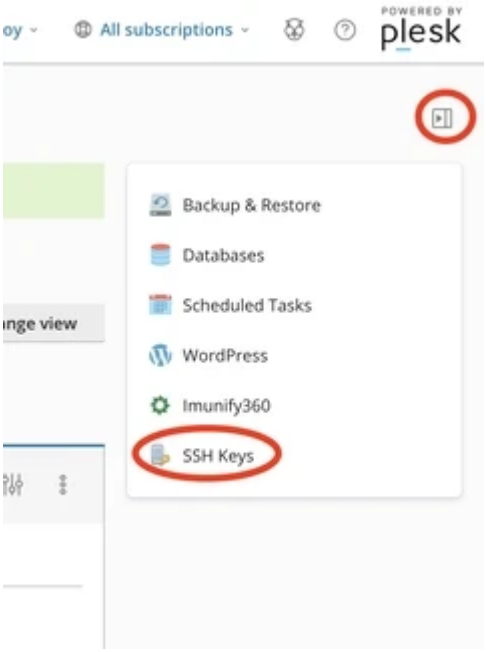
Security

- Managing SSH keys
- Changing your server password

Managing SSH keys

Plesk allows you to manage SSH keys. These keys are needed when you want to access your server via SSH command-line, use a software (like FileZilla or Forklift) to upload files via SFTP, or set the backup system bundled with your account.

When you are logged in Plesk with the right user, you can access the *keys manager* by opening the Plesk right-hand menu, then click on **SSH Key**:



Adding a SSH key to your server

To enable other computer or service to connect to your server via SSH (SFTP, rSync, SSHFS, etc.), you need to add a SSH key relating to this computer or service. In most cases, a key is provided by the service you wish to connect from.

To import this key into your server, in the *keys manager*, just choose to add a key and paste the key content.

> Note this key MUST contain a name, which is not always provided. If it's missing, you have to add it at the end of the key, after a space character (the name of the key itself must not contain spaces).

The format of the key to paste in Plesk should be something like that: `ssh-ed25519 ACR5fG...PKOe8MO my_key_name`

Removing key(s) from your server

You can delete one or more SSH keys at any time by selecting it/them in the *keys manager* and clicking on the **Remove** button.

After the deletion of a key, the external computer or service that was using it to connect will no longer be able to connect to your server.

Changing your server password

The easiest way to change your server password is to do it from your Hosterra account: click on the service you want to manage and then in the window that opened, click in the left side menu on **Change Password** and follow the procedure.

> It is imperative that you change your password after creating your server. The initial password was sent to you by email.