

ПРОГРАММНЫЙ КОМПЛЕКС
«МЕНЕДЖЕР УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕКРЕТАМИ
НАSPBOX»

Руководство пользователя

Листов 13

Оглавление

Термины и определения	3
Перечень сокращений.....	3
Общие сведения.....	4
Интерфейс сервиса	4
Веб-интерфейс	4
Подключение к веб-интерфейсу	5
Описание веб-интерфейса	5
Управление доступом	6
Профили подключений.....	7
Пользователи.....	8
Группы	9
Роли.....	9
Парольные политики	9
Внешние системы.....	11
Журнал событий.....	12
Алгоритм действий пользователя при первом запуске системы.....	12

Термины и определения

Термин	Определение
Модуль ротации и управления секретами	Компонент, отвечающий за хранение секретов
Программное обеспечение (ПО)	Совокупность компьютерных программ и программных документов, необходимых для эксплуатации этих программ.
Объект управления доступом	База данных, система виртуализации или служба, для которой производится ротация паролей учетных записей
Пользователь	Сотрудник Заказчика, обладающий правом доступа к Системе

Перечень сокращений

Сокращение	Расшифровка
API	Application Programming Interface
БД	База данных
ПО	Программное обеспечение
СУБД	Система управления базами данных

Общие сведения

ПО HASPBOX (далее HASPBOX) — это инструмент для хранения и управления паролями и секретами на основе парольных политик. Рабочий процесс HASPBOX обеспечивает контроль безопасности и интеграцию на нескольких уровнях, отслеживая и управляя доступом пользователей посредством:

- жестких ограничений на основе уникальных идентификаторов пользователя;
- доступа к учетным данным для сеансов через модуль ротации и управления секретами;
- управления инфраструктурой внутри кода для автоматизации настройки разрешений пользователей;

HASPBOX позволяет пользователям, аутентифицированным локально в системе, получать авторизованный доступ к целевым системам на основе заданных политик доступа, которые определены в HASPBOX. Доступ к целевым системам осуществляется с помощью уникальных идентификаторов.

Основные особенности и преимущества HASPBOX:

- доступ на основе уникальных идентификаторов;
- мониторинг событий;
- использование сертифицированных средств криптографической защиты (КриптоПРО CSP не ниже версии 5.0);
- возможность работы на отечественной ОС Astra linux SE не ниже версии 1.7
-

Интерфейс сервиса

Работа с сервисом осуществляется с помощью пользовательского веб-интерфейса.

Веб-интерфейс

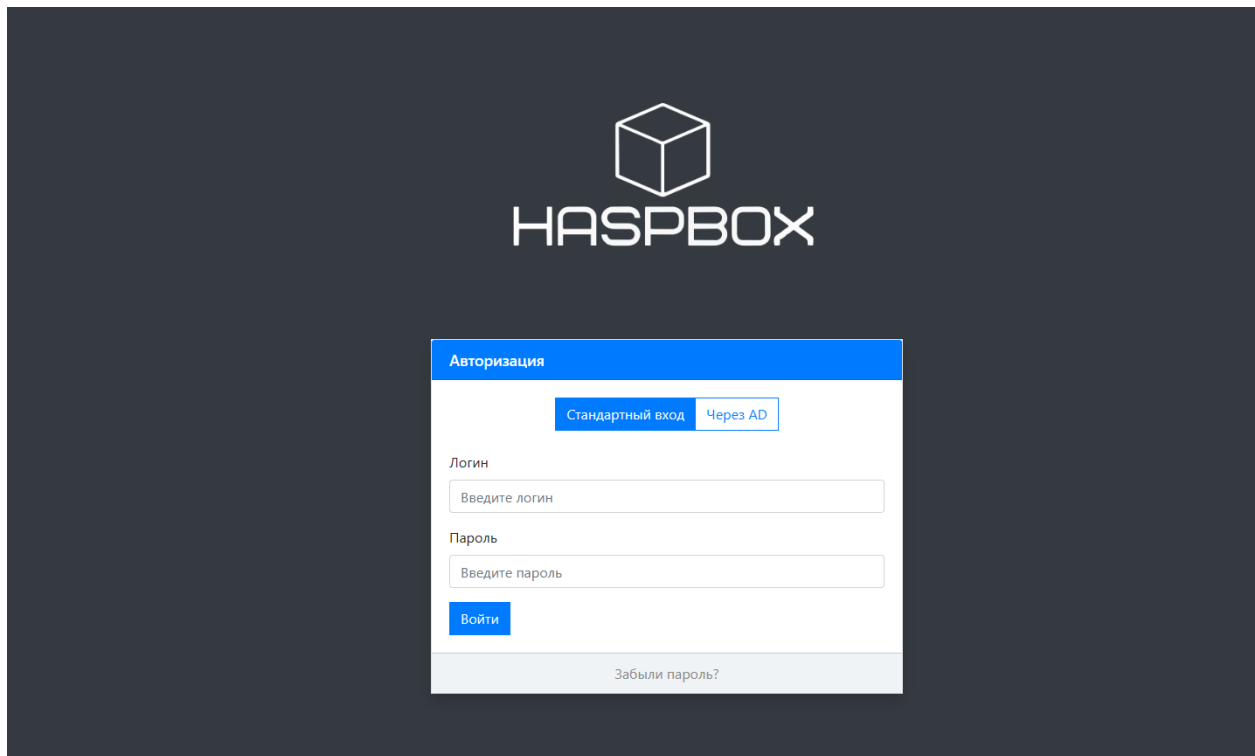
Веб-интерфейс используется для создания и настройки целевых систем, сеансов подключения к ним, конфигурации парольных политик и других настроек системы, необходимых для работы пользователя и решения основных задач решения.

