WANrockIT
Software Manual
Eli-v6.2.20

Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

1 Introduction **9**

1.1 Overview . . . 9

1.2 Manual Layout . . . 10

1.3 Definitions . . . 10

1.3.1 iSCSI Target Device . . . 10

1.3.2 iSCSI Qualified Name (IQN) . . . 10

1.3.3 iSCSI Challenge Handshake Authentication Protocol (CHAP) . . . 10

1.3.4 Logical Unit Number (LUN) . . . 11

1.3.5 Node . . . 11

1.3.6 Target Device . . . 11

1.3.7 Initiator Device . . . 11

1.3.8 Initiator Port . . . 11

1.3.9 Target Port . . . 11

2 Using the Web Interface **12**

2.1 Browsers . . . 12

2.2 Connecting to the Web Interface . . . 12

2.3 Network Setup via CLI . . . 14

2.4 Management Console (Home screen) . . . 17

3 Node Configuration **18**

3.1 Network Connections . . . 18

3.1.1 Network Interfaces . . . 19

3.1.2 General Settings . . . 19

3.1.2.1 Hostname . . . 19

3.1.2.2 Hostname on login page . . . 20

3.1.2.3 DNS Servers . . . 20

3.1.2.4 Default Route . . . 20

3.1.2.5 Dead Gateway Detection 20
3.1.2.6 Enable IPv6 22
3.1.3 Interface Statistics 22
3.1.3.1 Data Transmission Rate 23
3.1.3.2 Data Reception Rate 23
3.1.3.3 Legend 24
3.1.4 Network Routing 24
3.1.4.1 Add Static Route 24
3.1.5 Network Tools 25
3.1.5.1 Ping 26
3.1.5.2 Traceroute 27
3.1.6 Port Settings 28
3.1.6.1 Enable Port 29
3.1.6.2 Setting the MTU 29
3.1.6.3 Setting the IP Address 29
3.1.6.4 Committing the Changes 30
3.2 Passwords & Security 30
3.2.1 System Password 32
3.2.2 Password Reset Options 32
3.2.2.1 Password Reset via Email 32
3.2.2.1.1 Setup 32
3.2.2.1.2 Using Password Reset via Email 33
3.2.2.2 Password Reset via Local Console or SSH 34
3.2.2.2.1 Setup 34
3.2.2.2.2 Using Password Reset via Local Console or SSH 35
3.2.3 Secure Connection 37
3.2.3.1 Generate new Certificate Signing Request 38
3.2.4 User Settings 38
3.2.4.1 Session Timeout 39
3.2.4.2 Unit Display Format 39

3.2.5 Secure Shell (SSH) . . . 39
3.2.5.1 Managing Public Keys . . . 39
3.2.5.2 Using SSH . . . 40
3.3 Service Control . . . 41
3.3.1 Network Time Protocol (NTP) . . . 42
3.3.2 Simple Network Management Protocol (SNMP) . . . 43
3.3.2.1 System Information . . . 44
3.3.2.2 SNMP Trap Sinks . . . 44
3.3.2.3 Add SNMP Trap Sink . . . 44
3.3.2.4 Download MIB Files . . . 45
3.3.3 Email . . . 46
3.3.4 Event Notification Email . . . 47
3.3.5 Internet Storage Name Service (iSNS) . . . 47

4 WANrockIT Configuration 48

4.1 Node Management . . . 48
4.1.1 Remote Nodes . . . 49
4.1.1.1 Configured Nodes . . . 51
4.1.1.2 Non-Configured Nodes . . . 51
4.1.2 Add Remote Node . . . 51
4.1.3 Transfer Statistics . . . 52
4.1.3.1 Data Transfer Rate . . . 54
4.1.3.2 Download 24 Hour Transfer History . . . 54
4.1.4 Access Control . . . 54
4.1.4.1 Remote Administration . . . 55
4.1.4.2 Whitelist . . . 55
4.1.5 IPsec . . . 55
4.1.5.1 Enabling IPsec service . . . 56
4.1.5.2 Encrypting Accelerated Traffic . . . 56
4.1.5.3 Adding a PSK (Pre-Shared Key) . . . 57

4.2 WANrockIT Node Page 57
4.2.1 Node Status 58
4.2.2 Node Configuration 59
4.2.3 Applications & Utilities 59
4.2.4 Path Configuration 59
4.2.4.1 Setting Primary and Failover Paths 60
4.2.4.2 Filtering options 61
4.2.4.3 Configuring a Node's Bandwidth 61
4.2.5 Node Specific Transfer Statistics 62
4.2.5.1 Data Transfer Rate 62
4.2.5.2 Download 24 Hour Transfer History 63
4.2.6 Remove Node 63
4.2.7 Remote Control 64
4.2.8 Learn 65
4.2.8.1 Data Transfer Rate 67
4.2.9 SCSI Devices 67
4.2.9.1 Restoring of Devices 68
4.2.9.2 Disabling a Device 69
4.2.9.3 Enabling a Device 69
4.2.9.4 Refreshing SCSI Devices from a Remote Node 69

5 SAS Initiator 71

5.1 SAS Initiator Page 72
5.1.1 Hosts 72
5.1.2 Expanders 73
5.1.3 Display Options 73
5.2 Phy Status Page 74

6 Fibre Channel Initiator Connections 75

7 Fibre Channel Target Connections 79

7.1 Port Configuration 80
7.2 Connected Hosts 81
7.3 Port Map 82
7.3.1 Automatic 83
7.3.2 Manual 84

8 Fibre Channel Port Configuration 86

9 iSCSI Initiator Configuration 87
9.1 Discovering an iSCSI Target 87
9.2 Removing an iSCSI Discovery Portal 90
9.3 Log On to an iSCSI Target 90
9.3.1 Persistent Connection 91
9.3.2 CRC/Checksum 91
9.3.3 CHAP Login 92
9.4 Log Off an iSCSI Session 92
9.5 Refresh Targets 92
9.6 Remove Persistent Target 92

10 iSCSI Target Configuration 93
10.1 Authorisation (CHAP) 93
10.2 Network Interfaces 94
10.3 iSCSI Sessions 94

11 SCSI Device Management 96
11.1 Viewing Attached Devices 96

12 Port Mappings 98
12.1 Setting Port Mappings 99
12.2 Removing a Port Mapping 99
12.3 Saving Port Mappings 99
12.4 Available Port Mappings 99

13 Node Maintenance **101**

13.1 System Information . . . 101

13.2 System Log . . . 102

13.3 Load/Save Configuration . . . 103

13.3.1 Loading a Saved Configuration . . . 104

13.3.2 Saving the Configuration to Disk . . . 104

13.3.3 Restoring to Factory Defaults . . . 105

13.4 Firmware Updates . . . 105

13.4.1 Automatic Firmware Update Checking . . . 106

13.4.2 Updating Firmware Manually . . . 107

13.5 Licence Key Management . . . 108

13.5.1 Uploading a Licence Key . . . 109

13.5.2 Removing a Licence Key . . . 110

13.5.3 Downloading a Licence Key . . . 110

13.6 Diagnostics . . . 110

13.7 Task Scheduler . . . 111

13.7.1 Adding Tasks . . . 112

13.7.2 Removing/Editing Tasks . . . 112

13.7.3 Task Wizard . . . 114

13.7.3.1 Action - Email Performance Statistics . . . 114

13.7.3.2 Action - WANrockIT Bandwidth Limit . . . 115

13.7.3.3 Trigger . . . 116

13.7.3.4 Start Date . . . 117

13.7.3.5 End Date . . . 117

13.7.3.6 Summary . . . 118

14 Troubleshooting **119**

14.1 Network Connectivity Problems . . . 119

14.2 SCSI Device Related Problems . . . 119

14.3 Network Performance Problems . . . 120

14.4 iSCSI Performance Problems . . . 121
14.5 Recovery Wizard . . . 121
14.5.1 Factory Restore . . . 122
14.5.2 Delete Configuration . . . 124

Appendix A IP Protocols and Port Numbers 127
A.1 Inbound LAN Protocols and Port Numbers . . . 127
A.2 Outbound LAN Protocols and Port Numbers . . . 127
A.3 WAN Protocols and Port Numbers . . . 128

Appendix B Accessing the Node from Windows using a static IP Address 129

Appendix C Connecting to an iSCSI Device using the Microsoft iSCSI Initiator 133
C.1 General Set up . . . 133
C.2 Discovery of Devices . . . 135
C.2.1 Adding an iSCSI Target Portal . . . 136
C.2.2 Adding an iSNS Server . . . 140
C.3 Connecting to a Target . . . 142
C.4 Viewing iSCSI Session Details . . . 146
C.5 Creating Multiple Connections (Optional) . . . 148
C.6 Logging off an iSCSI Session . . . 154

Appendix D Connecting to an iSCSI Device using iscsiadm 156
D.1 Discovering iSCSI Targets . . . 156
D.2 Logging into a target . . . 157
D.3 Logging out of a target . . . 159
D.4 Logging out of all targets . . . 160

Appendix E WANrockIT Series Comparisons 161
E.1 Node Limits . . . 161

Appendix F Transfer Statistics Graphing Instructions for Excel 2010 162

Appendix G Useful Links **173**

1 Introduction

Thank you for purchasing the Bridgeworks WANrockIT Node.

The WANrockIT Node has been designed to ensure that in the majority of installations it will require minimal setup before use. However, we suggest you read the following section which will guide you through setting up your Node.

This Manual contains information for setting up all feature cards that may be installed in your WANrockIT Node. Therefore, some sections may refer to a feature card that may not be installed in your particular Node.

1.1 Overview

Bridgeworks latency mitigating technology allows you to accelerate your network traffic between two different sites. These sites may include data centres and your business centres. Each site will require a WANrockIT Node to accelerate your desired traffic. WANrockIT can only be physical hardware appliances.

The WANrockIT product range supports all major SCSI storage interfaces such as Fibre Channel, iSCSI and SAS.

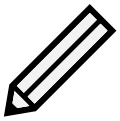
Each Node's storage interface can be configured to act either as a target interface—working in a similar mode to a storage device, or as an initiator—working in a similar mode to a server. Or, if the WANrockIT Node has multiple storage interfaces, one can be configured to be an initiator and one as a target device.

A unique part of WANrockIT functionality is that all the Nodes within a WANrockIT installation do not have to have the same storage interface.

A typical configuration is shown in the image below, where traffic from a server on site A is accelerated over a WAN link to site B.

1.2 Manual Layout

Throughout the manual, symbols will be used to quickly identify different pieces of information.

	This icon represents a note of interest about a step or section of information.
	This icon represents an important piece of information.
	This icon represents a warning. Care must be taken and the warning should be read thoroughly.

1.3 Definitions

Throughout this manual, selected terms will be used to describe pieces of equipment and concepts. This section provides an explanation of those terms.

1.3.1 iSCSI Target Device

iSCSI target devices are devices such as disk drives, tape drives or RAID controllers that are attached to the network. Each device is identified by an IQN (iSCSI Qualified Name).

1.3.2 iSCSI Qualified Name (IQN)

Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed. This is called the IQN. The IQN includes the iSCSI Target's name and an identifier for the shared iSCSI device.
Example: 2002-12.com.4bridgeworks.sdt600a014d10:5

1.3.3 iSCSI Challenge Handshake Authentication Protocol (CHAP)

CHAP is an authentication scheme used by iSCSI to validate the identity of iSCSI targets and initiators. When CHAP is enabled, the initiator must send the correct username and target password to gain access to the iSCSI target.

Optionally the initiator can request that the target authenticates itself to the initiator; this is called mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI target will authenticate itself with the initiator using the initiator secret.

1.3.4 Logical Unit Number (LUN)

Each device in a SCSI storage system can support multiple sub-devices; these Logical Units (LU) are indexed by numbers called Logical Unit Numbers (LUN). Within the iSCSI Connect Bridge each SCSI ID on the SCSI bus can support 7 LUNs.

1.3.5 Node

A Node refers to a WANrockIT unit.

1.3.6 Target Device

A device that services storage and management commands, sending responses to those commands. For example disk or tape drives.

1.3.7 Initiator Device

A computer or other piece of equipment, which sends storage and management commands to one or more target devices.

1.3.8 Initiator Port

The port or interface on an initiator device through which commands are transmitted and responses received.

1.3.9 Target Port

The port or interface on a target device through which commands are received and responses transmitted.

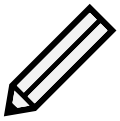
2 Using the Web Interface

The primary method for configuring any option is through the web interface. The following section highlights the requirements needed to access the web interface of the Node.

2.1 Browsers

This Node supports the following browsers:

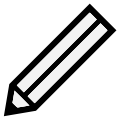
- Microsoft Edge[1]
- Mozilla Firefox[1]
- Google Chrome[1]



Note: JavaScript must be enabled within the web browser to use the web interface.

Important: If you choose to use a browser that is not in the list of supported browsers, Bridgeworks cannot guarantee the behaviour of the Node's functionality.

2.2 Connecting to the Web Interface



Note:

- DHCP is enabled by default on the management interface.
- The default hostname is `bridgeworks`.

For help locating management interfaces on hardware appliances, please refer to your hardware manual.

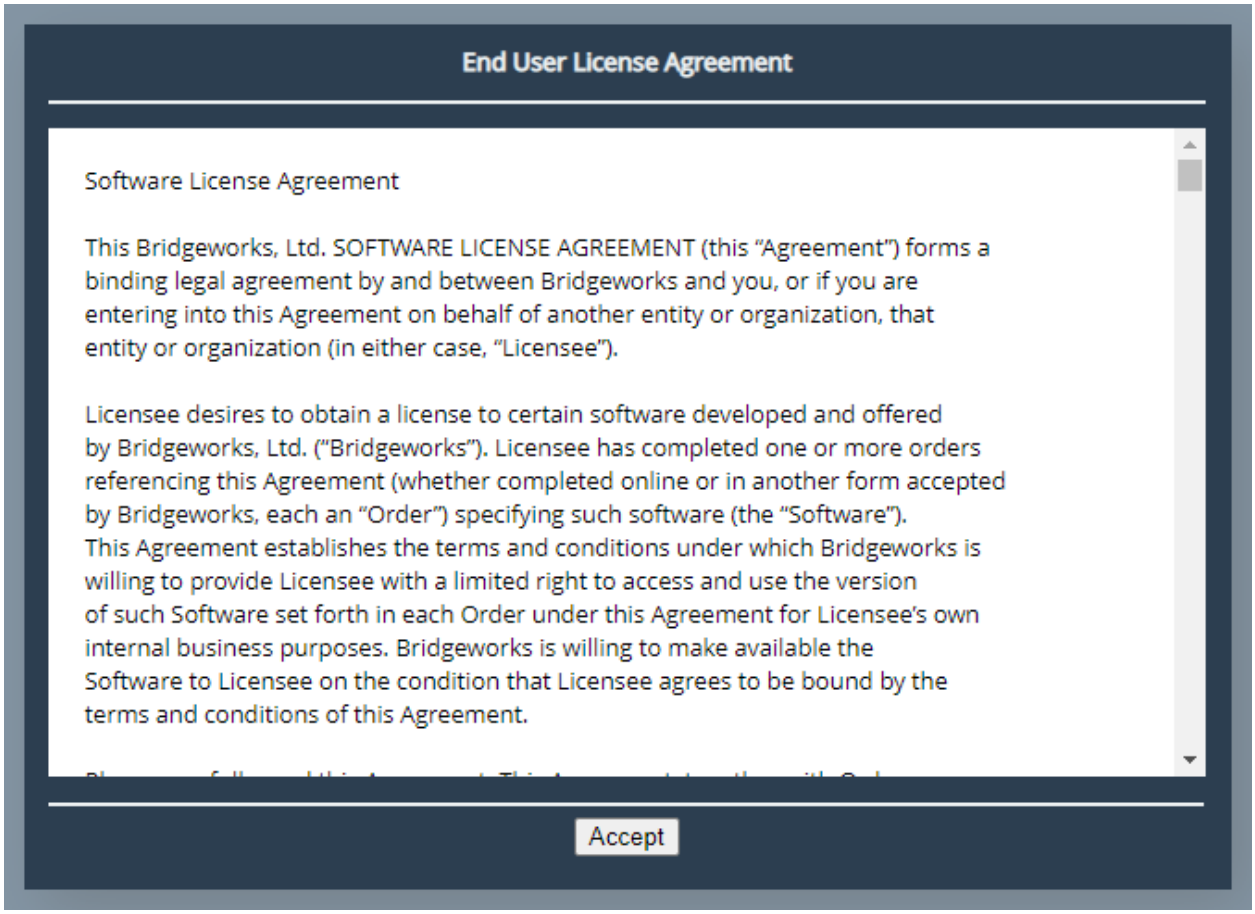
If the Node is successfully connected to your DHCP server, and DNS resolution is enabled on your network by default, you can access the Node's web interface from the default hostname by navigating to: `http://bridgeworks/`

Important: Your host will likely need to be directly-connected to the Node if DHCP is not enabled, and its subnet set appropriately. See Appendix B: Accessing the Node from Windows using a static IP Address for help with accessing the Node web interface without DHCP.

[1] Latest version as of release

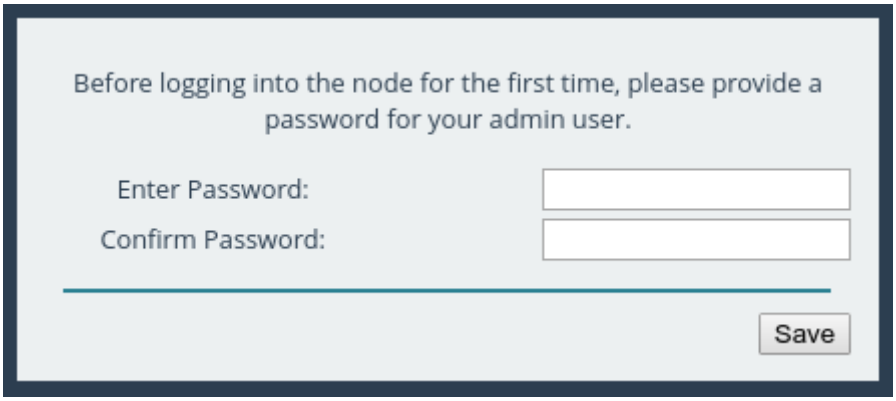
From within your web browser, connect to the Node's web interface using default hostname or IP address of a connected management interface.

Once you have connected to the web interface on the Node you will be provided with the Bridgeworks End User License Agreement (EULA) which must be accepted before you are able to access the Node. Ensure you read this agreement thoroughly. To proceed, you must accept the agreement by clicking the *Accept* button.

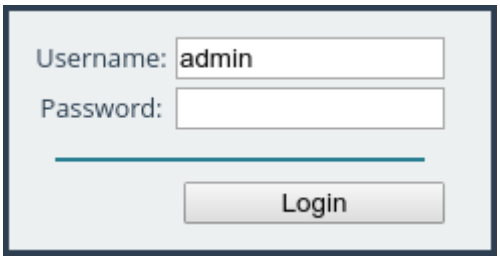


	Important: If you accepted the Bridgeworks EULA during the deployment of your Node, you will not need to accept it again.

You will then see the entry page shown below:



Enter and confirm the new web interface password to be presented with the login screen. The password must be between 5 and 64 characters and should contain both symbols and numbers.



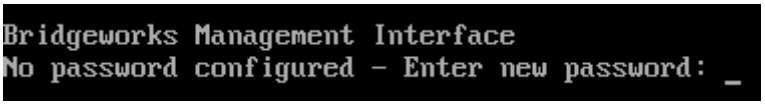
To access the web interface a username and password must be used. The default username is *admin*.

2.3 Network Setup via CLI

If you are initially unable to access the web interface, you may need to perform some initial setup via the CLI.

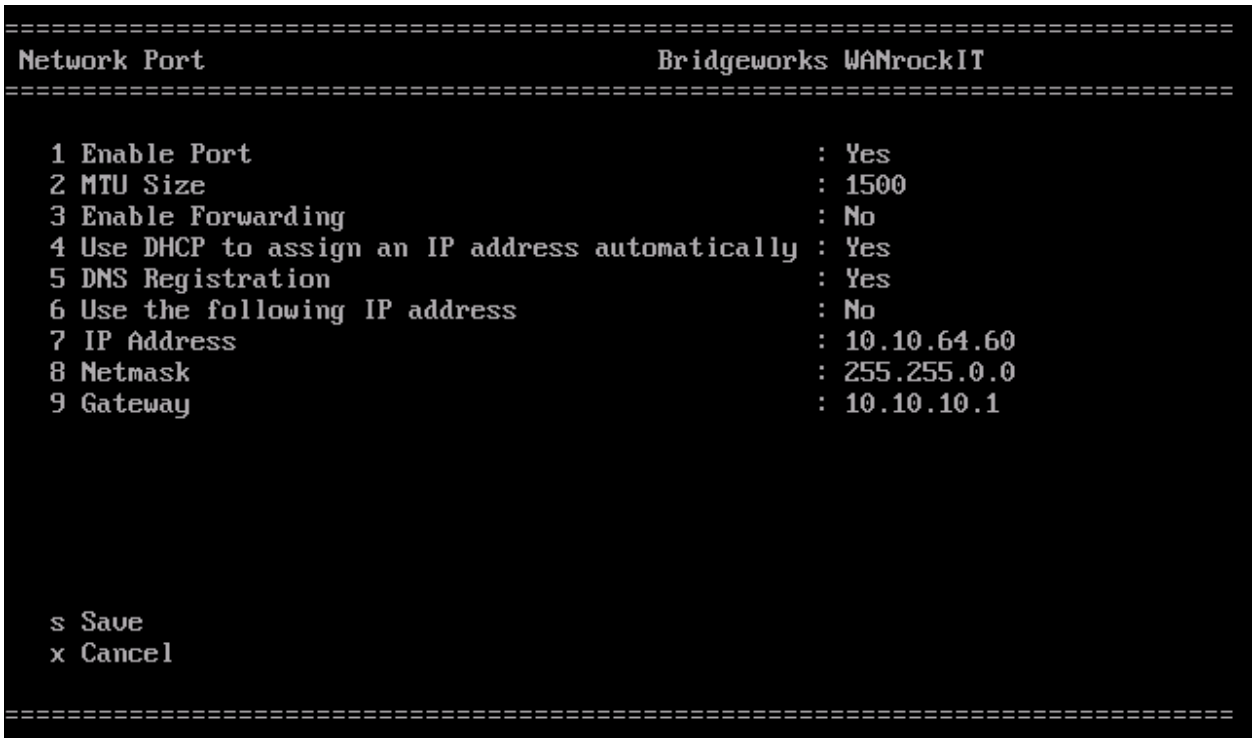
On the Node's interface, press Alt+F2 to enter the CLI.

If this is your first time logging into the Node, you will have to set a password.



You can now log into the Node using the default username *admin*, and the password you set.

Within the CLI, you can select an option by entering the number next to it. Navigate to *Network Connections* using *1*, then select the port you will be using to manage your Node.



Ensure this port is enabled by checking the *Enable Port* option. If this says *No* next to it, select it, then press *y* to enable it.

DHCP will be enabled by default. If you need to set a static IP address for your Node, select *Use the following IP address*.

Next, set your IP address by selecting *IP Address* and entering a valid IPv4 address. You may also need to adjust the netmask and default gateway.

