Manage root's SSH Keys

> This document is for a previous release of cPanel & WHM. To view our latest documentation, visit our Home page.

For cPanel & WHM 11.44

(*Home* >> *Security Center* >> *Manage root's SSH Keys*)

Overview
Generate a New Key
Import Key
Manage your keys

Overview

This interface allows you to add, import, and manage the SSH keys on your web server. The system divides SSH keys into public and private key sets in two separate lists.

> **Note:**
> You can use SSH keys to securely copy an account from one server (the remote server) to another server (the local or destination server). For more information, read our How to Copy an Account with SSH Keys documentation.

Generate a New Key

Use this section of the interface to create new SSH key sets, which include a public key and a private key.

To generate a new SSH key set, perform the following steps:

1. Click *Generate a New Key*.
2. To use a custom key name, enter the key name in the *Key Name (defaults to id_dsa):* text box.

   > **Note:**
   > If you use a custom key name, you **must** manually specify the SSH key when you log in to the server.
   >
   > To manually specify the SSH key, run the following command, where `user` is the username and `example` is the server name or IP address:
   >
   > ```
   > ssh user@example -i /root/.ssh/key_name
   > ```

3. To use a password for the SSH key:
   - Enter and confirm the new password in the appropriate text boxes.

     > **Notes:**
     > - The system grades the password that you enter on a scale of 100 points. *0* indicates a weak password, while *100* indicates a very secure password.
     > - Some web hosts require a minimum password strength. A green password *Strength* meter indicates that you met the required password strength.
     > - Click *Password Generator* to generate a strong password. For more information, read our *Password Generator* documentation.

4. Select the desired key type.
    - DSA keys provide quicker key generation and signing times.
    - RSA keys provide quicker verification times.
5. Select the desired key size.

> **Note:**
> Greater key sizes are more secure, but they result in larger file sizes and slower authentication times.

6. Click *Generate Key*. WHM will display the saved location of the key.

> **Important:**
> For the new SSH key to function, you **must** authorize the SSH key. Read the Manage your keys section below for more information.

Import Key

To import an existing SSH key, perform the following steps:

1. Click *Import Key*.
2. To use a custom key name, enter the key name in the *Choose a name for this key (defaults to id_dsa)* text box.

> **Important:**
> If you use a custom key name, you **must** manually specify the SSH key when you log in to the server.
>
> To manually specify the SSH key, run the following command, where `user` is the username and `example` is the server name or IP address:

```
ssh user@example -i /root/.ssh/key_name
```

3. To import a PPK file, enter the password in the *Private key passphrase (Needed for PPK import only)* text box.
4. Paste the public and private keys into the appropriate text boxes.

> **Important:**
> Do **not** enter the private key when you import another server's key to allow SSH connections between the two servers, or to use SSH for account transfers.
>
> Private keys should **always** remain on the server that generated them.

5. Click *Import*.

Manage your keys

The *Public Keys* and *Private Keys* tables display the following information about your existing keys:

Column	Description
Name	The key's name. Public and private keys share the same key name.

Authorization Status	Whether you have authorized the key. **Important:** You **must** authorize new keys before you attempt to use them. **Note:** This column only displays in the *Public Keys* table.
Actions	You can perform the following actions: • *Delete Key* — Click to delete the key, and then click *Yes* to confirm that you wish to delete the key. • *View/Download Key* — Click to view or download the key. To download the key, copy the contents of the text box that appears to a file on your computer. • *Manage Authorization* — Click to manage authorization for the key. In the new interface that appears, click *Authorize* to authorize the key, or *Deauthorize* to deauthorize the key. **Notes:** • This action is only available for public keys. • When you deauthorize a key, that key's users will **not** be able to log in with the associated private key.