray icon)
Консоль ERA будет представлена значком области уведомлений Windows.
- **Отображать на панели задач при сворачивании окна** (Show on taskbar when minimized)
При сворачивании окно консоли ERA становится доступным из области уведомлений Windows.
- **Использовать выделенный цветом значок системного лотка при обнаружении проблемных клиентов** (Use highlighted systray icon when problematic clients found)
Используйте данный флажок вместе с кнопкой **Правка** (Edit) для определения событий, которые вызовут изменения цвета значка консоли ERA в области уведомлений.

ПРИМЕЧАНИЕ. Если консоль ERA на компьютере администратора иногда должна подключаться к серверу ERA, рекомендуется установить флажок **Отображать на панели задач** (Show on taskbar) при свернутом окне и не разворачивать окно консоли, если она неактивна. В случае возникновения проблемы значок в области уведомлений станет красным, что призывает администратора к активным действиям. Также рекомендуется установить флажок **Использовать выделенный цветом значок системного лотка при обнаружении проблемных клиентов** (Use highlighted systray icon when problematic clients found), чтобы указать события, которые вызовут изменения цвета значка консоли ERA.

- **Отображать все группы на панели фильтров** (Show all groups in filter panes)
Меняет способ фильтрации групп.
- **Обучающие сообщения** (Tutorial messages)
Отключает (**Отключить все** (Disable All)) или включает (**Включить все** (Enable All)) все информативные сообщения.
- **Предупреждать об истечении лицензии сервера за X дней** (Warn if the server license is about to expire in X days)
При установке данного флажка программа отобразит уведомление об истечении лицензии за X дней до срока ее окончания.
- **Предупреждать, если в лицензии сервера осталось только X% свободных клиентов** (Warn if there is only X% free clients left in the server license)
При установке данного флажка консоль отобразит соответствующее уведомление, если осталось свободными менее X ячеек для клиентов (в каждой лицензии определяется число администрируемых клиентов).

4.6 Настройка ERA сервера, с использованием консоли

ERA сервер удобно настраивается непосредственно через **ERA Консоль** (ERA Console). В консольном меню выберите **Инструменты > Настройки сервера** (Tools > Server Options)...

4.6.1 Вкладка общие сведения

В вкладке Общие сведения содержится общая информация о ERA сервере (ERAS), данные ключа лицензии и статистические данные о работе ERA сервера (ERAS).

Выберите **Продление лицензии...** (Renew License) для дистанционной установки ключа лицензии ERA сервера (ERAS) чтобы избежать возможного прекращения действия лицензии. Подробнее ключи лицензии описаны в разделе 7.1.2, Установка ERA сервера (Installation of ERA Server).

4.6.2 Вкладка безопасность

Программные решения ESET security в версиях 3.x (ESET Smart Security, и так далее) предлагают защиту процесса передачи данных между клиентом и сервером ERA (передача данных через протокол TCP, порт 2222), которая предусматривает расшифровку информации.

Предыдущая версия (2.x) не обладает этими функциональными средствами. Для обратной совместимости с предыдущими версиями необходимо активировать режим **Разрешить доступ клиентов без проверки подлинности** (Enable unauthenticated access for Clients).

Вкладка Безопасность содержит опции для настройки одновременной работы программ поколений 2.x и 3.x.

- **Пароль для консоли**
Установка запроса пароля при входе позволяет защититься от неавторизованного проникновения через ERA консоль
- **Клиентский пароль** (Password for Clients) (ESET Security Products)
Устанавливает пароль для клиентов, имеющих доступ к серверу ERA
- **Пароль для репликации**
Устанавливает пароль для ранних версий ERA сервера для осуществления репликации с данной версией

■ Пароль для ESET Remote Installer

Устанавливает пароль для доступа исполнительной программы установки к серверу ERA. Что необходимо для дистанционной установки.

■ Разрешение доступа без запроса авторизации для клиентов

Разрешает доступ для клиентов сервера ERA, которые не имеют заданного действующего пароля (если текущий пароль отличается от клиентского пароля).

■ Разрешение доступа без запроса авторизации для репликации

Разрешает доступ к серверу ERA для клиентов более ранних версий сервера ERA, которые не имели указанного действующего пароля.

■ Разрешение доступа к программе удаленной установки ESET (Исполнительная программа)

Разрешает доступ к серверу ERA для исполнительных программ установки, которые не имеют указанного действующего пароля.

ПРИМЕЧАНИЕ. Если разрешена аутентификация и в сервере ERA и в клиентах [поколения 3.x], опция разрешение доступа для клиентов без запроса аутентификации может быть отключена.

4.6.3 Вкладка обслуживание сервера

При корректной настройке вкладки Обслуживание сервера, база данных ERA сервера будет автоматически обслуживаться, и оптимизироваться, без необходимости дальнейших настроек. По умолчанию, записи и журналы старше шести месяцев удаляются, и задача **Сжатие и исправление** (Compact & repair) осуществляется **каждые 15 дней**.

Для более точной настройки во вкладке Эксплуатация сервера предлагаются следующие опции:

■ Сохранять только последние X опасных события для каждого клиента

Сохраняет только указанное количество вирусов определенных для каждого клиента

■ Сохранять только последние X журналов файервола для каждого клиента

Сохраняет только указанное количество журналов файервола для каждого клиента

■ Сохранять только последние X событий для каждого клиента

Сохраняет только указанное количество системных событий для каждого клиента

■ Сохранять только последние X журналов сканера для каждого клиента

Сохраняет только указанное количество журналов сканера для каждого клиента

■ Удаление клиентов, не осуществлявших подключения в течение последних X месяцев (дней)

Удаление всех клиентов, которые не подключались к серверу ERA в течение обозначенного количества дней или месяцев

■ Удаление журналов обнаруженных угроз старше X месяцев (дней)

Удаляет все обнаруженные вирусы старше указанного количества месяцев или дней

■ Удаление журналов файервола старше X месяцев (дней)

Удаляет все журналы файервола старше указанного количества месяцев или дней

■ Удаление журналов событий старше X месяцев (дней)

Удаляет все системные события старше указанного количества месяцев или дней

■ Удаление журналов сканера старше X месяцев (дней)

Удаляет все журналы сканера старше указанного количества месяцев или дней

4.6.4 Вкладка журналы

В процессе работы сервер ERA создает журнал (имя файла журнала) о своей работе, который поддается настройке (наполнение журнала). Если выбрана опция **Журнал в текстовом файле** (Log to text file), новые файлы журнала будут создаваться (**Ротировать, если более X мегабайт** (Rotate when greater than X MB)) и удаляться ежедневно (**Удалять перемещенные журналы старше X дней** (Delete rotated logs older than X days)).

Опция **Журнал для журнала приложений операционной системы** (Log to OS application log option) позволяет копировать данные в журнал просмотра событий (доступный через **Панель управления – Администрирование – Просмотр событий** (Control Panel – Administrative Tools – Event viewer)).

Опция **Журнал отладки** (Debug Log) должна быть отключена при нормальных обстоятельствах. По умолчанию результаты тестового файла сохраняются по следующему пути:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs\era.log`

Примечание. Мы рекомендуем оставлять для параметра **Наполнение журнала** (Log verbosity) значение **Уровень 2 – сверх + ошибки сессии** (Level 2 – Above + Session Errors). Изменяйте уровень журнала, только при наличии проблем или по совету специалиста службы технической поддержки ESET.

4.6.5 Вкладка репликация

Понятие репликации уже было описано в разделе 2.1.2, "Иерархия ERA сервера в больших сетях (ERAS hierarchy at large networks)". Репликация используется преимущественно в больших сетях, где используется несколько ERA серверов, по всей структуре, в различных переходах и участках.

Опции во вкладке Репликация разделены на две части:

■ Репликация «в» установки

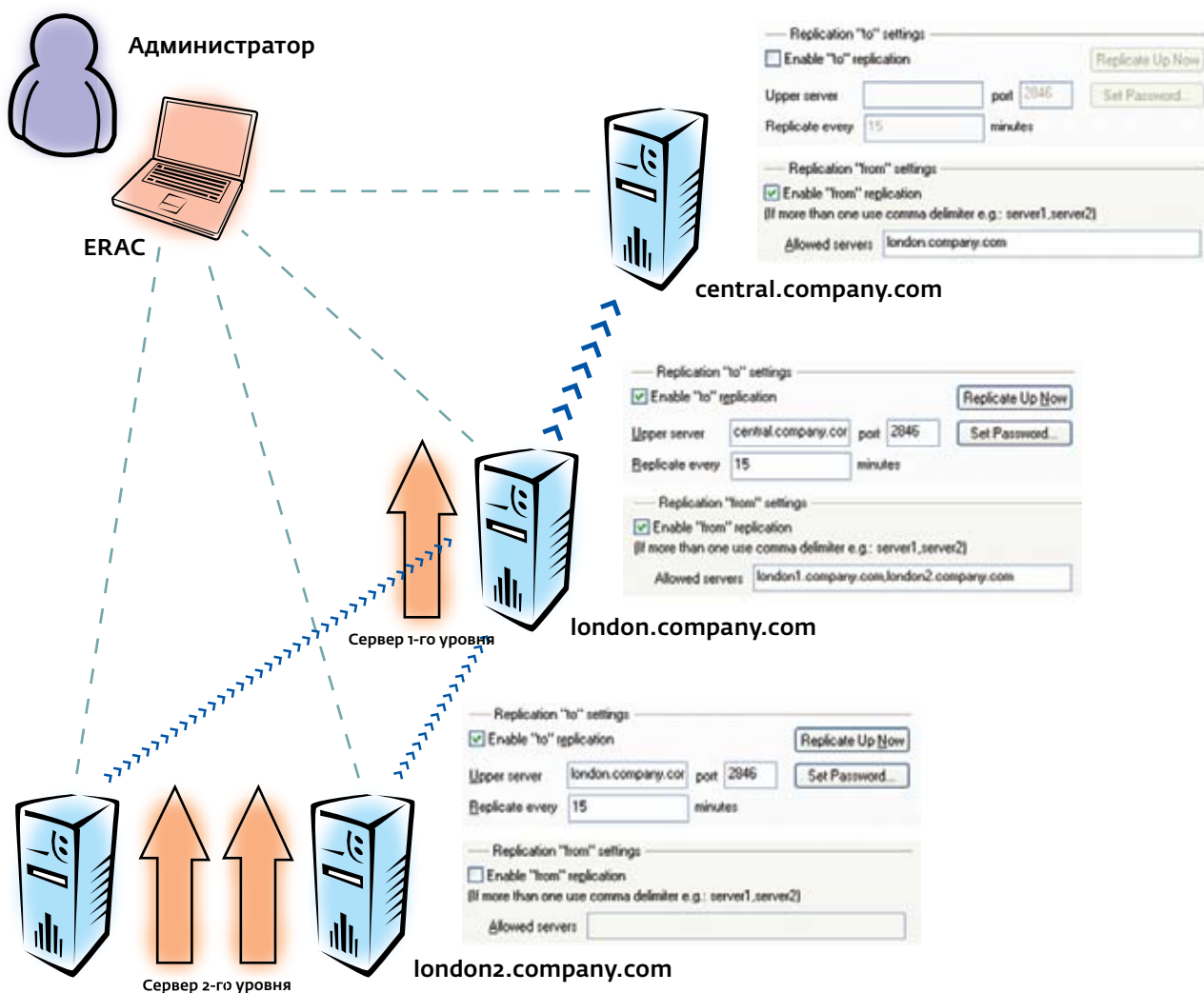
■ Репликация «из» установок

Раздел **Репликация «в» установки** используется для настройки младших ERA серверов. Опция **Запуск «в» репликации** должна быть активирована, и должны быть указаны IP адрес и имя мастер сервера ERA (старшего сервера). Тогда данные реплицируются с младшего сервера на мастер-сервер.

Репликация «из» установок дает возможность «старшему» ERA серверу получить доступ к данным младшего ERA сервера или возможность передачи данных мастер серверу. Опция **Разрешения «из» репликации** должна быть активирована, и должны быть указаны имена младших серверов (через запятую).

Обе эти опции должны быть активированы для ERA сервера расположенного в середине иерархии репликации (то есть, имеющего и старший, и младший сервер).

Все выше упоминавшиеся сценарии описаны в таблице ниже. Бежевые компьютеры представляют отдельные ERA серверы. Каждый ERA сервер представлен именем (которое должно быть таким же, как **%Имя компьютера (Computer Name)%** во избежание путаницы) и соответствующими установками в диалоговом окне репликации.



Другие опции имеющие влияние на процесс репликации серверов:

- Репликация журнала обнаруженных угроз, репликация журнала файрвола, репликация журнала системных событий, репликация журнала сканера
Если выбраны эти опции, то все данные, хранящиеся в клиентских журналах обнаруженных угроз, файрвола, системных событий, сканера и вкладке Задачи реплицируются в индивидуальные столбцы и строки. Часть данных хранится не в базе данных, а в отдельных файлах (то есть в *.txt или *.xml формате).
- Автоматическая репликация сведений о журнале обнаруженных угроз, автоматическая репликация сведений о журнале файрвола, автоматическая репликация сведений о журнале системных событий, автоматическая репликация сведений о журнале сканера
Эти опции позволяют реплицировать дополнительную информацию, хранящуюся в отдельных файлах. Они также могут быть загружены по запросу, после нажатия кнопки Запрос.

ПРИМЕЧАНИЕ. Напрашивается вопрос, почему некоторые журналы реплицируются автоматически, а журналы описаний и клиентские журналы реплицируются только по запросу

Это связано с тем, что некоторые журналы содержат большие объемы данных, которые могут быть не важны. Например, журнал сканнера с включенной опцией ведения журнала для всех файлов может занимать значительное место на диске. В этой информации обычно нет необходимости, и она может быть запрошена вручную.

4.6.6 Обновления

вкладка позволяет установить настройки для функции зеркала, которая встроена в ESET Remote Administrator (ERAS). Это альтернатива аналогичной функции, которая доступна в клиентском решении ESET Smart Security и антивирусе ESET NOD32 в версиях для корпоративных клиентов.

- **Сервер обновлений**
UNC-путь или URL-адрес сервера обновлений. В большинстве случаев нет необходимости изменять установку по умолчанию **Выбрать автоматически** (Choose automatically), которая позволяет автоматически загружать обновления с сервера ESET.
- **Интервал обновления**
Устанавливает промежуток времени между обновлениями (рекомендован промежуток в 60 минут)
- **Имя пользователя обновления**
Данные аутентификации, открывающие доступ к серверу обновлений
- **Пароль обновления**
Данные аутентификации, открывающие доступ к серверу обновлений
- **Обновить сейчас**
Нажмите эту кнопку для немедленного обновления
- **Создание зеркала обновлений**
При активации, программа позволяет загружать обновленные файлы для других клиентов сети в каталог указанный в поле **Каталог для хранения зеркальных файлов** (Folder to store mirrored files). Если активирована опция **Предоставить файлы обновлений через внутренний HTTP-сервер** (Provide update files via internal HTTP server), файлы обновлений будут доступны через внутренний веб-сервер (HTTP), через указанный порт (Номер серверного HTTP порта по умолчанию – 2221).
- **Аутентификация**
Позволяет администратору установить метод аутентификации для клиентов, подключающихся к ERA серверу. Выберите **НЕТ** (NONE) чтобы разрешить доступ к HTTP серверу всем клиентам. Выберите **Основная** (Basic) для использования основного кодирования по алгоритму base64. NTLM метод является наиболее доступным методом аутентификации. Он сверяет имена учетных записей пользователей, которые указаны в клиентской части формы имени пользователя и пароля, и разрешает доступ к серверу обновлений.