When you are done modifying your port settings, press *s* to save.

If you need to set your default route, you can navigate to *Network Connections*, then *General Settings*, then *Default Route*, and select the port you configured. Then press *s* again to save.

Once you have saved all your settings, press *r* to reboot your Node to apply them.

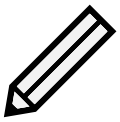
Once the Node has finished rebooting, you should see the status screen. If the port is working, you should see an IP address, and *UP*.

If you want to return to this screen without rebooting, you can do so with Alt+F1.

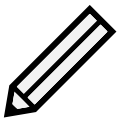
Once your port is set up correctly, you should be able to access the Node via a web browser as described in Section 2.2: Connecting to the Web Interface.

2.4 Management Console (Home screen)

The web interface will now display the Console Home screen as shown below:

	Note: The web interface may have different icons to the ones shown above depending on the configuration you have purchased.

The web interface is split into two sections. The left hand *Node Menu* panel typically remains constant wherever you are within the web interface. It allows you to reboot or logout of the web interface. The Home link may be used from any page to return to the Home screen.

	Note: Whenever a Reboot command is issued, it may take several minutes for the Node to become accessible again.

The Support link will open up a new tab in your browser at the Bridgeworks website support page.

The Help will provide you with information relevant to the display and configuration data.

3 Node Configuration

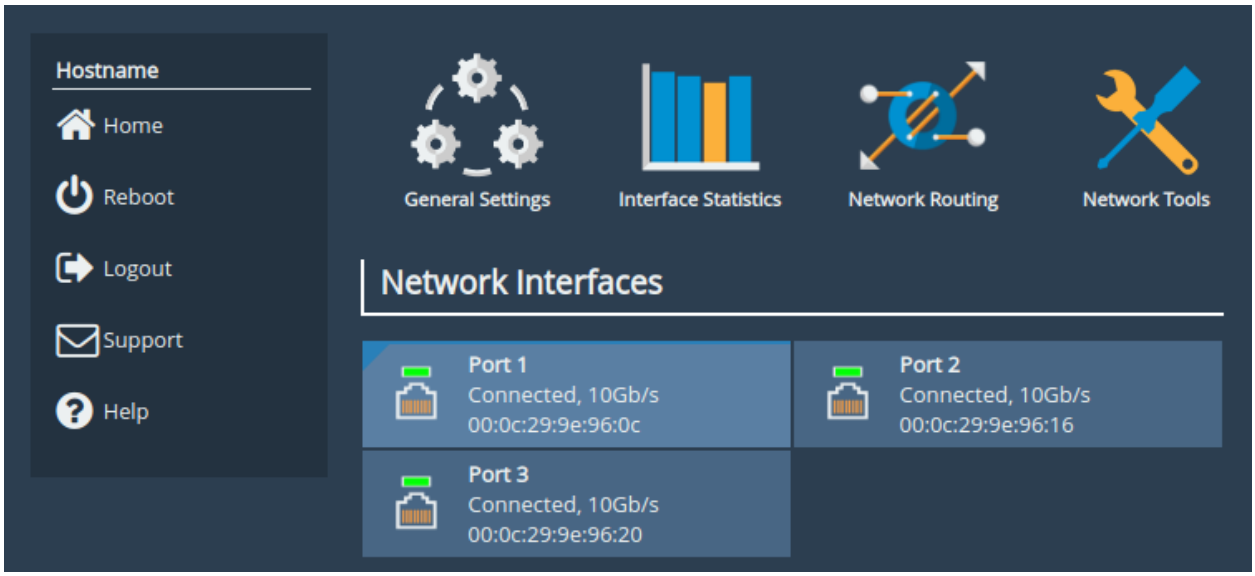
This section details the configuration of the Node's basic network and service settings.

3.1 Network Connections

This configuration page allows the administrator to configure network interface settings and view network statistics.

From the Home screen, select the *Network Connections* icon under the *Node Configuration* section.

The web interface will display the following:



Options at the top of the page allow you to access various network settings and tools. More information for these options can be found in the following sections:

- Section 3.1.2: General Settings
- Section 3.1.3: Interface Statistics
- Section 3.1.4: Network Routing
- Section 3.1.5: Network Tools

3.1.1 Network Interfaces

This section displays each network port present on the Node, along with its current status/link speed, and hardware identifier (MAC address).

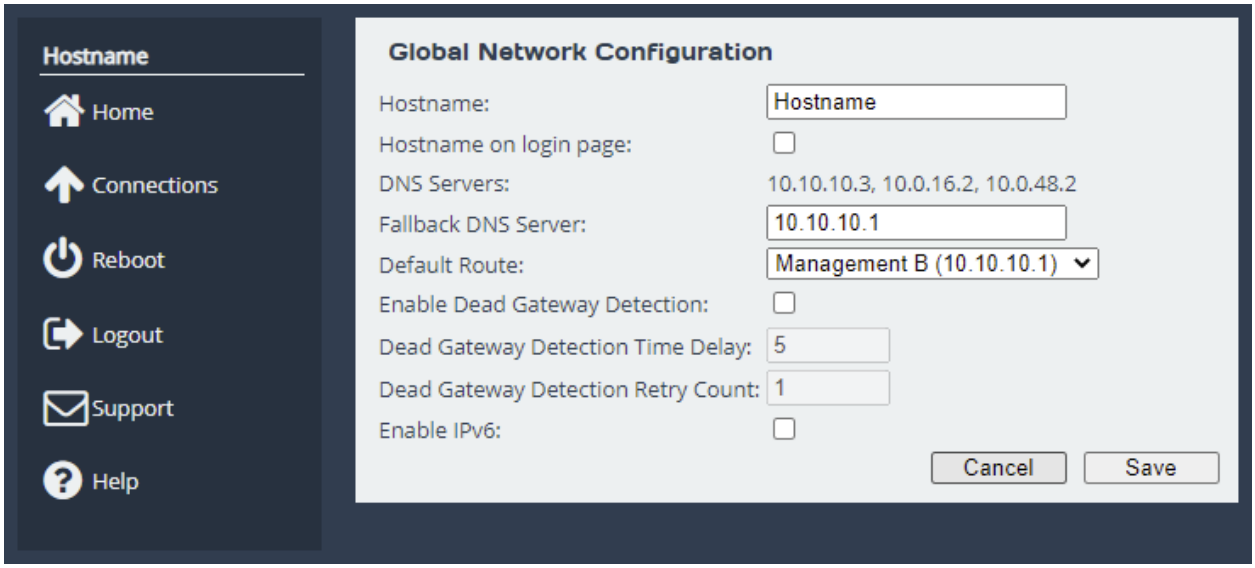
Clicking on a particular interface will navigate to a bespoke configuration page for that particular interface. More information on the different interface settings is available in Section 3.1.6: Port Settings.

3.1.2 General Settings

This configuration page allows the administrator to configure general network settings for the Node.

From the *Network Connections* page, select the *General Settings* icon.

When selected, you will be presented with the following screen.



3.1.2.1 Hostname

In the *Hostname* field, enter the name you wish to use to address this Node. It is a good idea to make the name relevant to the Node's location and/or purpose.

You can then access the web interface from this hostname in future, from any DHCP-enabled management interface.

3.1.2.2 Hostname on login page

Selecting the *Hostname on login page* checkbox enables the display of the system hostname, and if available the DHCP domain name on the login page. This may be useful to identify which device you are logging in to.

3.1.2.3 DNS Servers

Setting a DNS server enables the use of DNS names when configuring network services.

The *DNS Servers* field lists the DNS servers that are currently in use by the Node. If DHCP is enabled on an interface and returns DNS servers, then these will be displayed in the list, otherwise the *Fallback DNS Server* will be used.

3.1.2.4 Default Route

The *Default Route* is the interface that the Node will use to route packets when no specific interface has been specified.

Important: The selected interface must have a gateway configured for this to take effect.

In addition to being able to select a specific interface for the *Default Route* it is also possible to select the interface automatically with the *Auto* option. In this case an interface which has both *Management* mapped to it and a default gateway configured will be set as the default route. This operation is performed at startup only.

If the user requires no *Default Route* it is possible to set *None*. Factory default value for this setting is *Auto*.

3.1.2.5 Dead Gateway Detection

Selecting the *Enable Dead Gateway Detection* checkbox will allow the Node to detect dead gateways and remove network routes that specify those gateways. When the dead gateways are reachable again, the routes are restored. This provides a level of failover in the event that the gateways become unreachable.

Dead Gateway Detection Time Delay refers to the time in seconds between requests being sent to the gateway to see whether that gateway is still reachable.

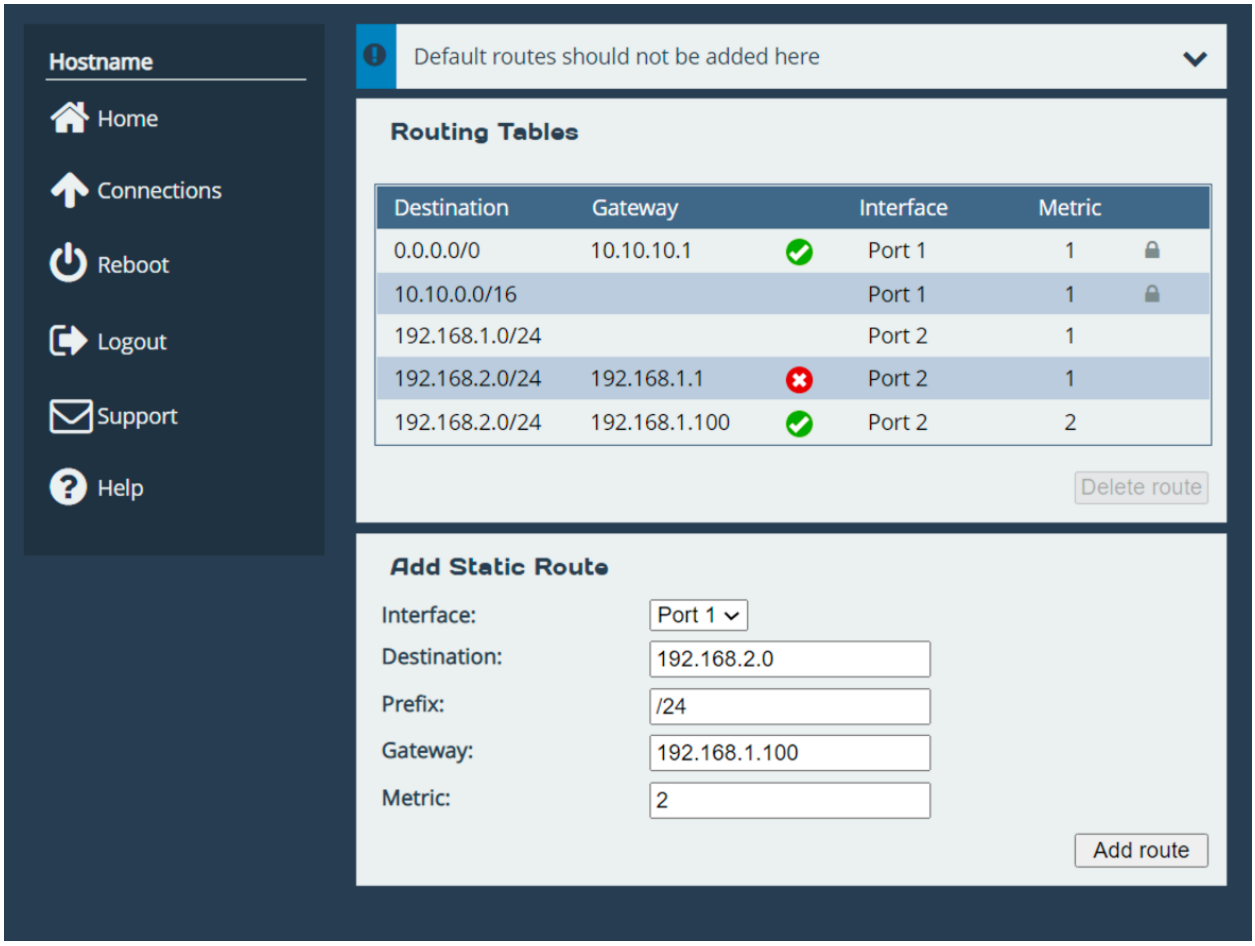
Dead Gateway Detection Retry Count refers to the number of times an unreachable gateway will be contacted before being set as a dead gateway and removed.

The status of each gateway is displayed on the *Routing* page. The status of the gateways for an individual port are also shown on the *Port Settings* pages. Refer to Section 3.1.4: Network Routing for information on viewing and modifying network routes. An icon next to each gateway indicates its state:

Live Gateway Represents a gateway that responds to ICMP echo

Dead Gateway Represents a gateway that no longer responds to ICMP echo requests; it is dead

Important: Dead gateway detection functions by sending periodic ICMP echo requests to each gateway. Please ensure that the gateways can respond to such requests; if they're blocked by a firewall, dead gateway detection will always consider the gateways to be dead.



In this example, dead gateway detection has been enabled and multiple redundant routes to `192.168.2.0/24` have been added with different gateways (`192.168.1.1` and `192.168.1.100`) and different metrics (`1` and `2`, respectively).

The gateway with the IP address of `192.168.1.1` isn't responding to ICMP echo requests, so it's deemed to be dead. The corresponding route has been removed, so any traffic to `192.168.2.0/24` will now go via `192.168.1.100` instead.

When the gateway with the IP address of
`192.168.1.1` starts to respond to ICMP echo requests again, the icon next to it will change from the red cross to the green tick and its route will be restored. Any traffic to `192.168.2.0/24` will go via `192.168.1.1`.

3.1.2.6 Enable IPv6

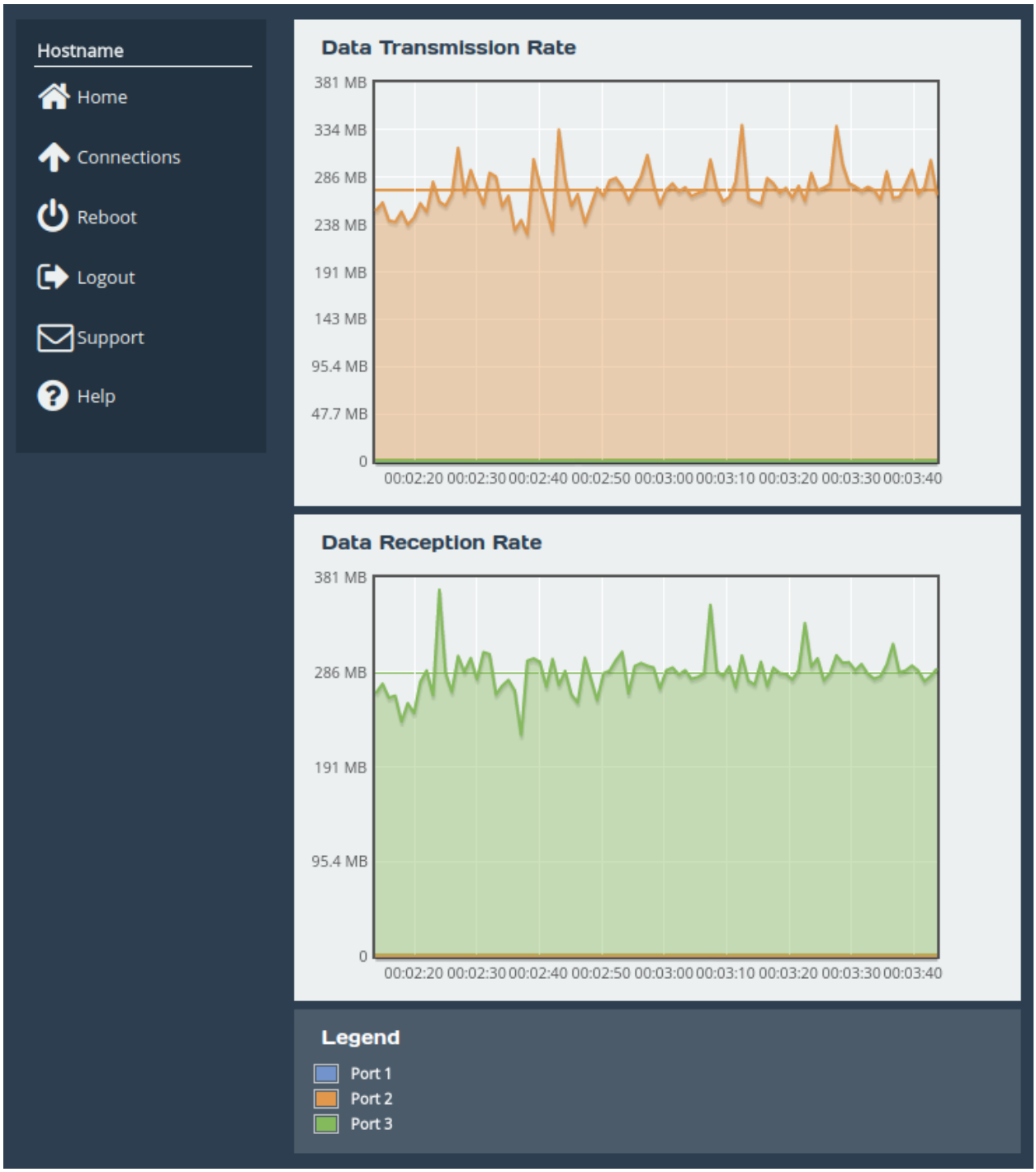
Selecting the *Enable IPv6* checkbox will enable the Node to use IPv6 addresses. As with IPv4, you can either choose automatic address assignment or assign a static IPv6 address.

3.1.3 Interface Statistics

This page displays live network interface data rate statistics.

From the *Network Connections* page, select the *Interface Statistics* icon.

When selected, you will be presented with the following screen.



3.1.3.1 Data Transmission Rate

This section displays a graph, representing the data transmission rate for each network interface over the last 90 seconds. Each interface is displayed using a unique colour specified in the *Legend*. The average transmission rate over the last 90 seconds is displayed by a horizontal line for each interface.

3.1.3.2 Data Reception Rate

This section displays a graph, representing the data reception rate for each network interface over the last 90 seconds. Each interface is displayed using a unique colour specified in the *Legend*. The

average reception rate over the last 90 seconds is displayed by a horizontal line for each interface.

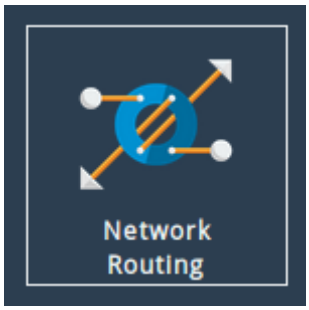
3.1.3.3 Legend

Each base network interface will be displayed using a unique colour for the data rate graphs. Each interfaces colour will be displayed alongside the ports name here.

3.1.4 Network Routing

This configuration page allows the administrator to view the network routes currently active on the Node. Routes can also be added or removed on this page.

From the *Network Connections* page, select the *Network Routing* icon.



3.1.4.1 Add Static Route

To add a route, fill in the following fields and click on the *Add route* button:

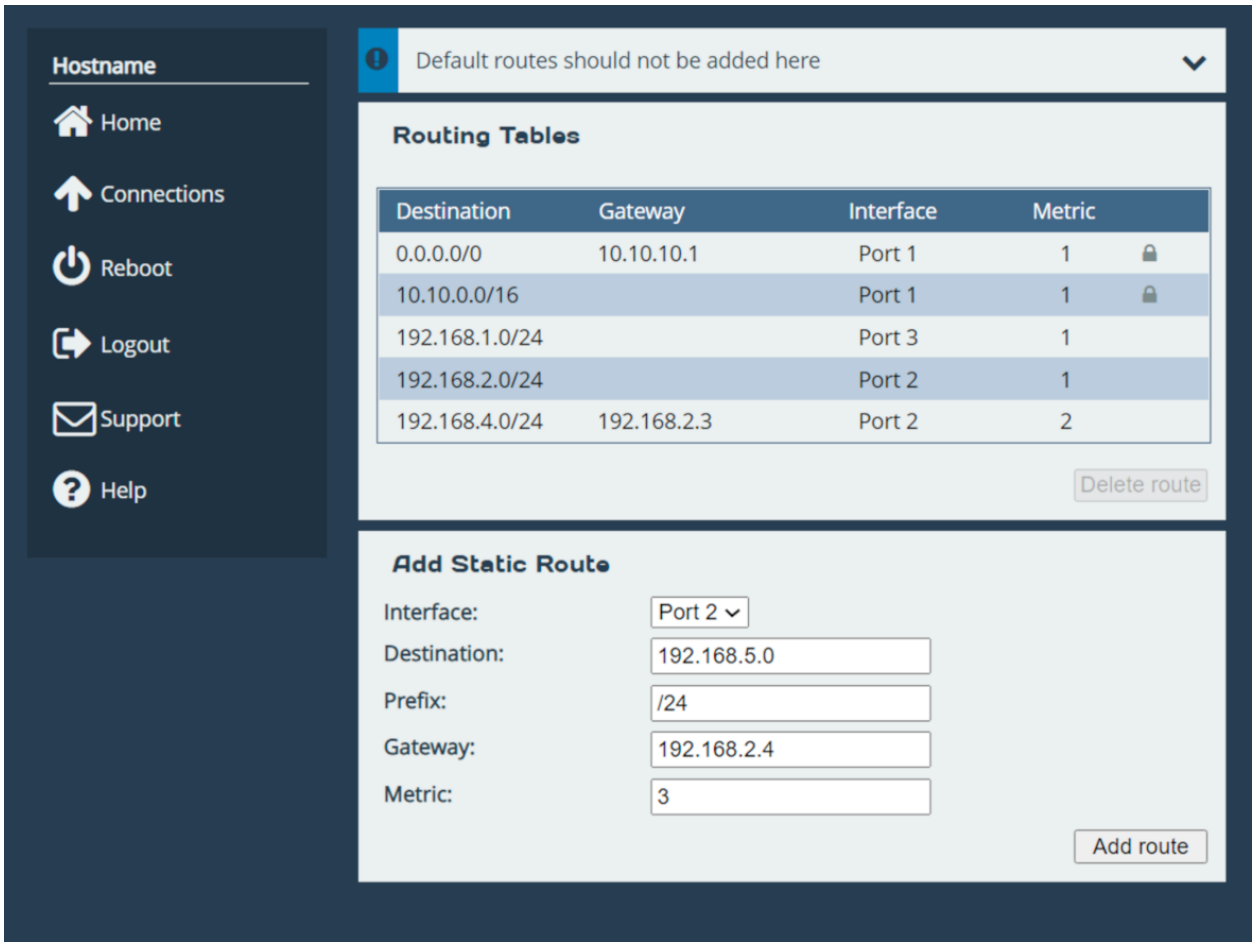
Interface The network interface to which the route applies.

Destination The IP address component of the CIDR block to which the route applies, e.g. `192.168.5.0`.

Prefix The prefix length component of the CIDR block to which the route applies, e.g. `/24`.

Gateway Route traffic via the gateway with this IP address. Optional.

Metric Metric (priority) of the route. Optional; defaults to `1`.



In this example, a route is being added to `192.168.5.0/24` via the gateway at `192.168.2.4` on Port 2. The route has a metric of `3`.

To remove an existing route, click on the *Delete* button next to it.

	Important: Routes created automatically by the system cannot be removed.

