VIPole Corporate Server

Security Domain Administrator Manual

v.3.0, 2017

VIPole
www.vipole.com

SECURE AND ENCRYPTED MESSENGER
for secure communications and encrypted data storage

Windows ▪ Mac OS ▪ Linux ▪ Android ▪ iOS ▪ Enterprise solutions

Содержание

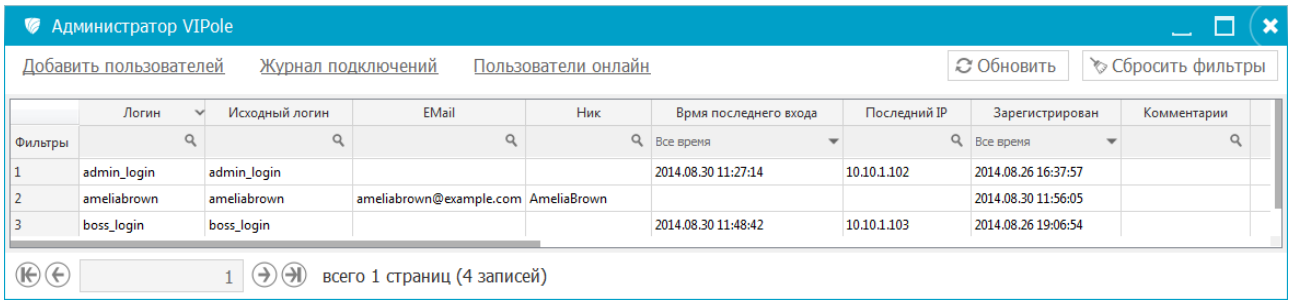
1. Введение 3
2. Создание Домена безопасности 5
3. Начало работы с Доменом безопасности 6
4. Запуск панели администратора 7
5. Окна программы 9
5.1. Администрирование пользователей 10
5.1.1. Вкладка «Профиль» 10
5.1.2. Вкладка «Подключения» 11
5.1.3. Вкладка «Безопасность» 12
5.1.4. Вкладка «Список контактов» 15
5.1.5. Вкладка «Логи» 16
5.2. Параметры 16
5.2.1. Вкладка «Параметры» 17
5.2.2. Вкладка «Администраторы» 17
5.2.3. Вкладка «Шаблоны безопасности» 18
5.2.4. Вкладка «Шаблоны списка контактов» 19
5.2.5. Вкладка «Логи» 20
5.3. Добавление пользователей 21
5.3.1. Вкладка «Один пользователь» 21
5.3.2. Вкладка «Несколько пользователей» 22
5.3.3. Вкладка «Импорт пользователей» 23
1.3.4 Вкладка LDAP 26
6. Журнал подключений 32
7. Пользователи онлайн 32

1. Введение

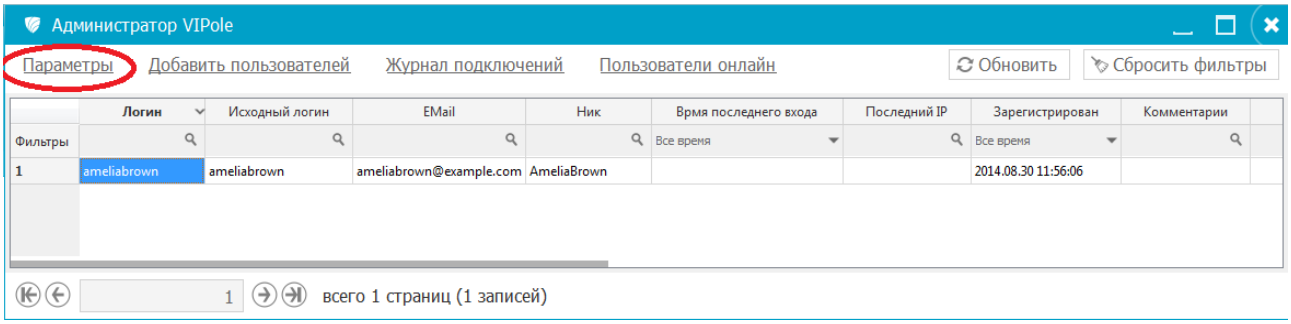
Домен безопасности позволяет централизовано управлять группой пользователей Корпоративного сервера VIPole. Вы можете добавлять и удалять пользователей, блокировать пользователей, настраивать политики безопасности. Вы также можете назначать пароли и секретные фразы, составлять списки контактов для пользователей.

При использовании VIPole Corporate Server, для управления рекомендуется создать Домен безопасности. Администратору Домена безопасности доступно больше возможностей управления пользователями, чем администратору Корпоративного сервера VIPole. Администратору сервера доступна только часть возможностей.

Администратор сервера



Администратор Домена безопасности



У администратора Домена безопасности, в отличие от администратора Корпоративного сервера VIPole, есть доступ к паролям и ключам пользователей.

Администратор Домена безопасности

Администрирование пользователя VIPole

Логин: ameliabrown

Обновить

Профиль | Подключения | Безопасность | Список контактов | Логи

Блокировка

- Заблокирован
- Заблокирован в бизнес-аккаунте

Разрешения

- Режим онлайн
- Может менять пароль
- Может менять ключи
- Может менять подменную секретную фразу
- Может менять настройки блокировки программы
- Может менять настройки автоматического выхода из программы

Пароль

Пароль

Секретная фраза и ключи

Секретная фраза

Автоматический выход из программы

- Включить автоматический выход при неактивности
- Включить автоматический выход при отключении от сервера

Блокировка программы

Использовать для разблокировки: Секретная фраза

- Включить автоблокировку при неактивности
- Отключать зашифрованное файловое хранилище VIPole при блокировке

Код быстрой разблокировки

Код быстрой разблокировки

Режим подменной секретной фразы

Режим подменной секретной фразы: Нет

Подменная секретная фраза

Подменная секретная фраза

Администратор сервера

Администрирование пользователя VIPole

Логин: ameliabrown

Обновить

Профиль | Подключения | Безопасность | Список контактов | Логи

Блокировка

- Заблокирован
- Заблокирован в бизнес-аккаунте

Разрешения

- Режим онлайн
- Может менять пароль
- Может менять ключи
- Может менять подменную секретную фразу
- Может менять настройки блокировки программы
- Может менять настройки автоматического выхода из программы

Пароль

Пароль

Автоматический выход из программы

- Включить автоматический выход при неактивности
- Включить автоматический выход при отключении от сервера

Блокировка программы

Использовать для разблокировки: Секретная фраза

- Включить автоблокировку при неактивности
- Отключать зашифрованное файловое хранилище VIPole при блокировке

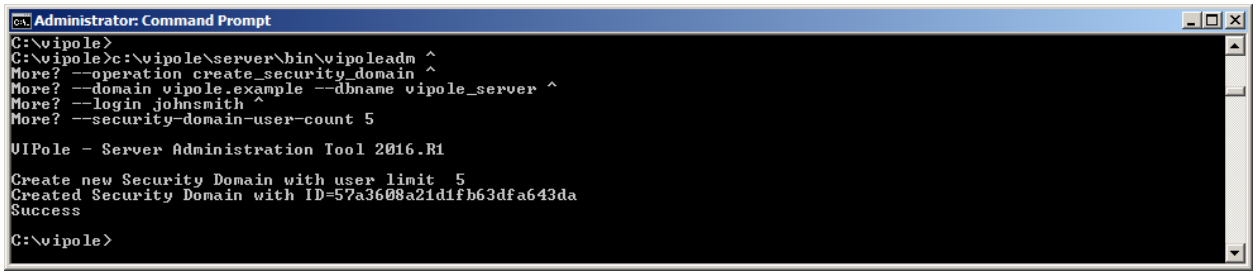
Режим подменной секретной фразы

Режим подменной секретной фразы: Нет

2. Создание Домена безопасности

Администратор сервера после установки может завести Домен безопасности командой

vipoleadm --domain vipole.example --operation create_security_domain --login <логин администратора>
--security_domain-user-count <количество пользователей>



<логин администратора> указывает логин пользователя, который будет управлять Доменом безопасности. Это может быть администратор сервера или любой вновь добавленный пользователь. Этот пользователь будет являться администратором Домена безопасности и получит расширенные возможности для управления пользователями, включенными в Домен.

<количество пользователей> - лимит пользователей Домена безопасности.

Можно завести несколько Доменов безопасности, например, для разных подразделений компании.

Вы всегда можете увеличить лимит пользователей Домена безопасности.

```
vipoleadm --domain Vipole.example --operation
add_security_domain_user_limit --security_domain_user_count
<количество пользователей>  --security-domain-id <id>
```

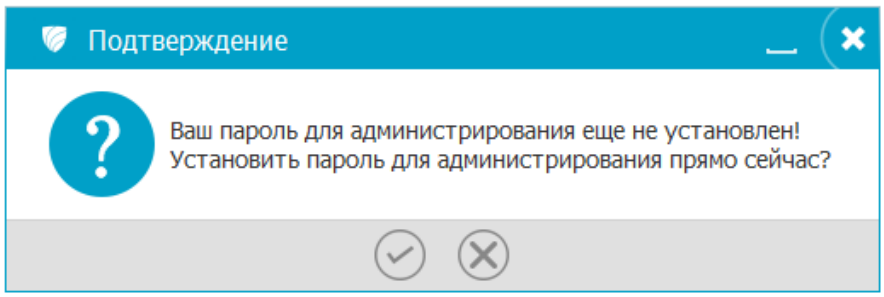
--domain – имя вашего домена.
<количество пользователей> - на сколько пользователей увеличивается лимит пользователей Домена безопасности.

<id> - идентификатор Домена безопасности, лимит пользователей которого изменяется. Идентификатор можно посмотреть на странице «Параметры» панели администратора.

3. Начало работы с Доменом безопасности

Для управления пользователями Домена безопасности используется встроенная в приложение VIPole панель администратора, которая позволяет владельцу Домена безопасности или назначенному им администратору управлять пользователями, их настройками и активностью:

1. Откройте панель администратора. В Главном меню приложения VIPole для компьютера перейдите в Расширения > Администратор VIPole.
2. Задайте пароль администратора. Нажмите на , а затем введите и повторите пароль, который необходимо вводить каждый раз для администрирования Домена безопасности.

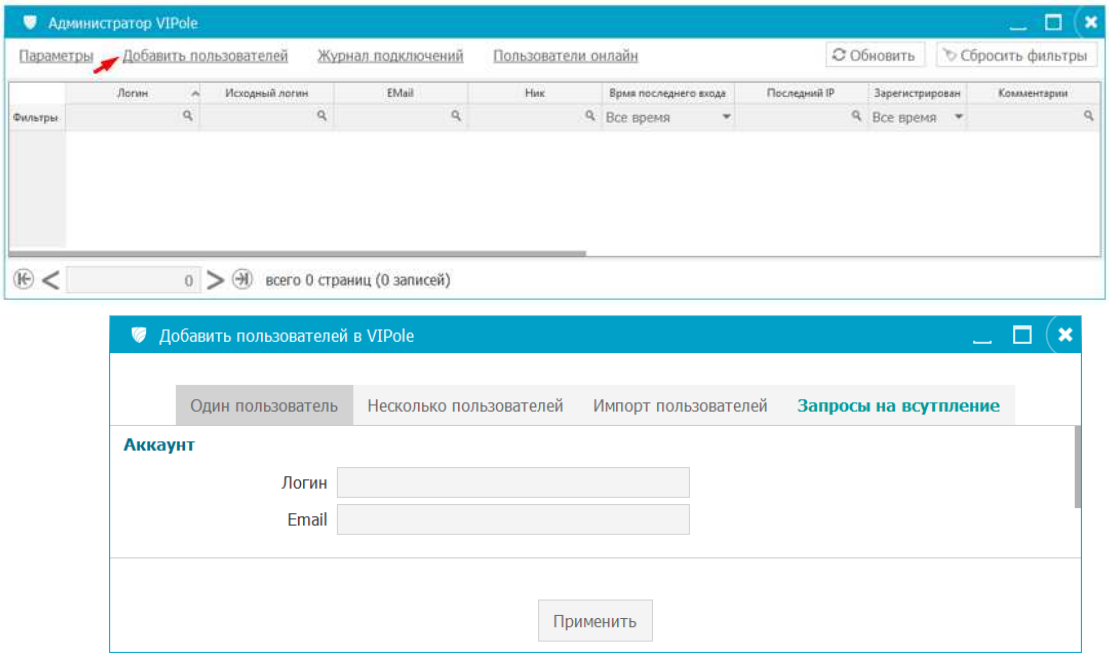


Панель администратора отображает информацию о членах Домена безопасности, и здесь вы можете создавать новые аккаунты пользователей.

