Содержание

SSH key for connecting to equipment

Connection to the equipment through the graphical interface is performed via SSH. Authorization can occur either by password or by using a key — the latter method is more secure.
In this section, we will cover the key-based authorization process.

Connection must be made under a user with sudo privileges or as root (not recommended).
Add a sudo user on the equipment: Sudo user.

sshd configuration

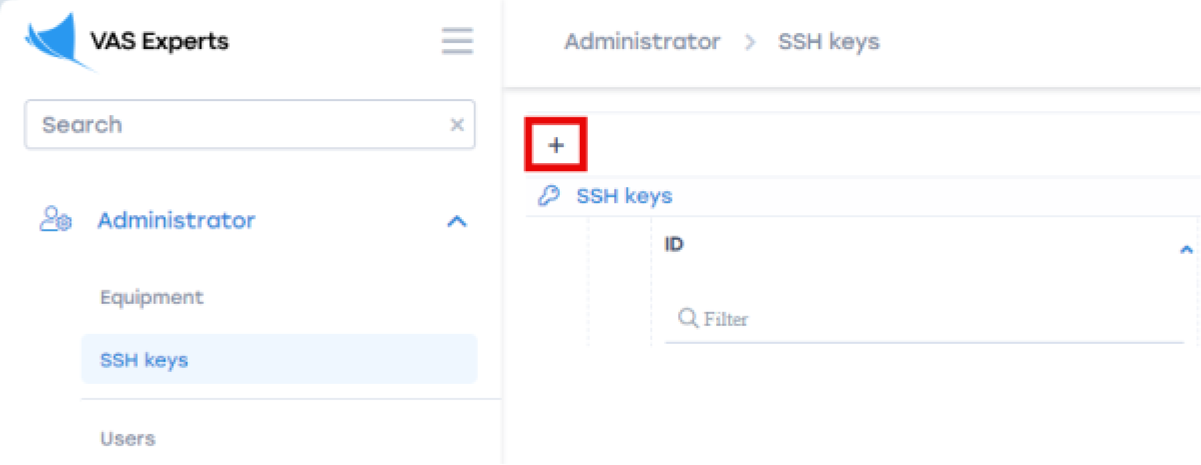
The configuration file is located at `/etc/ssh/sshd_config`. We recommend checking the `PubkeyAuthentication` property — if it is missing, commented out, or set to no, change the property value to `yes`.

After any changes to the `/etc/ssh/sshd_config` file, the sshd service must be restarted with the command

