How to Remove the SSH Login Details of an Already Logged-in Device?

TechRounder PDF Edition

Live article:
https://www.techrounder.com/how-to/how-to-remove-the-ssh-login-details-of-an-already-logged-in-device/

By Vipin PG | Published May 22, 2023 | Updated March 8, 2026 | Format: Guide | 3 min read

Quick answer

SSH is commonly used to control devices remotely. The command line features offer ultimate control over the device and can perform almost all the activities on the connected machine remotely.

SSH is commonly used to control devices remotely. The command line features offer ultimate control over the device and can perform almost all the activities on the connected machine remotely.

However, there are cases in which the host machine gets formatted, and the remote login via SSH may not work due to the fingerprint mismatch. In this artcile, we will see why the remote login via SSH doesn't work and how to fix the issue.

SSH Connection For Remote Access

Once you try to connect to a remote machine using an SSH connection, you must use the remote machine's username, IP address, or hostname. Once done, a unique fingerprint will be generated and stored on your machine to identify the remote machine.

Then you can use the password of the remote machine to establish the connection. The fingerprint will be saved in your machine and used once you try to log in to the remote machine again. This fingerprint will be unique and will securely identify the correct host machine.

Why is the Remote connection not working with SSH for Know Hosts

After you log in to the remote machine using the SSH connection, any change in the remote machine login configuration may result in an issue with the remote login. If you reset the remote machine and then try to log in with the same username and hostname, the fingerprint will mismatch, and you won't be able to log in via SSH.

How to Fix the SSH Remote Login Issue For Know Clients

If you reset the device, the fingerprint will get changed while login in remotely using SSH, in that case. You can follow two options to fix the fingerprint issue for Known Hosts.

1. You can change the hostname, username, or the device's IP address. Once you try to log in remotely from the previously used machine that previously used, the device will consider the new IP or hostname as a new device, and there won't be any fingerprint mismatch. So you can log in and use the SSH connection as before.

2. If you use the same IP address and username again after reinstalling, then. In contrast, if you log in remotely using an SSH connection with a previously used device, the fingerprint mismatch will happen since it will be considered a known host, and a previously used fingerprint exists within the device.

So the match will not happen and will show an error saying some malpractice happened on the host machine, etc. In this case, the solution is to remove the host machine's already saved SSH fingerprint configuration.

To do so, type ssh-keygen -f ~/.ssh/known_hosts -R

or

ssh-keygen -R

And hit enter. Replace with the correct IP address of the remote machine. Once done, the previously stored login details for the IP address (device) will be cleared, and you can use the exact information again to log in.

It will create a new fingerprint, and you are good to go. This will clear the know host issue with the fingerprint, and you can use the remote login again without any problem.