Обратите внимание, что по умолчанию владелец Домена безопасности не входит в него, так как у него может быть много аккаунтов.

Для заведения новых пользователей:

1. Перейдите во вкладку «Добавить пользователей»



2. Создайте нового пользователя. Придумайте логин, пароль, выберите пакет пользователей, в который вы хотите добавить пользователя, заполните необходимые поля, и нажмите «Применить».

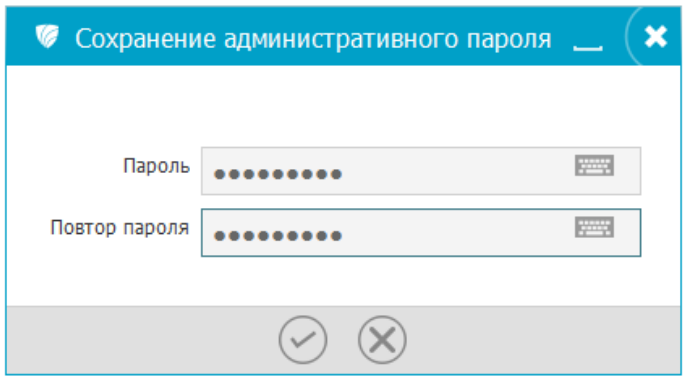
   В зависимости от желаемого уровня контроля, администратор может назначить пользователям пароль и секретную фразу или предоставить им возможность сгенерировать ключи самостоятельно. При назначении секретной фразы администратор получает доступ к переписке и файлам пользователя Домена безопасности.

4. Запуск панели администратора

Для управления пользователями Домена безопасности используется расширение, встроенное в клиентское приложение VIPole, которое вызывается через пункт меню «Расширения» > «Администратор VIPole».

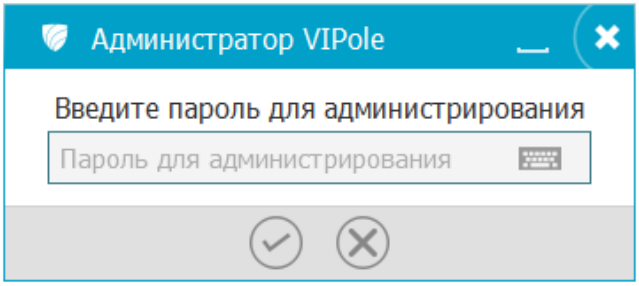
Перед запуском расширения для управления Доменом безопасности всегда запрашивается пароль. При первом запуске нажмите ✓, чтобы установить его.

Затем установите и подтвердите пароль для администрирования Домена безопасности.

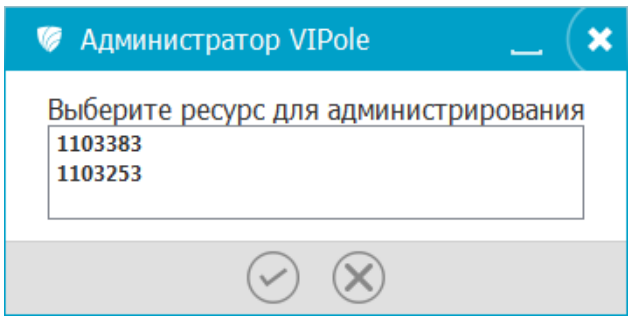


При первом запуске панели администратора вам будет предложено сгенерировать ключи шифрования данных Домена безопасности. Нажмите , чтобы сгенерировать ключи. После генерации ключей вы сможете начать работу с панелью администратора.

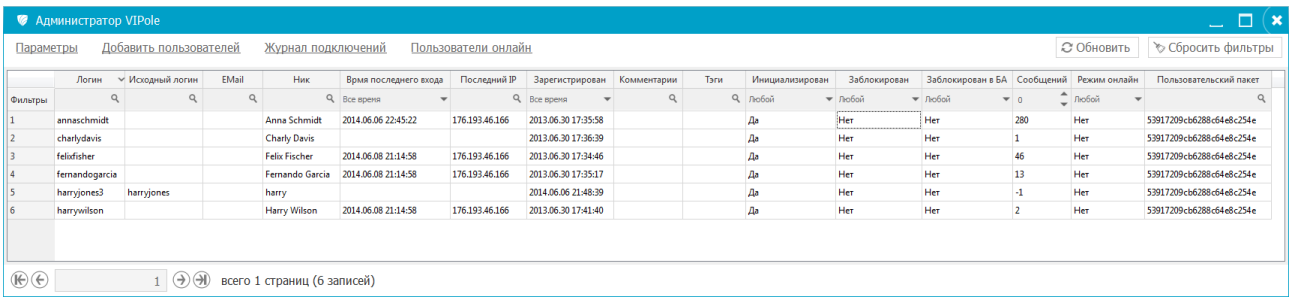
При каждом запуске расширения для управления Доменом безопасности необходимо ввести пароль, который вы сгенерировали при первом запуске. Рекомендуем сохранить пароль в Менеджере паролей VIPole.



Если у вас более одного Домена безопасности, выберите ID аккаунта, который будете администрировать в данный момент.



После этого перед вами откроется окно управления Доменом безопасности со списком пользователей VIPole – членами Домена безопасности.



Если вы ещё не добавили пользователей в Домен безопасности, окно будет пустым.

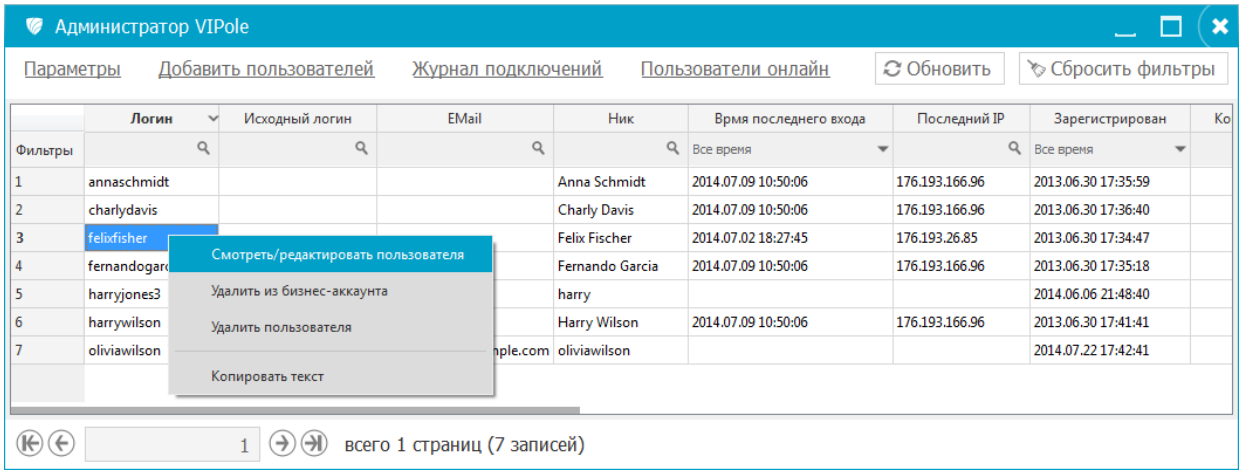
5. Окна программы

Основное окно панели администратора

В основном окне расширения администратора доступны несколько разделов для управления Доменом безопасности:

- Параметры
- Добавить пользователей
- Журнал подключений
- Пользователи онлайн

В основном окне при клике правой кнопкой мыши по имени пользователя открывается простое меню управления пользователем:

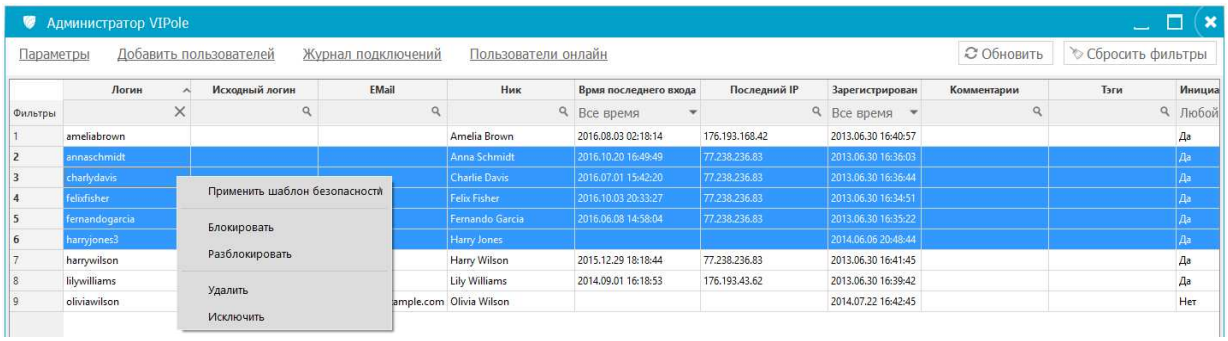


- **Смотреть/редактировать пользователя** - открывает окно «Администрирование пользователя». Также это окно можно открыть при двойном клике мышкой по имени пользователя.

- Удалить из Домена безопасности - исключает пользователя из Домена безопасности.
- Удалить пользователя - удаляется профиль пользователя, а аккаунт пользователя блокируется. Все данные пользователя становятся недоступными никому.
- Копировать текст - выделенный в таблице текст копируется в буфер обмена.

Массовые действия с пользователями

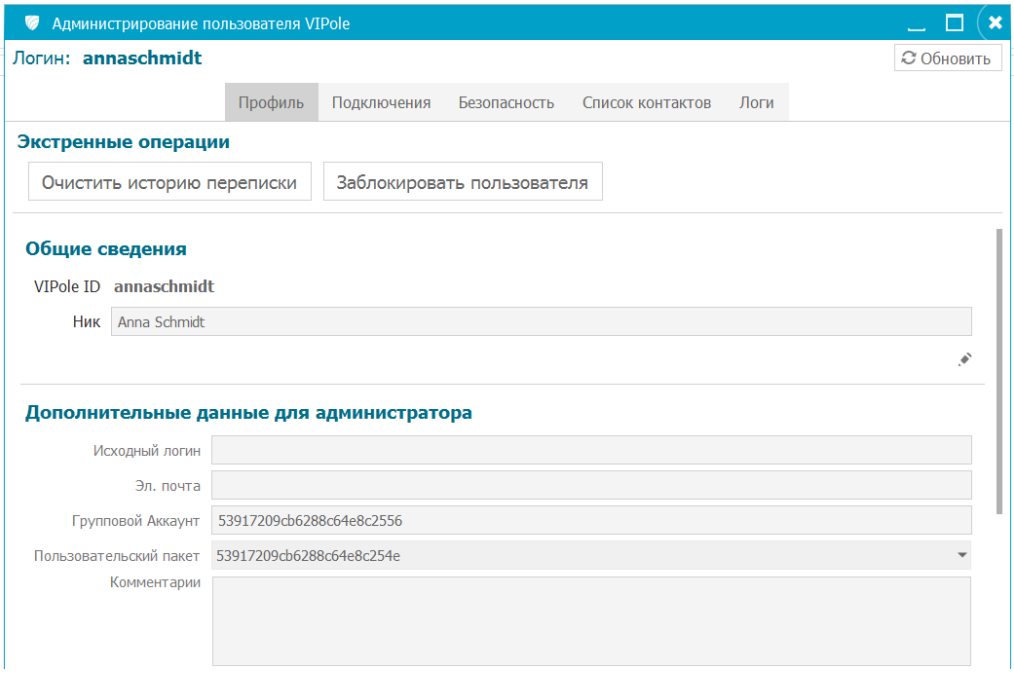
В главном окне расширения администратора вы можете совершать массовые действия с пользователями Домена безопасности. Для этого выделите нескольких пользователей левой кнопкой мыши, а затем кликните правой кнопкой мыши, чтобы вызвать контекстное меню. Затем выберите нужную опцию: применение шаблона безопасности к выделенным пользователям, блокировка, разблокировка, удаление или исключение из Домена безопасности.



