# Manage root's SSH Keys

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



## Overview

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

**Note:**
You can use SSH keys to securely transfer 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

To generate a new SSH key set, which includes a public key and private key, perform the following steps:

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

   **Note:**
   If you set a custom key name, you **must** manually specify the SSH key when you log in to the server.

   To manually set 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, perform the following step:
   - Enter and confirm the new password in the appropriate text boxes.

     **Notes:**
     - The system evaluates 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 the password is equal to or greater than the required password strength.
     - Click *Password Generator* to generate a strong password. For more information, read our Password & Security documentation.
4. Select the desired key type.
   - *DSA* — Provides quicker key generation and signing times.
   - *RSA* — Provide quicker verification times.
5. Select the desired key size.

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

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

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

## 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 (PuTTY Key Generator) 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:**
   Private keys should **always** remain on the server that generated them. 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.

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.<br><br>**Important:**<br>You **must** authorize new keys before you attempt to use them.<br><br>**Note:**<br>This column **only** displays in the *Public Keys* table. |

| | |
|---|---|
| *Actions* | You can perform the following actions:<br>• *Delete Key* — Click to delete the key, and then click *Yes* to confirm that you wish to delete the key.<br>• *View/Download Key* — Click to view or download the key. To download the key, copy the contents of the text box that appears and save it as a file on your computer.<br>• *Manage Authorization* — Click to manage authorization for the key. A new interface appears. Click *Authorize* to authorize the key, or *Deauthorize* to deauthorize the key.<br>**Notes:**<br>• The *Manage Authorization* action is **only** availabl e for public keys.<br>• When you deauthorize a key, that key's users **ca nnot** log in with the associated private key. |

## Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Manage root's SSH Keys
- Shell Fork Bomb Protection
- Manage Wheel Group Users
- Terminal in WHM
- Manage Shell Access

- SSH Access
- Terminal in cPanel
- SSL TLS Wizard
- Security Policy
- ModSecurity

- How to Secure SSH
- Manage root's SSH Keys
- Shell Fork Bomb Protection
- Manage Wheel Group Users
- Terminal in WHM

- WHM API 1 Functions - authorizesshkey
- WHM API 1 Functions - check_remote_ssh_connection
- WHM API 1 Functions - convertopensshtoputty
- WHM API 1 Functions - generatesshkeypair
- WHM API 1 Functions - deletesshkey