

Table of Contents

SSH key for connecting to equipment	3
<i>sshd configuration</i>	3
<i>Step 1. Creating a key</i>	3
<i>Step 2. Adding the ssh key to the equipment</i>	5
<i>Step 3. Adding the ssh key to the server</i>	7

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

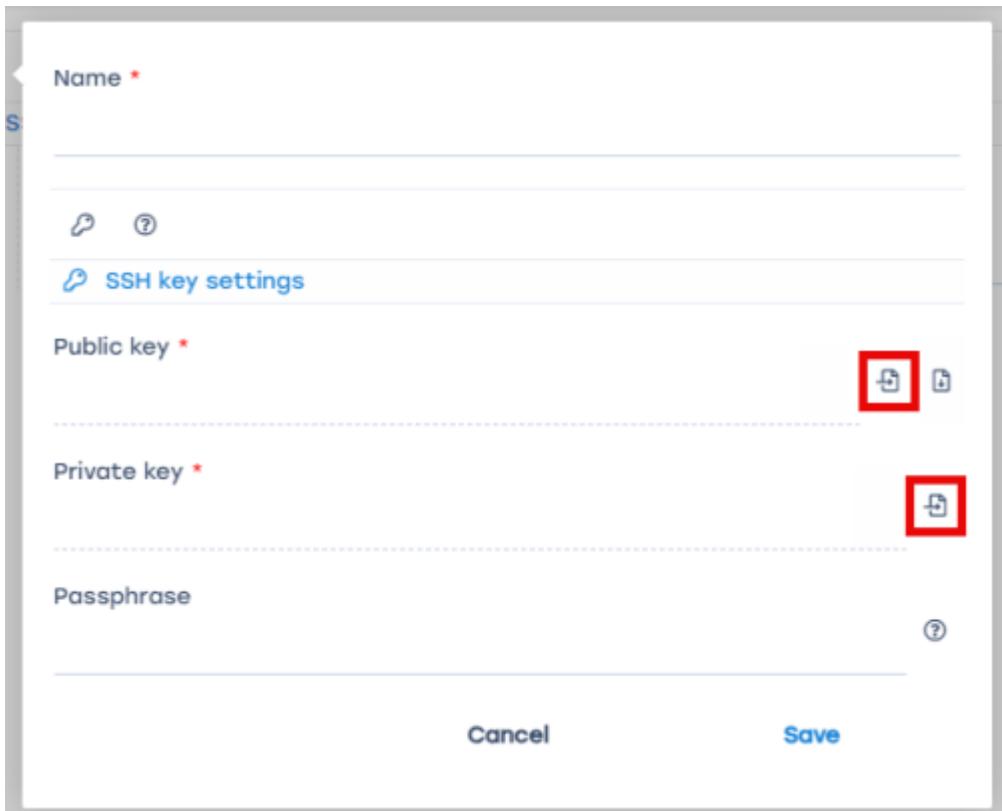
```
sudo systemctl restart sshd
```

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

The screenshot shows the VAS Experts software interface. The left sidebar has a tree structure with 'Administrator' expanded, showing 'Equipment' and 'SSH keys' (which is selected and highlighted in blue). The main content area is titled 'Administrator > SSH keys'. At the top of this area, there is a red box around a large blue '+' button. Below the '+' button is a table with a single column labeled 'ID'. At the bottom of the table is a search bar with the placeholder 'Filter'.

