

Синхронизация групп антивирусной сети с Active Directory под ОС семейства UNIX

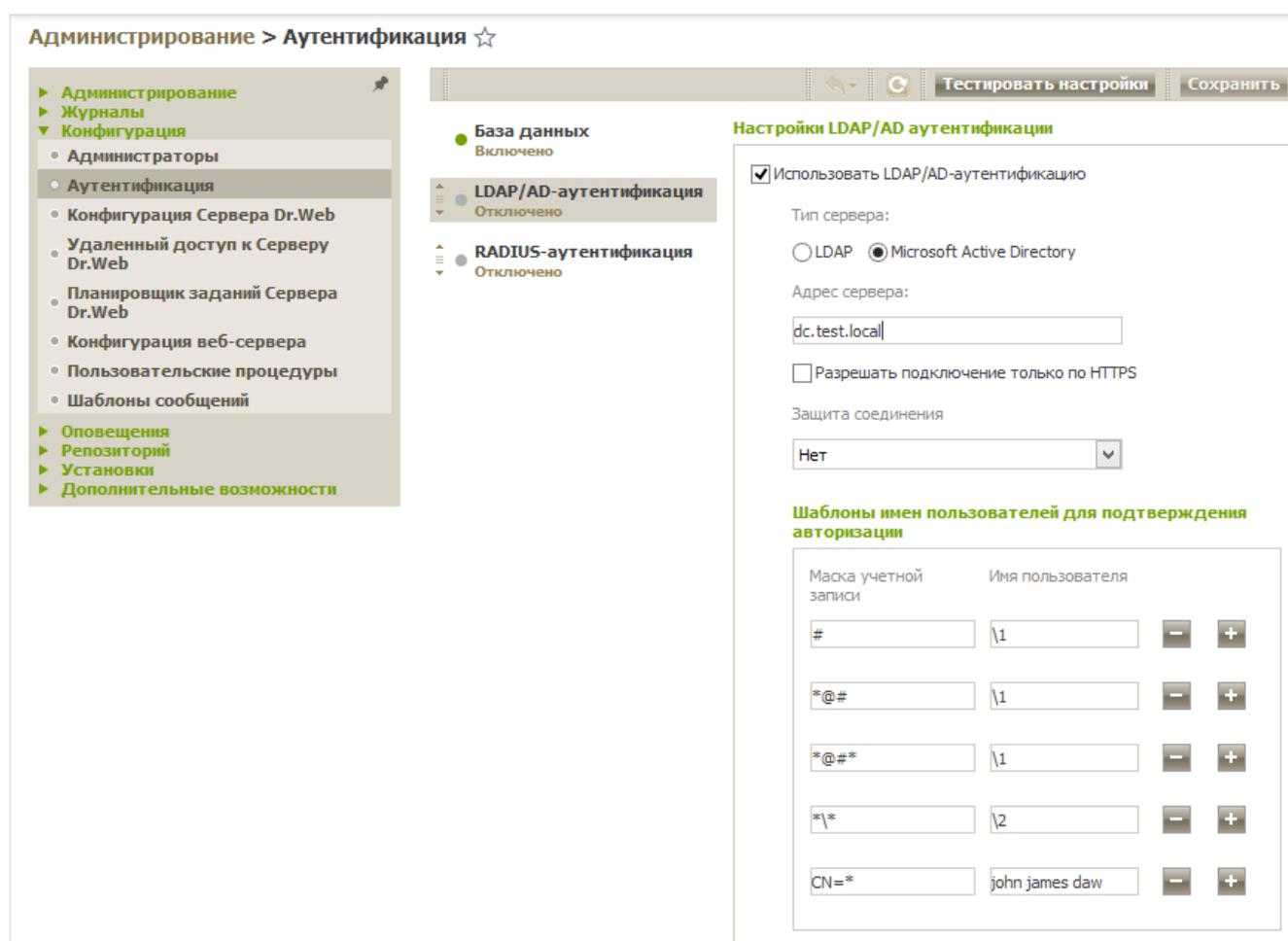


Синхронизация групп антивирусной сети с Active Directory под ОС семейства UNIX

В Dr.Web Enterprise Security Suite версии 11.0 и выше реализована возможность настройки схемы взаимодействия антивируса с сетевой инфраструктурой Active Directory под управлением ОС семейства UNIX. При этом сетевая схема AD органично встраивается в схему Антивирусной сети Сервера Dr.Web.

