



SSH Into Environment

Contents

Goals	2
What is SSH? What is a SSH Port? Why SSH?	2
How do you Connect via SSH from a Linux system?	2
How do you Connect via SSH from a Windows system?	4
Conclusion	10

Goals

This guide will help you understand how to remote login to your Linux server system via SSH (Secure Shell) to access the system contents from the back-end. Once you have successfully logged in, you will be able to view contents, edit contents, and execute commands from your system back-end.

To SSH into an environment, all you require is the remote system IP address, username, password, and an SSH client.

What is SSH? What is a SSH Port? Why SSH?

Secure Shell or SSH is a network protocol that is used to connect to a server system, transfer data, and execute commands via a secure line between two network systems. The default port number is 22.

You may ask why you would want to use SSH if there are many other remote protocols. This is because SSH is a replacement for other remote protocols such as rsh, telnet and rexec, which all send information as plain text (including passwords and other user information). Therefore, there is a high security risk factor with sending data using these protocols. SSH overcomes this security issue by encrypting the data and sending it via a secure line. SSH provides high confidentiality and integrity of data over any secured or unsecured network.

How do you Connect via SSH from a Linux System?

- 1) Open the terminal or shell (the command line).

```
[test_user1@CentOS ~]$
```

- 2) You can type the command below to connect to a remote system via SSH protocol.

```
ssh <username>@<remote system IP>
```

For example, if the username is “root” and the remote system IP is 10.0.0.239, you can type the following to connect to the system:

```
ssh root@10.0.0.239
```

```
[test_user1@CentOS ~]$ ssh root@10.0.0.239
```

- 3) If you are connecting to the system for the first time, you will be asked the following. You can type “Yes” to connect.

```
[test_user1@CentOS ~]$ ssh root@10.0.0.239
The authenticity of host '10.0.0.239 (10.0.0.239)' can't be established.
RSA key fingerprint is 86:4b:d6:af:51:ef:80:2f:7f:82:d3:17:d6:e8:d0:5c.
Are you sure you want to continue connecting (yes/no)?
```

In this section SSH is asking for host validation. This is an important feature of SSH for better security and prevention of hacking methods such as spoofing. SSH is simply asking you whether *this the system or server that you were expecting to connect to.*

- 4) In the next step, you will see a prompt to type the password.

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.239' (RSA) to the list of known hosts.
root@10.0.0.239's password: █
```

- 5) Type the remote user password and you will be connected to the system.

