

1. Документация Ideco Selecta	2
1.1 Общая информация	2
1.1.1 О продукте	2
1.1.2 Техническая поддержка	2
1.2 Установка	3
1.2.1 Системные требования	3
1.2.2 Установка Ideco Selecta	3
1.2.3 Первоначальная настройка	4
1.2.3.1 Добавление маршрутов	6
1.2.3.2 Настройка сети	6
1.2.4 Активация сервера	7
1.3 Настройка	8
1.3.1 Авторизация	8
1.3.2 Профили	8
1.3.3 Группы слов	11
1.3.4 Фильтрация по списку Роскомнадзора	12
1.3.5 Журнал	14
1.3.6 Учетные записи	14
1.3.7 Настройка фильтрации HTTPS	15
1.3.8 Настройка прямых подключений к прокси-серверу	20
1.3.9 Настройка интеграции с Active Directory	20
1.3.9.1 Настройка веб-авторизации в Active Directory	27
1.3.9.2 Интеграция с AD, авторизация на базе логов безопасности	28
1.3.10 Настройка SMS-авторизации	34
1.3.11 Настройка интеграции с внешними ICAP-сервисами	35
1.3.12 Настройка WCCP	36
1.3.13 Интеграция по eBGP	41
1.3.14 Настройка подключения Selecta к Центральной консоли	43
1.3.15 Отчеты	45
1.4 Обслуживание	47
1.4.1 Обновление системы	47
1.4.2 Разрешить доступ в интернет без фильтрации	48
1.5 Инструкции по интеграции	48
1.5.1 Инструкция для автоматического развертывания доверенного сертификата средствами Active Directory	48
1.5.2 Настройка СКФ Ideco Selecta в режиме интеграции с Active Directory и авторизации пользователей на прокси сервере	49

Документация Ideco Selecta

Система контентной фильтрации Ideco Selecta - это программное решение для фильтрации интернет-трафика для среднего и крупного бизнеса, образовательных учреждений и интернет-провайдеров.

Ideco Selecta позволяет осуществлять фильтрацию широкополосного (до 40 Гбит/сек) HTTP/HTTPS трафика как по категориям URL, так и по содержимому веб-страниц.

Для категоризации URL используется облачный сервис Ideco Cloud WebFilter (144 категории сайтов, более 500 млн URL в базе данных).

Общая информация

Текущий раздел содержит характеристику возможностей системы контентной интернет-фильтрации Ideco Selecta, ее назначение и применение.

О продукте

Система контентной интернет-фильтрации Ideco Selecta - это программное решение для фильтрации интернет-трафика для среднего и крупного бизнеса, образовательных учреждений и интернет-провайдеров.

Ideco Selecta позволяет осуществлять фильтрацию широкополосного (до 40 Гбит/сек) HTTP/HTTPS трафика, как по категориям URL, так и по содержимому веб-страниц.

Для категоризации URL используется обновляемая база данных (144 категории сайтов, более 500 млн URL в базе данных).

[Системные требования.](#)

[Техническое описание.](#)

Техническая поддержка

График работы службы технической поддержки

Техническая поддержка предоставляется 6 дней в неделю, за исключением праздничных дней. График работы представлен ниже.

Дни недели	Время работы (Московское)
понедельник – пятница	07:00 – 19:00
суббота	09:00 – 16:00
воскресенье и праздничные дни	–

Способы обращения в службу

Способы обращения в службу перечислены в следующей таблице.

Способ	Описание
Система HelpDesk	https://helpdesk.ideco.ru/
Телефон	+7 (495) 662-87-34 (многоканальный)
Электронная почта	support@ideco.ru
Форум	https://forum.ideco.ru

Почта и форум не являются гарантированными способами обращения, в случае отсутствия ответа – обратитесь по телефону или через систему HelpDesk.

При обращении будьте готовы предоставить специалистам следующую информацию:

- название организации;
- регистрационный номер.

Установка

Текущий раздел содержит информацию о минимальных системных требованиях, описывает процесс установки Ideco Selecta, включая подготовительные этапы. Информация, представленная здесь, позволяет произвести первоначальную настройку.

Системные требования

Для установки и работы Ideco Selecta не требуется предустановленная ОС и дополнительное программное обеспечение.

Ideco Selecta устанавливается на выделенный сервер с загрузочного DVD или USB-flash, при этом автоматически создается файловая система и устанавливаются все необходимые компоненты.

Работа Ideco Selecta возможна как на выделенном сервере, так и в качестве виртуальной машины на всех современных гипервизорах, поддерживающих ОС Debian 9.

Минимальные системные требования:

- Поддержка UEFI (рекомендуется)
- Процессор — 64-разрядный, двухъядерный (от 3 Ghz) Intel или AMD.
- Оперативная память - от 4 GB.
- Свободное место на диске — от 40 GB
- 3 сетевых интерфейса.

Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет или материнскую плату).

Получить рекомендации по подбору оборудования под ваши задачи или уточнить совместимость можно, обратившись в [техническую поддержку](#).

Установка Ideco Selecta

Установка с ISO-образа.

Скачайте ISO-образ Ideco Selecta с [нашего сайта](#).



Debian GNU/Linux installer boot menu

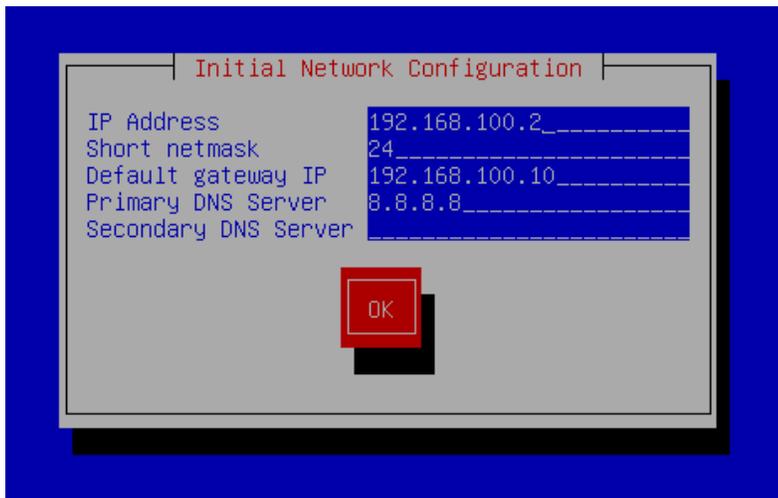
- Install
- Graphical install
- Advanced options >
- Help
- Install with speech synthesis

Press ENTER to boot or TAB to edit a menu entry

Если при установке система попросит выбрать какие-либо параметры и вы не знаете что вводить - оставьте значения по умолчанию.

Первоначальная настройка

При первом запуске система потребует ввода реквизитов для начальной настройки:



После указания начальных настроек будет доступен веб-интерфейс управления.

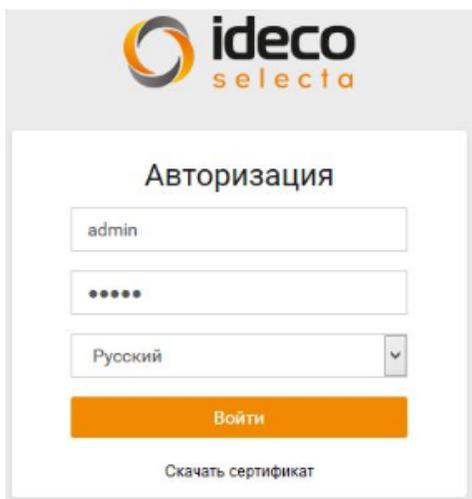
В случае если у вас несколько сетевых интерфейсов, то подключиться можно к любому из них – интерфейс будет доступен по тому же адресу, который был указан в окне первоначальной настройки.

Настройка самого продукта осуществляется через веб-интерфейс.

Для первоначального входа в него используйте следующие

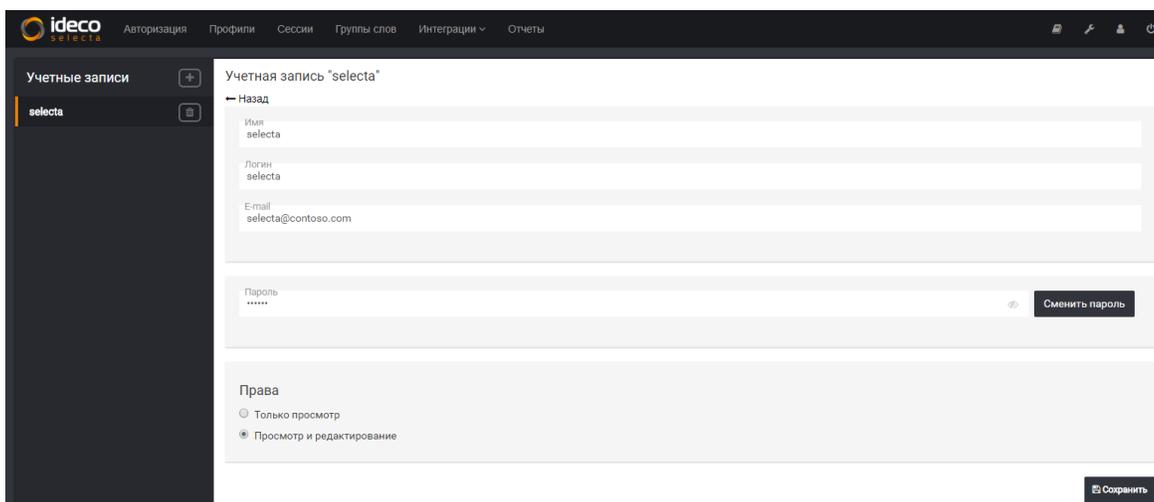
учетные данные:

- Логин: admin
- Пароль: admin



После первого входа в веб-интерфейс обязательно создайте новую учётную запись с правами на просмотр и редактирование, чтобы обезопасить сервер от попыток автоматического перебора паролей:

Настройки - Учетные записи



Внимание: после создания новой учётной записи с правами на редактирование с логином и паролем admin авторизоваться уже не получится.

Добавление маршрутов

Чтобы добавить маршрут, необходимо перейти в Настройки -> Сетевые настройки и выбрать для редактирования сетевое подключение. Далее необходимо перейти в меню Маршруты

ideco selecta Авторизация Профили Сессии Группы слов Интеграции Отчеты

Параметры соединения "wan"

← Назад

Маршруты

Название соединения
wan

Тип
Ethernet

Параметры IPv4

Устройство
Intel Corporation, 82540EM Gigabit Ethernet Controller, 08:00:27:57:aa:e9 (enp0s3)

Роль
Внешний

IP-адрес
10.80.220.1

Маска подсети
16

Сохранить

Далее нажать на кнопку Добавить

ideco selecta Авторизация Профили Сессии Группы слов Интеграции Отчеты

Параметры соединения "wan"

← Назад

Маршруты

Нет добавленных маршрутов

+ Добавить

На следующей странице в поле Подсеть/маска указать сеть назначения с префиксом, а в поле Шлюз указать адрес, на который следует отправлять трафик, предназначенный для указанной сети, и нажать кнопку Создать

ideco selecta Авторизация Профили Сессии Группы слов Интеграции Отчеты

Параметры соединения "Control"

← Назад

Маршруты

Подсеть/маска
192.168.1.0/24

Шлюз
192.168.1.1

+ Создать Отмена

Нет добавленных маршрутов

При добавлении маршрута нужно иметь в виду, что IP-адрес шлюза должен принадлежать той же сети, что и IP-адрес сетевого подключения, для которого создается маршрут.

Настройка сети

- Настройка сетевых интерфейсов при схеме интеграции в режиме роутера

Нужно настроить следующие сетевые подключения:

1. Подключение типа Ethernet с ролью "Административный";
2. Подключение типа Ethernet с ролью "Внешний" с IP-адресом из внешней сети;
3. Одно или несколько подключений типа Ethernet с ролью "Локальный" с IP-адресом из локальной сети;

При такой конфигурации IdecO Selecta будет производить маскердинг на интерфейсе, помеченном как "Внешний", при помощи SNAT.

Пример настройки:

Список подключений + Создать				
Имя	Тип	Роль	Устройство	Действия
control	Ethernet	Административный	RTL-8100/8101L/8139 PCI Fast Ethernet Adapter 52:54:00:21:45:D6	 
wan	Ethernet	Внешний	RTL-8100/8101L/8139 PCI Fast Ethernet Adapter 52:54:00:9C:C6:92	 
lan	Ethernet	Локальный	RTL-8100/8101L/8139 PCI Fast Ethernet Adapter 52:54:00:59:AC:F3	 

После настройки сетевых подключений необходимо перезагрузить сервер командой `reboot` в консоли, либо через веб-интерфейс нажатием кнопки Перезагрузить сервер в верхнем правом углу. Во втором случае, если IP-адрес административного интерфейса был изменен, подключение к веб-интерфейсу может пропасть на некоторое время, и нужно будет просто немного подождать и перезагрузить страницу в браузере.

- Настройка сетевых интерфейсов при схеме интеграции в разрыв сети

В разрыв:



Рис. 1 – типовая

схема подключения "в разрыв сети"

В данном режиме интеграции весь трафик от пользователей проходит прозрачно через мост.

Нужно настроить как минимум 4 подключения:

1. Подключение с ролью "Административный";
2. Подключение типа "Мост". IP-адрес на этом интерфейсе не нужен для корректной маршрутизации пакетов, на нём не будут доступны ни веб-интерфейс Ideco Selecta, ни SSH;
3. Подключение типа "Интерфейс моста" и ролью "Локальный", который ведёт в сторону клиентов;
4. Подключение типа "Интерфейс моста" и ролью "Внешний", который ведёт в сторону шлюза.

Пример настройки интерфейса типа "Мост":

Список подключений + Добавить				
Имя	Тип	Сеть	Устройство	Действия
Control Административный	Мост	10.80.220.2/16	br-1-slave-0, br-1-slave-1, br-1-slave-2	 
br-1-slave-0	Интерфейс моста		82574L Gigabit Network Connection 00:1B:21:63:3B:A0 (ens2)	 
br-1-slave-1	Интерфейс моста		NetXtreme BCM5720 Gigabit Ethernet PCIe 64:51:06:0E:0F:B0 (eno1)	 
br-1-slave-2	Интерфейс моста		NetXtreme BCM5720 Gigabit Ethernet PCIe 64:51:06:0E:0F:B1 (eno2)	 

Изменения будут применены только после перезагрузки сервера

В данном примере настроен один логический интерфейс типа "Мост", он же Административный, и три физических интерфейса, объединенные в этот мост. Таким образом, на веб-интерфейс и в SSH-консоль можно будет попасть по IP-адресу 10.80.220.2/16 с любого из трех физических интерфейсов.

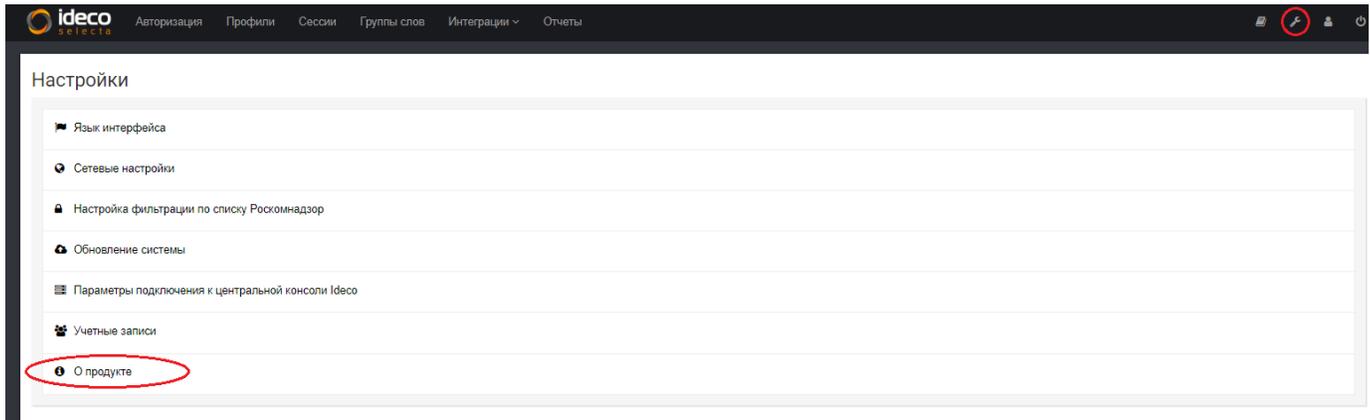
После настройки сетевых подключений необходимо перезагрузить сервер командой `reboot` в консоли, либо через веб-интерфейс нажатием кнопки Перезагрузить сервер в верхнем правом углу. Во втором случае, если IP-адрес административного интерфейса был изменен, подключение к веб-интерфейсу может пропасть на некоторое время, и нужно будет просто немного подождать и перезагрузить страницу в браузере.

Если вы настроили сеть неправильно и хотите сбросить настройки, то выполните команду `network-reset` в локальной консоли и следуйте инструкциям на экране.

Активация сервера

Для работы системы фильтрации в продукте требуется его обязательная регистрация.

Для того чтобы зарегистрировать сервер, нужно ввести лицензионный ключ в меню Настройки -> О продукте.



Настройка

Раздел включает в себя информацию об основных этапах настройки Idec Selecta.

Авторизация

На этой вкладке вы можете создавать авторизации для подсетей и хостов и настраивать их параметры.

Параметры авторизации:

- Имя;
- IP-адрес/CIDR - адрес хоста/сети (хост можно указывать без маски, сеть нужно указывать с "короткой" маской, например так: 192.168.0.0/24);
- Тип авторизации - статическая (по IP-адресу) либо динамическая (при помощи SMS, в данном случае должна быть настроена интеграция SMPP, или же веб-авторизация, в данном случае должна быть настроена интеграция с Active Directory);
- Профиль - в этом поле задается профиль фильтрации для данной авторизации;
- Разрешить подключение - этот чекбокс позволяет включать/выключать доступ к ресурсам сети Интернет для пользователей, попадающих под данную авторизацию;

Пример настройки статической авторизации:

Добавить авторизацию для подсети

Имя	client
IP-адрес/CIDR	192.168.10.0/24
Тип авторизации	Статический
Профиль	default
Разрешить подключение	<input checked="" type="checkbox"/>
<small>Выключите, если вы хотите запретить просмотр веб-страниц</small>	
Создать	

Профили

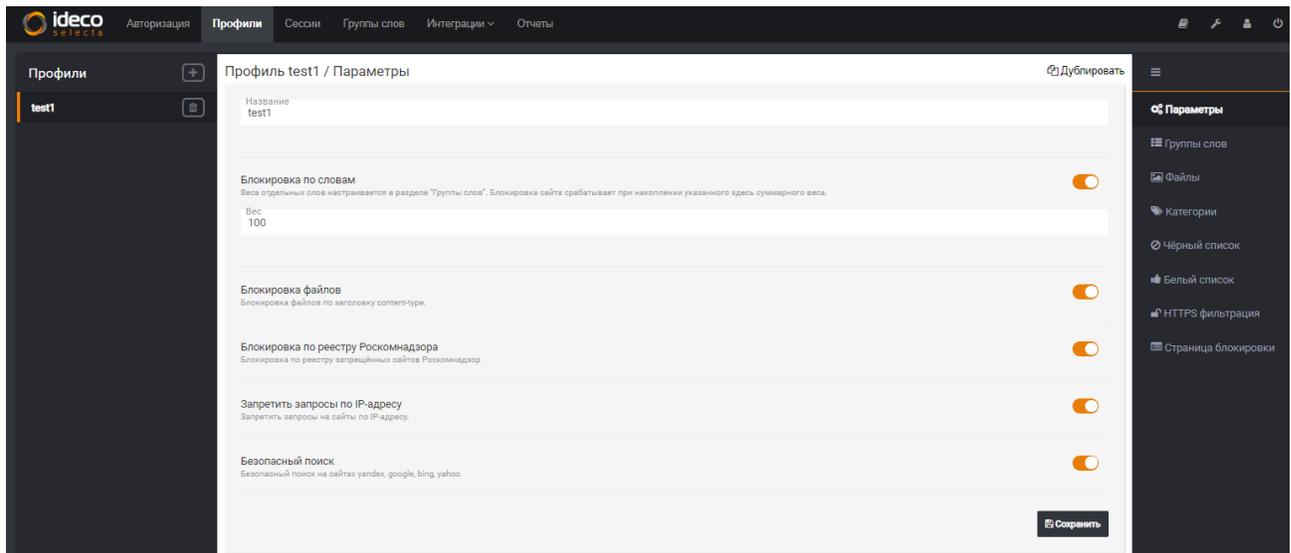
Профили используются для применения настроек выхода в Интернет для пользователей.