Для проведения синхронизации необходимо выполнить следующие действия:

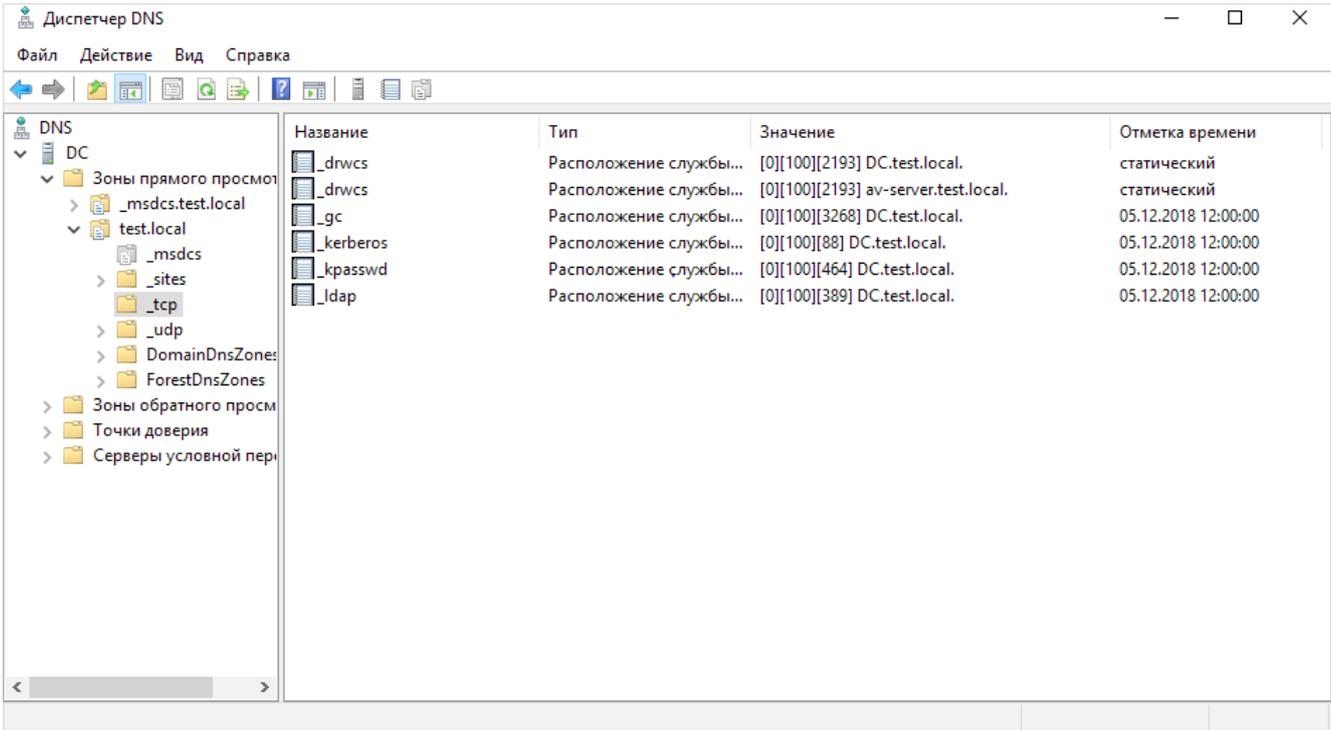
- 1) В разделе **Администрирование** → **Конфигурация** → **Аутентификация** включите возможность аутентификации по LDAP/AD, отметив флажком **Использовать LDAP/AD-аутентификацию**, настройте параметры доступа к серверу и нажмите **Сохранить**. Затем перезагрузите Сервер.



