

Особенности развертывания и эксплуатации Dr.Web Enterprise Security Suite на географически распределенных объектах с плоскими каналами связи



Особенности развертывания и эксплуатации **Dr.Web Enterprise Security Suite** на географически распределенных объектах с плохими каналами связи

Dr.Web Enterprise Security Suite имеет весь необходимый функционал для надежной защиты географически удаленных объектов с плохими каналами связи.

Несмотря на то, что географически распределенные сети могут иметь разную архитектуру и эксплуатироваться в разных условиях, представленные ниже общие рекомендации подойдут для большинства применений.

1. Постройте распределенную иерархическую сеть из нескольких антивирусных серверов

Это позволит:

- Получать обновления из Всемирной сети обновления (BCO) Dr.Web через один главный антивирусный сервер Dr.Web с последующей трансляцией их на подчиненные антивирусные серверы напрямую или через промежуточные звенья.
- Распределить рабочие станции по нескольким антивирусным серверам с уменьшением нагрузки на каждый из них.
- Получать консолидированную статистику с нескольких серверов на главном антивирусном сервере в Центре управления.
- Передавать свободные лицензии для защиты станций на соседние антивирусные серверы. При этом лицензионный ключ остается в распоряжении антивирусного сервера, который его раздает, а свободные лицензии выдаются соседнему серверу на определенный промежуток времени, по истечении которого отзываются обратно.

Dr.Web Enterprise Security Suite позволяет построить иерархическую сеть из нескольких антивирусных серверов разного типа связей: главный — *подчиненный* и *равноправный*.

В случае географически распределенной сети рекомендуем установить главный антивирусный сервер на основной серверной площадке, а подчиненные — на удаленных узлах.

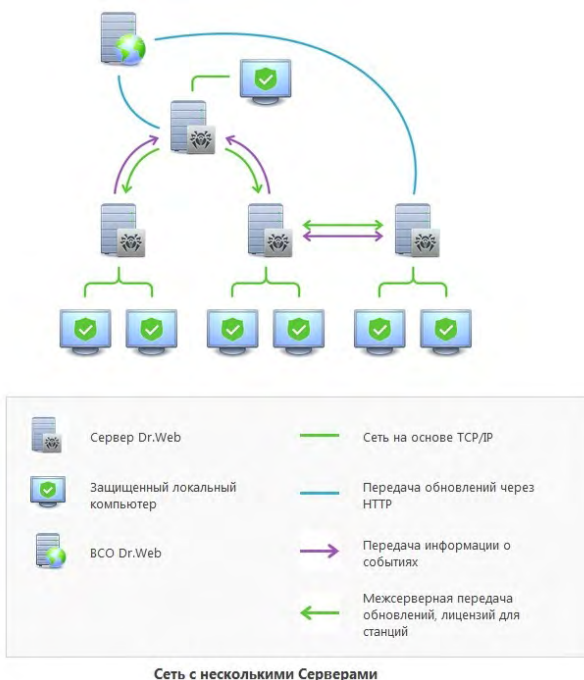
Разверните главный антивирусный сервер на своей основной серверной площадке и защитите объекты, с которыми имеются хорошие каналы связи.

Разверните подчиненные антивирусные серверы на своих удаленных площадках.

Разверните антивирусную сеть, установив антивирусные агенты на защищаемые объекты, имеющие хорошие каналы связи с местной площадкой.

Настройте межсерверную связь между главным и подчиненными антивирусными серверами в соответствии с п. 8.11.2 документа **Dr.Web Enterprise Security Suite**.

Руководство администратора и убедитесь в надежности канала между ними.



При данном типе связи главный антивирусный сервер получает обновления компонентов антивирусных агентов и вирусных баз с BCO, затем передает их на подчиненные серверы, которые, в свою очередь, обновляют антивирусные агенты, подключенные к ним.

Внимание! Подчиненные серверы не принимают обновления с BCO, даже при наличии такого задания в расписании.

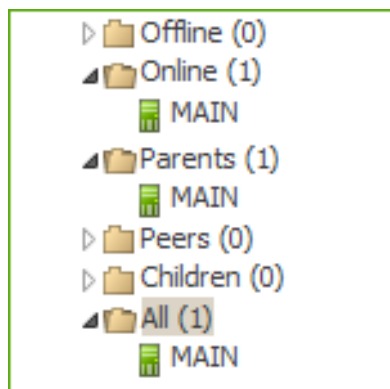
Однако на тот случай, если главный сервер будет временно недоступен, рекомендуется оставить в расписании подчиненных серверов задание на обновление их с BCO. Это позволит антивирусным агентам, подключенным к подчиненному серверу, получать обновление вирусных баз и программных модулей при техническом сбое.

