

Инструкция по установке и эксплуатации ПО PGI

Содержание

Оглавление

1 Введение	3
1.1 Цель документа	3
1.2 Термины и сокращения	3
2 Требования к аппаратному и системному программному обеспечению	4
3 Установка ПО	5
3.1 Описание системы PGI	5
3.2 Отказоустойчивость и поддержка кластера	5
3.3 Первоначальное развертывание PGI	6
3.3.1 Настройка Front-end	6
3.3.2 Настройка Back-end	7
3.3.3 Обновление системы PGI	8
3.3.4 Восстановление системы PGI после аварии	8
4 Эксплуатация ПО	10
4.1 Функциональные возможности	10
4.1.1 Доступ и привилегии пользователя	10
4.2 Функции пользователя консоли	10
4.3 Раздел Configuration	10
4.3.1 Менеджмент протоколов	10
4.3.2 Управление хостами	10
4.3.3 Управление эмитентами	10
4.3.4 Управление платежными системами	11
4.3.5 Менеджмент брендов	11
4.3.6 Управление параметрами платежных карт	11
4.3.7 Настройка параметров аутентификации	11
4.3.8 Просмотр правил Frictionless Flow	11
4.4 Раздел System preferences	12
4.5 Раздел Users	12
4.6 Управление отображением информации на страницах	12
4.7 Смена пароля пользователем	12
4.8 Завершение работы с консолью	12

1 Введение

1.1 Цель документа

Данный документ содержит описание по установке ПО, эксплуатации и функциональных возможностей пользователя партнерской консоли.

1.2 Термины и сокращения

В данном подразделе определяются термины и сокращения, используемые в документе.

Таблица 1 Термины и сокращения

Термин	Описание
PGI	Payguide™ Issuer - программный комплекс, обеспечивающий проведение аутентификации клиента при осуществлении безопасных электронных платежей.
3-D Secure	Протокол аутентификации владельца карты, который используется как дополнительный уровень безопасности для интернет-платежей.

2 Требования к аппаратному и системному программному обеспечению

Для обеспечения доступности на уровне 99.95% и производительности в 500 платежных транзакций в секунду, при высокой скорости исполнения базового запроса (не более 2 секунд собственной совокупной вносимой задержки), система должна эксплуатироваться на следующем программно-аппаратном комплексе (или аналогичном не меньшей производительности).

Назначение	Аппаратное обеспечение	Программное обеспечение	Кол-во узлов
Фронтальный сервер	CPU: 4-Core Xeon E5-4600 v2 RAM: 16 Gb HDD: SAS 500Gb*2 7.2K RAID-1	Минимальные требования к ОС: OS – CentOS Linux release 7.8.2003 (Core); рекомендуемые требования к ОС:– CentOS Linux release 7.8.2003 (Core); JDK 8 или OpenJDK 8	2
Сервер приложения	CPU: 2x 6-Core Xeon E5-4600 v2 RAM: 32 Gb HDD: SAS 300Gb*4 15K RAID-10	Минимальные требования к ОС: CentOS Linux release 7.8.2003 (Core); рекомендуемые требования к ОС: S – CentOS Linux release 7.8.2003 (Core); JDK 8 или OpenJDK 8	2
Сервер СУБД	CPU: 2x 6-Core Xeon E5-4600 v2 RAM: 32 Gb HDD: 500Gb	OS – CentOS Linux release 7.8.2003 (Core); PostgreSQL 14: минимальная конфигурация PostgreSQL 14: Standard Edition, рекомендуемая конфигурация PostgreSQL 14.	2
СХД	SAN/8Gbit/10 000 IOPS		1
Аппаратный модуль шифрования	PCI PL220		2

С целью повышения эффективности использования оборудования допускается использование технологии виртуализации для фронтальных серверов и серверов приложений. Для снижения степени влияния виртуализации на производительность серверов и работающих на них приложений рекомендуется 100% резервирование оперативной памяти, назначение виртуальным серверам выделенных ядер и установка приоритетов для операций дискового ввода-вывода.