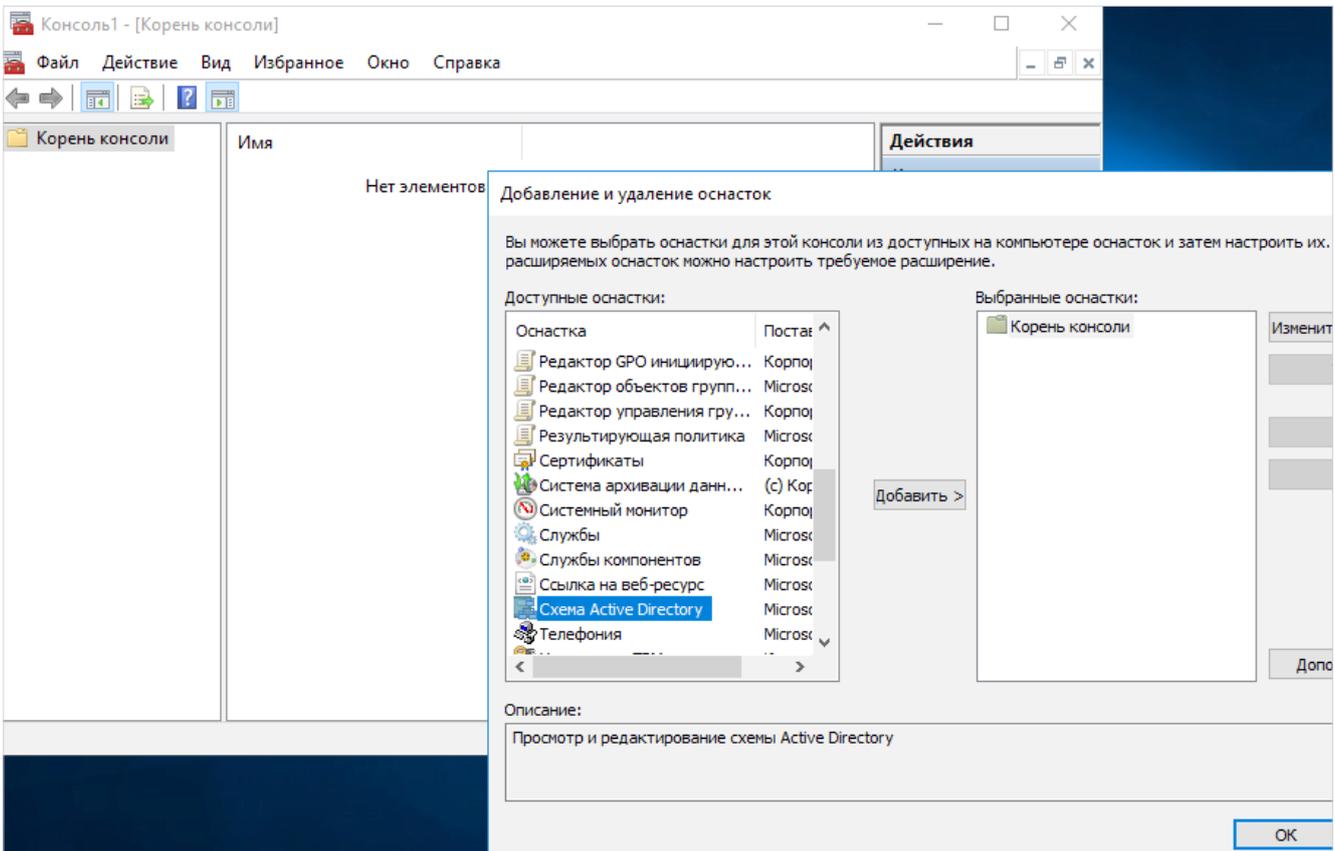
The screenshot shows the 'Администрирование > Аутентификация' configuration page. The left sidebar contains a tree view with 'Аутентификация' selected. The main area is titled 'Настройки LDAP/AD аутентификации'. It features a checkbox 'Использовать LDAP/AD-аутентификацию' which is checked. Below it, 'Тип сервера' is set to 'Microsoft Active Directory'. The 'Адрес сервера' field contains 'dc.test.local'. There is an unchecked checkbox for 'Разрешать подключение только по HTTPS'. The 'Защита соединения' dropdown is set to 'Нет'. At the bottom, there is a table for 'Шаблоны имен пользователей для подтверждения авторизации' with columns for 'Маска учетной записи' and 'Имя пользователя'. The table contains five rows with various masks and user names.