- Параметры
- Группы слов
- Файлы
- Категории

- Черный список
- Белый список
- HTTPS Фильтрация
- Страница блокировки

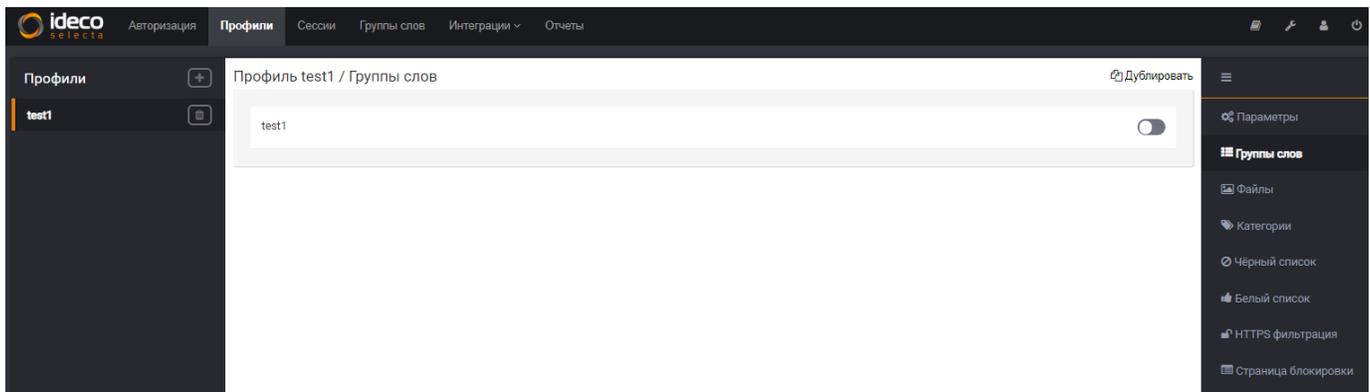
Параметры

- Название - имя профиля;
- Включить блокировку по словам - включает возможность блокировки веб-страниц, исходя из размещенного на них тестового контента;
- Вес - суммарный вес найденных на странице слов, при котором сработает блокировка. Слова и соответствующий им вес настраиваются в разделе Группы слов;
- Включить блокировку по файлам - включает возможность блокировки скачивания определенных на вкладке "Файлы" расширений и MIME-типов файлов;
- Включить блокировку по реестру Роскомнадзора - блокирует сайты, находящиеся в списке Роскомнадзора (список сайтов обновляется автоматически). Настройка загрузки и обновления списка осуществляется в Настройки -> Настройка фильтрации по списку Роскомнадзора;
- Запретить запросы по IP-адресу - запрещает пользователям обращаться к сайтам по IP-адресам, а не по доменным именам. Например: <http://1.2.3.4>;
- Включить безопасный поиск - принудительно включает безопасный поиск для пользователей на всех популярных поисковых сайтах.



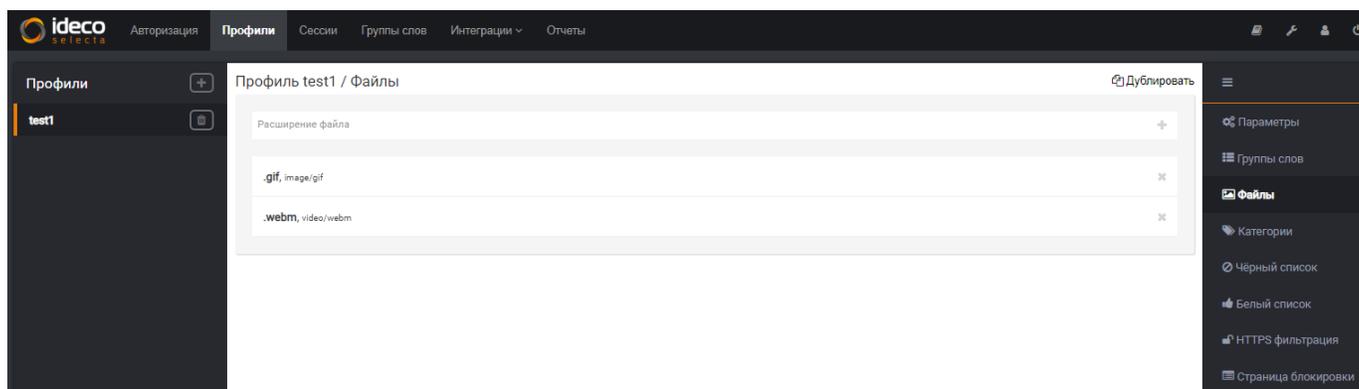
Группы слов

На данной вкладке для профиля можно активировать группы слов, вес которых учитывается при контентном анализе веб-страниц:



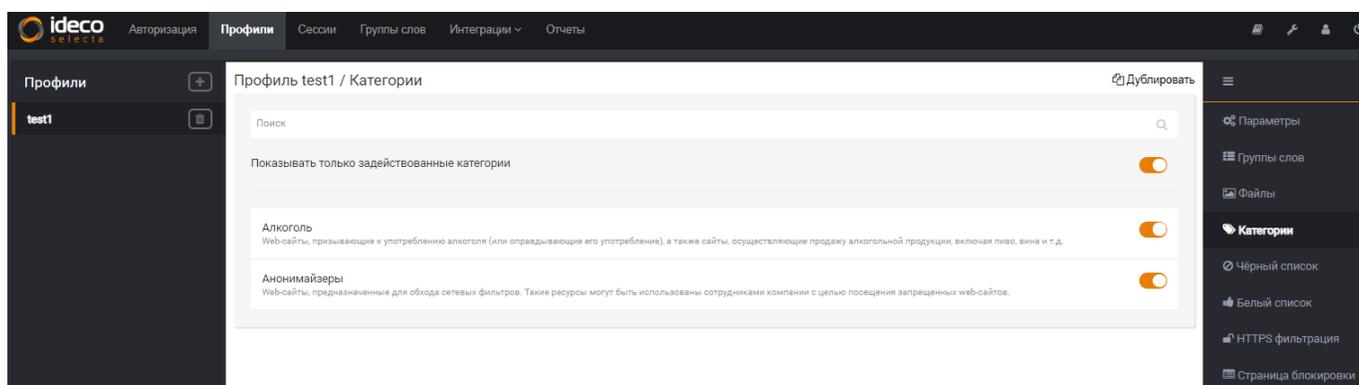
Файлы

На вкладке указываются запрещенные расширения файлов, скачивание которых запрещено для пользователей, которым назначен данный профиль. Система учитывает как расширение, так и MIME-тип содержимого страницы (видео-файл .avi не будет скачан, даже если его название не будет содержать данное расширение):



Категории

Список запрещенных категорий сайтов для пользователей, использующих данный профиль. Для категоризации по URL Idec Selecta использует облачные базы данных, информация в которых обновляется автоматически в режиме реального времени.

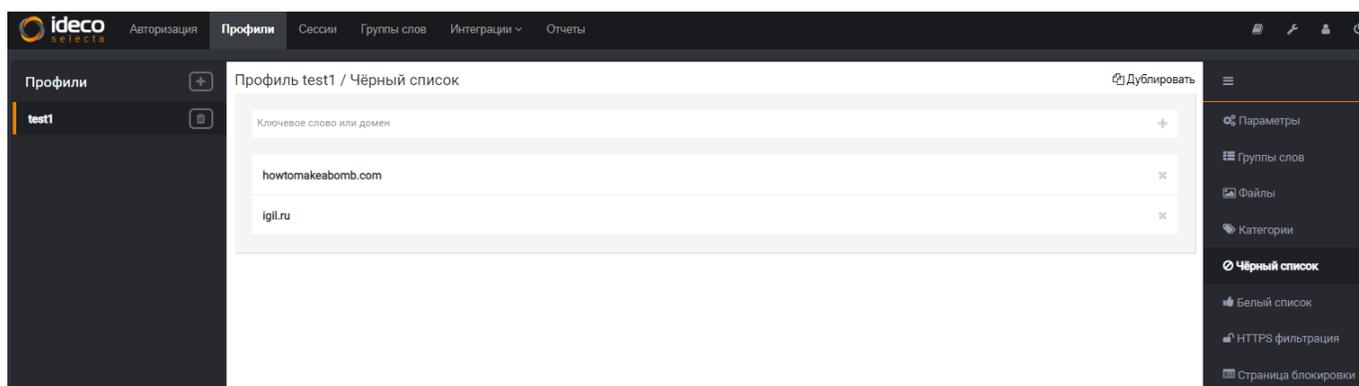


После установки системы категории могут медленно работать некоторое время. Для полноценной работы требуется скачать и установить образ базы (примерно 4Гб, это будет сделано автоматически).

Установка и обновление базы происходит в автоматическом режиме каждые 4 часа. Изменения применяются автоматически.

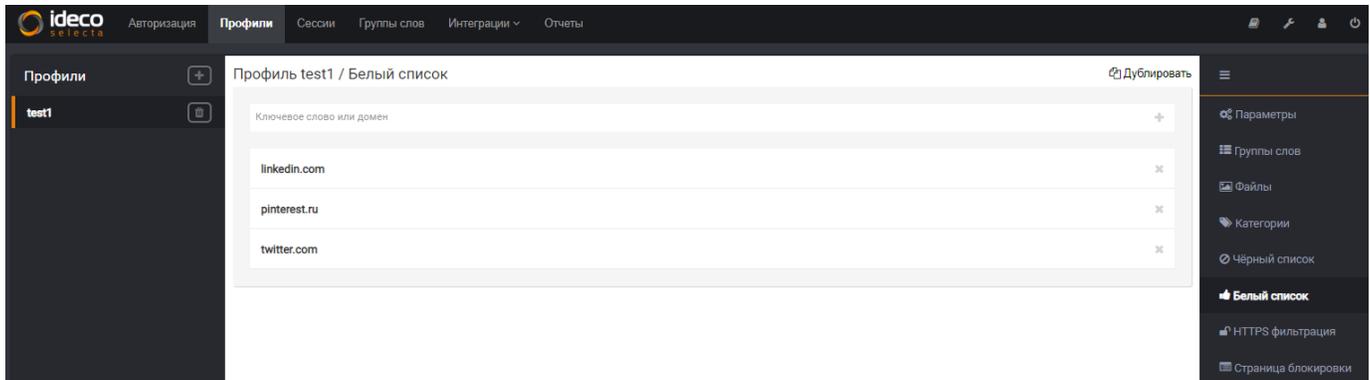
Черный список

Список URL, запрещенных для пользователей, которым назначен данный профиль.



Белый список

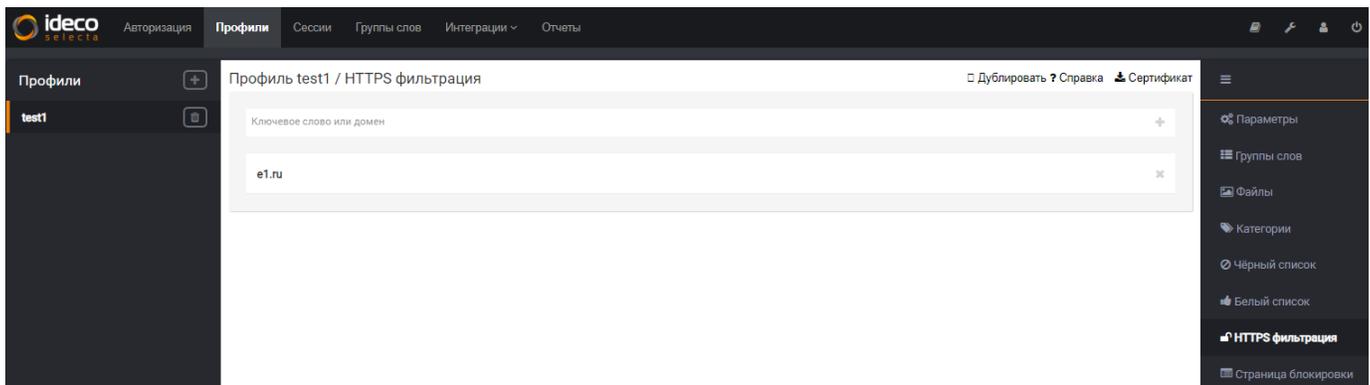
Список URL, разрешенных для пользователей, которым назначен данный профиль, вне зависимости от содержания веб-страниц на этих сайтах и их категоризации.



Белый список имеет приоритет перед черным списком.

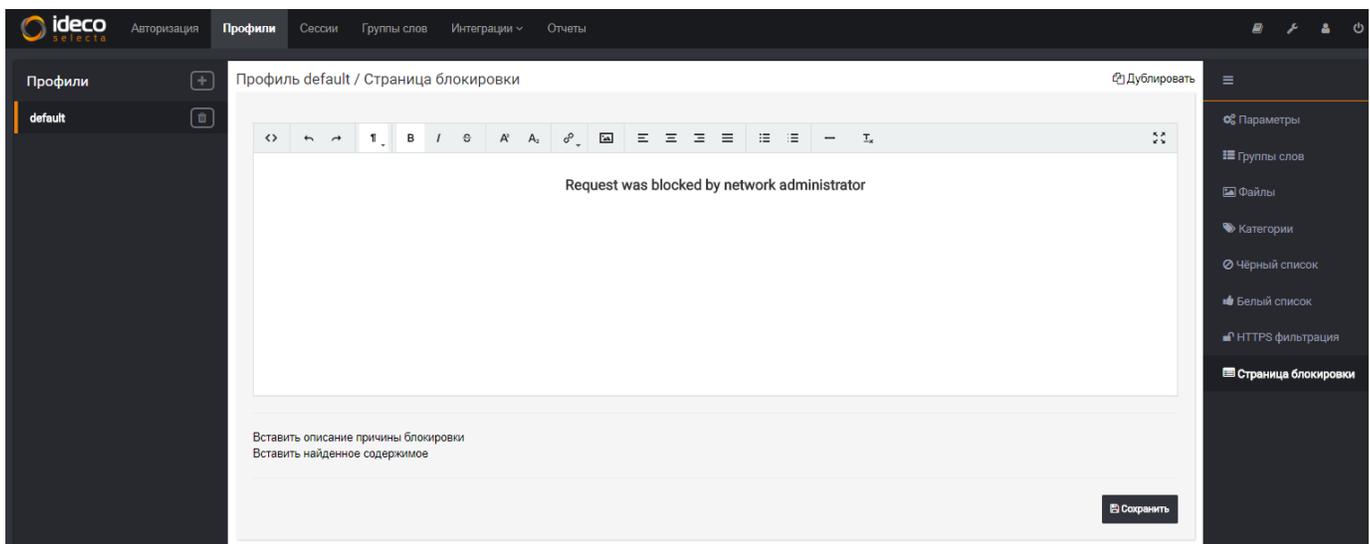
HTTPS Фильтрация

Список URL, для которых нужно производить подмену сертификата и применять полный набор фильтров.



Страница блокировки

На данной вкладке можно кастомизировать веб-страницу, которую пользователи будут видеть при попытке попасть на заблокированный ресурс.



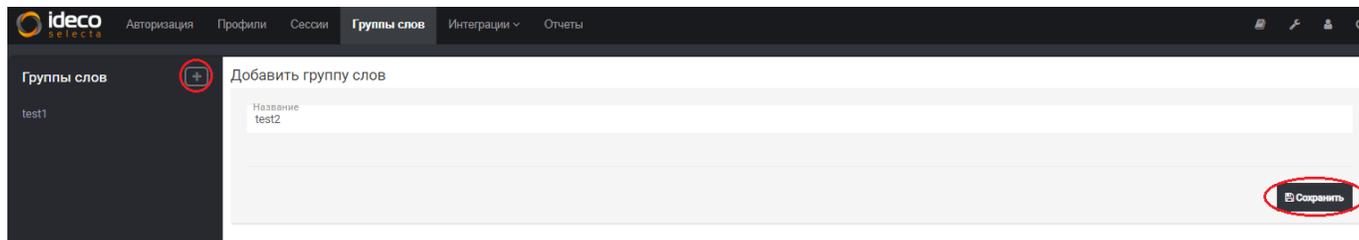
Группы слов

В данном разделе настраиваются группы слов, используемые при контентном анализе веб-страниц.

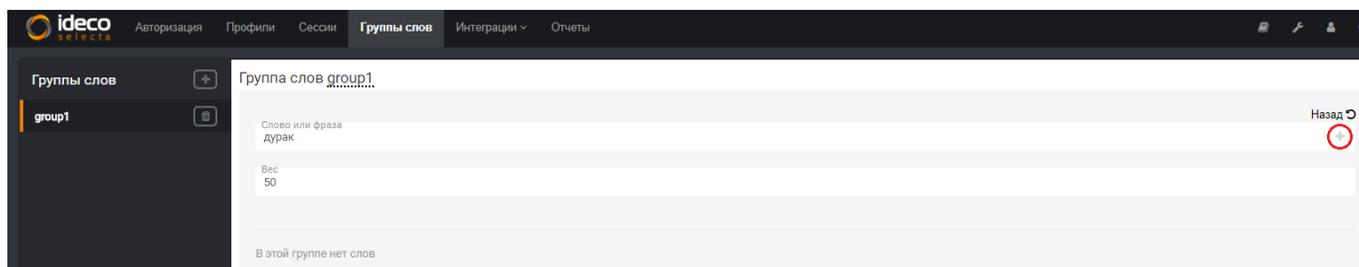
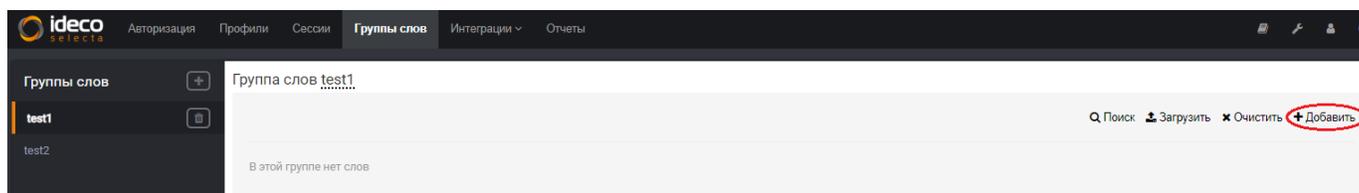
Возможна загрузка слов из файлов (формата .csv), также можно добавить слово и его вес вручную.

Сервер также учитывает морфологию слов (т.е. различные падежные формы добавленных в словарь слов) и ведёт учёт слов, набранных транслитом.

Добавление новой группы слов:



Добавление слов в группу:



Фильтрация по списку Роскомнадзора

Для настройки фильтрации трафика по списку Роскомнадзора нужно:

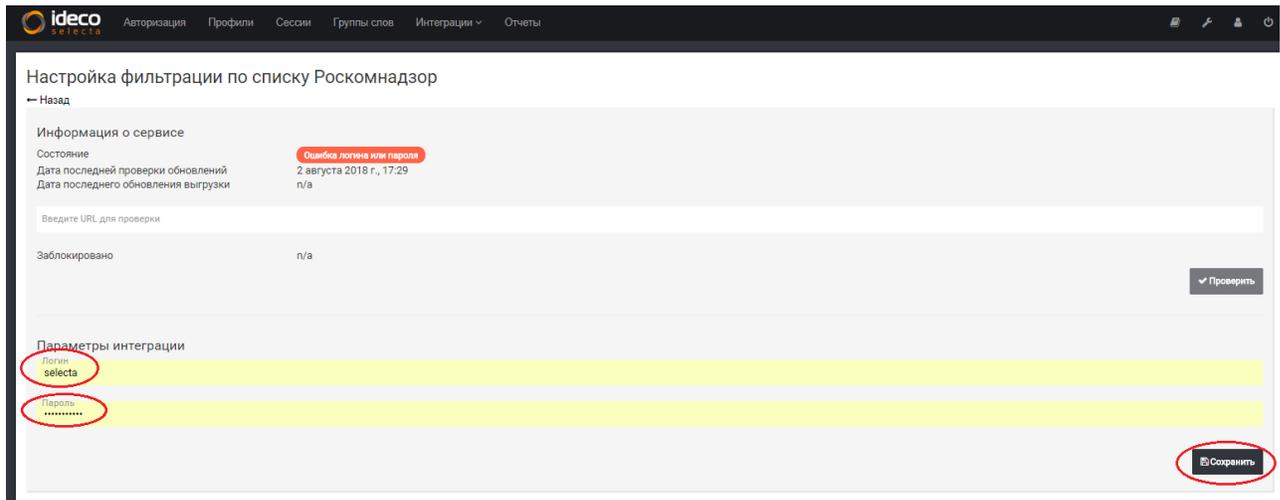
1. Предварительно получить реквизиты доступа к серверу для скачивания списков, для этого необходимо подготовить запрос по форме:

Наименование:	
ИНН:	
Контакт:	
Email:	
Рабочий телефон	
Перечень IP адресов, с которых будет осуществляться загрузка. (До 5 шт.)	

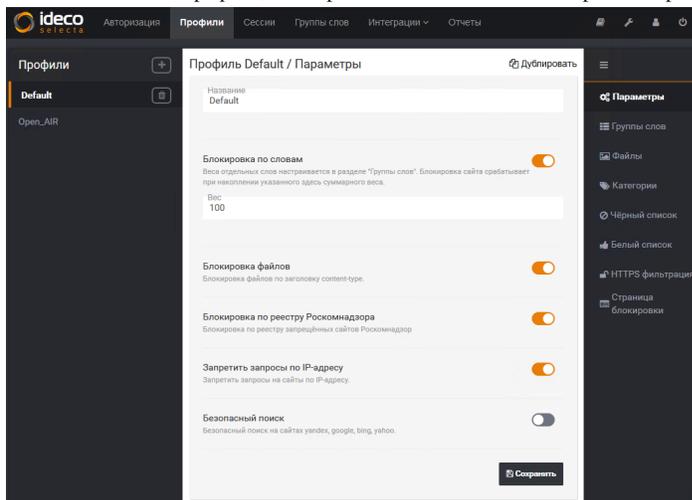
Далее, направить запрос в Роскомнадзор, либо в техническую поддержку Айдеко через <https://helpdesk.ideco.ru>

В течении 5 рабочих дней на указанный в запросе email придут реквизиты (логин и пароль).

