

# How to configure networking and firewall for use with Symantec Mobility

## Root Shell Access

1. The # symbol at the beginning of the command line signifies that this session has root privileges.

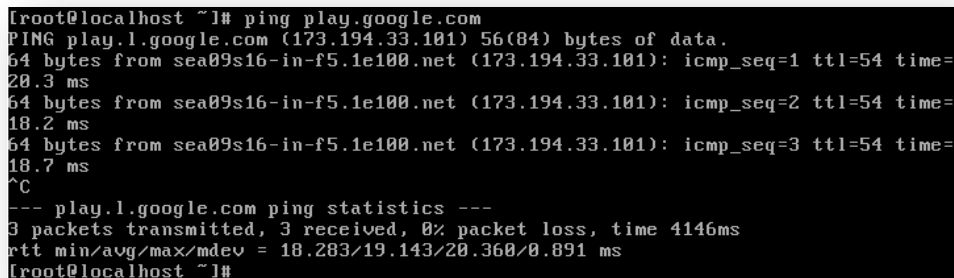
**Note:** If the server was deployed using a template and a user account is needed to access the console. Log into the console with the provided user credentials. Type **su** and hit **Enter** to elevate the session to root privileges. If the sudoer's methodology is being used type **sudo su** to elevate the account. Prefixing any command with **sudo** will elevate that command with root privileges. Mobility Suite requires full root shell access to complete its installation.

2. Continue to [Confirm Network Connectivity](#).

**Tip:** Press the **Tab** key after typing a few characters of the filename listed in a command, it should finish the remainder of it. This should make typing commands quicker. Pressing **Tab** twice will display all the available options beginning with that word, file or directory.

## Confirm Network Connectivity

1. Verify Internet communication by typing, as root: **ping play.google.com**, to cancel the echo: while holding down the **Ctrl** key press **c** this will return the console back to the **root** shell:



```
[root@localhost ~]# ping play.google.com
PING play.l.google.com (173.194.33.101) 56(84) bytes of data.
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=1 ttl=54 time=
20.3 ms
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=2 ttl=54 time=
18.2 ms
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=3 ttl=54 time=
18.7 ms
^C
--- play.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4146ms
rtt min/avg/max/mdev = 18.283/19.143/20.360/0.891 ms
[root@localhost ~]# _
```

**Tip:** If no ICMP response is received, verify whether ICMP is blocked or type **/sbin/ifconfig** to verify the network settings. To edit the network configuration type **vi /etc/sysconfig/network-scripts/ifcfg-eth0** and **Enter**. A vi edit view will appear. Type **i** to begin editing. The up, down, left & right arrows must be used to navigate through this configuration file. Make the appropriate changes to the network settings. Hit the **Esc** key once and while holding **Shift** press the **:** (colon) key once and release. Now type **wq** and hit **Enter**; this will write the changes to the file. To exit without making any changes, instead of **wq** type **q!** and hit **Enter**. Now restart the network services to reapply this configuration script by typing, as root: **service network restart** and **Enter**. Repeat these steps until the correct network configuration is obtained.

For example:

```
root@multife1:~  
DEVICE=eth2  
TYPE=Ethernet  
ONBOOT=yes  
NM_CONTROLLED=yes  
BOOTPROTO=None  
USERCTL=no  
IPV6INIT=no  
IPADDR=172.19.215.10  
NETMASK=255.255.255.0  
GATEWAY=172.19.215.1  
DNS1=172.19.216.6  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~
```

**Important:** A working network configuration is required before proceeding further. It is highly recommended to set the **ONBOOT=** to **yes** as shown above. The hardware and ID of the NIC may be shown but they are optional. Remember that after any changes are made it will be necessary to restart the network services.

**Tip:** Quick guide to **vi**:

**i**  $\rightarrow$  Insert

**Esc key** → End insert mode and returns to command mode which allows the below two commands:

**:q!** → Colon followed by **q!** quits without making any changes.

**:wq** → Colon followed by **wq** writes and quits, saving changes.

2. Ping the server's hostname, which was set in step 28 of [Install CentOS 6.5 \(HOWTO110253\)](#). The return should be on the IPV4 loopback address: **127.0.0.1**. If it is not then **vi** into **/etc/hosts** and append the server's hostname to the end of the line containing **127.0.0.1**:



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

: wqf\_

5. Continue to [Configure IPTables](#).

## Configure IPTables ([HOWTO110255](#))

For more information on hardening Linux for Mobility see [HOWTO98546](#).

## Using IPTables (HOWTO110235):

Add 80 and 443 to the IPTables chain by entering the following lines, as root:

```
/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
/etc/init.d/iptables save
```

## No IPTables (HOWTO110255):

If the Mobility Suite FE (server) is deployed behind a firewall and IPTABLES is not needed, run the following two commands, as root:

```
/etc/init.d/iptables stop
chkconfig iptables off
```

For more information on ports used by Symantec Mobility Suite see [HOWTO94496](#). More information on IPTables may be found at <http://wiki.centos.org/HowTos/Network/IPTables>.

Once IPTables is configured, as needed, continue to [SSH](#).

SSH ([HOWTO110256](#))

1. To install SSH, as root enter:  
**sudo yum -y install openssh-server openssh-clients**
2. Set the service to start with the machine:  
**chkconfig sshd on**
3. Start the service:  
**service sshd start**
4. Make sure port 22 is opened:  
**netstat -tulpn | grep :22**

Look for a link showing TCP 22 as open.

**Tip:** The | (**pipe**) symbol in the above command can be **shift** (key) + \

5. If port 22 is not open, enter the following two lines into terminal:  
**/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT**  
**/etc/init.d/iptables save**
6. Reboot the system by typing:  
**sudo reboot**

**Tip:** Now is a good time to take a [snapshot](#) of the current hard drive state.