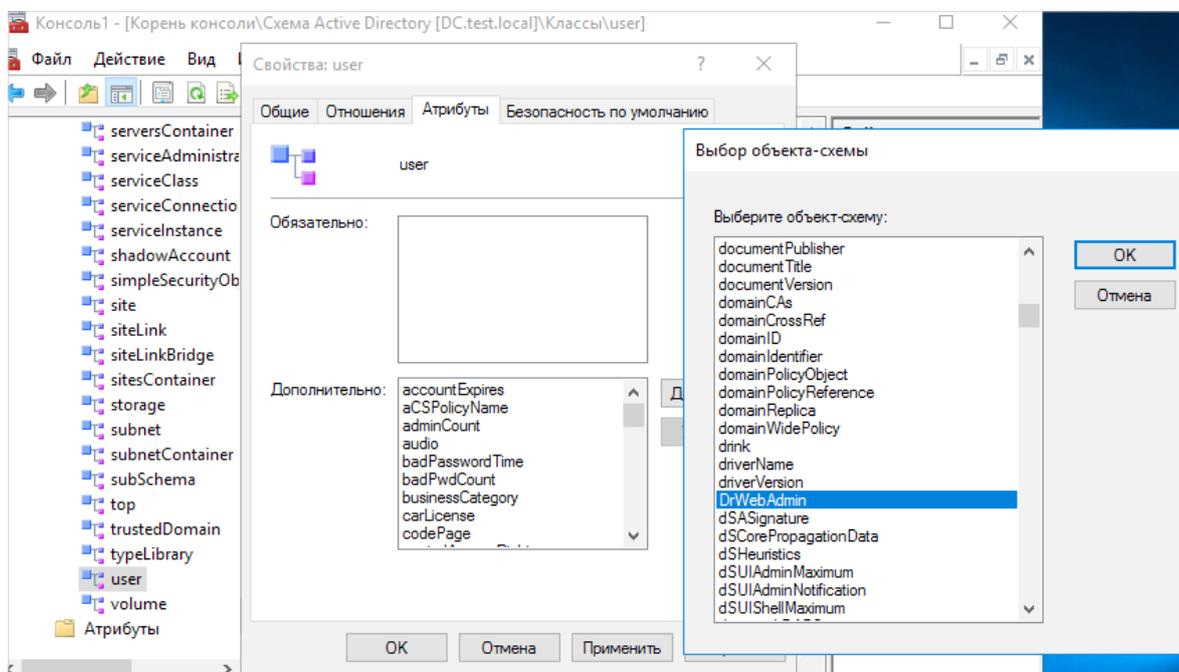
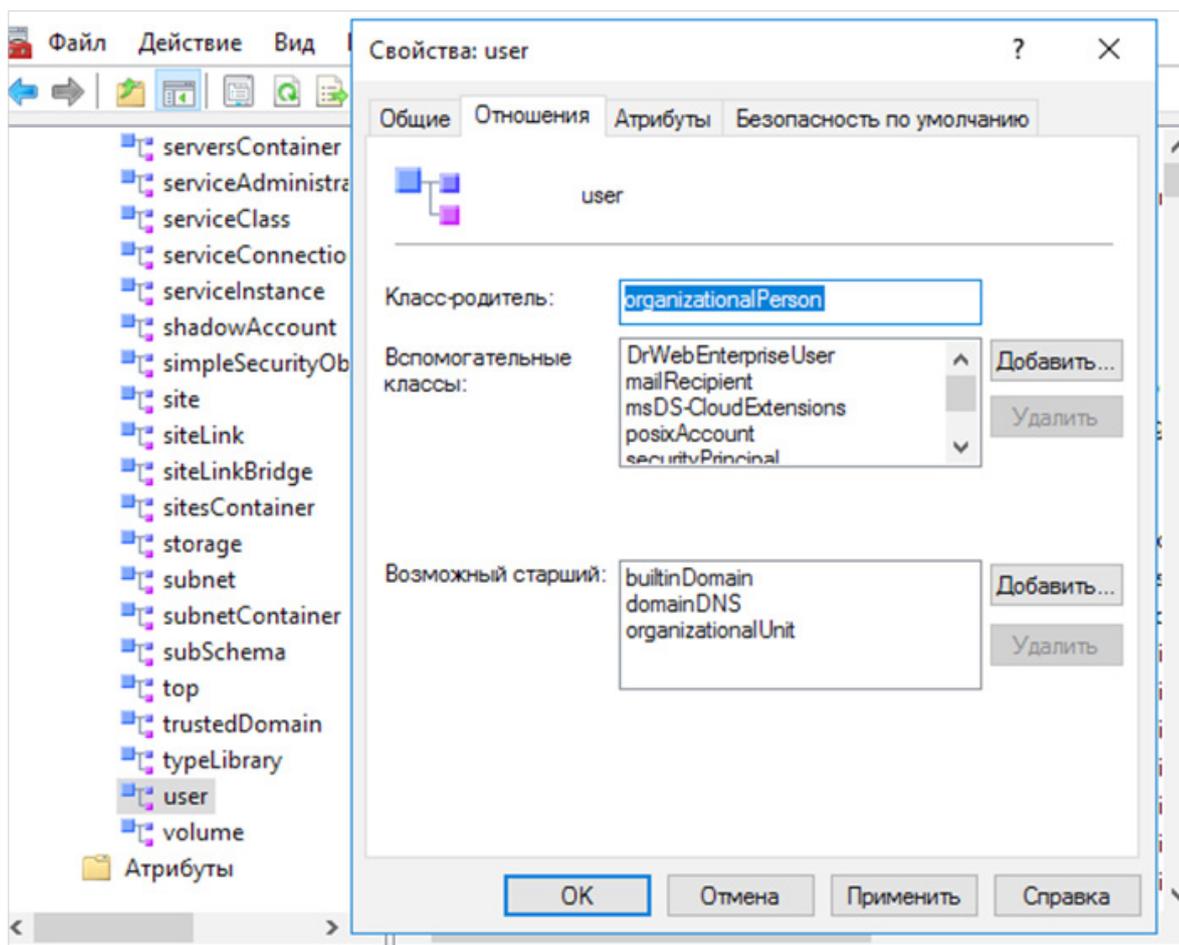
Маска учетной записи	Имя пользователя	-	+
#	\1	-	+
*@#	\1	-	+
@#	\1	-	+
**	\2	-	+
CN=*	john james daw	-	+