5.1. Администрирование пользователей

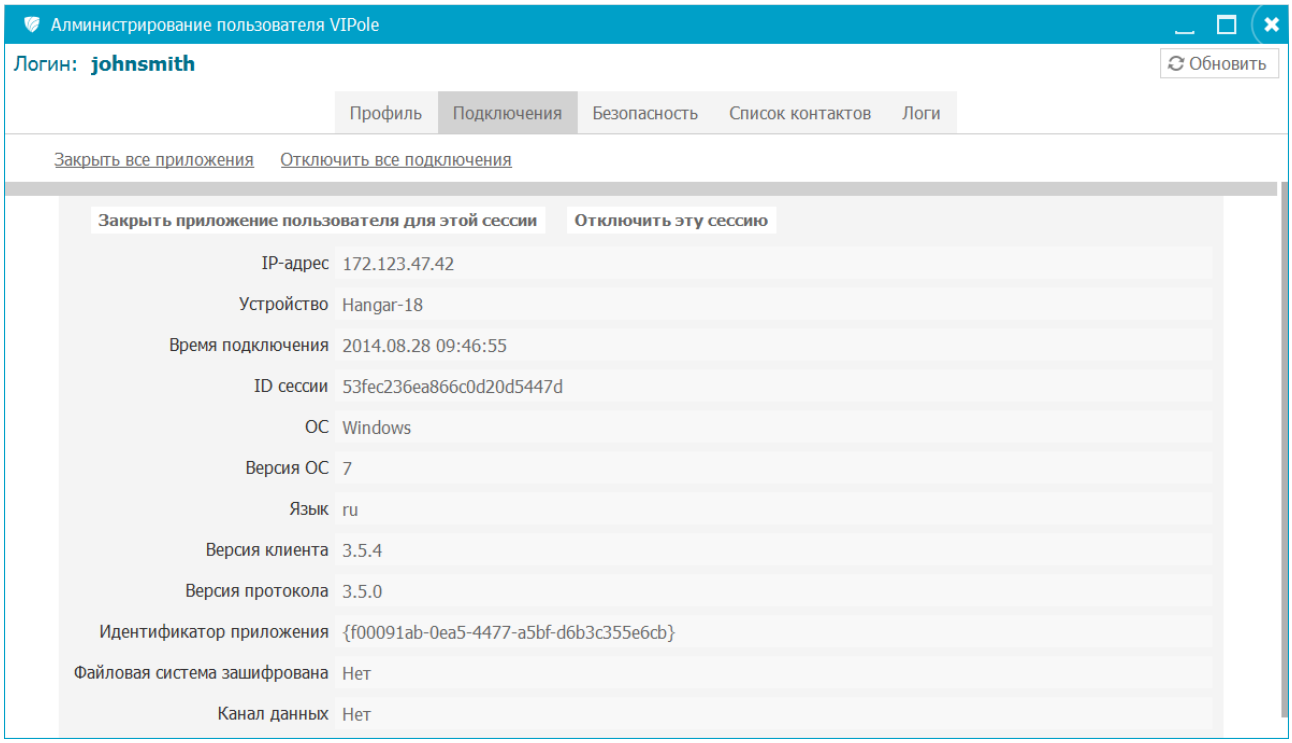
5.1.1. Вкладка «Профиль»

На вкладке «Профиль» вы можете отредактировать все те сведения, которые доступны пользователям в клиентском приложении через пункт меню «Мой профиль».



5.1.2. Вкладка «Подключения»

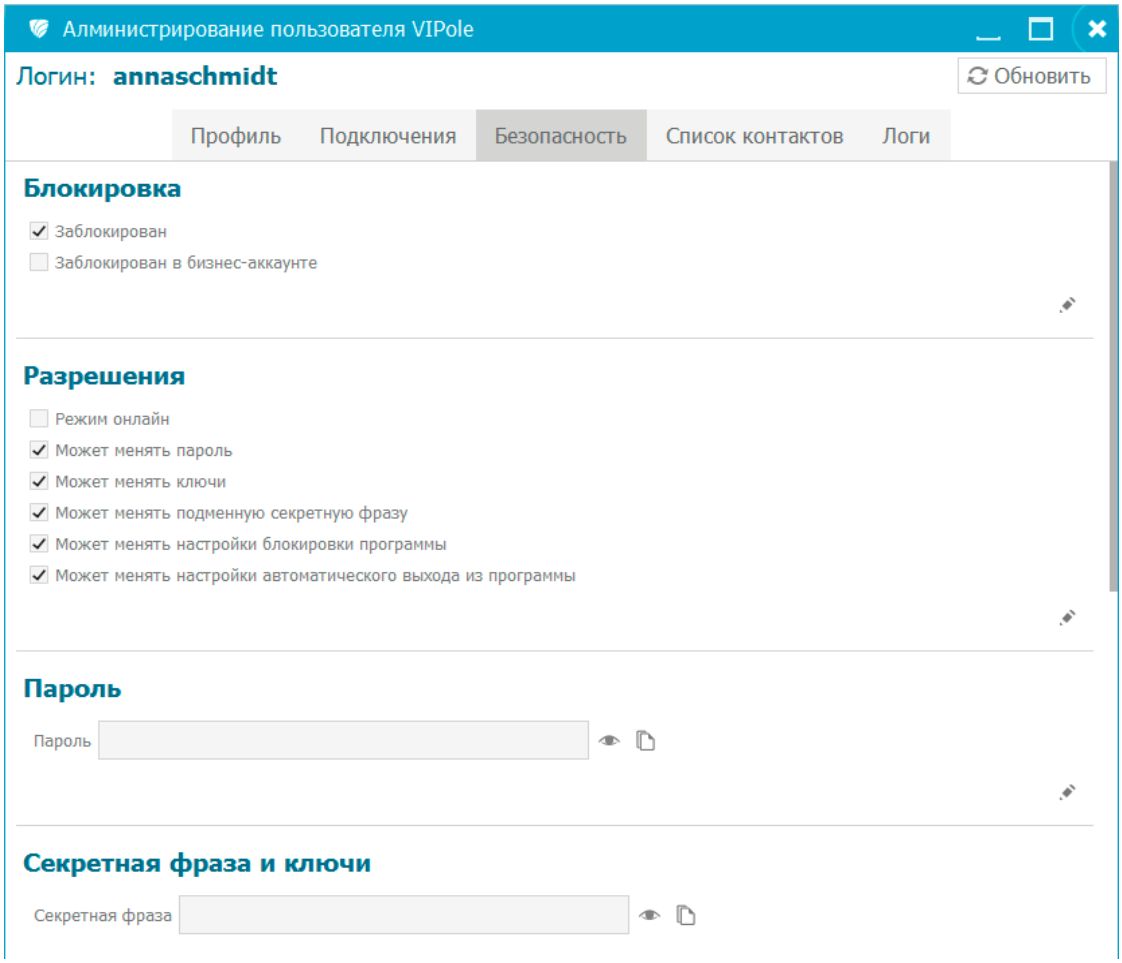
В этом разделе администратор Домена безопасности может оперативно закрыть клиентское приложение пользователя или отключить его от сервера. При наличии нескольких подключений пользователя (при подключении с разных устройств) – вы можете отключать подключения по отдельности или все сразу.



5.1.3. Вкладка «Безопасность»

Часть настроек на вкладке «Безопасность» соответствует настройкам раздела «Безопасность» программы-клиента. Эти настройки можно использовать для первоначальной настройки параметров безопасности нового пользователя Домена безопасности.

В дальнейшем пользователь может изменять настройки безопасности по своему усмотрению. Администратор Домена безопасности может запретить изменение этих настроек пользователем - всех сразу или по отдельности.



Раздел «Блокировка»

- Заблокирован – блокировка пользователя на сервере. Эта опция доступна только администратору Корпоративного сервера.

- Заблокирован в Домене безопасности – администратор Домена безопасности может заблокировать пользователя и прекратить его доступ к серверу.

Раздел «Разрешения»

- Режим online разрешает пользователю использовать программу-клиент только при наличии связи с сервером. В этом режиме невозможно автономное использование клиента, например, для просмотра переписки и заметок.
  Данный режим позволяет заблокировать доступ пользователя к данным, хранящимся на устройстве пользователя. Для этого заблокируйте пользователя на вкладке «Безопасность» и закройте программу-клиент пользователя на вкладке «Подключения» окна «Администрирование пользователя». После чего вы можете быть уверенными в отсутствии доступа к данным, хранящимся локально у пользователя.
- Остальные разрешения позволяют пользователю менять соответствующие настройки безопасности в своем профиле.

Остальные разделы соответствуют странице «Безопасность» программы-клиента. Эти настройки принудительно выставляются в программе-клиенте, которой присвоен данный шаблон.

Раздел «Пароль»

Администратор Домена безопасности может установить или сменить пароль пользователя. Это пароль для доступа к серверу.

Раздел «Секретная фраза и ключи»

Администратор Домена безопасности может сгенерировать ключи шифрования и установить секретную фразу для пользователя без его участия.

Раздел «Автоматический выход из программы»

- Устанавливается время, через которое автоматически произойдет закрытие профиля пользователя.

- Отдельно устанавливается время неактивности пользователя, отдельно – отсутствие связи с сервером.

Раздел «Блокировка программы»

- Указывается, что будет использоваться для разблокировки программы – пароль, секретная фраза или специальный код быстрой разблокировки.
- Устанавливается время до блокировки программы при неактивности пользователя. При блокировке сворачиваются все открытые окна программы.

Раздел «Код быстрой разблокировки»

Указывается код, используемый для разблокировки программы. Он используется, если в разделе «Блокировка программы» для разблокировки был выбран код быстрой разблокировки.

Раздел «Режим подменной секретной фразы»

Используется для защиты данных пользователя, если пользователя заставляют ввести секретную фразу, чтобы получить доступ к данным. Режим позволяет установить подменную секретную фразу и выбрать реакцию клиентской программы на ввод такой фразы:

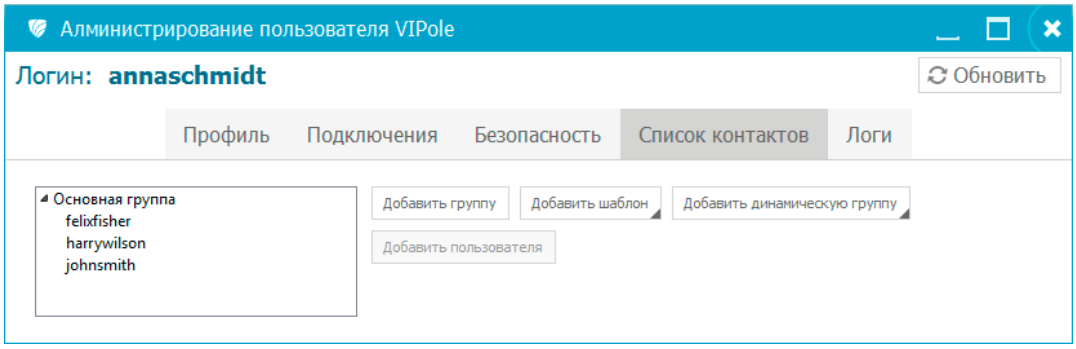
  - нет – режим не используется
  - падение программы – происходит аварийное завершение работы программы
  - удаление локальных данных и падение программы – перед аварийным завершением удаляется локальная копия данных.

Раздел «Подменная секретная фраза»

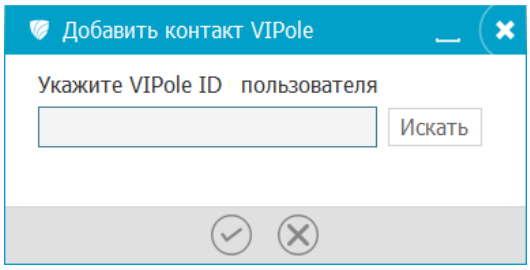
Введите подменную секретную фразу, которая будет активировать защиту данных, если пользователя заставят открыть профиль под принуждением.

5.1.4. Вкладка «Список контактов»

Вкладка «Список контактов» позволяет быстро заполнить список контактов пользователя без необходимости отправки запросов авторизации и получения разрешений на авторизацию. Пополнение списка контактов происходит обоюдно: пользователь будет также добавлен в список тех пользователей, которые занесены в его список контактов.



- Добавить группу – добавляет в список имя группы. Группа используется для объединения контактов по какому-либо признаку.
- Добавить пользователя – добавляет контакт в группу. Кликните на имя группы, затем нажмите «Добавить пользователя». Введите VIPole ID добавляемого пользователя, убедитесь, что такой пользователь есть в системе, и затем добавьте нажатием ✓. Взаимная авторизация происходит автоматически.

