



Changing the Configurable Ports available on a Nomadix Gateway with version 7.0.030.

Purpose: Illustrate what steps are taken to configure ports to be used for DNS redirection, HTTP/Web Management Interface (WMI) and Telnet. With the x.4.2 release certain ports are now configurable. If you do not have a release that supports this feature please contact your reseller for firmware upgrade options.

DNS Redirection:

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

The screenshot shows the web interface of a Nomadix Gateway. The left sidebar contains a tree view of configuration options, with 'DNS' selected. The main content area is titled 'Domain Name System (DNS) Settings'. It contains several input fields for configuration:

- Host Name: your host name
- Domain: yourdomain.com
- Primary DNS Server: 192.0.0.0
- Secondary DNS Server: 192.1.0.0
- Tertiary DNS Server: (empty)
- DNS Redirection Port: 1029
- Proxy DNS Port: 1028

Below the input fields, there are two red notes:

- NOTE: Ports must be different and between 1024 and 5000.
- NOTE: If DHCP Client or PPPoE Client is enabled, the Primary and Secondary DNS Server may not be configured, since the DHCP/PPPoE server may provide those items. Furthermore, if DHCP Client is configured, the Domain may not be configured.

There is also a red note: NOTE: You must reboot for configuration changes to take effect.

At the bottom of the settings section, there is a checkbox for 'Reboot after changes are saved?' with the 'Yes' option selected. Below this are 'Submit' and 'Reset' buttons.

The bottom section of the interface is titled 'Available NIS Services' and contains three links:

- [Nomadix Support Services](#) -- Software, hardware and call center support for your NSE Gateway
- [Intelligent Roaming](#) -- Aggregation service designed to increase network usage
- [SMTP Relay](#) -- Application prioritization service designed to limit SMTP (SPAM) abuse



WMI 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. Reboot

Access Control

Configurable Ports

| | | |
|-------------|----------------------------------|--|
| Telnet Port | <input type="text" value="23"/> | Make sure that the port is not allocated already |
| HTTP Port | <input type="text" value="80"/> | Make sure that the port is not allocated already |
| HTTPS Port | <input type="text" value="443"/> | Make sure that the port is not allocated already |

Block Network-side Interfaces

| | | |
|--|--|---|
| Block Network-side Telnet Access | <input type="checkbox"/> Enable | |
| Block Network-side Web Management Access (HTTP) | <input type="checkbox"/> Enable | Please note that this will terminate the current network-side session |
| Block Network-side Web Management Access (HTTPS) | <input type="checkbox"/> Enable | |
| Block Network-side FTP Access | <input type="checkbox"/> Enable | |
| Block Network-side SFTP Access | <input checked="" type="checkbox"/> Enable | |
| Block Network-side SSH Shell Access | <input checked="" type="checkbox"/> Enable | |

Block Subscriber-side Interfaces

| | | |
|---|--|--|
| Block Subscriber-side Telnet Access | <input checked="" type="checkbox"/> Enable | |
| Block Subscriber-side Web Management Access (HTTP) | <input checked="" type="checkbox"/> Enable | Please note that this will terminate the current subscriber-side session |
| Block Subscriber-side Web Management Access (HTTPS) | <input checked="" type="checkbox"/> Enable | |
| Block Subscriber-side FTP Access | <input checked="" type="checkbox"/> Enable | |
| Block Subscriber-side SFTP Access | <input checked="" type="checkbox"/> Enable | |
| Block Subscriber-side SSH Shell Access | <input checked="" type="checkbox"/> Enable | |

Source IP-based Access Control

| | |
|----------------|---------------------------------|
| Access Control | <input type="checkbox"/> Enable |
|----------------|---------------------------------|

NOTE: You must reboot for setting changes to take effect.

Reboot after changes are saved? Yes

Please enter an IP address/range:
Note: Up to 50 Access Control IP addresses/ranges can be entered.
Note: Please make sure to enter the correct addresses.

| | | | |
|--------------------------|----------------------|------------------------|-----------------------------------|
| Access Control Start IP: | <input type="text"/> | Access Control End IP: | <input type="text" value="None"/> |
|--------------------------|----------------------|------------------------|-----------------------------------|

Currently Access is Permitted for IP's:
172.30.30.173

Number of Access Control Addresses/Ranges: 1



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 port 161
- 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)**