```
root@10.0.0.239's password:
Last login: Sat Mar 17 12:22:11 2012 from 10.0.0.239
[root@CentOS ~]# █
```

- 6) Now you have successfully logged into your server system via SSH!

How do you Connect via SSH from a Windows System?

If you are on a Windows PC, you can also connect to your server system via SSH. There are a number of SSH clients available on the market and most of them are free to use. One example of an SSH client is PuTTY.

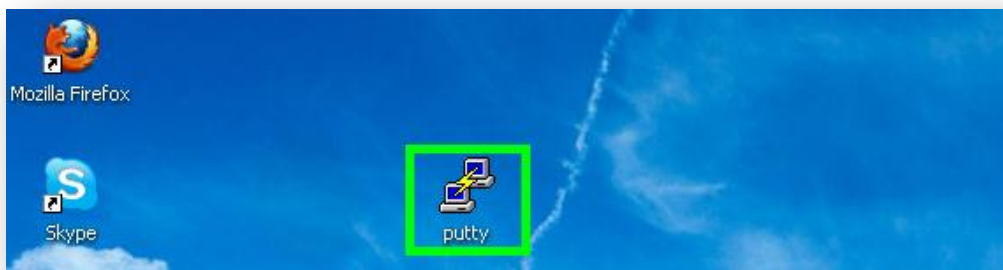
In this section we will discuss about how to connect to a remote PC via SSH using PuTTY.

- 1) First, you have to install PuTTY software on your system.