Для корректной работы функции зеркала, необходимо указать (в окне расширенных настроек), какие компоненты будут загружаться с сервера обновлений, в том числе языковые версии. Нажмите F5 в главном программном окне ESET Smart Security или антивируса ESET NOD32, затем выберите раздел **Обновить** (Update) в дереве расширенных настроек. Нажмите кнопку **Настроить...** (Setup...) и перейдите на вкладку **Зеркало** (Mirror). Необходимо выбрать все версии и компоненты, которые будут использоваться.

4.6.7 Вкладка другие настройки

- **SMTP настройки (Сервер, Адрес отправителя, Имя пользователя, Пароль)**
Некоторые функции ESET Remote Administrator требуют определения настроек SMTP сервера. Эти функции включают удаленную установку через электронную почту или отправку создаваемых отчетов на указанные адреса электронной почты.
- **Разрешение добавления клиентов**
Если эта функция отключена, на вкладку клиентов нельзя добавлять новых клиентов – даже клиенты, передающие данные через сервер ERA, не будут отображаться на вкладке **Клиенты** (Clients).
- **Сброс флага «Новый» (New) новыми клиентами**
Если эта функция включена, флаг Новый (New) удаляется для клиентов, впервые подключающихся к ERAS. Для получения дополнительных сведений просмотрите раздел 4.4.3 «Вкладка **Клиенты** (Clients)».
- **Порты (Консоль, Клиент, Порт репликации данного сервера, ESET Remote Installer)**
Определяет адреса портов, через которые ERA сервер будет ожидать сигнала о подключении, устанавливаемом через:
 - Консоль (по умолчанию TCP 2223)
 - Клиент (по умолчанию TCP 2222)
 - процесс репликации (Порт репликации (Replication port), по умолчанию TCP 2846)
 - агент удаленной установки (ESET Remote Installer, по умолчанию TCP 2224)
- **Разрешение передачи данных ThreatSense.Net на ESET сервер**
Если включено, ERA сервер передает сомнительные файлы и статистические данные от клиента на сервер ESET. Это полезно в тех случаях, когда передача этих данных непосредственно с клиентских рабочих станций нежелательна.
- **Изменение расширенных настроек...**
Эти командные кнопки открывают ESET Configuration Editor, где можно произвести точную настройку ERA сервера.

5. Задачи

ESET Remote Administrator позволяет дистанционно выполнять задачи на клиентской рабочей станции. Эти задачи выполняются в момент установки клиентом подключения к ERA серверу (через TCP 2222), которые происходят каждые 5 минут.

Имеется три типа задач:

- Конфигурирование – Изменяет клиентские конфигурации
- Сканирование по запросу – Выполняет сканирование по запросу
- Обновить сейчас – выполняет задачу обновления

Для открытия мастера задач из консоли ERA, нажмите **CTRL+N**, выберите **Файл – Новая задача...**(File – New Task...) или нажмите значок в панели инструментов ERAC. Мастер задач также можно вызвать нажатием правой кнопки мыши по выбранному клиенту (эта опция пропускает несколько диалоговых окон – для полного конфигурирования используйте один из двух первых способов вызова мастера задач).

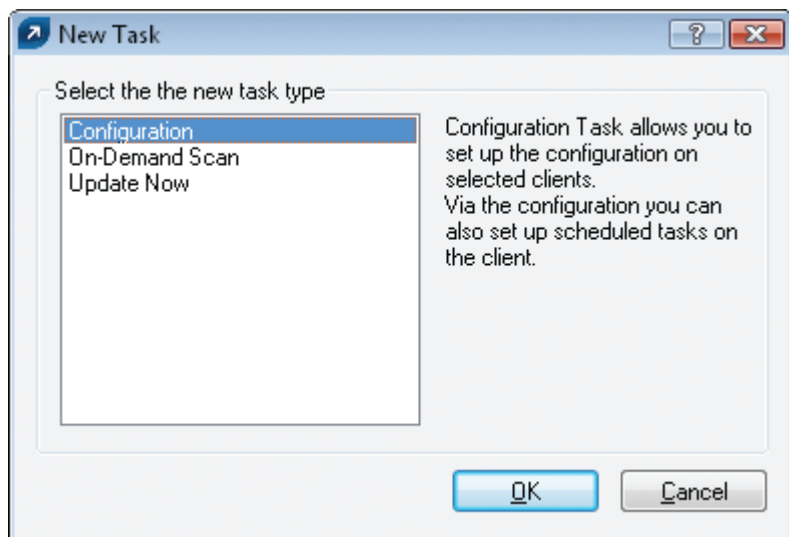


Рис. 8 ERA предлагает три типа задач

5.1 Задача конфигурирование

Для запуска этого типа задачи нажмите **Создать** (Create...) для создания новой задачи (*.xml файл). Чтобы выбрать к применению для удаленных клиентов уже существующий файл конфигурации.xml, нажмите **Выбрать...** (Select...)

ПРИМЕЧАНИЕ. Файлы конфигурации *.xml взаимно совместимы, не зависимо от их происхождения. Это означает, что вы можете использовать *.xml файл конфигурации, который присвоен к пакету установки, загруженному с клиентского компьютера, или локально экспортированный (например, из ESET Smart Security).

Изменения файла конфигурации выполняются в ESET Configuration Editor, который описан выше. Пожалуйста, обратите внимание на значки соответствующие каждой из установок, при изменении значки меняют цвет на голубой. Для просмотра выбранной конфигурации нажмите **Вид** (View). Для изменения выбранной конфигурации нажмите **Правка** (Edit).

Нажмите **Создать из шаблона...** (Create from Template...) чтобы открыть существующий *.xml файл конфигурации, и используйте его в качестве отправной точки для создания абсолютно новой конфигурации. После внесения изменений, файл шаблона сохранится без изменений.

Нажмите **Далее** (Next) и выберите клиентов (по отдельности, по группам или по серверам), к которым будет применен XML-файл конфигурации, перетащив их в столбец **Выбранные элементы** (Selected items). Чтобы переместить клиентов, отображенных в области **Клиенты** (Clients), в столбец **Выбранные элементы** (Selected items), выберите **Специальное добавление...** (Add Special...), выберите вариант **Добавить клиентов, загруженных в области «Клиенты»** (Add clients loaded in the Clients pane), а затем нажмите кнопку **Добавить** (Add). Позже из числа клиентов, добавленных из области **Клиенты** (Clients pane), можно указать отдельных клиентов, выбрав их в столбце **Серверы** (Servers) и установив параметр **Только выбранные** (Only selected).

Нажмите **Далее** (Next). Последний шаг – создать **Имя** (Name) и **Описание** (Description) для новой задачи. В том же диалоговом окне можно отложить задачу (параметр **Применить задачу позже** (Apply task after)) или задать ее автоматическое удаление сразу после успешного выполнения на клиентских компьютерах. Для автоматического удаления успешно завершенной задачи на вкладке **Задачи** (Tasks) выберите параметр **Удалять задачи автоматически при успешном завершении** (Delete tasks automatically by cleanup if successfully completed).

5.2 Задача Сканирование по запросу

Для создания задачи сканирование по запросу необходимо указать, какой из клиентских компьютеров применяет задачу (С технической точки зрения, нет большой разницы между установками задачи сканера поколений 2.x и 3.x).

ПРИМЕЧАНИЕ. Если администратор активирует одновременно опции **Задача сканера по запросу для Windows NOD32** (On-demand Scan task for Windows NOD32) и **Задача сканера по запросу для Windows ESET Security Product** (On-demand Scan task for Windows ESET Security Product), одни и те же задачи будут использоваться для новых и старых версий программы. Для этого надо использовать опцию **Исключить эту секцию из сканирования по запросу** (Exclude this section from On-Demand Scan).

Для выполнения задачи по запросу на клиенте с ESET NOD32 версии 2.x, необходимо выбрать **Задача сканирование по запросу для Windows NOD32 версии 2** (On-demand Scan task for Windows NOD32 version 2) и и выполнить написанному далее последовательность действий.

- Выберите профиль, который необходимо применить к сканеру на клиенте (**Имя профиля** (Profile name)), вы можете вручную ввести имя не представленное в списке.
- Выберите диски, которые необходимо включить в список сканера (**Диски для сканирования** (Drives to scan))
- При необходимости, добавьте новый профиль или измените (**Правка** (Edit button)) существующую конфигурацию профиля, описанного в первом пункте
- Нажмите **Далее** (Next), чтобы продолжить и выбрать клиентов, к которым будет применена задача.
- Нажмите **Готово** (Finish)

ПРИМЕЧАНИЕ. Сканирование по запросу на клиенте использует конфигурацию выбранного профиля + конфигурацию, прикрепленной XML-конфигурации (кнопка **Правка** (Edit)). Профиль сканирования меняется только на время выполнения задачи.

Опция **Сканирование без удаления** (Scan without cleaning) аналогична к опциям **Только сканирование** (Scan only) и **Сканирование и удаление** (Scan and clean) в модуле NOD32 в ESET NOD32 для Windows 2.x. Разница между этими опциями следующая.

- **Сканирование без удаления** (Scan without cleaning) активировано: Не предпринимать никаких действий над найденными зараженными элементами, сканер создает журнал.
- **Сканирование без удаления** (Scan without cleaning) не активировано: Предпринимаются действия, определенные в соответствующей конфигурации для удаляемых и не удаляемых угроз.

Если на клиентском компьютере установлено программное решение поколения 3.x (ESET Smart Security или антивирус ESET NOD32), то необходимо выбрать **Задача сканирование по запросу для Windows ESET Security Product** (On-demand Scan task for Windows ESET Security Product), и выполнить следующие действия:

- Выберите профиль, который необходимо применить к сканеру на клиенте (**Имя профиля** (Profile name)), вы можете вручную ввести имя не представленное в списке.
- Выберите диски, которые необходимо включить в список сканера (**Диски для сканирования** (Drives to scan) или назовите собственные объекты сканирования **Добавить путь** (Add path)).
- Нажмите **Далее** (Next), чтобы продолжить и выбрать клиентов, к которым будет применена задача.
- Нажмите **Готово** (Finish)

5.3 Задача обновить сейчас

Для выполнения задачи обновления необходимо указать, какой из клиентских компьютеров применяет задачу (С технической точки зрения, нет большой разницы между установками задачи сканера поколений 2.x и 3.x).

ПРИМЕЧАНИЕ. Если администратор активирует одновременно опции **Задача сканера по запросу для Windows NOD32 version 2** (On-demand Scan task for Windows NOD32) и **Задача сканера по запросу для Windows ESET Security Product** (On-demand Scan task for Windows ESET Security Product), одни и те же задачи будут использоваться для новых и старых версий программы. Для этого используйте опцию **Не подвергать эту секцию сканированию по запросу** (Exclude this section from On-Demand Scan).

Дальнейшие действия фактически одинаковы для обеих версий программы.

- Выберите профиль, который необходимо применить к сканеру на клиенте (**Имя профиля** (Profile name)), вы можете вручную ввести имя не представленное в списке. Обычно нет необходимости указывать какой-либо профиль (оставьте не активной опцию **Указать имя профиля** (Specify profile name))
- Нажмите **Далее** (Next), чтобы продолжить и выбрать клиентов, к которым будет применена задача.
- Нажмите **Готово** (Finish)

ПРИМЕЧАНИЕ. Клиентские решения (Антивирус ESET NOD32, ESET Smart Security...) содержат автоматические задачи обновления по умолчанию. Поэтому задача **Обновить сейчас** (Update Now) является дополнительной и единовременной функцией.

6. Установка клиентского решения ESET

Эта глава посвящена установке (и прямой, и удаленной) клиентских решений ESET для операционных систем Microsoft Windows.

ПРИМЕЧАНИЕ. Не смотря на техническую возможность удаленной установки продуктов ESET для серверов, мы рекомендуем использовать эту функцию только для рабочих станций.

6.1 Параметры командной строки для прямой установки клиентского решения

Несколько параметров могут оказывать влияние на процесс установки. Они могут быть использованы как во время прямой установки администратором на рабочей станции, так и при удаленной установке. При удаленной установке, параметры выбираются во время процесса конфигурирования пакета установки, выбранные параметры автоматически применяются к выбранным клиентам.

Дополнительные параметры для ESET Smart Security и антивируса ESET NOD32 можно впечатать после имени *.msi пакета установки (например, `ea_nt64_ENU.msi /qn`):

- `/qn`
Скрытый режим установки – диалоговые окна не выводятся
- `/qb!`
Вмешательство пользователя невозможно, но процесс установки показывается в индикаторе хода
- `REBOOT=»ReallySuppress«`
Блокирование перезапуска после установки программы
- `REBOOT=»Force«`
Автоматическая перезагрузка после установки
- `REBOOTPROMPT =» «`
После завершения установки выводится окно с предложением о перезагрузке для пользователя (невозможно использовать совместно с /qn).
- `ADMINCFG="path_to_xml_file"`
В ходе установки к клиентскому решению ESET применяются параметры из определенного *.xml файла. Параметр не требуется при удаленной установке. Пакет установки содержит собственный *.xml файл конфигурации, который применяется автоматически.

Параметры для антивируса ESET NOD32 версии 2.x необходимо впечатать после файла `setup.exe`, который может быть извлечен вместе с другими файлами из пакета установки (например, `setup.exe /silentmode`):

- `/SILENTMODE`
Скрытый режим установки – диалоговые окна не выводятся
- `/FORCEOLD`
Установит новую версию поверх старой.
- `/CFG=" path_to_xml_file"`
В ходе установки, параметры устанавливаются в определенном *.xml файле, примененном к клиентскому решению ESET. Параметр не требуется при удаленной установке. Пакет установки содержит собственный *.xml файл конфигурации, который применяется автоматически.
- `/REBOOT`
Автоматическая перезагрузка после установки.
- `/SHOWRESTART`
После завершения установки выводится окно с предложением о перезагрузке для пользователя.
- `/INSTMFC`
Установка, требующая библиотеку базовых классов Microsoft (MFC libraries) для операционной системы Microsoft Windows 9x. Этот параметр может использоваться всегда, даже если имеются библиотеки базовых классов Microsoft (MFC libraries).

6.2 Методы установки

6.2.1 Прямая установка с предопределенной XML конфигурацией

При прямой установке, администратор должен находиться за компьютером, на который производится установка клиентского решения ESET. Этот метод не требует дополнительной подготовки, и применим в небольших компьютерных сетях или в ситуациях, когда ESET Remote Administrator не используется.

Эта задача может быть сильно упрощена использованием предопределенной *.xml конфигурации. Никаких дополнительных изменений, как определение сервера обновлений (имя пользователя и пароль, путь к зеркальному серверу и так далее), скрытый режим, расписание сканирования и так далее, в ходе или после установки не требуется.

Есть различия в применении формата *.xml конфигурации для версий 3.x и 2.x клиентского решения ESET.

- Версия 3.x: Загрузите файл установки с веб-страницы ESET (например, ess_nt32_enu.msi). Вставьте файл конфигурации *.xml (cfg.xml) в каталог, где хранятся файлы установки. Если вы используете программу установки, она автоматически получает конфигурацию из файла конфигурации *.xml. Если файл *.xml имеет другое имя или расположен в другом месте, можно применить параметр `ADMINCFG="path_to_xml_file"`. (Например, `ess_nt32_enu.msi ADMINCFG="\\server\xml\settings.xml"` для применения конфигурации расположенной на сетевом диске).
- Версия 2.x: Загрузите файл установки с веб-страницы ESET (например, ndntenst.exe). Извлеките загруженный файл в папку. Папка будет содержать файлы установки, в том числе `setup.exe`. Скопируйте файл конфигурации *.xml с именем pod32.xml в папку. Запустите файл `setup.exe` и конфигурация из pod32.xml будет автоматически применена. Если файл конфигурации *.xml имеет другое имя или расположен в другом месте, можно применить параметр:
`/cfg="path_to_xml_file"`.