Важно! Если ввести имя контроллера домена и выбрать аутентификацию через Active Directory, то при сохранении этих параметров необходимо использовать учетную запись либо администратора домена, либо DNS, поскольку в этот момент в DNS создается запись типа SRV.

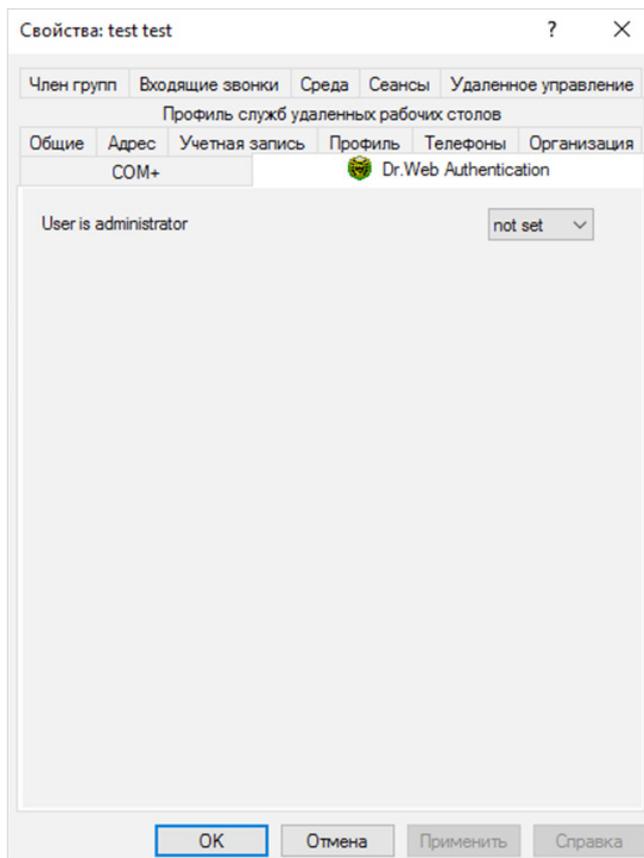


- 2) На контроллере домена с ролью мастера схемы в режиме командной строки (cmd) выполните регистрацию библиотеки *schmmgmt.dll*, введя команду: `regsvr32 schmmgmt.dll`
- 3) Там же откройте оснастку Active Directory Schema и в соответствующие классы (*User* и/или *Group*) добавьте вспомогательный класс *DrWebEnterpriseUser*.