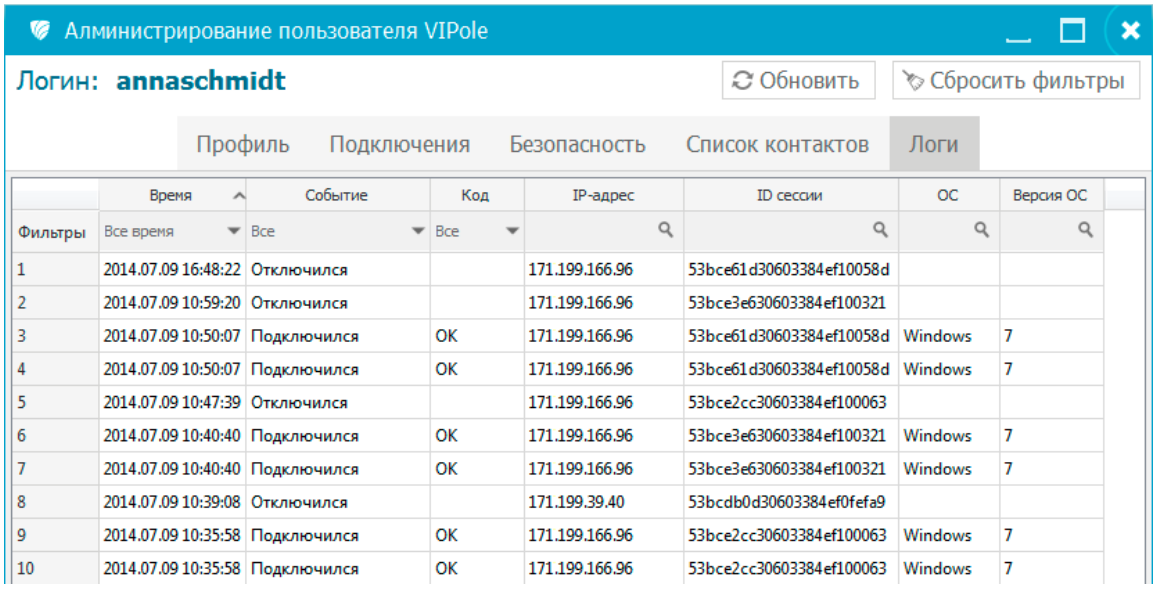


- Добавить шаблон – добавить контакты пользователей, объединенных в группы и в данный момент перечисленных в указанном шаблоне. Шаблон удобно использовать, если вам необходимо создать одинаковые списки контактов нескольким пользователям. Пользователь, которому добавляется шаблон списка контактов, будет также включен в список контактов всем пользователям, перечисленным в шаблоне. Контакты, в дальнейшем добавляемые в шаблон, текущему пользователю автоматически копироваться не будут.

- Добавить динамическую группу – пользователь включается в динамическую группу с указанным именем. При этом ему будут добавлены контакты пользователей, состоящих в этой динамической группе. В дальнейшем новые члены динамической группы будут добавляться в контакты такого пользователя.

5.1.5. Вкладка «Логи»

Здесь вы можете отслеживать события, относящиеся к пользователю.



	Время	Событие	Код	IP-адрес	ID сессии	ОС	Версия ОС
Фильтры	Все время	Все	Все				
1	2014.07.09 16:48:22	Отключился		171.199.166.96	53bce61d30603384ef10058d		
2	2014.07.09 10:59:20	Отключился		171.199.166.96	53bce3e630603384ef100321		
3	2014.07.09 10:50:07	Подключился	OK	171.199.166.96	53bce61d30603384ef10058d	Windows	7
4	2014.07.09 10:50:07	Подключился	OK	171.199.166.96	53bce61d30603384ef10058d	Windows	7
5	2014.07.09 10:47:39	Отключился		171.199.166.96	53bce2cc30603384ef100063		
6	2014.07.09 10:40:40	Подключился	OK	171.199.166.96	53bce3e630603384ef100321	Windows	7
7	2014.07.09 10:40:40	Подключился	OK	171.199.166.96	53bce3e630603384ef100321	Windows	7
8	2014.07.09 10:39:08	Отключился		171.199.39.40	53bcdb0d30603384ef0fefa9		
9	2014.07.09 10:35:58	Подключился	OK	171.199.166.96	53bce2cc30603384ef100063	Windows	7
10	2014.07.09 10:35:58	Подключился	OK	171.199.166.96	53bce2cc30603384ef100063	Windows	7

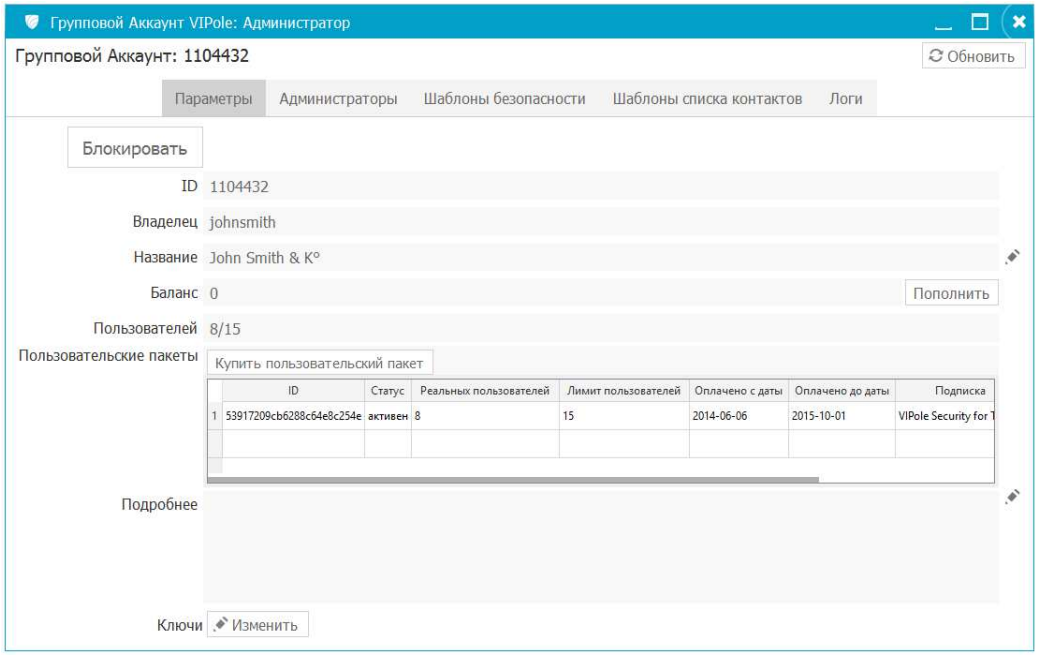
5.2. Параметры

Окно «Параметры» содержит следующие вкладки:

- Параметры - основные настройки Домена безопасности, включая список пользовательских пакетов.
- Администраторы - список администраторов Домена безопасности. Возможность добавлять и удалять администраторов.
- Шаблоны безопасности - возможность централизовано настроить параметры безопасности программ-клиентов пользователей – участников Домена безопасности.
- Шаблоны списка контактов - возможность создать пользователям Домена безопасности заполненный список контактов.
- Логи - просмотр активности по администрированию Домена безопасности.

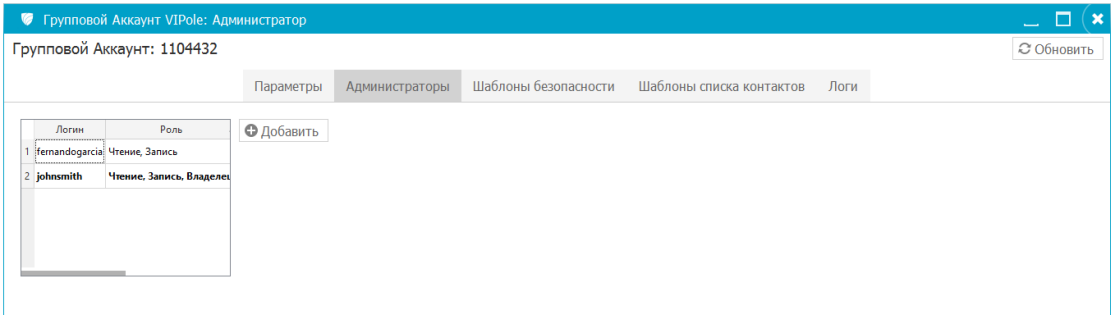
5.2.1. Вкладка «Параметры»

На этой вкладке вы можете следить за балансом счета Домена безопасности, сроком действия подписки пользовательских пакетов, а также пополнять баланс аккаунта и приобретать дополнительные пользовательские пакеты.



5.2.2. Вкладка «Администраторы»

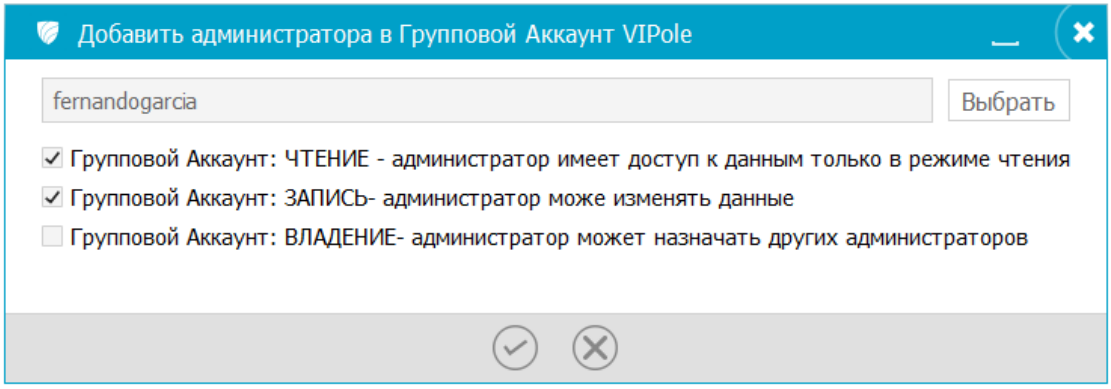
Здесь вы можете добавлять администраторов в Домен безопасности.



Для добавления нового администратора:

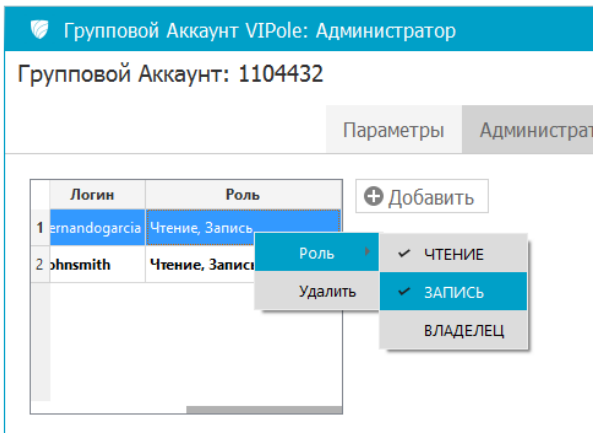
- Нажмите кнопку «Добавить».

- Нажав кнопку «Выбрать», вы можете назначить дополнительным администратором Домена безопасности одного из его членов.