Подключение к веб-интерфейсу

Подключение к веб-интерфейсу осуществляется с помощью браузера.

В адресной строке вводится адрес сервера (или виртуального сервера), на котором развернут сервер HASPBOX.

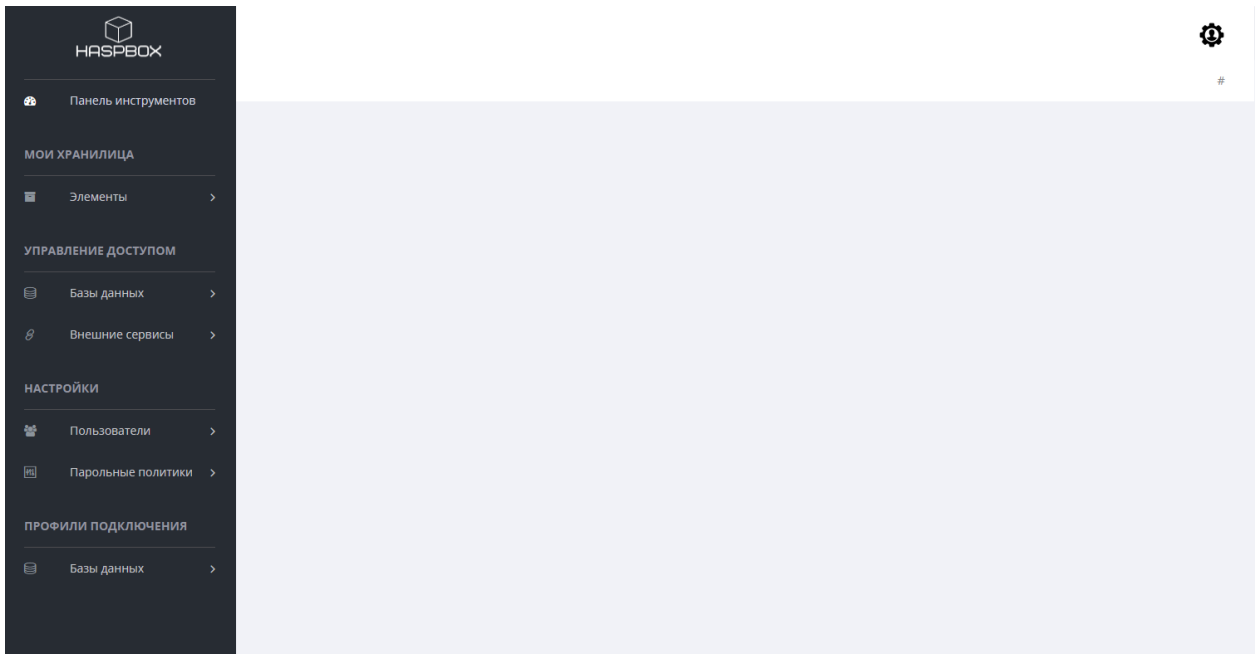
Откроется окно авторизации, в котором надо ввести логин и пароль, которые были сгенерированы на этапе инициализации HASPBOX (по умолчанию, при первом запуске – admin@example.com:P@ssw0rd).