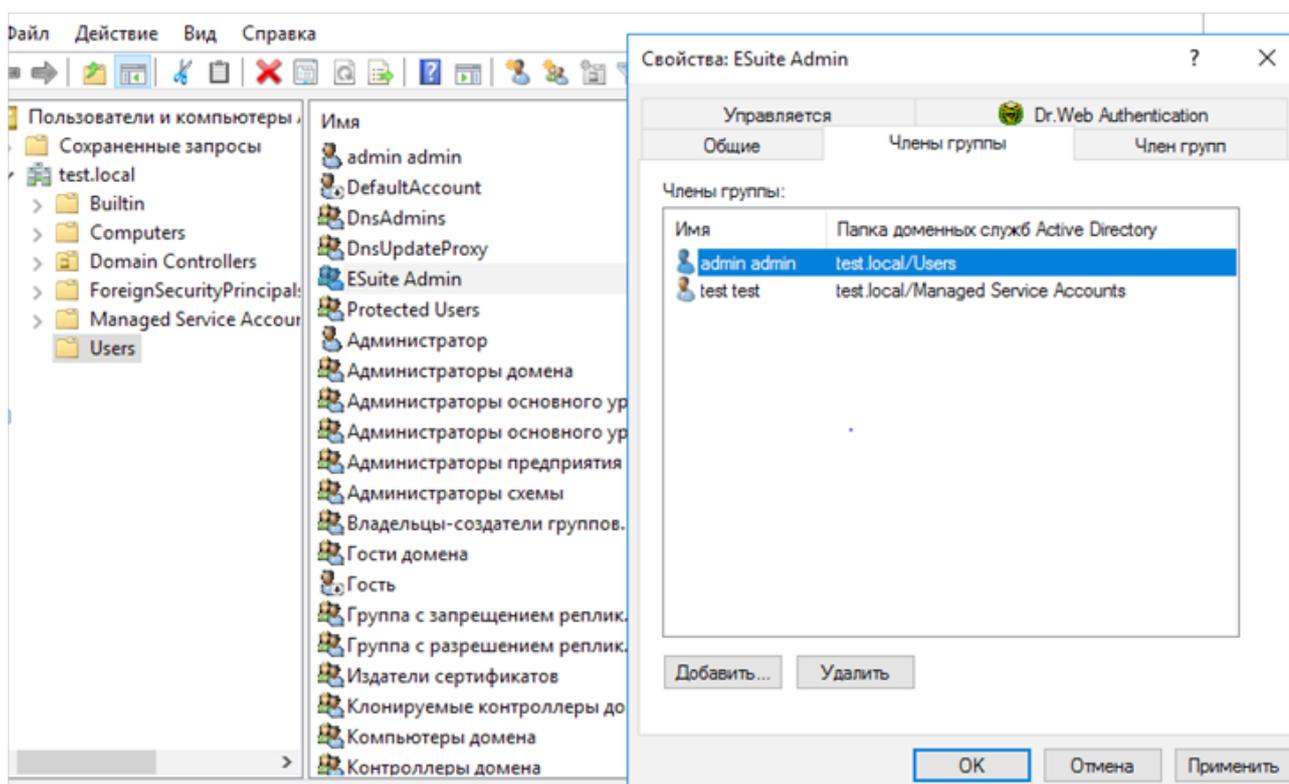




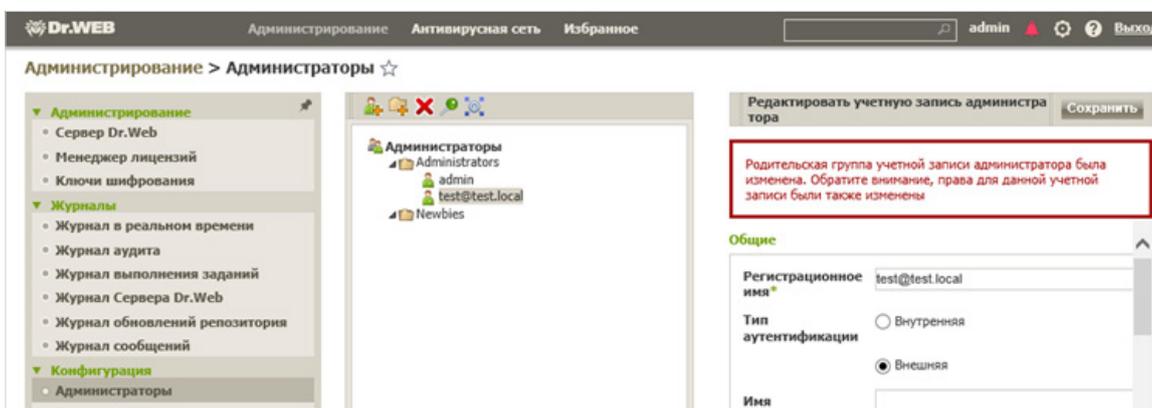
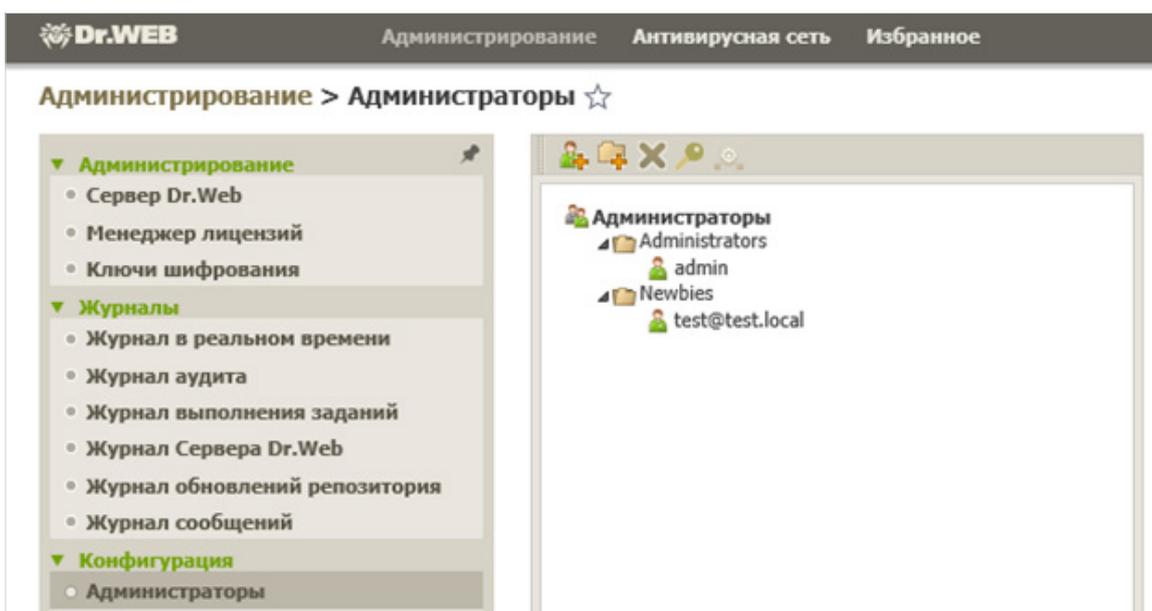
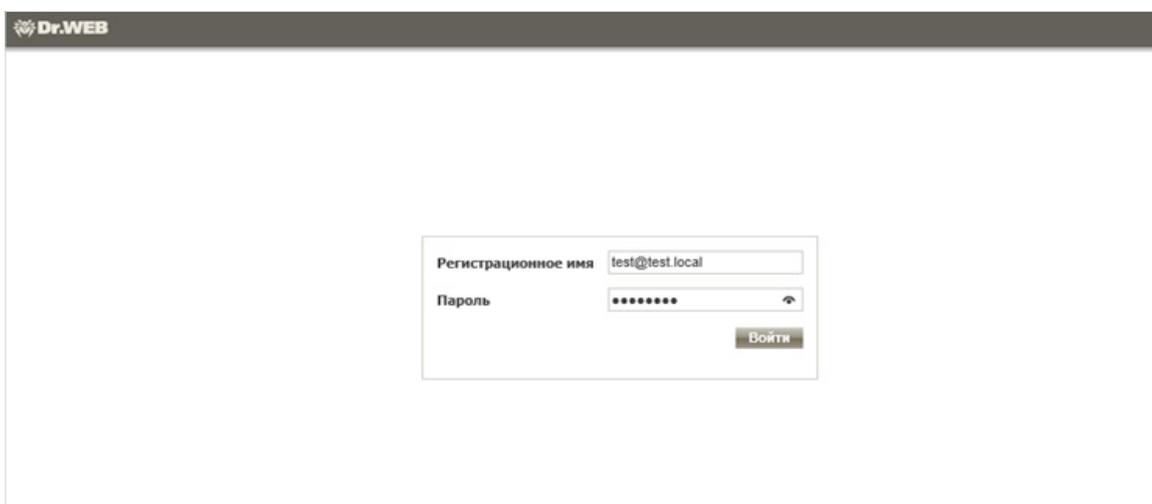
- 4) Закройте Active Directory Schema, запустите с административными полномочиями файл `drweb-11.00.1-<сборка>-esuite-aduac-<версия_OC>.msi` (входит в дистрибутив Dr.Web Enterprise Security Suite 11.0.1) и дождитесь окончания установки.
- 5) Запустите Active Directory Users and Computers и выполните настройку атрибута *Dr.Web Authentication*, задав его свойство *User is administrator = yes*.