3 Установка ПО

3.1 Описание системы PGI

Схема развертывания Payguide™ Issuer предполагает использование выделенного демилитаризованного сегмента DMZ для создания дополнительного уровня безопасности.

Система разделена на 2 части: front-end и back-end.

Компоненты front-end располагаются в сегменте DMZ и ориентированы на обработку большого числа сетевых соединений и интенсивный обмен сообщениями с внешними системами и клиентами. Сегмент DMZ отделен межсетевым экраном от Интернета и сегмента LAN.

Back-end сервер расположен в сегменте LAN. На нем реализована основная бизнес-логика Payguide™ Issuer. Связь между частями front-end и back-end реализована через межсетевой экран.

Отличительной особенностью схемы является обратное подключение с узлов приложения в сегменте LAN к фронтальным компонентам в сегменте DMZ. Такая схема позволяет полностью блокировать любые входящие запросы в сегмент LAN.

Каждый узел может работать с несколькими аппаратными модулями шифрования, используемых для безопасного хранения криптографических ключей и шифрования конфиденциальной информации в соответствии с требованиями стандарта PCI DSS.

Payguide™ Issuer использует эффективное пакетно-оптимизированное шифрование для безопасного хранения логов транзакций, БД клиентов, конфигураций и схем протоколов.

3.2 Отказоустойчивость и поддержка кластера

Для обеспечения высокой доступности система поддерживает работу в кластере. В этом режиме происходит дублирование всех компонентов и сетевых подключений.

При работе в кластере поток входящих запросов равномерно распределяется на компоненты front-end средствами сетевого маршрутизатора.

Компоненты front-end предназначены для обработки большого количества сетевых подключений и обмена сообщениями с клиентами и внешними системами.

Компоненты front-end не хранят какого-либо состояния и аварийное отключение любого из них, в худшем сценарии, может привести только к прерыванию активных запросов от клиентов или внешних систем, что будет корректно обработано системой. Все последующие запросы будут маршрутизироваться на оставшийся узел, сохраняя полную функциональность системы.

Весь поток входящих сообщений с каждого из front-end узлов транслируется по бинарному протоколу на оба узла приложения. При этом обработкой запросов в каждый момент времени занимается только один из узлов (основной). Второй узел находится в горячем резерве. Такая схема позволяет организовать эффективную репликацию состояния основного узла на резервный в режиме реального времени и выполнять практически моментальное переключение на резервный узел, как при штатном останове, так и при аварийном завершении работы основного узла.

Кроме репликации состояния в резервном узле происходит постоянная фиксация состояния приложения в БД, что позволяет системе корректно восстановиться после перезапуска, даже при отсутствии резервного узла. Фиксация состояния приложения в БД выполняется инкрементально для минимизации накладных расходов, и атомарно, что гарантирует согласованность данных в БД и состояния приложения после восстановления.

Аппаратные модули шифрования используются для безопасного хранения криптографических ключей и шифрования конфиденциальной информации в соответствии с требованиями стандарта PCI DSS. Схема развертывания предполагает использование двух аппаратных модулей шифрования с общим набором криптографических ключей, что позволяет Payguide™ Issuer осуществлять балансировку нагрузки между модулями и обеспечивать бесперебойную работу при выходе из строя одного из них.

Узлы приложения поддерживают прозрачное переключение нагрузки между серверами БД. Сохранность клиентских сессий и незавершенных транзакций обеспечивается и при аварийном переключении. Определение доступных узлов БД и переключение нагрузки на них происходит в автоматическом режиме с использованием механизмов, предоставляемых СУБД PostgreSQL и не требует внесения изменений в конфигурацию приложения.