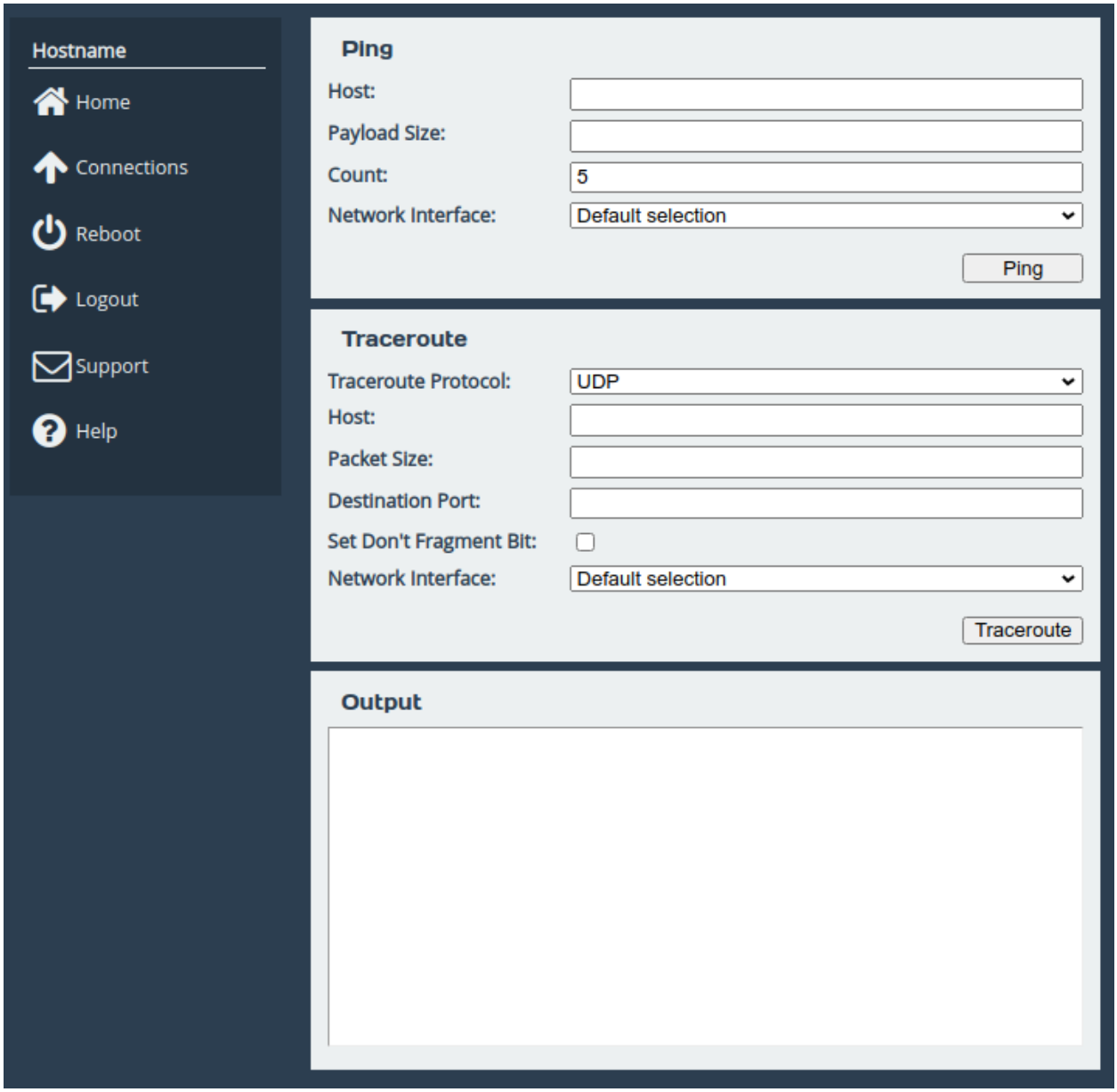
When dead gateway detection is enabled, each gateway in the table will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.2.5: Dead Gateway Detection for more information.

3.1.5 Network Tools

The WANrockIT product provides some network tools that can be used for verifying network connectivity and behaviour between the Node and network hosts.

From the *Network Connections* page, select the *Network Tools* icon.

When selected, you will be presented with the following screen.



3.1.5.1 Ping

Ping can be used to verify the connectivity between the Node and a network host.

To test connectivity, fill in the following fields and click on the *Ping* button:

Host The IP address of the network host.

Payload Size The ping payload size. Leave blank to default to 56 bytes.

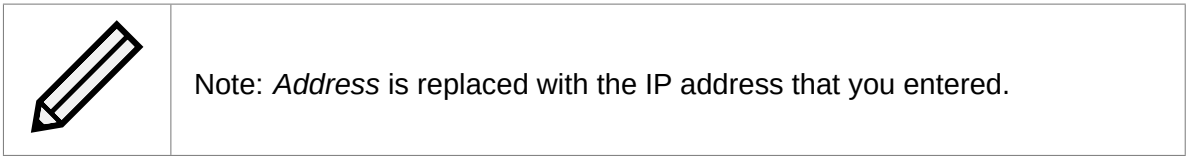
Count The number of ping attempts that you wish the Node to perform. Setting the count to 0 will send pings indefinitely, until the page is navigated away from, or another ping/traceroute operation is initiated.

Network Interface The interface that you want to ping from. If you are checking the routing on the unit, leave this option set to

On a successful ping, the *Output* box will fill with text similar to that below.

```
PING Address (Address): 56 data bytes
64 bytes from Address: seq=0 ttl=64 time=0.600 ms
64 bytes from Address: seq=1 ttl=64 time=0.129 ms
64 bytes from Address: seq=2 ttl=64 time=0.096 ms
64 bytes from Address: seq=3 ttl=64 time=0.143 ms
64 bytes from Address: seq=4 ttl=64 time=0.094 ms

--- Address ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.094/0.212/0.600 ms
```



3.1.5.2 Traceroute

Traceroute can be used to determine the route packets take from the Node to a network host.

To test the routing, fill in the following fields and click on the *Traceroute* button:

Traceroute Protocol The type of protocol you wish to use: UDP, ICMP or TCP. UDP is the default option, ICMP can be used if firewalls block UDP datagrams. TCP is useful for testing access lists and firewall protocol rules.

Host The IP address of the network host.

Packet Size The traceroute payload size. Leave blank to default to 46 bytes for IPv4 or 72 bytes for IPv6.

Destination Port The destination port can be selected. This may be useful, alongside TCP probes, when testing policy based routing; or for testing specific ports, especially Dynamic Ports (also known as Private or Ephemeral Ports). It is disabled when using ICMP.

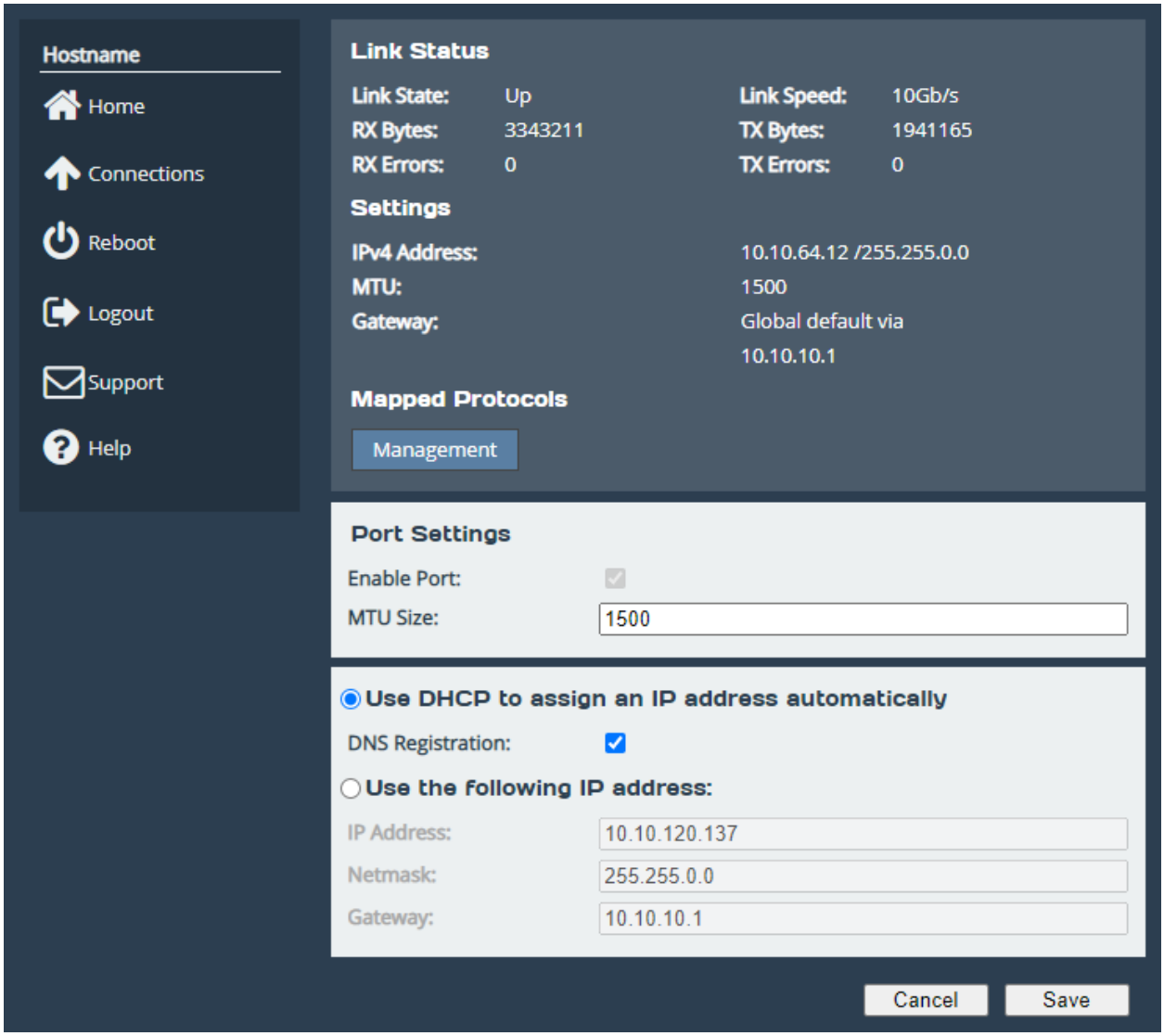
Set Don't Fragment Bit Select to set the don't fragment (DF) bit on the traceroute packets. This can be used to diagnose MTU issues on your network.

Network Interface The interface that traceroute packets will be sent from. Leave as *Default selection* for the interface to be selected according to the routing table.

The result from traceroute will appear in the *Output* box.

3.1.6 Port Settings

Clicking on an interface will navigate to a bespoke settings page for that particular interface. Depending on the type of interface that was selected and the current options that are enabled, different settings will be presented.



When dead gateway detection is enabled, each gateway on the port will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.2.5: Dead Gateway Detection for more information.

Important: IPv6 Options will only be displayed if IPv6 has been enabled (see Section 3.1.2: General Settings).

3.1.6.1 Enable Port

An interface may be enabled or disabled by toggling this option.

3.1.6.2 Setting the MTU

The maximum transmission unit (MTU) may be adjusted from the default of 1500 bytes. Lower values are sometimes required for best performance with some types of network VPN equipment. However it is recommended to leave this value unchanged, unless advised by documentation for any external VPN equipment used in conjunction with the Node.

Enabling larger frames on a jumbo frame-capable network can improve your network throughput. Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU).

Before enabling jumbo frames, ensure that all the devices/hosts located on the network support the jumbo frame size that you intend to use to communicate with the Node. If you experience network-related problems while using jumbo frames, use a smaller jumbo frame size. Consult your networking equipment documentation for additional instructions.

Important: Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches it might be required to add the necessary bytes needed for the frame header to the MTU size you specify in the Node's port configuration. Typical header size is 28 bytes, so a 9000 byte MTU could translate to a 9028-byte total size. Refer to your switch documentation to understand what the maximum frame size settings are for your switch.

3.1.6.3 Setting the IP Address

There are two possibilities when configuring the IP address of a network port:

DHCP The Node will seek out your network's DHCP server and obtain an IP address for this port each time it boots.

If the server is not found, this port will fall back to its saved static IP settings.

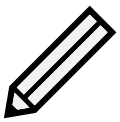
When DHCP is selected the option to register the system's hostname with DNS is made available, this is enabled by default on management interfaces.

Static IP The IP address, netmask and gateway set in the corresponding fields will be used for this port.

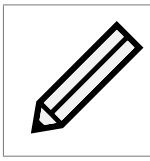
The gateway field may be left blank.

The IPv4 netmask field must be specified in dot-decimal form, e.g. `255.255.255.0`.

If IPv6 is enabled from the *Network Connections* page, you can choose to use automatic address assignment to assign an IPv6 address, or you can set a static IPv6 address.



Note: DHCP is enabled by default on management interfaces.

	Note: If DHCP is enabled, we recommend that your DHCP server is set to automatically update the DNS server.

3.1.6.4 Committing the Changes

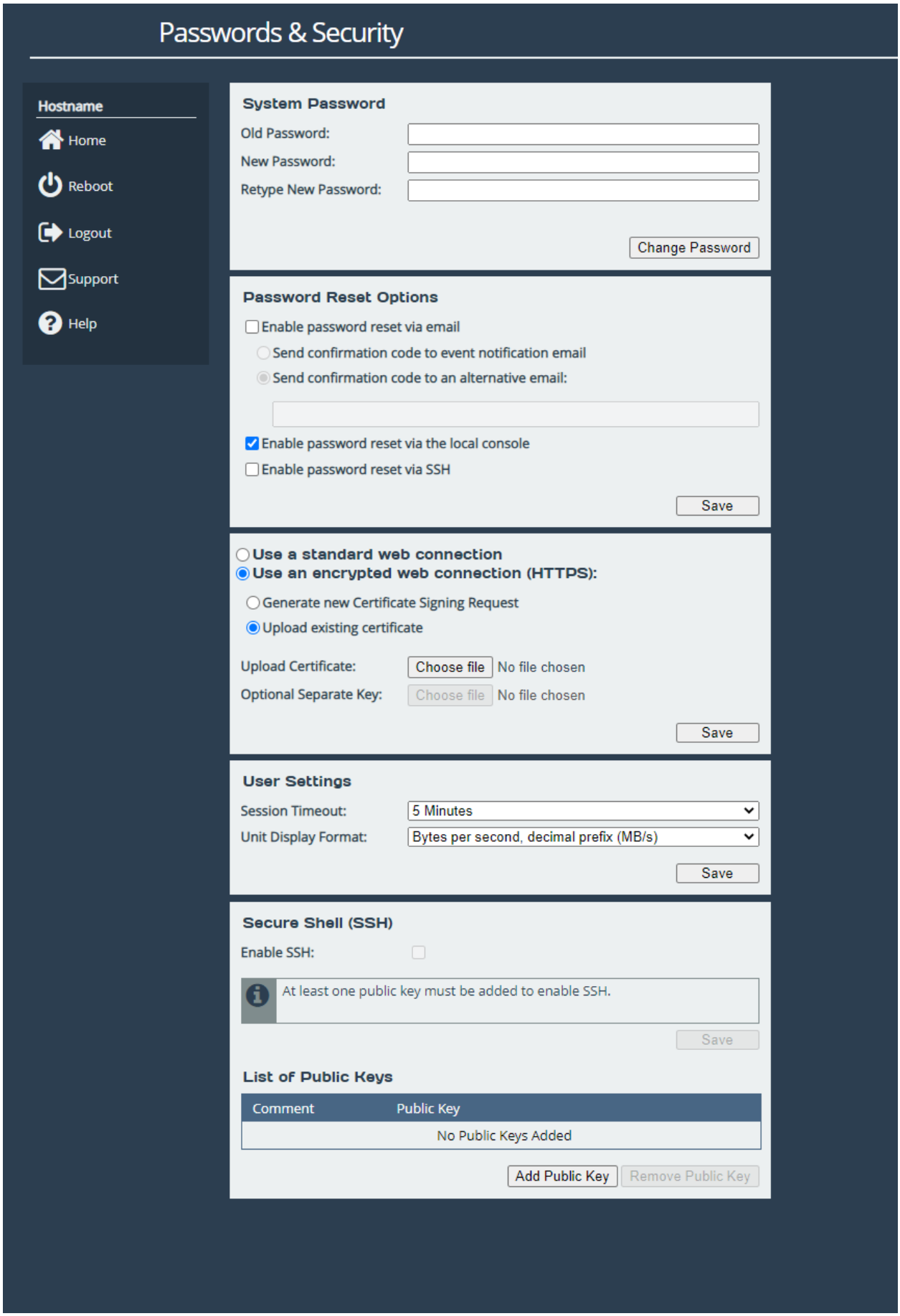
Click the *Save* button to save these parameters, then reboot the Node to apply them.

3.2 Passwords & Security

This configuration page allows the administrator to change the security settings of the Node.

From the Home screen, select the *Passwords & Security* icon under the *Node Configuration* section.

The web interface will display the following:


Passwords & Security
Hostname
Home
Reboot
Logout
Support
Help
System Password
Old Password:
New Password:
Retype New Password:
Change Password
Password Reset Options
Enable password reset via email
Send confirmation code to event notification email
Send confirmation code to an alternative email:
Enable password reset via the local console
Enable password reset via SSH
Save
Use a standard web connection
Use an encrypted web connection (HTTPS):
Generate new Certificate Signing Request
Upload existing certificate
Upload Certificate:
Choose file
No file chosen
Optional Separate Key:
Choose file
No file chosen
Save
User Settings
Session Timeout:
5 Minutes
Unit Display Format:
Bytes per second, decimal prefix (MB/s)
Save
Secure Shell (SSH)
Enable SSH:
At least one public key must be added to enable SSH.
Save
List of Public Keys
Comment
Public Key
No Public Keys Added
Add Public Key
Remove Public Key

3.2.1 System Password

This section allows the administrator to change the access password for the web interface. The new password must be between 5 and 64 characters and should contain both symbols and numbers.

Important: The word “RESET” is reserved by the system and cannot be used as a password.

Enter the existing password into the *Old Password* field; then enter the desired new password into the two following fields. Then click *Change Password*.

3.2.2 Password Reset Options

This section allows the administrator to enable and disabled different methods of password reset on the Node.

3.2.2.1 Password Reset via Email

3.2.2.1.1 Setup

This method of password reset allows a user that is authorised to access a pre-configured email address to reset the password of any user account on the Node.

When a user forgets their password, they will be able to click on the *Forgot your password?* link on the login page to reset their password.

To successfully reset your password using this method, an confirmation code will be sent to an email address previously configured in the web interface. This code will have to be obtained by the user and entered in to the password reset wizard to complete the password reset procedure.

Important: Resetting a password will log out any current sessions under that user name.

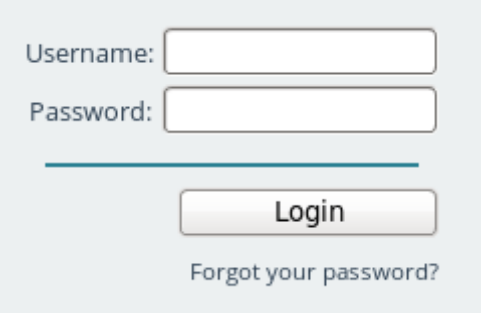
To enable password reset via email, SMTP settings will have to be configured first to allow the Node to send emails. Navigate to the *Service Control* page and enter your SMTP settings under the *Simple Mail Transfer Protocol (SMTP)* section. Refer to Section 3.3.3: Email for information on SMTP configuration.

Next, navigate to the *Passwords & Security* page and tick the *Enable password reset via email* checkbox. You must then select whether you wish to have the confirmation code sent to the “event notification email” which is configured on the *Service Control* page, or to an alternative email which can be entered in the text box underneath.

Refer to Section 3.3.4: Event Notification Email for information on setting an event notification email. You will be required to enter an email address in to the *alternative email* text box if an event notification email has not been set.

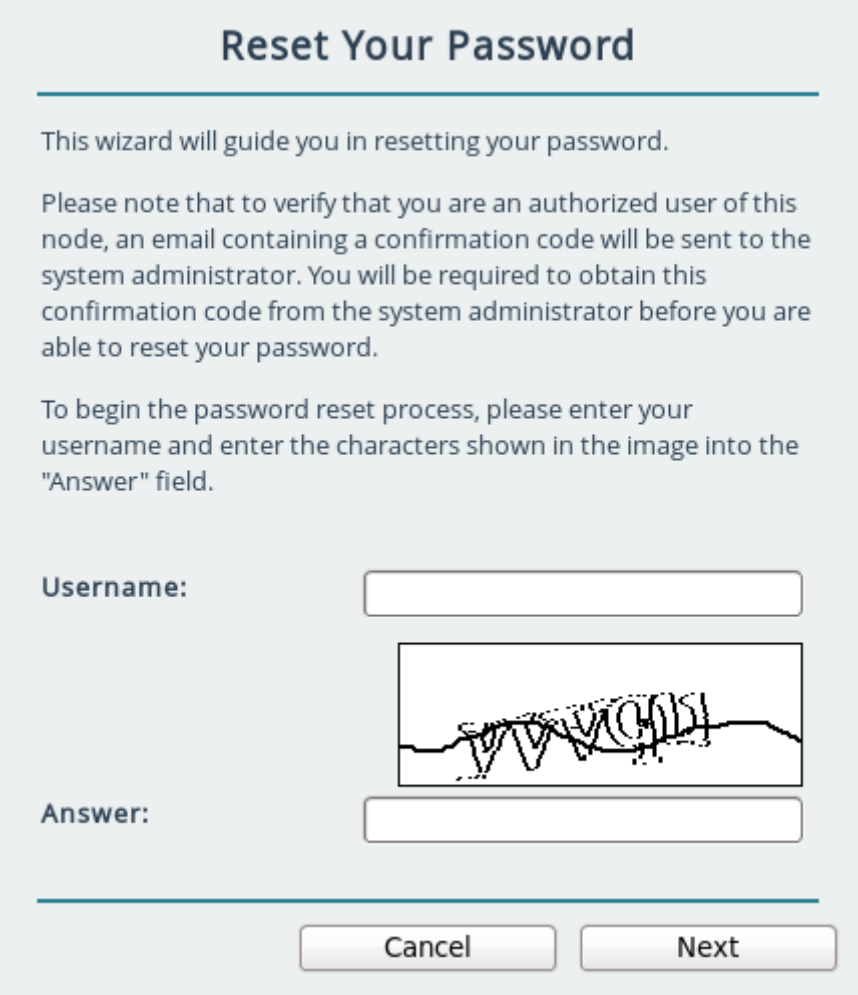
3.2.2.1.2 Using Password Reset via Email

To reset the password of a user account using the email method, navigate to the login page of the Node you wish to reset the password for. If password reset via email is enabled, there will be a "Forgot your password?" link underneath the login button as shown:



	Important: If the "Forgot your password?" link is not present, then password reset via email has not been enabled on the Node.

Enter the username you wish to reset the password for and complete the captcha challenge by entering the characters in the image in to the *Answer* text box. Then click *Next* to continue.