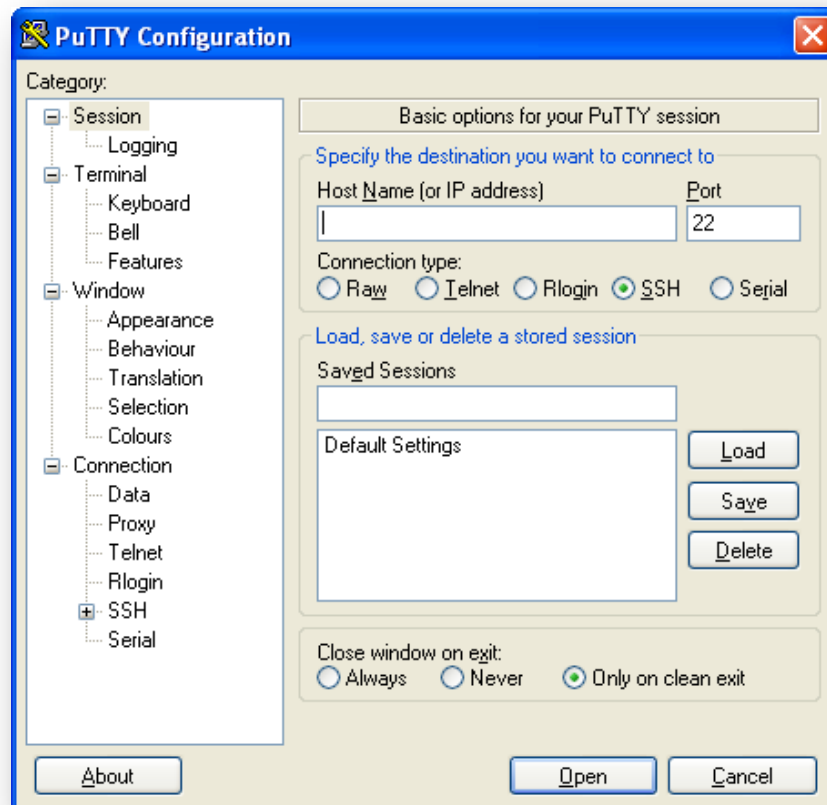
You can go to the official PuTTY website for downloading the latest version of PuTTY:

<http://putty.nl/download.html>.

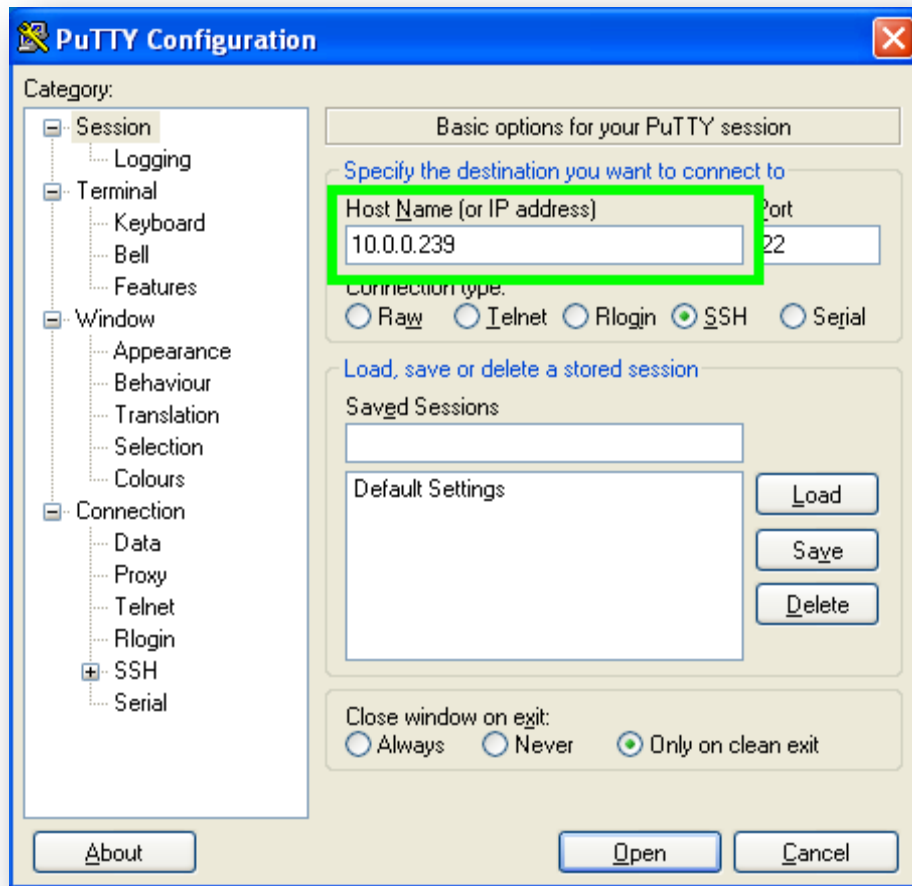
- 2) After installation, simply click on the PuTTY icon to execute the program.



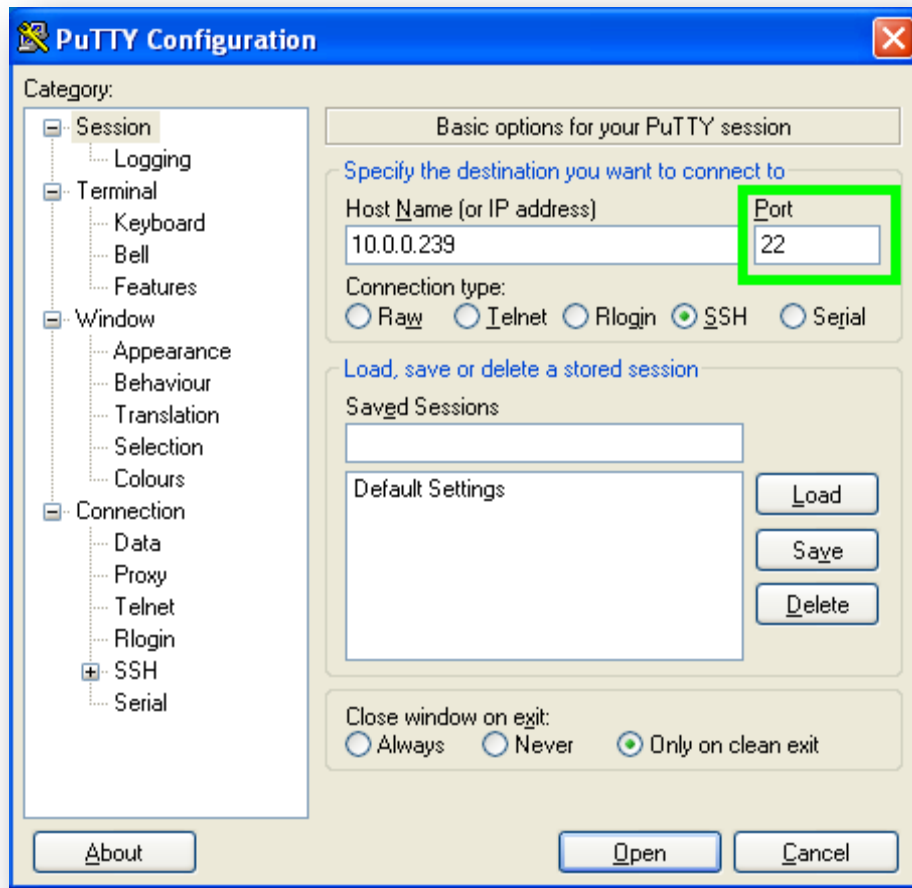
- 3) Now you will get the PuTTY connection screen.



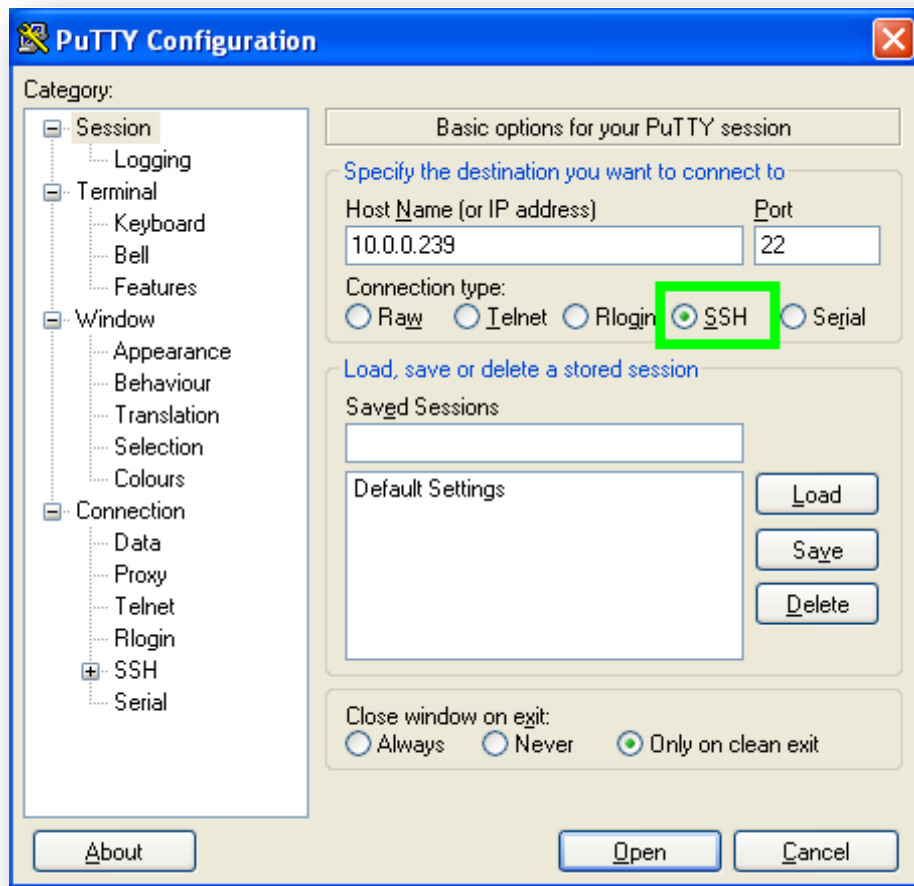
- 4) In the Host Name (or IP address) field, please provide your remote system IP or the system host name.



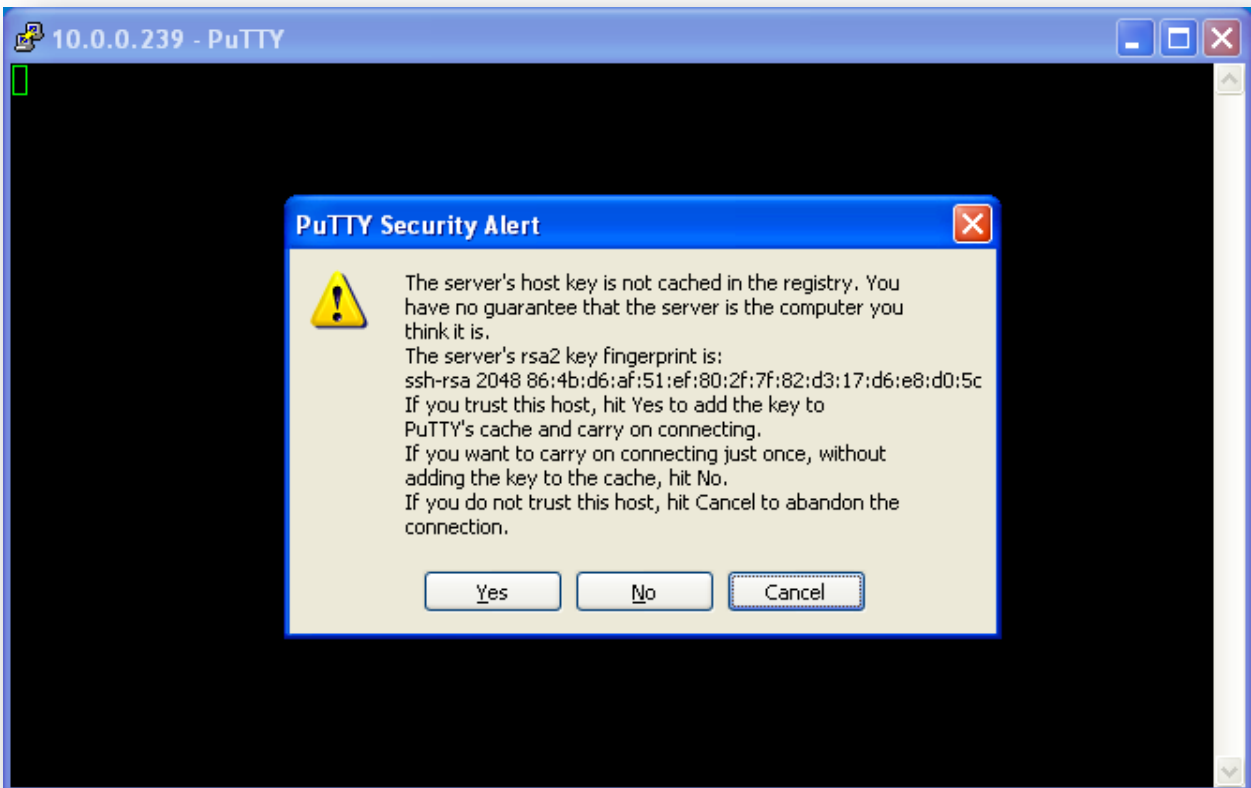