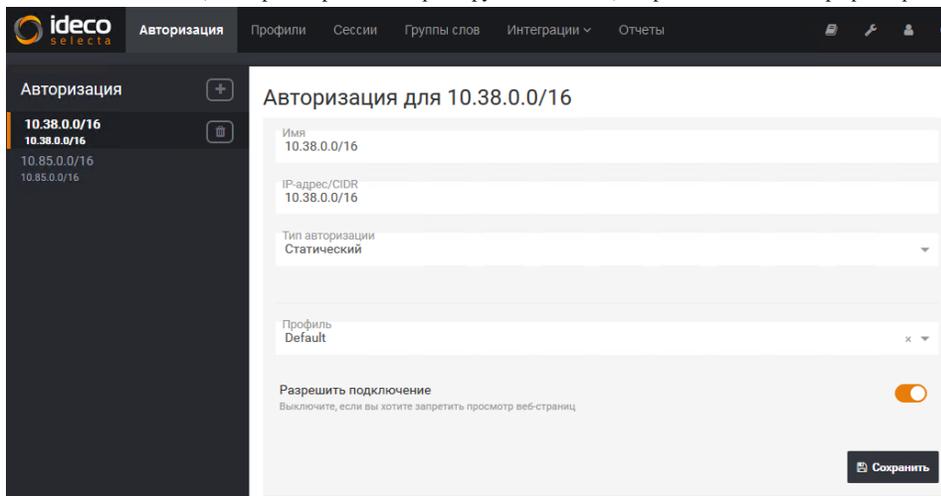
2. Перейти в меню Настройки → Настройка фильтрация по списку Роскомнадзор, ввести полученные логин и пароль в разделе параметры интеграции.



3. После этого создать профиль, в котором включить опцию "Блокировка по реестру Роскомнадзора"



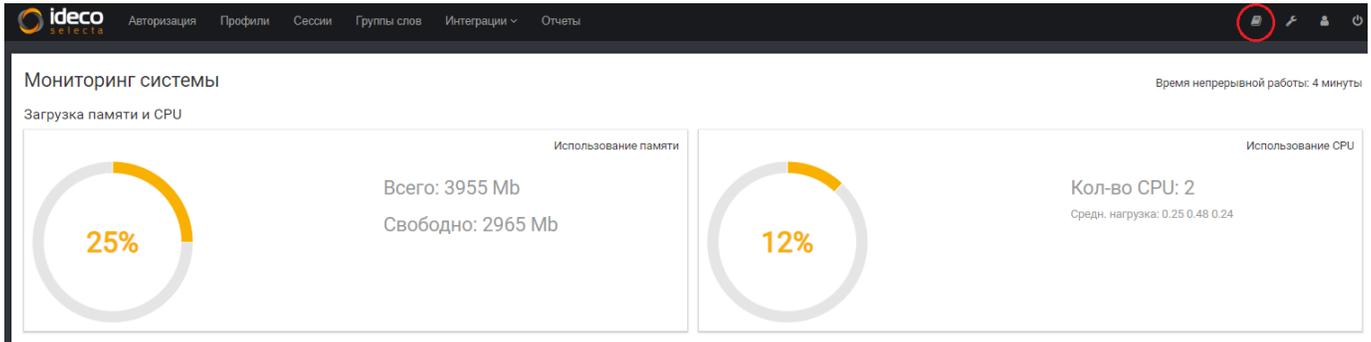
4. Создать пользователя (в котором перечислить фильтруемые подсети) и применить данный профиль фильтрации.



Selecta автоматически обращается за обновлением списка РКН раз в минуту.

Журнал

В данном разделе доступен вывод статистики пользователей по посещенным ими ресурсам с возможностью сортировки по наличию факта блокировки сайта, а также по времени.



Журнал

Фильтр по доменному имени

Имя домена

Фильтр по пользователям

Поиск

Фильтр по дате

23.05.2018 23.08.2018

23.05.2018 08.07.2018 23.08.2018

00:00 23:59

00:00 06:00 12:00 17:59 23:59

Фильтр по типу блокировки

все

незаблокированные

заблокированные

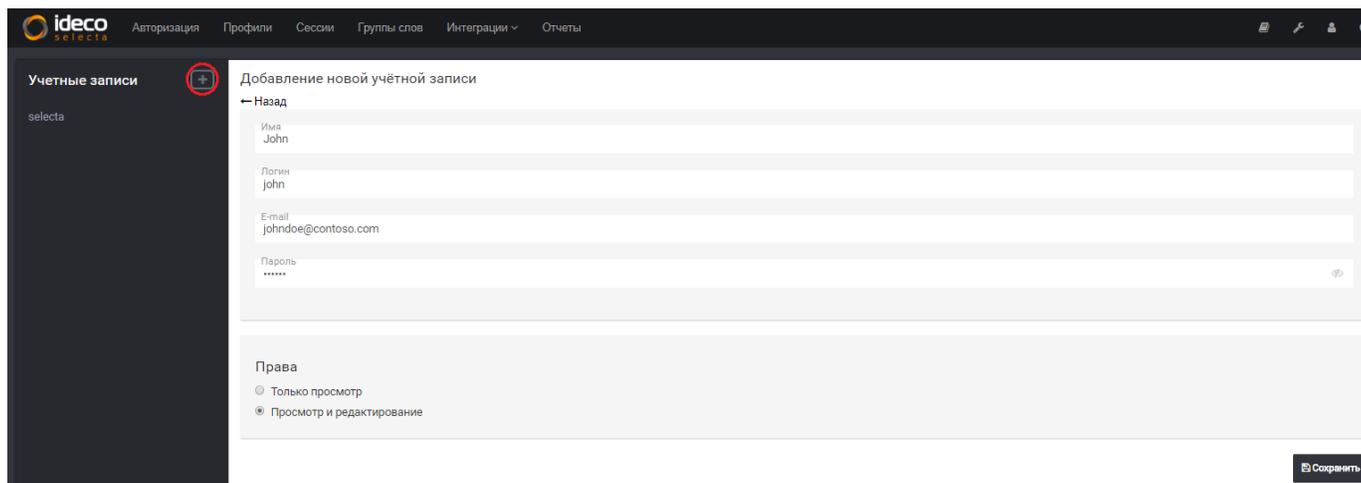
Время	Пользователь	Домен	Категории	Причина блокировки
8 августа 2018 г.				
14:01:50	auth-dc 192.168.0.2	clients2.google.com	Поисковые системы	
12:02:06	auth-dc 192.168.0.2	update.googleapis.com	Технологии (в целом)	
7 августа 2018 г.				
14:09:35	Михаил Демин 192.168.0.3	clients5.google.com	Поисковые системы	
14:01:50	auth-dc 192.168.0.2	clients5.google.com	Поисковые системы	
12:47:31	Михаил Демин 192.168.0.3	update.googleapis.com	Технологии (в целом)	
12:47:03	auth-dc 192.168.0.2	update.googleapis.com	Технологии (в целом)	
12:39:02	auth-dc 192.168.0.2	clients2.google.com	Поисковые системы	
12:38:50	Михаил Демин 192.168.0.3	clients2.google.com	Поисковые системы	
6 августа 2018 г.				
12:38:50	auth-dc 192.168.0.2	clients5.google.com	Поисковые системы	
12:38:49	auth-dc 192.168.0.2	update.googleapis.com	Технологии (в целом)	
12:38:31	Михаил Демин 192.168.0.3	clients5.google.com	Поисковые системы	
12:38:28	Михаил Демин 192.168.0.3	update.googleapis.com	Технологии (в целом)	
12:30:55	auth-dc 192.168.0.2	clients2.google.com	Поисковые системы	

Учетные записи

В данном разделе можно настроить учетные записи администраторов сервера.

Возможны следующие параметры доступа для администраторов:

- Только просмотр - режим "только для чтения";
- Просмотр и редактирование - полный административный доступ в веб-интерфейс.



Настройка фильтрации HTTPS

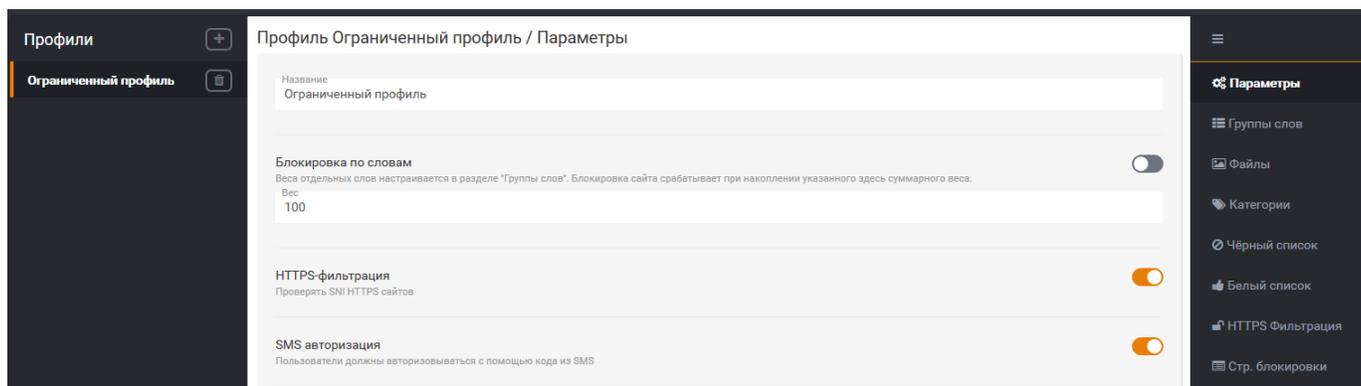
- Настройка сервера Idec Selecta
- Настройка рабочей станции пользователя
- Добавление сертификата через политики домена Microsoft Active Directory.
- Исключения Интернет-сервисов из фильтрации HTTPS

Фильтрация HTTPS-трафика обеспечивает возможность обработки сервером сайтов, доступных по HTTPS. Фильтрация реализуется следующими методами:

- Проверкой SNI HTTPS-сайта (при этом системе контентной фильтрации будет доступно только доменное имя сайта). Данный способ не требует установки доверенного сертификата на клиентские устройства.
- Путём подмены "на лету" сертификата, которым подписан запрашиваемый сайт. Оригинальный сертификат сайта подменяется новым, подписанным не центром сертификации, а корневым сертификатом Idec Selecta. Таким образом, передающийся по HTTPS-соединению трафик становится доступным для обработки контент-фильтром Idec Selecta. Специфика реализации данного метода фильтрации HTTPS-трафика требует настройки обеих сторон подключения: сервера Idec Selecta и рабочей станции каждого пользователя в локальной сети.

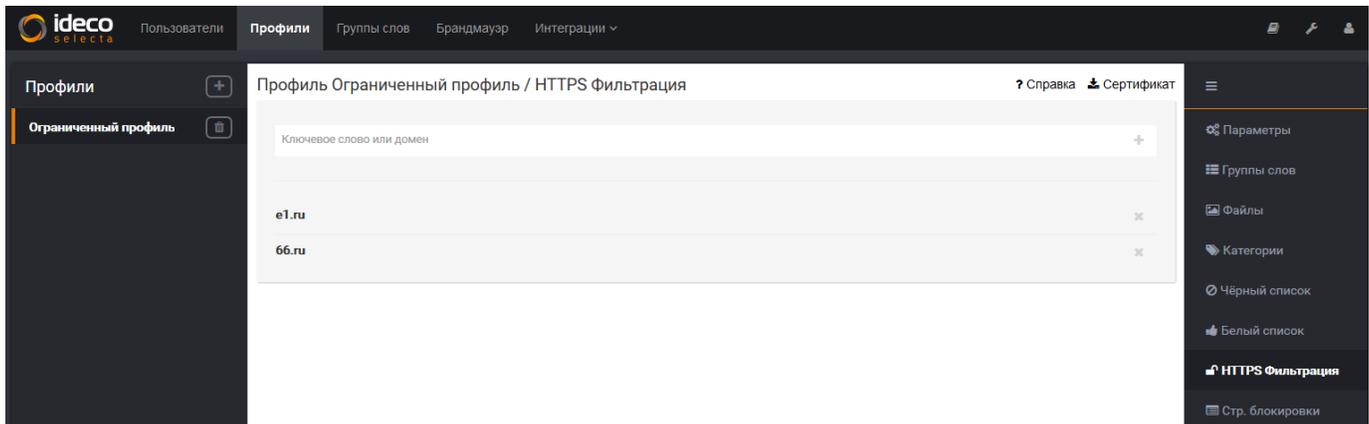
Настройка сервера Idec Selecta

Настройки фильтрации HTTPS находятся в профилях.



Переключатель "HTTPS Фильтрация" включает SNI-фильтрацию HTTPS-трафика на сервере.

В разделе HTTPS Фильтрация настраивается список доменов для полной фильтрации с подменой сертификатов:

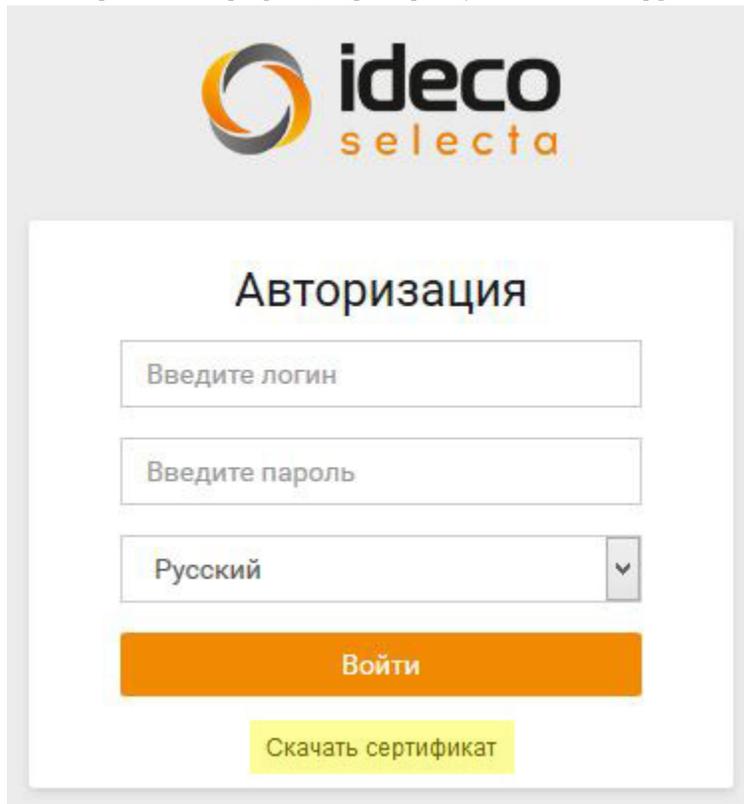


Настройка рабочей станции пользователя

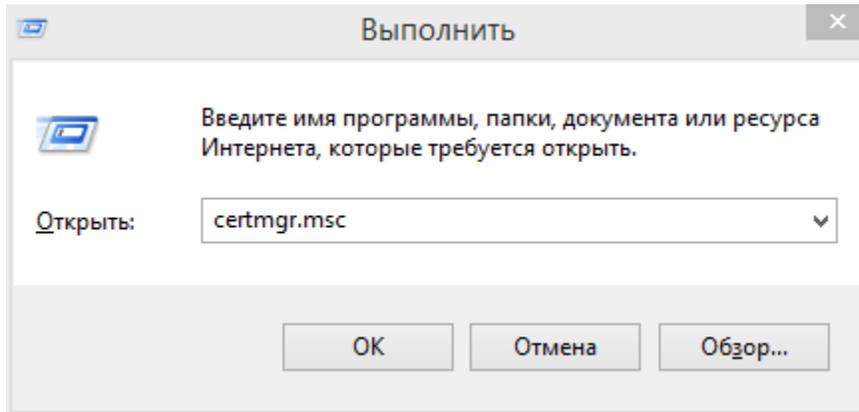
При включенной фильтрации HTTPS-трафика с использованием подмены сертификата, браузер и другое сетевое ПО (например антивирусы, клиенты IM и пр.) на рабочей станции пользователя потребует явного подтверждения на использование подменного сертификата, созданного и выданного сервером Idec Selecta. Для повышения удобства работы пользователя следует установить в операционную систему рабочей станции корневой сертификат сервера Idec Selecta и сделать его доверенным. Корневой SSL-сертификат доступен для скачивания со страницы логина в панели управления сервером.

Чтобы установить корневой сертификат на рабочей станции пользователя (с установленной ОС Windows) требуется выполнить следующие действия:

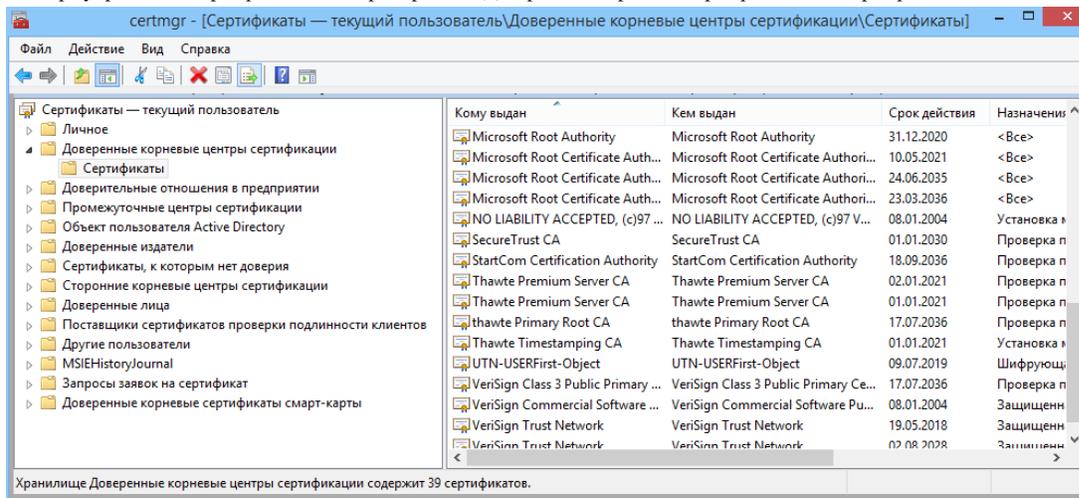
1. Скачать корневой SSL-сертификат, открыв страницу логина в web-интерфейсе панели управления сервера Idec Selecta:



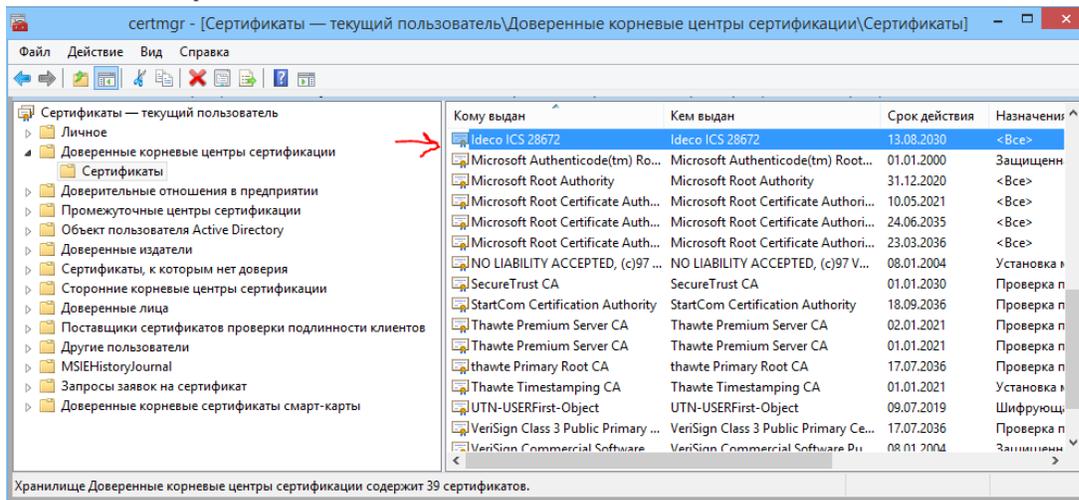
2. Открыть центр управления сертификатами с помощью меню "Пуск" - "Запустить", выполнив в диалоге команду certmgr.msc:



3. В центре управления сертификатами выбрать раздел "Доверенные корневые сертификаты" - "Сертификаты":



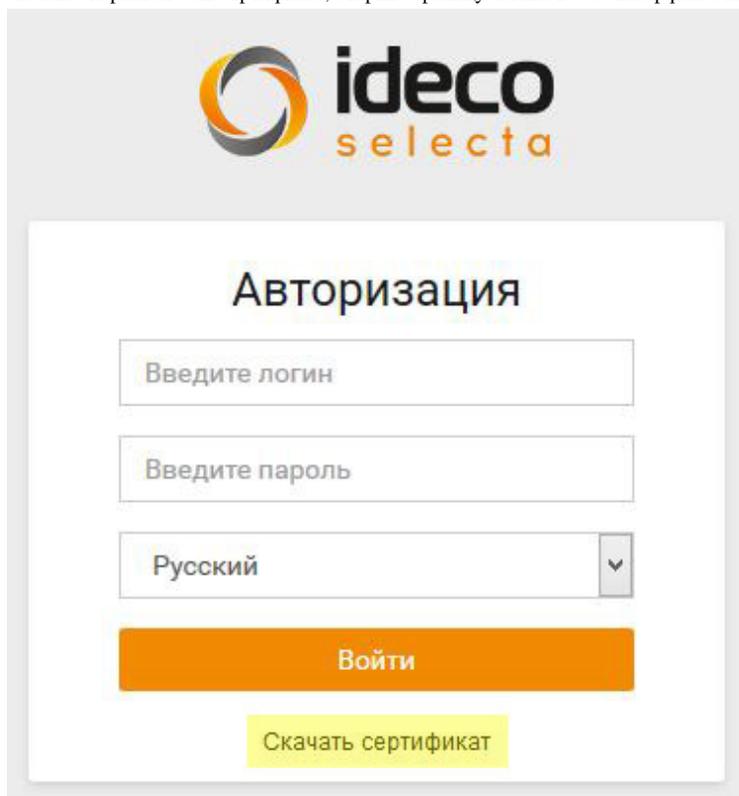
4. В правой части окна нажать правую кнопку мыши и выбрать действие "Все задачи" - "Импорт...". Откроется окно мастера импорта сертификатов. Следуя инструкциям мастера, импортировать корневой сертификат сервера Ideco Selecta. Импортированный сертификат появится в списке в правой части окна.