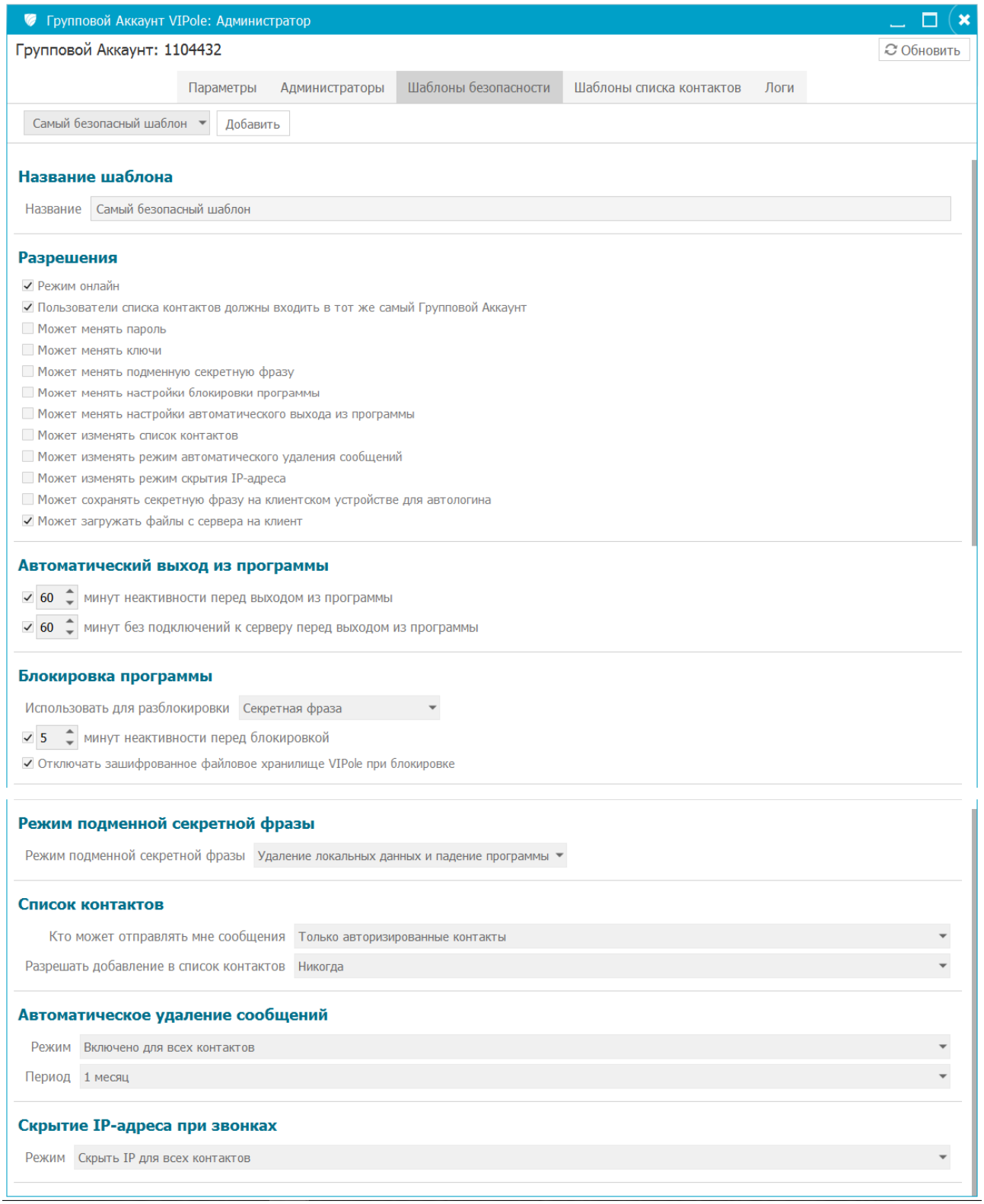
- Отметьте галочками права нового администратора и нажмите ✓

Кликнув по имени администратора правой кнопкой мыши, вы можете отредактировать его права или удалить его из списка администраторов.



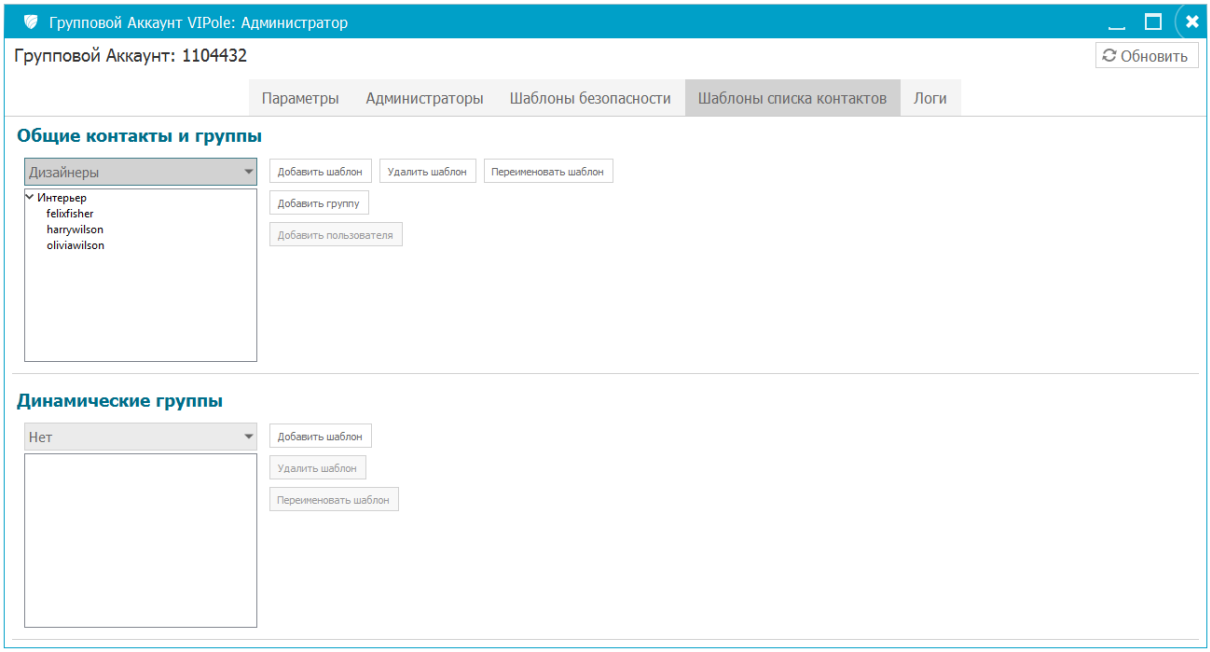
5.2.3. Вкладка «Шаблоны безопасности»

Чтобы создать новый шаблон безопасности, нажмите на кнопку Добавить. Для быстрого поиска и применения шаблона в дальнейшем, задайте его название. Затем сформируйте настройки шаблона, выбрав необходимые опции и нажмите на кнопку Сохранить. Описание разделов шаблона безопасности находится в описании вкладки «Безопасность» окна «Администрирование пользователя».

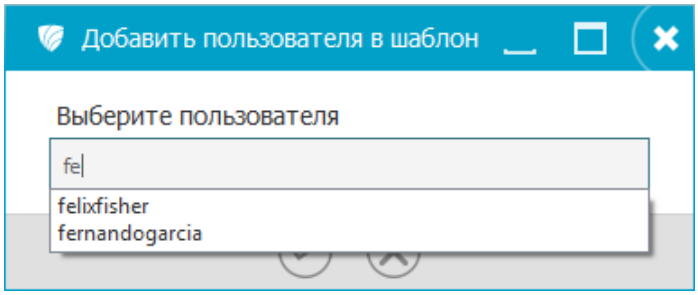


5.2.4. Вкладка «Шаблоны списка контактов»

Здесь администратор Домена безопасности создает и редактирует шаблоны списка контактов пользователя. Также на этой вкладке можно добавлять, удалять или изменять названия динамических групп контактов.



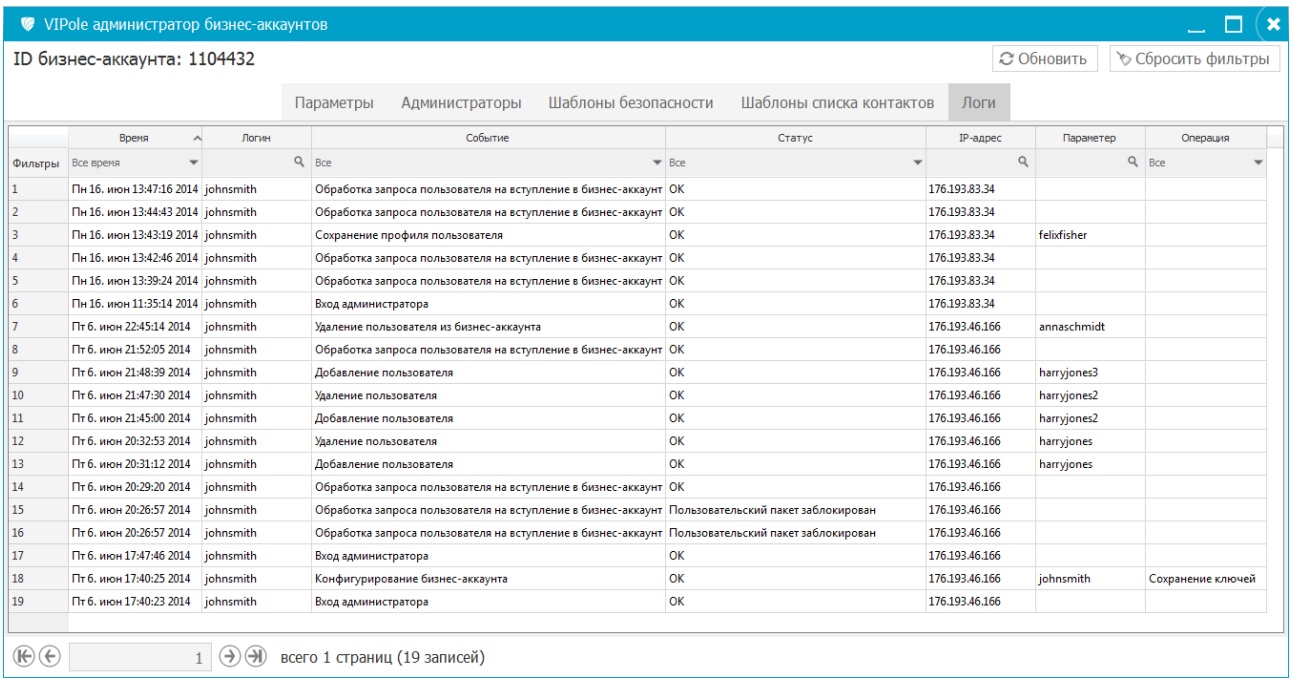
Чтобы добавить пользователя в шаблон контактов, нужно предварительно выбрать группу.



Начните печатать VIPole ID пользователя. После второй буквы появится подсказка по логинам пользователей Домена безопасности.

5.2.5. Вкладка «Логи»

Во вкладке «Логи» вы можете просмотреть активность администраторов Домена безопасности.



	Время	Логин	Событие	Статус	IP-адрес	Параметер	Операция
Фильтры	Все время		Все	Все			Все
1	Пн 16. июн 13:47:16 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.83.34		
2	Пн 16. июн 13:44:43 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.83.34		
3	Пн 16. июн 13:43:19 2014	johnsmith	Сохранение профиля пользователя	OK	176.193.83.34	felixfisher	
4	Пн 16. июн 13:42:46 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.83.34		
5	Пн 16. июн 13:39:24 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.83.34		
6	Пн 16. июн 11:35:14 2014	johnsmith	Вход администратора	OK	176.193.83.34		
7	Пт 6. июн 22:45:14 2014	johnsmith	Удаление пользователя из бизнес-аккаунта	OK	176.193.46.166	annaschmidt	
8	Пт 6. июн 21:52:05 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.46.166		
9	Пт 6. июн 21:48:39 2014	johnsmith	Добавление пользователя	OK	176.193.46.166	harryjones3	
10	Пт 6. июн 21:47:30 2014	johnsmith	Удаление пользователя	OK	176.193.46.166	harryjones2	
11	Пт 6. июн 21:45:00 2014	johnsmith	Добавление пользователя	OK	176.193.46.166	harryjones2	
12	Пт 6. июн 20:32:53 2014	johnsmith	Удаление пользователя	OK	176.193.46.166	harryjones	
13	Пт 6. июн 20:31:12 2014	johnsmith	Добавление пользователя	OK	176.193.46.166	harryjones	
14	Пт 6. июн 20:29:20 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	OK	176.193.46.166		
15	Пт 6. июн 20:26:57 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	Пользовательский пакет заблокирован	176.193.46.166		
16	Пт 6. июн 20:26:57 2014	johnsmith	Обработка запроса пользователя на вступление в бизнес-аккаунт	Пользовательский пакет заблокирован	176.193.46.166		
17	Пт 6. июн 17:47:46 2014	johnsmith	Вход администратора	OK	176.193.46.166		
18	Пт 6. июн 17:40:25 2014	johnsmith	Конфигурирование бизнес-аккаунта	OK	176.193.46.166	johnsmith	Сохранение ключей
19	Пт 6. июн 17:40:23 2014	johnsmith	Вход администратора	OK	176.193.46.166		

5.3. Добавление пользователей

Это окно позволяет управлять пользователями Домена безопасности. Здесь вы можете добавлять пользователей по одному, группой или импортировать данные пользователей из файла формата CSV.