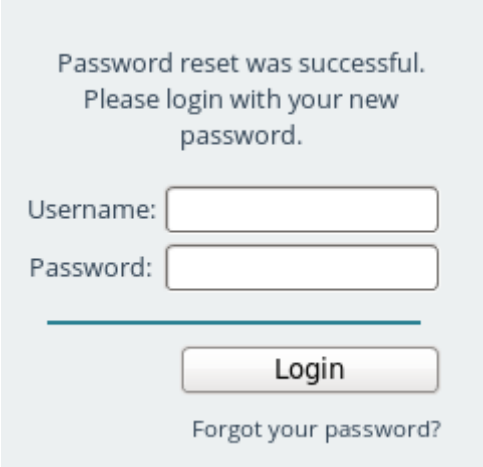


	Important: You can try a different captcha challenge by refreshing the web page.

An email containing a confirmation code will be sent to the email address set in the *Passwords & Security* page. Enter the confirmation code sent in the email to the *Confirmation Code* text box.

Enter your new password in to the *New Password* and *Confirm Password* text fields and press the *Next* button.

If password reset was successful, a message will be displayed and you will be able to log in with your new password.



3.2.2.2 Password Reset via Local Console or SSH

3.2.2.2.1 Setup

These methods of password reset allow any user that either has access to the local console or remote access via SSH to reset the password of any user account on the Node.

	Warning: These methods of password reset should be disabled if unauthorised users may either have access to the local console or remote access via SSH.

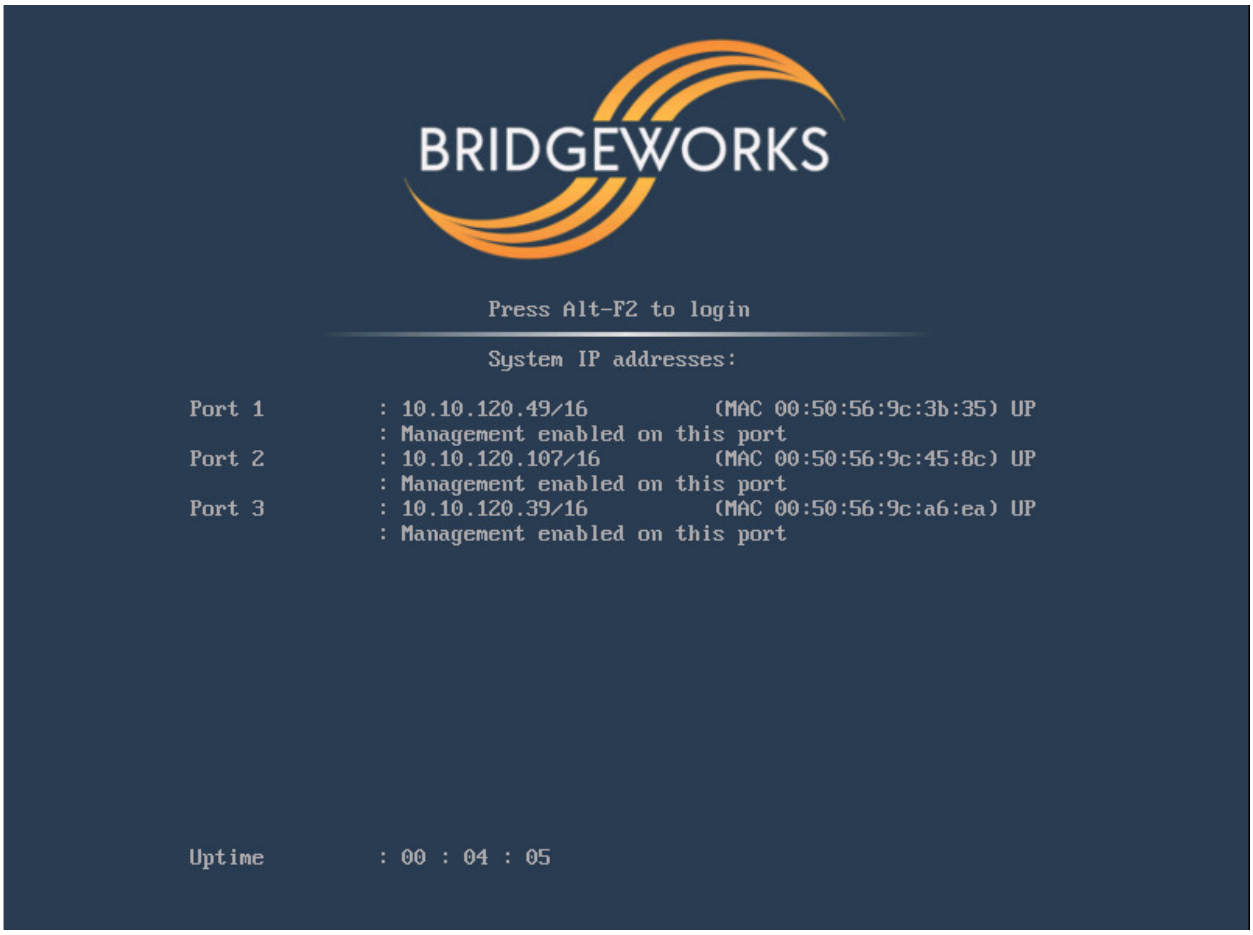
	Important: Resetting a password will log out any current sessions under that user name.

To enable password reset via local console, tick the *Enable password reset via the local console* checkbox or to enable via SSH, tick the *Enable password reset via SSH* checkbox. Then click *Save*.

	Important: Password reset via local console is enabled by default.

3.2.2.2.2 Using Password Reset via Local Console or SSH

To reset the password of a user account using the local console method, connect a keyboard and monitor to the Node. You will see the following screen:

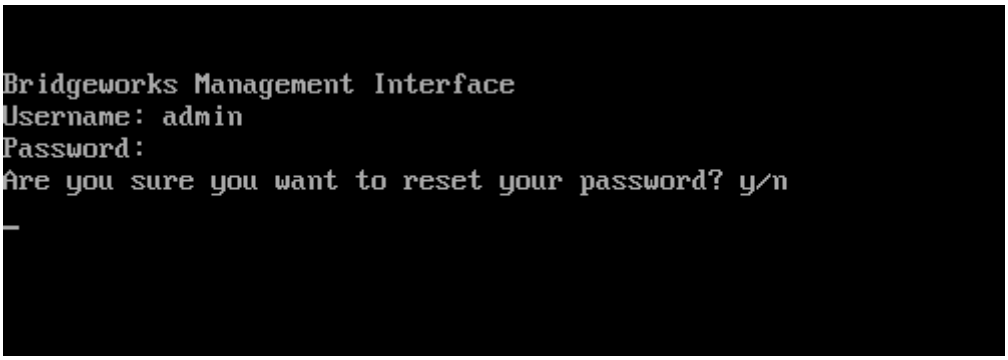


Press the “Alt” and “F2” keys at the same time to get access to the login prompt as shown:

To reset the password of a user account using the SSH method, connect to the Node via SSH to access the login prompt.

Enter the username you wish to reset the password for, such as “admin”. Then enter the password as “RESET”. Both the username and password are case-sensitive.

You will then be asked whether you wish to continue resetting the password. Press the “y” key then press the “Enter” key. Entering any other key will abort the password reset process.



Next, enter the new password you wish to set for the user selected. You will then be asked to enter the password again.

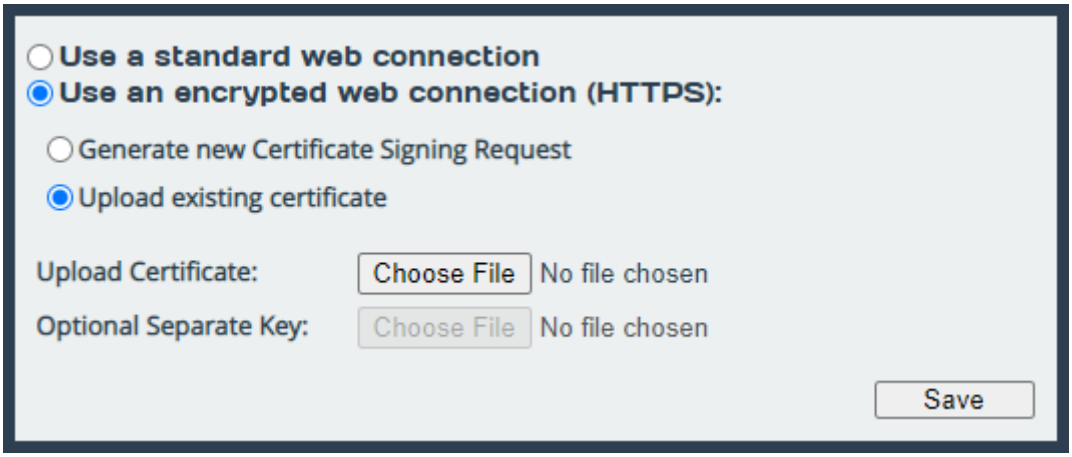
	Important: If the two passwords do not match, or you are attempting to set the password as “RESET”, then password reset will fail.

If your new password is accepted, the “Password set successfully” message will appear as shown:

You will now be able to log in to the web interface using your username and new password.

3.2.3 Secure Connection

To enable HTTPS, select the *Use an encrypted web connection (HTTPS)* radio button, then *Upload existing certificate*, and click Save.

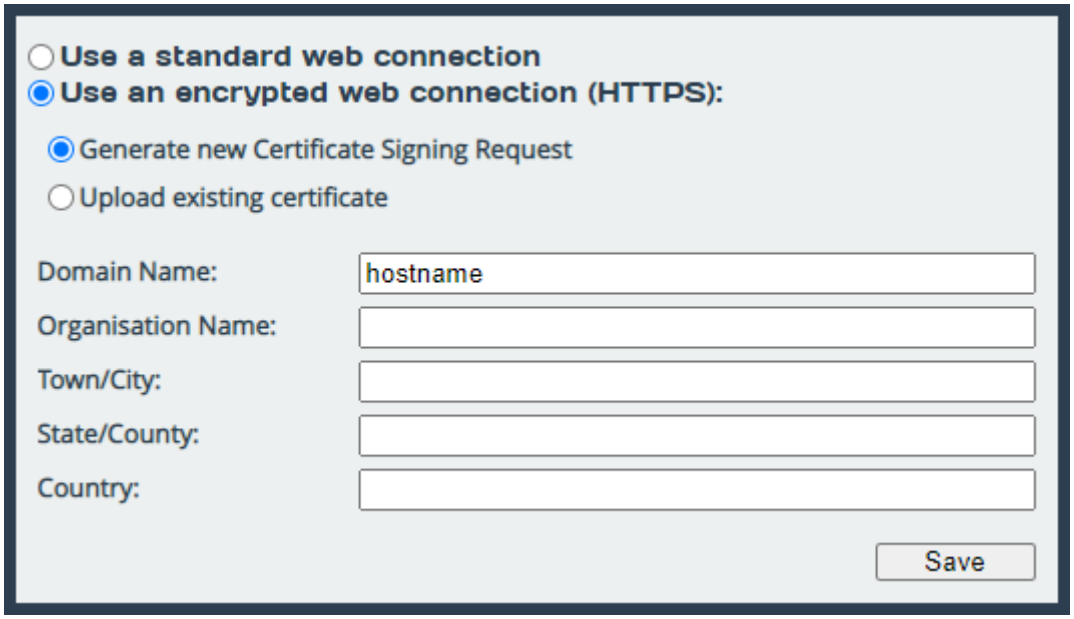


If you simply click *Save* without uploading any files for the certificate or key, a self-signed certificate will be automatically generated by the Node.

Alternatively, You can use your own certificate & key pair by selecting files to upload with the file-picker buttons. You may upload the key pair as two separate files, or one combined file.

You will be logged out of the Node's web interface, and further transactions with the web interface will use SSL/TLS encryption.

3.2.3.1 Generate new Certificate Signing Request



If you need a certificate signed by an external certificate authority, you may use the *Generate new Certificate Signing Request* option to do so. Select *Use an encrypted web connection (HTTPS)*, then *Generate new Certificate Signing Request* to open the form.

The fields which appear below this option when selected should be filled in with the details you want to appear on the certificate. The *Domain Name* field should be filled in with the IP address or fully qualified domain name which you use to access your Node. The following four fields should identify your company or organisation. Note that the *Country* field should contain a two-letter country code (ISO 3166-1 alpha-2), not a full country name.

Clicking *Save* will then download a CSR file. You should then send this file to your certificate authority, who should send you back a signed certificate file.

You can then upload this signed certificate file to the Node, using the *Upload existing certificate* option, leaving the *Optional Separate Key* field empty.

3.2.4 User Settings

Settings in this section allow you to change parameters for the user interface.

3.2.4.1 Session Timeout

After not interacting with the interface for a certain period of time, you will automatically be logged out. The Session Timeout setting allows you to adjust the length of time that must pass before you are logged out.

3.2.4.2 Unit Display Format

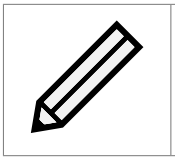
To allow a user to view system graphs in a unit that is applicable to their use case, the system may be switched to display in one of 6 different unit scales:

- Bits per second, decimal prefix (Mbit/s)
- Bytes per second, decimal prefix (MB/s)
- Bits per second, binary prefix (Mibit/s)
- Bytes per second, binary prefix (MiB/s)
- Bytes per hour, decimal prefix (TB/h)
- Bytes per hour, binary prefix (TiB/h)

3.2.5 Secure Shell (SSH)

Secure Shell (SSH) is a protocol that allows for secure access to a Node's configuration console.

To enable SSH on network interfaces with the "Management" protocol mapped, tick the *Enable SSH* checkbox and click *Save*.

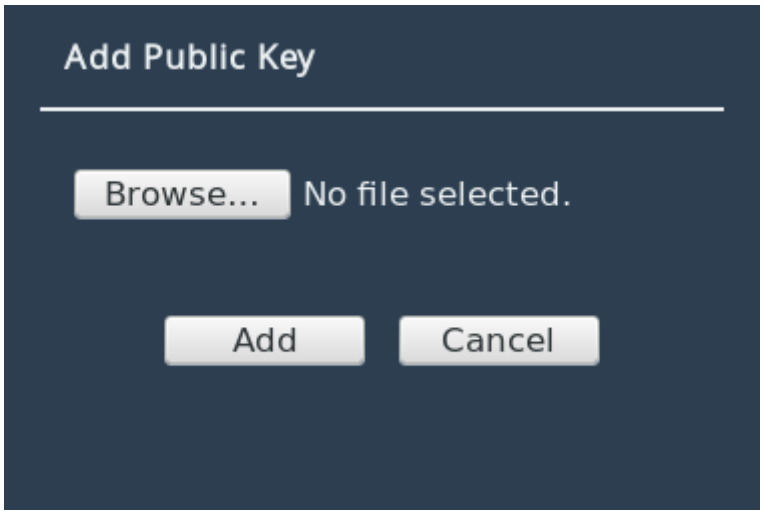


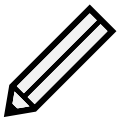
Note: At least one public key must uploaded, as described below, before SSH can be enabled.

3.2.5.1 Managing Public Keys

To log on to a Node's configuration console using SSH, a public key is required to be uploaded first. Users connecting to the Node without having uploaded the corresponding public key to the Node first will be refused access.

To upload a public key, click on the *Add Public Key* button. The *Add Public Key* dialog box will appear. Click on the *Browse* button to select a public key file.



	Note: Only RSA keys in the OpenSSH or RFC4716 format are supported.

Click on the *Add* button to upload the selected public key file. The public key should then appear in the *List of Public Keys*.

To delete a public key, click on the public key to delete in the *List of Public Keys* and then click on the *Remove Public Key* button.

	Important: Open SSH connections will not be closed when a public key is removed, or if SSH is disabled. Only new SSH connections will be rejected.

3.2.5.2 Using SSH

To connect to a Node which has a management port with an IP address of 192.168.0.20 using the OpenSSH SSH client, use the command:

```
ssh admin@192.168.0.20
```

You will then be prompted for the username and password of the Node to log in to the configuration console.

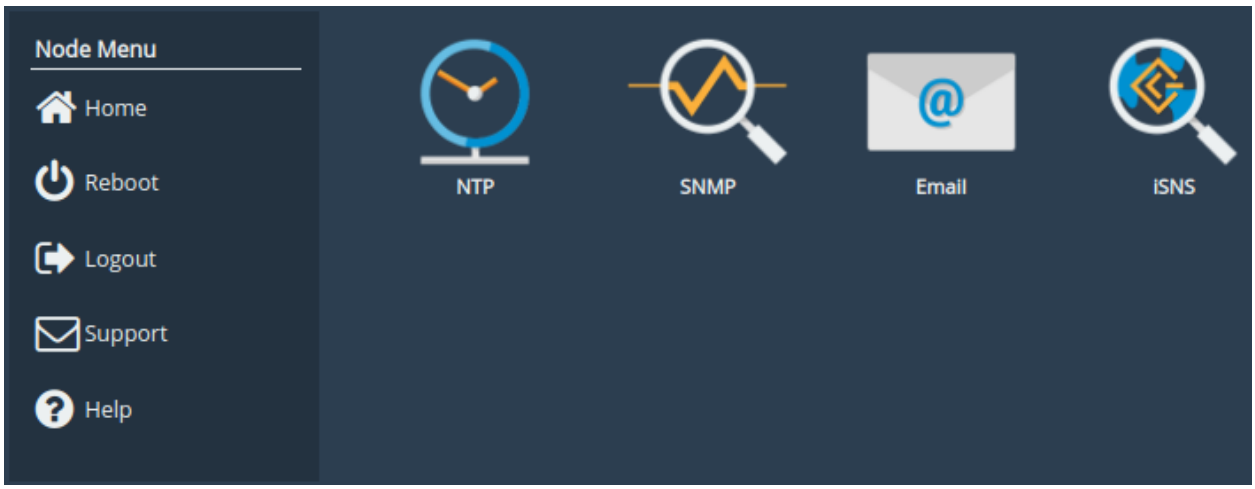
You will be denied entry to the configuration console if you have not uploaded a public key to the Node prior to connecting via SSH. A valid username and password for the Node is also required to log in using SSH.

	Important: Logging in as root user is disabled on SSH.

3.3 Service Control

This configuration page allows the administrator to configure network services for the Node. From the Home screen, select the *Service Control* icon under the *Node Configuration* section.

The web interface will display the following:



Each link leads to a different service.

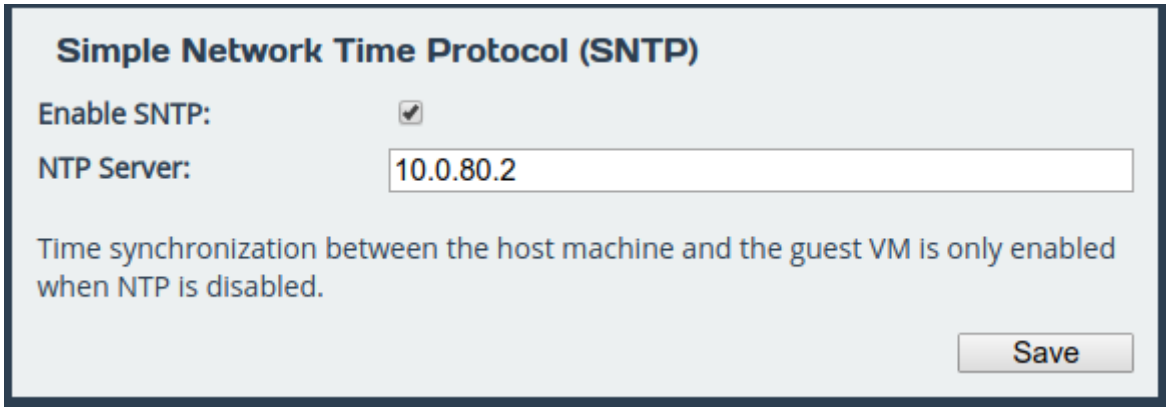
The *NTP* (Network Time Protocol) page allows you to configure various settings available for NTP on the Node.

The *SNMP* (Simple Network Management Protocol) page allows you to configure various settings available for SNMP on the Node.

The *Email* page allows you to configure various settings available for Email alerts on the Node.

The *iSNS* page allows you to configure various settings available for iSNS on the Node.

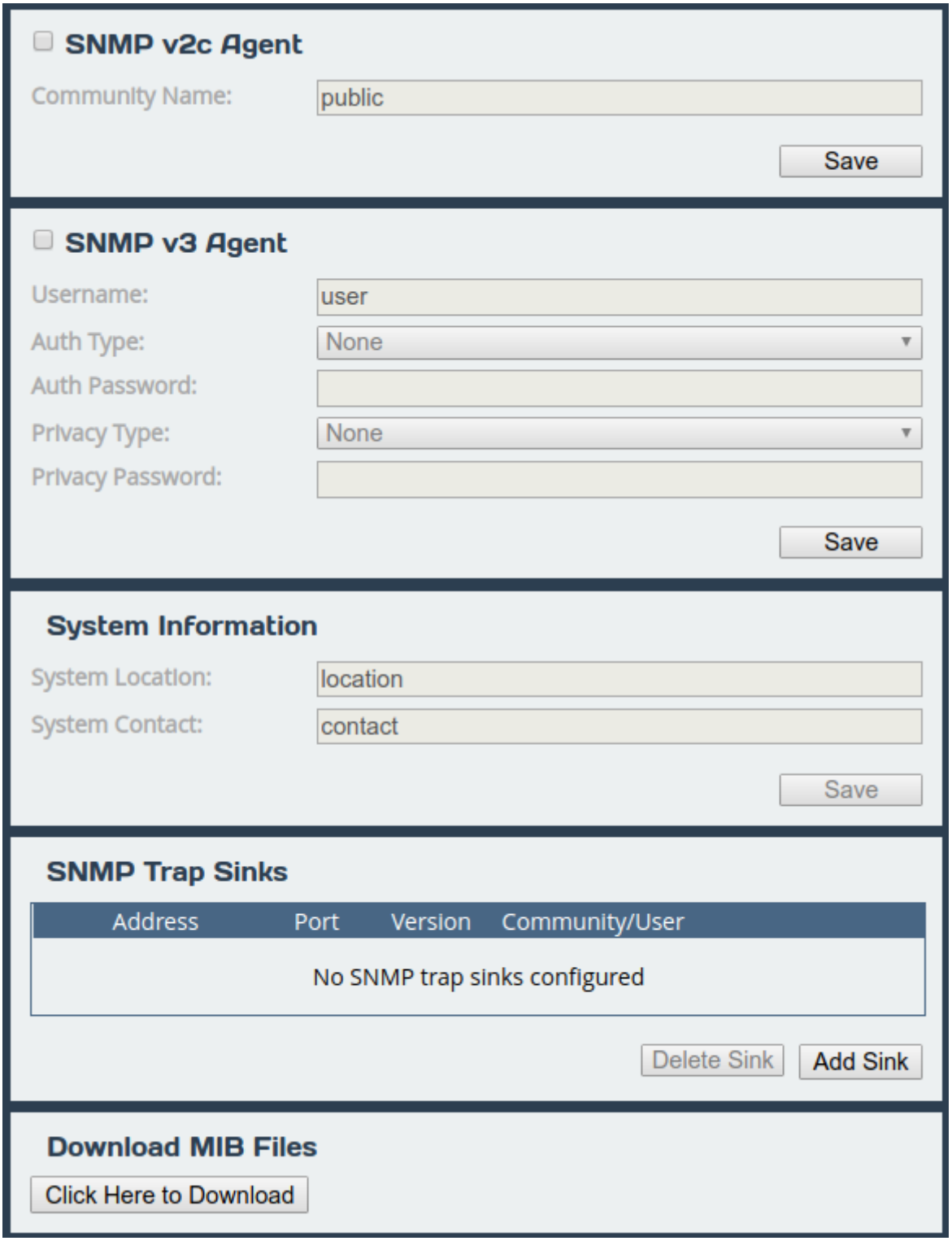
3.3.1 Network Time Protocol (NTP)



SNTP is a protocol for synchronising the clock of computer systems. This feature is critical if you are planning on using the scheduler or useful when viewing the logs to determine when an event occurred. Refer to Section 13.2: System Log for more information.