При условии корректного функционирования БД система обеспечивает непрерывное обслуживание клиентов в случае планового или аварийного останова любого одного узла кластера. При этом возможны следующие ситуации:

- Плановый останов front-end узла. Полностью прозрачен для клиентов.
- Аварийный останов front-end узла. Возможны потери активных клиентских соединений и запросов, а также кратковременное увеличение времени отклика для новых запросов.
- Плановый или аварийный останов резервного узла приложения. Полностью прозрачен для клиентов.
- Плановый останов активного узла приложения. Кратковременное увеличение времени обработки запросов (до 10 секунд).
- Аварийный останов активного узла приложения. Кратковременное увеличение времени обработки запросов (до 30-60 секунд). Данное время необходимо резервному узлу для гарантированного переключения активности на себя.

3.3 Первоначальное развертывание PGI

3.3.1 Настройка Front-end

1. Скопировать содержимое архива `aces-front-*.zip` в домашний каталог;
2. Назначить файлам `aces-front`, расположенному в `$HomeDir/.../bin`, права доступа 755;
3. В файле настроек `startup.conf` в `$HomeDir/.../conf` произвести настройку необходимых параметров, описанных в таблице:

Параметр	Назначение параметра	Значение по умолчанию
<code>APP_NAME</code>	Название приложения	<code>aces</code>
<code>APP_LONG_NAME</code>	Название узла приложения	<code>aces-front</code>
<code>JAVAPATH</code>	Путь к библиотекам <code>java</code>	<code>java</code>
<code>DEFAULT_STDOUT_LOGS</code>	Путь к стандартному выводу приложения	<code>/dev/null 2>&1</code>
<code>PATH_TO_LIB</code>	Путь к библиотекам приложения	<code>"\$BASEDIR/lib/*"</code>
<code>PATH_TO_CONF</code>	Путь к папке с файлом конфигурации	<code>"\$BASEDIR/conf/"</code>
<code>PIDDIR</code>	Путь для хранения ID процесса приложения	<code>"\$BASEDIR/logs"</code>
<code>PIDFILE</code>	Название файла для хранения ID процесса приложения	<code>\$PIDDIR/\$APP_NAME.pid</code>
<code>Java_additional_1=-Dmetrics.graphite.prefix</code>	Настройка префикса для сбора логов	<code>acs</code>
<code>Java_additional_2=-Dmetrics.graphite.tags</code>	Настройка тега для сбора логов	<code>node=front</code>
<code>Java_additional_3=-Dmetrics.graphite.host</code>	Хост для отправки логов	<code>10.11.12.13</code>
<code>Java_additional_4=-Dmetrics.graphite.interval=10</code>	Настройка интервала отправления логов приложения, измеряется в секундах.	<code>10</code>
<code>Java_additional_5=-Dmetrics.graphite.port=9109</code>	Порт для отправки логов	<code>9109</code>
<code>java_initmemory</code>	Минимальное значение используемой памяти RAM	<code>1024m</code>
<code>java_maxmemory</code>	Максимальное значение используемой памяти RAM	<code>4096m</code>

4. Настроить рекомендованный набор шифрования TLS1.2 для безопасного клиентского HTTPS-соединения. Установить переменные в файле `startup.conf`
5. Указать порт подключения к front-end серверу в файле `aces-front.properties` в `$HomeDir/.../conf`
6. Добавить символическую ссылку на `$HomeDir/.../bin/aces-front` в `/etc/init.d/` для запуска как службы;

Команды скрипта `/bin/aces-front` для управления демоном приложения PGI на узлах:

- `Start` – запуск приложения;
- `Stop` – остановка приложения;
- `Restart` – перезапуск приложения.
- `Status` – статус приложения

3.3.2 Настройка Back-end

1. Скопировать содержимое архива `aces-back-*.zip` в домашний каталог `$Home_Dir` с правами доступа 777;
2. Назначить файлам `aces`, расположенному в `$HomeDir/.../bin`, права доступа 755;
3. В файле настроек `startup.conf` в `$HomeDir/.../conf` произвести настройку необходимых параметров, описанных в таблице:

Параметр	Назначение параметра	Значение по умолчанию
<code>APP_NAME</code>	Название приложения	<code>aces</code>
<code>APP_LONG_NAME</code>	Название узла приложения	<code>aces-front</code>
<code>JAVAPATH</code>	Путь к библиотекам <code>java</code>	<code>java</code>
<code>DEFAULT_STDOUT_LOGS</code>	Путь к стандартному выводу приложения	<code>/dev/null 2>&1</code>
<code>PATH_TO_LIB</code>	Путь к библиотекам приложения	<code>"\$BASEDIR/lib/*"</code>
<code>PATH_TO_CONF</code>	Путь к папке с файлом конфигурации	<code>"\$BASEDIR/conf/"</code>
<code>PIDDIR</code>	Путь для хранения ID процесса приложения	<code>"\$BASEDIR/logs"</code>
<code>PIDFILE</code>	Название файла для хранения ID процесса приложения	<code>\$PIDDIR/\$APP_NAME.pid</code>
<code>Java_additional_1=-Dmetrics.graphite.prefix</code>	Настройка префикса для сбора логов	<code>acs</code>
<code>Java_additional_2=-Dmetrics.graphite.tags</code>	Настройка тега для сбора логов	<code>node=front</code>
<code>Java_additional_3=-Dmetrics.graphite.host</code>	Хост для отправки логов	<code>10.11.12.13</code>
<code>Java_additional_4=-Dmetrics.graphite.interval=10</code>	Настройка интервала отправления логов приложения, измеряется в секундах.	<code>10</code>
<code>Java_additional_5=-Dmetrics.graphite.port=9109</code>	Порт для отправки логов	<code>9109</code>
<code>java_initmemory</code>	Минимальное значение используемой памяти RAM	<code>1024m</code>
<code>java_maxmemory</code>	Максимальное значение используемой памяти RAM	<code>4096m</code>

4.
 - Указать путь установки актуальной версии пакета `JDK` в параметре `JAVA`;
 - Настроить рекомендованный набор алгоритмов шифрования для безопасного `HTTPS`-соединения. Установить переменные в файле `startup.conf`;
 - Выставить настройку во `startup.conf` для возможности указывать нужные `cipher suites` на версии `openjdk version «1.8.0_101»` и более ранних;
 - Выставить настройки в `startup.conf` для конфигурации `DataExtractWorker`;
 - Выставить настройку для возможности принимать аутентификационный запрос с любых `ip`-адресов;
 - Настроить рекомендованный набор шифрования `TLS1.2` для безопасного клиентского `HTTPS`-соединения. Установить переменные в файле `startup.conf`, добавив параметр `Java_additional_N`;
5. Заполнить параметры файла `aces.properties` в `$HomeDir/.../conf`.

В файле каждого бэка содержатся параметры всего кластера, т.е. адреса всех фронтов, всех бэков и всех административных консолей.

В примере используется рабочая конфигурация для старта кластера. Необходимо заменить `IP` адреса и порты на те, которые вы будете использовать.

`N` - является порядковым номером, т.е. в примере ниже под 1 номером описаны настройки для одного `back` и все настройки для этого `back` узла будут под номером 1. Для `front` узла используется 2 порядковый номер, также все настройки для этого фронт узла будут под 2 номером. Если понадобится дополнительно добавить `front` узлы и/или `back` узлы, то в файл конфигурации `aces.properties` необходимо добавить дополнительные настройки для `front` узлов и/или `back` узлов, `N` нужно использовать по порядку. Настройки `aces.properties` должны быть одинаковые для всех узлов кластера.