(например, `setup.exe /cfg="\\server\xml\settings.xml"` для применения конфигурации расположенной на сетевом диске).

ПРИМЕЧАНИЕ. Также можно использовать другие параметры, описанные в предыдущей главе.

6.2.2 Удаленная установка в общем случае

ESET Remote Administrator предлагает несколько способов удаленной установки, описанных ниже. Различие между способами в том, каким образом пакет установки доставляется на рабочую станцию.

- Удаленная push-установка
- Удаленная установка через сценарий входа
- Удаленная установка через электронную почту

Удаленная установка не обязательно осуществляется средствами ERA, существуют и другие способы (центральное распределение среднего уровня интеграции (MSI), LANDesk и так далее). В конце концов, главное доставить файл установки (или агент) к клиенту и убедиться, что он доступен под учетной записью администратора. Для этого может быть также использована прямая установка, описанная в предыдущем разделе.

Удаленная установка при помощи ESET Remote Administrator содержит следующие шаги:

- Создание пакетов установки
- Описание пакетов для клиентской рабочей станции (метод push-установки, установка через сценарий входа, установка через электронную почту, другие решения)

Первый шаг запускается через ERA консоль, но сам пакет установки располагается на ERA сервере, по следующему пути:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\packages`

Для получения пакета установки через ERA консоль, выберите вкладку **Удаленная установка (Remote Install)** и нажмите кнопку **Пакеты...** (Packages...).

Каждый пакет установки определяется именем (см. (1) в рисунке 9 выше). Другие секции диалогового окна относятся к содержимому пакета, который будет применен после успешной доставки на соответствующую клиентскую станцию. Каждый пакет содержит:

- Файлы установки (2) клиентского решения ESET
- Файлы конфигурации *.xml (3)
- Параметры командной строки (4)

Выпадающее меню **Тип (Type)** в секции 1 расширяет возможности ERA. В дополнение к удаленной установке, клиентское решение ESET может быть деинсталлировано удаленно с использованием опции **Удалить ESET Security Products и NOD32 version 2 (Uninstall ESET Security Products and NOD32 version 2)**. Удаленная установка сторонних приложений также может быть осуществлена, если выбрать **Специальный пакет (Custom package)**.

ПРИМЕЧАНИЕ. По техническим причинам, установка старой версии ESET решений (версия 2.x) является отдельной функцией от установки решений поколения 3.x. По той же причине пакеты хранятся в двух разных папках на ERA сервере.

ПРИМЕЧАНИЕ. Опция **Выборочный пакет (Custom package)** предлагает ряд методов, в том числе деинсталляцию решений по безопасности других разработчиков (если используется соответствующая команда пакетного режима).

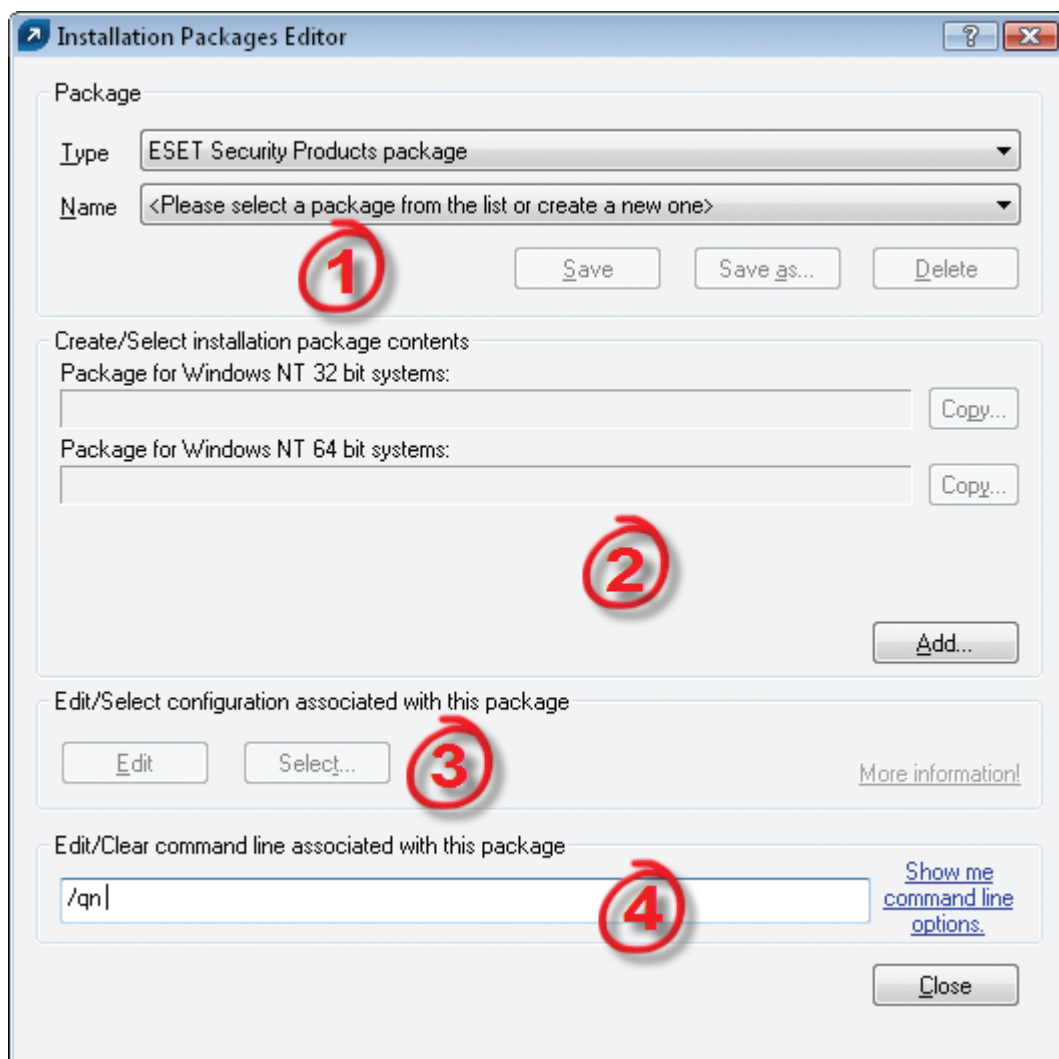


Рис. 9 Диалоговое окно Редактора пакетов установки (installation packages Editor)

Каждый пакет автоматически включается в агент ESET Remote Installer, который предусматривает целостную установку и связь между рабочими станциями и ERA сервером. Агент ESET Remote Installer называется `installer.exe` и содержит имя ERA сервера и имя и тип пакета, к которому он принадлежит. В следующих главах дается подробное описание данного агента.

6.2.3 Удаленная push-установка

Данный метод удаленной установки немедленно перемещает клиентское решение ESET на целевой компьютер. Целевой компьютер должен находиться в сети. Для инсталляции необходимо выполнение следующих условий (дополнительные требования приведены в главе 2 «ERA сервер»):

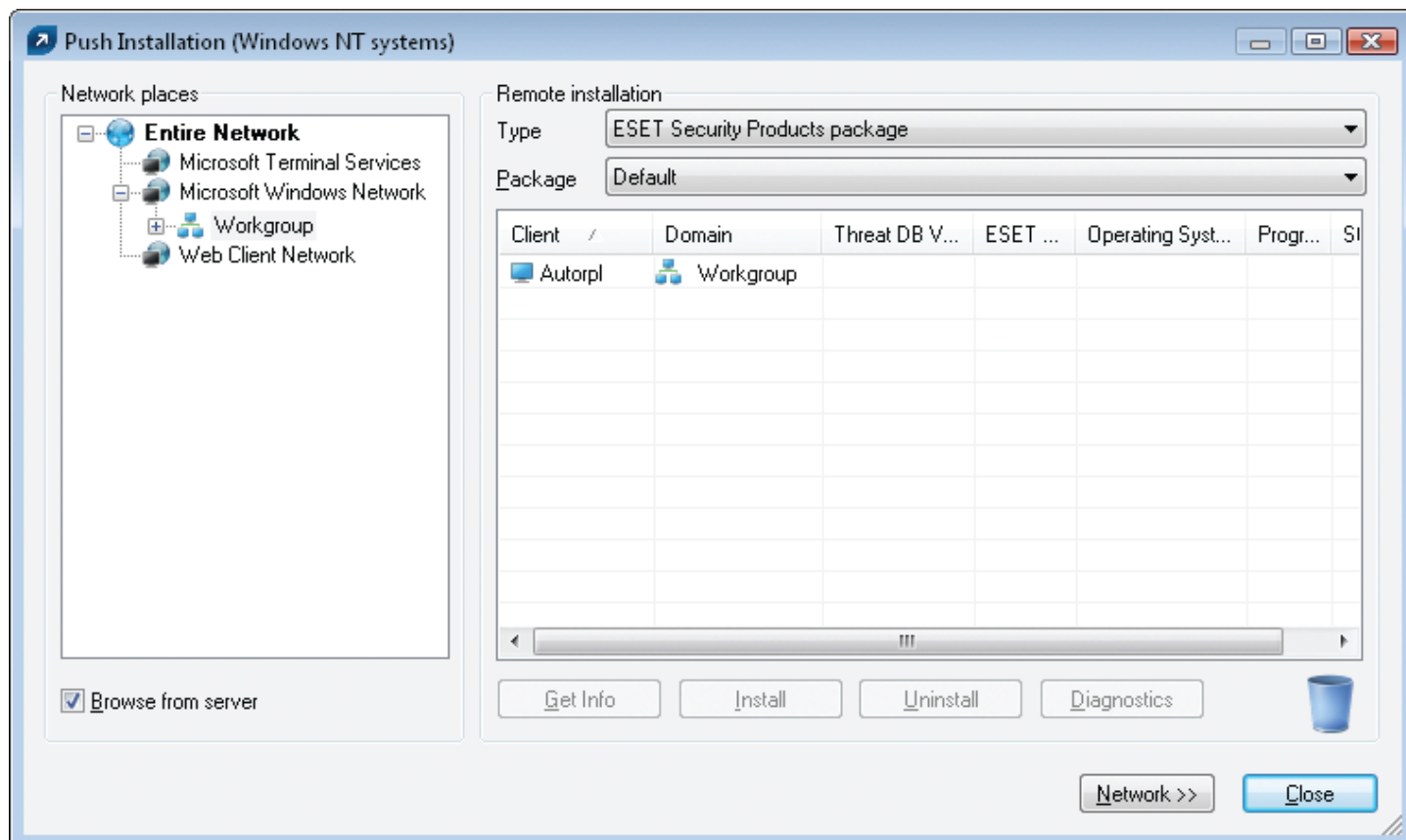
- Активировать сетевой клиент Microsoft (функция сетевого адаптера)
- Активировать службу совместного использования (функция сетевого адаптера)
- Активировать службу совместного использования файлов в файрволе
- Службы: Служба удаленной регистрации, удаленный диспетчер служб, сервер
- Имя пользователя и пароль администратора для клиентской рабочей станции (предпочтительно имя пользователя и пароль доменного администратора).

Для запуска push-установки, выполните следующие действия:

Нажмите **Установить...** (Install...) в ERA консоли (вкладка **Удаленная установка** (Remote Install)).

В разделе **Сетевое окружение** (Network places) слева, найдите рабочие станции, на которые необходимо переместить пакет установки. Переместите их в пустую часть окна справа (перетащите (drag & drop)).

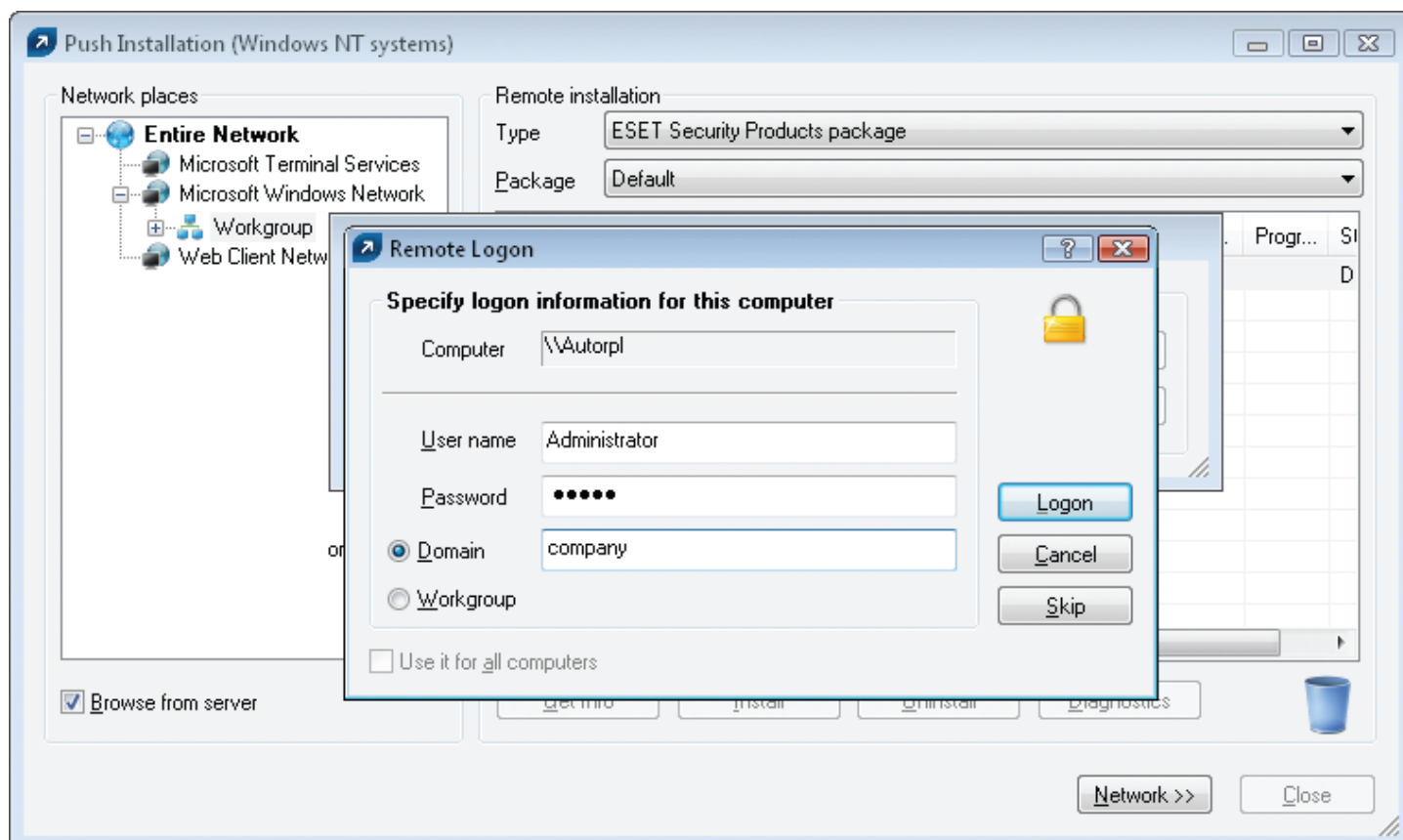
Из выпадающего меню **Пакет** (Package), выберите пакет установки, который необходимо доставить на целевую рабочую станцию.