Добавляя одного пользователя, вы можете полностью заполнить его профиль и сгенерировать ключи шифрования. После добавления вам остается только сообщить пользователю пароль и секретную фразу. То же самое возможно и при импорте данных из файла.

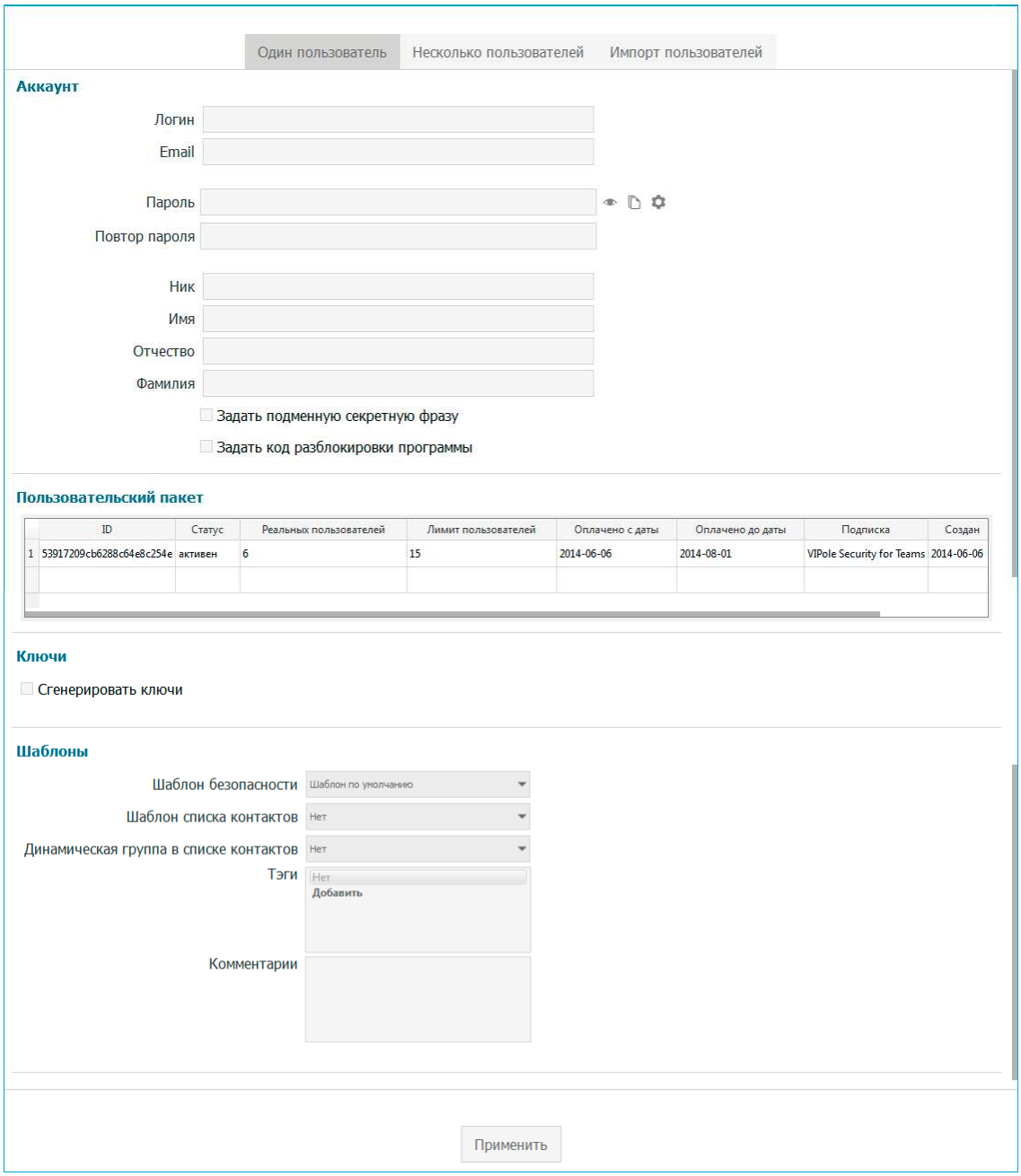
При добавлении группы логины пользователям генерируются автоматически путем добавления чисел в конец буквенного префикса.

5.3.1. Вкладка «Один пользователь»

Для добавления одного пользователя:

- Укажите логин и пароль и подтвердите пароль.
- Затем выберите пользовательский пакет и нажмите «Применить».

Пользовательский пакет используется для учета количества пользователей в вашем Домене безопасности.



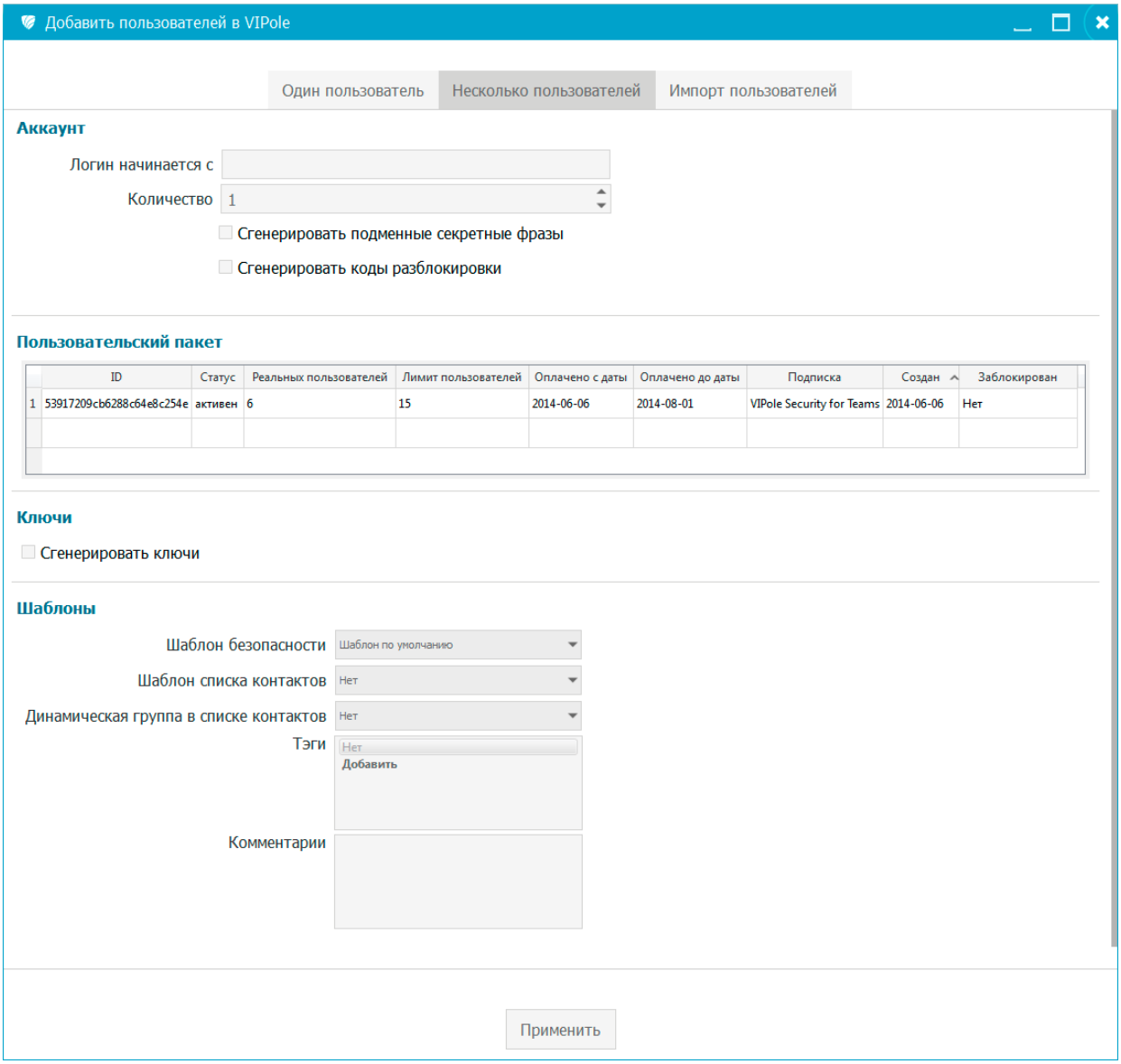
5.3.2. Вкладка «Несколько пользователей»

Для добавления нескольких пользователей:

- Укажите символы, с которых будут начинаться логины, и количество добавляемых пользователей.
- Затем выберите пользовательский пакет и нажмите «Применить».

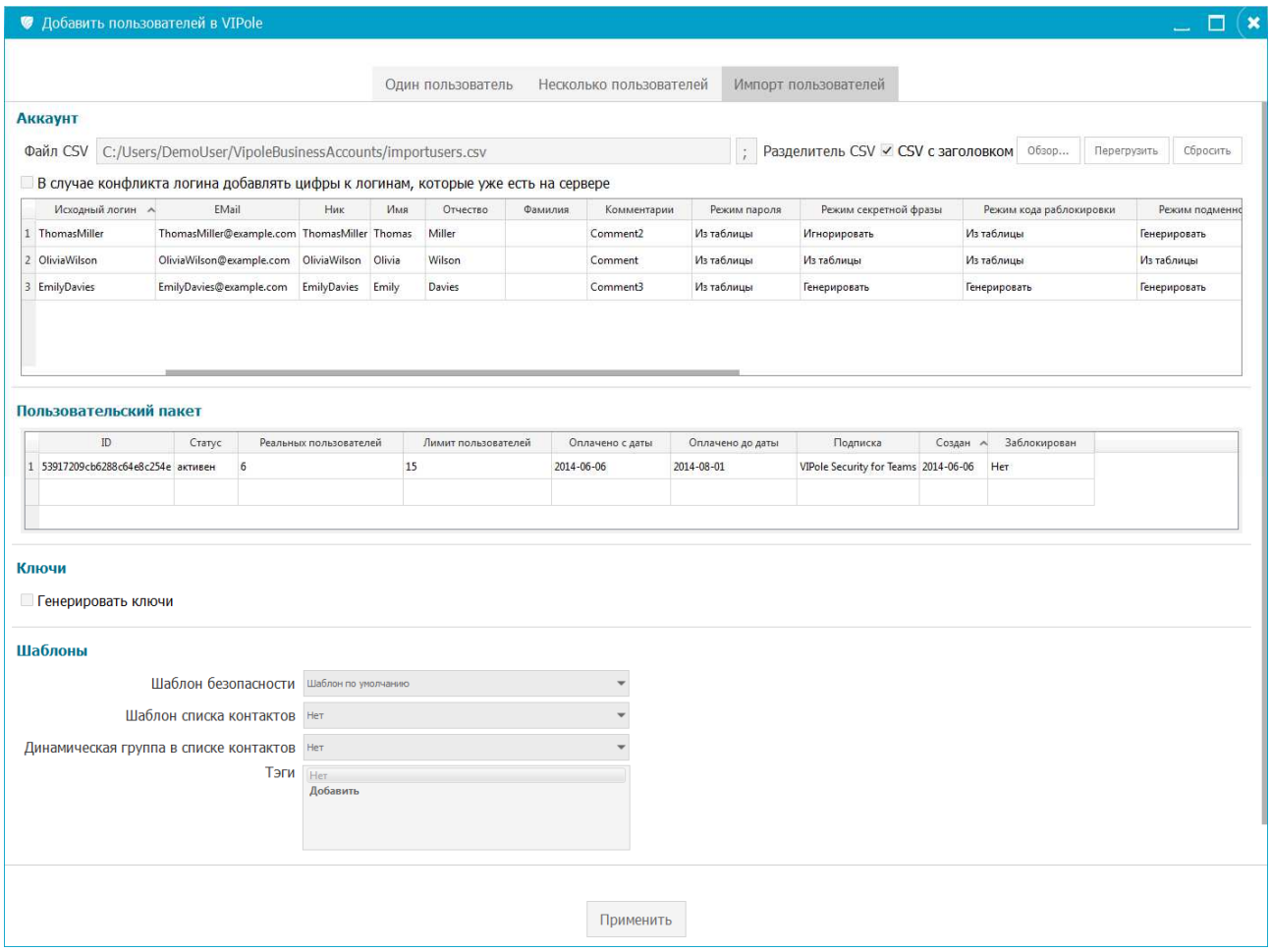
Пользовательский пакет используется для учета количества пользователей в вашем Домене безопасности.

Логины пользователям будут создаваться добавлением числа к начальному набору символов. Например, Designer1, Designer2, Designer3 и так далее.



