Dealing with the "Remote Host Identification Has Changed" warning

When connecting to a Linux server via SSH, and successfully logging in, your local machine will save the address and the "fingerprint" for the server in your list of known hosts.

If you ever decide to reinstall the VPS, or have its IP changed, upon the next login you will receive the following warning:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
5a:52:16:46:b7:dc:31:11:3b:a2:2e:d7:12:cd:99:2a.
Please contact your system administrator.
Add correct host key in /home/user/.ssh/known_hosts to get rid of this message.
Offending key in /home/user/.ssh/known_hosts:8
RSA host key for ras.mydomain.com has changed and you have requested strict checking.
Host key verification failed.
```

The easiest way to deal with this error message would be to remove the "Offending key". In this example that would be the key 8 in our hosts file. To do this, execute the following command:

```
sed -i 8d ~/.ssh/known_hosts
```

Where "8" denotes the line in the hosts file to remove.

Now upon connecting you will receive the usual warning:

```
The authenticity of host '99.99.99.99 ()' can't be established.
ECDSA key fingerprint is 4e:10:42:39:53:85:7f:89:89:dc:89:84:8d:79:e7:ed.
Are you sure you want to continue connecting (yes/no)?
```

After confirming with "yes", the new fingerprint will be added to your known hosts and you will be logged in to your VPS.

⚠ If you receive this error and you have not reinstalled your server or requested IP change for it, please contact us via a support ticket