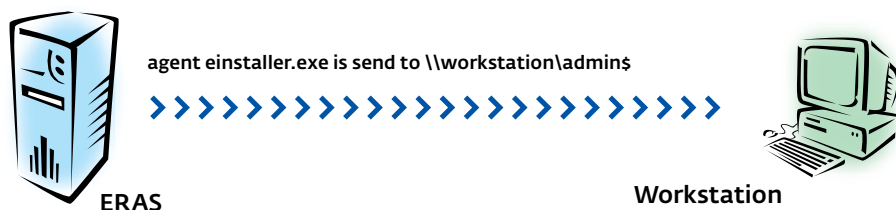
В правой панели выберите рабочие станции, на которые надо установить пакет.

Нажмите **Установить** (Install) (также вы можете выбрать **Получить информацию** (Get Info) для просмотра информации о выбранных клиентах).

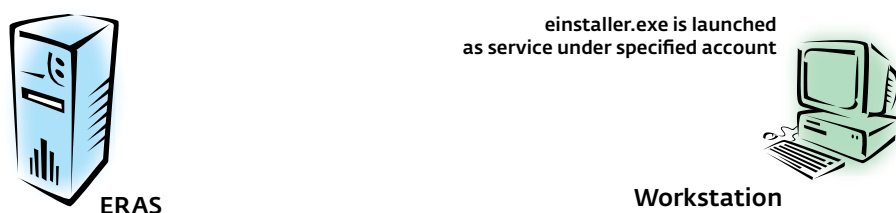
В большинстве случаев, вам будет предложено вписать имя пользователя и пароль для учетной записи, под которой осуществляется установка (это должна быть учетная запись с правами администратора).



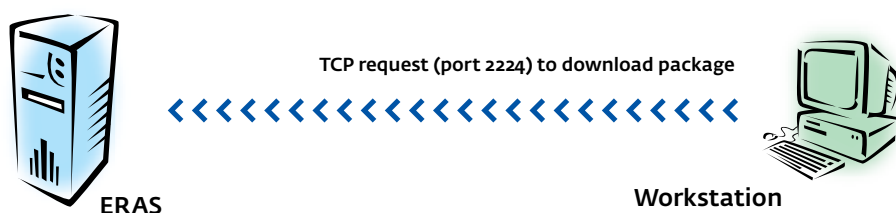
Дальнейшая работа отображается в индикаторе выполнения и сопровождается текстовым сообщением. Процесс описан ниже: ERA сервер отправляет агента `installer.exe` на рабочую станцию при помощи административного общего каталога `admins$`.



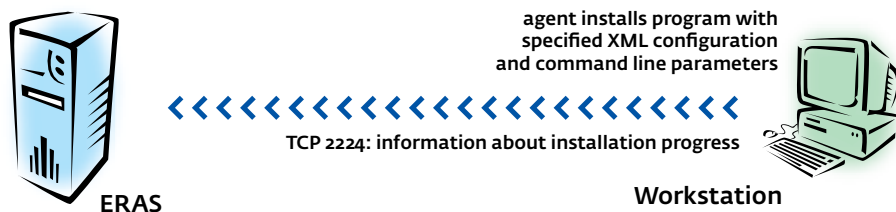
Агент запускается как служба под учетной записью описанной в пункте 6.



Агент устанавливает связь со своим «родительским» ERA сервером и загружает соответствующий пакет установки через TCP порт 2224.



Агент устанавливает пакет, под учетной записью администратора, описано в пункте 6, также применяются соответствующая *.xml конфигурация и параметры командной строки.



Сразу после завершения установки агент посылает сообщение обратно на ERA сервер. Некоторые ESET решения требуют перезагрузки. В этом случае высвечивается сообщение об этом требовании.

Контекстное меню диалогового окна push-установки предлагает следующие опции:

- **Получить информацию (Get Info)**
Эта функция выясняет текущий статус клиентского решения ESET на выбранной рабочей станции (необходимы имя пользователя и пароль администратора). Эта функция использует общий каталог [admins\\$](#).
- **Деинсталляция (Uninstall)**
Удаление программы – агент пытается удаленно деинсталлировать программу. Режим деинсталляции не принимает во внимание, какой пакет был выбран из меню **Пакет (Package)**.
- **Диагностика (Diagnostics)**
Проверяет возможную пригодность клиентов и служб к использованию в удаленной установке. Для более подробной информации просмотрите диагностику процесса удаленной установки.
- **Удаление остатков установщика**
Отключает агенты из диспетчера служб на клиентской станции и удаляет их с жесткого диска. Если данные действия завершены, флажок, предотвращающий повторную установку, во вкладке пакет удаляется (см. раздел 6.4, «Предотвращение повторной установки» (Avoiding repeated installations)).
- **Вход в систему... (Logon...)**
Открывает диалоговое окно для ввода имени пользователя и пароля администратора, который иначе высвечивается автоматически (пункт 6). Эта функция обеспечивает вход в систему рабочей станции.
- **Выход из системы (Logoff)**
Завершает сессию входа в систему на рабочей станции.
- **Добавить клиента... (Add Client...)**
Добавляет отдельного клиента (рабочую станцию) в список. Введите IP адрес или имя клиента. Несколько дополнительных клиентов могут быть добавлены одновременно.

6.2.4 Удаленная установка при входе в систему или через электронную почту

Способы удаленной установки через электронную почту или вход в систему очень похожи. Они различаются только способом доставки агента [einstaller.exe](#) на рабочую станцию. ESET Remote Administrator позволяет запускать агент через сценарий входа или через электронную почту. Агент [einstaller.exe](#) может быть использован отдельно или запускаться другими способами (для более подробной информации ознакомьтесь со следующей главой).

В то время, как сценарий входа выполняется автоматически в момент входа пользователя в систему, способ электронной почты требует вмешательства со стороны пользователя, который запускает агент [einstaller.exe](#) из вложения в электронное сообщение. При повторном запуске [einstaller.exe](#) не будет осуществлять еще одну установку решения ESET. Для более детальной информации ознакомьтесь с разделом 6.4 «Предотвращение повторной установки» (Avoiding repeated installations).

ПРИМЕЧАНИЕ. Строка, вызывающая агент [einstaller.exe](#) из сценария входа в систему, может быть введена при помощи редактора или другого частного инструмента. Также, файл [einstaller.exe](#) может быть послан по электронной почте, в качестве вложения любым почтовым клиентом. Независимо от используемого способа, убедитесь, что вы используете правильный файл [einstaller.exe](#). Нет необходимости выполнять описанные ниже действия.

ПРИМЕЧАНИЕ. Для запуска [einstaller.exe](#), пользователь, находящийся в системе в текущий момент не обязательно должен быть администратором. Агент примет необходимое имя пользователя, пароль и домен администратора с сервера ERA. Для более подробной информации ознакомьтесь с окончанием данной главы.

Внесение строки (пути к [einstaller.exe](#)) в сценарий входа в систему:

- Во вкладке **Удаленная установка (Remote Install)** нажмите **Экспорт...** (Export...) и выберите **Тип (Type)** и имя **Пакета (Package)** для установки.
- Нажмите на кнопку «...» рядом с **Папка (Folder)** и выберите каталог для хранения [einstaller.exe](#), и где он будет доступен через сеть.
- Убедитесь, что путь в поле **Общие (Share)** указан правильно или при необходимости исправьте его.
- Нажмите на кнопку «...» рядом с **Папка сценария (Script Folder)** для выбора папки для хранения сценария.
- В нижней части выберите файл, в который будет внесена строка (вызов [einstaller.exe](#)).
- Нажмите **Экспорт в сценарий входа в систему (Export to Logon Script)** для внесения строки.
- Местоположение строки можно изменить в расширенном режиме, нажав **Изменить (Edit)** и сохранить, нажав кнопку **Сохранить (Save)**.

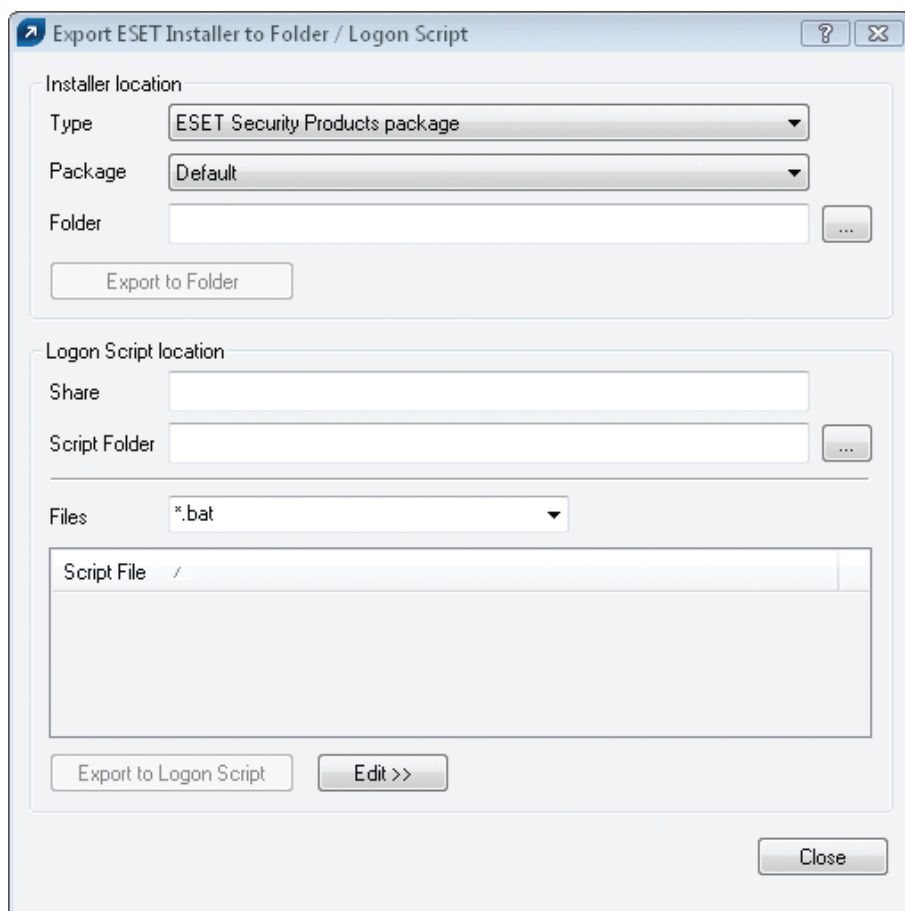


Рис. 10 Диалоговое окно Удаленная установка через электронную почту или вход в систему

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

- Нажмите **Электронная почта...** (Email...) во вкладке **Удаленная установка** (Remote Install) и выберите тип и имя пакета для установки.
- Нажмите **Кому** (To...), чтобы выбрать адрес из адресной книги* (или введите новые адреса).
- Введите тему сообщения в поле **Тема** (Subject).
- Наберите текст сообщения в поле **Тело сообщения** (Body).
- Нажмите **Отправить** (Send).

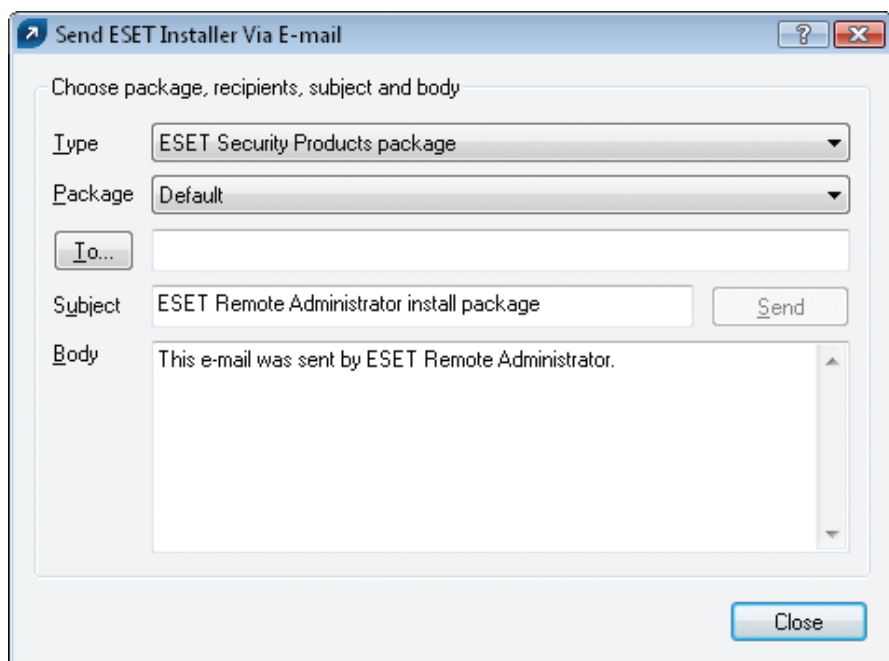
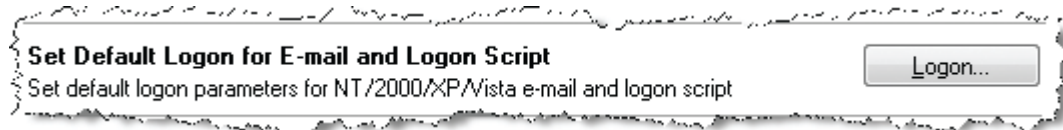


Рис. 11 Отправка установщика ESET через диалоговое окно электронной почты

* Консоль ERA открывает адресную книгу Microsoft Outlook (подразумевается, что она установлена на том же компьютере что и консоль ERA)

В ходе удаленной установки происходит обратная связь с сервером ERA и агент ([einstaller.exe](#)) использует настройки параметра **Установить вход в систему по умолчанию для электронной почты и сценария входа в систему** (Set Default Logon for E-mail and Logon Script) на вкладке **Удаленная установка** (Remote Install).



Нажмите **Вход в систему** (Logon) для указания имени пользователя и пароля учетной записи под которой будет производиться установка. (Это должна быть учетная запись администратора или, что предпочтительно, администратора домена).

ПРИМЕЧАНИЕ. Данные, введенные в диалоговом окне **Вход в систему** (Logon) удаляются при каждом перезапуске службы (ERA сервер).

6.2.5 Выборочная удаленная установка

Использование инструментов входящих в ESET Remote Administrator, не является обязательным требованием. В конце концов, самое важное – это доставить и запустить [einstaller.exe](#) на клиентской станции.

ПРИМЕЧАНИЕ. Для запуска [einstaller.exe](#), пользователь, находящийся в системе в текущий момент, не обязательно должен быть администратором. Агент примет необходимое имя пользователя, пароль и домен администратора с сервера ERA. Для более подробной информации ознакомьтесь с окончанием данной главы.

Файл [einstaller.exe](#) может быть получен следующим образом:

- Во вкладке **Удаленная установка** (Remote Install) нажмите **Экспорт...** (Export...) и выберите **Тип** (Type) и имя **Пакета** (Package) для установки.
- Нажмите на кнопку «...» рядом с **Папка** (Folder) и выберите каталог для экспорта [einstaller.exe](#).
- Нажмите кнопку **Экспорт в папку** (Export to Folder)
- Используйте извлеченный [einstaller.exe](#)

ПРИМЕЧАНИЕ. Способ «Прямая установка с предопределенной XML конфигурацией» может быть использован, например, там, где можно обеспечить права администратора для установки. Пакеты среднего уровня интеграции запускаются с использованием параметра /qn (для версии 3) или /silentmode (для версии 2), что позволяет осуществлять установку без выведения уведомления для пользователя.