Dr.Web Enterprise Security Suite автоматически отслеживает ситуации, когда из-за несовершенного планирования топологии сети и настройки антивирусных серверов на один и тот же сервер повторно поступает уже принятое из другого источника обновление. В этом случае обновление не будет принято повторно.

Связь между антивирусными серверами позволяет передавать информацию о вирусных событиях и статистику работы, а также передавать свободные лицензии между ними.

Для просмотра информации о вирусных событиях на подчиненных серверах, зайдите в Центр управления главного антивирусного сервера.

В дереве **Антивирусной сети**, в группе **Neighbors** выберите сервер, информацию о котором хотите просмотреть.



Далее в разделе управляющего меню **Таблицы** выберите пункт **Суммарный отчет**. Подробнее о работе сети с несколькими серверами см. в п. 8.11 документа **Dr.Web Enterprise Security Suite. Руководство администратора**.

1.1. Соединение главного и подчиненного ES-серверов

Чтобы настроить связь между двумя Серверами Dr.Web, один из которых будет выбран в качестве главного, а второй — подчиненного, необходимо выполнить следующие действия:

- 1) Убедитесь, что оба Сервера Dr.Web запущены и нормально функционируют.
- 2) Включите на обоих серверах сетевой протокол, по которому будет осуществляться связь. Для этого в пункте **Администрирование** → **Конфигурация** → **Конфигурация Сервера Dr.Web** перейдите на вкладку **Модули** и отметьте флажком пункт **Протокол Сервера Dr.Web**. Нажмите **Сохранить**.

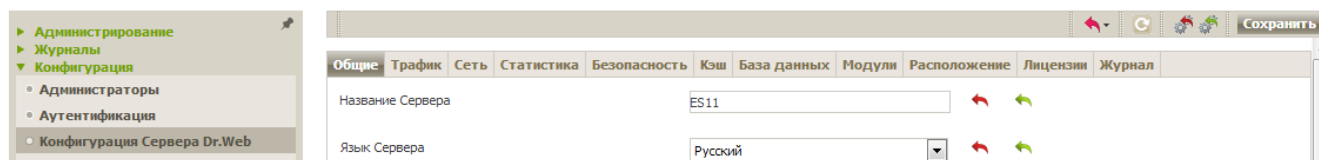
Если серверный протокол не включен, при создании новой связи в Центре управления будет выведено сообщение о необходимости включения данного протокола и дана ссылка на соответствующий раздел настроек.



Администрирование > Конфигурация Сервера Dr.Web ☆



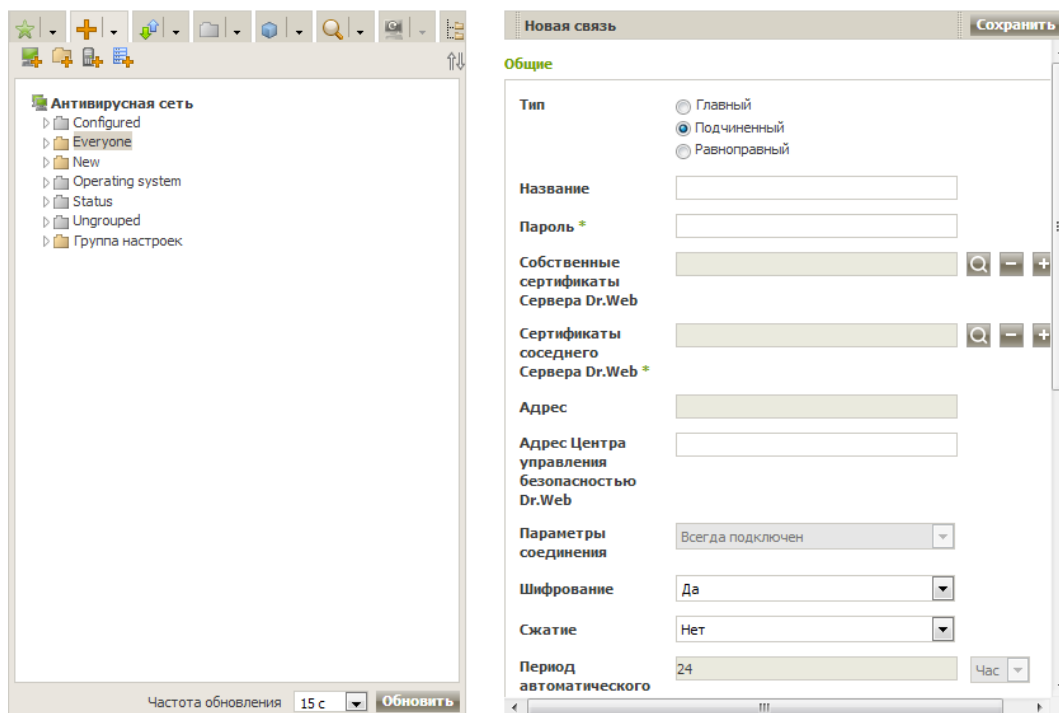
- 3) Убедитесь, что соединяемым серверам даны «говорящие» имена, по которым вам будет удобно их идентифицировать, например MAIN для главного и AUXILIARY для подчиненного. Чтобы дать серверу имя, в пункте **Администрирование** → **Конфигурация** → **Конфигурация Сервера Dr.Web** перейдите на вкладку **Общие** и заполните поле **Название Сервера**. Нажмите **Сохранить**.