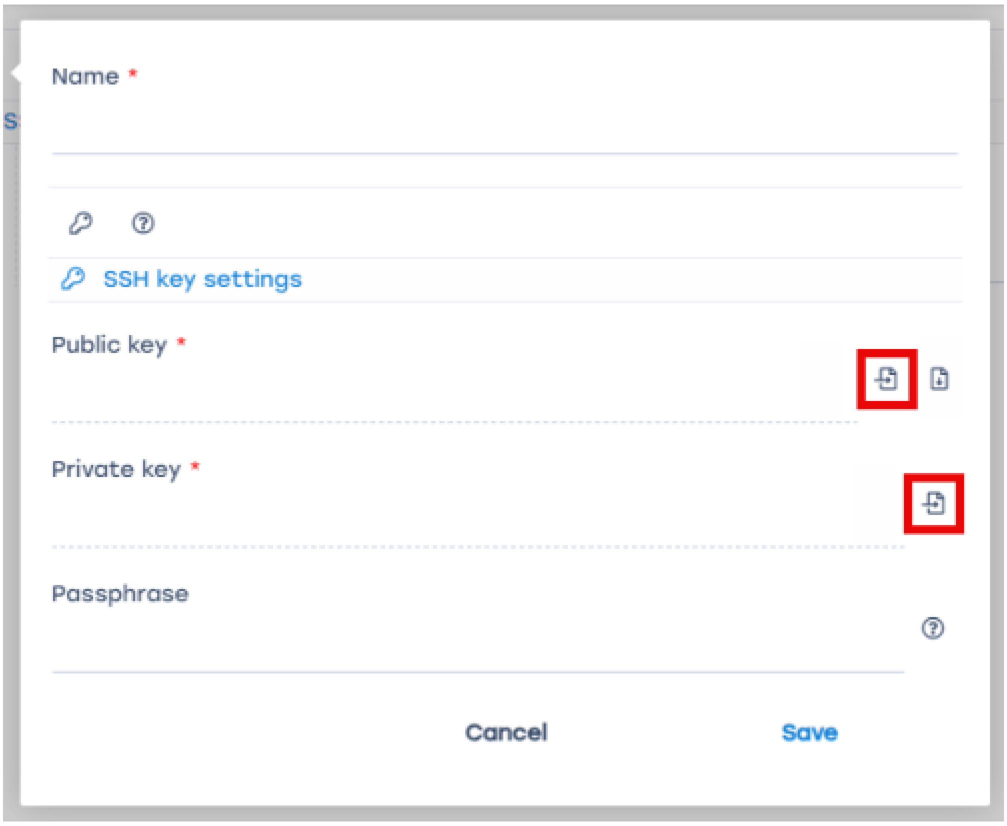
```
sudo systemctl restart sshd
```

Step 1. Creating a key

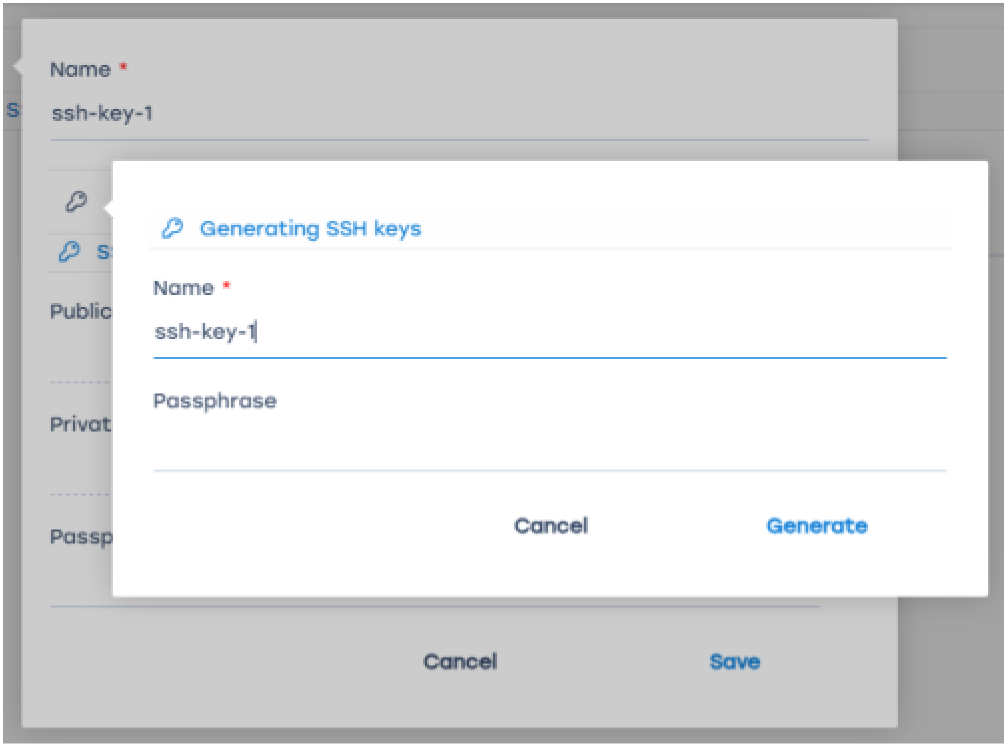
1. Navigate to the Administrator → SSH Keys section
2. Click on the + at the top of the screen to add a new key



3. Enter the key name
4. Upload the public and private key files
    1. If you already have ready-made keys, you can upload them by clicking the appropriate buttons