To enable SNTP, select the *Enable SNTP* checkbox and enter the IP address for the NTP server. Then click *Save*.

3.3.2 Simple Network Management Protocol (SNMP)



Two versions of SNMP are supported, 2c and 3. V3 is recommended as it has everything 2c has plus vastly superior security.

To enable SNMPv2c, check the box in the top left of the *SNMP v2c Agent* box, enter a *Community Name* and click *Save*.

To enable SNMPv3, check the box in the top left of the *SNMP v3 Agent* box, then enter a *Username*. Authentication verifies the sender of data while privacy protects the data. *SHA1* and *AES-128* are the superior and recommended hash function and encryption protocol respectively. Once done configuring the security settings, click *Save*.

3.3.2.1 System Information

The information configured here is accessible over SNMP.

System Location is the location of this Node. The value of this property should provide enough information for an administrator to locate this Node.

System Contact is the contact information for the person or department responsible for managing this Node. Click *Save* to save changes to System Information.

3.3.2.2 SNMP Trap Sinks

The Node notifies all configured *Trap Sinks* when a system event occurs. This means your SNMP manager can be notified should the Node encounter an error.

Click *More Info* link to view more information about a specific sink.

To add a new sink, click the *Add Sink* button to open the Add SNMP Trap Sink dialog.

3.3.2.3 Add SNMP Trap Sink

Address is the IP Address of the trap sink. Must be a valid IP address. Reserved and multicast addresses are not supported.

Port is the port of the trap sink.

Version is the version of SNMP the sink uses. It is recommended to use SNMPv3 where possible since it allows for authentication and privacy. The following versions are supported:

- v1: SNMPv1 (not recommended)
- v2c: SNMPv2c allows acknowledged traps
- v3: SNMPv3 allows privacy and authentication, making it more secure than SNMPv1 and SNMPv2c. (recommended)

Type is the type of notification sent to the trap sink. It is recommended to use the *Inform* notification type since it is acknowledged and therefore the notification is less likely to be unintentionally lost.

- Trap: Unacknowledged message
- Inform: Acknowledged message, not supported with SNMPv1

Community is the community string to use for the trap sink. Supported in SNMPv1 and SNMPv2c. Cannot contain spaces.

Username is the SNMPv3 unique identifier to associate these security details with. Must be 1-32 characters in length, and cannot contain spaces.

Engine ID is the SNMPv3 Engine ID of the trap sink. The Node should automatically discover the engine ID if this is left blank. If an Engine ID is provided, it must be 5-32 characters in length, and cannot contain spaces.

Authentication is the SNMPv3 authentication hash function used by the trap sink. Authentication allows only SNMP engines with the correct authentication password to connect to the trap sink. It is recommended to use authentication where available. It is not recommended to use the MD5 hash function since it suffers from vulnerabilities.

- SHA1: Uses the SHA1 hash function (recommended)
- MD5: Uses the MD5 hash function (not recommended)
- None: Authentication Disabled (not recommended)

Auth Password is the authentication password used to log in to the trap sink. An authentication password must be provided if *Authentication* is not set to *None*.

Privacy is the SNMPv3 privacy type used by the trap sink. *Authentication* must be enabled to use privacy. Privacy allows SNMP engines to communicate privately using encrypted messages. It is recommended to use privacy where available. It is not recommended to use the DES cipher function since it is cryptographically weak.

- AES-128: Uses the AES-128 cipher function (recommended)
- DES: Uses the DES cipher function (not recommended)
- None: Privacy Disabled (not recommended)

Privacy Password is the privacy password used to communicate privately with the trap sink. A privacy password must be provided if *Privacy* is not set to *None*. If the sink has privacy enabled but doesn't have a specific privacy password, then the privacy password is likely the same as the authentication password.

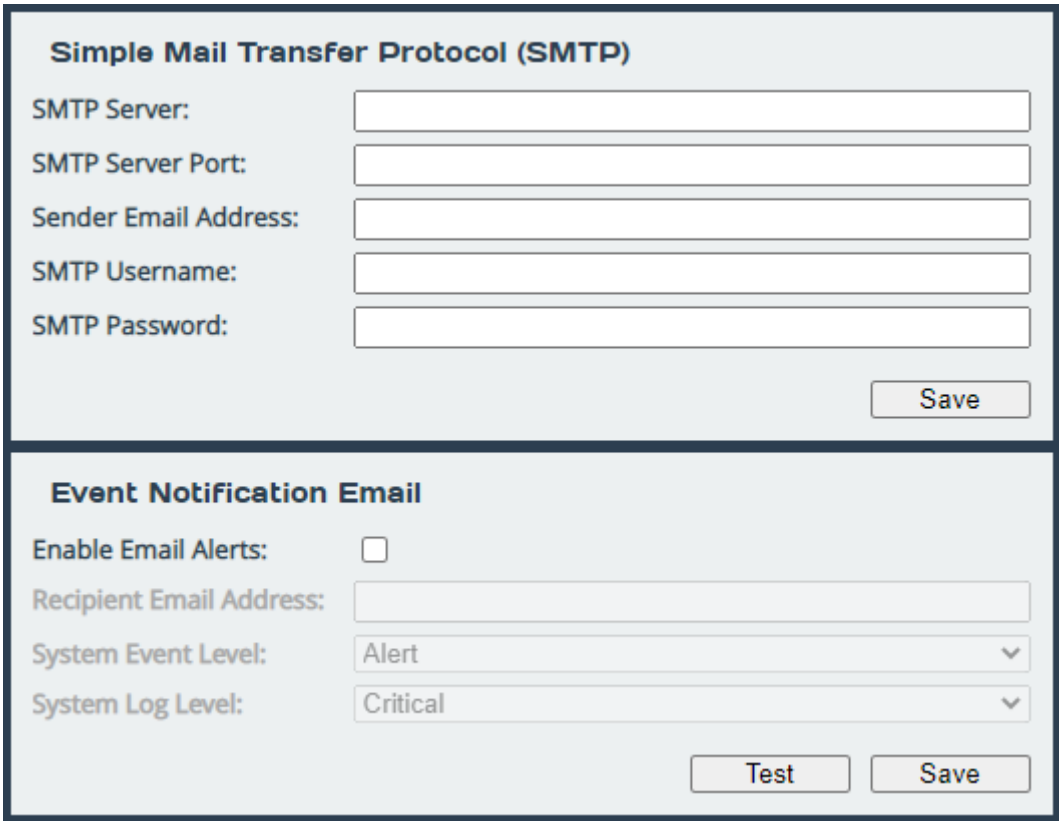
3.3.2.4 Download MIB Files

Several Management Information Bases (MIBs) are available for querying on this unit using SNMP and these MIBs can be accessed using unique Object Identifiers (OIDs).

MIB	OID
System	1.3.6.1.2.1.1
Interfaces	1.3.6.1.2.1.2
IP	1.3.6.1.2.1.4
ICMP	1.3.6.1.2.1.5
TCP	1.3.6.1.2.1.6
UDP	1.3.6.1.2.1.7
Bridgeworks Node Management Statistics	1.3.6.1.4.1.49599.11
Bridgeworks Service Statistics	1.3.6.1.4.1.49599.12

The MIBs describing data within the Bridgeworks' OID can be downloaded by clicking *Click Here to Download*. A MIB file can be imported in to an SNMP manager in order to provide useful information about data returned by the SNMP agent or sent in an SNMP trap.

3.3.3 Email



This section allows an SMTP server to be configured, to send emails on behalf of the Node.

The fields in this subsection are:

SMTP Server To enable an SMTP server, enter its IP address or hostname in this field. The server must be reachable from the Node's Management interface (or whichever port the default route is set to) on this address. Refer to Section 3.1.2.4: Default Route for information on setting the default route.

SMTP Server Port Enter the port number of the SMTP server. If no port number is specified, it will use the default port (25).

Sender Email Address The address from which emails will be sent. This needn't be a previously in-use address; it can be anything your SMTP server will allow. This can be used to identify the emails from this Node.

Must be of the form: _____@_____.___

SMTP Username Username credential to be used to send emails from the SMTP server. May be blank, depending on your server's configuration.

SMTP Password Password credential to be used to send emails from the SMTP server. May be blank, depending on your server's configuration.

Click *Save* to apply any changes made to the SMTP configuration.

3.3.4 Event Notification Email

The Node can notify a systems administrator when events of a certain urgency occur in the Node log. Before this can be done, SMTP settings must be configured. Refer to Section 3.3.3: Email for information on SMTP settings.

To enable email alerts on the Node, select the *Enable Email Alerts* checkbox. The two following fields should then be completed:

Recipient Email Address The email address/addresses to which the emails will be sent. Multiple email addresses can be specified, separated by a semicolon, e.g.: `office@example.com; home@example.com`.

Trigger Event Log Level The minimum log level to trigger an email. Events of higher urgency than the selected level will also trigger an email. The available levels are, in descending order of urgency:

Critical Example: The Node is running at non-recommended temperatures.

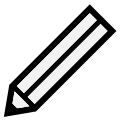
Error Example: A device attached to the Node has been disconnected.

Warning Example: An invalid configuration file was uploaded.

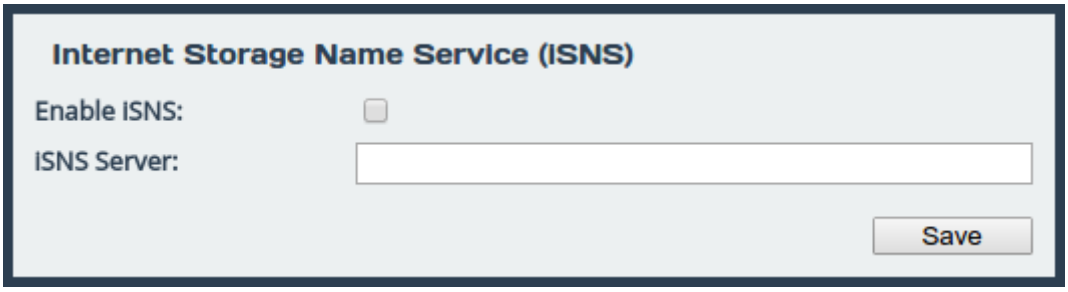
Confirm these settings by clicking *Save*.

The *Test* button will send a test email to the recipient email address/addresses to confirm that the email configuration is working correctly.

3.3.5 Internet Storage Name Service (iSNS)



Note: iSNS is only available if your WANrockIT Node has an iSCSI target feature card installed.



Internet Storage Name Service allows automated discovery, management and configuration of iSCSI resources from a central point. With this option enabled, the Node's iSCSI target will be registered with an iSNS server, from which it can be discovered.

To enable this feature, select *Enable iSNS*, and enter the IP address or hostname of the iSNS server with which to register in the *iSNS Server* field. Then click *Save* to apply changes.

4 WANrockIT Configuration

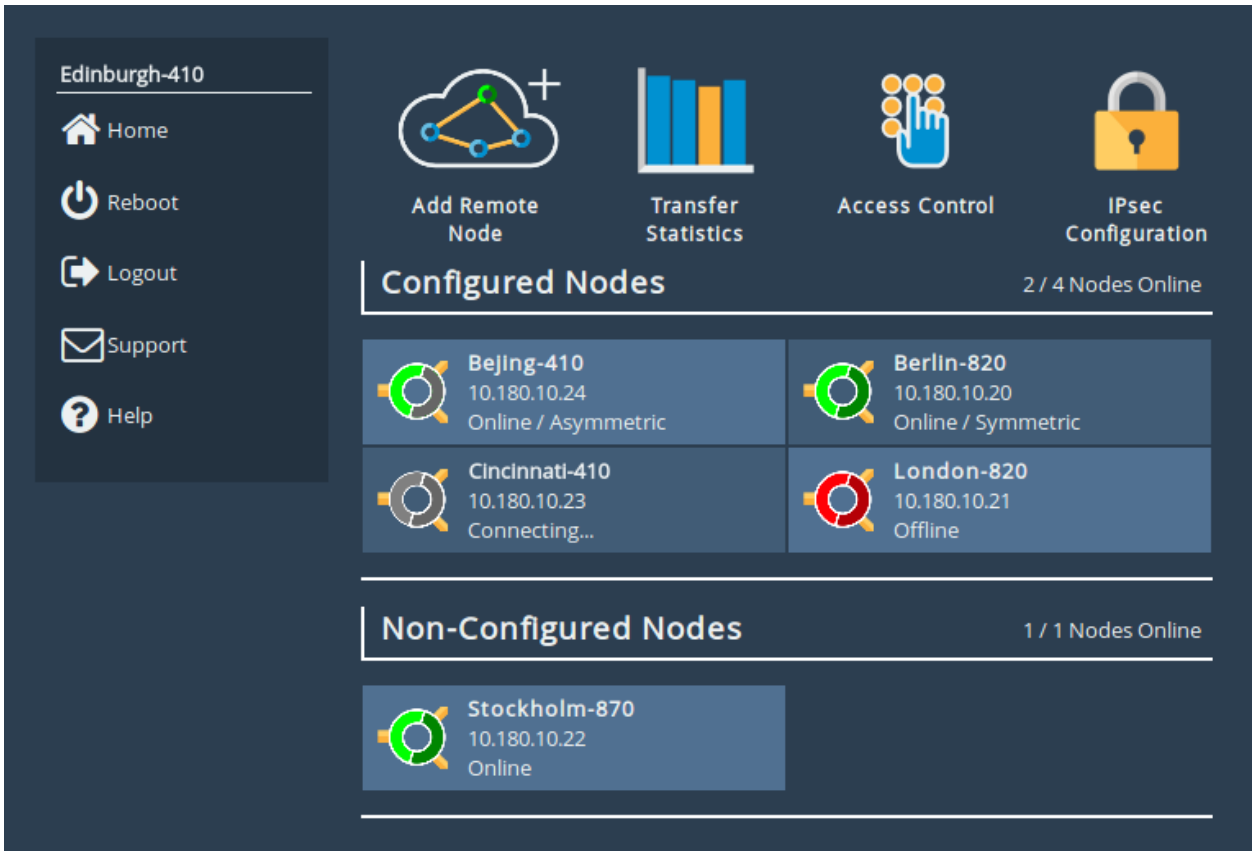
The *WANrockIT* section of the web interface allows the administrator to configure different aspects of the WANrockIT Node.

4.1 Node Management

The *Node Management* page has all the tools necessary to connect to remote Nodes, set security options, view transfer statistics and configure your linked Nodes.

From the Home screen, select the *Node Management* icon under the *WANrockIT* section.

The web interface will now display the following:

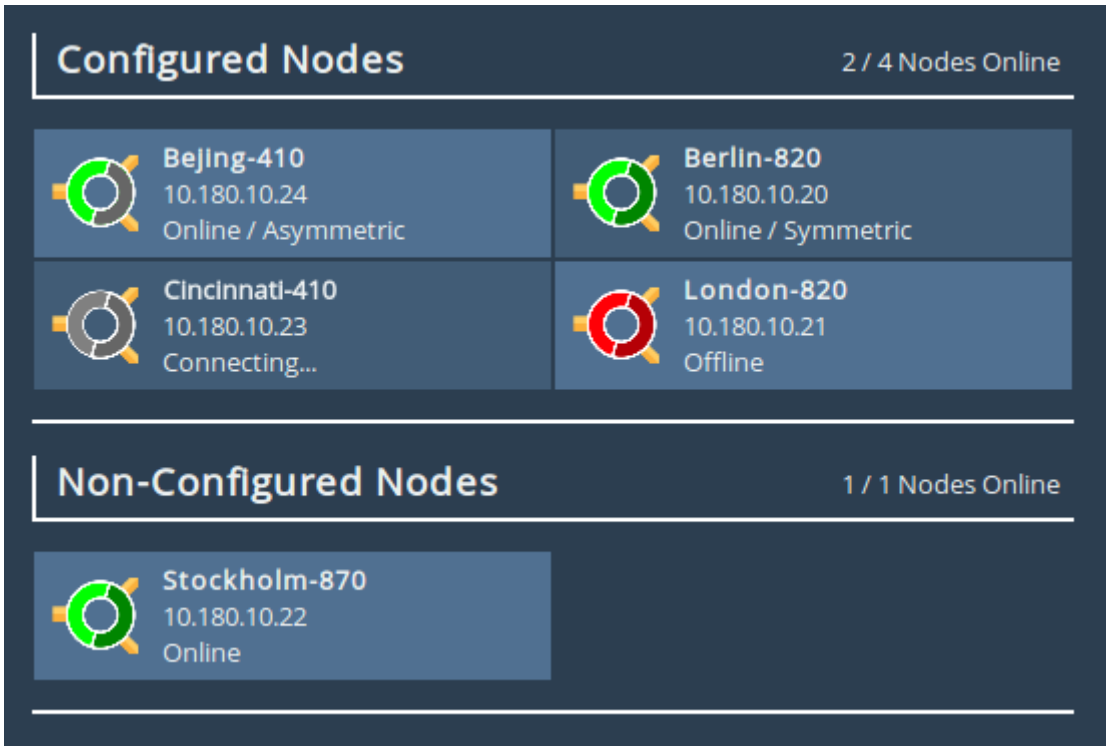


Options at the top of the page allow you to configure settings for your current Node. More information for these options can be found in the following sections:

- Section 4.1.2: Add Remote Node
- Section 4.1.3: Transfer Statistics
- Section 4.1.4: Access Control
- Section 4.1.5: IPsec

4.1.1 Remote Nodes

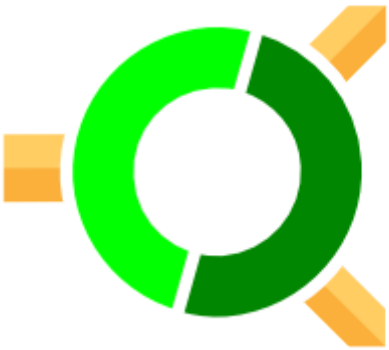
This section details the Nodes that have been configured with your appliance.



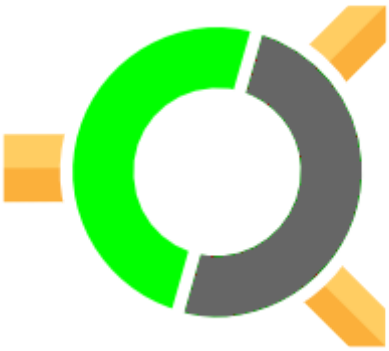
Each Node can be identified by the Node's hostname. The hostname of each Node can be configured on it's own Web interface under the *Hostname* field of the *Network Connections* page.

In addition to the hostname, the leading IP address will be displayed. This will usually be the IP address which was used to add the Node on the *Add Remote Node* page.

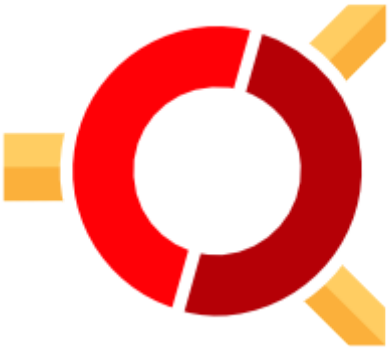
Finally the current status of the Node is displayed alongside an icon. The connection to the Node can be in one of four states:



Connection Active (Symmetric) Node is active with connected paths. Node also has a fully configured connection back.



Connection Active (Asymmetric) Node is active with connected paths. Node does not have a fully configured connection back. Note that acceleration will still work as normal with a Node in this state.



Connection Inactive Connection can not be made to a previously available Node. You may still remove the remote Node as usual.

Connecting Remote Node is configured with this device and is waiting upon a connection to be made. You may still remove the remote Node configuration as usual.

Clicking on the icon for a remote Node will take you to the management page for the remote Node.

4.1.1.1 Configured Nodes

This list represents Nodes that have been directly added. Nodes in this list have additional configuration options available for them.

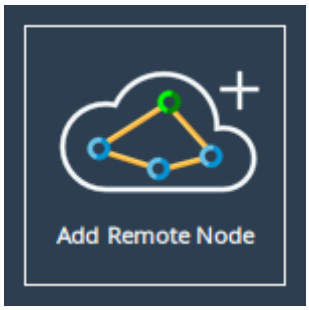
4.1.1.2 Non-Configured Nodes

This list represents Nodes that have made an inbound connection, but have not been directly added. *Relationships* and *VPN* tunnels can still be created for Nodes in this state and acceleration can still be performed. A *Non-Configured Node* can become a *Configured Node* by performing the *Add Remote Node* operation on it; doing so will enable additional configuration options.

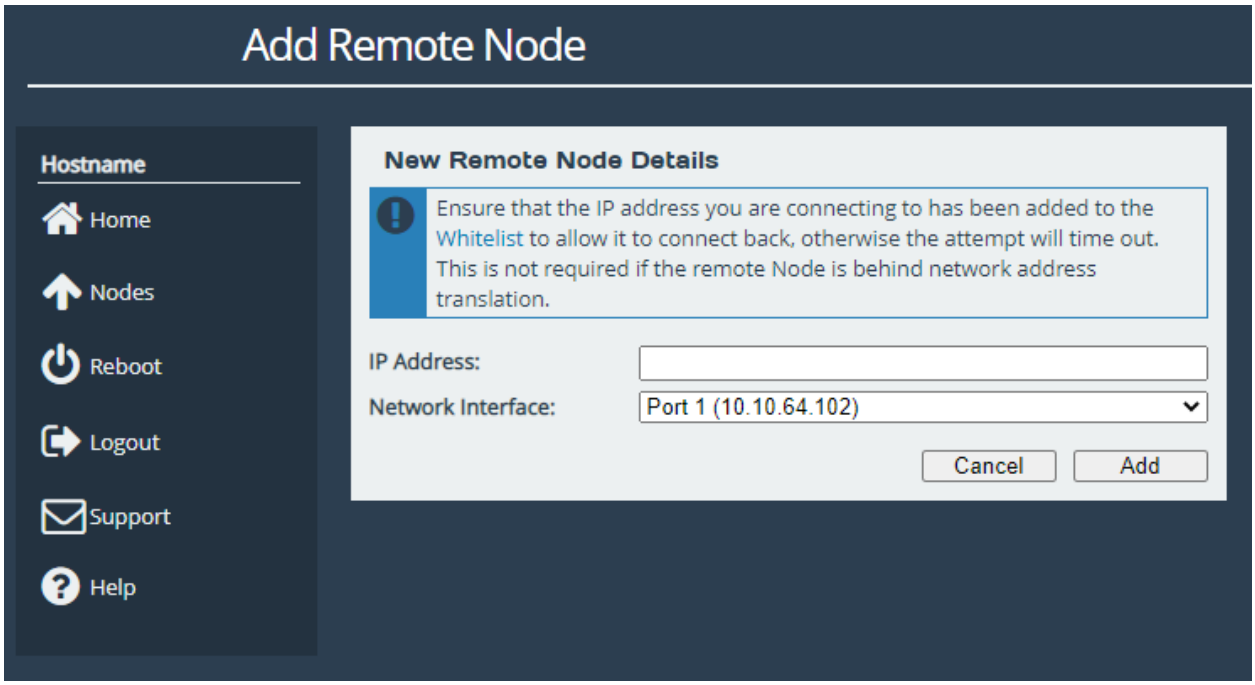
4.1.2 Add Remote Node

	Important: If you want to encrypt accelerated traffic, this step should be done after configuring IPsec.

