

SOP for Blocking Port 1131 and 1113 on ioPAC 8500/8600 Series

1. Block incoming ports 1131 and 1113 using the "iptables" command

```
# sudo iptables -A INPUT -p tcp --destination-port 1131 -j DROP
# sudo iptables -A INPUT -p tcp --destination-port 1113 -j DROP
```

2. Check the firewall rules listed below have been added

```
# sudo iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:1131
DROP       tcp  --  anywhere              anywhere               tcp dpt:1131
DROP       tcp  --  anywhere              anywhere               tcp dpt:1113
```

3. Save the firewall rules settings

```
# sudo iptables-save > /etc/iptables.rules
```

4. Set up "iptables.up" files, which will reactivate the firewall rules every time the ioPAC 8500/8600 Series is rebooted

```
# sudo vi /etc/NetworkManager/dispatcher.d/pre-up.d/iptables.up
#!/bin/sh
/sbin/iptables-restore < /etc/iptables.rules
```

```
# sudo chmod 755 /etc/NetworkManager/dispatcher.d/pre-up.d/iptables.up
```

5. Reboot

```
# sudo reboot
```

SOP for Reopening Port 1131 and 1113 on ioPAC 8500/8600 Series

1. Check if the incoming ports 1131 and 1113 have been blocked by the firewall rules

```
# sudo iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:1131
DROP      tcp  -- anywhere             anywhere              tcp dpt:1131
DROP      tcp  -- anywhere             anywhere              tcp dpt:1113
```

2. Delete the blocked firewall rules

```
# sudo iptables -D INPUT 2
# sudo iptables -D INPUT 1
```

3. Check the firewall rules again (no rules to 'DROP' TCP port 1131 and 1113)

```
# sudo iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
```

4. Save the firewall rules settings

```
# sudo iptables-save > /etc/iptables.rules
```

5. Reboot

```
# sudo reboot
```