- 5) In the Port field, please provide the port number “22”. (It is the default SSH port. If the server is using a different SSH port, then you have to specify that port here.)



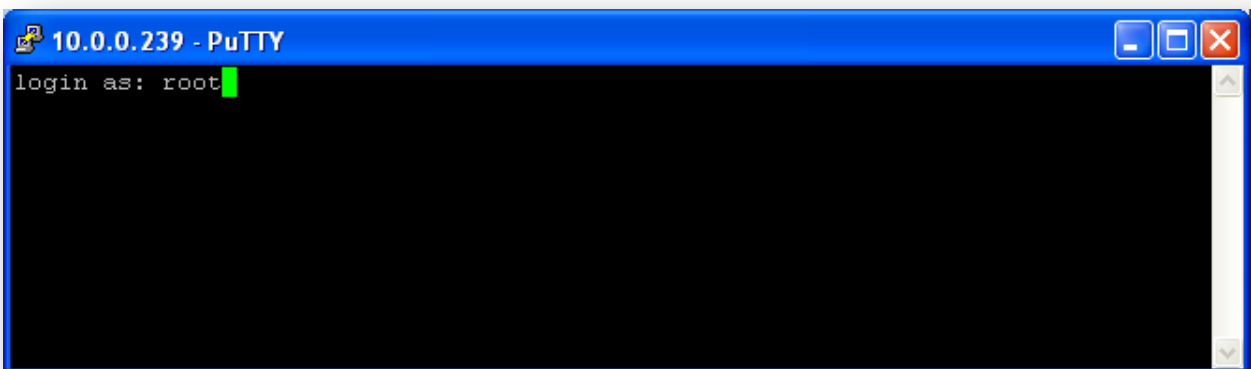
6) In the Connection type section, please select SSH.



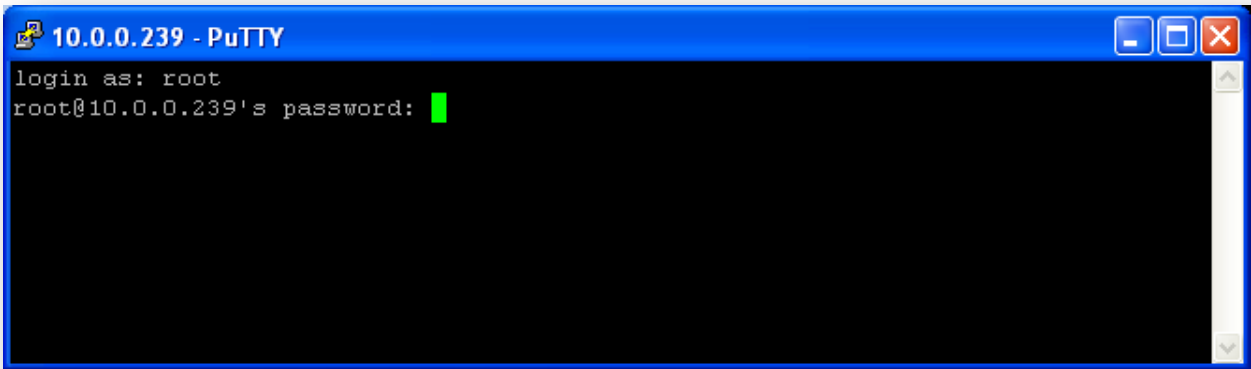
- 7) Now click Open to connect to the remote system. If you are connecting for the first time, you will receive a host key validation prompt. This is an important feature of SSH for better security and prevention of hacking methods such as spoofing. SSH is simply asking you if this is the system or server that you were expecting to connect to. You can click “Yes” to continue.