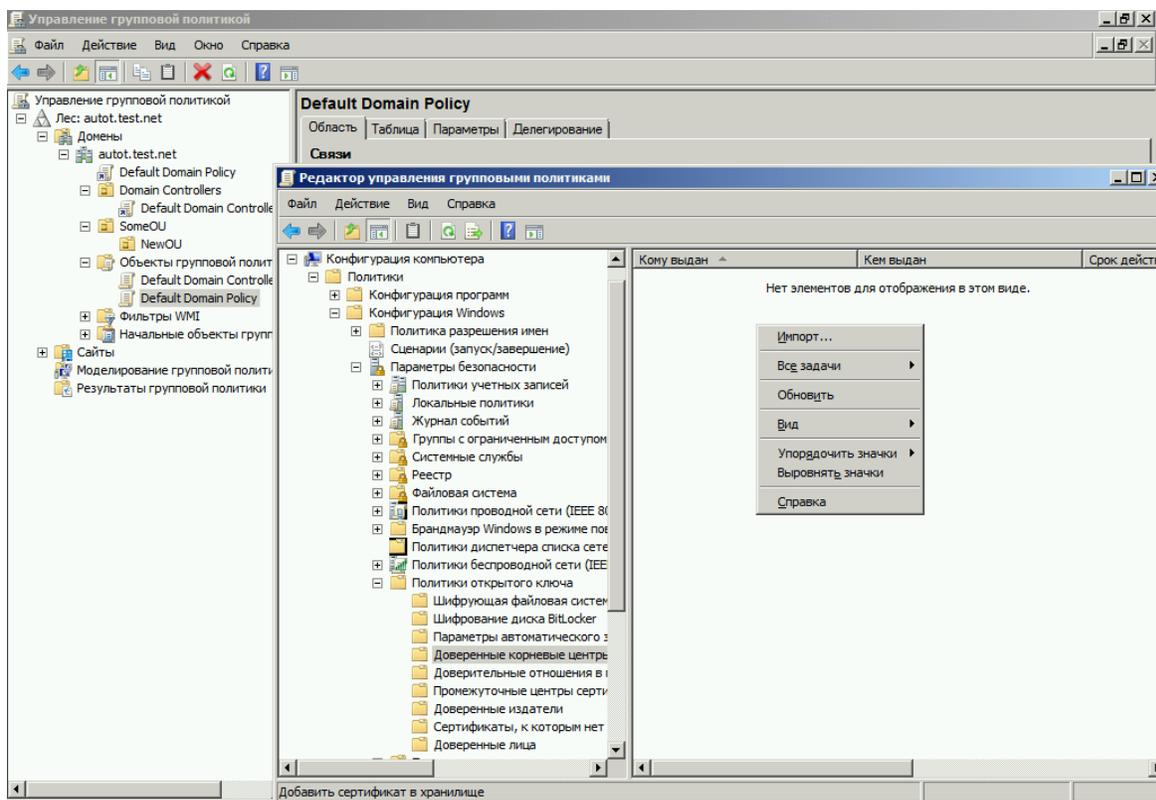
Добавление сертификата через политики домена Microsoft Active Directory.

В сетях, где управление пользователями осуществляется с помощью Microsoft Active Directory, вы можете установить сертификат Ideco Selecta для всех пользователей автоматически с помощью Active Directory.

1. Скачайте корневой SSL-сертификат, открыв страницу логина в web-интерфейсе панели управления сервера Ideco Selecta:



2. Зайдите на контроллер домена с помощью аккаунта, имеющего права администратора домена.
3. Запустите оснастку управления групповой политикой, выполнив команду `grpms.msc`.
4. Найдите политику домена, использующуюся на компьютерах пользователей в "Объектах групповой политики" (на скриншоте - Default Domain Policy).
Нажмите на нее правой кнопкой мышки и выберите "Изменить".
5. В открывшемся редакторе управления групповыми политиками выберите:
Конфигурация компьютера - Политики - Конфигурация Windows - Параметры безопасности - Политики открытого ключа - Доверенные корневые центры сертификации.
6. Нажмите правой кнопкой мыши по открывшемуся списку, выберите "Импорт..." и импортируйте ключ Ideco Selecta.



- После перезагрузки рабочих станций или выполнения на них команды `gpupdate /force` сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Исключения Интернет-сервисов из фильтрации HTTPS

Некоторые сервисы в Интернет не работают если их HTTPS трафик расшифровывать. Чтобы они продолжили работать а остальной HTTPS трафик в Интернет продолжал расшифровываться, нужно исключать домены этих служб из расшифровки HTTPS:

Для работы клиента dropbox нужно добавить следующие URL в белый список:
client.dropbox.com - для работы клиента

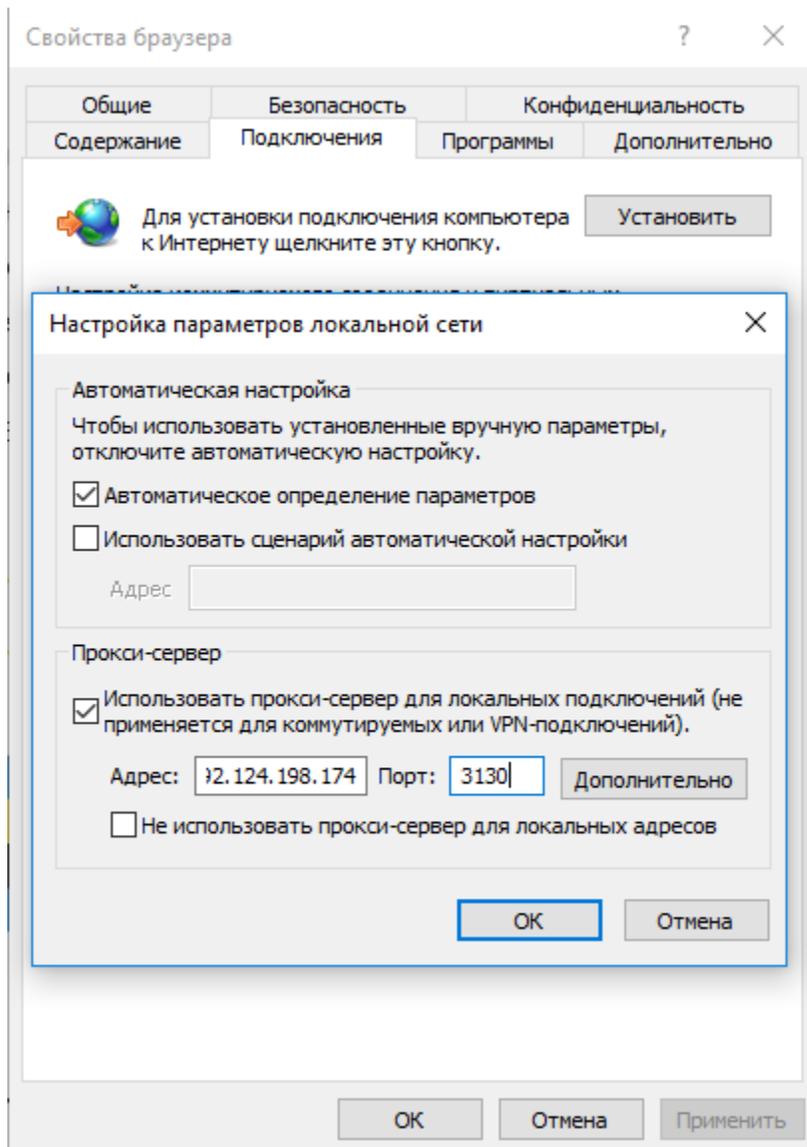
dropboxstatic.com - для возможности загрузки файлов из облака

Для работы yandex диск:

push.yandex.ru - чтобы работала синхронизация

Настройка прямых подключений к прокси-серверу

Для прямых подключений к прокси-серверу по HTTP/HTTPS необходимо настроить в браузере подключение к Selecta по порту 3130. Например, в Internet Explorer:



Если настроена интеграция с Active Directory, то для прямых подключений можно использовать порт, указанный в параметрах интеграции, при этом будет использоваться прозрачная авторизация по Kerberos-токенам (negotiate-авторизация).

Настройка интеграции с Active Directory

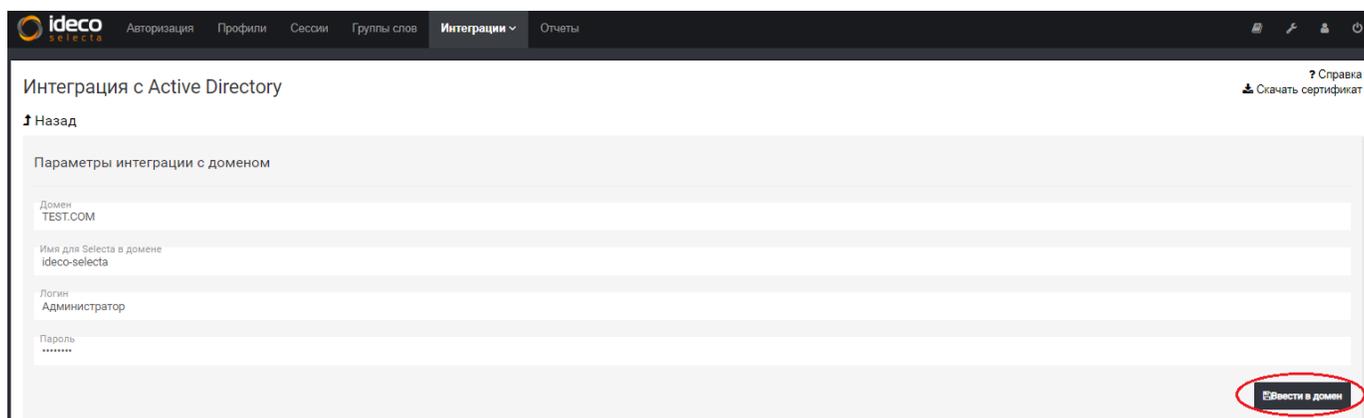
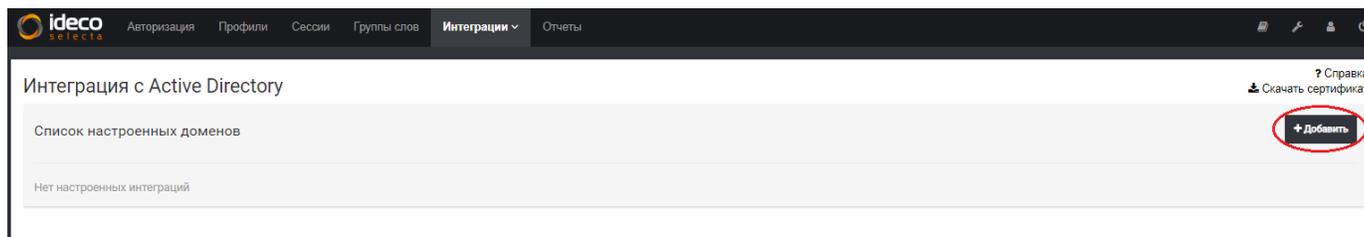
Для корректной работы интеграции нужно обеспечить следующие условия:

1. Время на всех машинах, которые участвуют в интеграции (в т.ч. и клиентские машины), должно быть синхронизировано. Разница не должна превышать 5 минут (требование для работы kerberos);
2. В сети работает один или несколько DNS-серверов, которые доступны всем участникам интеграции (требование для работы kerberos).

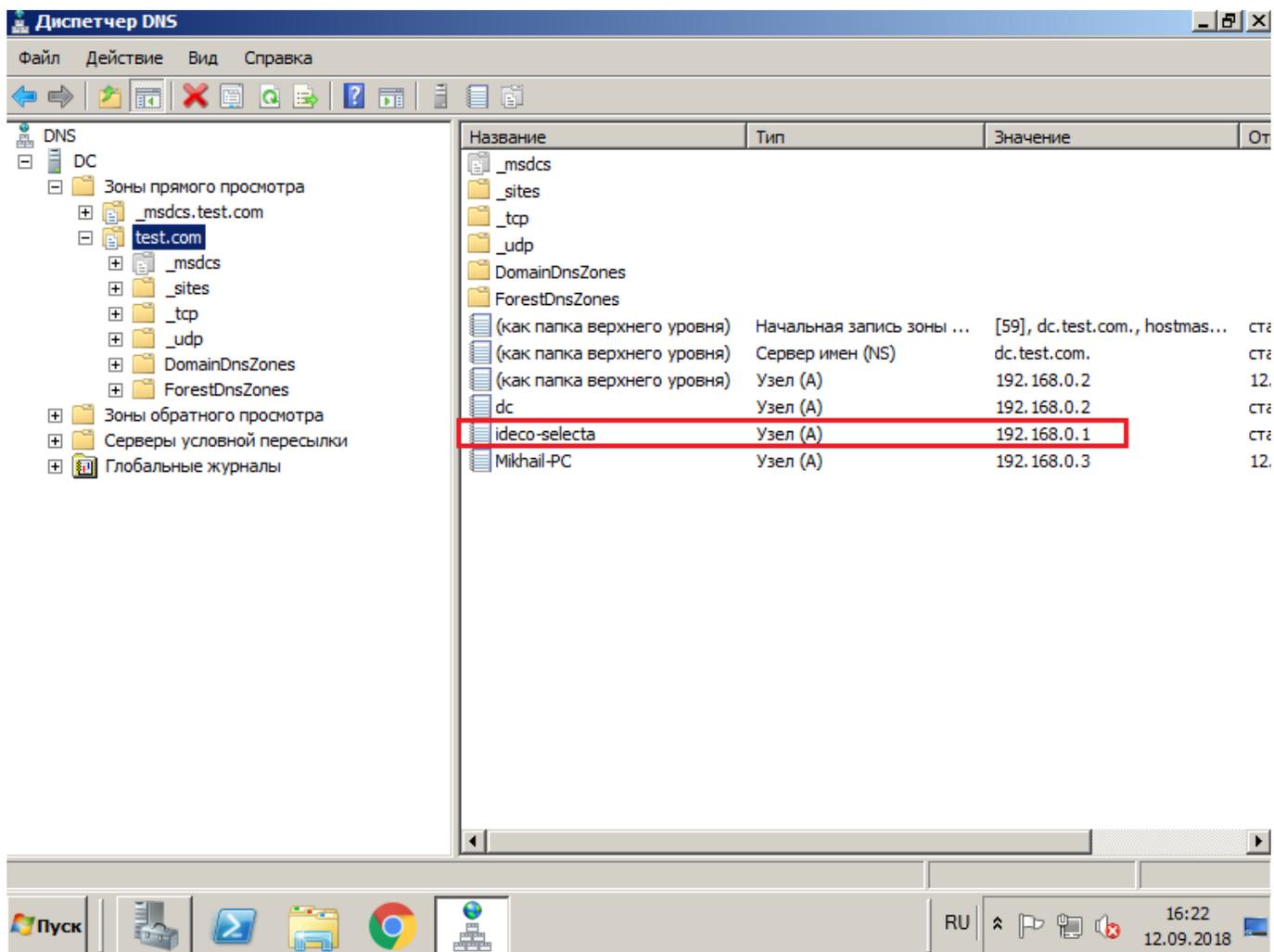
Настройка включает в себя следующие этапы:

1. В веб-интерфейсе в разделе "Настройки - Сетевые настройки" нужно указать основным DNS сервер, на котором в зоне прямого просмотра должна быть А-запись о контролере домена, с которым необходима интеграция, чтобы система могла обнаружить контролер домена, и работал Kerberos.
2. В веб-интерфейсе перейти в Интеграции -> Active Directory и нажать кнопку Добавить для добавления нового домена. При этом указать:
 - Домен, с которым происходит интеграция (например domain.com);
 - Имя компьютера для Selecta в домене (например ideco-selecta);
 - Логин и пароль пользователя AD с правами ввода машины в домен.

Нажать Ввести в домен:



3. На контроллере домена создать в DNS А-запись для Selecta:

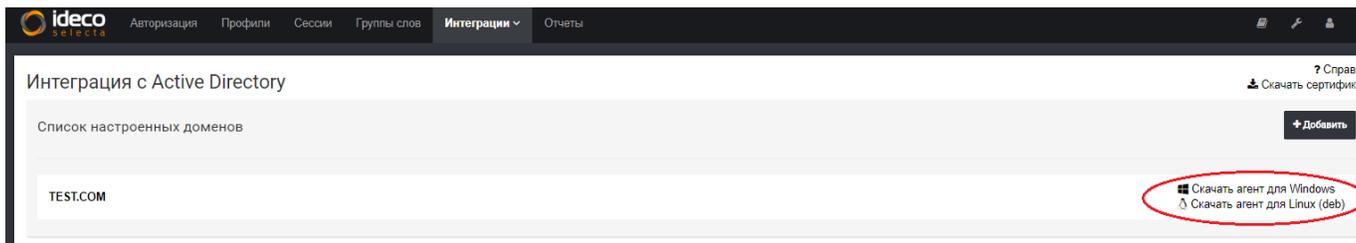


4. После добавления домена на этой же странице появится раздел Профили фильтрации групп безопасности, в котором нужно нажать кнопку Обновить

для импорта групп из AD. Получив список групп, здесь же нужно назначить на них профили для фильтрации, после чего нажать Сохранить:



5. На клиентские машины необходимо скачать и установить Ideco Agent, ссылка на него доступна на странице с общим списком доменов:



Агент может быть также установлен через групповую политику. В любом случае после установки необходимо перезагрузить клиентскую машину. После перезагрузки агент автоматически запустится, и пользователь будет авторизован.

Для каждого домена используется отдельный экземпляр агента.

6. Если пользователь, из под которого запущен агент является доменным, то авторизация должна произойти автоматически. Если пользователь локальный - то покажется окно ввода логина и пароля, куда нужно ввести логин и пароль пользователя AD.

Настройка выгрузки групп безопасности и пользователей из конкретного OU:

Для того, чтобы в разделе "Профили фильтрации групп безопасности" были выведены группы безопасности только из определенного OU, необходимо в разделе "Настройки подключения" указать контролер домена и OU для загрузки групп безопасности, после чего нажать "Сохранить и показать":



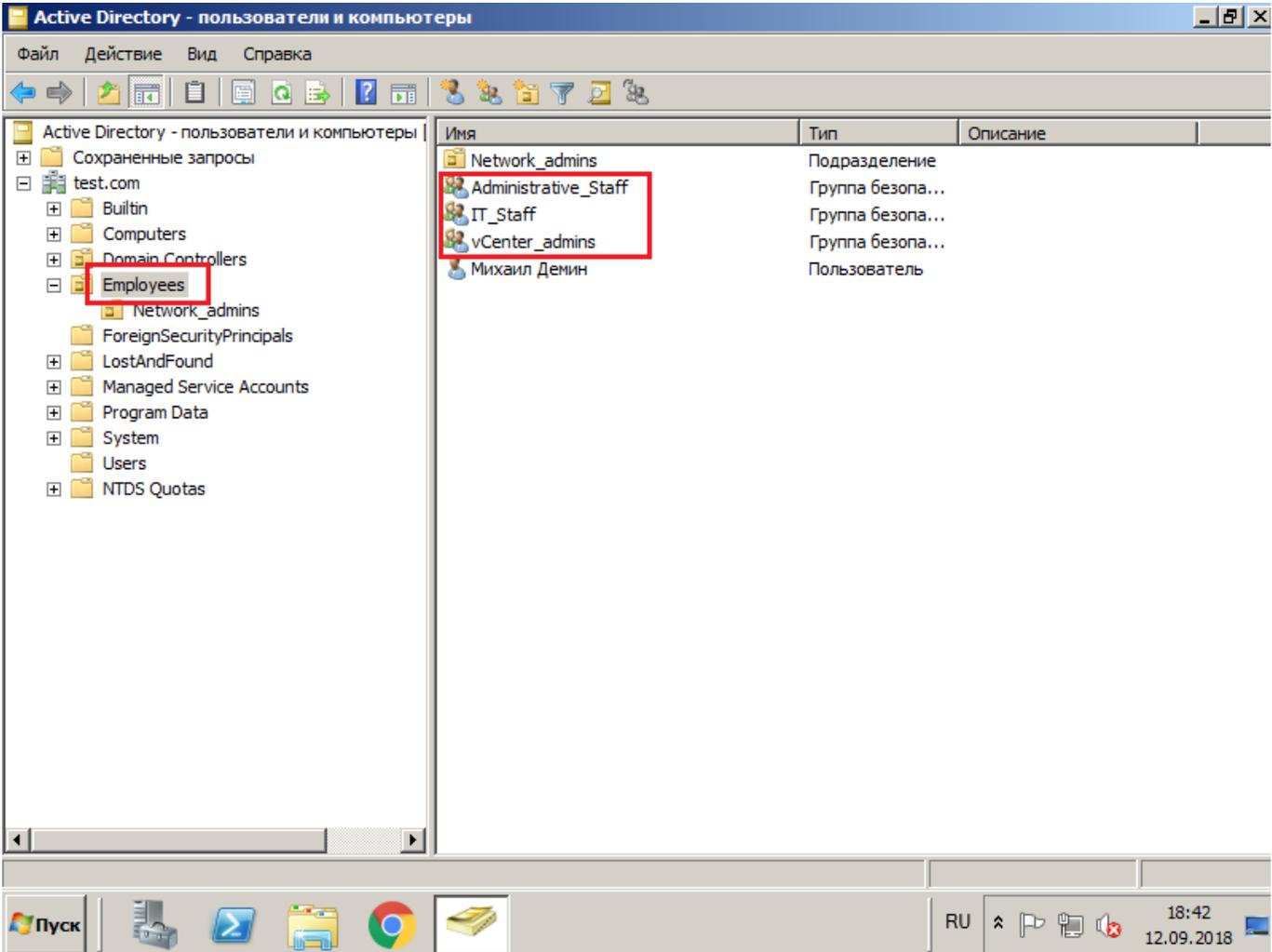
Таким образом, в профилях фильтрации будут выгружены группы безопасности из указанного и вложенных в него OU:

Профили фильтрации групп безопасности

Поиск

Administrative_Staff	Выберите профиль для фильтрации
vCenter_admins	Выберите профиль для фильтрации
IT_Staff	Выберите профиль для фильтрации

В этом можно убедиться, посмотрев группы в ADUC:



Для того, чтобы выгрузить группы безопасности только из вложенной OU, необходимо в разделе "Настройки подключения" в поле "OU для загрузки групп безопасности" указать имя вышестоящей OU и вложенной через ",":

Настройки подключения

Контроллер домена
dc.test.com

OU для загрузки групп безопасности
Employees,Network_admins

OU для загрузки пользователей

Показывать группы по шаблону

Допускается добавление знака *. В этом случае будут показаны группы, в которых присутствуют символы до/после *.

