

[\[Home\]](#) [\[Forum\]](#)

ESXi 4.0 does ship with the ability to run SSH, but this is disabled by default (and is not supported). If you just need to access the console of ESXi, then you only need to perform steps 1 - 3.

- 1) At the console of the ESXi host, press ALT-F1 to access the console window.
- 2) Enter **unsupported** in the console and then press Enter. You will not see the text you type in.
- 3) If you typed in unsupported correctly, you will see the Tech Support Mode warning and a password prompt. Enter the password for the root login.
- 4) You should then see the prompt of ~#. Edit the file inetd.conf (enter the command **vi /etc/inetd.conf**).
- 5) Find the lines that begins with #ssh and remove the #. Then save the file. If you're new to using vi, then move the cursor down to #ssh line and then press the **Insert** key. Move the cursor over one space and then hit backspace to delete the #. Then press **ESC** and type in **:wq** to save the file and exit vi. If you make a mistake, you can press the **ESC** key and then type it **:q!** to quit vi without saving the file. **Note:** there are two lines for SSH with ESXi 4.0 now - one for regular IP and the other for IPv6. You should the line appropriate to the protocol you'll use to access your host.
- 6) Once you've closed the vi editor, you can either restart the host or restart the inetd process. To restart inetd run **ps | grep inetd** to determine the process ID for the inetd process. The output of the command will be something like 1299 1299 busybox inetd, and the process ID is 1299. Then run **kill -HUP <process\_id>** (kill -HUP 1299 in this example) and you'll then be able to access the host via SSH.

**Tip** - with some applications like WinSCP, the default encryption cipher used is AES. If you change that to Blowfish you will likely see significantly faster transfers.

## Changing the port for SSH

To change the port for SSH, edit the file /etc/services and change the SSH port listed in the file. Save the file and repeat step 6 above.

## Enable Telnet

The steps are the same as with SSH, but you'll remove the # from the 2 telnet entries in /etc/inetd.conf. Enabling telnet is not recommended if security is a concern.

You can also download an [oem.tgz](#) file which will enable SSH (and FTP). Copy the file to a datastore with the VI client and then to bootbank with the command `cp /vmfs/volumes/<datastore>/oem.tgz /bootbank/oem.tgz` and then reboot.

## Enable SSH access for a non-root account

Use the following process to enable SSH access for a non-root account

- 1) Access SSH or the console with a root account.
- 2) Create a new account with the command **useradd <account\_name> -M -d/**. This will set the home directory to / instead of requiring a /home directory.
- 3) Use the command **passwd <account\_name>** to set the password for your new login.
- 4) Edit the passwd file with **vi /etc/passwd**. For the entry for your new account, change the /bin/sh part to /bin/ash. Save the file and exit. See the example for the test1 user below.

```

root:x:0:0:Administrator://:bin/ash
nobody:x:99:99:Nobody://:sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User://:sbin/nologin
dcui:x:100:100:DCUI User://:sbin/nologin
daemon:x:2:2:daemon://:sbin/nologin
vimuser:x:12:20:vimuser:/:sbin:/sbin/nologin
test1:x:500:500:Linux User,,,://:bin/ash

```

You should now be able to connect with SSH using this new account.

### Disable SSH access for the root account

If you have created non-root accounts for SSH access you can also disable root access via SSH. Edit the `/etc/inetd.conf` file using the initial process on this page and add the option `-w` after the `-i` option. The line in `inetd.conf` will appear similar to the below.

```

ssh stream tcp nowait root /sbin/dropbearmulti dropbear
++min=0,swap,group=shell -i -w -K60

```

Once you have made the change, save the file and run the `kill -HUP` command to restart the `inetd` process. You will now be able to login with a non-root account, but will get access denied if you use a root account. Once you have established a SSH session with your non-root account you can issue the command `su -` to switch to the root account.

---

[[-](#)] [Martin Ruegg](#) 08-23-2009

thanks for your great hints!

if one can paste code to the console (eg. when accessing the host via a remote control card) the follow

```
sed -ri "s/^\#ssh/ssh/g" /etc/inetd.conf
```

```
kill -HUP `ps | grep inetd | sed -r "s/^\([0-9]+\).*\1/"`
```

regards,

martin.

---

[[-](#)] [Overand](#) 02-02-2010

In my experience with 3.5 U3 and U4, you can type:

```
kill -HUP $(pidof inetd)
```

My guess is this will work on 4.0 as well.

---

[[-](#)] [André Franciosi](#) 03-12-2010

Still going for ESXi 4

---

[[-](#)] [hugo](#) 04-29-2010

How to enable passwordless SSH ?

---

[ - ] [Dave Mishchenko](#) 04-29-2010

@hugo - see this thread - <http://communities.vmware.com/thread/183867>.

---

[ - ] ChrisG 05-25-2010

Hi,

No problems getting SSH working on ESX1 4 U1 but when I connect using PuTTY I can only connect other VMware messages coming up followed by the "~ #" prompt. Is this normal?

I've also noticed I cannot see everything I would see on a full ESX system (for instance, I want to be able to see the output of the 'ls' command, this is the same symptom when using vcli or vMA on ESX instead of using SSH.)

Any help you may be able to give would be very much appreciated.

Thanks, ChrisG

---

[ - ] [Dave Mishchenko](#) 05-26-2010

Hi Chris, I've updated the instructions above to allow for non-root access. The tech support message I checked a system and /etc/opt/vmware/vpxa/vpxa.cfg does exist on it.

---

[ - ] ChrisG 05-28-2010

Thanks Dave, much appreciated. I'll give that a try tomorrow.

Cheers, Chris

---

[ - ] Julian Pawlowski 07-01-2010

One could also use option -g instead of -w.

This way root is still able to login via key and one could still use root to copy any data via scp.

---

[ - ] Peter 07-16-2010

Thanks You!

Useful article!

---

[ - ] Andy 07-16-2010

SUDDENLY!!! Enable/Disable option for local (console) and remote (SSH) TechSupport mode wa

---

[ - ] Dave 11-19-2010

Great post. But why does Step 5 end suddenly? "You should" what???

[-] Brantley 12-14-2010

Dave, You should - you should enable ssh on IPv6 if needed on your network. Since most networks

[-] ckgreenman 12-20-2010

Just a quick FYI. You can avoid step 4 in the "Enable SSH access for a non-root account" by using busybox for the useradd binary then it should also work in 4 as well.

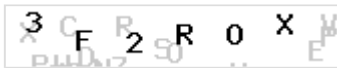
**ADD YOUR COMMENT - IF YOU HAVE A QUESTION PLEASE USE THE [FORUM](#)**

Name (required)

Web site (optional)

Email address (required - will not be displayed)

Comment (required)



Please enter code