В ходе удаленной установки, происходит обратная связь с ERA сервером и агент ([einstaller.exe](#)) использует установки из **Установить вход в систему по умолчанию для электронной почты и сценария входа в систему** (Set Default Logon for E-mail and Logon Script) из вкладки удаленной установки.



Нажмите **Вход в систему** (Logon) для указания имени пользователя и пароля учетной записи, под которой будет производиться установка. Это должна быть учетная запись администратора или, что предпочтительно, администратора домена.

Если агент [einstaller.exe](#) запущен вручную на рабочей станции, то удаленная установка обеспечивается следующим образом:

- Агент [einstaller.exe](#) отправляет запрос ERA серверы (TCP порт 2224)
- ERA сервер начинает push-установку соответствующего пакета (пересылая через общую папку [admins](#))
- Установка пакета запускается, с применением приписанной конфигурации *.xml, параметры командной строки под учетной записью определяются на ERA сервере (кнопка **Вход в систему** (Logon)).

6.3 Подробное описание агента einstaller.exe

Каждому пакету автоматически назначается агент ESET Remote Installer, который облегчает процесс установки и связи между целевыми рабочими станциями и сервером ERA. Агент ESET Remote Installer называется [einstaller.exe](#) и содержит следующую информацию:

- Имя сервера ERA (+ IP-адрес сервера ERA)
- Имя и тип установочного пакета

Процесс удаленной установки с использованием агента [einstaller.exe](#) состоит из двух этапов. На первом этапе на рабочую станцию доставляется программа установки небольшого размера (около 200 КБ). При условии, что выполняются все требования, агент начинает загружать весь установочный пакет (несколько МБ) с сервера ERA.

Деятельность агента [einstaller.exe](#) регистрируется в файле `%TEMP%\einstaller.log`, и если это технически возможно – также на сервере ERA (номер целевого TCP-порта 2224).

При запуске агента `installer.exe` на рабочей станции с операционной системой Microsoft Windows NT4/2000/XP/Vista:

`installer.exe` соединяется с сервером ERA через TCP-порт 2224 и принимает имя пользователя и пароль, определенные в ERA (при установке, либо при помощи кнопки **Вход в систему...** (Logon...)).

(1) – это сигнал, чтобы сервер ERA отправил соответствующий пакет установки через системного администратора.

Ожидаящий агент `installer.exe` принимает пакет и начинает установку под определенной учетной записью, применяя соответствующие XML-настройки и параметры командной строки.

Если пользователь не обладает необходимыми правами, или были введены неправильные имя пользователя и пароль, агент `installer.exe` пытается произвести установку под текущим пользователем (при условии, что у него есть права администратора). Соответствующий пакет установки загружается непосредственно агентом `installer.exe` через TCP/IP-порт 2224.

При операционной системе Microsoft Windows 95/98/Me, где не существует иерархии учетных записей, пакеты установки загружаются агентом `installer.exe` (без проверки подлинности) и устанавливаются под текущим пользователем.

6.4 Предотвращение повторных установок

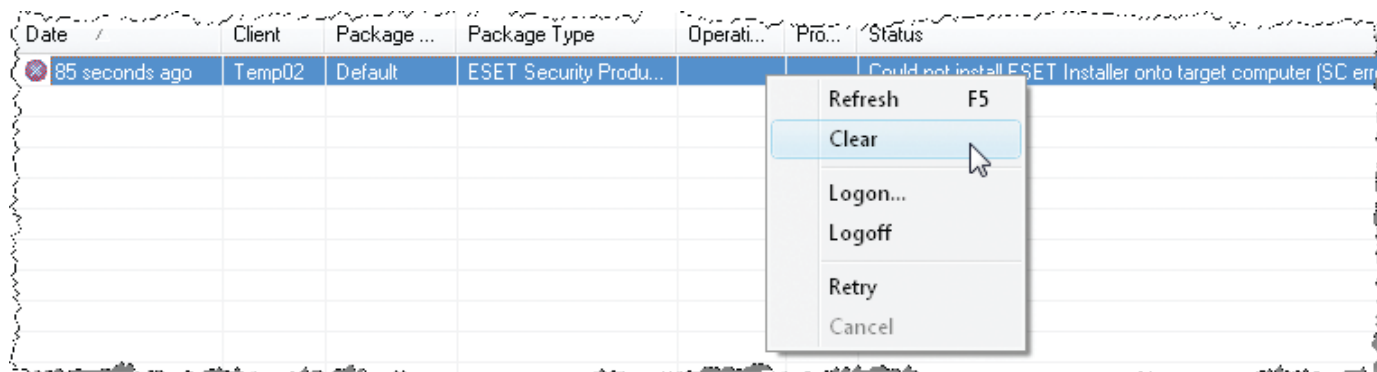
Сразу после успешного завершения удаленной установки агент помечает удаленного клиента «флажком», чтобы предотвратить повторную установку того же пакета. Флажок ставится у следующего ключа регистрации:

`HKEY_LOCAL_MACHINE\Software\Eset\Eset Remote Installer`

Если **Тип** (Type) и **Имя** (Name) пакета, определенные в агенте `installer.exe`, совпадают с данными ключа регистрации, то установка производиться не будет. Это предотвращает повторные установки пакета на целевую рабочую станцию. Если агент `installer.exe` запускается повторно, сервер ERA обеспечивает дополнительный уровень защиты против повторных установок в тот момент, когда программа установки устанавливает обратное соединение с сервером ERA (TCP-порт 2224). Если появилось сообщение об ошибке, связанной с рабочей станцией, или установка была успешно завершена, попытки повторной установки будут отклонены.

Агент записывает сообщение об ошибке в журнале установочной программы, расположенной в `%TEMP%\installer.log`.

Статус 20001: Программа установки ESET получила команду прекратить сеанс через сервер «X:2224».



Для того чтобы сервер ERA разрешил повторную установку, необходимо удалить записи во вкладке **Удаленная установка** (Remote Install). Для этого щелкните правой кнопкой мыши и выберите команду **Очистить** (Clear) в контекстном меню.

6.5 Процесс установки – сообщения об ошибках

Во время удаленной установки ошибки могут произойти по двум сценариям:

- При доставке агента `installer.exe` на рабочую станцию
- После начала работы `installer.exe`, например, во время самой установки

Во время удаленной установки агент `installer.exe` может отобразить сообщение об ошибке, включающее код SC и GLE. Например:

Не получается установить IPC-соединение с целевым компьютером (SC-код ошибки 6, GLE-код ошибки 1326)

SC-коды ошибки в основном используются для внутренней идентификации, в то время как GLE-коды представляют большую важность для пользователя. Это обычные «коды ошибки Win32, которые можно найти по следующему URL-адресу:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp

Описанная выше ошибка (GLE-ошибка 1326) произошла из-за ввода неправильного имени пользователя и пароля в учетной записи, используемой для установки.

Самая распространенная ошибка – это GLE-ошибка 5 – «Доступ запрещен». Существует несколько причин запрещения доступа:

- У файрвола удаленного клиента отключена функция совместного использования файлов и принтера.
- Отключен сервис сервера, или выключен сетевой адаптер совместного использования файлов и принтера.
- Рабочие станции клиента Windows XP не находятся в домене (политика).

Сообщения об ошибках, которые происходят после того, как агент [installer.exe](#) доставлен на целевую рабочую станцию в [%TEMP%\installer.log](#). Наиболее важные сообщения отправляются обратно на сервер ERA (TCP-порт 2224). Конечно, это происходит только при условии, что отсутствуют проблемы соединения между рабочей станцией и сервером ERA.

На данном этапе установки можно столкнуться со следующими ошибками:

Программа установки Eset получила команду прекратить сеанс через сервер «X:2224».

Программа установки не может установить соединение с сервером X.

Первое сообщение описано в главе 6 «Предотвращение повторных установок». Второе сообщение появляется тогда, когда у агента [installer.exe](#) не получается установить обратную связь с сервером ERA.

6.5.1 Диагностика удаленной установки

Для использования средства диагностики удаленной установки ERA, нажмите кнопку **Установка...** (Install...) во вкладке **Удаленная установка** (Remote Install). После выбора клиента нажмите кнопку **Диагностика** (Diagnostics) чтобы проверить, что не было обнаружено ошибок, и ничто не препятствует удаленной установке. В случае обнаружения ошибок, проверка позволит администратору исправить их до начала удаленной установки.

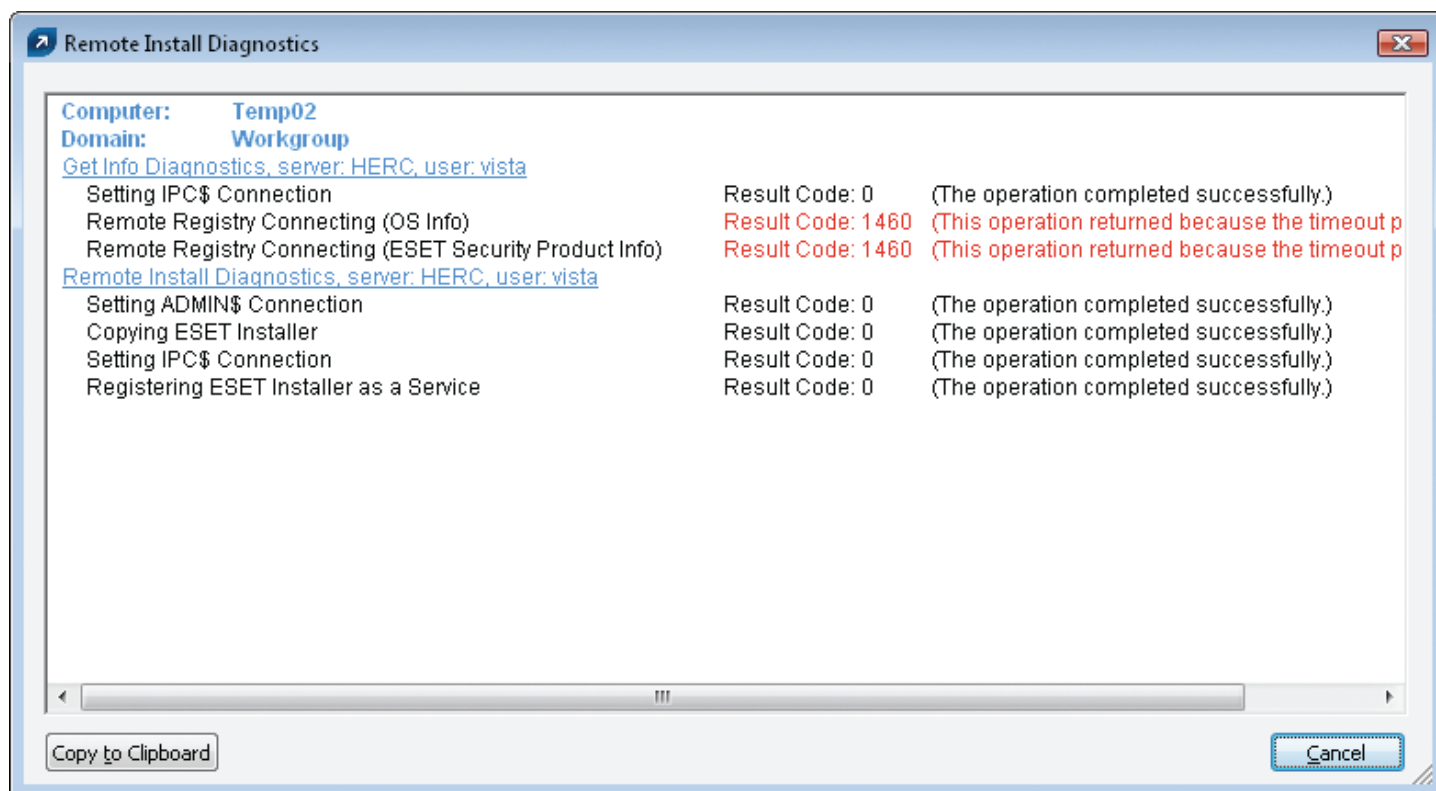


Рис. 12 Средство диагностики обнаруживает возможные проблемы до начала установки

7. Сценарии внедрения удаленного администратора ESET NOD32 Remote Administrator, сервера зеркала и клиентских решений ESET

7.1 Маленькая сеть – 1х сервер ERA, 1х сервер зеркала

Предположим, что все клиенты – это рабочие станции Microsoft Windows 2000/XP и портативные компьютеры, объединенные в сеть.

Сервер под названием GHOST, который включен круглые сутки, может быть рабочей станцией Windows, Professional или Server edition (это необязательно Active Directory Server). Кроме того, допустим, что портативные компьютеры находились вне сети компании во время установки клиентских решений ESET. Структура сети будет выглядеть следующим образом:

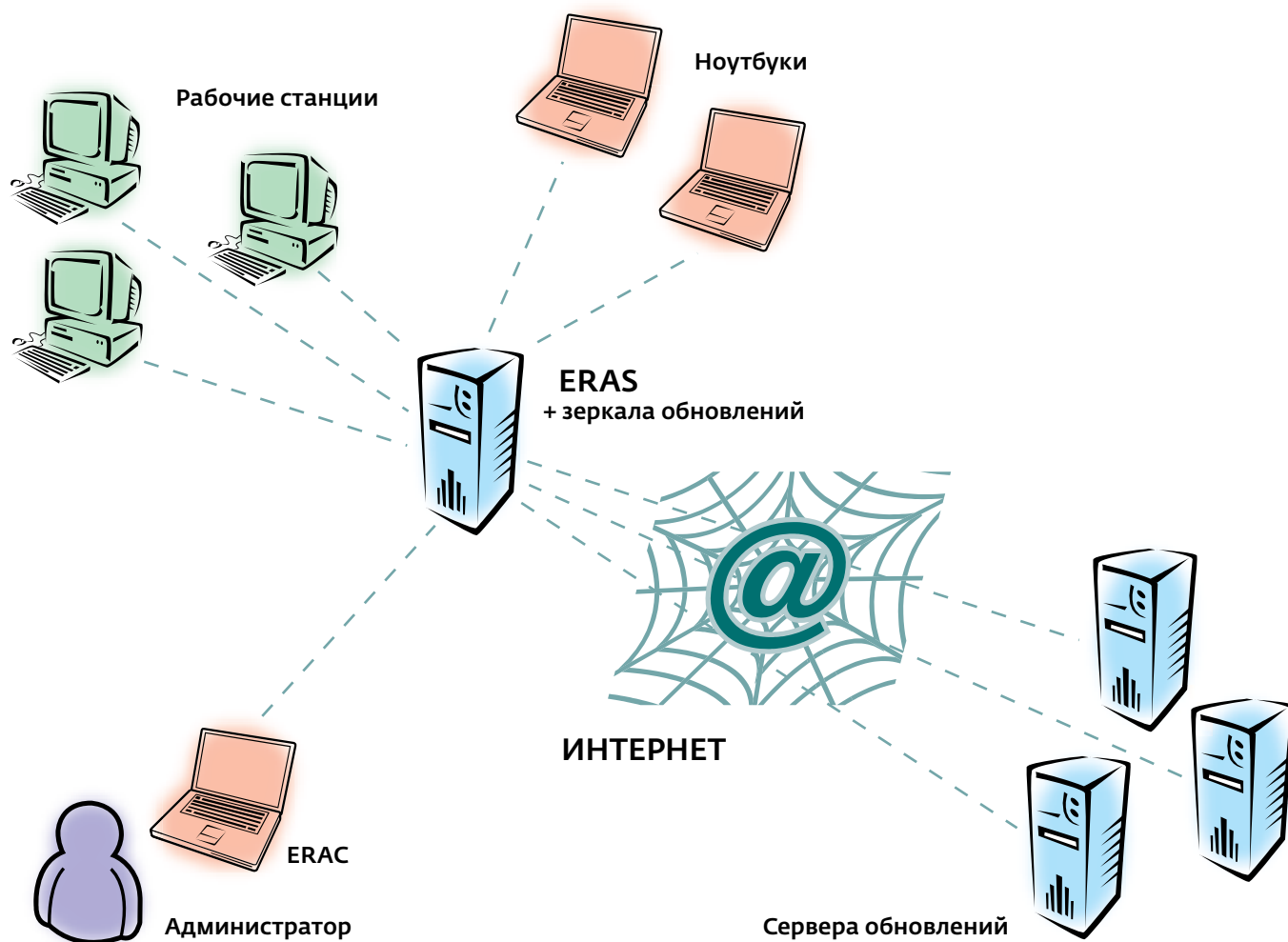


Рис. 13 Структура сети в небольшой компании

7.1.1 Установка HTTP-сервера зеркала

Сначала установите сервер обновлений локальной сети (зеркало) на машине GHOST. Необходимо установить пакет, содержащий функции зеркала (ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition). Во время установки введите имя пользователя и пароль, полученные от ESET (или посредника), – это ваши аутентификационные данные, которые позволят загружать обновления вирусных сигнатур.

