

Содержание

| | |
|---|---|
| SSH ключ для подключения к оборудованию | 3 |
| <i>Конфигурация sshd</i> | 3 |
| <i>Шаг 1. Создание ключа</i> | 3 |
| <i>Шаг 2. Добавление ssh ключа к оборудованию</i> | 6 |
| <i>Шаг 3. Добавление ssh ключа на сервер</i> | 7 |

SSH ключ для подключения к оборудованию

Подключение к оборудованию через графический интерфейс осуществляется по SSH. Авторизация может происходить по паролю или с использованием ключа — этот метод является более безопасным.

В данном разделе рассмотрим процесс авторизации по ключу.



Подключение необходимо осуществлять под пользователем с `sudo` привилегиями, либо под пользователем `root` (не рекомендуется).

Добавить `sudo` пользователя на подключаемом оборудовании: [Пользователь sudo](#).

Конфигурация sshd

Конфигурационный файл находится по пути `/etc/ssh/sshd_config` Рекомендуем проверить конфигурационное свойство `PubkeyAuthentication` — если оно отсутствует, закомментированно, или равно значению `no`, следует изменить значение свойства на `yes`.

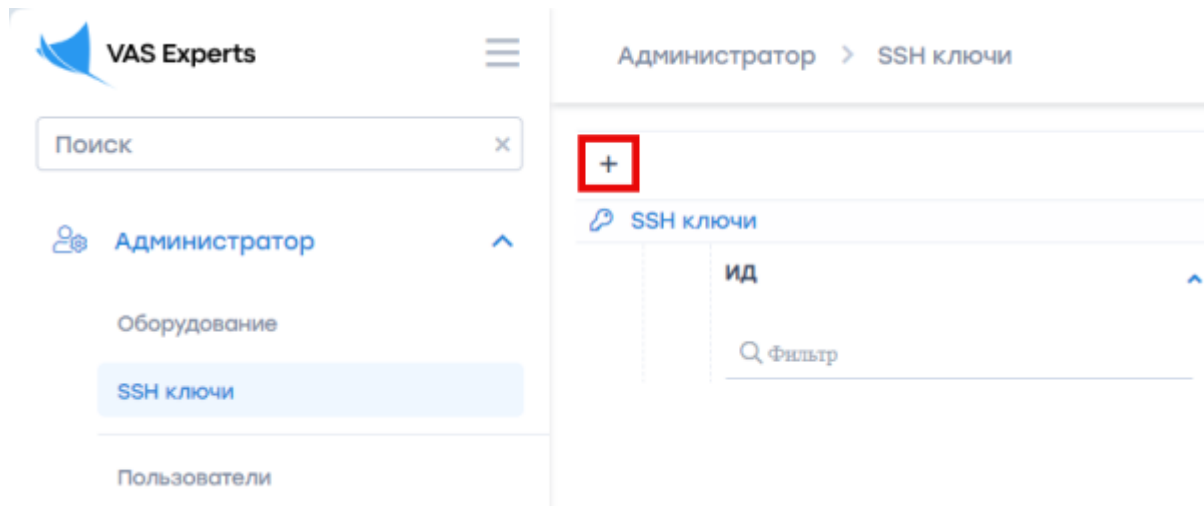


После любых изменений в файле `/etc/ssh/sshd_config` необходимо перезапустить сервис `sshd` командой

```
sudo systemctl restart sshd
```

Шаг 1. Создание ключа

1. Перейти в раздел Администратор → SSH ключи
2. Нажать на + в верхней части экрана для добавления нового ключа