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



Name *

SSH key settings

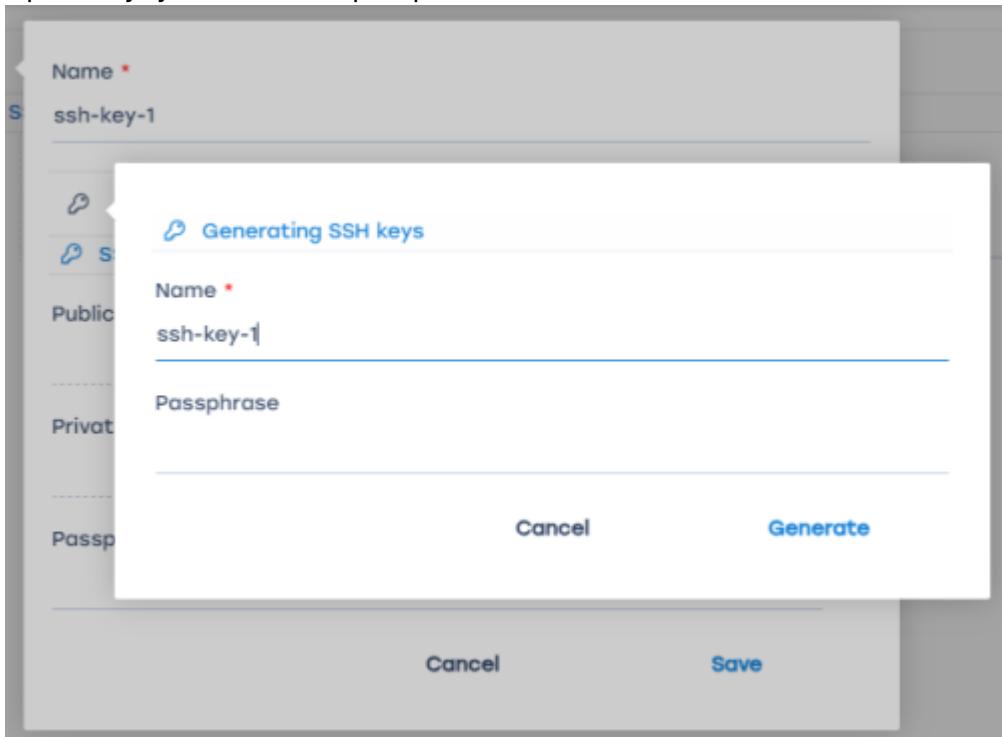
Public key *

Private key *

Passphrase

Cancel Save

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

Generating SSH keys

Name *

ssh-key-1

Passphrase

Cancel Generate

Cancel Save

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

SSH key settings

Public key *
ssh-key-1.pub

Private key *
ssh-key-1

Passphrase

Cancel Save

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

Administrator > Equipment

	ID	Name	Type
<input type="checkbox"/>	18	[REDACTED]	[REDACTED]
<input type="checkbox"/>	25	[REDACTED]	[REDACTED]

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

+

Equipment

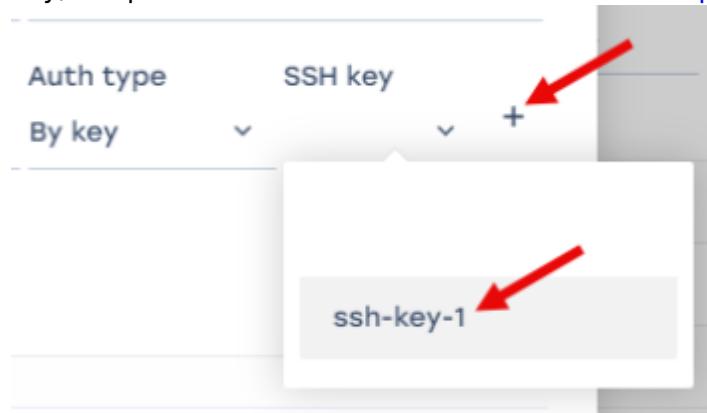
	ID	Name
<input type="checkbox"/>	18	[REDACTED]
<input type="checkbox"/>	25	[REDACTED]
<input type="checkbox"/>	45	[REDACTED]
<input type="checkbox"/>	50	[REDACTED]
<input type="checkbox"/>	52	[REDACTED]
<input type="checkbox"/>	54	[REDACTED]
<input type="checkbox"/>	55	[REDACTED]

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 *	Hardware type	
equip-1	FastDPI server	
Host *	Port *	
192.168.1.184	22	
Login *	Auth type	SSH key
root	By key	[REDACTED]
Sudo user	By password	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Syncronization settings		
Enable logs sync	Enable CGNAT sync	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Enable subscribers sync	Enable subscribers auth status sync	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	
IPFIX settings		
Id on IPFIX collector		
0		
	Cancel	Save

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)



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	Actions
Ssh connection	OK ok	↻
Scp command	OK ok	↻
File sending	OK ok	↻
Internet connection	OK ok	↻

Close