Описание веб-интерфейса

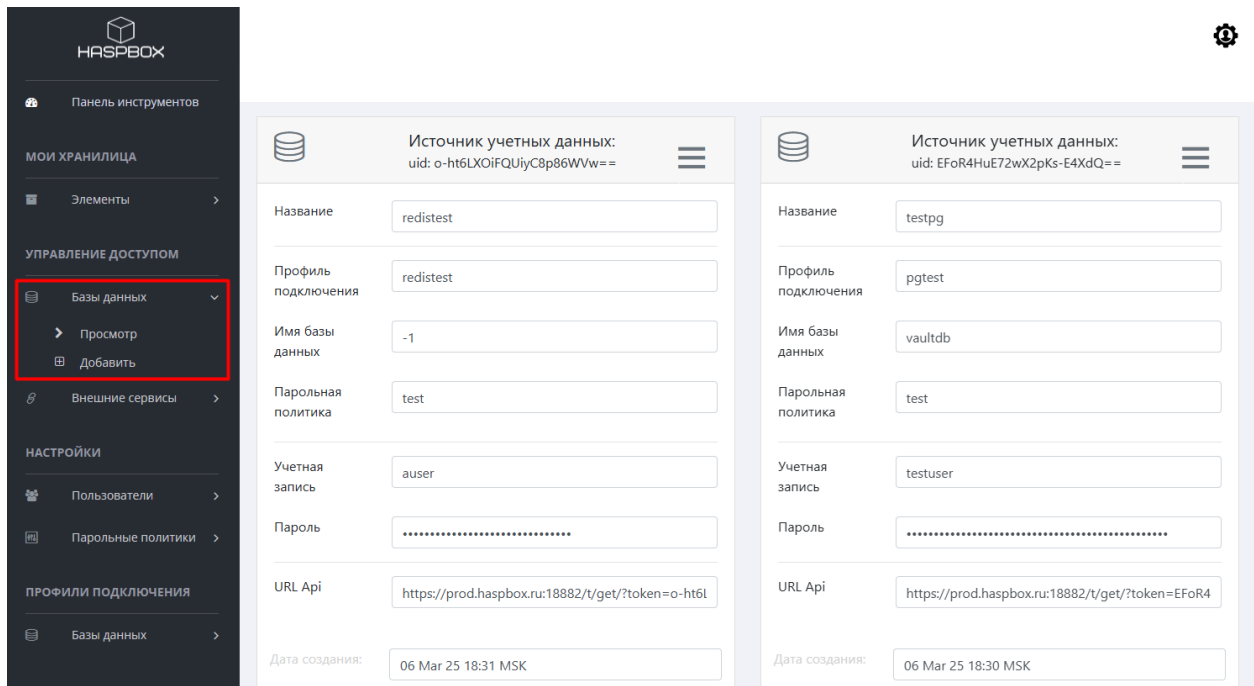
Окно веб-интерфейса сервиса содержит следующие области:

- «Мои хранилища»;
- «Управление доступом»;
- «Настройки»;
- «Профили подключения».



Управление доступом

«Управление доступом» — это тип области, используемый для организации доступа и управления учетными данными. Объединяет «Базы данных», «Службы», «Системы виртуализации».



Чтобы создать новый объект управления доступом (далее объект), нажмите кнопку «Добавить», заполните соответствующие поля:

- «Профиль подключения» - выбирается из заранее созданных;
- «Парольная политика» - выбирается из заранее созданных
- «Период ротации» - периодичность обновления пароля для указанной учетной записи.

После сохранения источник получит уникальный идентификатор, который сохранится в базе данных HASPBOX.