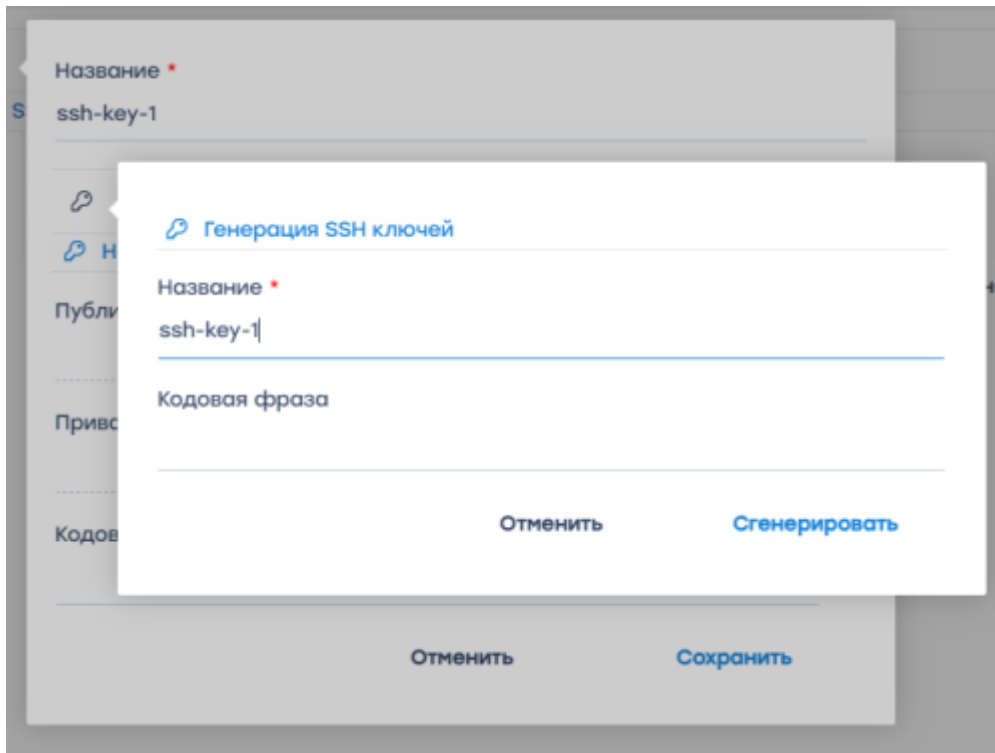


3. Ввести название ключа

4. Добавить файлы: публичный и приватный ключ

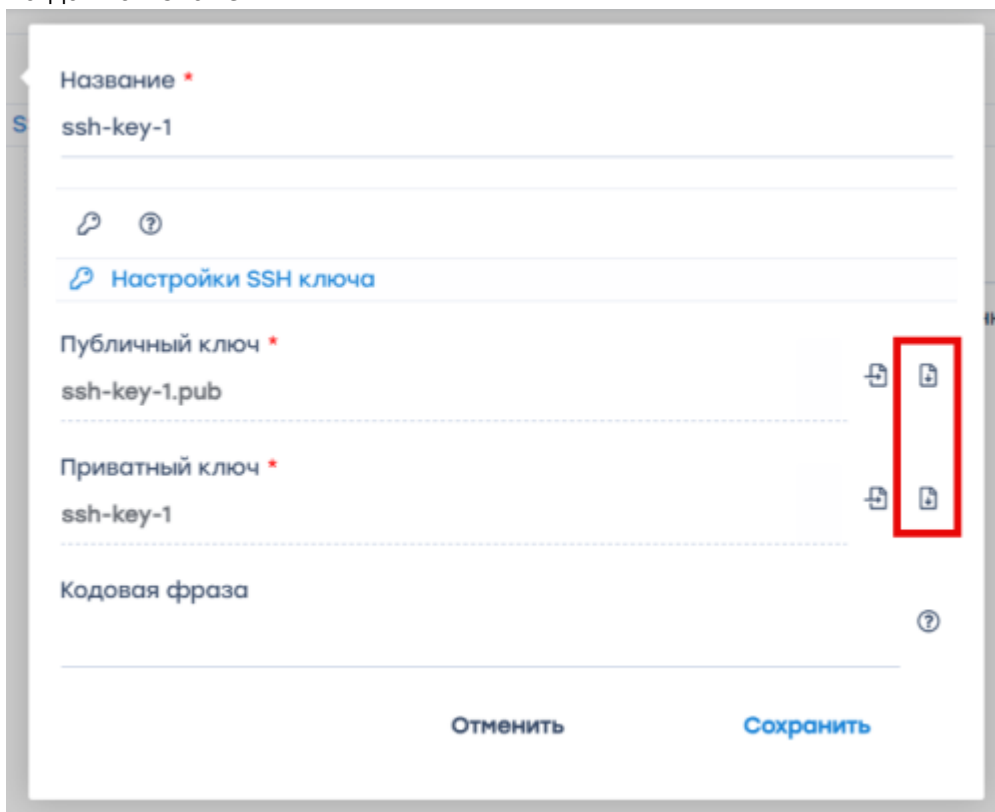
1. Если уже есть уже готовые ключи — можно загрузить их, нажав соответствующие кнопки

2. Если нужные ssh файлы отсутствуют, их можно сгенерировать, нажав на иконку ключа. При желании можно добавить кодовую фразу. После чего нажать на кнопку Сгенерировать



После генерации ssh файлов необходимо скачать публичный ключ для добавления его на сервер.

Также при необходимости можно скачать и приватный ключ — это возможно только на данном этапе.



