



## Changing the Configurable Ports available on a Nomadix

**Purpose:** Illustrate what steps are taken to configure ports to be used for DNS redirection, HTTP/HTTPS Web Management Interface (WMI), Telnet and SNMP.

### DNS Redirection:

1. Navigate to Configuration -> DNS
2. Change to a port already not in use between 1030 and 5000
3. Reboot

**Domain Name Service (DNS) Settings**

Setup AG presence in DNS

Host Name

Proxy UDP DNS Port

DNS Redirection Port  Fixed   Floating ⓘ

DNSSEC Support  Enabled

**Note:** Ports must be different and between 1024 and 5000.

(Floating port will be chosen randomly between 5001 and 65535.)



## Web Management and Telnet:

1. Navigate to Network Info - > Sockets, check to make sure port is not listed
2. Navigate to Configuration - > Access Control and change the port number(s)
3. Click on Save then Reboot to apply the change

**Access Control**

---

**Configurable Ports** Note: Make sure that the ports are not allocated already

Telnet Port	<input type="text" value="23"/>
HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>

NOTE: Port number changes require a reboot to be put into operational effect.

---

**Block Network-side Interfaces**

Block Network-side Telnet Access	<input type="checkbox"/> Blocked	
Block Network-side Web Management Access (HTTP)	<input type="checkbox"/> Blocked	<span style="color: red;">Note: This will terminate the current network-side session</span>
Block Network-side Web Management Access (HTTPS)	<input type="checkbox"/> Blocked	
Block Network-side FTP Access	<input type="checkbox"/> Blocked	
Block Network-side SFTP Access	<input type="checkbox"/> Blocked	
Block Network-side SSH Shell Access	<input type="checkbox"/> Blocked	

---

**Block Subscriber-side Interfaces**

Block Subscriber-side Telnet Access	<input checked="" type="checkbox"/> Blocked	
Block Subscriber-side Web Management Access (HTTP)	<input checked="" type="checkbox"/> Blocked	<span style="color: red;">Note: This will terminate the current subscriber-side session</span>
Block Subscriber-side Web Management Access (HTTPS)	<input checked="" type="checkbox"/> Blocked	
Block Subscriber-side FTP Access	<input checked="" type="checkbox"/> Blocked	
Block Subscriber-side SFTP Access	<input checked="" type="checkbox"/> Blocked	
Block Subscriber-side SSH Shell Access	<input type="checkbox"/> Blocked	

---

**General Protocol Restrictions and Allowances**

Allow SSLv2 and SSLv3 (Note: TLS is always allowed)	<input type="checkbox"/> Enabled	<span style="color: red;">▲ Important</span>
-----------------------------------------------------	----------------------------------	----------------------------------------------

---

**Source IP-based Access Control**

Access Control to NSE management interfaces ⓘ	<input type="checkbox"/> Enabled	<span style="color: red;">▲ Important</span>
Allow access to IPv6 subscriber-side devices	<input type="checkbox"/> Enabled	<span style="color: blue;">i</span>

IP Access Control List Management [Show >>>](#)

---



The following port numbers cannot be used:

- FTP port 21
- SSH port 22
- Telnet port 23 (WMI, DNS)
- SMTP port 25
- DHCP server port 67
- DHCP client port 68
- HTTP port 80 (Telnet, DNS)
- HTTPS port 443 (Telnet, DNS)
- NTP port 123
- NTP port 301
- SNMP trap port 162
- HTTPS port 443
- IKE port 500
- Syslog port 514
- DNS port 1025 (WMI, Telnet)
- DNS port 1026 (WMI, Telnet)
- DNS port 1027 (WMI, Telnet)
- DNS port 1028 (WMI, Telnet)
- DNS port 1029 (WMI, Telnet)
- Port 1111
- Port 1112
- RADIUS ports 1645, 1812
- RADIUS Acct ports 1646, 1813
- L2TP port 1701
- ICC port 2111
- Splash Page port 3111
- IPsec port 4500
- DAT'd ports
- Configured DNS ports (WMI, Telnet)
- Configured Passthrough port
- Configured RADIUS proxy port
- Configured Static Mapping port(s)



## SNMP:

**SNMP Settings**

Setup AG remote administration by SNMP

SNMP Daemon  Enabled

SNMP Daemon Listening Port  Valid port range: 1 - 5000

---

System Contact

System Location

Get (Read) Community

Set (Write) Community

Trap Community

Trap Recipient IP

DAT Trap Interval (15-600) sec

Ethernet Link Traps  Enabled