Профили подключений

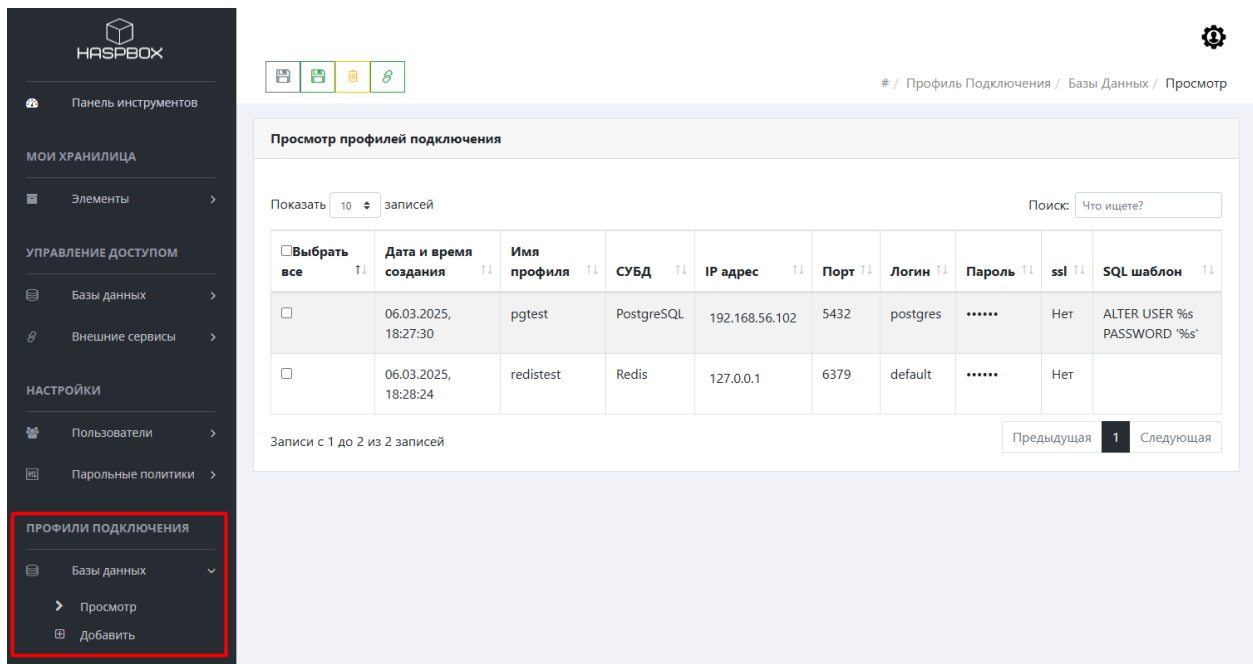
«Профили подключения» содержит следующие области:

- «Базы данных»
 - «Просмотр»
 - «Добавить»
- «Службы»
 - «Просмотр»
 - «Добавить»
- «Системы виртуализации»
 - «Просмотр»
 - «Добавить»

В соответствующих вкладках задаются параметры служебных учетных данных, для подключения к целевым системам для дальнейшего управления и ротации.

Чтобы создать новый профиль, необходимо нажать кнопку «Добавить» и в открывшемся окне заполнить соответствующие поля. На примере добавления нового профиля для СУБД:

- Название профиля;
- Тип СУБД;
- IP адрес;
- Порт;
- Логин;
- Пароль;
- Защищенное ssl соединение (для некоторых типов СУБД)
- Шаблон SQL запроса (Индивидуален, для каждого типа СУБД).