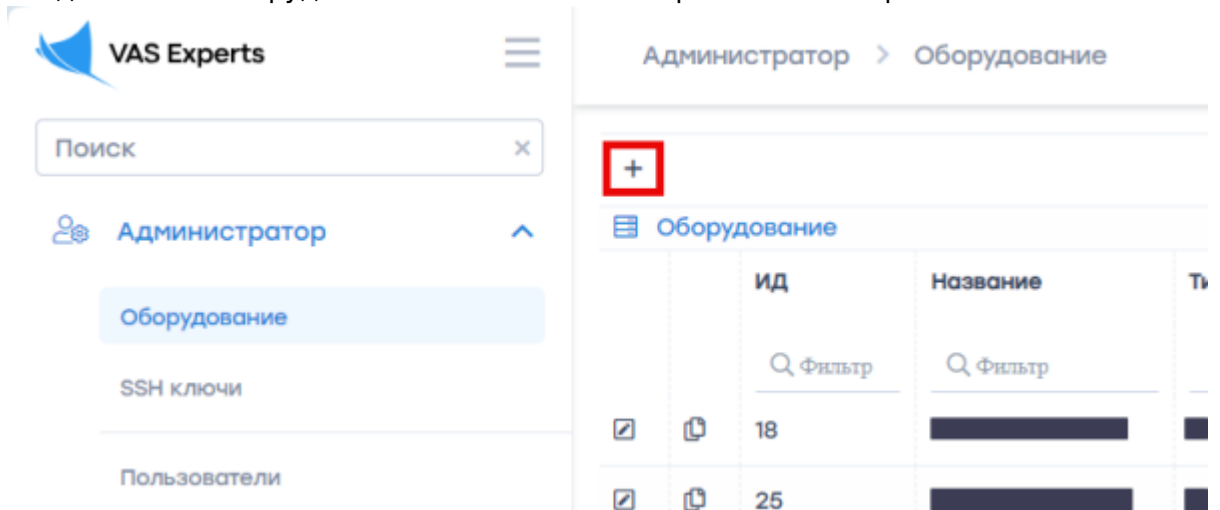
5. Если приватный ключ зашифрован, необходимо предоставить кодовую фразу, указанную при создании ключа