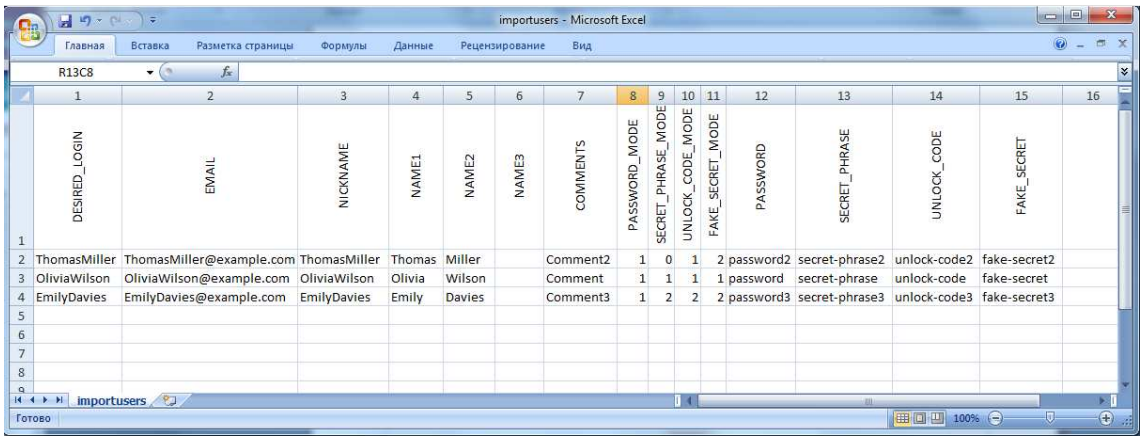
5.3.3. Вкладка «Импорт пользователей»

Здесь можно импортировать группу пользователей из текстового файла или таблицы Excel в формате CSV.



Для импорта пользователей:

- Создайте в Excel таблицу со следующими полями (Названия полей не имеют значения, важна очередность):



DESIRED_LOGIN – исходный логин. Если такой логин уже существует, возможно автоматически добавлять цифры к логину.

EMAIL – адрес электронной почты пользователя

NICKNAME – ник пользователя

NAME1 – имя пользователя

NAME2 – отчество пользователя

NAME3 – фамилия пользователя

COMMENTS – комментарий к учетной записи

PASSWORD_MODE –

1 – пароль берется из загруженной таблицы

2 – пароль генерируется автоматически

SECRET_PHRASE_MODE –

0 – игнорируется (пользователь должен будет сам создать секретную фразу)

1 – пароль берется из загруженной таблицы

2 – пароль генерируется автоматически

UNLOCK_CODE_MODE –

0 – игнорируется (пользователь должен будет сам установить код разблокировки)

1 – код разблокировки берется из загруженной таблицы

2 – код разблокировки генерируется автоматически

FAKE_SECRET_MODE –

0 – игнорируется (пользователь должен будет сам создать подменную секретную фразу)

1 – подменная секретная фраза берется из загруженной таблицы

2 – подменная секретная фраза генерируется автоматически

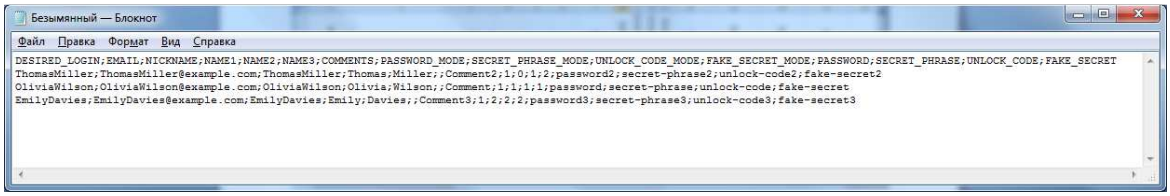
PASSWORD – пароль для входа для скачивания профиля

SECRET_PHRASE – секретная фраза

UNLOCK_CODE – код разблокировки

FAKE_SECRET – подменная секретная фраза

- Сохраните таблицу в формате CSV. Это текстовый файл следующего формата:



- В поле «Разделитель CSV» поставьте символ **;**
- Галочка в поле «CSV с заголовком» означает, что первая строка файла CSV содержит имена полей, как в примере.
- Нажмите кнопку «Обзор» и выберите файл для импорта. В таблице появятся импортированные записи пользователей. Если при импорте произошла ошибка, например, вы указали неправильную строку email, в колонке «Статус» появится разъясняющая ошибку красная надпись.

- После этого выберите пользовательский пакет, в который вы хотите добавить пользователей. Укажите шаблоны, которые будут применены ко всем импортируемым пользователям и нажмите кнопку «Применить».

1.3.4 Вкладка LDAP

Интеграция с LDAP(Lightweight Directory Access Protocol) в разы ускоряет разворачивание Корпоративного сервера VIPole, так как при этом нет необходимости вручную вносить в систему данные каждого нового пользователя.

Есть два способа интеграции Microsoft Active Directory(AD)/LDAP с сервером VIPole:

1. Импорт пользователей в базу VIPole из AD/LDAP.
    - Пароли пользователей при этом не импортируются.
    - Аутентификация пользователей при подключении к серверу VIPole осуществляется с использованием сервера AD/LDAP.
2. Экспорт пользователей из AD/LDAP в CSV файл.
    - CSV файл может быть импортирован в базу сервера VIPole (возможно, если это необходимо, после редактирования).
    - Пароли в этом случае автоматически генерируются при импорте или берутся из CSV файла.

Импорт пользователей в Домен безопасности VIPole осуществляется владельцем Домена.

Для начала работы с AD/LDAP сервером выполните настройку сервера VIPole, используя следующие параметры файла конфигурации **server.config**:

Включите поддержку AD/LDAP
ldap-enabled = 1

Укажите уникальное имя (DN) пользователя AD/LDAP, которому разрешён импорт данных из дерева AD/LDAP
ldap-admin-dn = CN=Admin,CN=Users,DC=vipole,DC=ldap,DC=sample

Укажите пароль пользователя, которому разрешен импорт
ldap-admin-password = SecretPassword

URI AD/LDAP сервера
ldap-uri = ldap://192.168.1.155

DN, с которого начинается поиск пользователей по поддереву (в поддереве должен быть хотя бы один пользователь, чтобы сервер VIPole смог проверить корректность подключения с серверу AD/LDAP)
ldap-users-search-base = CN=Users,DC=vipole,DC=ldap,DC=sample

Имя атрибута, который используется как логин пользователя
ldap-users-login-mapping=cn

После настройки этих параметров перезапустите сервер VIPole.

Импорт пользователей в базу VIPole из AD/LDAP

Операции импорта пользователей выполняются с помощью консольной утилиты vipole-ldap или с помощью расширения «Администратор VIPole» программы-клиента.

Импорт пользователей с помощью консольной утилиты vipole-ldap:

Параметры работы утилиты vipole-ldap задаются в командной строке:

-l [--login] - логин администратора Домена безопасности VIPole, в который будет выполняться импорт пользователей.
--passwd - пароль администратора, указанного параметром **–login.**
--passwd-file - файл с паролем администратора (используется вместо --passwd).
--domain - доменное имя вашего сервера VIPole (это имя, которое добавляется к логину после символа @, например, admin@example.com)

--server-host arg (=127.0.0.1) - IP адрес сервера VIPole

--server-port arg (=37210) - порт сервера VIPole.

--certificate arg - путь к файлу цепочки сертификатов сервера VIPole, который указан в параметре **certificate-chain-file** в файле server.config.

--security-domain arg - идентификатор Домена безопасности (необходимо указывать в случае, если у администратора домена их несколько). Идентификатор можно посмотреть при создании Домена безопасности или на вкладке «Параметры» расширения «Администратор VIPole» клиентского приложения.

--admin-password arg - административный пароль для управления Доменом безопасности (этот пароль создается и вводится при запуске расширения «Администратор VIPole»).

--base-dn arg - DN, с которого начинается поиск пользователей. Если не указано – используется значение параметра ldap-users-search-base файла конфигурации сервера VIPole.

--filter arg (=(|(&(objectCategory=person)(objectClass=user))(objectClass=inetOrgPerson)) - фильтр записей пользователей, в соответствии с которым происходит отбор. Подробное описание синтаксиса и примеры см. Active Directory: LDAP Syntax Filters.

--skip-imported [0|1] (=0) - пропуск уже существующих пользователей при импорте.

--morph-login - в случае дублирования логина пользователя добавляет в конце логина уникальное число.

-t [--timeout] arg (=300) - время ожидания отклика AD/LDAP сервера в секундах.

--dry-run - добавление пользователей в базу не производится, а выводится только информация о пользователях, которые были добавлены.

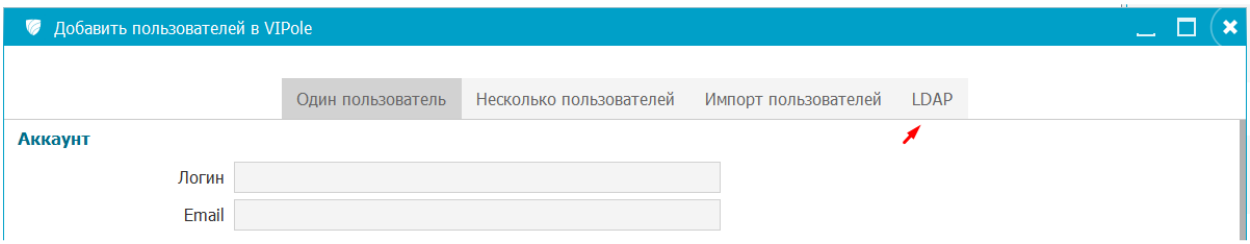
--mapping - установка соответствия полей при импорте базы LDAP и внутренней базы пользователей сервера VIPole. При импорте в базе VIPole можно заполнить следующие поля: login, name1, name2, name3, email, nickname, comments.

Например, **--mapping comments=description** устанавливает соответствие между значением атрибута **description** базы LDAP и полем **comments** базы данных пользователей сервера VIPole.

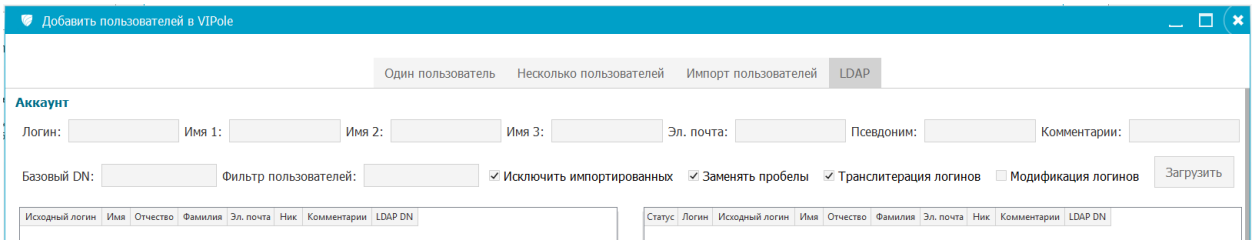
Чтобы указать соответствие нескольких полей, нужно использовать несколько параметров **–mapping.**

Импорт пользователей с помощью расширения «Администратор VIPole» клиентского приложения:

Выберите вкладку LDAP.



Откроется окно импорта LDAP



Поля «Логин», «Имя 1», «Имя 2», «Имя 3», «Эл.почта», «Псевдоним», «Комментарии» предназначены для маппинга. В них можно ввести имена полей базы LDAP, которые будут импортироваться в соответствующие поля внутренней базы пользователей сервера VIPole.

«Базовый DN» - DN, с которого начинается поиск пользователей. Если не указано – используется значение параметра ldap-users-search-base файла конфигурации сервера VIPole.

«Фильтр пользователей» - Фильтр записей пользователей, в соответствии с которым происходит отбор. Подробное описание синтаксиса и примеры: Active Directory: LDAP Syntax Filters.

«Исключить импортированных» - Не импортировать уже существующих пользователей

«Заменять пробелы» - пробелы в поле будут заменены на подчеркивание.

«Транслитерация логинов» - поле с кириллическими символами будет заменено на латинские символы транслитерацией.

«Модификация логинов» - в случае дублирования логина добавляется уникальное число в конце такого логина.