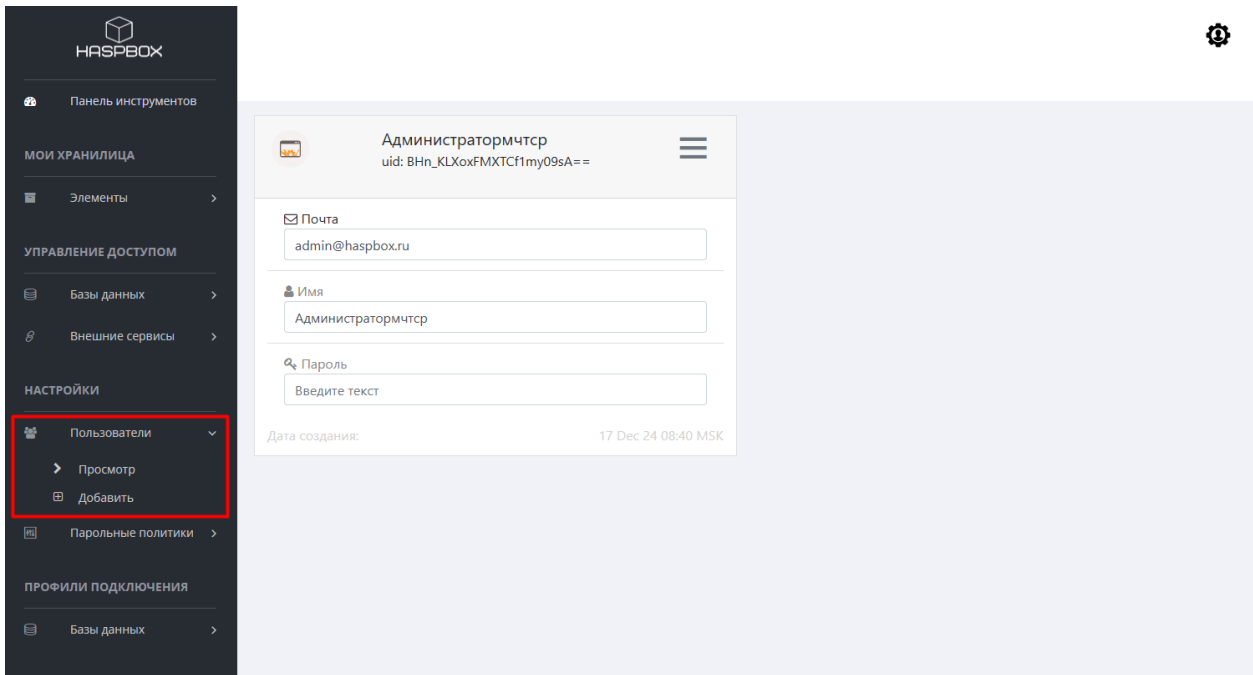
Перед сохранением, можно проверить корректность введенных данных, для этого нужно нажать кнопку «Проверить соединение». После завершения настроек нажать «Сохранить».

«Настройки» содержит следующие области:

- «Пользователи»
 - Группы
 - «Просмотр»
 - «Добавить»
 - «Роли»
 - «Просмотр»
 - «Добавить»
 - «Просмотр»
 - «Добавить»
- «Парольные политики»
 - «Просмотр»
 - «Добавить»
- «Внешние системы»
 - «Просмотр»
 - «Добавить»

Пользователи

Пользователи являются субъектами доступа. Пользователей можно создавать в соответствующей форме.



Чтобы создать нового пользователя, необходимо нажать кнопку «Добавить», ввести имя пользователя, логин и пароль, а также выбрать роль.

Группы

Для удобства управления пользователей можно объединять в группы. Таким образом, роли можно назначать не конкретному пользователю, а сразу группе пользователей.

Роли

Роли характеризуют наборы определенных правил и разрешений для пользователей или групп пользователей.