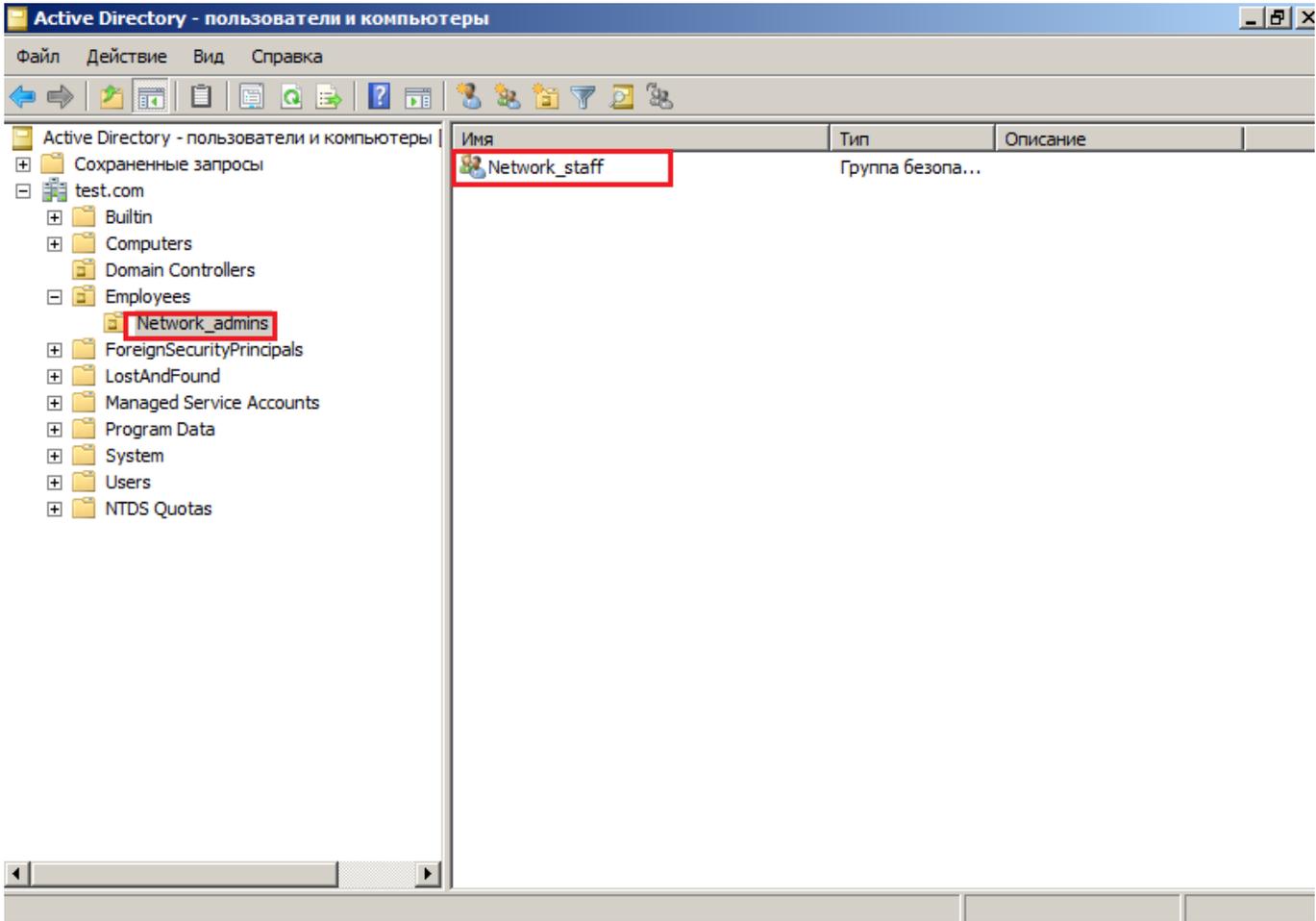
Таким образом, в профилях фильтрации будут выгружены группы безопасности только из вложенной OU:

Профили фильтрации групп безопасности

Поиск

Network_staff Выберите профиль для фильтрации ▾

В этом можно убедиться, посмотрев группы в ADUC:



Настройка выгрузки информации о пользователях из определенной OU аналогична настройке выгрузки групп. В этом случае нужно изменить значение поля "OU для загрузки пользователей". Ниже пример настройки выгрузки информации о пользователе из вложенной OU:

Настройки подключения

Контроллер домена
dc.test.com

OU для загрузки групп безопасности

OU для загрузки пользователей
Employees,Network_admins

Показывать группы по шаблону

Допускается добавление знака *. В этом случае будут показаны группы, в которых присутствуют символы до/после *.

Инструменты

Обновить профиль авторизованных пользователей

Проверить пользователя
johndoe

Поле	Значение
userPrincipalName	johndoe@test.com
sAMAccountName	johndoe
Фильтрация основанная на группах безопасности	Пользователи домена

Такой пользователь действительно есть в AD:

Active Directory - пользователи и компьютеры

Файл Действие Вид Справка

Active Directory - пользователи и компьютеры

Имя	Тип	Описание
John Doe	Пользователь	
Network_staff	Группа безопа...	

test.com

- Builtin
- Computers
- Domain Controllers
- Employees
- Network_admins
- ForeignSecurityPrincipals
- LostAndFound
- Managed Service Accounts
- Program Data
- System
- Users
- NTDS Quotas

Настройка отображения групп по шаблону

Можно также выводить группы, содержащие определенные слова в названии. Для этого нужно заполнить поле "Показывать группу по шаблону". Можно выполнить вывод групп по словесной маске, используя символ "*" до/после слова:

Настройки подключения

Контроллер домена
dc.test.com

OU для загрузки групп безопасности

OU для загрузки пользователей

Показывать группы по шаблону
vCenter*

Допускается добавление знака *. В этом случае будут показаны группы, в которых присутствуют символы до/после *.

Сохранить и показать

Как видим, в вывод попали только группы, соответствующие словесной маске. Убедимся в этом:

Профили фильтрации групп безопасности

Поиск

vCenter_admins

Выберите профиль для фильтрации

Обновить Сохранить

Настройка веб-авторизации в Active Directory

1) Настроить интеграцию с Active Directory в соответствующем разделе:

ideco selecta

Авторизация Профили Сессии Группы слов **Интеграции** Отчеты

Интеграция с Active Directory

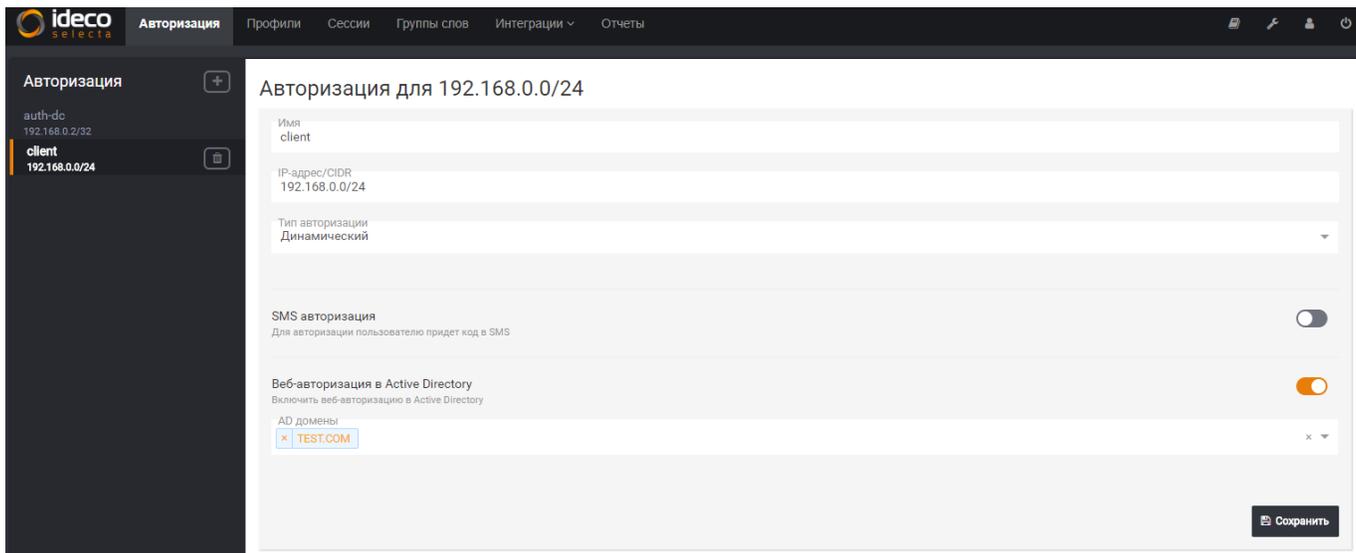
Справка
Скачать сертификат

Список настроенных доменов

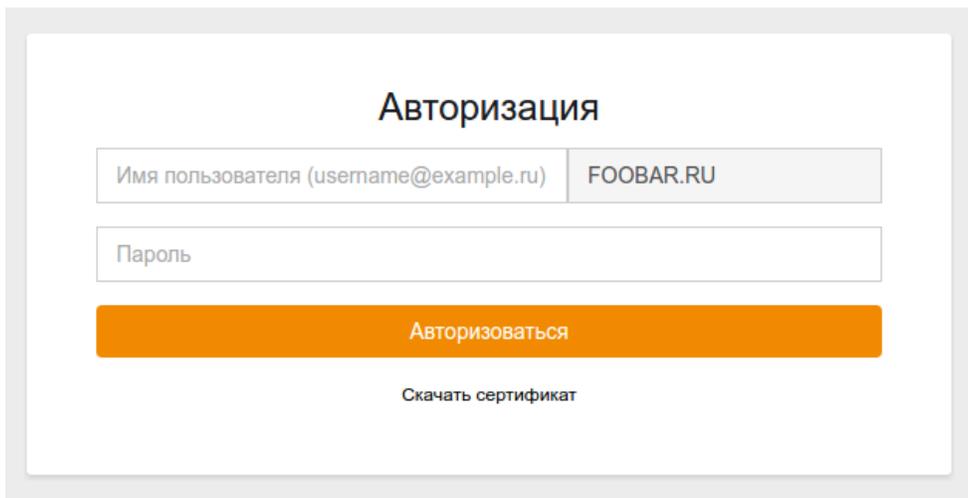
+ Добавить

TEST.COM	Скачать агент для Windows Скачать агент для Linux (deb)
----------	--

2) Создать авторизацию в соответствующем разделе: указать сегмент сети, пользователей из которого требуется авторизовать; указать тип авторизации "Динамическая"; включить веб-авторизацию, указав домен; нажать "Сохранить":



3) На стороне клиента пройти авторизацию с указанием логина/пароля от его доменной учетной записи:



Веб-авторизация в Active Directory и SMS-авторизация пользователя могут быть настроены параллельно, тогда пользователь выбирает способ авторизации.

При авторизации через AD конкретный профиль фильтрации будет вычислен на основе групп безопасности, в которых состоит пользователь.

Интеграция с AD, авторизация на базе логов безопасности

Принцип работы

Авторизация пользователей на базе логов возможна при интеграции с Windows Server начиная с версии 2003.

Общий принцип работы: Selecta периодически выкачивает и анализирует логи безопасности Active Directory. На основе полученных из логов данных строит следующие таблицы:

1. Имя компьютера → логин пользователя, который последним прошёл вошел в систему на данном компьютере;
2. Имя компьютера → IP-адрес.

При входе пользователя в систему, в Selecta создаётся новая сессия в которую заносится:

1. IP-адрес компьютера, с которого осуществлен вход в систему;
2. Информация о пользователе (из LDAP);
3. Профиль фильтрации, вычисленный на основе групп безопасности, в которых состоит пользователь.

После создания сессии трафик пользователя будет подвержен фильтрации в соответствии с профилем фильтрации.

Список обрабатываемых событий

- Логин пользователя на компьютере, на котором никто не зарегистрирован: будет создана новая сессия;
- Логин пользователя на компьютере, на котором уже кто-то зарегистрирован: сессия предыдущего пользователя будет удалена, будет создана сессия для нового пользователя;
- Администратор пытается войти в систему, за которой никто не зарегистрирован: будет создана сессия для администратора.
- Администратор пытается войти в систему, за которой уже кто-то зарегистрирован: событие будет расценено, как попытка выполнить действия с правами администратора и сессия предыдущего пользователя изменена не будет.
- Во время работы пользователя были выполнены действия от имени администратора: сессия пользователя не изменится.
- Пользователь был переключен: сессия для компьютера будет замена сессией для нового пользователя.
- IP-адрес компьютера изменён (по DHCP, или вручную): у текущей сессии пользователя будет изменен IP-адрес.

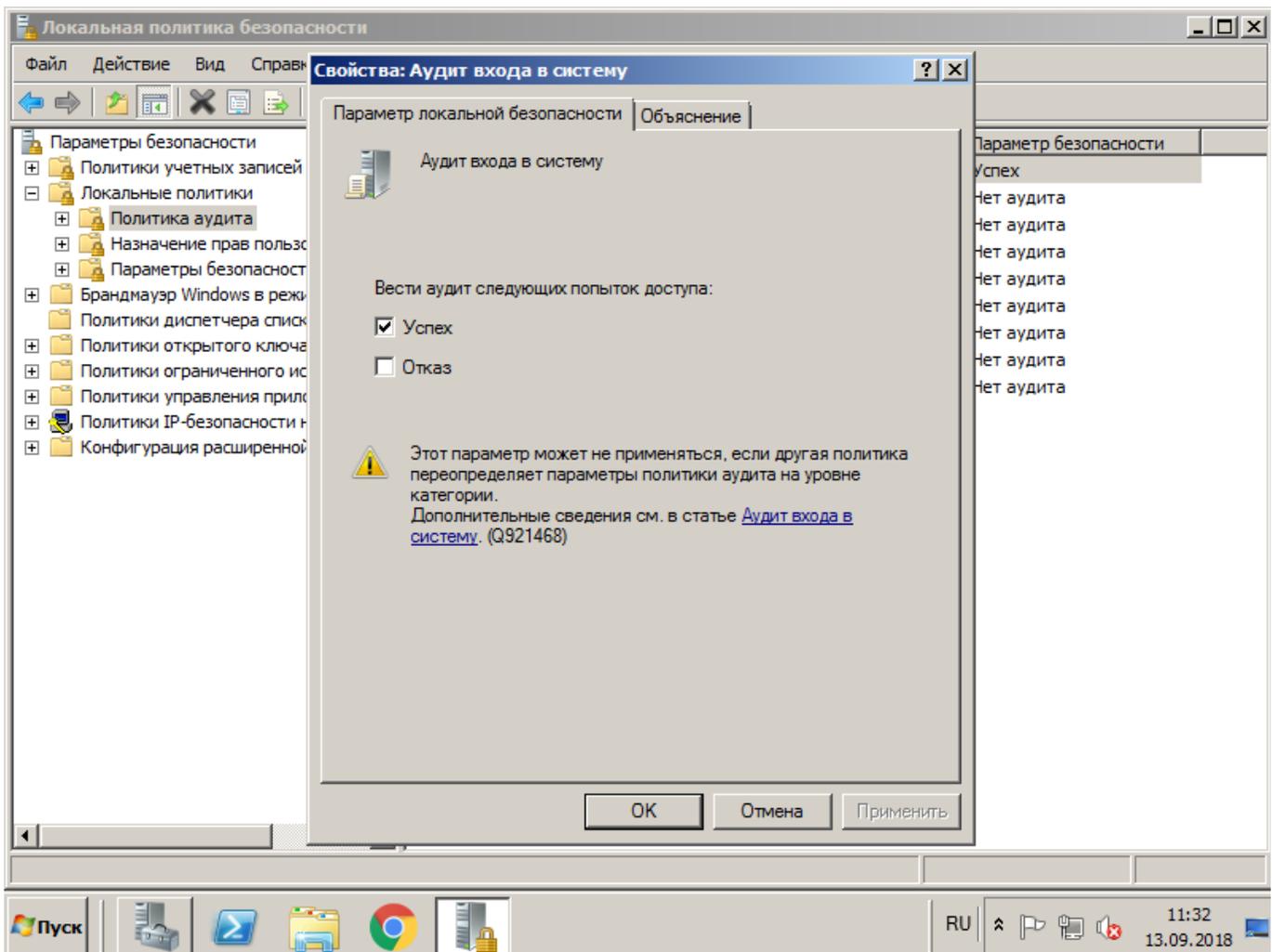
Настройка

Настройка включает в себя следующие шаги:

1. Настройка аудита входов в систему на AD сервере;
2. Настройка пользователя WMI;
3. Настройка интеграции с Active Directory на Selecta.

Настройка аудита входов в систему

1. Открыть редактор групповых политик: Пуск → Администрирование → Локальная политика безопасности (или Выполнить → gpedit.msc в Windows);
2. Перейти в Локальные политики → Политика аудита;
3. Для политики Аудит входа в систему включить ведение аудита доступа: Успех.



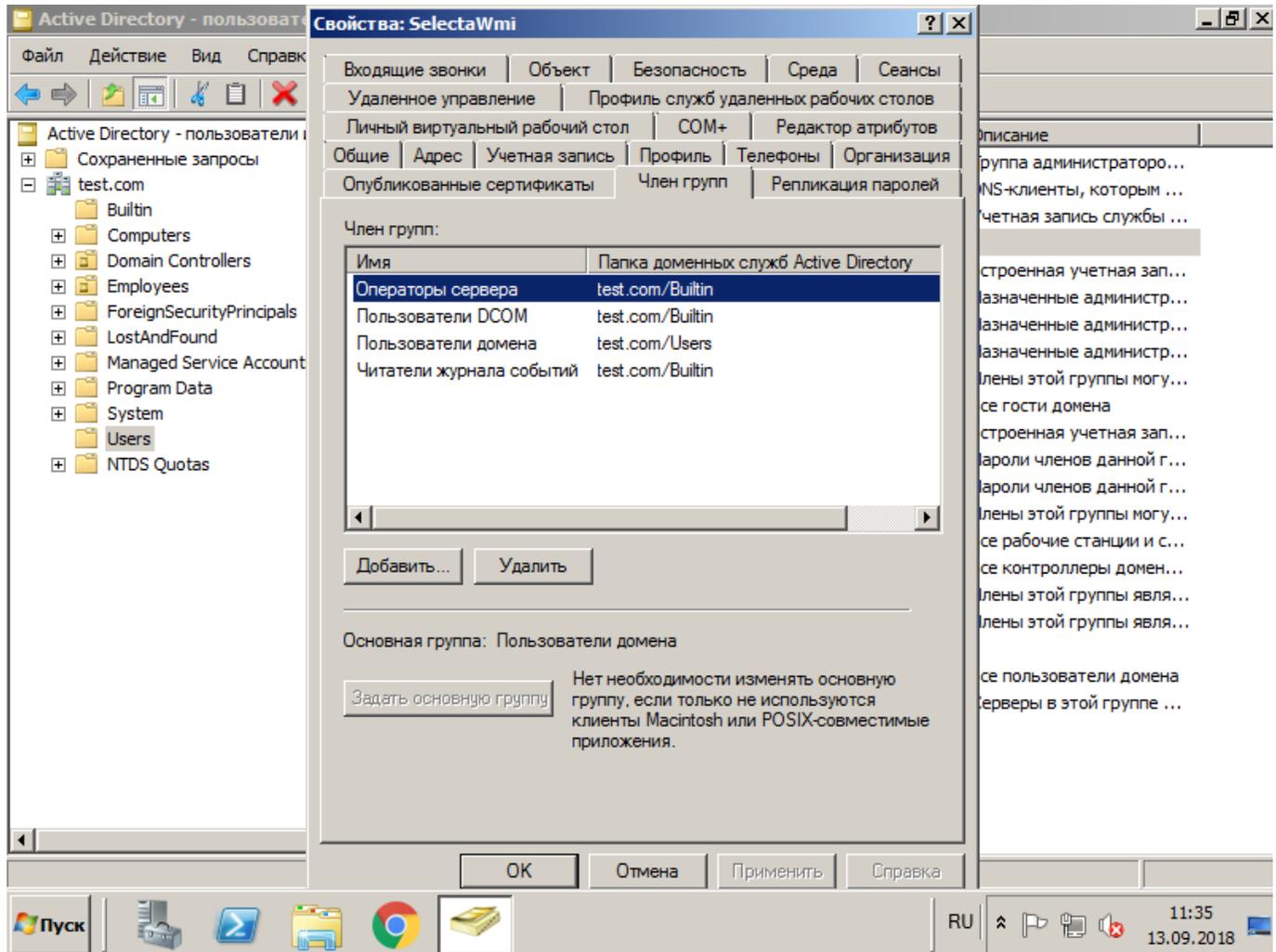
Теперь в журналах безопасности Windows будут сохраняться логи аудита пользовательского входа в систему. Для просмотра и настройки необходимо перейти в Просмотр событий → Журналы Windows → Безопасность.