Далее добавьте в систему файл лицензии. Вызовите окно расширенной настройки, нажав клавишу F5. В дереве расширенной настройки выберите пункты меню **Разное – Лицензии** (Miscellaneous – Licenses) и нажмите кнопку **Добавить...** (Add...). Найдите файл [nod32.lic](#) и запустите его двойным щелчком мыши. Функциональность дерева активирована. Убедитесь, что зеркало появилось в расширенной настройке обновлений. Из дерева расширенной настройки выберите команду **Обновить** (Update) и нажмите кнопку **Настройка...** (Setup...) – вкладка **Зеркало** (Mirror) будет активной. Выберите эту вкладку и внесите следующие изменения в настройки зеркала:

- Установите флажок **Создать зеркало обновлений** (Create update mirror)
- Установите флажок **Предоставить файлы обновлений через внутренний HTTP-сервер** (Provide update files via internal HTTP server)
- Нажмите кнопку **Папка...** (Folder...) и выберите папку, в которой будут храниться файлы обновлений (например, **C:\ESET**).
- В разделе **Доступные версии** (Available versions) выберите компоненты операционной системы, которые будут получать обновления с зеркала. Если обновления с зеркала будут получать только рабочие станции Microsoft Windows 2000/XP/2003/Vista, то следует отмечать только эти операционные системы.
- Нажмите кнопку **ОК** (OK) для подтверждения.

Затем обновите базу данных вирусных сигнатур, выбрав в главном программном окне команду **Обновить – Обновить базу данных вирусных сигнатур** (Update – Update virus signature database). Эти действия позволят загрузить все необходимые файлы в папку C:\ESET и активировать сервер зеркала.

7.1.2 Установка сервера ERA

Рекомендуется устанавливать сервер ERA на компьютер, в котором хранятся файлы обновления (зеркала), в нашем примере это – GHOST. При установке необходимо указать файл ключа лицензии для работы сервера ERA на протяжении определенного времени. После установки служба сервера ERA запускается автоматически. Деятельность службы сервера ERA записывается в следующем файле:

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

7.1.3 Установка консоли сервера ERA

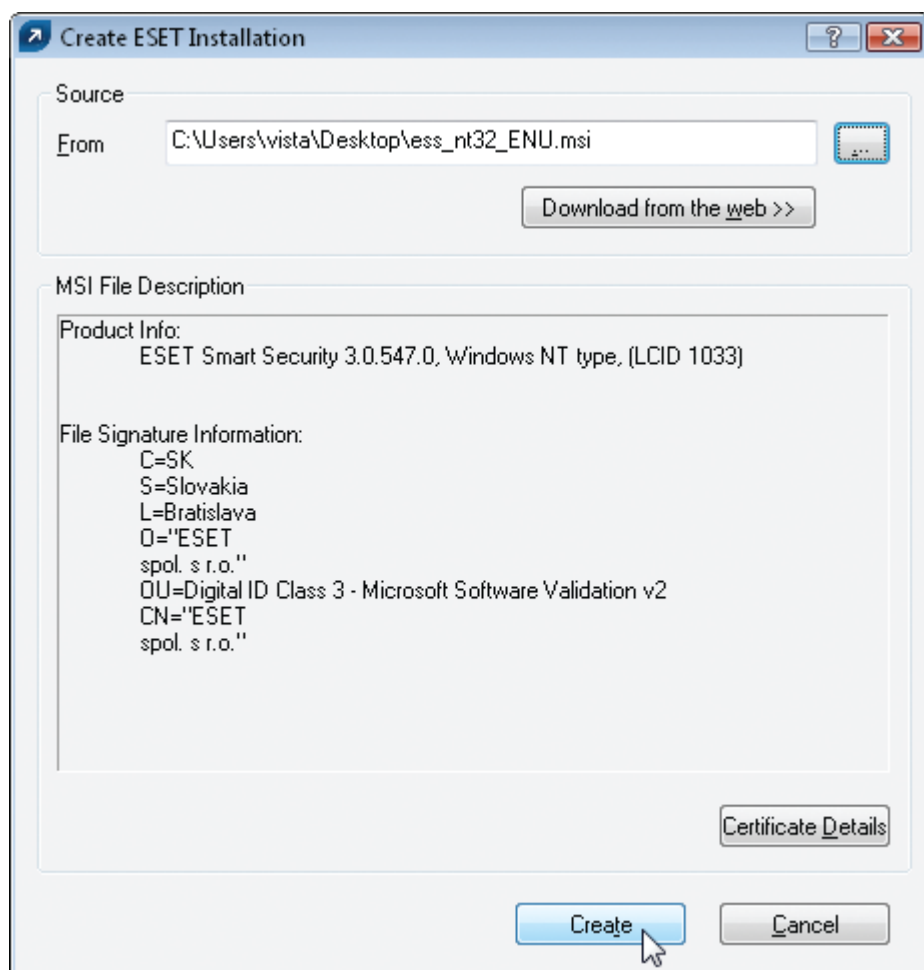
Установите консоль удаленного администратора ESET Remote Administrator на компьютер/ноутбук администратора, как показано в нижней части рисунка. При установке консоли на компьютер, где установлен сервер ERA, имя сервера ERA (в данном случае GHOST) должно быть автоматически введено в настройки консоли. Если консоль и сервер ERA установлены на разных компьютерах, выберите команду **Файл – Изменить подключения...** (File – Edit Connections...) и перейдите на вкладку **Подключение** (Connection). Нажмите кнопку **Добавить/Удалить...** (Add/Remove...) и добавьте имя сервера ERA.

Более подробную информацию см. в разделе 4.1 «Подключение к ERAS».

7.1.4 Удаленная установка на рабочих станциях, находящихся в сети

Если все рабочие станции включены, то самым эффективным методом установки будет принудительная установка. Перед началом установки следует загрузить установочные MSI-файлы для ESET Smart Security или ESET NOD32 Antivirus с веб-сайта ESET. Затем выполните следующие действия:

- Откройте консоль ERA и подключитесь к серверу ERA (в данном случае GHOST). Во вкладке **Удаленная установка** (Remote Install) нажмите кнопку **Пакеты...** (Packages...).
- Нажмите кнопку **Добавить...** (Add...) для вывода окна **Создание установки ESET** (Create ESET Installation), затем нажмите кнопку «...», чтобы ввести загруженные ранее MSI-файлы установки.



- Нажмите кнопку **Создать** (Create) чтобы ввести установочный файл в пакет (отправка MSI-файлов в сервер ERA может занять несколько минут).

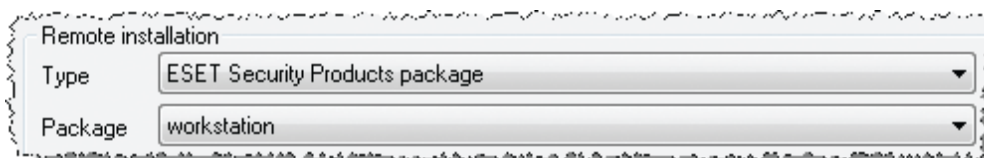
- Нажмите кнопку **Изменить** (Edit) в окне **Редактор установочных пакетов** (Installation Packages Editor) чтобы присвоить пакету XML-файл конфигурации. Этот файл конфигурации будет применен позже при установке пакета.
- В ESET Configuration Editor следует сконцентрировать внимание на следующих настройках:
- **ESET Smart Security – Ядро – Настройка – Удаленное администрирование** (ESET Smart Security – Kernel – Setup – Remote administration)
Следует установить настройки, как показано на рисунке (IP-адрес можно также ввести в настройке **Адрес сервера** (Server address))



- В **ESET Smart Security, ESET NOD32 Antivirus – Обновить – Профиль (Мой профиль) – Настройка** (ESET Smart Security, ESET NOD32 Antivirus – Update – Profile (My profile) – Setup) укажите имя **Сервера обновлений** (Update server) (GHOST).



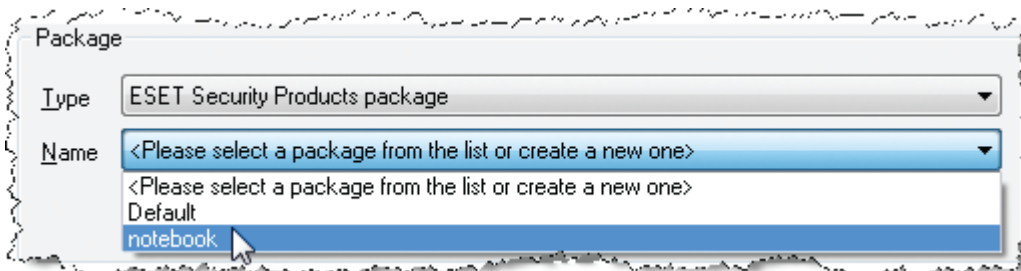
- Это минимальные требования для рабочих станций в сценарии внедрения. Нажмите кнопку **Консоль** (Console) в правой части ESET Configuration Editor, чтобы вернуться в окно **Редактор установочных пакетов** (Installation Packages Editor).
- Нажмите кнопку **Закрыть** (Close) в диалоговом окне **Редактор установочных пакетов** (Installation Packages Editor). Потребуется определить имя пакета, например, рабочая станция. Установочный пакет создан.
- Теперь можно произвести принудительную установку: Нажмите кнопку **Установка...** (Install...) на вкладке **Удаленная установка** (Remote Install) и следуйте инструкциям, описанным в предыдущих главах. Важно выбрать пакет рабочей станции, как показано на рисунке ниже:



7.1.5 Удаленная установка на портативных компьютерах, не присутствующих в сети

Для портативных компьютеров, которые иногда находятся вне локальной сети, требуется другой тип удаленной установки. Для них предлагается применять метод с использованием сценария входа. Выполните следующие действия:

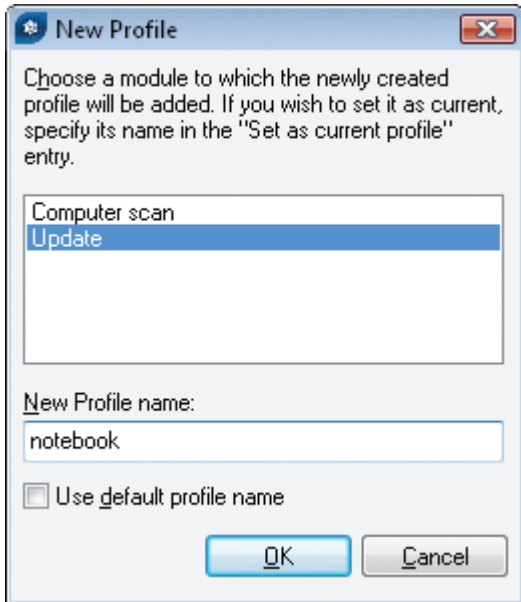
- откройте консоль ERA и подключитесь к серверу ERA (в данном случае GHOST). На вкладке **Удаленная установка** (Remote Install) нажмите кнопку **Пакеты...** (Packages...).
- из меню **Имя** (Name) выберите установочный пакет **Ноутбук** (Notebook).



Для того чтобы ноутбуки получали обновления с сервера зеркала «GHOST» (если они подключены к сети) и серверов обновлений ESET (если они находятся вне сети), выполните следующие действия:

- нажмите кнопку **Изменить** (Edit) для того чтобы изменить XML-файл, создание которого при помощи ERAC Editor описано в разделе 7.1.4.

- выберите команду **ESET Smart Security, ESET NOD32 Antivirus – Обновить – Профиль (Мой профиль)** (ESET Smart Security, ESET NOD32 Antivirus – Update – Profile (My profile)).
- щелкните правой кнопкой мыши **Профиль (Мой профиль)** (Profile (My profile)) и выберите в контекстном меню команду **Новый профиль...** (New Profile...).
- в диалоговом окне **Новый профиль** (New Profile) проверьте, что выделен раздел **Обновления** (Update), затем снимите флажок **Использовать имя профиля по умолчанию** (Use default profile name).
- введите **Новое имя профиля** (New Profile name), например, ноутбук (notebook).



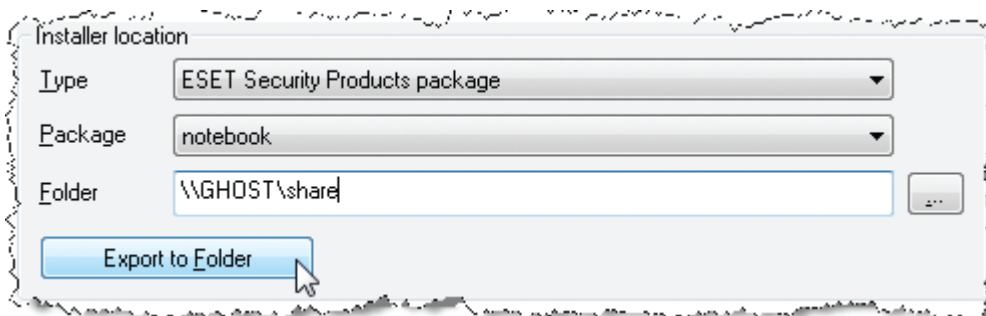
- нажмите кнопку **OK** (OK) для подтверждения. Теперь наряду с **Профиль (Мой профиль)** (Profile (My profile)) появляется **Профиль (ноутбук)** (Profile (notebook)). Выберите команду **Профиль (ноутбук) – Настройка** (Profile (notebook) – Setup) и настройте следующие три параметра, как показано на рисунке:



- параметр **Выбрать автоматически** (Choose Automatically) позволяет проводить обновление с серверов ESET, а не с локальной сети (зеркала), для проверки подлинности серверам передаются **Имя пользователя** (User name) и **Пароль** (Password), предоставленные фирмой ESET при приобретении.
- нажмите кнопку **Консоль** (Console) в правой части ESET Configuration Editor, чтобы вернуться в окно **Редактор установочных пакетов** (Installation Packages Editor).
- в окне **Редактор установочных пакетов** (Installation Packages Editor) нажмите кнопку **Да** (Yes), а затем **Сохранить как...** (Save as...) и сохраните измененный установочный пакет как ноутбуки (notebooks). Нажмите кнопку **Заккрыть** (Close) и вернитесь в консоль ERA.