Добавить символическую ссылку на `$HomeDir/.../bin/aces /etc/init.d/aces` для запуска как службы;
Команды скрипта `/bin/escr-back` для управления демоном приложения PGA на узлах:

- Start – запуск приложения;
 - Stop – остановка приложения;
 - Restart – перезапуск приложения.
6. Выполнить первый запуск `Pauguide™ Issuer`. При этом сервер может использовать два варианта создания таблиц в базе данных – это автоматический и ручной. Автоматический рекомендуется использовать в тестовой среде, а в боевой среде рекомендуется использовать ручной метод, во избежание проблем с БД. При этом сервер может сгенерировать файл `unrun.sql` с sql скриптами для создания таблиц и индексов базы данных.
- 6.1. Автоматическое создание таблиц в БД:
- Создать новую БД;
 - Подключить её к PGI (настраивается в файле `aces.properties`);
 - Запустить PGI. Если подключение к БД настроено верно, то таблицы в БД будут созданы автоматически, включая все необходимые сущности.
- 6.2. Ручное создание таблиц в БД:
- Закомментировать или удалить строку в файле `startup.conf` в настройках `back` части PGI;
 - Выполнить первый запуск `Pauguide™ Issuer`. При этом сервер сгенерирует файл `unrun.sql` с sql скриптами для создания таблиц и индексов базы данных;
 - Выполнить скрипт `unrun.sql` в БД;
 - Выполнить второй запуск `Pauguide™ Issuer`.
7. Выполнить скрипт `unrun.sql` в БД.
8. Выполнить второй запуск `Pauguide™ Issuer`.

3.3.3 Обновление системы PGI

1. Скачать архив с `Pauguide™ Issuer`;
2. Остановить приложения `back` и `front`;
3. Сохранить backup с номером сборки (номер сборки на сервере):
 - 3.1 [back] Переименовать папку `$HomeDir/aces` в папку `$HomeDir/#{version}_aces`;
 - 3.2 [front] Переименовать папку `$HomeDir/aces-front` в папку `$HomeDir/#{version}_aces-front`;
4. [back] Распаковать архив с `aces-back-*.zip` в домашний каталог `$Home_Dir`, с правами доступа 755;
5. [back] Назначить файлам `aces`, расположенному в `$HomeDir/.../bin`, права доступа 755;
6. [back] Указать в параметре `JAVA` путь установки актуальной версии пакета `Java JDK` в файле настроек `startup.conf` в `$HomeDir/.../conf`;
7. [back] Заполнить параметры файла `aces.properties` в `$HomeDir/.../conf`;
8. [front] Распаковать архив с `aces-front-*.zip` в домашний каталог `$Home_Dir` с правами доступа 755;
9. [front] Назначить файлам `aces-front`, расположенным в `$HomeDir/.../bin`, права доступа 755;
10. [front] Указать порт подключения к `front-end` серверу в файле `aces-front.properties` в `$HomeDir/.../conf`;
11. Запустить приложения на `back` и `front`;
12. Проверить логи на наличие ошибок;
13. Проверить появление `unrun.sql`. В случае появления `unrun.sql` выполнить скрипт в базе данных;
14. Запустить `back`;
15. Проверить логи на наличие ошибок;
16. Проверить запуск консоли;
17. Провести тесты.

3.3.4 Восстановление системы PGI после аварии

1. Остановить приложения `back` и `front`;
2. Запустить приложения на `back` и `front`;
3. Проверить логи на наличие ошибок;
4. Проверить появление `unrun.sql`. В случае появления `unrun.sql` выполнить скрипт в базе данных;
5. Запустить `back`;
6. Проверить логи на наличие ошибок;



7. Проверить запуск консоли;
8. Провести тесты.

4 Эксплуатация ПО

4.1 Функциональные возможности

Для подключения к консоли пользователю консоли с ролью Администратор необходимо ввести в адресную строку адрес, по которому доступна консоль. Данную информацию можно получить у специалиста внедрения. Адрес для подключения к консоли содержится в значении параметра console.addresses в файле конфигурации. Далее необходимо ввести свой логин/пароль.

4.1.1 Доступ и привилегии пользователя

Доступ пользователей к функциональности системы осуществляется в соответствии с ролями.

V – View – доступен только просмотр;

M – Manage – доступно редактирование;

R – просмотр запрещен, но сущность отображается в других подразделах для просмотра ее названия.