Настройка пользователя WMI

Создайте новую учетную запись пользователя в AD. Созданного пользователя нужно добавить в следующие группы безопасности:

- Пользователи DCOM;
- Читатели журнала событий;
- Операторы сервера.

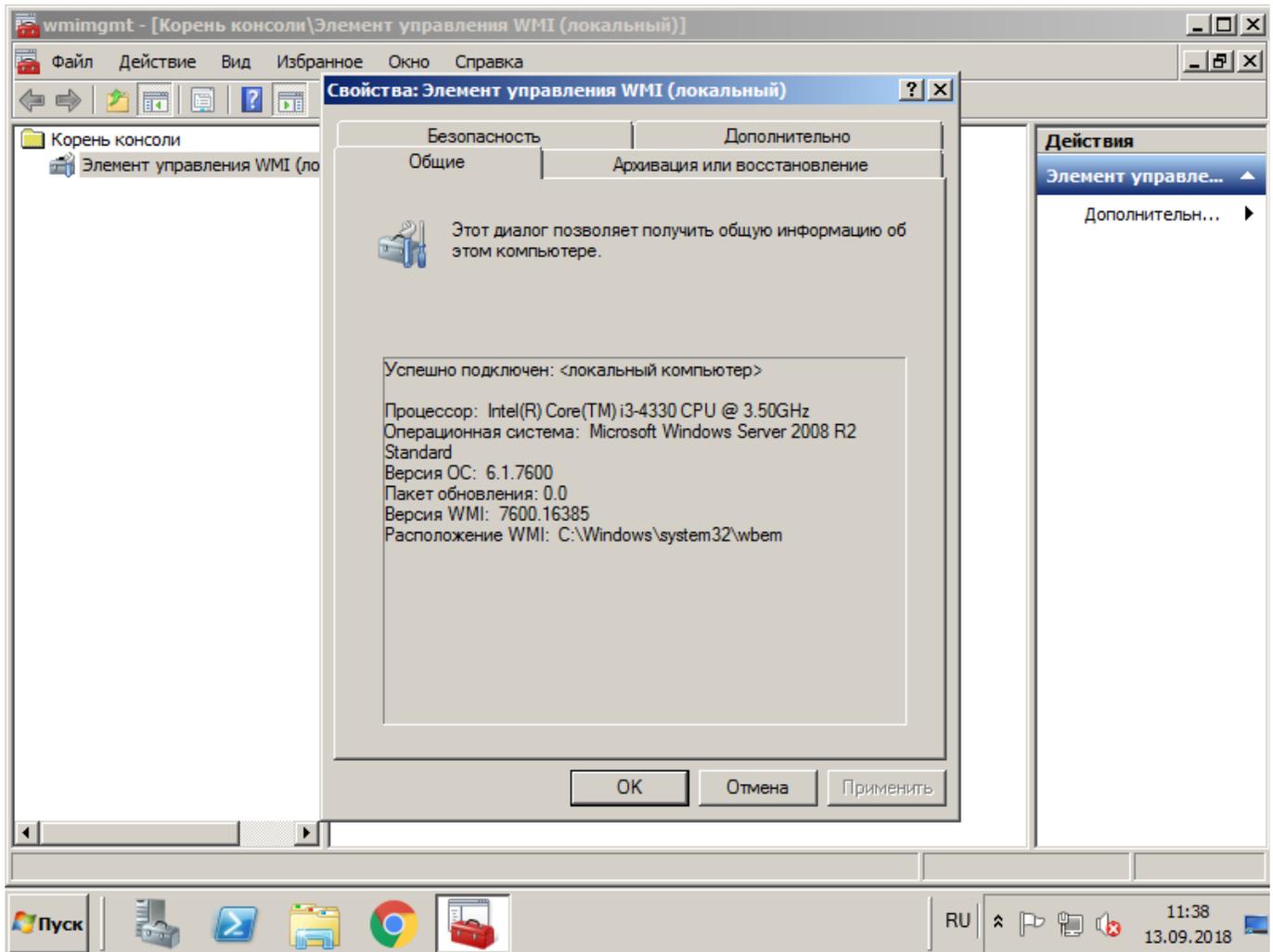
Для правильной работы учетной записи службы идентификатора пользователя не требуются привилегии администратора домена. Исключение составляет Windows 2003, где встроенная группа с именем «Читатели журнала событий» недоступна. Поэтому в данном случае необходимо добавлять пользователя в группу администраторов домена.



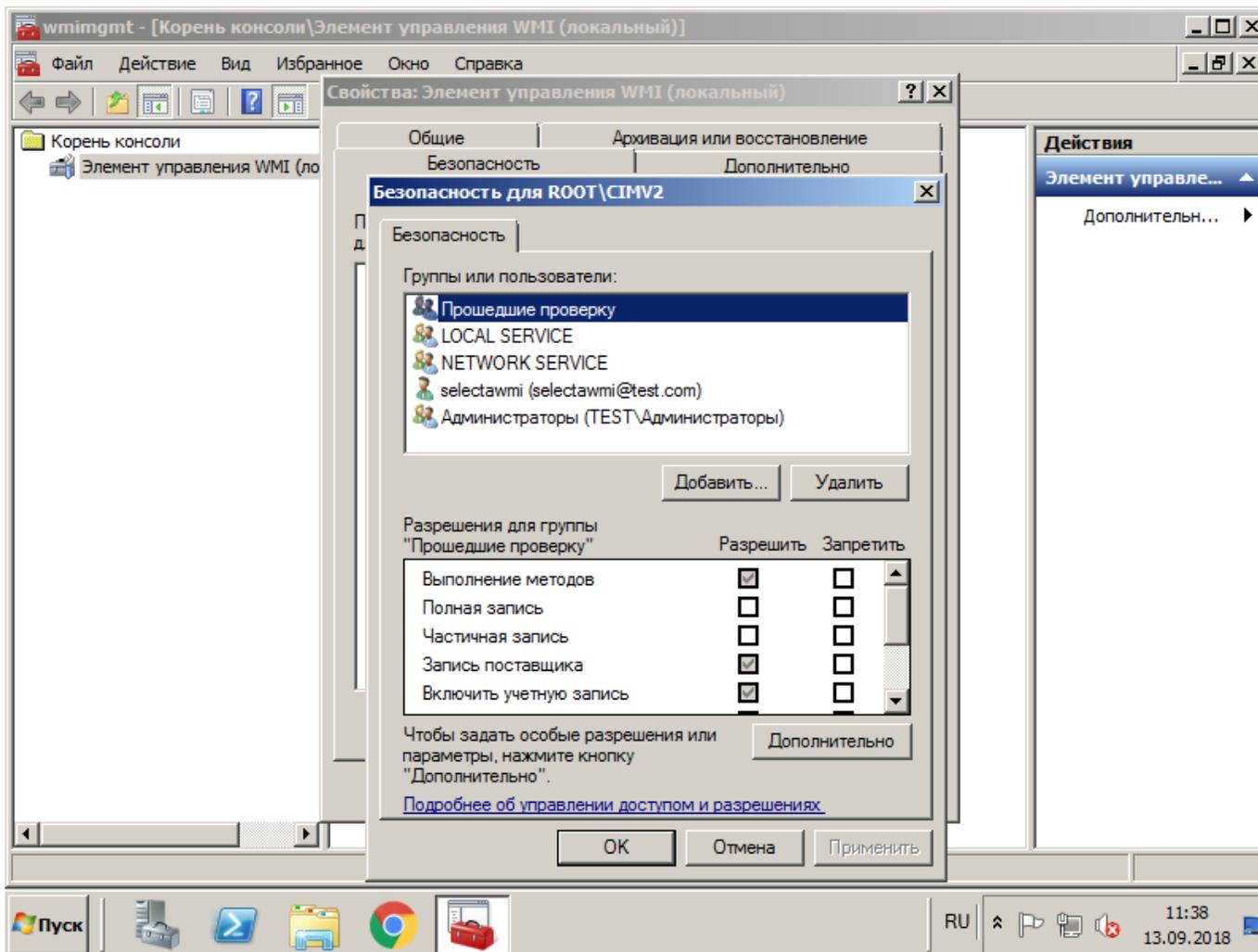
Интеграция использует [WMI Authentication](#), и необходимо изменить свойства безопасности CIMV2 на сервере AD.

Запустите Выполнить → `wmimgmt.msc` в Windows, чтобы открыть консоль:

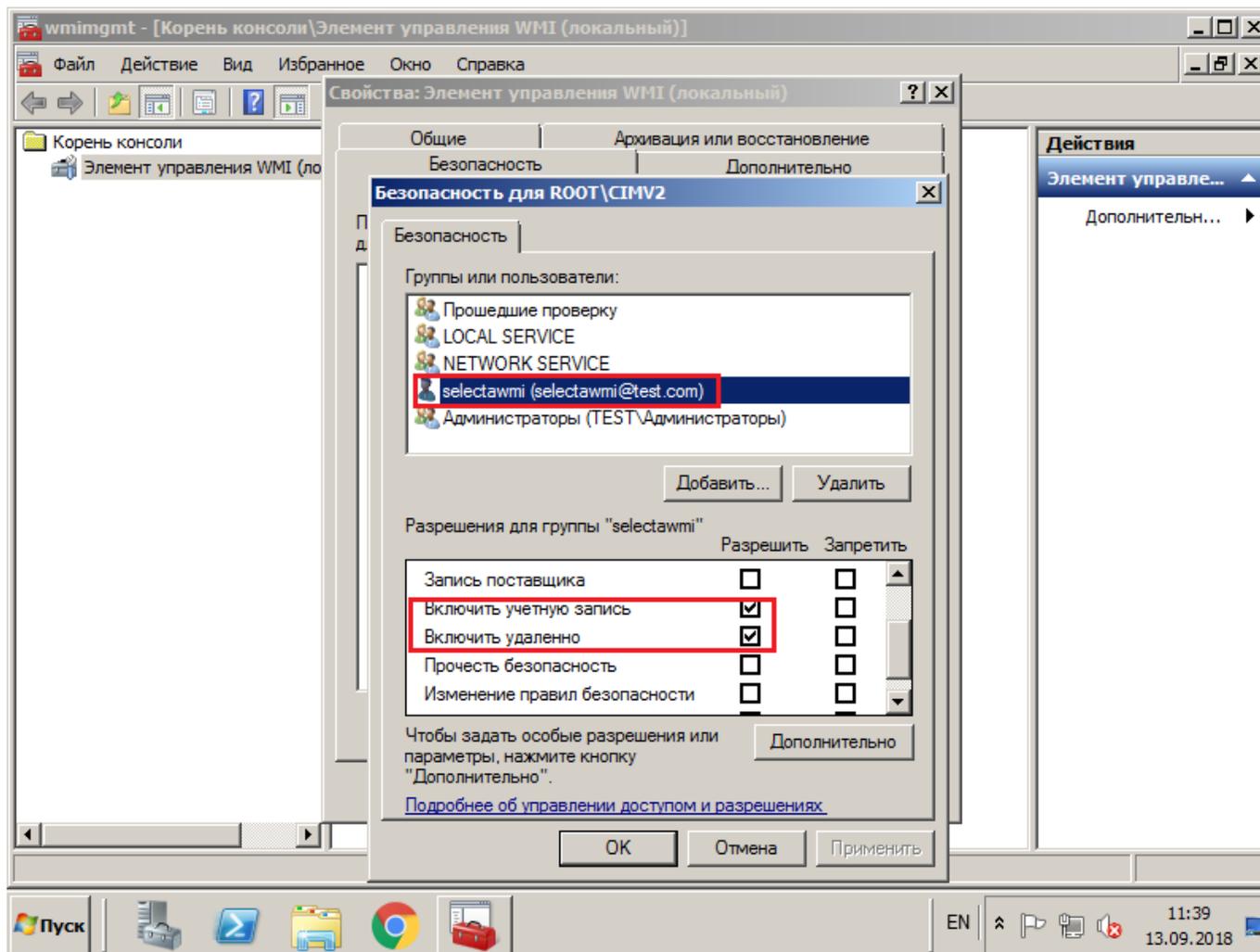
- Нажмите Действие → Свойства;



- Перейдите на вкладку Безопасность;
- Раскройте дерево папок Root Выберите папку CIMV2;
- Нажмите Безопасность;



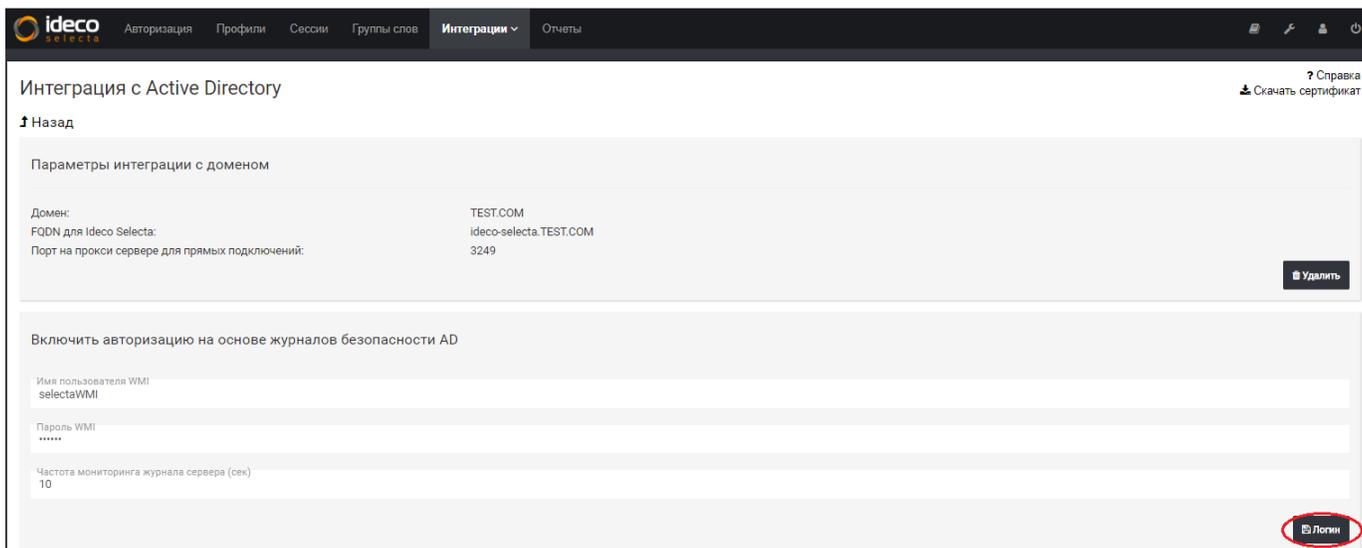
- Нажмите Добавить, а затем выберите ранее созданную учетную запись;
- Для этой учетной записи установите флажки Разрешить для параметров Включить учетную запись и Включить удаленно;



- Затем нажмите OK.

Настройка интеграции с Active Directory

В веб-интерфейсе Selecta в меню Интеграции → Active Directory необходимо перейти в уже добавленный домен и ввести данные созданной ранее учетной записи WMI (логин и пароль). Так же стоит указать частоту сбора логов с сервера AD. Используйте большие интервалы в случае редких изменений сетевой конфигурации пользовательских компьютеров. После нажать Логин.



После применения настроек начнется сбор и обработка логов.

Настройка SMS-авторизации

Перед началом настройки

Прежде чем приступить к настройке, вы должны получить аккаунт у поставщика услуг по рассылке СМС.

В Idec Selecta предустановлены параметры SMPP для "SMS Центр" и "МТС Коммуникатор". Для остальных поставщиков вы должны получить параметры самостоятельно.

Для настройки авторизации пользователей по SMS перейдите в раздел Интеграции > SMPP.

Параметры СМС-авторизации

? Спра

Параметры протокола SMPP	
Выбрать предустановки	▼
system_id	test
password	*****
source_addr	
host	smpp.smsc.ru
port	3700
source_addr_ton	5
source_addr_npi	1
dest_addr_ton	1
dest_addr_npi	1
<input type="button" value="Сохранить"/>	
Отправить тестовый SMS	
Телефон	
Сообщение	

Параметры протокола SMPP

Отправка СМС-сообщений в Ideco Selecta реализована через протокол SMPP. Доступны предустановки для двух поставщиков услуг – "SMS Центр" и "МТС Коммуникатор", но если вам известны параметры SMPP вашего поставщика услуг, то вы можете использовать их.

Проверка настроек

Для проверки правильности настроек можно воспользоваться формой отправки тестовых СМС-сообщений.

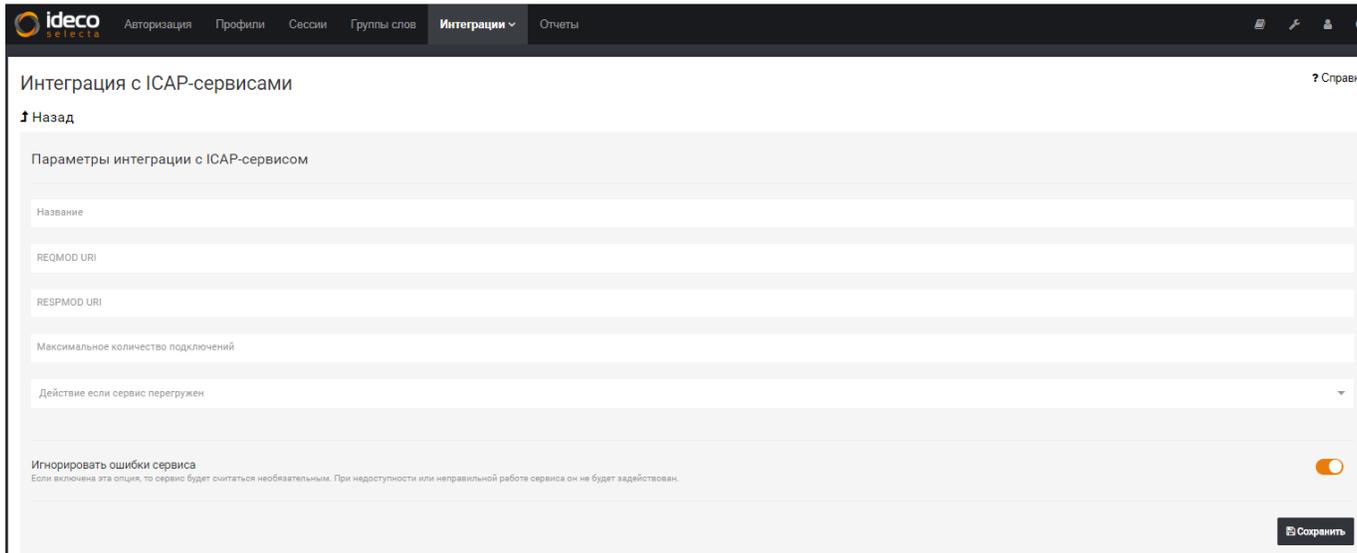
Настройка интеграции с внешними ICAP-сервисами

Существует возможность отправки HTTP(S)-трафика на анализ сторонним серверам по протоколу ICAP.

При этом трафик этим серверам (в роли которых могут быть DLP-системы, антивирусы, веб-фильтры) передается в расшифрованном виде (в случае настройки HTTPS-фильтрации методом подмены сертификата).

Возможно подключение к нескольким внешним серверам.

Настройки подключения к серверам по ICAP находятся на вкладке – ICAP .



Integration with ICAP services

Назад

Параметры интеграции с ICAP-сервисом

Название

REQMOD URI

RESPMOD URI

Максимальное количество подключений

Действие если сервис перегружен

Игнорировать ошибки сервиса

Если включена эта опция, то сервис будет считаться необязательным. При недоступности или неправильной работе сервиса он не будет задействован.

Сохранить

Настройка WCCP

Ideco Selecta поддерживает перенаправление https(s) трафика на себя с устройств Cisco, организованное по протоколу WCCP.