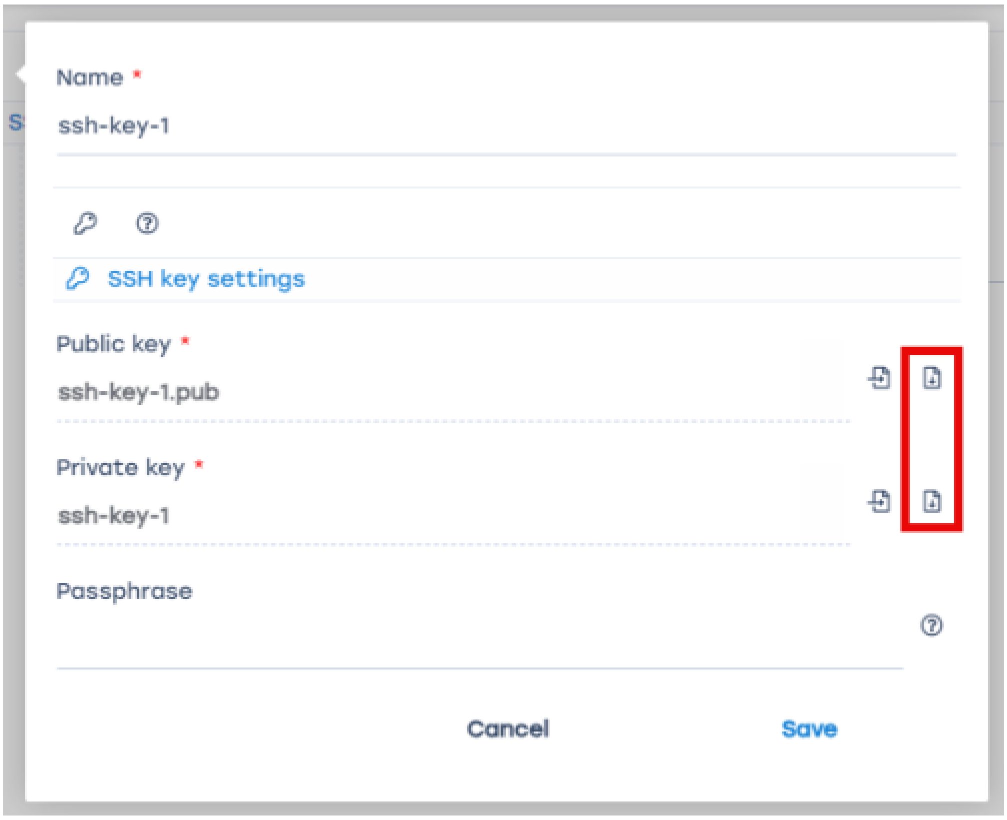
2. If the necessary ssh files are missing, they can be generated by clicking on the key icon. Optionally, you can add a passphrase. Then click Generate



Name *
ssh-key-1

Name *
ssh-key-1

After generating the ssh files, download the public key to add it to the server.
If necessary, you can also download the private key — this is only possible at this stage.