Администрирование > Конфигурация Сервера Dr.Web ☆

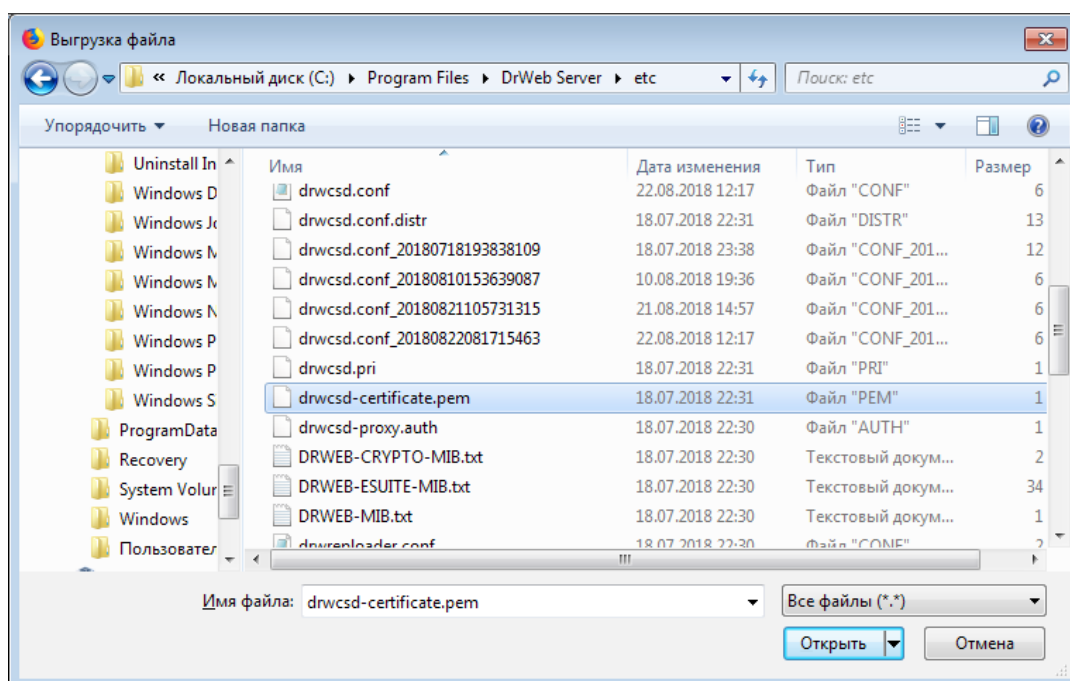




- 4) Перезапустите оба сервера, чтобы применить внесенные изменения, используя значок .
- 5) Через Центр управления подчиненного Сервера (AUXILIARY) добавьте главный Сервер (MAIN) в список соседних Серверов. Для этого выберите пункт **Антивирусная сеть** в главном меню. Откроется окно, содержащее иерархический список антивирусной сети. Чтобы добавить соседний Сервер, на панели инструментов выберите **+ Добавить объект сети** →  **Создать связь**.

Откроется окно настройки связи между текущим и добавляемым Сервером. Задайте следующие параметры:



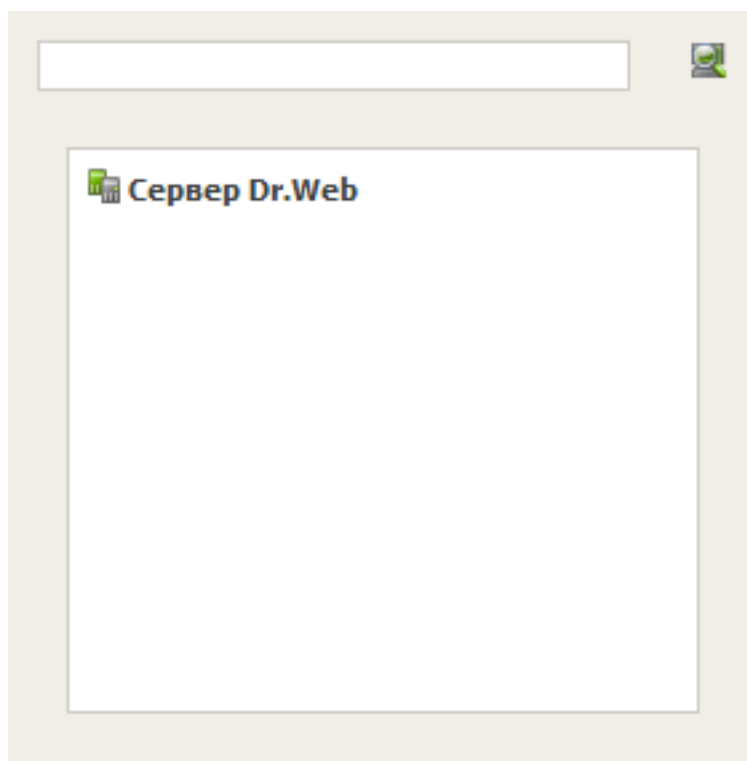
- **Тип** создаваемой связи — **Главный**.
- **Название** — название главного Сервера (MAIN).
- **Пароль** — произвольный пароль для доступа к главному Серверу.
- **Собственные сертификаты Сервера Dr.Web** — список SSL-сертификатов настраиваемого Сервера. Нажмите кнопку  и выберите файл сертификата drwcsd-certificate.pem, относящийся к текущему Серверу. Для добавления еще одного сертификата нажмите  и добавьте сертификат в новое поле.




- **Сертификаты соседнего Сервера Dr.Web** — список SSL-сертификатов подключаемого главного Сервера. Нажмите кнопку  и выберите файл сертификата drwcsd-certificate.pem, относящийся к главному Серверу. Для добавления еще одного сертификата нажмите  и добавьте сертификат в новое поле.
- **Адрес** — сетевой адрес главного Сервера и порт для подключения. Задается в формате <адрес_Сервера>:<порт>.

Возможен поиск списка Серверов, доступных в сети. Для этого:

1) Нажмите стрелку справа от поля **Адрес**.

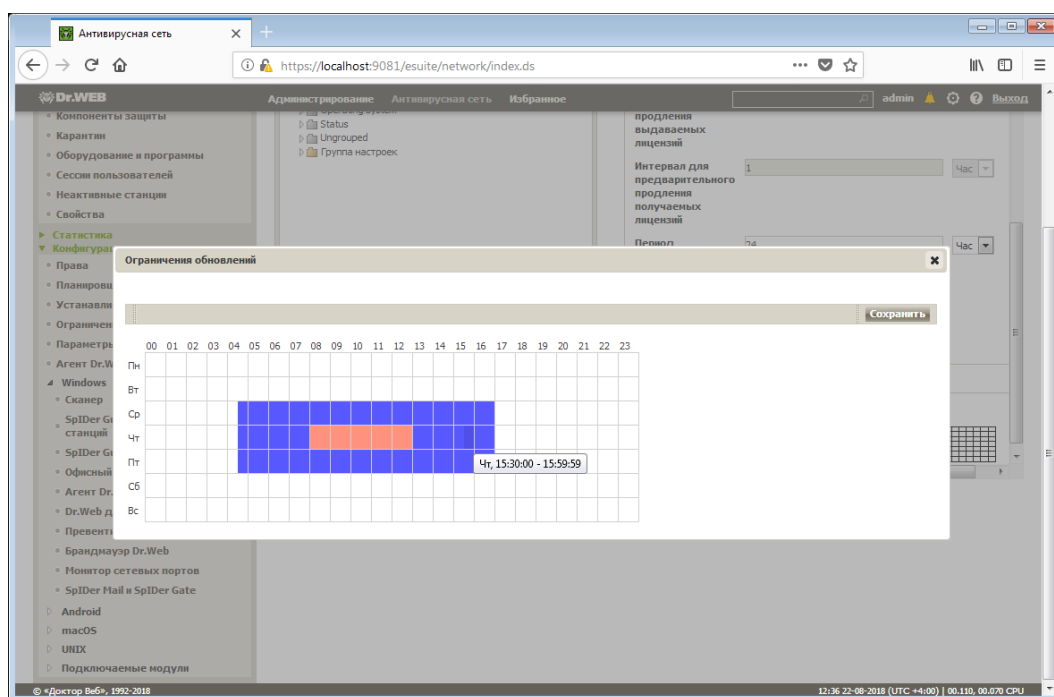


- 2) В открывшемся окне укажите перечень сетей в формате: через дефис (например, 10.4.0.1-10.4.0.10), через запятую и пробел (например, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90), с использованием префикса сети (например, 10.4.0.0/24).
- 3) Нажмите кнопку . Начнется обзор сети на наличие доступных Серверов.
- 4) Выберите Сервер в списке доступных Серверов. Его адрес будет записан в поле **Адрес** для создания связи.

Примечание. При создании равноправной связи между Серверами рекомендуется указывать адрес подключаемого Сервера в настройках только одного из них. Это не повлияет на взаимодействие между Серверами, однако позволит избежать записей типа Link with the same key id is already activated в журнале работы Серверов.