Порядок настройки

Схема сети:

- 192.168.100.0/24 - Локальная сеть
- 192.168.100.1 - IP-адрес Cisco роутера
- 192.168.100.10 - IP-адрес Ideco Selecta
- 10.108.1.1 - Loopback адрес на Cisco для GRE туннеля
- fa0/0 - интерфейс на роутере, который смотрит в Интернет
- fa0/1 - интерфейс на роутере, который смотрит в локальную сеть

Настройка Cisco роутера

1. Настроить сеть на роутере: один порт в интернет, другой в локальную сеть. В локальной сети находятся клиенты и Ideco Selecta
2. Создать Loopback интерфейс, который будет отвечать за GRE туннель

```
cisco> enable
cisco# configure terminal
cisco(config)# interface loopback 1
cisco(config)# ip address 10.108.1.1 255.255.255.255
```

3. Создать ACL со списком адресов WCCP клиентов

```
cisco(config)# access-list 10 permit 192.168.100.10
cisco(config)# ip wccp web-cache group-list 10
```

4. Создать ACL с правилами, по которым роутер будет маршрутизировать трафик на Ideco Selecta

```
cisco(config)# ip access-list extended WCCP_ACCESS
cisco(config-ext-nacl)# remark ACL for HTTP/HTTPS
cisco(config-ext-nacl)# remark Selecta bypass WCCP
cisco(config-ext-nacl)# deny ip host 192.168.100.10 any
cisco(config-ext-nacl)# remark LAN clients proxy port 80/443
cisco(config-ext-nacl)# permit tcp 192.168.100.0 0.0.0.255 any eq www 443
cisco(config-ext-nacl)# remark all others bypass WCCP
cisco(config-ext-nacl)# deny ip any any
```

Это означает, что трафик от Selecta маршрутизировать в интернет, а tcp трафик с портами 80 и 443 из подсети 192.168.100.0/24 маршрутизировать в Selecta.

5. Установить параметры WCCP: правила редиректа и пароли

```
# HTTP
cisco(config)# ip wccp web-cache redirect-list WCCP_ACCESS password 0 foo123

# HTTPS
cisco(config)# ip wccp 70 redirect-list WCCP_ACCESS password 0 foo123
```

6. Включить редирект на интерфейсе

```
cisco(config)# interface fa0/1
cisco(config-if)# ip wccp web-cache redirect in
cisco(config-if)# ip wccp 70 redirect in
```

7. Завершить конфигурирование роутера и сохранить конфигурацию

```
cisco(config)# end
cisco# copy running-config startup-config
```

Настройка сети на Ideco Selecta

1. Создать Ethernet-соединение. Нужно убедиться, что роутер, с которым производится интеграция, доступен через это соединение

Общие параметры

Название соединения
Сеть

Тип
Ethernet

Параметры IPv4

Устройство
Realtek Semiconductor Co., Ltd., RTL-8100/8101L/8139 PCI Fast Ethernet Adapter, 52:54:00:d9:1c:2f

Роль
Внешний

IP-адрес
192.168.100.10

Маска подсети
24

Шлюз по-умолчанию
192.168.100.1

DNS 1

DNS 2

2. Создать соединение типа "IP туннель" на базе созданного Ethernet-соединения. Здесь IP-адрес удалённой точки означает адрес Loopback интерфейса на маршрутизаторе cisco, который будет отвечать за GRE туннель.

Общие параметры Маршруты

Название соединения
WCCP

Тип
IP-туннель

Параметры туннеля

Основное подключение
Сеть

Роль
WCCP

Тип туннеля
GRE

IP-адрес удалённой точки
10.108.1.1

3. Перейти в раздел: Интеграции -> WCCP
4. Установить флажок "Режим WCCP"
5. Указать IP роутера (IP интерфейса роутера, который смотрит в локальную сеть)
6. Указать Пароль, который был указан при настройке WCCP на роутере в п. 5
7. Нажать сохранить и перезагрузить Selecta для применения новых сетевых настроек.

Интеграция по WCCP ? Справка

Режим WCCP

IP роутера
192.168.100.1

Пароль

Сохранить

Проверка

1. На роутере выполнить `show ip wccp`. Вывод должен быть похож на следующий:

```
cisco#show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          10.108.1.1
    Protocol Version:          2.0

  Service Identifier: web-cache
    Number of Cache Engines:    1
    Number of routers:          1
    Total Packets Redirected:    535271
    Redirect access-list:       WCCP_ACCESS
    Total Packets Denied Redirect: 0
    Total Packets Unassigned:    5540
    Group access-list:          -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 7976
    Total Bypassed Packets Received: 0

  Service Identifier: 70
    Number of Cache Engines:    1
    Number of routers:          1
    Total Packets Redirected:    1656910
    Redirect access-list:       WCCP_ACCESS
    Total Packets Denied Redirect: 0
    Total Packets Unassigned:    11538
    Group access-list:          -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 32
    Total Bypassed Packets Received: 0
```

Важно, что бы Number of Cache Engines был не 0

2. Правила фильтрации для пользователей должны применяться.
3. После выключения Idecu Selecta у пользователей должен сохраняться доступ в Интернет.

Настройка WCCP + TPROXY

Idecu Selecta поддерживает перенаправление https(s) трафика на прозрачный прокси сервер с устройств Cisco, организованное по протоколу WCCP.

Прозрачный HTTP-прокси называется так потому, что все клиенты, обращающиеся к внешним веб-серверам из внутренней сети, проходят через него автоматически, не внося никаких изменений в настройки на своей стороне (не указывая явно прокси во всех используемых программах, в части из которых может вовсе не быть поддержки прокси).

Порядок настройки

Схема сети

- 192.168.0.0/16 - Локальная сеть
- 192.168.100.1 - IP-адрес Cisco роутера в пользовательской локальной сети
- 192.168.200.1 - IP-адрес Cisco роутера в сети Idecu Selecta
- 192.168.200.10 - IP-адрес Idecu Selecta
- fa0/0 - интерфейс на роутере, который смотрит в Интернет
- fa0/1 - интерфейс на роутере, который смотрит в локальную сеть
- fa1/0 - интерфейс на роутере, который смотрит на Idecu Selecta

Настройка Cisco роутера

На Router необходимо выполнить следующие команды:

1. Настроить NAT:

```

Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255

Router(config)# ip nat inside source list 1 interface FastEthernet0/0
overload

Router(config)# access-list 2 permit 192.168.200.0 0.0.0.255

Router(config)# ip nat inside source list 2 interface FastEthernet0/0
overload

Router(config)# interface FastEthernet0/0

Router(config-if)# ip nat outside

Router(config)# interface FastEthernet0/1

Router(config-if)# ip nat inside

Router(config)# interface FastEthernet1/0

Router(config-if)# ip nat inside

```

2. Создать ACL со списком адресов WCCP клиентов:

```

Router# conf t

Router(config)# ip access-list extended wccp

Router(config-ext-nacl)# exit

Router(config)# ip access-list extended
wccp_to_inside

Router(config-ext-nacl)# end

```

3. Создать Loopback интерфейс, который будет отвечать за GRE туннель

```

Router# conf t

Router(config)# interface loopback 1

Router(config-if)# ip address 10.108.1.1
255.255.255.0

Router(config-ext-nacl)# end

```

4. Включаем WCCP

```

Router(config)# ip wccp 80 redirect-list wccp
Router(config)# ip wccp 90 redirect-list wccp_to_inside

```

5. Включить перенаправление на нужных интерфейсах. В нашем случае f0/0 и f1/0

```

Router(config)# int f0/0

Router(config-if)# ip wccp 80 redirect out
Router(config-if)# ip wccp 90 redirect in

Router(config-if)# exit

Router(config) int f1/0
Router(config-if)# ip wccp redirect exclude
in

Router(config-if)# exit

```

Настройка Ideco Selecta

1. Создать внешнее Ethernet-соединение. Нужно убедиться, что роутер, с которым производится интеграция, доступен через это соединение.

2. Создать соединение типа "IP туннель" на базе созданного Ethernet-соединения. Здесь IP-адрес удалённой точки означает IP-адрес Loopback интерфейса на маршрутизаторе cisco, который будет отвечать за GRE туннель.

3. Перейти в раздел: Интеграции -> WCCP
4. Активировать флажок "Режим WCCP"
5. Активировать флажок "Режим TPROXY"
6. Указать IP роутера (IP интерфейса роутера, который смотрит в сеть с Ideco Selecta)
7. Нажать "Сохранить" и перезагрузить Ideco Selecta для применения новых сетевых настроек.

Проверка

1. На роутере выполнить show ip wccp. Вывод должен быть похож на следующий:

```
Router#show ip wccp
Global WCCP information:
Router information:
Protocol Version: 2.0

Service Identifier: 80
Number of Service Group Clients: 1
Number of Service Group Routers: 1
Total Packets s/w Redirected: 4116
Process: 0
Fast: 0
CEF: 4116
Redirect access-list: wccp
Total Packets Denied Redirect: 0
Total Packets Unassigned: 21240
Group access-list: -none-
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0

Service Identifier: 90
Number of Service Group Clients: 1
Number of Service Group Routers: 1
Total Packets s/w Redirected: 4547
Process: 2
Fast: 0
CEF: 4545
Redirect access-list: wccp_to_inside
Total Packets Denied Redirect: 0
Total Packets Unassigned: 25675
Group access-list: -none-
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0
```

2. Правила фильтрации для пользователей должны применяться.
Важно, что бы Number of Service Group Clients был не 0.
3. После выключения Ideco Selecta у пользователей должен сохраняться доступ в Интернет.

Интеграция по eBGP

В режиме интеграции в сеть по eBGP Ideco Selecta производит анонсирование себя как gateway (с as_path, состоящим из автономной системы, в которой работает Ideco Selecta) для сетей:

1. 0.0.0.0/0 (в режиме default gateway).
2. Для конкретных IP-адресов из списка Роскомнадзора, если режим default gateway отключен.

Схема включения в сеть



Ideco Selecta по eBGP экспортирует на маршрутизатор провайдера список подозрительных маршрутов (список Роскомнадзора + настраиваемый чёрный список), пропуская этот трафик через себя.

[online diagramming & design] [creately.com](https://www.creately.com)

Сеть должна быть построена таким образом, чтобы трафик, который проходит через Ideco Selecta, возвращался обратно по тому же маршруту (т.е. через неё же).

Настройка интеграции

Перейдите в Интеграции - eBGP. Затем нажмите кнопку Редактировать.

ideco SELECTA Авторизация Профили Сессии Группы слов **Интеграции** Отчеты

Интеграция по eBGP ? Справка

Статус
BGP-статус off

Режим BGP

Параметры [Редактировать](#)

- ID автономной системы
- IP-адрес BGP-соседа
- ID автономной системы провайдера
- Анонсировать Ideco Selecta как маршрут по умолчанию Да

Параметры:

- ID автономной системы - ID автономной системы, в которой работает Ideco Selecta;
- IP-адрес BGP-соседа - IP-адрес маршрутизатора провайдера, с которым будет установлена связь по eBGP;
- ID автономной системы провайдера - ID автономной системы, в которой работает маршрутизатор, с которым будет установлена связь;
- Анонсировать Ideco Selecta как маршрут по умолчанию - в данном режиме Ideco Selecta будет анонсировать себя как маршрут для 0.0.0.0/0. В случае отказа маршрутизатор в состоянии вернуть свой маршрут по умолчанию. Если эта опция не активирована, то Ideco Selecta строит у себя таблицу всех доменов, внесённых в список Роскомнадзора, и 1 раз в 10 секунд получает для них список IP-адресов, после чего анонсирует себя как шлюз для данных IP-адресов.

После настройки нажать Сохранить и на первой странице активировать опцию Режим BGP.

Внимание

В случае, если Selecta работает не в режиме анонсирования себя как маршрута по умолчанию, нужно учитывать следующие вещи:

1. В сети желателен свой кэширующий DNS-сервер, чтобы Ideco Selecta максимально быстро делала запросы. Это связано с тем, что данный режим основан на постоянном обновлении IP-адресов из A-записей DNS;
2. В данном режиме блокировка таких сайтов как youtube.com, google.com будет работать нестабильно в связи с тем, что у них очень часто обновляются DNS-записи (~ каждые 120 секунд).

Настройка подключения Selecta к Центральной консоли

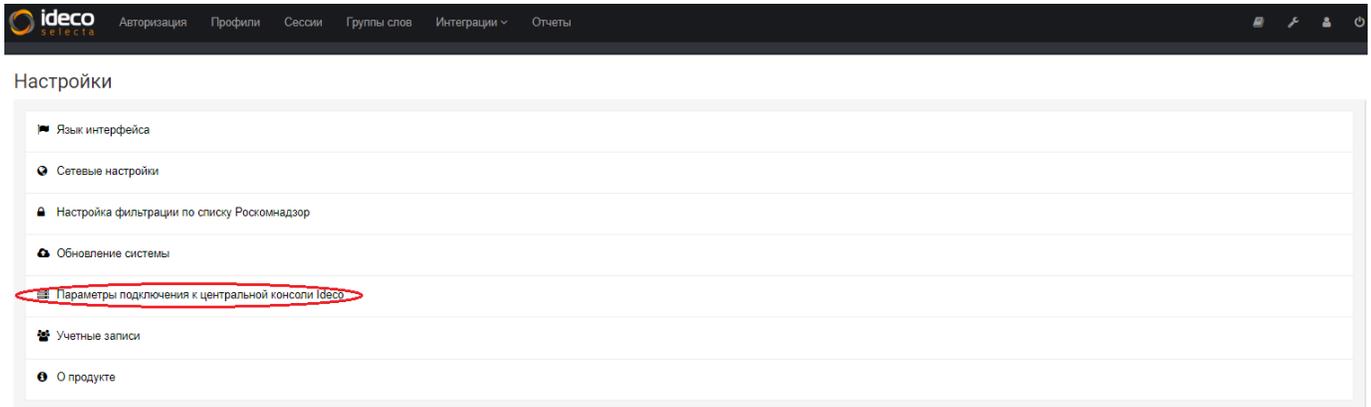
Предполагается, что Центральная консоль [установлена](#) и [настроена](#).

Ниже описаны настройки, которые необходимо выполнить на серверах Selecta, управление которыми должно осуществляться из Центральной консоли.

Перед настройкой подключения необходимо получить у администратора Центральной консоли реквизиты для подключения:

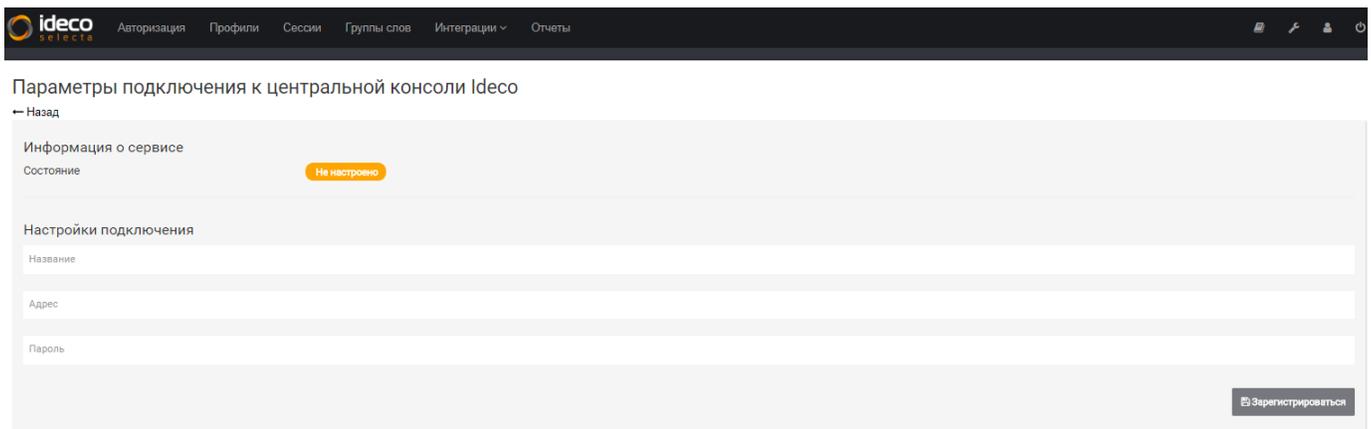
- IP-адрес Центральной консоли;
- Пароль для подключения.

Настройка подключения к Центральной консоли осуществляется в меню: Настройки - Параметры подключения к Центральной консоли Ideco.



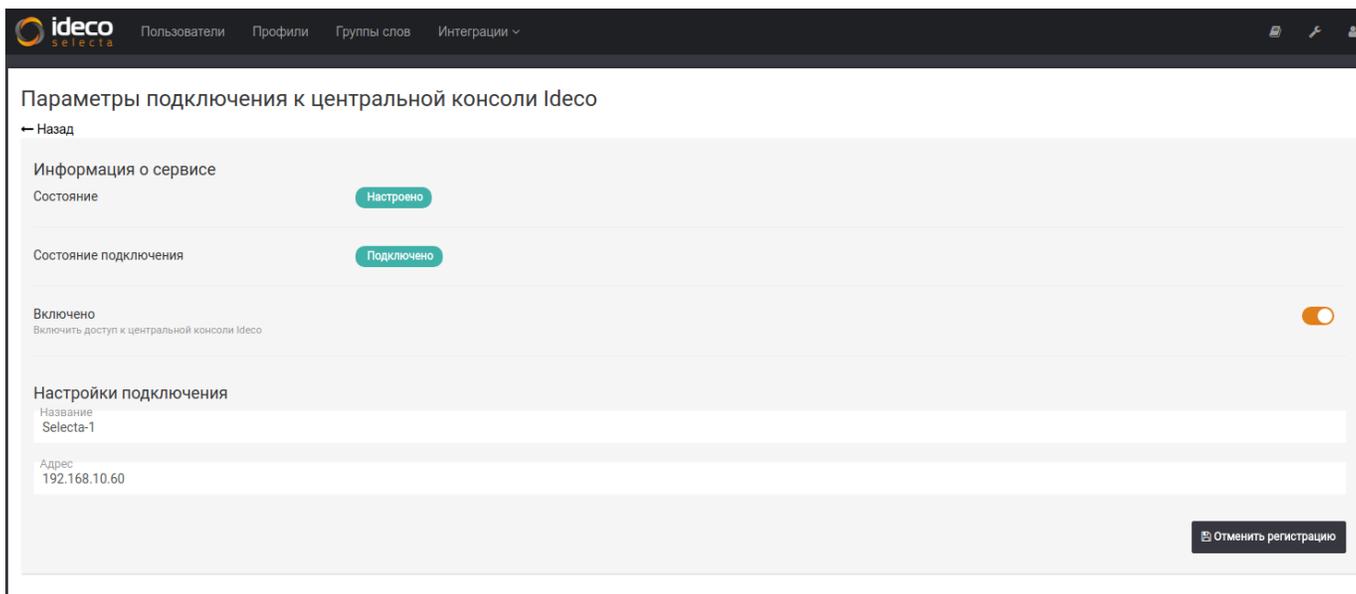
Для подключения необходимо ввести следующие данные:

- Название - имя сервера Ideco Selecta для удобства идентификации сервера администратором Центральной консоли;
- Адрес - IP-адрес сервера Центральной консоли;
- Пароль - пароль для подключения (администратор Центральной консоли может изменить его в веб-интерфейсе Центральной консоли).



После нажать кнопку Зарегистрироваться.

После подключения к Центральной консоли в данном меню будет отображен статус подключения.



Отчеты

Просмотр отчетов

При первой установке Idec Selecta вам будет доступен базовый набор отчетов. Их можно редактировать и удалять, а так же создавать свои отчеты.

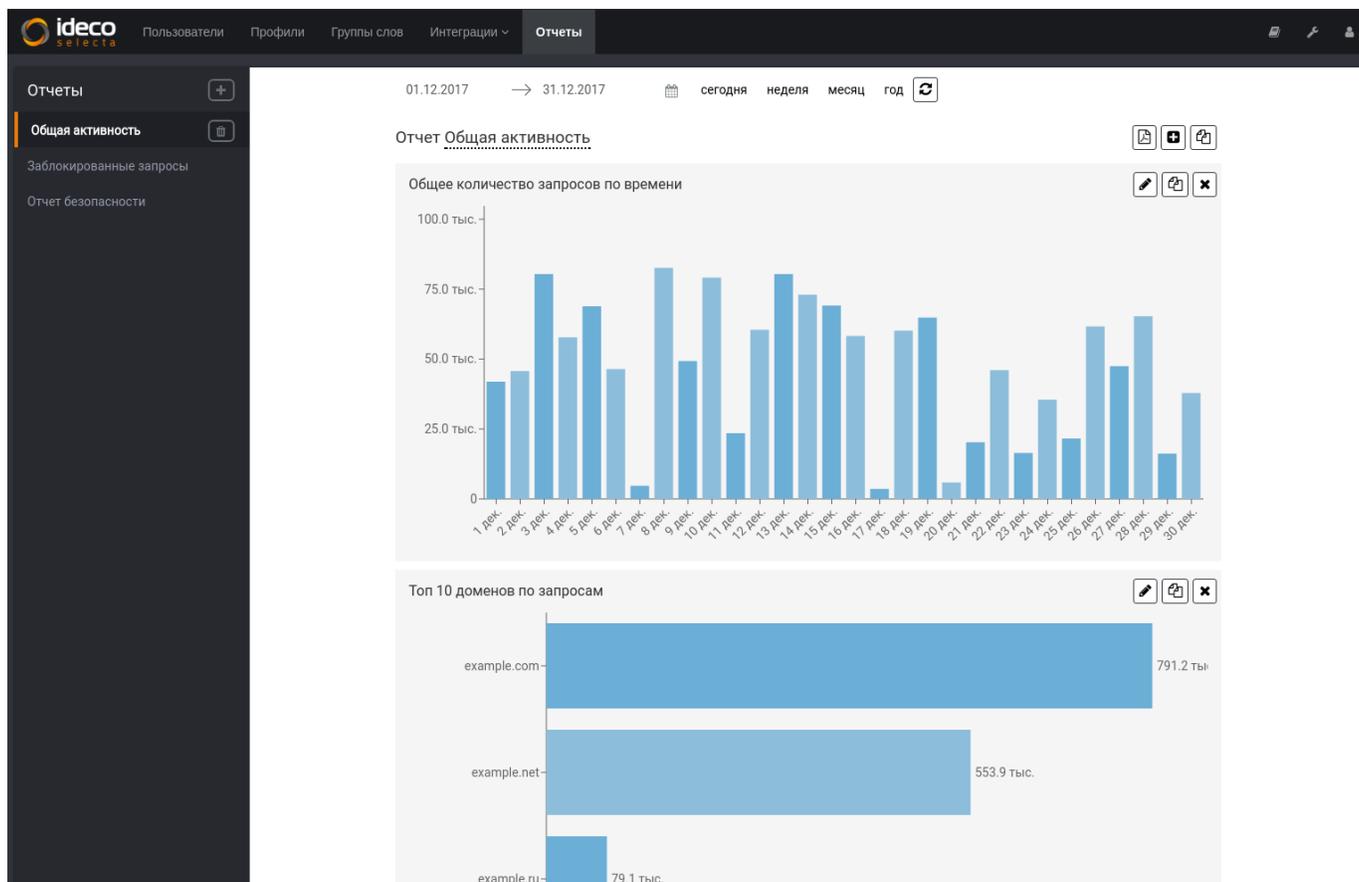
Общая активность - предоставляет общую информацию о распределении запросов по времени, доменам и категориям сайтов.