Если кодовая фраза не была установлена — оставить поле пустым

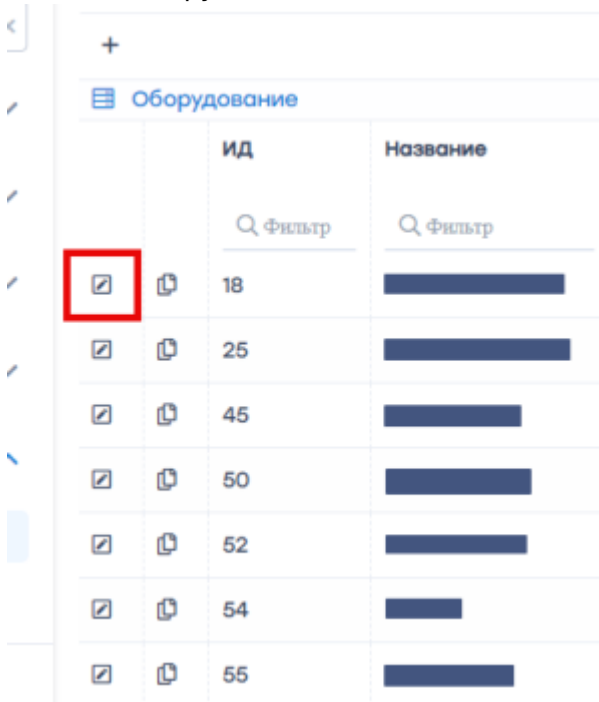
6. Нажать кнопку Сохранить

Шаг 2. Добавление ssh ключа к оборудованию

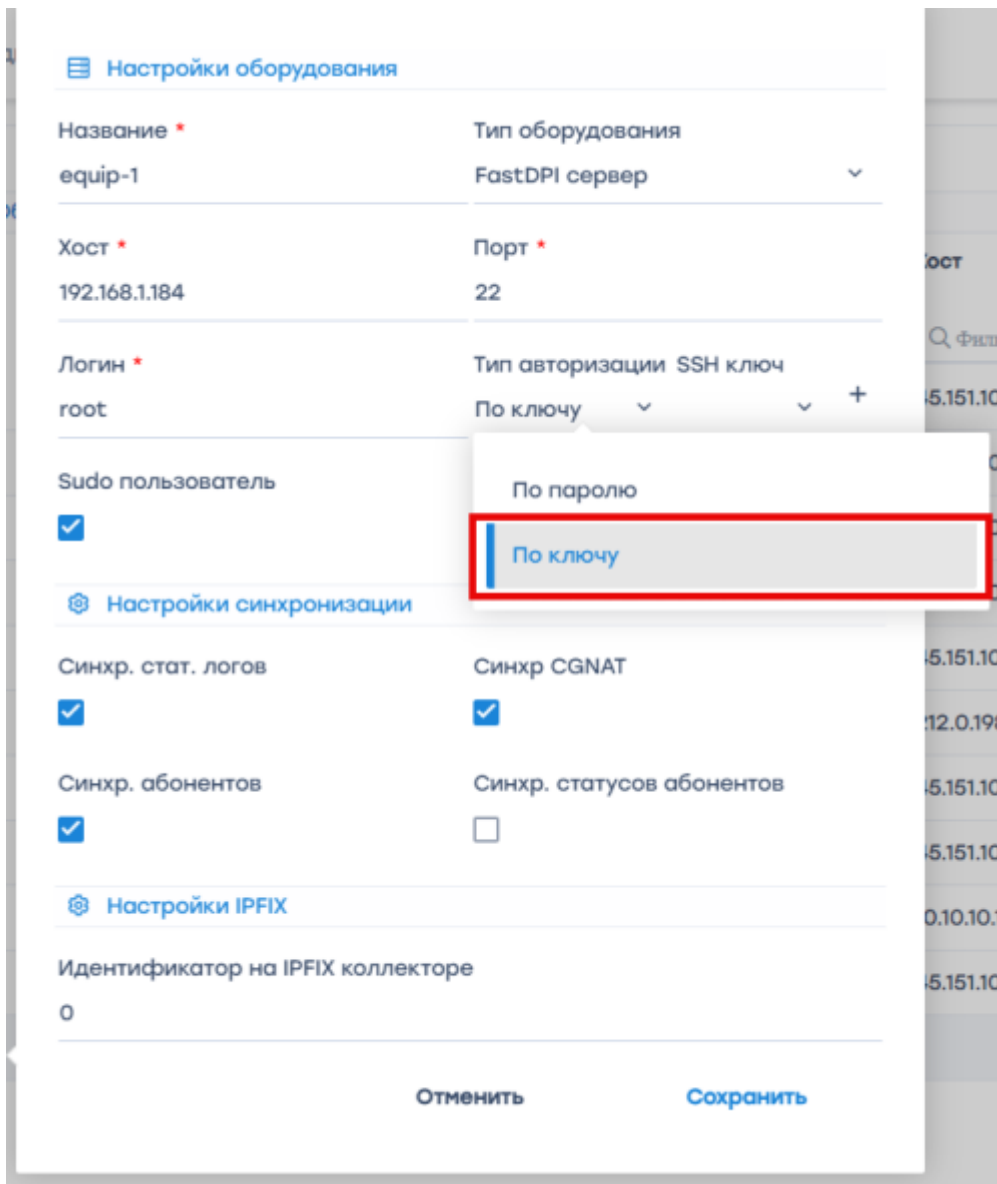
1. Перейти в раздел Администратор → Оборудование
2. Перейти в настройки оборудования. Добавить ssh ключ можно как новому, так и уже имеющемуся оборудованию.
 1. Создать новое оборудование: нажать на + в верхней части экрана



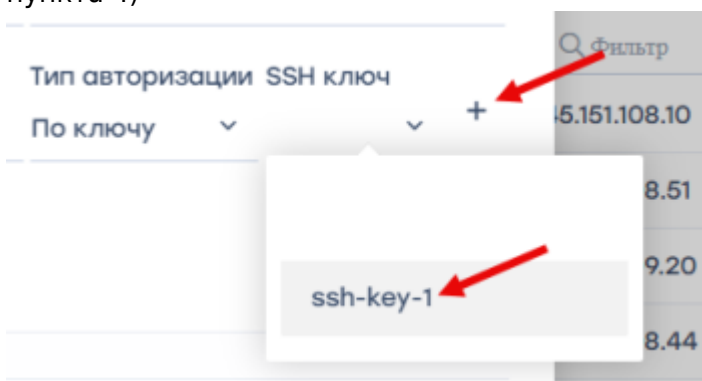
2. Редактировать существующее оборудование: нажать на иконку редактирования слева от оборудования



3. При создании нового оборудования заполнить все поля нужной информацией. Подробнее в разделе [Управление оборудованием](#).
4. Выбрать тип авторизации По ключу



5. В поле SSH ключ выбрать созданный ранее ключ. Либо по нажатию на + создать новый SSH ключ, процесс идентичен с описанным в разделе [Шаг 1. Создание ключа](#) (начиная с пункта 4)



6. Нажать Сохранить

Шаг 3. Добавление ssh ключа на сервер

1. Под пользователем root перейти в папку /root/
Под обычным пользователем перейти в папку /home/<имя пользователя>/

2. Перейти в скрытый каталог `/.ssh/`
3. Открыть файл `authorized_keys`
4. Добавить в файл содержимое **публичного** ключа

После проделанной работы проверить подключение по кнопке Состояние оборудования в разделе Администратор → Оборудование.

Если все свойства в состоянии “Ok” — значит подключение прошло успешно.