Name *

ssh-key-1

Public key *

ssh-key-1.pub

Private key *

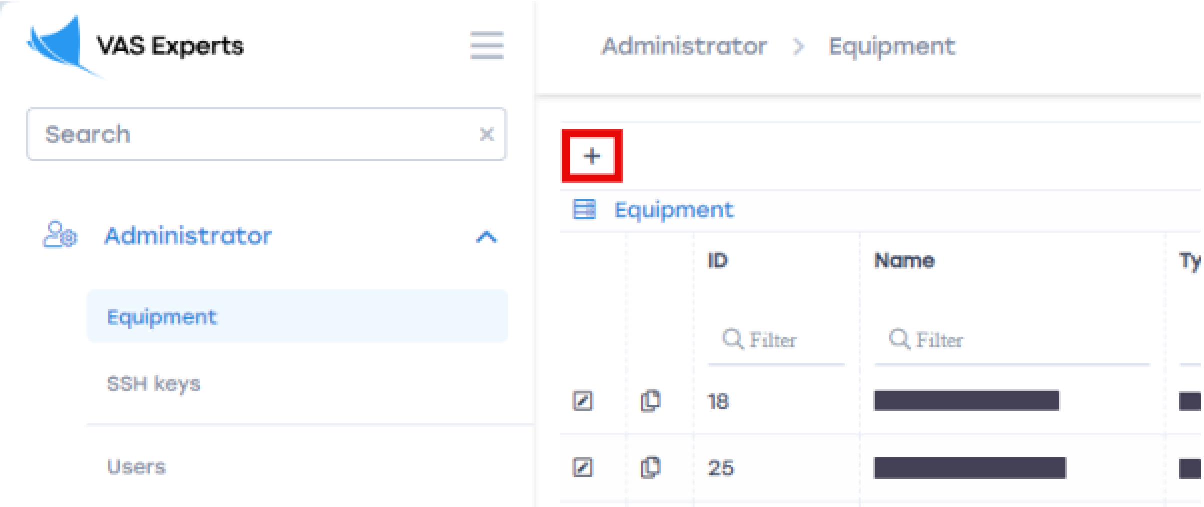
ssh-key-1

Passphrase

5. If the private key is encrypted, provide the passphrase set during key creation
   If no passphrase was set, leave the field blank
6. Click Save

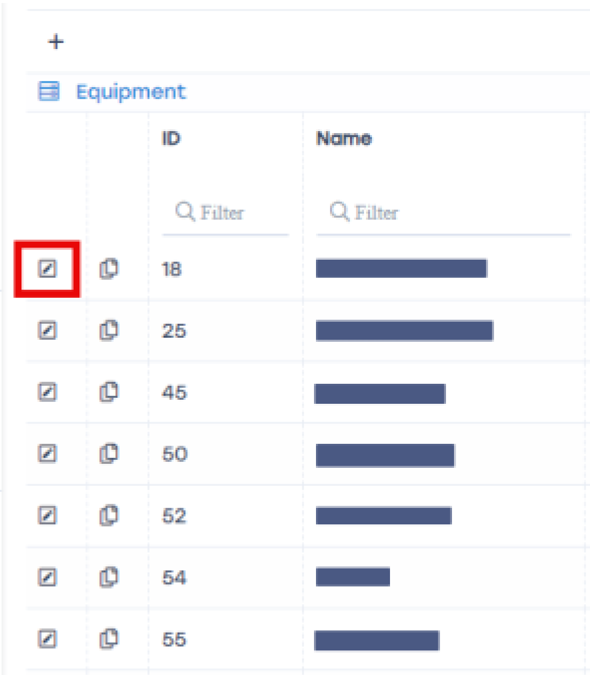
Step 2. Adding the ssh key to the equipment

1. Navigate to Administrator → Equipment
2. Open the equipment settings. The ssh key can be added to new or existing equipment.
   1. Create new equipment: click on the + at the top of the screen