Затем введите агент **installer.exe** в пакет для ноутбуков (notebooks) в сценарий входа. Далее выполните следующие действия:

- Во вкладке **Удаленная установка** (Remote Install) нажмите кнопку **Экспорт...** (Export...).
- В раскрывающемся меню **Пакет** (Package) щелкните значок ноутбуки (notebooks) и нажмите кнопку «...» чтобы выбрать папку, куда будет сохранен агент **installer.exe**. Данная папка должна быть доступна для всех ноутбуков, когда они подключены к сети компании (или домену). Для этих целей используется папка, определенная в пути **UNC: \\GHOST\share**



- Нажмите кнопку **Экспортировать в папку** (Export to Folder), а затем – **ОК** (OK). Теперь файл `installer.exe` находится в папке `\\GHOST\share`.

Если вы уже используете сценарий входа для других целей, ERAC может автоматически добавить строку в уже существующий сценарий. Благодаря этому портативные компьютеры смогут получать последние обновления вирусных сигнатур каждый раз при подключении к домену.

Для того чтобы добавить строку в уже существующий сценарий, выполните следующие действия:

- В правой части поля **Папка сценария** (Script Folder) нажмите кнопку ... и выберите ту папку, в которой хранится ваш сценарий.
- Во вкладке **Удаленная установка** (Remote Install) нажмите кнопку **Вход...** (Logon...). Введите **Имя пользователя** (User name), **Пароль** (Password) (и **Домен** (Domain)) Windows администратора, затем нажмите **ОК** (OK). С помощью этих данных происходит активации сценария входа.
- Теперь, каждый раз при подключении к домену, сценарий входа будет запускаться и загружать последние обновления вирусных сигнатур автоматически.

7.2 Компания с подразделением – 2х сервера ERA, 2х сервера зеркала

Необходимо использовать копию структуры предыдущей сети и добавить одно подразделение с несколькими клиентами и одним сервером, который называется LITTLE. Предположим, между основными офисами и подразделением существует канал виртуальной частной сети. В данном случае сервер зеркала необходимо установить на сервере LITTLE. Чтобы сделать среду более удобной и минимизировать объем передаваемых данных следует установить второй сервер ERA на LITTLE.

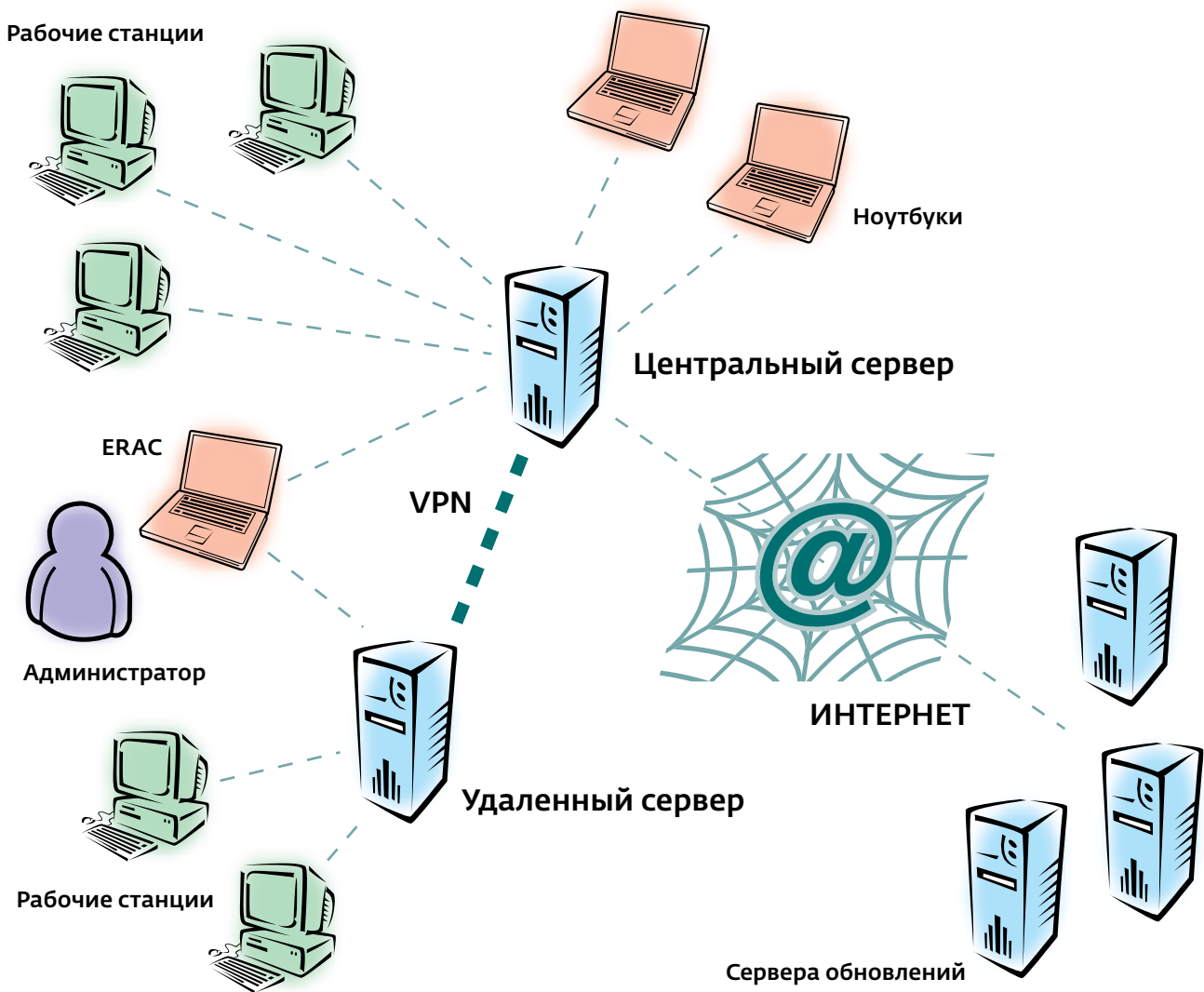
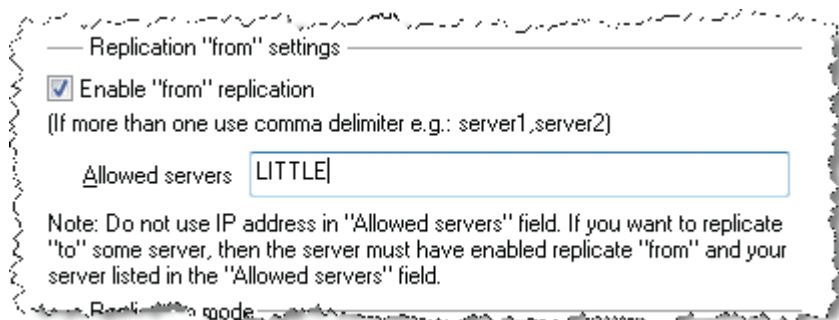


Рис. 14 Структура сети – компания с одним подразделением.

7.2.1 Установка в основных офисах

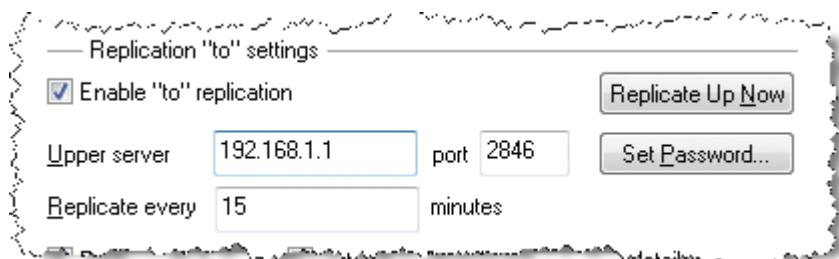
Установка сервера ERA, клиента ERA и клиентских рабочих станций будет проходить по сценарию, похожему на предыдущий. Единственное различие заключается в настройках главного сервера ERA (GHOST) – необходимо указать, что серверу LITTLE разрешается получать обновления с сервера GHOST.

Для этого откройте консоль ERA, подключенный к серверу GHOST. Выберите пункты меню **Инструменты – Опции сервера... – Репликация (Replication)**. Установите флажок **Включить репликацию «из»** (Enable "from" replication) и введите LITTLE в поле **Разрешенные серверы (Allowed servers)**.



7.2.2 Подразделение: установка сервера ERA

Как и в предыдущем примере, установите второй сервер ERA. Снова поставьте флажок и установите настройки репликации. Установите флажок **Включить репликацию «в»** (Инструменты – Опции сервера... – Репликация (Replication) и введите IP-адрес* главного сервера ERA в поле **Главный сервер (Upper server)**. В данном примере это IP-адрес сервера GHOST.



7.2.3 Подразделение: Установка HTTP-сервера зеркала

Как образец можно использовать пример установки сервера зеркала, описанный выше. Единственное различие заключается в определении следующих секций:

- Источник файлов обновлений
- Имя пользователя и Пароль

Как видно из рис. 14, обновления для подразделения загружаются не с сервера обновлений ESET, а с сервера основных офисов (GHOST). Источник обновлений определен следующим URL-адресом: <http://ghost:2221> (или http://IP_address_of_ghost:2221).

Указывать имя пользователя и пароль нет необходимости, потому что интегрированный HTTP веб-сервер не требует проверки подлинности.

7.2.4 Подразделение: Удаленная установка на клиенты

Напомним еще раз, что как образец можно использовать предыдущую модель, она подходит для проведения всех операций с клиентом ERA, подключенным напрямую к серверу ERA подразделения (LITTLE)**.

* Это позволяет предотвращать возможные проблемы с DNS-переводами во время преобразования имен в IP-адреса между сетями (в зависимости от настроек DNS).

** Благодаря этому установочные пакеты не передаются через канал виртуальной частной сети, который работает медленнее.

8.1 Экспорт и другие функции XML-конфигурации клиента

В консоле ERA выберите любой из клиентов во вкладке **Клиенты** (Clients). Щелкните правой кнопкой мыши и выберите команду **Конфигурация...** (Configuration...) в контекстном меню. Нажмите кнопку **Сохранить как...** (Save As...) и экспортируйте установленные настройки данного клиента в XML-папку*. В дальнейшем XML-файл может использоваться для выполнения различных операций:

- Для удаленных установок XML-файл может использоваться как шаблон для предопределенной конфигурации. Это означает, что не нужно создавать новый XML-файл – существующий XML-файл присваивается (**Выбрать...** (Select...)) новому установочному пакету.
- Для настройки множественных клиентов: выбранные клиенты получают загруженный ранее XML-файл и принимают определенные в нем настройки (новая конфигурация не создается, а присваивается после нажатия кнопки **Выбрать...** (Select...)).

Пример.

Решение ESET устанавливается только на одну рабочую станцию. Измените настройки непосредственно в программном интерфейсе. Закончив изменения, экспортируйте настройки в XML-файл. В дальнейшем этот XML-файл может использоваться для удаленных установок на другие рабочие станции. Этот способ можно использовать для таких задач, как уточнение правил работы файрвола, если применяется режим на основе политик.

8.2 Комбинированное обновление для портативных компьютеров и мобильных устройств

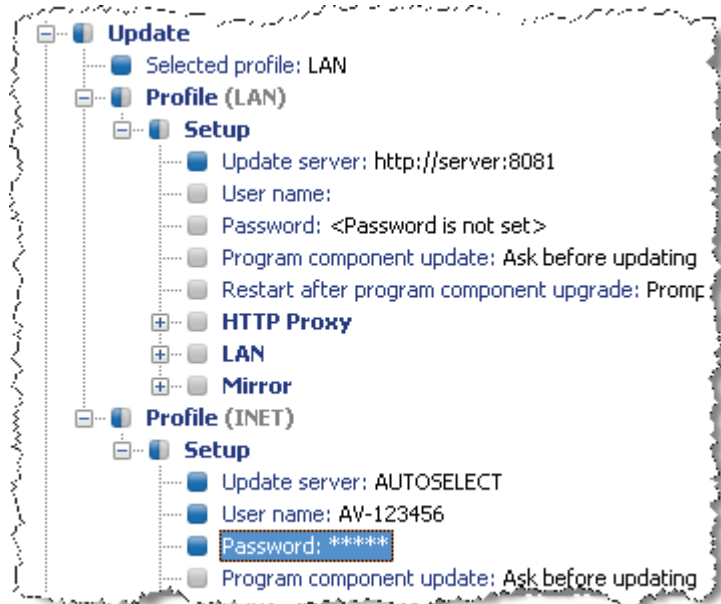
Если в локальной сети есть какие-либо мобильные устройства (например, ноутбуки), рекомендуется настроить комбинированное обновление из двух источников: серверов обновлений ESET и локального сервера обновлений – зеркала. Сначала ноутбуки устанавливают контакт с локальным сервером зеркала, в случае неудачи (когда ноутбуки находятся вне офиса), они загружают обновления непосредственно с серверов ESET. Для этого необходимо:

- Создать два профиля обновлений, один из которых направлен на сервер зеркала (в приведенном ниже примере такой профиль называется «LAN») и второй – на серверы обновлений ESET.
- Создать новую задачу обновления или изменить уже существующую в планировщике (**Инструменты – Планировщик** (Tools – Scheduler) в главном программном окне ESET Smart Security или ESET NOD32 Antivirus).

Эти настройки можно установить непосредственно на ноутбуках, или дистанционно – используя ESET Configuration Editor. Их можно применить во время установки, либо в любое другое время как задачу настроек.

Для того чтобы создать новый профиль в ESET Configuration Editor щелкните правой кнопкой мыши раздел Обновления (Update) и выберите команду Новый профиль (New profile) в контекстном меню.

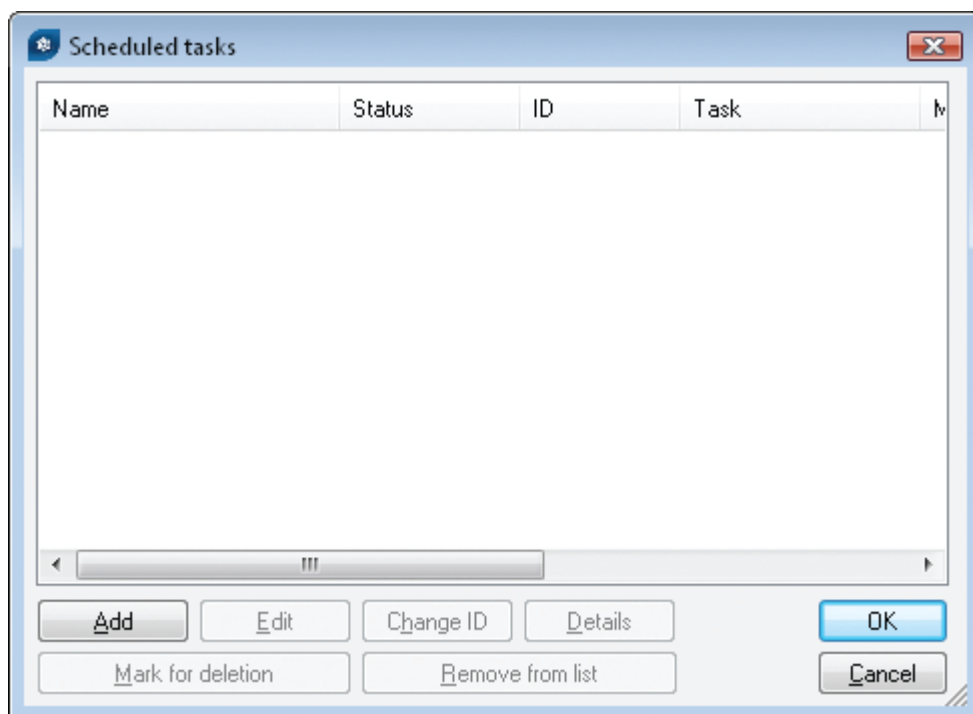
В результате изменений должно получиться примерно следующее



Профиль LAN (LAN) загружает обновления с локального сервера зеркала компании (<http://server:8081>), в то время как INET (INET) подключается к серверам ESET (**Выбрать автоматически** (Choose Automatically)).