To add a remote Node, click on the *Add Remote Node* icon on the Node Management page.



The following page will allow you to add a remote Node using the *IP Address*.



This page allows a remote Node to be added to the list of connected Nodes. The *IP Address* field takes input of the IPv4 address of the remote Node. The *Network Interface* drop-down menu allows for the selection of the WAN interface on this Node to be used to initiate the connection to the remote Node, if this Node has WAN capabilities mapped to more than one. See Chapter 12: Port Mappings for information on adding and removing WAN capabilities to network interfaces.

To add a remote Node, enter the IPv4 address of a WAN port on the remote Node which is visible to this Node, and click the *Add* button. If the remote Node is behind a NAT connection, the public IP address for the NAT connection should be used.

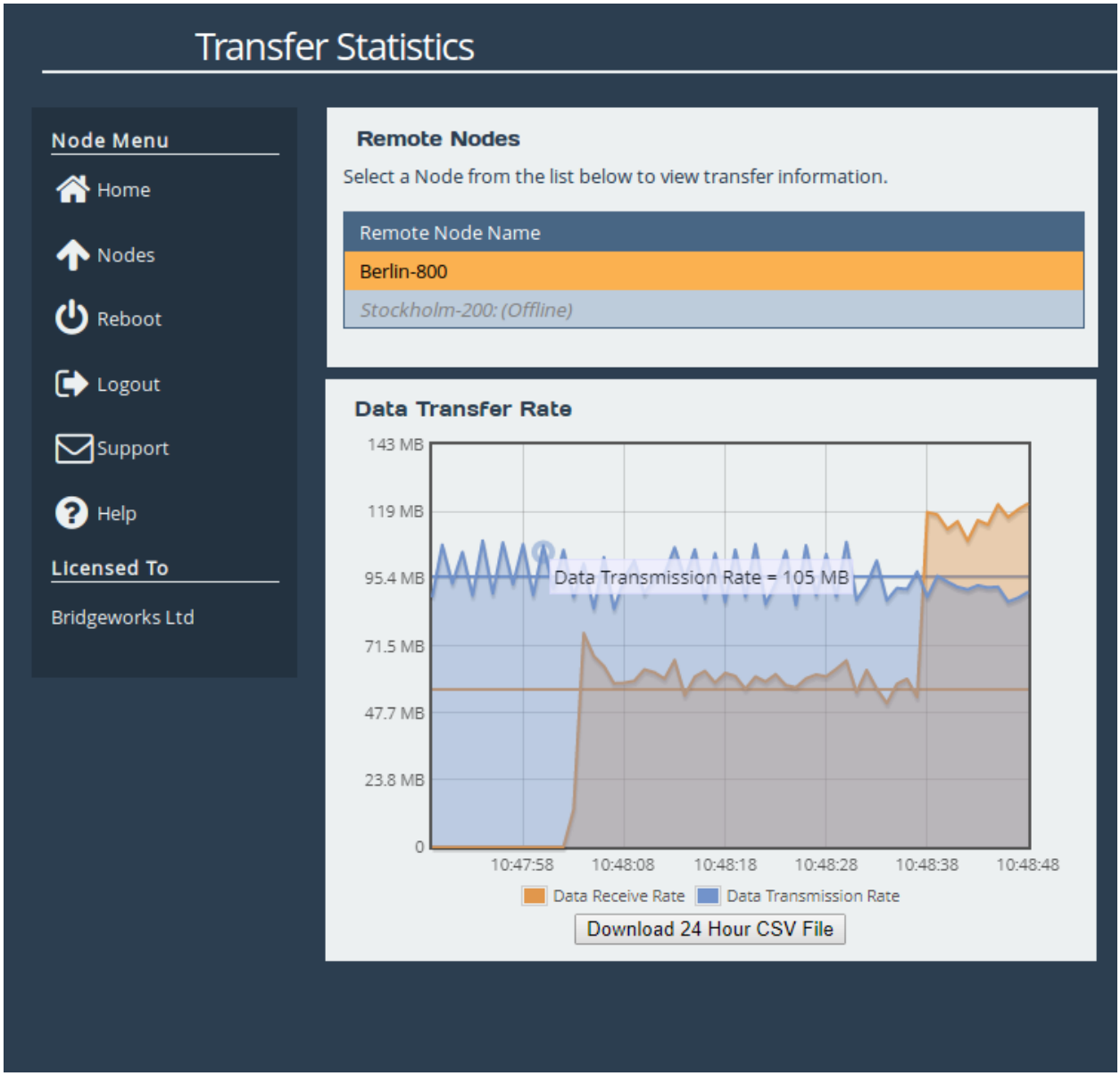
A dialog box will appear indicating the connection attempt to the remote Node, and will alert you to the success or failure of the Node connection. Any remote Node connection that has been added to the local Node in this way will be automatically saved, and will restore on reboot until the Node is removed.

4.1.3 Transfer Statistics

This configuration page will allow you to monitor, in real time, the performance of a link over the span of a minute and download the performance data between the local and the remote Node over the last 24 hours.

From the Node Management screen, select the *Transfer Statistics* icon.

The web interface will now display the following window:



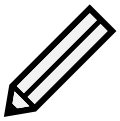
To view a remote Node's transfer rate, click on the name of the Node from the *Remote Node Name* list, and graphing will start automatically.

A remote Node will be shown as offline if the link to it has not been re-established after a system restart. You cannot start monitoring performance data to a remote Node until the link has been re-established. An offline Node is indicated if the name of the Node has *Offline* next to it, as shown.

	Important: If there are no remote Nodes online then you will not be able to see the *Data Transmission Rate* graph or the *24 Hour Transfer History* button.

4.1.3.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.

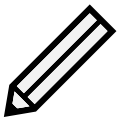
	Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.1.3.2 Download 24 Hour Transfer History

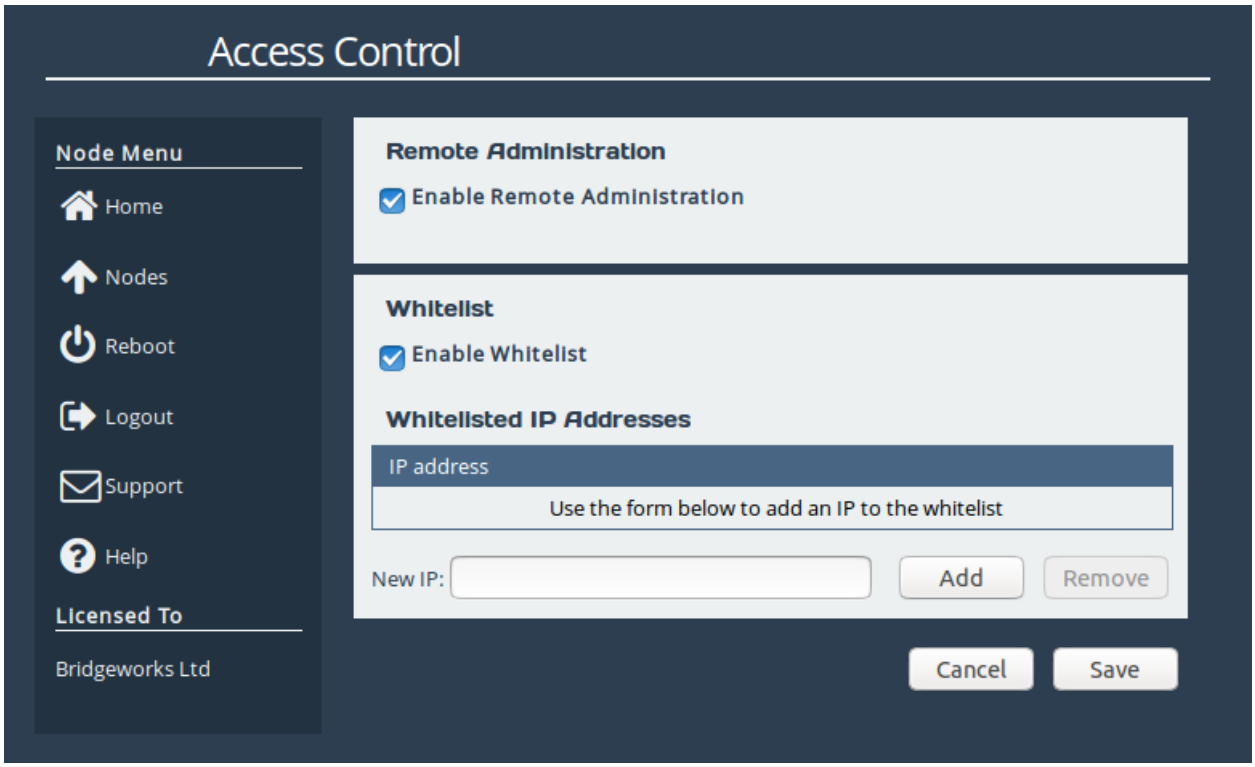
You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Download 24 Hour CSV File* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix F: Transfer Statistics Graphing Instructions for Excel 2010 for information on viewing this file.

	Note: The 24 hour statistics are cleared on reboot.

4.1.4 Access Control

To configure access control settings, click on the *Access Control* icon on the Node Management page.

The following page will be displayed:



4.1.4.1 Remote Administration

The *Enable Remote Administration* checkbox allows for the disabling or enabling of remote access of this Node. You can start a Remote Access session from the Node Management page of the remote Node, see Section 4.2.7: Remote Control.

4.1.4.2 Whitelist

By default, the *Enable Whitelist* checkbox will be selected, which stops incoming WANrockIT connections from IP addresses not explicitly specified. Clearing the checkbox will instead allow all incoming WANrockIT connections.

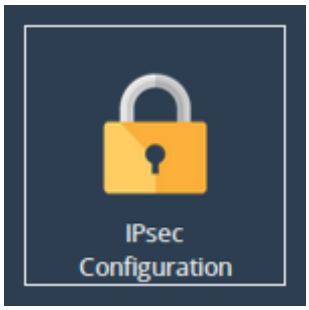
To allow a new connection from a remote Node, enter the IP address of the remote Node's WAN interface in to the *New IP* field and click *Add*. Multiple addresses can be added for each connected remote Node, and are required for multiple paths.

To delete a listing, select the entry in the *Whitelisted IP Addresses* table and then click *Remove*.

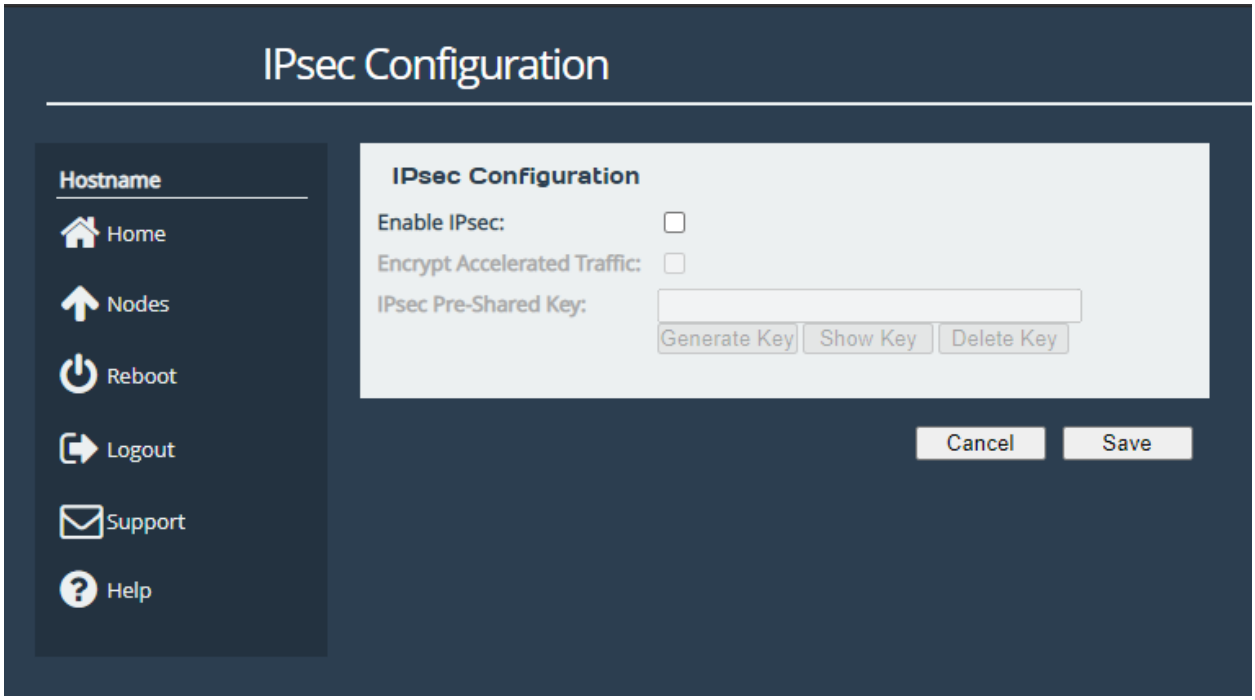
	Important: Adding or removing entries from the whitelist will not take effect until the *Save* button is clicked.

4.1.5 IPsec

IPsec can be enabled on all WAN connections, using AES encryption. To configure IPsec, click on the *IPsec Configuration* icon found at the top of the Node Management page.



The web interface will now display the following window:



	Important: Additional UDP ports must be open on any firewalls between the Node and the external WAN connection before configuring IPsec. For more information on which ports need to be opened, please see Appendix A: IP Protocols and Port Numbers

4.1.5.1 Enabling IPsec service

Checking the *Enable IPsec* checkbox will allow the IPsec encryption service to start after clicking the *Save* button. Traffic moving through the Node will not be encrypted at this point. Unchecking this box will stop the IPsec service without removing any of the configurations on this page.

4.1.5.2 Encrypting Accelerated Traffic

Accelerated traffic can be encrypted using the *Encrypt Accelerated Traffic* checkbox as long as the service has been started and a PSK has been set.

	Important: A pre-shared key is necessary for both VPN connections, and WAN link encryption.

4.1.5.3 Adding a PSK (Pre-Shared Key)

In the *IPsec Pre-Shared Key* field, enter a value or use the *Generate Key* button to set the PSK. If the *Generate Key* button was used to create the key, copy and paste it to the *IPsec Configuration* page of each connected Node.

	Important: A matching pre-shared key must be entered on all connected Nodes.

	Important: The PSK must be at least 16 characters and at most 256 characters.

The pre-shared key will not display automatically when returning to this page. If you need to copy it to another Node, click the *Show Key* button.

	Important: A warning will appear when configuring IPsec over an unsecured connection (i.e. HTTP rather than HTTPS). To ensure your pre-shared key cannot be intercepted over your network connection, enable HTTPS before configuring IPsec as explained in Section 3.2.3: Secure Connection.

The entered pre-shared key is saved in a secure configuration store, and is not removed automatically when IPsec is disabled. To delete your pre-shared key, click *Delete Key*. This will disable any VPN connections, and WAN link encryption, if either is enabled.

4.2 WANrockIT Node Page

The *WANrockIT Node* page has all the configuration settings and applications used to set up a specific remote Node. Clicking on any *Remote Node* icon on the *Node Management* page will take you to the equivalent *WANrockIT Node* page for that remote Node.

Once loaded, the following page should be displayed:

	Note: Available configuration options and applications shown will vary based on the specific *Product Type* of the remote Node.

	Note: Available configuration options and applications are limited if the selected remote Node is considered *Non-Configured*.

4.2.1 Node Status

This section contains information about the remote Node:

State The current connection state for the remote Node. Potential values include: *Online*, *Connecting* or *Offline*.

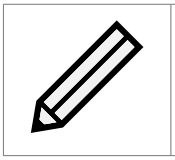
Active Paths Both the total number of available paths to the remote Node as well as the number that are currently active.

Model Model number of the remote Node.

Negotiated Bandwidth Maximum licensed bandwidth limit between the two Nodes.

TX/RX Current transfer and receive statistics to and from the remote Node respectively.

Remote Configuration *Present* or *Not Present* indicating whether or not the remote Node has a full configuration back to this Node. This value may take a few seconds to update after a configuration change.



Note: Some status elements may appear as *Unknown* if the selected remote Node is considered *Non-Configured*.

4.2.2 Node Configuration

All settings specific to this remote Node are located here. More information for these options can be found in the following sections:

- Section 4.2.4: Path Configuration
- Section 4.2.5: Node Specific Transfer Statistics
- Section 4.2.6: Remove Node

4.2.3 Applications & Utilities

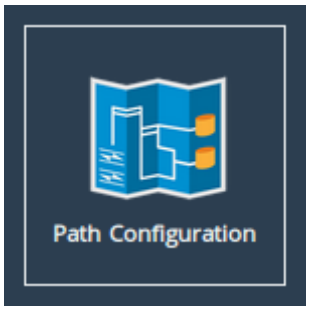
Any available *Applications* or *Utilities* are displayed here. More information for these options can be found in the following sections:

- Section 4.2.7: Remote Control
- Section 4.2.8: Learn
- Section 4.2.9: SCSI Devices

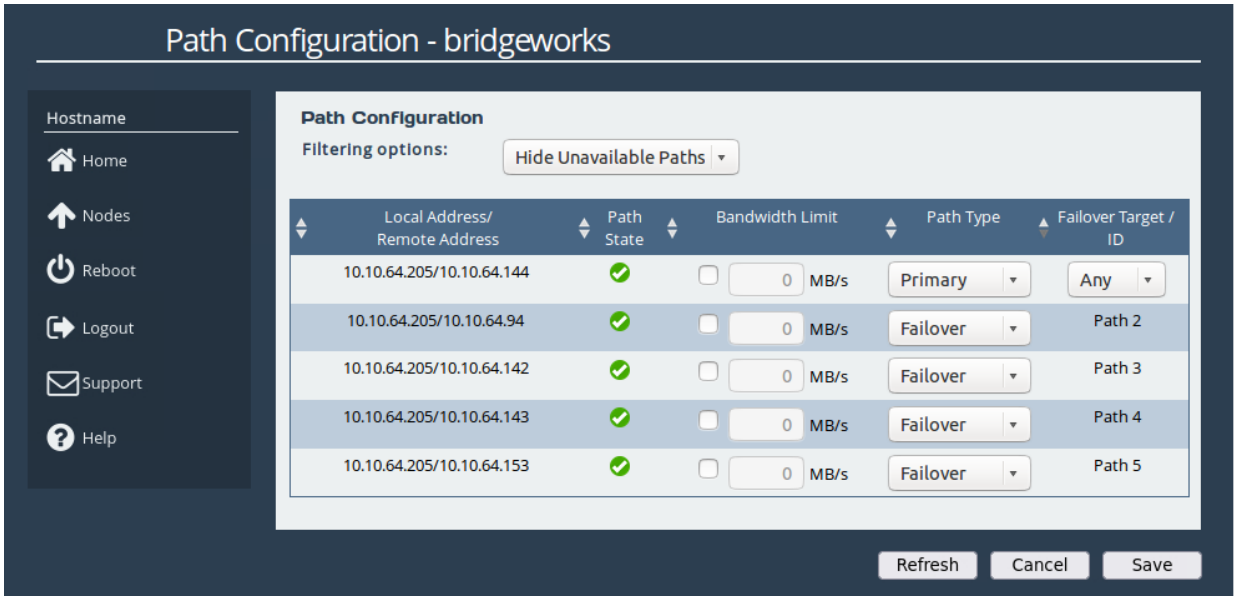
4.2.4 Path Configuration

The WANrockIT Node will always attempt to get the best performance possible for the data it is transferring. Upon establishing a connection between two WANrockIT Nodes, an automatic check for other connections through their WAN ports will occur.

To view and modify link settings between two Nodes, navigate to the *Path Configuration* page from the management page of the remote Node.

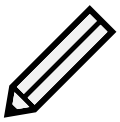


A table will be displayed showing all paths between the current Node and the remote Node.

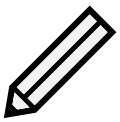


4.2.4.1 Setting Primary and Failover Paths

A path is a connection between two IP addresses when you establish a link between two WANrockIT Nodes. Once the “primary” path is established, the Nodes will then automatically check for other available connections to each other through their WAN ports. Any additional connections that are found will automatically be set as ‘failover’ paths. A failover path will not be used unless the primary path fails. You can also select a *Primary Failover* path which will be the first used in the event of a failure with the primary path. To choose a Primary Failover path, select the path that you wish to use from the *Failover Target/ID* drop down box on the far right of the path table.

	Note: The order in which failover paths are used, after any initial Primary Failover path, is set automatically and cannot be manually changed.

To change the primary path, click on the *Path Type* drop-down of the primary path and select *Failover* from the drop down list. Click on the *Path Type* drop box of the path that you wish to set as the new primary path and select *Primary* from the drop down list. Click on *Save* to save your changes.

	Note: Multiple links can be assigned as “primary paths”; the WANrockIT Node will automatically attempt to use all available primary links simultaneously. There must be at least one primary path designated at any time.

An icon in the *Path State* box will indicate the state of each path:

Link Up Represents a known link that is up.

Known Link Down Represents a known link that is down.

Unavailable Link Represents a possible link that has not been connected to.

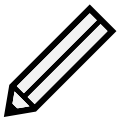
4.2.4.2 Filtering options

By default, this page will hide unavailable paths. In order to show unavailable paths, select *None* from the *Filtering options* drop-down.

4.2.4.3 Configuring a Node's Bandwidth

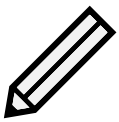
If there is other traffic on your network that needs to access a share of your bandwidth, you can limit the bandwidth between your Nodes. The limit is applied on a per path basis.

To set a limit on a connection, select the *Bandwidth Limit* checkbox next to the connection that you wish to limit. This will enable the bandwidth limit field next to the checkbox. Enter a value in megabytes per second and click the *Save* button.



Note: The minimum bandwidth limit you can set is 1 MB/s.

To remove a *Bandwidth Limit* untick the *Bandwidth Limit* checkbox on the desired connection, and click *Save*. The limit will then be lifted. A bandwidth limit of 0MB/s indicates that no restriction is being applied.