Для импорта обязательно заполните поле «Базовый DN». После нажатия кнопки «Загрузить» в таблице слева появится список пользователей из базы LDAP. Если поля в таблице заполняются неправильно, измените маппинг, указав в полях «Имя 1», «Имя 2»,

«Имя 3», «Эл.почта», «Псевдоним», «Комментарии» имена атрибутов, соответствующие вашему шаблону базы LDAP.

Выберите пользователей, которых необходимо импортировать в VIPole кликом мыши:

- Клик с нажатой клавишей Ctrl выделяет несколько строк.
- Клик с нажатой клавишей Shift выделяет диапазон строк.
- Кнопкой ➡ перенесите выбранные записи в правую таблицу.

После нажатия клавиши «Применить» пользователи, перечисленные в таблице справа, будут импортированы в базу VIPole.
Опция «Сгенерировать ключи» позволяет сразу генерировать для импортируемого пользователя ключи шифрования. При этом пароль и секретная фраза генерируются автоматически. Посмотреть их администратор может на вкладке «Безопасность» окна «Администрирование пользователя VIPole».
При импорте к пользователю могут быть применены шаблоны безопасности и шаблоны списка контактов, которые необходимо выбрать перед нажатием клавиши «Применить».

Экспорт пользователей из AD/LDAP в CSV-файл с помощью консольной утилиты vipole-ldap.

Если консольной утилите vipole-ldap среди других параметров указать параметр **`--csv-file arg`**, то будет выполняться экспорт данных в CSV файл.

С этой опцией автоматически включается опция **`--dry-run`**. Таким образом, импорта пользователей в базу не происходит. Все остальные параметры работают как при импорте в базу VIPole.

CSV файл может быть при необходимости отредактирован и затем импортирован в базу VIPole с помощью расширения «Администратор VIPole» в клиентском приложении для компьютера.

> Обратите внимание, в различных реализациях AD/LDAP (в том числе AD в различных версиях Windows Server) используется различная схема именования атрибутов.
>
> Поэтому перед импортом пользователей обязательно убедитесь в соответствии импортируемых полей.

> Если вы используете импорт пользователей в базу VIPole, сначала выполняйте утилиту vipole-ldap с параметром **`--dry-run`** и по логу программы убедитесь, что импортируются нужные пользователи и дополнительные поля заполнены правильно.

> Для просмотра схемы базы LDAP, названия атрибутов и т.п. можно использовать программу LDAP Admin или подобные.

Пример импорта новых пользователей из AD vipole.ldap.sample .

Поиск ведется среди всех пользователей, логины которых начинаются на testuser (напр. testuser04 или testusername). Пользователи импортируются как testuser04@vipole.ldap.

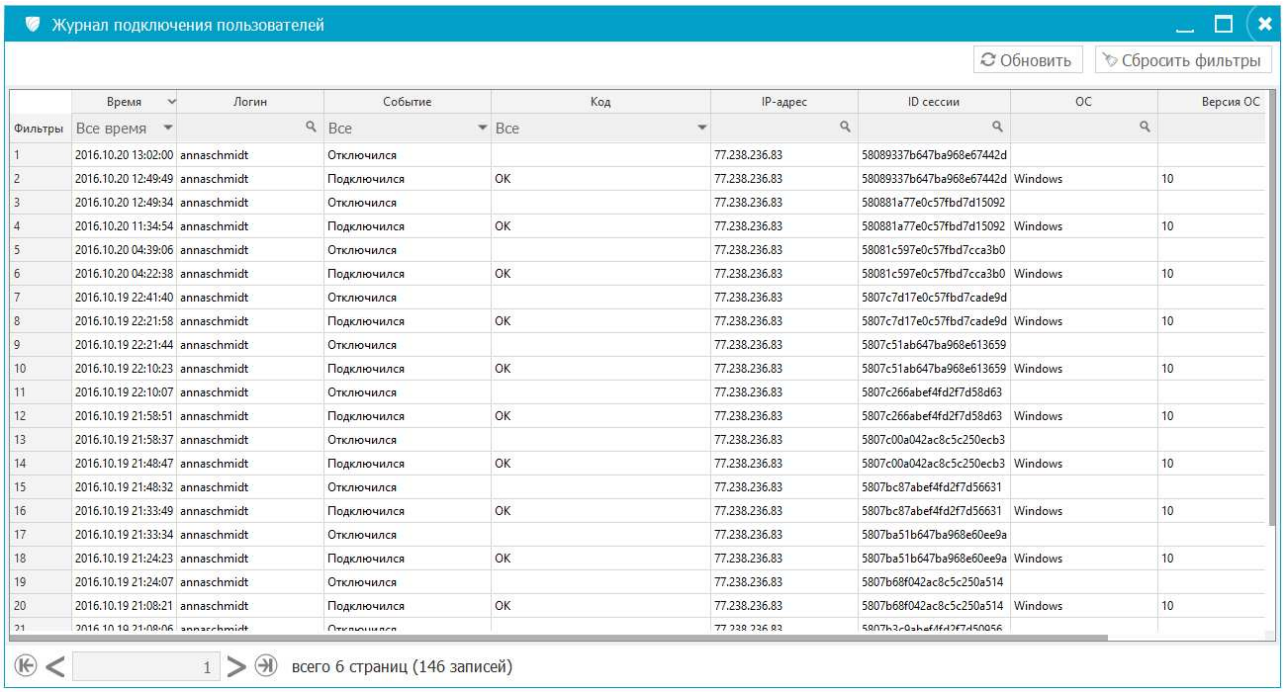
```
vipole-ldap  \
--admin-password 1234567890  \
--base-dn CN=Users,DC=vipole,DC=ldap,DC=sample \
--certificate /etc/vipole/cacert.pk \
--domain vipole.ldap \
--login sd_admin --passwd 12345678 \
--server-host 192.168.1.175
--filter "(CN=testuser*)"
```

Экспорт в CSV-файл пользователей, с переносом значения атрибута «description» из записи LDAP в поле «comments» базы пользователей VIPole и логин которых заканчивается числом, большим 31 (напр. testuser_41 или testuser_55).

```
vipole-ldap --admin-password 1234567890 \
--base-dn OU=OfficeInSPB,DC=vipole,DC=ldap,DC=sample\
--certificate /etc/vipole/cacert.pk \
--domain vipole.ldap \
--login sd_admin \
--passwd 12345678 \
--server-host 192.168.1.175 \
--server-port 37210 \
--filter "(CN>=testuser_31)" \
--mapping comments=description \
--csv-file ldap-users.csv
```

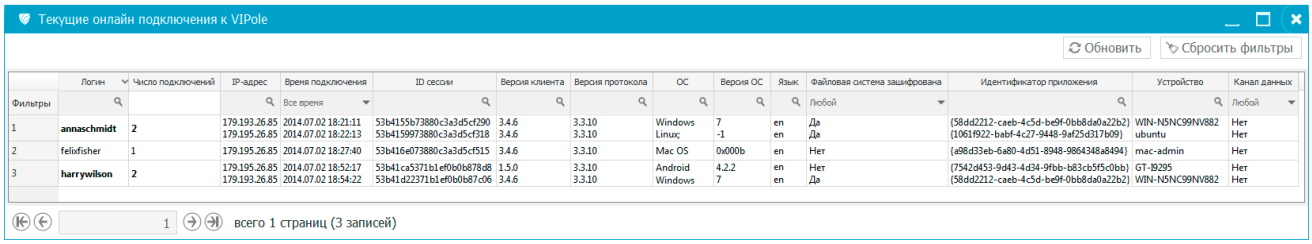
6. Журнал подключений

Здесь фиксируются подключения и отключения участников вашего Домена безопасности, IP-адрес и версия клиента.



	Время	Логин	Событие	Код	IP-адрес	ID сессии	ОС	Версия ОС
Фильтры	Все время		Все	Все				
1	2016.10.20 13:02:00	annaschmidt	Отключился		77.238.236.83	58089337b647ba968e67442d		
2	2016.10.20 12:49:49	annaschmidt	Подключился	OK	77.238.236.83	58089337b647ba968e67442d	Windows	10
3	2016.10.20 12:49:34	annaschmidt	Отключился		77.238.236.83	580881a77e0c57fbd7d15092		
4	2016.10.20 11:34:54	annaschmidt	Подключился	OK	77.238.236.83	580881a77e0c57fbd7d15092	Windows	10
5	2016.10.20 04:39:06	annaschmidt	Отключился		77.238.236.83	58081c597e0c57fbd7cca3b0		
6	2016.10.20 04:22:38	annaschmidt	Подключился	OK	77.238.236.83	58081c597e0c57fbd7cca3b0	Windows	10
7	2016.10.19 22:41:40	annaschmidt	Отключился		77.238.236.83	5807c7d17e0c57fbd7cade9d		
8	2016.10.19 22:21:58	annaschmidt	Подключился	OK	77.238.236.83	5807c7d17e0c57fbd7cade9d	Windows	10
9	2016.10.19 22:21:44	annaschmidt	Отключился		77.238.236.83	5807c51ab647ba968e613659		
10	2016.10.19 22:10:23	annaschmidt	Подключился	OK	77.238.236.83	5807c51ab647ba968e613659	Windows	10
11	2016.10.19 22:10:07	annaschmidt	Отключился		77.238.236.83	5807c266abef4fd2f7d58d63		
12	2016.10.19 21:58:51	annaschmidt	Подключился	OK	77.238.236.83	5807c266abef4fd2f7d58d63	Windows	10
13	2016.10.19 21:58:37	annaschmidt	Отключился		77.238.236.83	5807c00a042ac8c5c250ecb3		
14	2016.10.19 21:48:47	annaschmidt	Подключился	OK	77.238.236.83	5807c00a042ac8c5c250ecb3	Windows	10
15	2016.10.19 21:48:32	annaschmidt	Отключился		77.238.236.83	5807bc87abef4fd2f7d56631		
16	2016.10.19 21:33:49	annaschmidt	Подключился	OK	77.238.236.83	5807bc87abef4fd2f7d56631	Windows	10
17	2016.10.19 21:33:34	annaschmidt	Отключился		77.238.236.83	5807ba51b647ba968e60ee9a		
18	2016.10.19 21:24:23	annaschmidt	Подключился	OK	77.238.236.83	5807ba51b647ba968e60ee9a	Windows	10
19	2016.10.19 21:24:07	annaschmidt	Отключился		77.238.236.83	5807b68f042ac8c5c250a514		
20	2016.10.19 21:08:21	annaschmidt	Подключился	OK	77.238.236.83	5807b68f042ac8c5c250a514	Windows	10
21	2016.10.19 21:08:06	annaschmidt	Отключился		77.238.236.83	5807b3c8abef4fd2f7d50956		

7. Пользователи онлайн



	Логин	Число подключений	IP-адрес	Время подключения	ID сессии	Версия клиента	Версия протокола	ОС	Версия ОС	Язык	Файловая система зашифрована	Идентификатор приложения	Устройство	Канал данных
Фильтры				Все время							Любой			Любой
1	annaschmidt	2	179.193.26.85 179.195.26.85	2014.07.02 18:21:11 2014.07.02 18:22:13	53b4155b73880c3a3d5cf290 53b4159973880c3a3d5cf318	3.4.6 3.4.6	3.3.10 3.3.10	Windows Linux	7 -1	en en	Да Да	{58dd2212-caeb-4c5d-be9f-0bb8da0a22b2} {1061f922-babf-4c27-9448-9af25d317b09}	WIN-N5NC99NV882 ubuntu	Нет Нет
2	felixfisher	1	179.195.26.85	2014.07.02 18:27:40	53b416e073880c3a3d5cf515	3.4.6	3.3.10	Mac OS	0x000b	en	Нет	{a98d33eb-6a80-4d51-8948-9864348a8494}	mac-admin	Нет
3	harrywilson	2	179.195.26.85 179.193.26.85	2014.07.02 18:52:17 2014.07.02 18:54:22	53b41ca53710b1ef0b0b878d8 53b41d22371b1ef0b0b87c06	1.5.0 3.4.6	3.3.10 3.3.10	Android Windows	4.2.2 7	en en	Нет Да	{7542d453-9d43-4d34-9fbb-b83cb5f5c0bb} {58dd2212-caeb-4c5d-be9f-0bb8da0a22b2}	GT-I9295 WIN-N5NC99NV882	Нет Нет

В этом окне показывается список участников вашего Домена безопасности, которые находятся онлайн в данный момент. Показываются все подключения, если их несколько. Вы можете посмотреть IP-адрес компьютера, операционную систему, версию клиента, а также зашифрована ли файловая система на компьютере пользователя.