Linux SSH Key Management

See this article for an update based on obsolete SHA-1 RSA key usage: Ubuntu 22.04 SSH the RSA key isn't working since upgrading from 20.04

NOTE: We currently have two tutorials for this, that need to be consolidated into one. So, maybe this alternate tutorial fills your use-case: How to Setup SSH Key Authentication to Linux

Step 1 - Key Creation

Follow this page for creating keys in Linux: Creating SSH Keys in Linux

Or, Follow this page for creating keys in Windows: Creating SSH Keys in Windows

After following one of the above tutorials, you should have a public and private key that you can use to authenticate.

The next step is to place the public key on your server so that you can use SSH-key-based authentication to log in.

Step 2 — Copying the Public Key to a Linux Server

There’s a couple ways to add an SSH public key to a remote host:

- Using SSH-Copy-ID
- Using CAT
- Manually Copying

Using SSH-Copy-ID

The quickest way to copy your public key to the Ubuntu host is to use a utility called `ssh-copy-id`. Due to its simplicity, this method is highly recommended if available.

See this page for how to use it: Adding SSH Keys with ssh-copy-id

Using CAT

If you do not have `ssh-copy-id` available, but you have password-based SSH access to an account on your server, you can upload your keys using a conventional SSH method.

Here's a method for uploading an SSH key with cat: Adding SSH Keys with CAT

Manually Copying

If you don't have SSH access to the remote host, you will need to directly paste in a user's SSH public key.

See this page for how to manually add SSH keys to a Linux host: Linux: Manually Installing SSH Keys

Step 3 — Authenticating to Your Ubuntu Server Using SSH Keys

If you have successfully completed one of the procedures above, you should be able to log into the remote host *without* providing the remote account's password.

See this page for how to: Authenticating to Linux Server with SSH Keys

If key-based authentication was successful, continue on to learn how to further secure your system by disabling password authentication.

Step 4 — Disabling Password Authentication on Your Server

Once you have confirmed that you can access the VM, with SSH key authentication, follow this page to disable password authentication: Linux: Disabling Password Authentication

Conclusion

You should now have SSH-key-based authentication configured on your server, allowing you to sign in without providing an account password.

If you'd like to learn more about working with SSH, take a look at our SSH Essentials Guide.

Revision #1
Created 1 September 2025 08:10:50 by glwhite

Updated 1 September 2025 08:12:01 by glwhite