- б) Затем создайте в Active Directory группу *Esuite admin* и сделайте текущего пользователя членом этой группы. При этом данный пользователь получит разрешение на вход в консоль администратора с правом просмотра и попадание этой учетной записи в группу **Newbies**.



- 7) Единожды авторизуйтесь под учетной записью, включенной в группу *Esuite admin*, чтобы она появилась в списке *Newbies*; затем, войдя под встроенной учетной записью Администратора, перенесите ее в список *Администраторы*.



- 8) Проведите синхронизацию групп Антивирусной сети и Active Directory, используя расписание Сервера Dr.Web (подробнее см. в [Руководстве администратора](#)).

Важно! При задании параметра **LDAP DN из Active Directory** необходимо:

- 1) Включить задание **Синхронизация с Active Directory** в расписании Сервера Dr.Web (раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web**).

Название	Состояние	Серьезность	Тип запуска	Периодичность	Действие
Backup repository	Запрещено	Не критическое	Синхронно	Еженедельно в субботу, 01:45	Резервное копирование репозитория, Только важные ревизии
Backup sensitive data	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Purge old data"	Резервное копирование критичных данных Сервера
Key expiration reminder	Разрешено	Не критическое	Синхронно	Ежедневно в 07:30	Окончание срока действия лицензионного ключа
Long time unseen servers	Разрешено	Не критическое	Синхронно	Ежечасно в 30 минут	Соседний Сервер давно не подключался
Long time unseen stations	Разрешено	Не критическое	Синхронно	Ежедневно в 07:30	Станция давно не подключалась
Purge old data	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Remove outdated messages"	Очистка старых записей
Purge old stations	Разрешено	Не критическое	Асинхронно	Ежедневно в 00:13	Очистка старых станций
Purge unsent IS events	Разрешено	Не критическое	Синхронно	Ежечасно в 17 минут	Очистка неотправленных событий
Remove outdated messages	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Purge old stations"	Очистка устаревших сообщений
Synchronize groups with Microsoft Active Directory	Запрещено	Не критическое	Синхронно	Каждые 180 минут	Синхронизация с Active Directory

- 2) В правилах членства в качестве строки условия для параметра **LDAP DN из Active Directory** задать требуемое значение DN, например:

OU=OrgUnit,DC=Department,DC=domain,DC=com

После выполнения задания синхронизации организационная структура Active Directory появляется в виде списка в меню **Антивирусная сеть**:

Антивирусная сеть

- test.local
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Keys
 - Managed Service Accounts
 - Program Data
 - System
 - Users

Свойства группы Everyone

Общие

- Идентификатор: 20e27d73-d21d-b211-a788-85
- Название: Everyone
- Родительская группа: Нет родительской группы
- Описание: All stations

Сведения о станциях

- Всего станций: 0
- Первичная группа для: 0
- Станций в сети: 0
- Расположение: Нет объектов для отображе карте

Конфигурация

- Права. Заданы персональные настройк
- Планировщик заданий. Заданы персо

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.

<u>Сертификаты ФСТЭК России</u>	<u>Сертификаты Минобороны России</u>	<u>Сертификаты ФСБ России</u>	<u>Все сертификаты и товарные знаки</u>
---	--	---	---

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



© ООО «Доктор Веб»,
2003–2018

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>