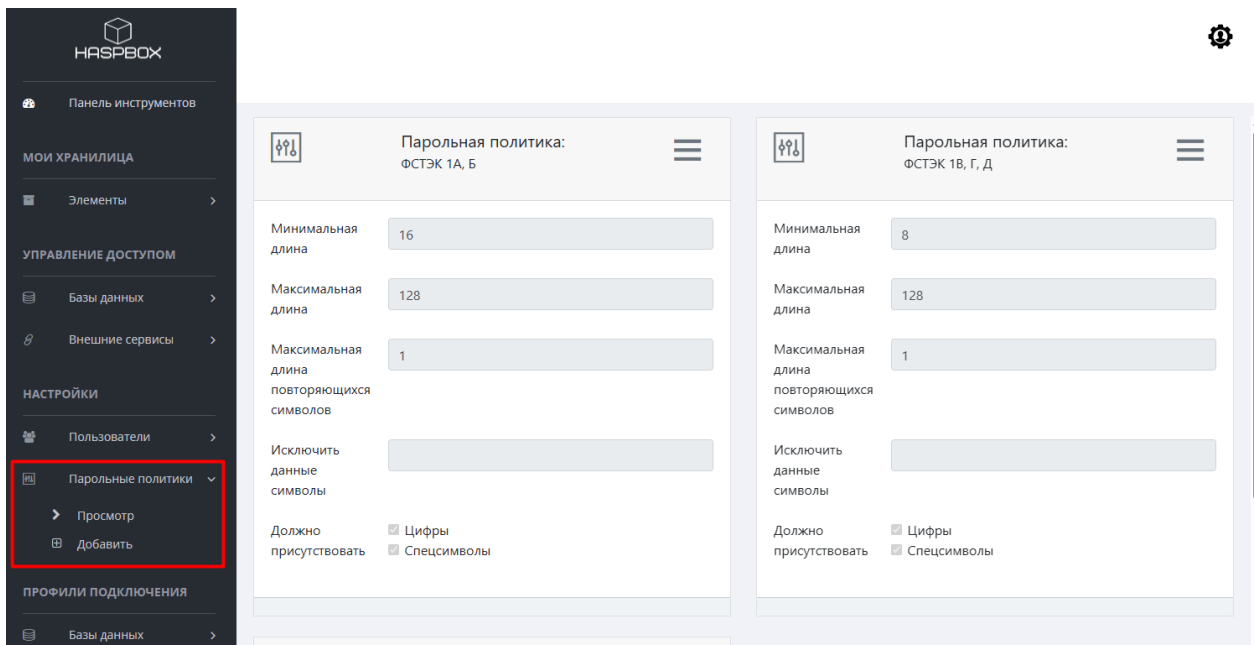
Можно создать определенную роль, в настройках которой указываются название, описание, область использования в конкретном объекте, а также назначить конкретных для роли пользователей и привилегии (гранты).

Парольные политики

Набор правил генерации новых паролей, для добавления новой политики нажмите кнопку «Добавить» и заполните соответствующие поля:

- Название политики;
- Минимальная длина пароля (максимум 32 символа);

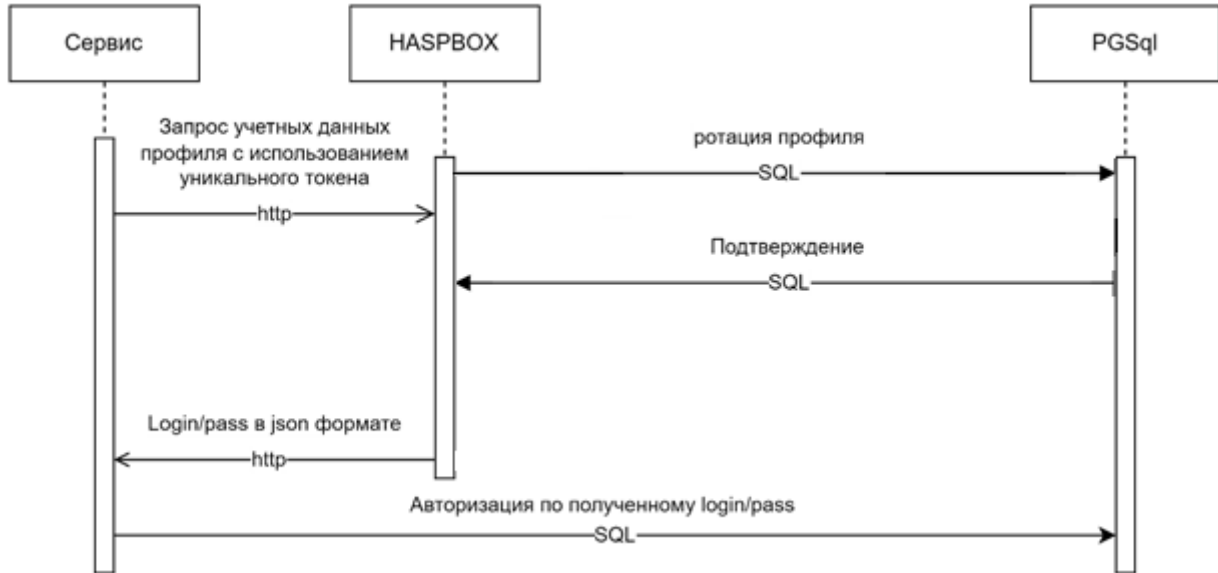
- Максимальная длина пароля (максимум 128 символов);
- Максимальная длина повторяющихся символов (0 – без ограничения);
- Исключить следующие символы (Символы выводятся по одному, без пробелов и с учетом регистра, например: Qwerty123456 – все символы будут исключены, причем q – будет доступна, а Q – исключена);
- Галочками отметьте нужные позиции



После этого нажмите кнопку «Сохранить». Парольные политики – глобальны для всей системы и доступны при создании любого объекта.