Заблокированные запросы - предоставляет информацию о количестве заблокированных запросов пользователей.

Отчет безопасности - предоставляет информацию о количестве запросов до небезопасных категорий сайтов:

- Ботнеты - web-сайты, на которых запущено программное обеспечение, используемое хакерами для рассылок спама и осуществления различных интернет-атак;
- Взлом - web-сайты, содержащие информацию или утилиты, которые могут быть использованы для совершения онлайн-преступлений;
- Скомпрометированные - web-сайты, которые были скомпрометированы злоумышленниками, и выглядят как официальные web-сайты, но на самом деле содержат вредоносный код;
- Фишинг/мошенничество - web-сайты, используемые для мошенничества. Как правило, представляются официальными web-страницами финансовых или иных учреждений с целью несанкционированного доступа к конфиденциальной информации, например, пин-кодам банковских карт;
- Центры распространения вредоносного ПО - web-сайты, на которых размещены вирусы, эксплойты и другое вредоносное ПО;
- Центры управления и контроля - серверы, использующиеся для управления ботнетами;
- Шпионское и сомнительное ПО - web-сайты с шпионским ПО (например, key-logger'ы), пересылающим информацию на центральный сервер.

Отчеты также можно экспортировать в .pdf



Редактирование отчетов

В отчетах можно редактировать и удалять виджеты по нажатию соответствующих кнопок. При добавлении/редактировании виджета используются следующие параметры:

Заголовок виджета - позволяет дать название виджету;

Вид виджета - выбор типа графика (горизонтальная/вертикальная гистограммы, линейный график, круговая диаграмма);

Поле для отображения на графике (ось X) - выбор поля данных для отображения на оси X графика (например, IP-адреса);

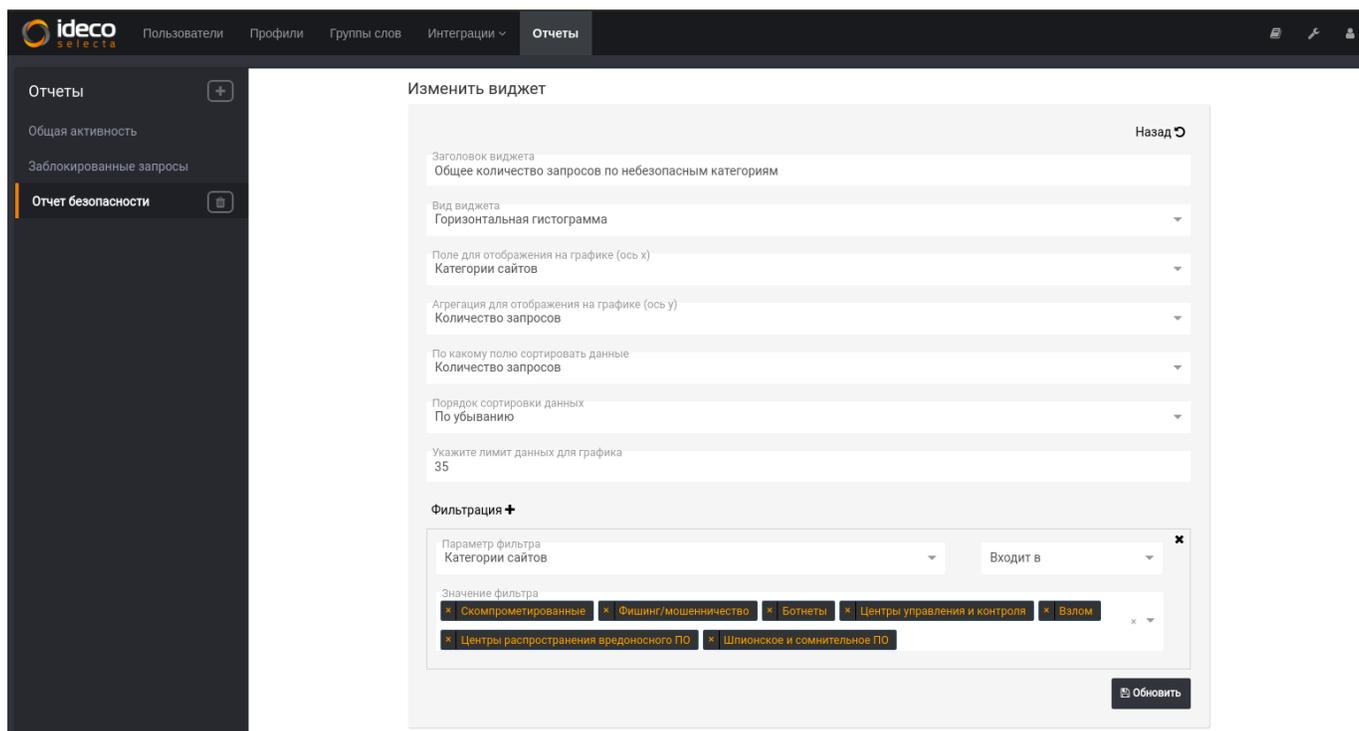
Агрегация для отображения на графике (ось Y) - выбор поля данных для отображения на оси Y графика (например, количество запросов или объем трафика);

По какому полю сортировать данные - выбор критерия сортировки (по дате или по количеству запросов);

Порядок сортировки данных - по возрастанию/убыванию;

Укажите лимит данных для трафика - ограничение количества записей, которые будут отображены по оси X;

Фильтрация - позволяет создавать дополнительные фильтры. Выбирается параметр (например, имя пользователя или IP-адрес) и критерий отбора (входит/не входит/конкретное значение параметра). Например, можно настроить вывод отчета по отдельным категориям сайтов:



Обслуживание

Текущий раздел содержит информацию, касающуюся обслуживания сервера Ideco Selecta.

Обновление системы

В данном разделе представлена информация о новых версиях продукта, а также есть возможности проверить наличие обновлений и включить опцию автоматического обновления. Также по мере обновлений можно удалять более старые версии ОС.

Внимание: для установки обновлений необходимо свободное место на файловой системе не менее 20% от ее общего размера.

Внимание!
После обновления следует очищать кэш браузера (CTRL+F5)!

Обновление системы

← Назад История изменений

Автоматически скачивать и распаковывать обновления при наличии
Обновление будет применено только после перезагрузки вручную

Сведения о системе

Номер сборки	25 июня 2018 г., 11:22 (1806251122)
Размер файловой системы	206.3 GiB
Свободное место на файловой системе	201.5 GiB
Доступное место для обновлений	180.9 GiB

Проверить обновления
последняя проверка: час назад

Сведения о доступных обновлениях
нет доступных обновлений

Управление установленными версиями

25 июня 2018 г., 11:22 (1806251122)	активна
-------------------------------------	---------

Обновление системы

← Назад История изменений

Автоматически скачивать и распаковывать обновления при наличии
Обновление будет применено только после перезагрузки вручную

Сведения о системе

Номер сборки	25 июня 2018 г., 11:22 (1806251122)
Размер файловой системы	206.3 GiB
Свободное место на файловой системе	201.5 GiB
Доступное место для обновлений	180.9 GiB

Проверить обновления
последняя проверка: час назад

Сведения о доступных обновлениях
нет доступных обновлений

Управление установленными версиями

25 июня 2018 г., 11:22 (1806251122)	активна
-------------------------------------	---------

Разрешить доступ в интернет без фильтрации

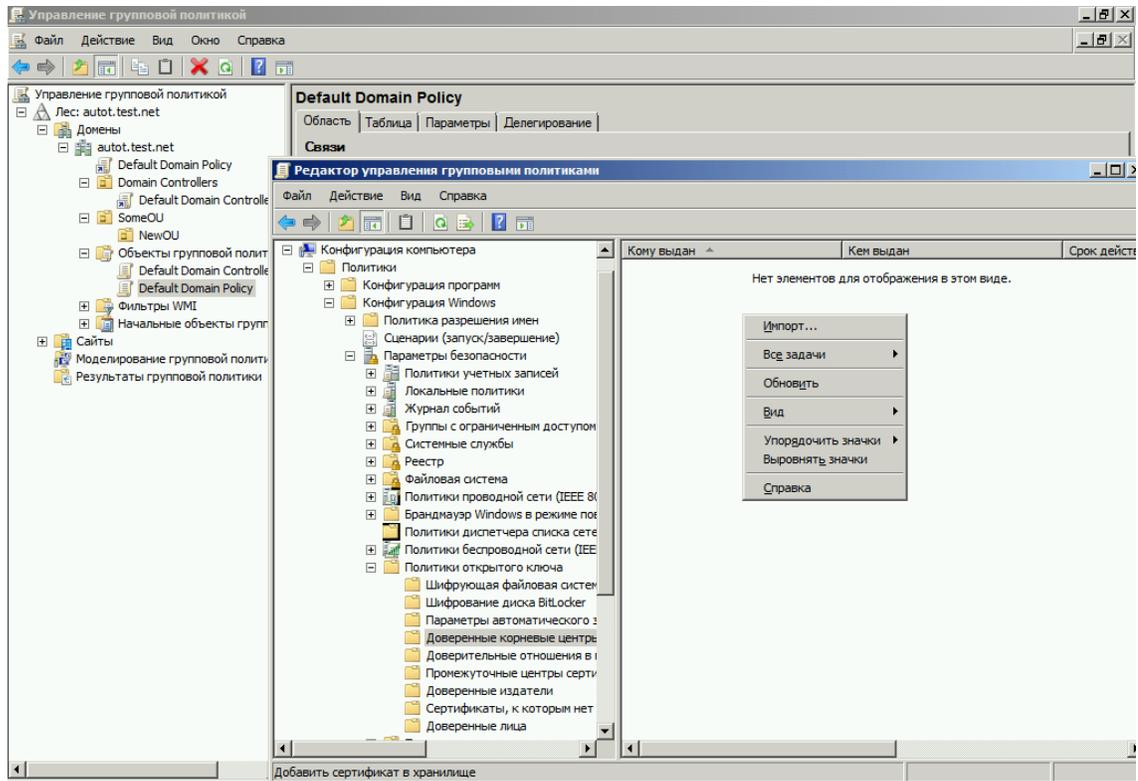
Сервисный режим, при включении которого Ideco Selecta пропускает всех в Интернет без какой-либо фильтрации и авторизации пользователей.

Инструкции по интеграции

Инструкция для автоматического развертывания доверенного сертификата средствами Active Directory

1. Зайдите на контроллер домена с помощью аккаунта, имеющего права администратора домена.
2. Запустите оснастку управления групповой политикой, выполнив команду `grpms.msc`. Найдите политику домена, использующуюся на компьютерах пользователей в «Объектах групповой политики» (на скриншоте - Default Domain Policy).
3. Нажмите на неё правой кнопкой мышки и выберите «Изменить».
4. В открывшемся редакторе управления групповыми политиками выберите:
5. «Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики открытого кл

юча → Доверенные корневые центры сертификации».



6. Нажмите правой кнопкой мыши по открывшемуся списку, выберите «Импорт...» и импортируйте сертификат из файла, загруженного предварительно из веб-интерфейса продукт.
7. Данная настройка будет автоматически применена через 2 часа, либо при перезагрузке рабочих станций.
8. Для более быстрого применения выполните следующие пункты на контроллере домена: В качестве альтернативного способа немедленного применения настроек GP, на рабочих станциях выполните: `gpupdate /force`, либо перезагрузите их.
 - a. Скачайте набор утилит по ссылке <https://technet.microsoft.com/ru-ru/sysinternals/bb897553.aspx> и распакуйте архив на контроллере домена в произвольную папку. Утилиту `psexec.exe` скопируйте в `C:\psexec.exe`.
 - b. Создайте текстовый файл с помощью блокнота и поместите туда следующее содержимое:

```
set WSHShell = CreateObject("WScript.Shell")
Set rootDSE = GetObject("LDAP://RootDSE")
base = "LDAP://CN=Computers," & rootDSE.Get("defaultNamingContext")
Set G = GetObject("", & base)
For Each T in G
    Command = "C:\psexec.exe \\" & Right(T.name, Len(T.name)-3) & " gpupdate /force "
    WSHShell.run Command,0,TRUE
Next
WSHShell.Echo "Done"
```
 - c. Файл - Сохранить как -> Тип файла - "все файлы", Имя файла "update.vbs" -> сохранить на рабочий стол.
 - d. Запустите `update.vbs` и ждать.
9. Сертификат появится в локальных хранилищах сертификатов и будет установлен нужный уровень доверия к нему.

Настройка СКФ Ideco Selecta в режиме интеграции с Active Directory и авторизации пользователей на прокси сервере

Принцип работы авторизации на прокси сервере:

Ideco Selecta производит интеграцию с Active Directory.

В браузерах пользователя указывается FQDN адрес Ideco Selecta в качестве прокси сервера. После этого, если компьютер пользователя введен в домен, браузер прозрачно производит negotiate (kerberos) авторизацию на прокси сервере.

Преимущества:

- Простота интеграции в сеть;
- Не требует ручного добавления пользователей в Ideco Selecta;
- Работает в условиях DHCP;

- Прозрачно авторизует трафик пользователей сети.

Недостатки:

- Требуется изменение параметров прокси сервера браузера и клиентских приложений.

Шаг 1. Установка СКФ Ideco Selecta на сервере либо виртуальной машине.

После завершения установки Ideco Selecta объединяет все доступные её интерфейсы в единый сетевой мост. Для того, чтобы избежать нарушения работы сети, советуется оставить лишь один сетевой интерфейс подключенным к локальной сети. После установки и перезагрузки в консоли Ideco Selecta появится интерфейс для ввода настройки параметром подключения bridge интерфейса. На начальном этапе настройки необходимо указать IP-адрес, который будет использоваться в дальнейшем для настройки Ideco Selecta.

Шаг 2. Интеграция в сеть.

Далее используя ранее указанный IP-адрес переходим в web-интерфейс управления Ideco Selecta (он будет доступен по данному IP-адресу). Выполняем вход в интерфейс управления, используя учетную запись (по умолчанию логин: "admin", пароль: "admin", логин и пароль возможно изменить в настройках). Далее в основном меню с помощью значка "настройки", выбрать пункт "Настройки" - "Настройка сетевых подключений". На данной странице представлены настройки подключений с изначальным сетевым мостом (см. Рисунок 1).

Рисунок 1. Окно настройки сетевых подключений с изначальным сетевым мостом

На данной вкладке представлен интерфейс по настройке сетевых подключений. Для минимальной работы интеграции Ideco Selecta с Active Directory в режиме авторизации пользователей на прокси сервере будет достаточно настроить один сетевой интерфейс. Удаляем текущие настройки подключения (удаление, изменение, добавление сетевых настроек применяется после перезагрузки Ideco Selecta) и создаем соединение, указываем имя, выбираем тип сетевого подключения - "Ethernet", выбираем подключенное к сети устройство, "роль" - "Административный", указываем основные сетевые настройки. В качестве DNS сервера должен выступать сервер MS Windows, контроллер домена Active Directory (см. Рисунок 2). После этого необходимо произвести перезагрузку сервера Ideco Selecta.

Рисунок 2. Окно настройки нового сетевого соединения

В случае, если были указаны неверные сетевые настройки или произошли иные ошибки, имеется возможность переустановить сетевые настройки Ideco Selecta. Для этого необходимо войти в терминал Ideco Selecta и выполнить команду network-reset. Далее, следуя инструкциям, сбросить сетевые настройки. Для их применения необходимо перезагрузить Ideco Selecta.

Шаг 3. Создание профиля фильтрации для пользователей.

Перейти в меню «Профили». Создаем новый профиль фильтрации. Указываем имя профиля фильтрации. Далее включаются или отключаются параметры профиля фильтрации такие как (см. Рисунок 3):

- Группы слов;
- Расширение файлов;
- Категории сайтов;
- Черные списки;
- Белые списки;
- HTTPS фильтрация.

После указания необходимых параметров фильтрации необходимо нажать кнопку "Сохранить". Появится уведомление, что профиль сохранен.

Рисунок 3. Окно настройки профиля фильтрации

Шаг 4. Настройка интеграции с Active Directory в СКФ Ideco Selecta.

Для корректной работы интеграции нужно обеспечить следующие условия:

- Время на всех машинах, которые участвуют в интеграции (в т.ч. и клиентские машины), должно быть синхронизировано. Разница не превышает 5 минут (требование для работы kerberos);
- В сети работает один или несколько DNS-серверов, которые доступны всем участникам интеграции (требование для работы kerberos).

Для выполнения интеграции необходимо перейти в пункте основного меню «Интеграция» - «Active Directory». В веб-интерфейсе при добавлении домена указать (см. Рисунок 4):

- Домен, с которым происходит интеграция (например TEST.COM);
- Имя компьютера для Ideco Selecta в домене (например ideco-selecta);
- Логин и пароль пользователя AD с правами ввода в домен (они будут использованы только один раз и нигде не сохраняются).

Рисунок 4. Окно ввода параметров интеграции с Active Directory

Нажать "Ввести в домен". После интерфейс в случае успеха изменит свое состояние и отобразит "Параметры интеграции с доменом" (см. Рисунок 5).

Рисунок 5. Параметры интеграции с Active Directory

В случае возникновения ошибок необходимо убедиться что:

- Настройки времени синхронизированы;
 - Введен верный логин и пароль учетной записи Active Directory;
 - У используемой учетной записи имеются права на ввод компьютера в домен;
 - Сетевая доступность контроллера Active Directory. Убедиться можно, используя терминал и команду nslookup (например nslookup test.com).
1. На контроллере домена создать DNS запись вида "[Имя компьютера для Ideco Selecta].[Домен]" (например ideco-selecta.test.com), A-запись которой должна содержать IP-адрес Ideco Selecta, до которого имеют доступ все клиенты сети.
 2. На странице интеграции появится раздел "Импорт групп безопасности", где нужно нажать кнопку "Обновить" для импорта групп безопасности из Active Directory (выгружаются глобальные группы безопасности).

Шаг 5. Указание профиля фильтрации для групп безопасности Active Directory.

Получив список групп, здесь же нужно назначить профиль фильтрации на группы безопасности, в которых состоят пользователи (см. Рисунок 6). После нажать кнопку "Сохранить". Появится уведомление, что настройки сохранены.

Если пользователь состоит в группе безопасности, то для него будет применен соответствующий профиль фильтрации. Если пользователь состоит в нескольких группах безопасности, для которых выбран профиль фильтрации, фильтрация будет осуществляться по одному из них. Для того, чтобы принудительно обновить профиль фильтрации активных сессий пользователей Active Directory, можно воспользоваться кнопкой "Обновить профиль авторизованных пользователей".

Рисунок 6. Импорт групп безопасности и применение профиля фильтрации для группы безопасности

Шаг 6. Настройка браузера пользователей.

Для того, чтобы трафик клиентов проходил обработку СКФ Ideco Selecta, необходимо в настройках используемого клиентом браузера указать использование прокси сервера. Настройками будет являться FQDN адрес Ideco Selecta в качестве прокси сервера и порт, указанный на странице «Интеграция» - «Active Directory». Пример настроек для Firefox (см. Рисунок 7).

Рисунок 7. Параметры прокси сервера для браузера Firefox

Шаг 7. Настройка фильтрации HTTPS.

Фильтрация HTTPS-трафика обеспечивает возможность обработки сервером сайтов, доступных по HTTPS. Более подробное описание принципа работы и настройки пользователей: <https://doc.ideco.ru/pages/viewpage.action?pageId=4325444>

Шаг 8. Проверка работы интеграции.

Чтобы проверить работу фильтрации и то, что интеграция прошла успешно, можно провести тестирование блокировки сайта. Для примера, в профиле фильтрации, применяемому для пользователей в данной интеграции, можем добавить сайт www.yandex.ru в черный список. Для этого перейдем в меню "Профиль" - "Выбираем ранее созданный профиль фильтрации" - "Черный список". В данной форме ввода добавляем сайт в черный список. После можно убедиться, что у пользователей выбранный сайт блокируется. Если сайт блокируется, то интеграция прошла успешно.