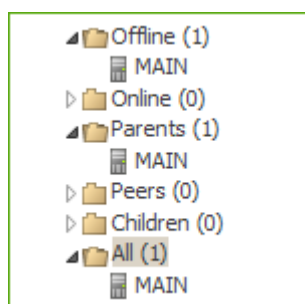
- **Адрес Центра управления безопасностью Dr.Web** — укажите адрес начальной страницы Центра управления главного Сервера (см. п. [Центр управления безопасностью Dr.Web](#)).
- В выпадающем списке **Параметры соединения** задайте принцип соединения Серверов создаваемой связи.
- В выпадающих списках **Шифрование** и **Сжатие** задайте параметры шифрования и сжатия трафика между соединяемыми Серверами (см. п. [Использование шифрования и сжатия трафика](#)).

- **Срок действия выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на главном Сервере. Настройка используется, если главный Сервер будет выдавать лицензии текущему Серверу.
- **Период для продления получаемых лицензий** — настройка не используется при создании связи до главного Сервера.
- **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами.
- Флаги в разделах **Лицензии**, **Обновления** и **События** установлены в соответствии с принципом связи *главный — подчиненный* и не подлежат изменению:
 - главный Сервер отправляет лицензии на подчиненный Сервер;
 - главный Сервер отправляет обновления на подчиненный Сервер;
 - главный Сервер принимает информацию о событиях от подчиненного Сервера.
- В разделе **Ограничения обновлений** → **События** при необходимости задайте расписание передачи событий от текущего Сервера главному (редактирование таблицы **Ограничения обновлений** осуществляется аналогично редактированию таблицы расписания в разделе [Ограничение обновлений рабочих станций](#)).

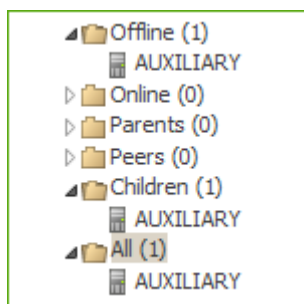


Нажмите кнопку **Сохранить**.

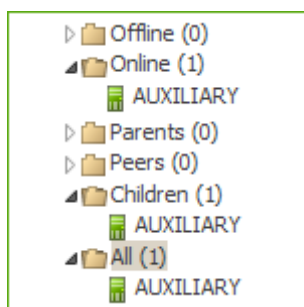
В результате главный Сервер попадет в папки **Parents** и **Offline**.



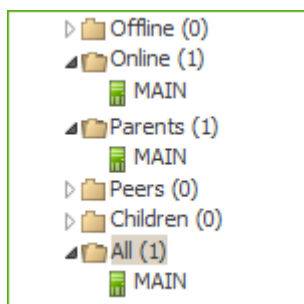
Аналогично добавьте подчиненный сервер в список соседних серверов главного сервера через его Центр управления. Не заполняйте поле **Адрес**. Укажите тот же пароль, что и в первом случае, ключ drwcsd.pub должен относиться к подчиненному серверу. В результате подчиненный сервер будет включен в папки **Children** и **Offline**.



Дождитесь установления соединения между Серверами (обычно это занимает не более минуты). Для проверки периодически обновляйте список Серверов с помощью клавиши F5. После установления связи подчиненный Сервер (AUXILIARY) перейдет из папки **Offline** в папку **Online**.

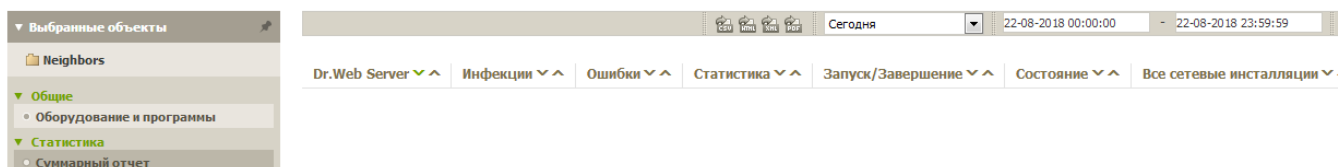


Откройте Центр управления подчиненного Сервера (AUXILIARY) и убедитесь в том, что главный Сервер (MAIN) подключен к подчиненному (AUXILIARY).



Просмотреть информацию о работе других серверов можно, используя пункт **Статистика** → **Суммарный отчёт** для группы **Neighbors** меню **Антивирусная сеть**. Выведенная таблица содержит сведения об обнаруженных инфекциях, ошибках сканирования, сетевых инсталляциях, запуске и завершении заданий, статистику.