4.2 Функции пользователя консоли

Раздел/подраздел консоли	Функции Пользователя
Configuration -> Protocols	Информация о поддерживаемых 3-D Secure протоколах
Configuration -> Hosts	Список хостов
Configuration -> Issuers	Список банков-эмитентов
Configuration -> Payment Systems	Список платежных систем
Configuration -> Brands	Информация о платежных системах банков-эмитентов
Configuration -> Card Ranges	Диапазоны банковских карт
Configuration -> Challenge Methods	Информация о методах аутентификации банков-эмитентов
Configuration ->Frictionless Flow rules	Просмотр правил принятия решения по транзакции
System preferences	Управление политикой настройки пароля и отчетов
Users	Управление пользователями консоли

4.3 Раздел Configuration

В разделе Configuration можно управлять информацией о протоколах (подраздел Protocols), хостах (подраздел Hosts), банках-эмитентах (подраздел Issuers), платежных системах (подраздел Payment Systems), брендах (подраздел Brands), банковских картах (подраздел Card Ranges), методах аутентификации (подраздел Challenge Methods), просматривать правила принятия решения по транзакции (подраздел Frictionless Flow rules).

4.3.1 Менеджмент протоколов

Подраздел Protocols содержит список, используемых системой протоколов:

- ACS - 3D-Secure Protocols;
- Other – другие протоколы;
- PSIT - протоколы ПСИТ.

При нажатии на появляется список протоколов. Зеленый флаг обозначает, что протокол сконфигурирован, серый – не сконфигурирован.

4.3.2 Управление хостами

Подраздел Hosts содержит список хостов, оформленный в виде таблицы с полями:

- ID – идентификатор хоста;
- Title – публичный IP адрес в системе.

4.3.3 Управление эмитентами

Подраздел Issuers содержит список банков-эмитентов В подразделе Issuers отображается таблица, содержащая следующие поля:

- Identifier – уникальный идентификатор банка-эмитента;

- Title – наименование банка-эмитента.

4.3.4 Управление платежными системами

Подраздел Payment systems содержит список платежных систем, отображенных в виде таблицы, в которой указаны:

- ID – уникальный идентификатор платежной системы;
- Payment System – название платежной системы.

Для сохранения изменений нажмите Save, для отмены изменений - Reset.

4.3.5 Менеджмент брендов

Подраздел Brands объединяет информацию о банках-эмитентах и платежных системах. В подразделе Brands отображается таблица, содержащая следующие поля:

- ID – уникальный идентификатор для связи банка-эмитента и платежной системы, которую банк поддерживает;
- Name – наименование бренда;
- Issuer – наименование банка-эмитента;
- Payment System – наименование платежной системы.

В подразделе доступны фильтры поиска: по идентификатору бренда (ID), по наименованию бренда (Name), по наименованию банка-эмитента (Issuer). При нажатии на кнопку Find список брендов будет отфильтрован в зависимости от указанных значений в фильтрах. При нажатии на кнопку Clear фильтры будут очищены.

4.3.6 Управление параметрами платежных карт

Подраздел Card Ranges содержит информацию о диапазонах банковских карт. В подразделе Card Ranges отображается таблица, содержащая следующие поля:

- ID – уникальный идентификатор БИНа карты;
- Issuer – банк-эмитент карты;
- Brand – бренд карты;
- BIN – БИН карты;
- First PAN – начальное значение диапазона номеров карт;
- Last PAN – конечное значение диапазона номеров карт;
- On Demand Enrollement – признак проведения попытки подключения карты в момент первой покупки (Activation During Shopping) для карт, не участвующих в программе 3D-Secure;
- External Authentication – признак доступности методов внешней аутентификации для данного диапазона карт.

На странице доступны фильтры поиска по ID, Issuer, BIN и Brand. При нажатии на кнопку Find список диапазонов карт будет отфильтрован в зависимости от указанных значений в фильтрах. При нажатии на кнопку Clear фильтры будут очищены.