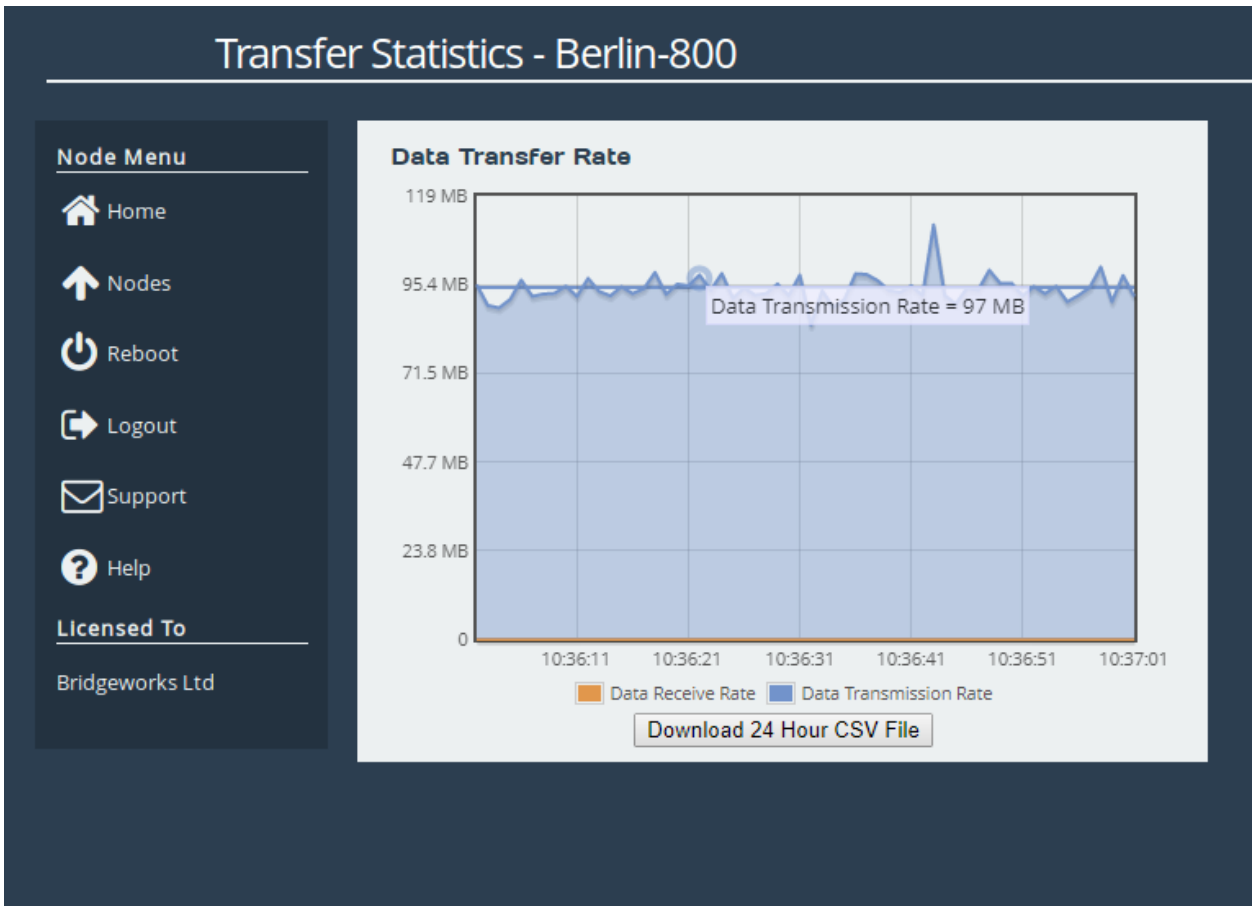
Note: Any changes to the bandwidth limit will become effective immediately on pressing *Save*.

4.2.5 Node Specific Transfer Statistics

This page allows you to monitor, in real time, the performance of the link between your Node and a remote Node.

Navigate to the management page of the remote Node and click the *Transfer Statistics* icon.

The web interface will then display the following window:



4.2.5.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.

	Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.2.5.2 Download 24 Hour Transfer History

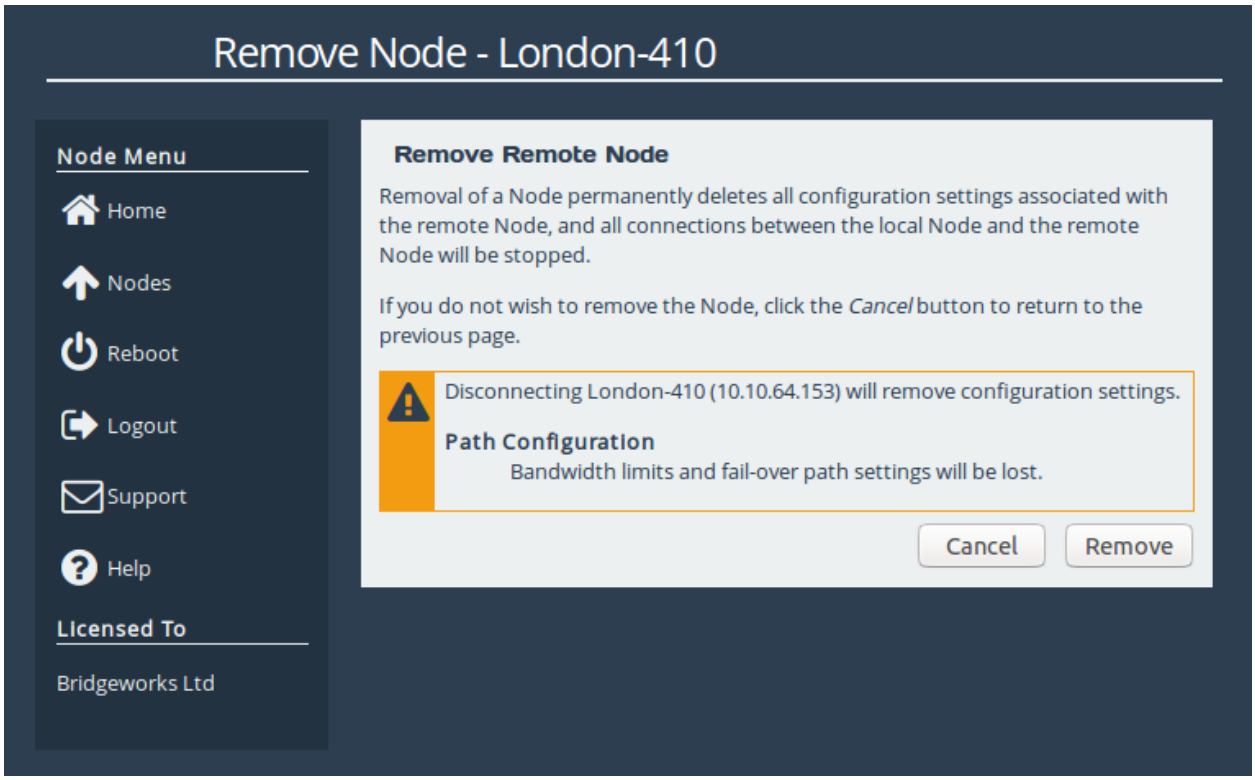
You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Download 24 Hour CSV File* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix F: Transfer Statistics Graphing Instructions for Excel 2010 for information on viewing this file.

	Note: The 24 hour statistics are cleared on reboot.

4.2.6 Remove Node

To remove outgoing configurations for a remote Node, navigate to the management page of the remote Node and click the *Remove Node* icon.

The following page will be displayed:



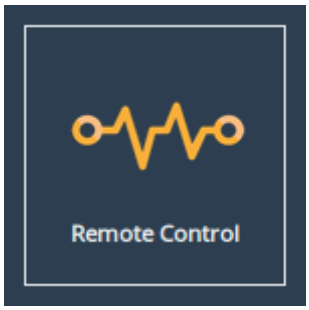
This page allows the administrator to disconnect from a remote Node, removing it from the list of connected Nodes and permanently deleting all outgoing configurations to that Node. To disconnect from a remote Node, click the *Remove* button.

Disconnecting from a Node will immediately terminate traffic between the local and remote subnets, and you will lose any configured Node settings that may have been set.

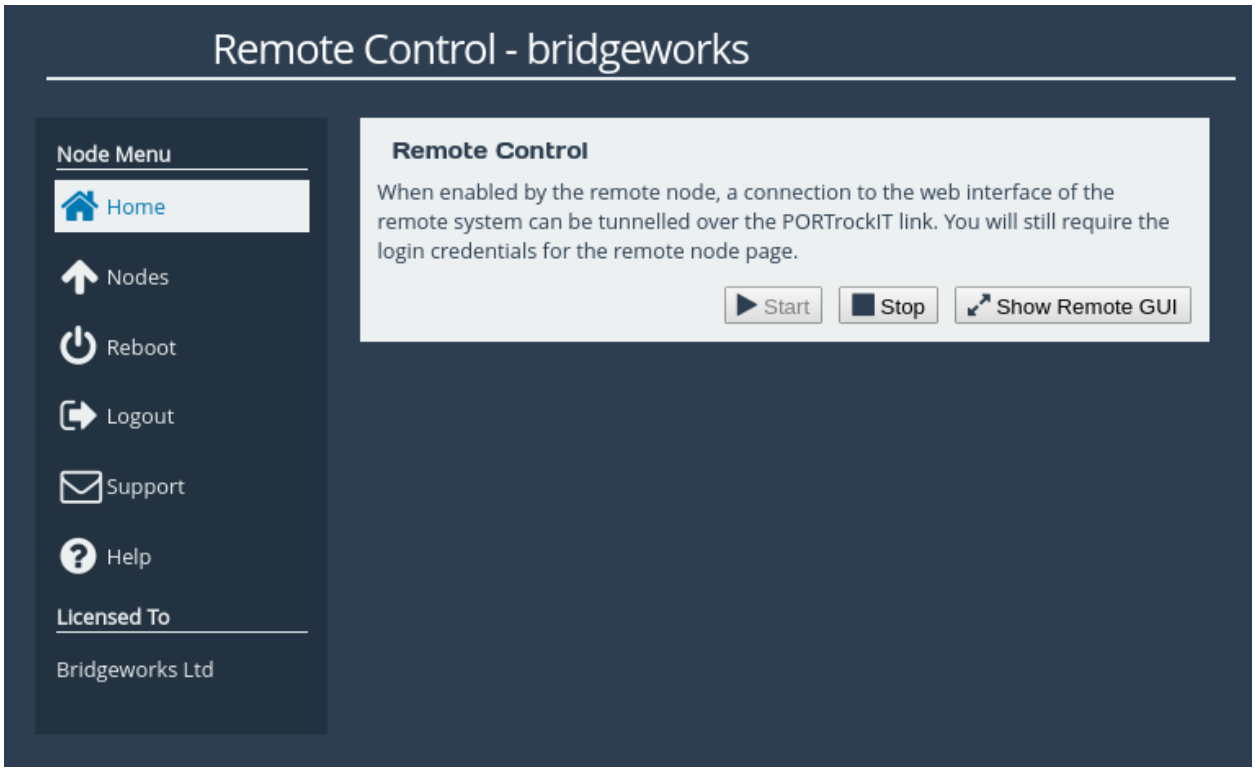
4.2.7 Remote Control

This page allows remote web interface access to a Node, which is useful when it is not possible to directly access the web interface of a remote Node.

To use remote control functionality, go to the management page of the remote Node and select the *Remote Control* icon.

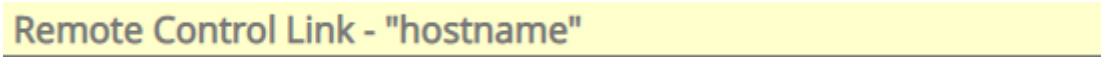


To enable remote control, click the *Start* button.



The web interface will appear in a new window or tab, displaying the login screen of the remote Node. At the top of the web page will be a yellow bar displaying the name of the remote Node you are connected to. The rest of the page will display the login screen of the remote Node. You can log in with the remote Node's usual credentials.

	Important: Your web browser may prevent the new window from appearing. Consult your web browser's documentation for information on how to allow the new window.

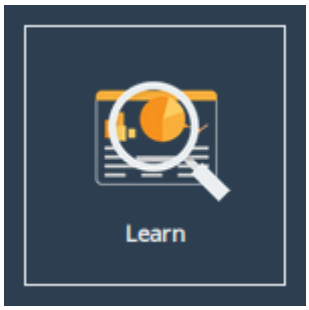


If you close the remote Node window with an HTTP connection, the session will continue to run. You may resume an HTTP remote session at any time by returning to the remote Node page and clicking the *Show Remote GUI* button. An HTTPS remote session to a Node will require reauthorisation if the session is left. To stop a remote Node session, click the *Stop* button.

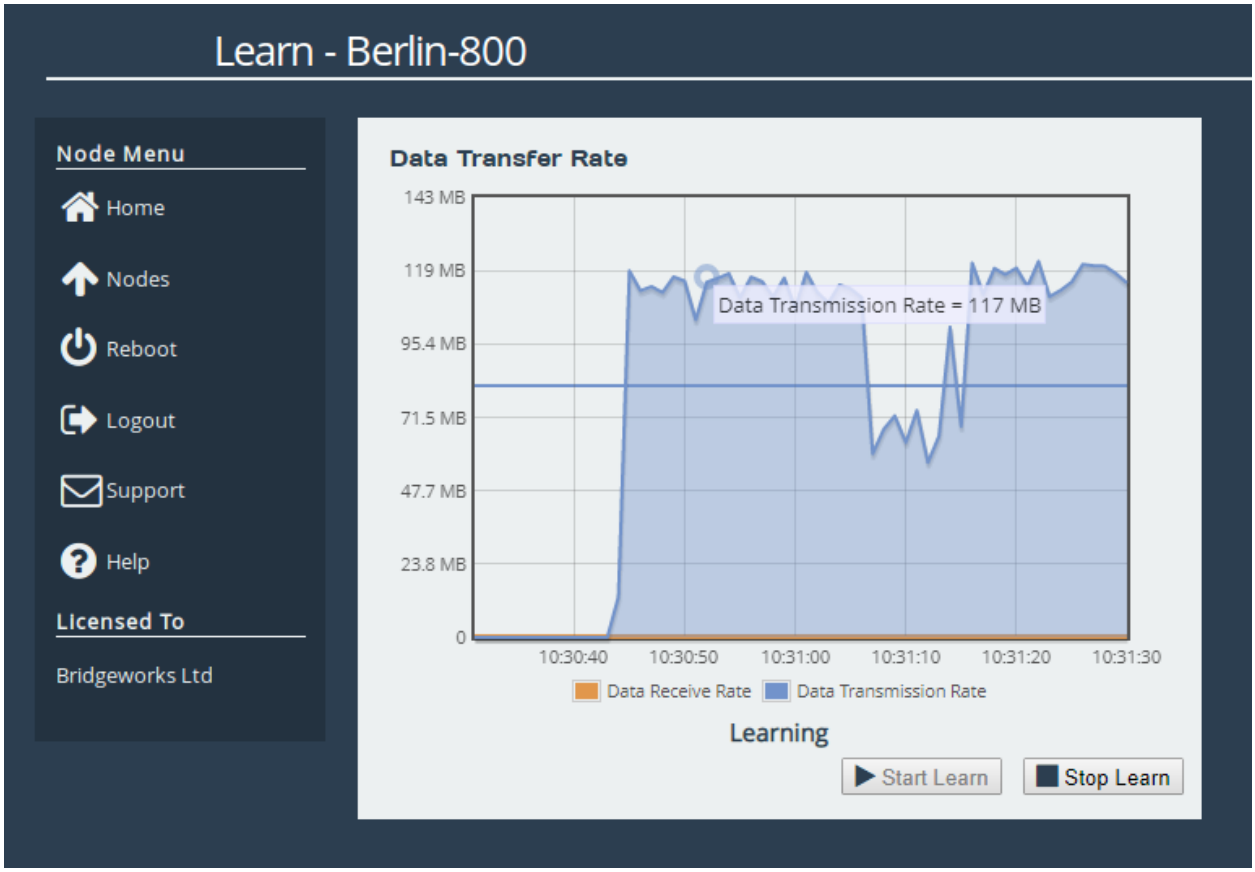
4.2.8 Learn

The learn procedure will initiate the *Artificial Intelligence* module, analysing the characteristics of the link network. Once it has completed, it will store these values to improve future data transfers.

A learn can be started by navigating to a Node's management page and selecting the *Learn* icon.



Clicking the *Start Learn* button will begin the learn procedure. A graph of the data transferred during the process will be displayed:



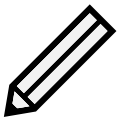
The learn process will take approximately five minutes. Navigating away from this page will not terminate the learn. The learn procedure can be run concurrently for multiple Nodes.

	Important: Running a Learn operation uses large amounts of data between this Node and the remote Node, and thus may incur data charges.

Once the learn procedure is complete, the status message below the graph will read *Learn Successful*. A learn can be terminated before completion by clicking the *Stop Learn* button.

4.2.8.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.

	Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.2.9 SCSI Devices

This configuration page will allow you to force a refresh of any SCSI devices that may have been added to the remote Node.

From the management page of the remote Node, select the *SCSI Devices* icon under the *Applications & Utilities* section.

The web interface will then display the following:

4.2.9.1 Restoring of Devices

When a Node has been restarted and is in the process of re-establishing its link to another Node, the Node's name, and the name of any connected devices, may have *(Connecting)* after them as shown:

All the functionality that can be used when a Node is active can be used whilst a Node is connecting but the effects will not occur until the link is up.

4.2.9.2 Disabling a Device

To disable a device from the remote Node, uncheck the *Enable* checkbox. All connected devices can be disabled at once using the *Disable all Devices* button.

4.2.9.3 Enabling a Device

To enable a device from the remote Node, check the *Enable* checkbox. All connected devices can be enabled at once using the *Enable all Devices* button.

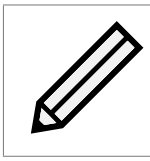
4.2.9.4 Refreshing SCSI Devices from a Remote Node

To refresh the list of devices, click on the *Refresh Devices* button at the bottom of the screen. A loading dialog box will appear as shown:

Once the refresh process has completed, a dialog box will appear to notify you about the connected Node and attached devices, as shown:

SCSI Devices - London-410
Node Menu
Home
Nodes
Reboot
Logout
Support
Help
Licensed To
Bridgeworks Ltd
Connected Devices
Device Name
Enable
naa.200000041b6f09aa
eui.500041b0000000002: (Connecting)
eui.500041b0000000003: (Connecting)
eui.500041b0000000004: (Connecting)
Refresh Devices
Connected to Node
Host Name bridgeworks
With 1 SCSI devices
OK
Go to Node Management

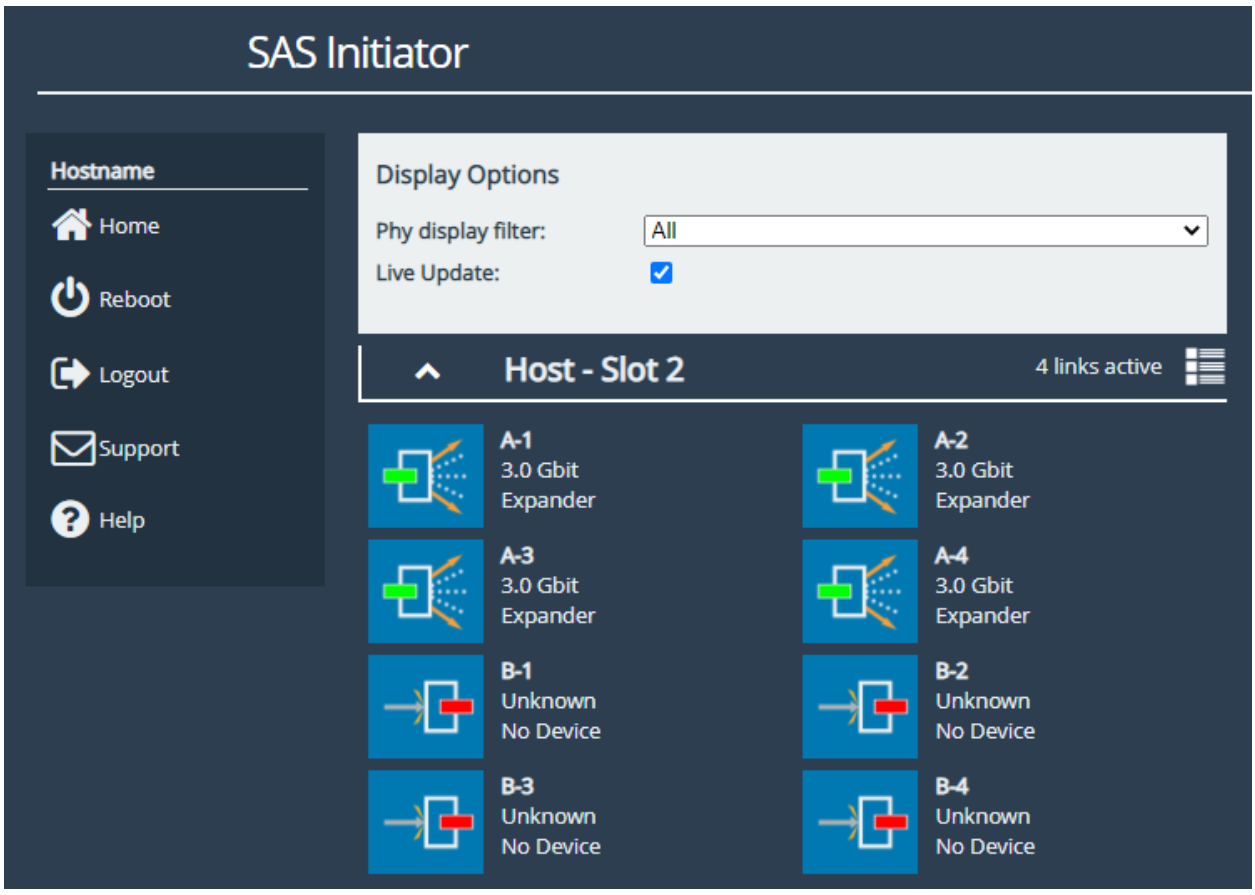
5 SAS Initiator

	Note: You may skip reading this section if your WANrockIT Node does not have a SAS feature card installed.

This section details the information displayed on the *SAS Initiator* page. This page allows the administrator to examine physical connections (hereinafter referred to as “phys”) from their SAS devices.

From the Home screen of the web interface, select the *SAS Initiator* icon from the *Devices and Protocols* section.

You will see the following page:



Note: The *SAS Initiator* page may look different than pictured depending on your configuration.

5.1 SAS Initiator Page

This page displays physical SAS cards (or “hosts”) contained within your unit, and any devices to which they are connected (such as disk drives or expanders). A host will contain four phys for every physical port on the card.

5.1.1 Hosts

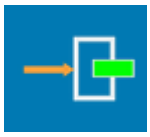
The heading of a host section shows the following information:

Chevron An arrow for expanding or collapsing the section.

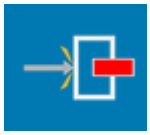
Name (e.g. Host 1).

Active Connections A display of the number of connections available (e.g. 4 links active).

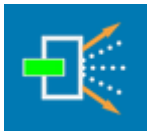
Under the host heading, a number of phys will be displayed. The icon represents their state.



End Device A device is connected



No Device No device is connected



Expander Device An expander is connected

The text to the right of each icon displays information relating to the phy:

Device identifier The identifier of the device, shown with a letter and a number (e.g. “B-3”). The letter pertains to the physical port, as displayed on your port mapping page.