Антивирусная сеть > Суммарный отчет ☆



Установка соединения между Серверами **Dr.Web Enterprise Server** невозможна в следующих случаях:

- Проблемы связи по сети.
- При настройке связи задан неверный адрес главного Сервера.
- Заданы неверные открытые сертификаты на одном из Серверов.
- Задан неверный пароль доступа на одном из Серверов (заданы несовпадающие пароли на соединяемых Серверах).

Если необходимо установить новую межсерверную связь между Серверами версий 10 и 11, дополнительно выполните следующие действия.

1. При создании связи укажите открытый ключ Сервера версии 11 на Сервере версии 10.
2. Сгенерируйте сертификат из закрытого ключа Сервера версии 10 при помощи утилиты drwsign (команда gencert) из состава Сервера версии 11 (см. документ **Приложения**, п. [Н9.1. Утилита генерации цифровых ключей и сертификатов](#)). Укажите этот сертификат при создании связи на Сервере версии 11.

2. Настройте расписание и параметры обновлений на антивирусных серверах

Получение обновлений антивирусными серверами и скачивание дистрибутивов агентов может производиться во время минимальной нагрузки на сети передачи данных. При необходимости можно также ограничить используемую при этом ширину канала. Для ограничения общей скорости передачи обновлений для всех станций настройка ограничений осуществляется с помощью параметра **Ограничить трафик обновлений**, вкладки **Трафик** → **Обновления** раздела **Администрирование** → **Конфигурация** → **Конфигурация** → **Сервера Dr.Web**.

Перейдите в раздел **Администрирование**, выберите **Конфигурация Сервера Dr.Web** и установите необходимые ограничения.

The screenshot shows the 'Администрирование > Конфигурация Сервера Dr.Web' interface. The left sidebar contains a tree view with categories: 'Администрирование', 'Журналы', 'Конфигурация', 'Оповещения', and 'Репозиторий'. The main content area is titled 'Обновления' and includes a 'Трафик' tab. Under 'Обновления', there are settings for 'Количество одновременных процессов обновления' (set to 0) and 'Ограничить трафик обновлений' (checked). Below this, 'Максимальная скорость передачи (КБ/с)' is set to 1024. A calendar grid shows a blue shaded area from Monday 08 to Friday 22. A legend at the bottom indicates: 'Без ограничений' (white), 'Скорость ограничена до 1024 КБ/с' (blue), and 'Передача данных запрещена' (red).

3. Используйте полный инсталлятор антивирусного агента и режим новичков

В случае нестабильных и узких каналов связи между антивирусным сервером и защищаемым объектом рекомендуем использовать для установки полный инсталлятор антивирусного агента. Такой дистрибутив содержит все компоненты агента без необходимости их скачивания с антивирусного сервера при запуске персонального инсталлятора.

Скачайте полный инсталляционный пакет *drweb- <сборка >-esuite-agent-full-windows.exe*, входящий в комплект поставки Dr.Web Enterprise Security Suite, с Мастера загрузки на сайте www.drweb.ru.

Запустите его установку и введите настройки для подключения к ближайшему антивирусному серверу, а также публичный (открытый) ключ шифрования (*drwcsd.pub*).

Если установленный с помощью полного инсталляционного пакета агент имеет неактуальную версию компонентов, то после первого подключения агента к серверу произойдет их обновление.

Подробнее об особенностях установки агентов с использованием полного инсталлятора см. в документе **Агент Dr.Web для Windows. Руководство пользователя**.

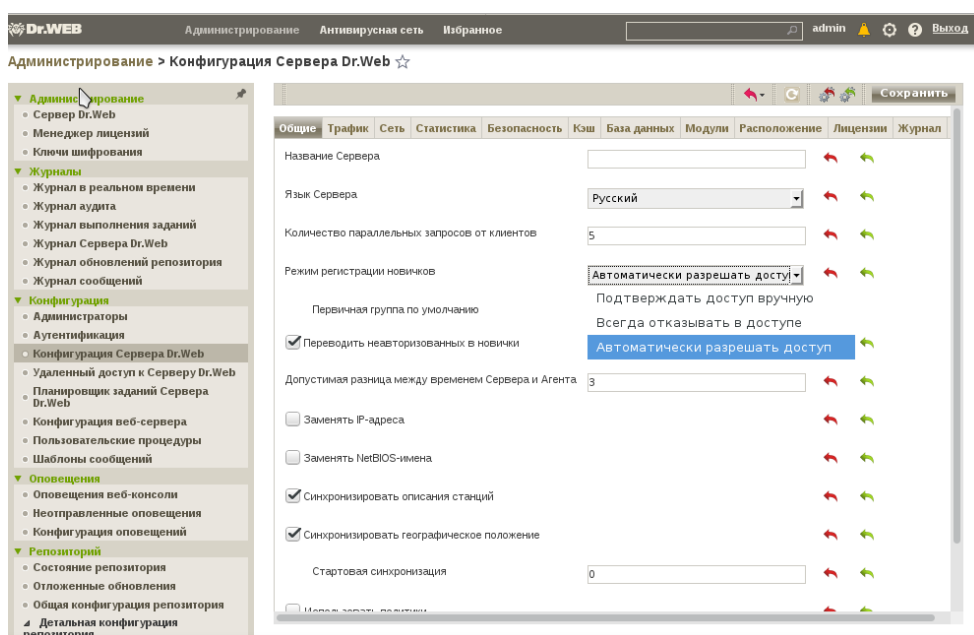
Рекомендуем также использовать режим новичков для подключения антивирусных агентов к серверу, т. е. без необходимости предварительного создания станций в антивирусной сети. Авторизация таких агентов может происходить на сервере в автоматическом или ручном режиме.