4.3.7 Настройка параметров аутентификации

На вкладке Challenge methods отображается информация о методах аутентификации для банка-эмитента. Информация включает уникальный идентификатор метода (ID), его наименование (Name), наименование банка-эмитента (Issuer), тип метода (Type), статус метода аутентификации Enabled или Blocked (Status) и признак метода аутентификации по умолчанию для эмитента (Default Issuer). Метод аутентификации привязывается к банковской карте с помощью устройства.

4.3.8 Просмотр правил Frictionless Flow

Подраздел Frictionless Flow rules предназначен для просмотра правил принятия решения по транзакции. Список правил принятия решения по транзакции оформлен в виде таблицы, содержащей:

- Identifier – идентификатор правила;
- Issuer – банк-эмитент, для которого используется правило;
- Brand – бренд, для которого используется правило;
- PAN – PAN карты, для которого используется правило;
- First PAN - начальное значение диапазона номеров карт, для которого используется правило;
- Last PAN - конечное значение диапазона номеров карт, для которого используется правило;
- Priority – приоритет правила;
- Status – статус транзакции аутентификации;

- Criterion – правило принятия решения по транзакции.

Из подраздела Fictionless Flow rules доступна информация о банке-эмитенте из подраздела Issuers при нажатии на активную ссылку в столбце Issuer и информация о бренде из подраздела Brands при нажатии на активную ссылку в столбце Brand.

4.4 Раздел System preferences

Подраздел System preferences subsection содержит:

- Expired cards removal worker;
- Password policy settings – конфигурация политики настройки паролей;
- Reports settings – конфигурация настройки отчетов.



4.5 Раздел Users


Управление учетными записями пользователей консоли осуществляется в подразделе раздела Users. В подразделе отображается таблица, содержащая следующие поля:

- Логин – уникальный идентификатор пользователя;
- Имя – имя пользователя;
- Роли – роль пользователя в консоли;
- Статус – статус пользователя в консоли;
- Вход в консоль – статус входа в консоль.

4.6 Управление отображением информации на страницах


На страницах, где информация представлена в виде таблиц, пользователь может изменять количество отображаемых параметров в таблице. При наведении курсора на заголовок столбца появляется стрелка раскрытия, при нажатии на которую появляется выпадающее меню. При наведении курсора на Columns появляется список с названиями столбцов. Отображаемые столбцы отмечены флагами. При снятии флага соответствующий столбец перестает отображаться в окне раздела. Для использования фильтров необходимо задать требуемые параметры и нажать на кнопку Find. Для отключения фильтров необходимо нажать на кнопку Clear.

Чтобы изменить число отображаемых строк на одной странице необходимо для параметра Page size в выпадающем меню задать требуемое значение. Переключение между страницами осуществляется при помощи кнопок  .


Для обновления информации на странице необходимо нажать на кнопку .

4.7 Смена пароля пользователем

Для смены пароля используется команда необходимо нажать в верхнем правом углу консоли кнопку с именем пользователя. Появится окно, в котором необходимо заполнить поля Текущий пароль и Новый пароль. Для подтверждения изменения пароля, необходимо нажать кнопку «ОК».

Для выхода из системы используется кнопка  в правом верхнем углу консоли. При этом принудительно завершается текущая сессия. Также текущая сессия завершается автоматически, если в течение N минут в консоли не производилось никаких действий (таймаут устанавливается в настройках Веб-сервера). В целях обеспечения безопасности рекомендуется всегда явно завершать работу.

4.8 Завершение работы с консолью

Для выхода из системы используется кнопка  в правом верхнем углу консоли. При этом принудительно завершается текущая сессия. Также текущая сессия завершается автоматически, если в течение N минут в консоли не производилось никаких действий (таймаут устанавливается в настройках Веб-сервера). В целях обеспечения безопасности рекомендуется всегда явно завершать работу.