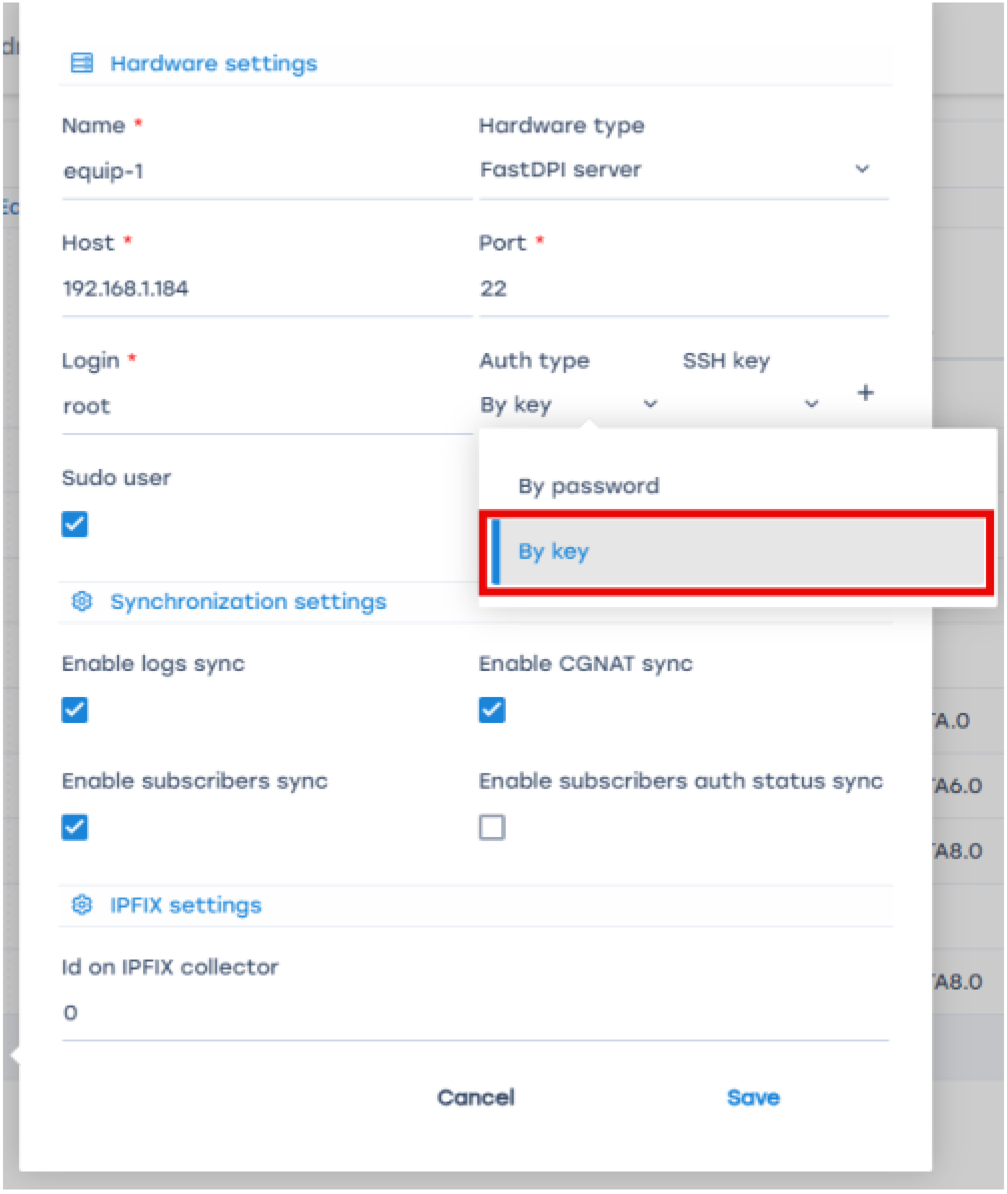
ID	Name	Ty
Filter	Filter	
18	[redacted]	[redacted]
25	[redacted]	[redacted]

   2. Edit existing equipment: click the edit icon to the left of the equipment



	ID	Name
	18	[redacted]
	25	[redacted]
	45	[redacted]
	50	[redacted]
	52	[redacted]
	54	[redacted]
	55	[redacted]

3. When creating new equipment, fill in all fields with the necessary information. More details in the Equipment management section.
4. Select the Key-based authorization type



Hardware settings

Name * equip-1

Hardware type FastDPI server

Host * 192.168.1.184

Port * 22

Login * root

Auth type By key

SSH key

Sudo user ☑

By password

By key

Synchronization settings

Enable logs sync ☑

Enable CGNAT sync ☑

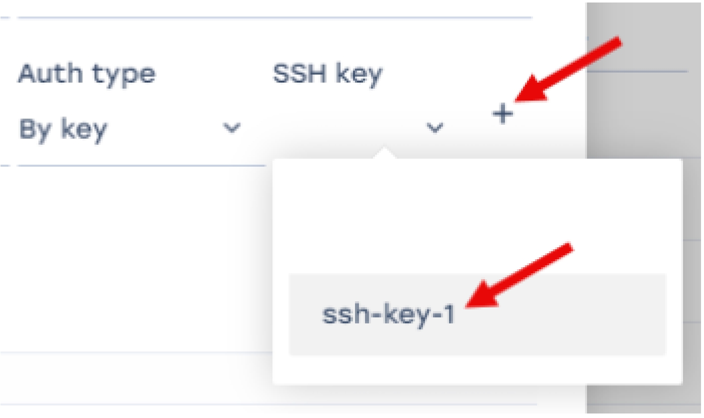
Enable subscribers sync ☑

Enable subscribers auth status sync ☐

IPFIX settings

Id on IPFIX collector 0

5. In the SSH Key field, select the previously created key. Or by clicking on the + create a new SSH key, the process is identical to that described in Step 1. Creating a key (starting from point 4)



