Table of Contents

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

 \bigcirc

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 \rightarrow SSH Keys section
- 2. Click on the + at the top of the screen to add a new key

	VAS Experts	=	Administrator > SSH keys	
Sec	irch	×	+	
20	Administrator	^	SSH keys	
	Equipment		Q. Filter	-
	SSH keys			
	Users			

- 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 *		Ð
Private key *		Ð
Passphrase		0
	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

2			
s	Ø Generating SSH keys		
blic	Name *		
	ssh-key-1		
ivat	Passphrase		
ISSD		Cancel	Generate

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		
<i>P</i> 0		
SSH key settings		
Public key *		
ssh-key-1.pub		-9 0
Private key *		
ssh-key-1		-9 D
Passphrase		
		0
	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 \rightarrow 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

\checkmark	VAS Experts	=	A	dmini	strator > I	Equipment	
Sec	ırch	×	+				
දු	Administrator	~		Equipr	nent		
					ID	Name	ту
	Equipment				Q Filter	Q Filter	
	SSH keys			¢	18		-
	Users			¢	25		

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

+			
	Equipn	nent	
		ID	Name
		Q Filter	Q, Filter
	ø	18	
	¢	25	
	¢	45	
	ø	50	
	¢	52	
	¢	54	
	¢	55	

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

equip-1	FastDPI server	
Host *	Port *	
192.168.1.184	22	
Login * root	Auth type SSH key By key ~ +	
Sudo user	By password	
<u> </u>	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)



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 \rightarrow Equipment section.

If all properties are in the "Ok" state, the connection was successful.

				5 4
& Hardware state				
			e	
Property	State			
Ssh connection	Ø OK		Ø	
Scp command	Ø OK		Ø	
File sending	Ø ok		ß	8
Internet connection	Ø OK		ß	8
				8
				8
				8
				8
				8
				8
				8
		Close		8
		-		0