- 8) In the next step, you will see a prompt to type the username. Please provide your username there.

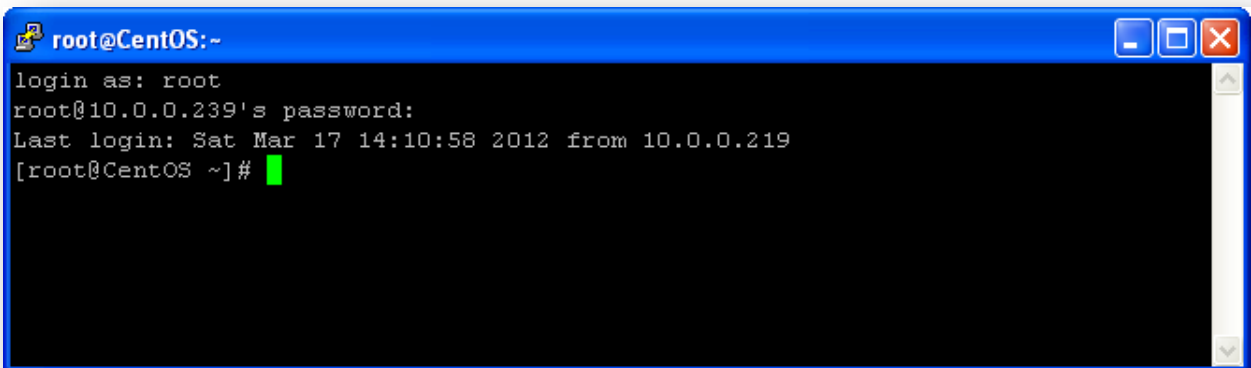


- 9) In the next step, you will see a prompt to type the password. Type your password there. (Note that, in PuTTY, you cannot paste the password. You have to manually type it into the screen.)



```
10.0.0.239 - PuTTY
login as: root
root@10.0.0.239's password: █
```

10) Now you have successfully connected to your system using PuTTY.



```
root@CentOS:~
login as: root
root@10.0.0.239's password:
Last login: Sat Mar 17 14:10:58 2012 from 10.0.0.219
[root@CentOS ~]# █
```

Conclusion

Now you have successfully logged into your remote server system via SSH. You can view your system contents, edit those contents, and execute commands from the system back-end. Even if you have a control panel, it is sometimes necessary to access contents from the back-end. If you encountered any issues with this guide, please also note that there is additional information available in our Wiki database at <http://myhosting.com/kb>. Finally, we encourage you to contact our technical support team by email at vps@myhosting.com, or calling us at 1-866-289-5091 with any questions or concerns.