Внешние системы

Настройка доступа внешних сервисов к целевым системам с использованием API HASPBOX и уникального токена. Общий принцип взаимодействия внешних сервисов, на примере доступа к учетным данным СУБД PostgreSQL представлен на рисунке:



Для добавления внешнего сервиса, необходимо нажать кнопку «Добавить» и заполнить соответствующие поля:

- Название;
- IP адрес, с которого сервис будет обращаться по HASPBOX API;
- Выбрать тип объекта, к которому будет предоставлен доступ;
- Указать в списке конкретные объекты, к которым будет предоставлен доступ.

Список зарегистрированных внешних сервисов

Show 10 entries Search:

Дата и время добавления ↑	Имя ↑	Ip адрес ↑	Подробности ↑
06.03.2025, 18:33:57	testsrv	192.168.100.100	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHRlcm5hbGwjaWoiMTkyLjE2OC4xMDAuMTAwIiwiaWF0IjoiYGFzZGJveC5jb3Jlln0.H-CmlrMlryX-dvxGih3MeFB-eEqRp2sOWCCAQuF3Uc

Showing 1 to 1 of 1 entries Previous 1 Next

После нажатия кнопки «Сохранить», сервис будет добавлен в систему HASPBOX, при этом, для него будет сгенерирован уникальный токен. Данный токен используется для авторизации сервиса в системе, при запросе учетных данных объекта.

Журнал событий

Данный раздел содержит информацию о событиях системы, включающую в себя информацию о работе планировщика управления внешними секретами в рамках контролируемых систем.

Журнал событий

Показать 10 записей

Поиск: Что ищете?

Дата и время	Код события	Источник	Подробности
10.03.2025, 00:24:36	Информация	sheduler	Задача[pg: 0] [addr: 192.168.56.102:5432]: Пароль успешно ротирован
10.03.2025, 00:24:12	Информация	sheduler	Задача[redis: 1] [addr: 127.0.0.1:6379]: Пароль успешно ротирован
10.03.2025, 00:23:36	Информация	sheduler	Задача[pg: 0] [addr: 192.168.56.102:5432]: Пароль успешно ротирован
10.03.2025, 00:23:12	Информация	sheduler	Задача[redis: 1] [addr: 127.0.0.1:6379]: Пароль успешно ротирован
10.03.2025, 00:22:36	Информация	sheduler	Задача[pg: 0] [addr: 192.168.56.102:5432]: Пароль успешно ротирован
10.03.2025, 00:22:11	Информация	sheduler	Задача[redis: 1] [addr: 127.0.0.1:6379]: Пароль успешно ротирован
10.03.2025, 00:21:35	Информация	sheduler	Задача[pg: 0] [addr: 192.168.56.102:5432]: Пароль успешно ротирован
10.03.2025, 00:21:11	Информация	sheduler	Задача[redis: 1] [addr: 127.0.0.1:6379]: Пароль успешно ротирован
10.03.2025, 00:20:35	Информация	sheduler	Задача[pg: 0] [addr: 192.168.56.102:5432]: Пароль успешно ротирован
10.03.2025, 00:20:11	Информация	sheduler	Задача[redis: 1] [addr: 127.0.0.1:6379]: Пароль успешно ротирован

Записи с 1 до 10 из 9 301 записей

Предыдущая 1 2 3 4 5 ... 931 Следующая

Алгоритм действий пользователя при первом запуске системы

Шаг первый – Сменить логин и пароль администратора на вкладке – «Настройки» - «Пользователи»;

Шаг второй – Настроить парольные политики, в соответствии с регламентами и требованиями Вашей организации;

Шаг третий – настроить профили подключения, для систем в которых будет производиться ротация паролей, в соответствии с выбранными типами систем и учетными данными, предоставленными ответственными лицами Вашей организации;

Шаг четвертый – настроить объекты, у которых будет производиться ротация паролей

Шаг пятый – добавить и настроить «Роли», «Группы» и пользователей, который будут получать доступ к указанным объектам;

Шаг шестой – при необходимости, добавить и настроить внешние сервисы.