Auth type: By key

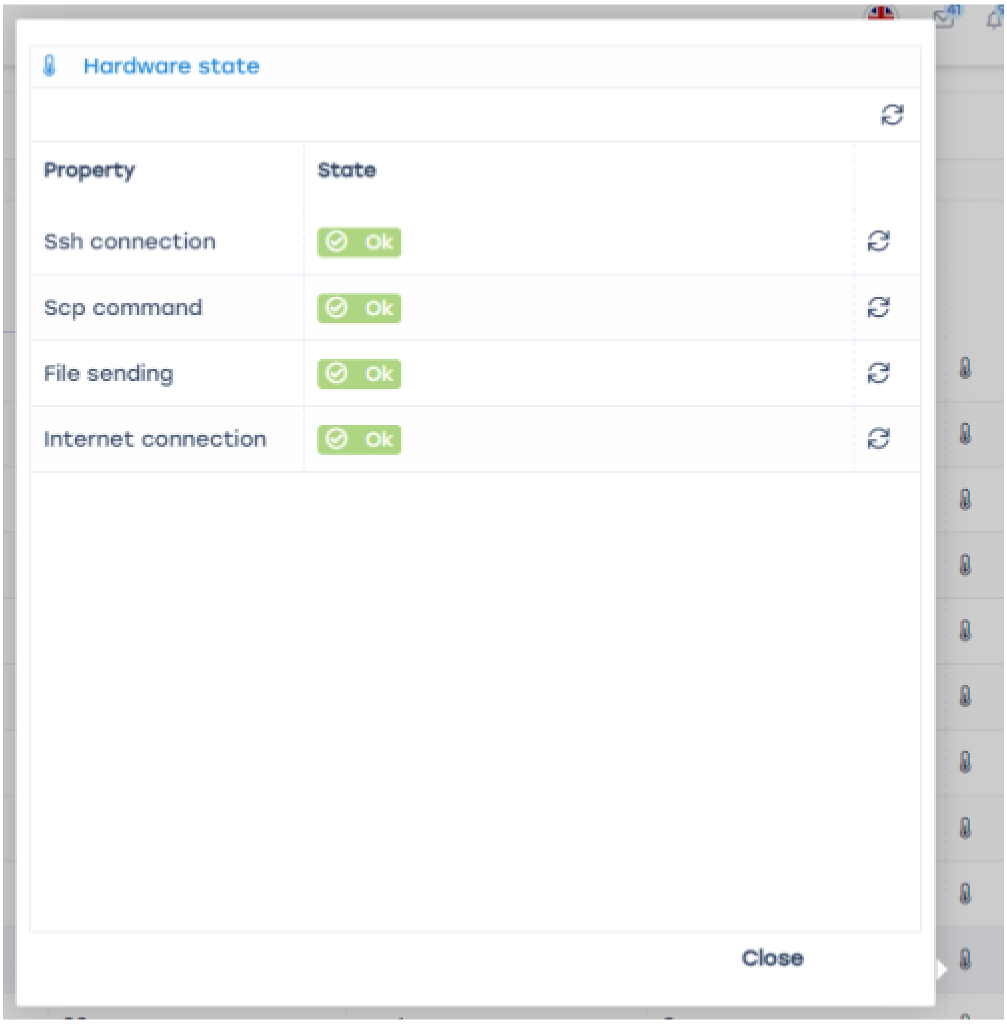
SSH key

6. Click Save

Step 3. Adding the ssh key to the server

1. Under the root user, navigate to the `/root/` folder
   Under a regular user, navigate to the `/home/<username>/` folder
2. Go to the hidden directory `/.ssh/`
3. Open the `authorized_keys` file
4. Add the **public** key content to the file

After completing these steps, check the connection by clicking on the Hardware State button in the Administrator → Equipment section.
If all properties are in the “Ok” state, the connection was successful.



Hardware state

Property	State
Ssh connection	Ok
Scp command	Ok
File sending	Ok
Internet connection	Ok