Затем определите задачу обновления, которая последовательно запускает каждый профиль обновления. Для этого выберите пункты меню **ESET Smart Security, ESET NOD32 Antivirus – Ядро – Настройка – Планировщик** (ESET Smart Security, ESET NOD32 Antivirus – Kernel – Setup – Scheduler/Planner) или **NOD32 версия 2 – Общие сведения – Настройка – Планировщик** (NOD32 version 2 – General – Setup – Scheduler/Planner). Нажмите кнопку **Изменить** (Edit) для того чтобы вывести окно **Запланированные задачи** (Scheduled tasks).

* XML-файлы конфигурации также могут быть извлечены непосредственно из программного интерфейса ESET Smart Security.



- Для создания новой задачи нажмите кнопку **Добавить** (Add). В раскрывающемся меню **Запланированная задача** (Scheduled task) выберите команду **Обновление** (Update) и нажмите кнопку **Далее** (Next).
- Введите **Имя задачи** (Task name) (например, комбинированное обновление), выберите команду **Периодически** (Repeatedly) и нажмите кнопку **Далее** (Next).
- Установите **Интервал между выполнением задач** (Interval between task execution) на 60. **Дважды** нажмите кнопку **Далее** (Next) чтобы принять значения по умолчанию и нажмите кнопку **Готово** (Finish).
- Для этой задачи выберите **Основной** (Primary) и **Вспомогательный** (Secondary) профиль обновления (LAN, INET – или наоборот).
- Если рабочие станции ноутбука сначала соединяются с сервером зеркала, то **Основной профиль** (Primary profile) следует установить на LAN, а Вспомогательный профиль – на INET. Профиль INET будет применяться только в том случае, если не удастся получить обновления с LAN.

РЕКОМЕНДАЦИИ. Экпортируйте текущую XML-конфигурацию из клиента (более подробную информацию см. в главе 8.1) и произведите описанные выше изменения экспортированного XML-файла. Таким образом, избегается разрастание числа конфигураций между планировщиком и нерабочими профилями.

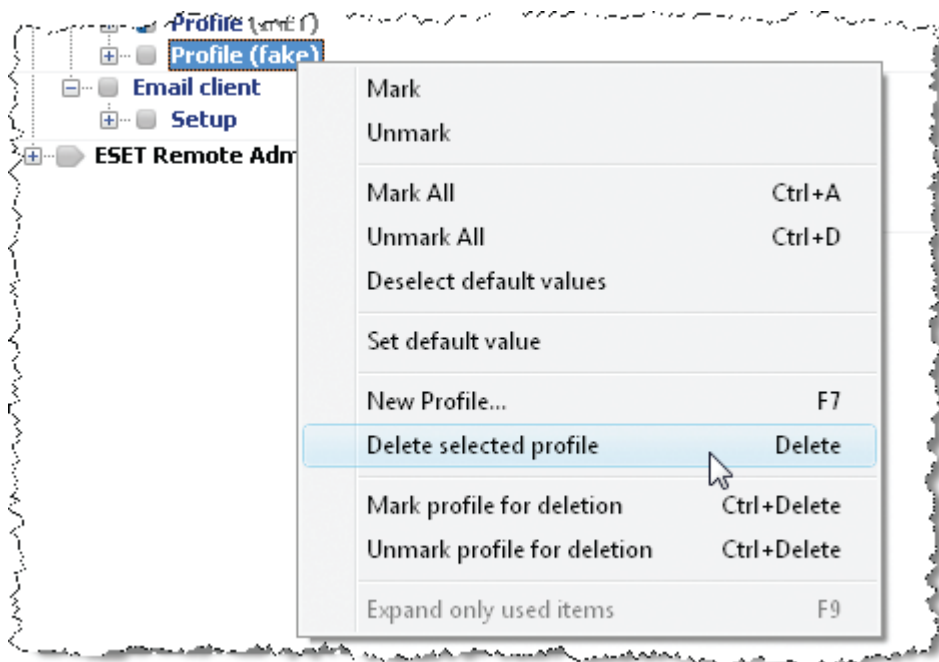
8.3 Удаление существующих профилей

Если на рабочей станции клиента по ошибке были созданы неиспользуемые или повторные профили, их можно удалить дистанционно.

Чтобы удалить нежелательный профиль, выполните следующие действия:

- В консоле ERA выберите вкладку **Клиенты** (Clients) и щелкните дважды по проблемному клиенту.
- В окне **Свойства клиента** (Client Properties) выберите вкладку **Настройки** (Configuration).
- Выберите опции **Запустить ESET Configuration Editor для изменения файла** (Then Run ESET Configuration Editor to edit the file) и **Использовать загруженные настройки в новой задаче конфигурации** (Use the downloaded configuration in the new configuration task), затем нажмите кнопку **Новая Задача** (New Task).
- В мастере задачи щелкните значок **Изменить** (Edit) чтобы открыть редактор настроек. Нажмите **CTRL+D** чтобы снять выделение со всех настроек (пометить серым). Это поможет предотвратить случайные изменения, так как все новые изменения будут выделяться голубым.
- Щелкните правой кнопкой мыши профиль, который необходимо удалить, и выберите команду **Отметить профиль для удаления** (Mark profile for deletion) в контекстном меню.
- В редакторе настроек выберите команды **Файл – Сохранить** (File – Save).
- Убедитесь, что выбранный вами клиент находится в колонке **Выбранные** (Selected items) справа. Нажмите кнопку **Далее** (Next), а затем – **Готово** (Finish).

Нежелательный профиль будет удален с выбранной рабочей станции.



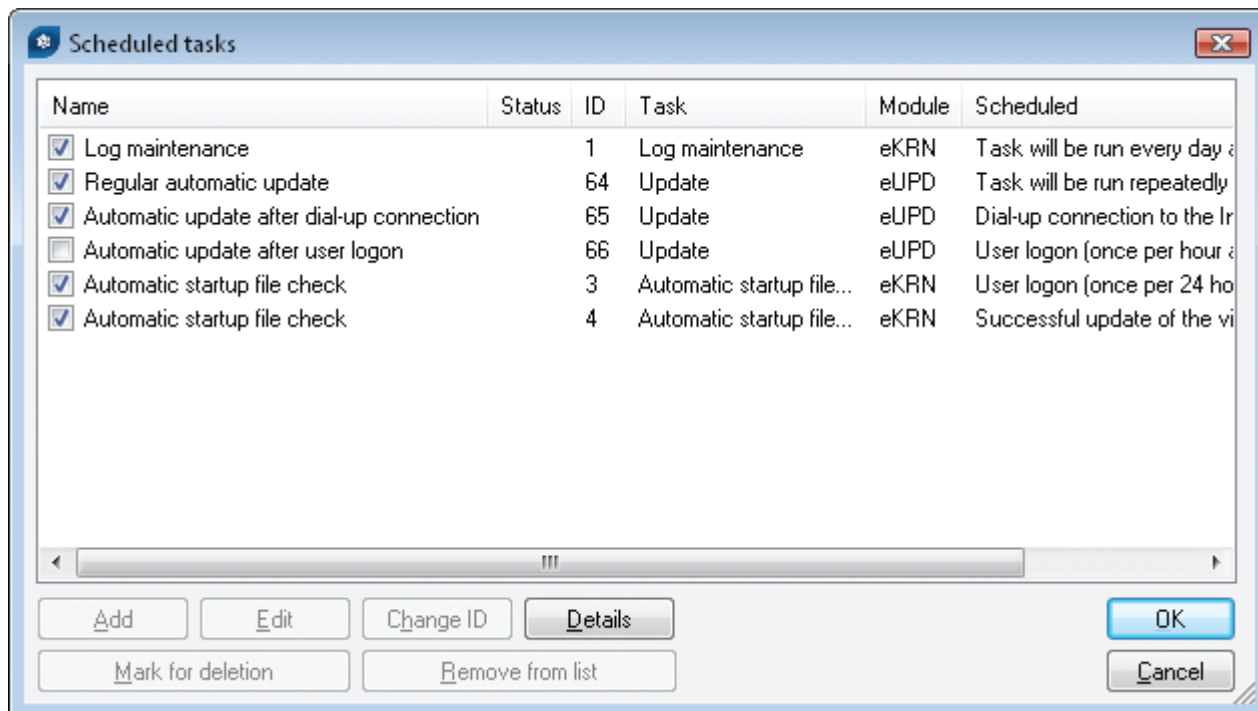
- Далее нажмите кнопку консоль в настройках расширенного режима чтобы сохранить изменения.
- Затем выберите целевых клиентов, которые примут изменения, определенные в настройках расширенного режима, и выйдите из мастера.

8.4 Настройка планировщика

Для дистанционного изменения задач планировщика, выберите пункты меню **Eset Smart Security – Ядро – Настройки – Планировщик** (Eset Smart Security / Kernel / Settings / Scheduler) или **NOD32 версия 2 – Общие сведения – Настройки – Планировщик** (NOD32 version 2 / General / Settings / Scheduler/Planner) в расширенном режиме ESET Configuration и нажмите кнопку **Изменить** (Edit).

Если вы хотите добавить новые задачи, то можно использовать абсолютно новые (пустые) XML-настройки. Если вы хотите изменить или удалить существующие задачи, необходимо:

- использовать либо XML-настройки, экспортированные из данного клиента,
- либо идентификаторы задач, которые необходимо изменить/удалить.



Каждой задаче присваивается идентификационный номер (так называемый первичный ключ), все задачи по умолчанию имеют десятичные идентификационные номера (1, 2, 3...). Что касается пользовательских задач, то им присваиваются шестнадцатеричные ключи (например, 4AE13D6C), сформированные в виде случайного числа при создании новой задачи.

Флажки определяют активность соответствующих задач – это означает, что задача будет выполнена на данном клиенте.

Функциональность кнопок диалогового окна:

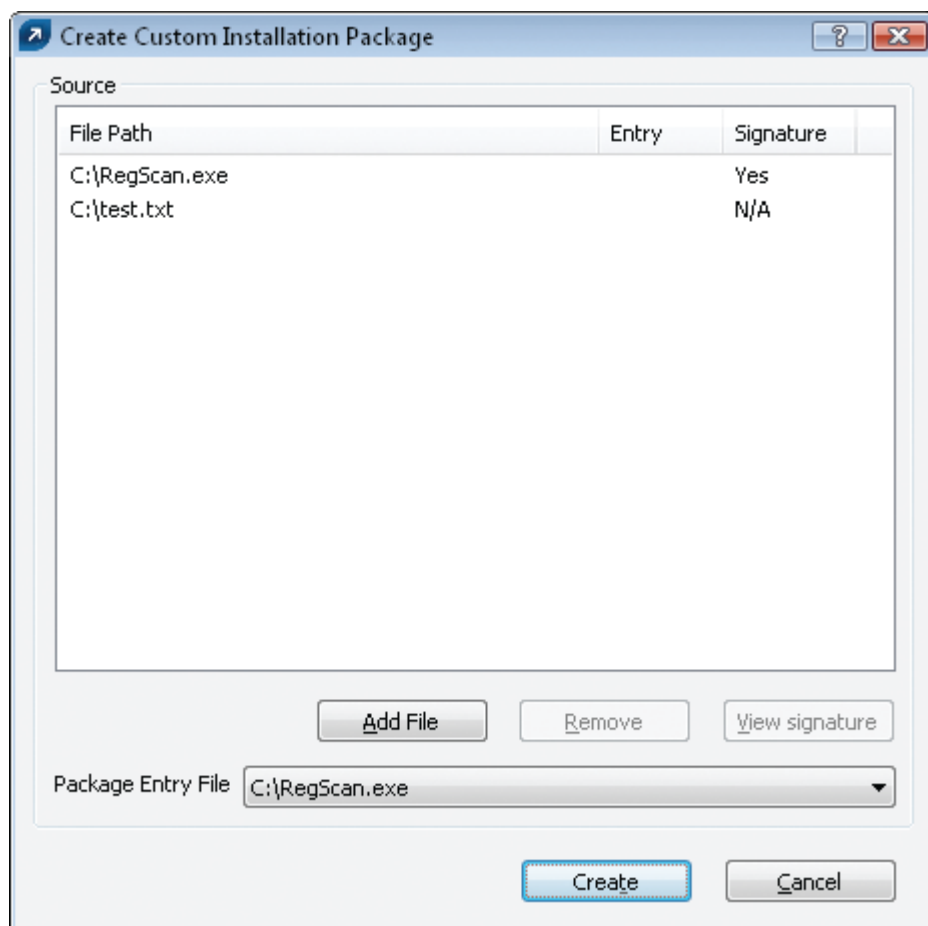
- **Добавить** – добавляет новые задачи.
- **Изменить** – изменяет выбранные задачи.
- **Изменить идентификационный номер** – изменяет идентификационный номер выбранных задач.
- **Сведения** – краткое описание выбранной задачи.
- **Выделить для удаления** – приложение XML-файла удалит задачи, выделенные щелчком мыши, из целевых клиентов.
- **Удалить из списка** – удаляет выбранные задачи из списка. Обратите внимание, что задачи, удаленные из списка в XML-настройках, не будут удалены с целевых рабочих станций.

Поскольку значения идентификационных номеров формируются в виде случайного числа (при определении новых задач), могут возникнуть осложнения, если администратор будет применять один и тот же тип задач повторно. Пример: в сети 40 компьютеров. Администратор добавляет новую задачу под именем ABC, которой присваивается идентификационный номер 4A2B8CA5. Компания приобретает 10 новых компьютеров, и администратор снова добавляет задачу ABC с идентификационным номером, допустим, 8D5A6D1B. Когда необходимо изменить задачу, администратор экспортирует XML-настройки из одного из 40 первоначальных компьютеров, изменяет их и применяет как задачу настроек на всех 50 рабочих станциях. Вот тогда и возникает проблема. Один и тот же тип задачи имеет два разных идентификационных номера (4A2B8CA5, 8D5A6D1B), поэтому на первых 40 компьютерах изменения будут проведены правильно, а вот на 10 новых компьютерах будет создана новая идентичная задача (у задачи ABC изначально был идентификационный номер 8D5A6D1B, но задача XML-настроек изменила задачу ABC с номером 4A2B8CA5). Чтобы предотвратить это, нажмите кнопку Изменить идентификационный номер (Change ID) и установите общий идентификационный номер для всех задач одного типа.

8.5 Пользовательские установочные пакеты

Расширенный режим установочных пакетов позволяет создавать пользовательский пакет. В пользовательский пакет можно включить любой файл при помощи кнопки **Добавить файл** (Add File), но один из них должен быть главным установочным файлом (**Регистрационный файл пакета** (Package entry file)).

Процесс распределения по удаленным клиентам схож с удаленной установкой любой клиентской программы ESET. Пакет автоматически извлекается на целевом компьютере и запускается регистрационный файл пакета.



Этот тип пакета может использоваться для деинсталляции любого программного обеспечения систем безопасности других поставщиков.