При ручном подтверждении доступа новые станции помещаются в подгруппу *Newbies* до их непосредственного рассмотрения системным администратором, имеющим соответствующие права.

При автоматическом подтверждении все новые станции помещаются в первичную группу, заданную в разделе **Конфигурация Сервера Dr.Web** на вкладке **Общие**.

Настройка режима доступа новичков производится в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → **Общие** → **Режим регистрации новичков**.

Установите галочку напротив пункта **Переводить неавторизованных в новички**.



Нажмите кнопку **Сохранить** для применения настроек и перезагрузите сервер.

4. Используйте прокси-сервер внутри локальной сети организации

Основная задача прокси-сервера — обеспечение связи Сервера Dr.Web и Агентов Dr.Web в случае невозможности организации прямого доступа (например, если Сервер Dr.Web и Агенты Dr.Web расположены в различных сетях, между которыми отсутствует маршрутизация пакетов).

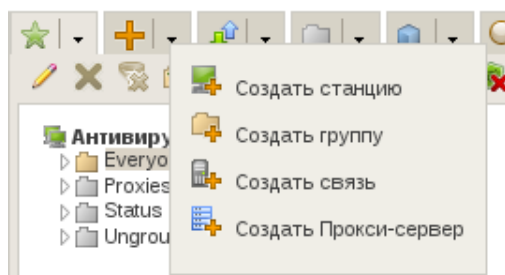
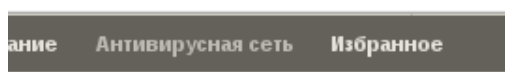
Внимание! Для установки соединения между Сервером и клиентами через прокси-сервер рекомендуется отключить шифрование трафика. Для этого установите значение нет для параметра **Шифрование** в разделе [Конфигурация Сервера Dr.Web](#) → [Общие](#).

В целях экономии трафика рекомендуется установить прокси-сервер на один из защищаемых объектов внутри локальной сети.

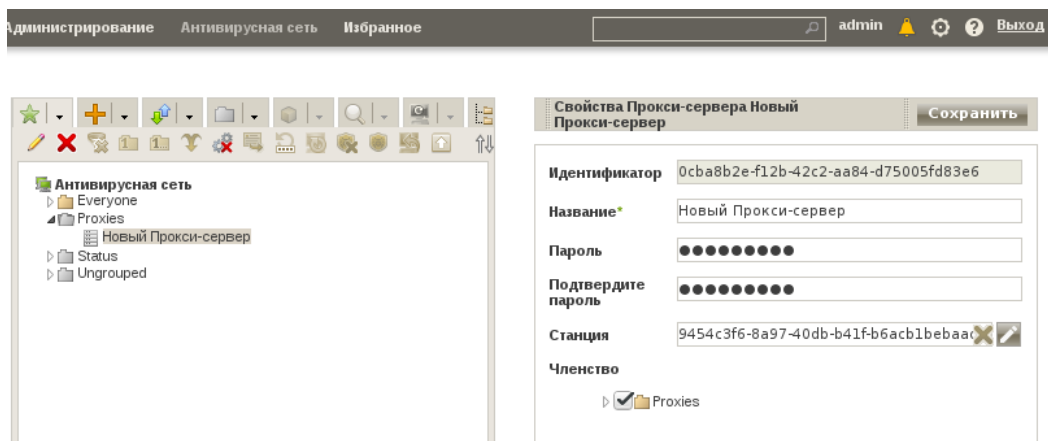
Прокси-сервер поддерживает функции сжатия и кеширования трафика (баз/компонентов) с последующей раздачей внутри локальной сети.



Для установки прокси-сервера нажмите кнопку **Добавьте объект сети** и выберите **Создать Прокси сервер**.



Выберите защищаемый объект (станцию), на который будет установлен прокси-сервер. Все установленные прокси-серверы будут помещены в группу **Proxies**.

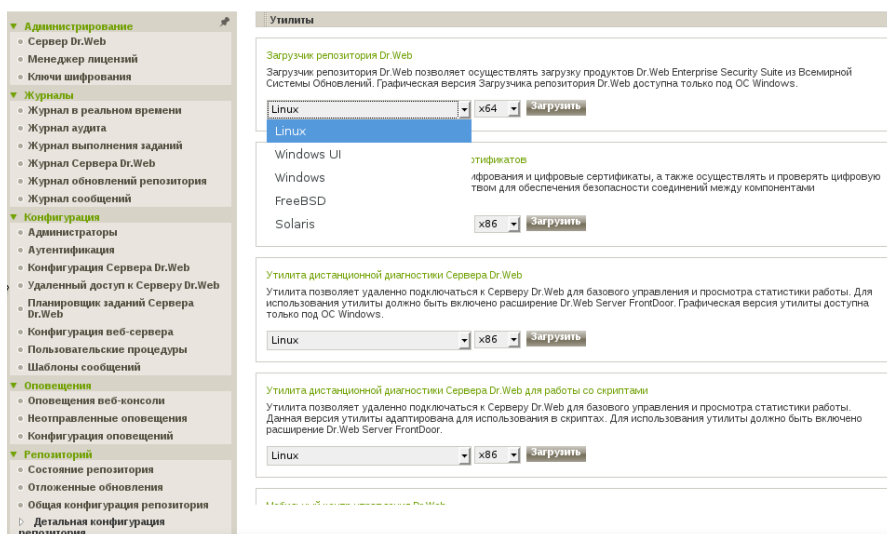


Настройте антивирусные агенты для получения обновлений с прокси-сервера в локальной сети.

Подробнее об использовании и настройке прокси-сервера см. в п. 10.1 документа **Dr.Web Enterprise Security Suite. Руководство администратора.**

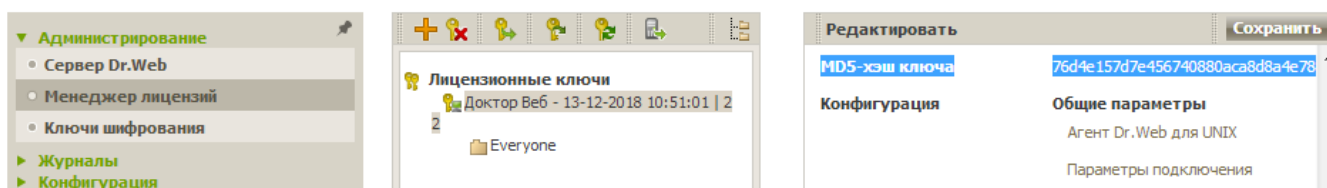
5. Используйте утилиту Загрузчик репозитория Dr.Web

В случае невозможности подключения антивирусных серверов к Интернету предусмотрено скачивание репозитория с BCO с последующим обновлением сервера.



Для использования данной утилиты необходим лицензионный ключ **Dr.Web Enterprise Security Suite** либо его MD5-хэш, который доступен для просмотра в **Центре управления**, в разделе **Администрирование** → **Менеджер лицензий**.

Администрирование > Менеджер лицензий ☆



Скачайте утилиту **Загрузчик репозитория Dr.Web** при помощи Центра управления, в разделе **Администрирование** → **Дополнительные возможности** → **Утилиты**.

Укажите тип и разрядность ОС, с которой будет запускаться эта утилита, после чего нажмите **Загрузить**. Обратите внимание, что графическая версия утилиты доступна только для Windows (вариант **Windows UI**), для других ОС существует только консольная утилита. По умолчанию скачивается консольная версия для Windows.

Администрирование > Утилиты ☆

Утилиты

Загрузчик репозитория Dr.Web
Загрузчик репозитория Dr.Web позволяет осуществлять загрузку продуктов Dr.Web Enterprise Security Suite из Всемирной Системы Обновлений. Графическая версия Загрузчика репозитория Dr.Web доступна только под ОС Windows.

Windows x86 **Загрузить**

Утилита генерации цифровых ключей и сертификатов
Утилита позволяет генерировать ключи шифрования и цифровые сертификаты, а также осуществлять и проверять цифровую подпись файлов. Является важным средством для обеспечения безопасности соединений между компонентами антивирусной сети.

Ознакомьтесь с подробностями использования утилиты и ручного обновления репозитория антивирусного сервера в п. 9.2 и 9.4.2 документа **Dr.Web Enterprise Security Suite. Руководство администратора**.

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: <https://customers.drweb.com>.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недеklarированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
 - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
 - отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	Сертификаты Минобороны России	Сертификаты ФСБ России	Все сертификаты и товарные знаки
--	---	--	--

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.



© ООО «Доктор Веб»,
2003–2019

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97

<https://антивирус.рф> | <https://www.drweb.ru> | <https://curenet.drweb.ru> | <https://free.drweb.ru>