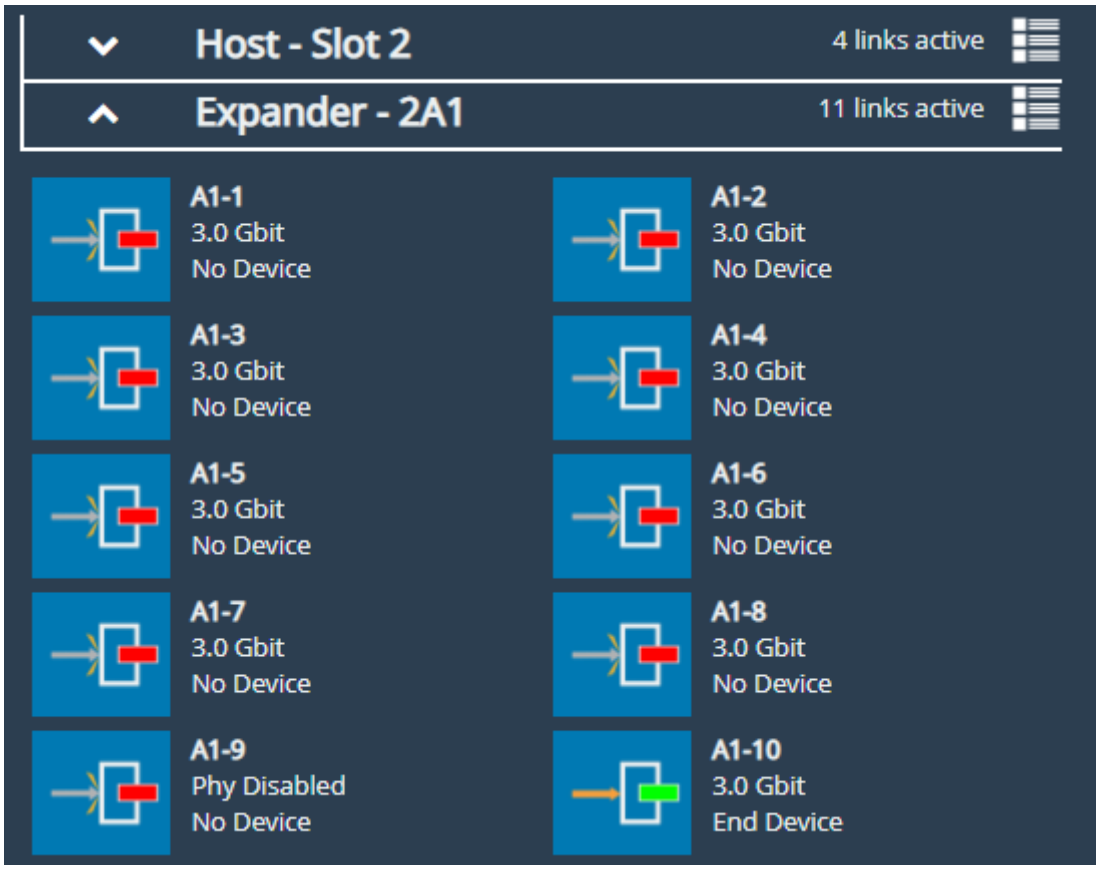
Link speed The negotiated link speed of the device. This will show a speed if a physical connection is made (e.g. “6.0 Gbit”), or otherwise displays “Unknown”.

Device type Whether there is an end device, no device, or expander (as represented by the icon).

If expanders are connected to a host, they will appear in their own sections starting underneath all listed hosts. The header contains number and letter designations pertaining to host it is connected to. For example, the **1**st expander connected to port **A** of Host **2** will be labelled “SAS Expander - 2A1”. The display of the heading and the phys of an expander mirrors the host phys exactly.

5.1.2 Expanders

Expanders are displayed in a similar manner to hosts. The title bar continues to show a chevron, the name of the expander, and the links active. All the phys of expander are shown underneath this heading, using the same icons as hosts.



The name of an expander signifies its origin, and its level. For example, an expander named **2A1** originates from the **2**nd host, from physical port **A**, and is the **1**st level of expander from that port.

Phys from an expander are similarly named. A phy from expander **2A1** may be labelled **A1-12**, where **A** represents the physical origin port, **1** represents the level of expander from that port, and **12** represents the number of the phy.

5.1.3 Display Options

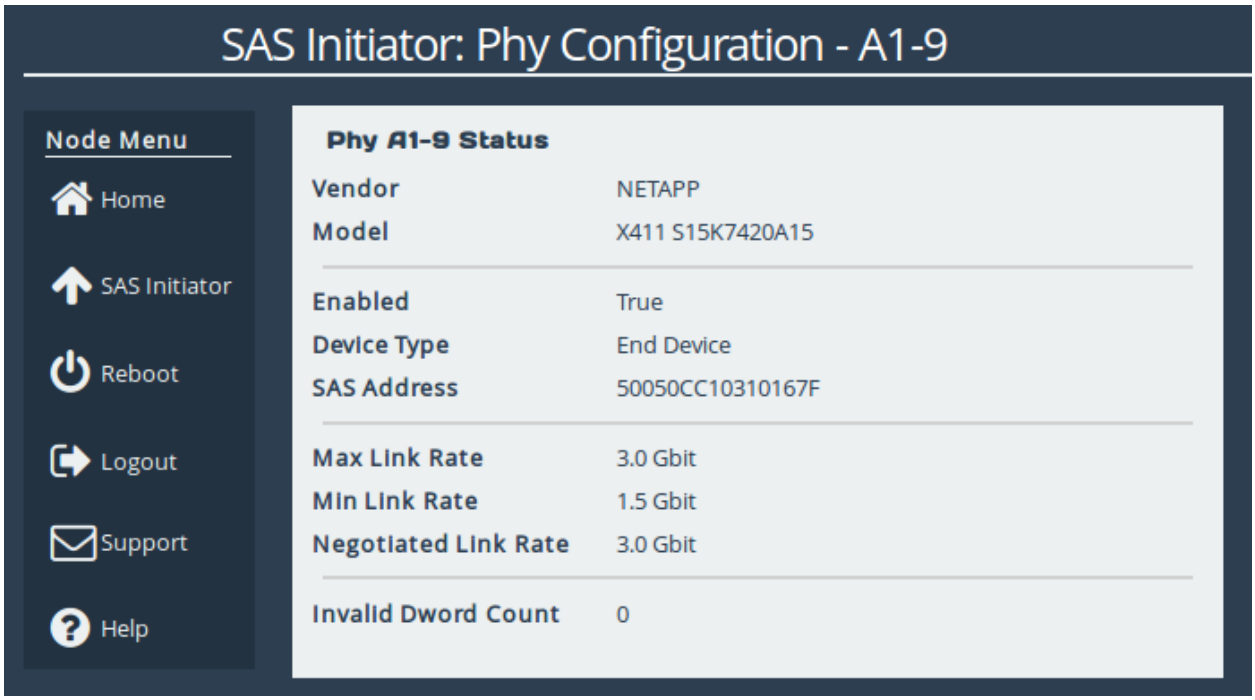
Options are available for configuring how devices are viewed. These are:

Phy display filter Show all phys, or choose to display phys based on whether they are connected.

Live update Ticked will update all phy information on the page every two seconds. Unticked will leave device information as it is at the time of unticking.

5.2 Phy Status Page

Clicking on a phy, either under a host or an expander, will lead to a status page showing information about that phy, as shown below. This shows information about the device as it was at the time of page load.



Information differs per connected device and not all fields will show on the page. Possible data includes:

Vendor Manufacturer of the device.

Product Product name of the attached expander.

Model Model name of the attached end device.

Enabled True or false.

Device Type No device, end device, or expander.

SAS Address Unique address of the SAS host the phy is from.

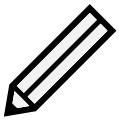
Max Link Rate Maximum link speed allowed by the hardware.

Min Link Rate Minimum link speed allowed by the hardware.

Negotiated Link Rate Link speed currently used for transfers. Unknown if no link rate has been decided.

Invalid Dword Count Number of malformed Dwords received.

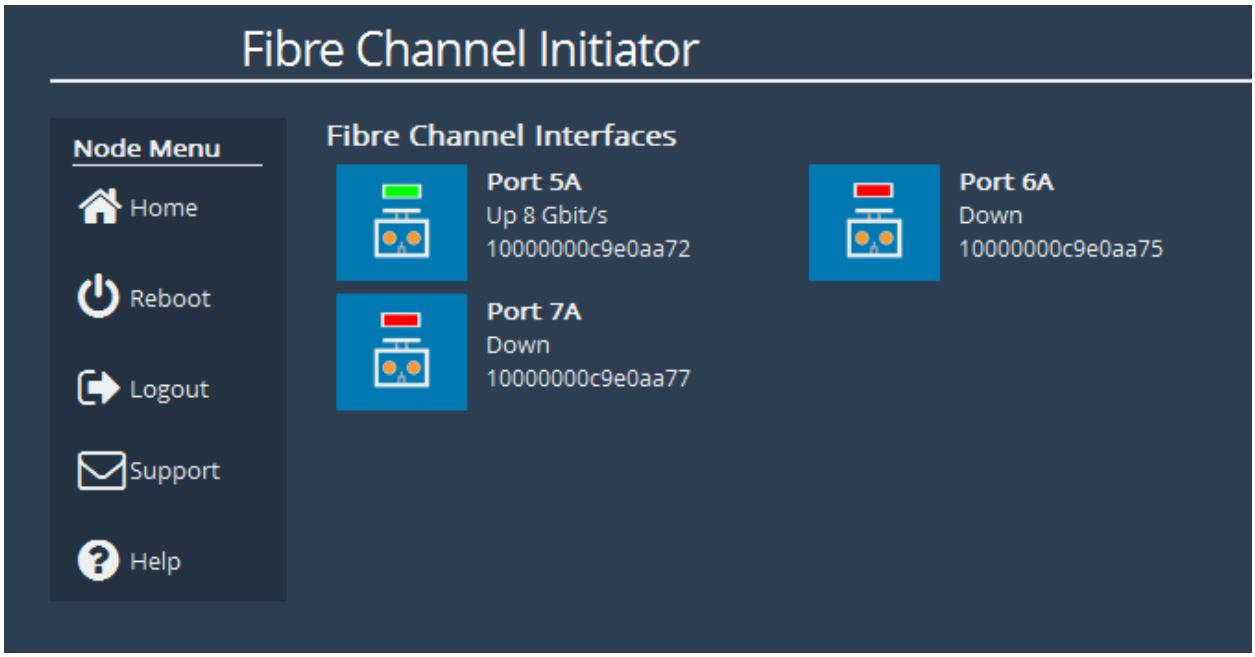
6 Fibre Channel Initiator Connections

	Note: You may skip reading this section if your WANrockIT Node does not have a Fibre Channel feature card installed.

This configuration page allows the administrator to configure ports designated as Fibre Channel Initiator interfaces. To designate a Fibre Channel port as an initiator, see Chapter 8: Fibre Channel Port Configuration.

From the Home screen of the web interface, select the *FC Initiator* icon from the *Devices and Protocols* section.

You will see the following page:



This page lists each Fibre Channel port which has been designated as an initiator. Three pieces of information are displayed about each port next to an icon. In order they are:

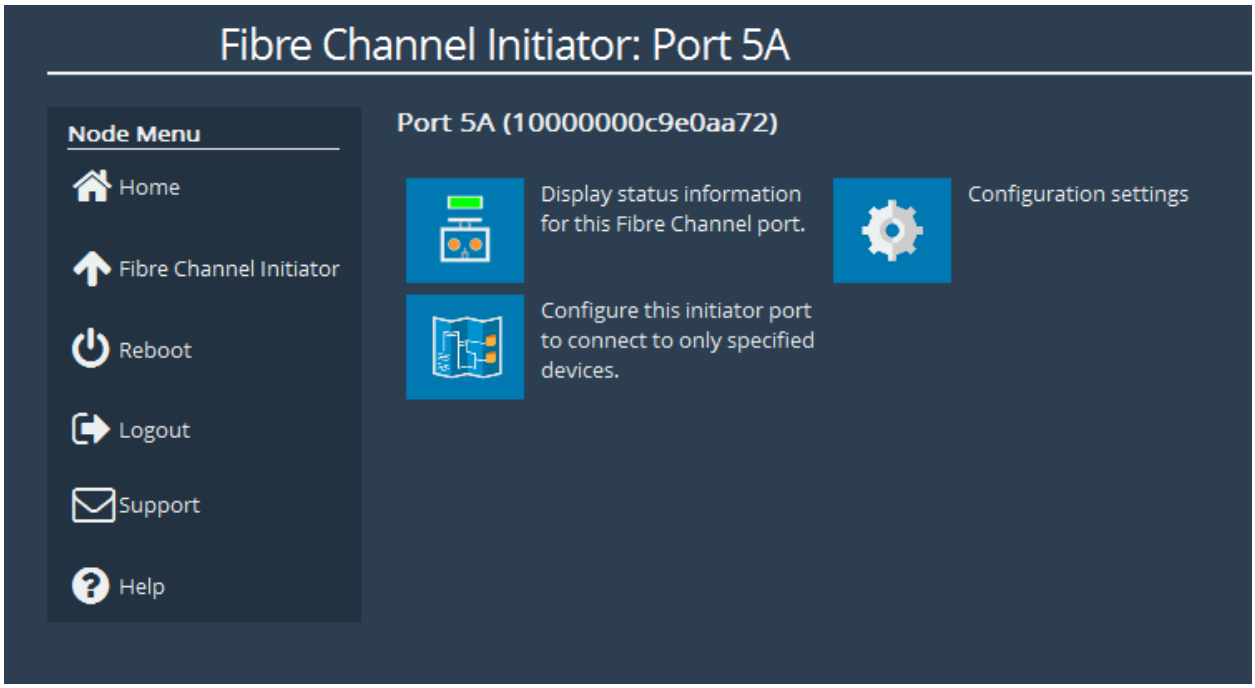
Port designation the number is the designation of the PCI slot, and the letter ‘A’ or ‘B’ denotes that this is the left, or right-hand port of that slot, respectively.

Current state This shows whether the Fibre Channel link for this port is up or down, and the speed

of the link if it is currently up.

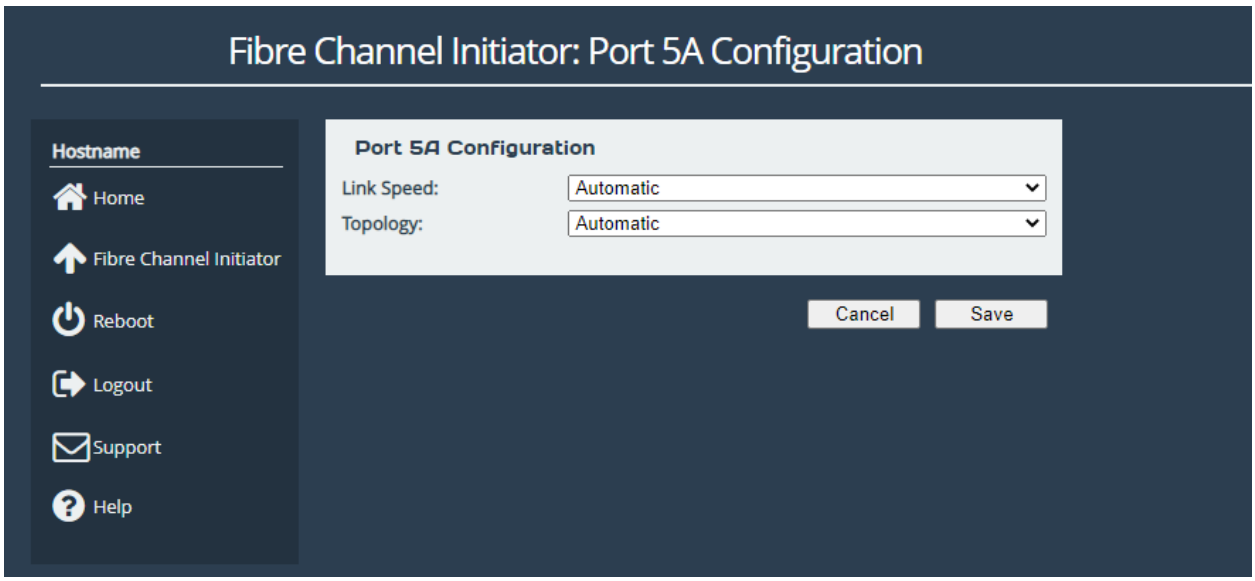
WWPN The unique World Wide Name identifier for this port.

Selecting one of the icons will navigate to the page for that initiator port, with 3 options:



Display status information for this Fibre Channel port allows you to see verbose information about the Fibre Channel port.

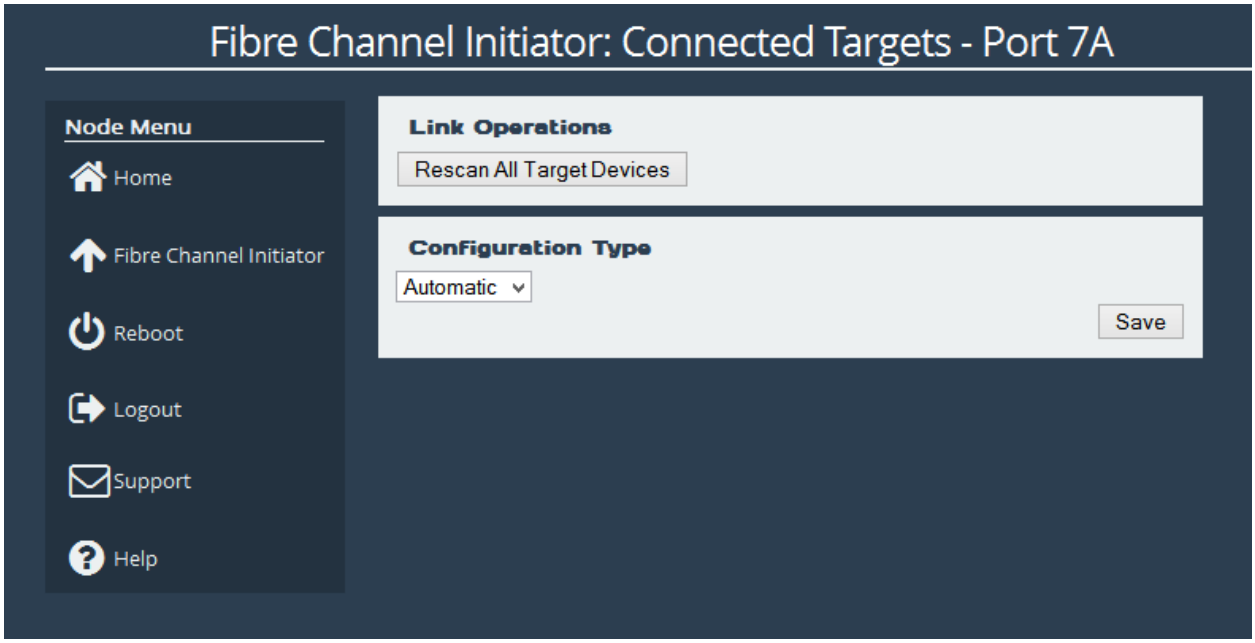
Configuration settings allows you to manually configure the *Link Speed* and *Port Topology*:



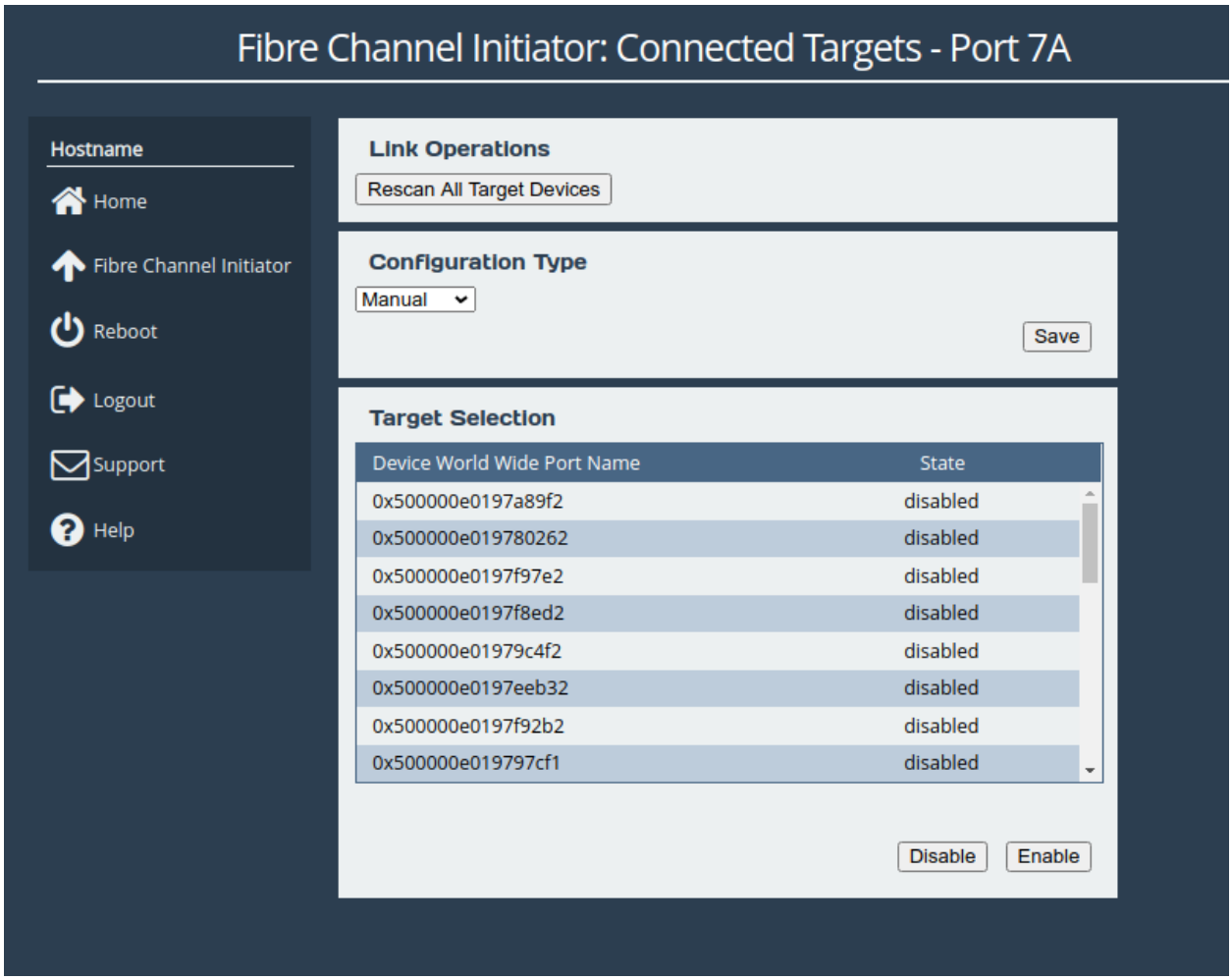
1. The *Link Speed* can be set to *Automatic* or one of the speeds supported by the Fibre Channel port. In most cases this option may be left set to *Automatic*. If you are unsure, set the link speed to the SFP speed. This option is not available on some products.

2. The *Topology* pull down menu has 3 options: *Automatic*, *Loop (arbitrated Loop, FC-AL)*, and *Point-to-Point (FC-P2P)*. It is recommended that you leave this option at *Automatic* unless you wish to force the link into a known topology.

Configure this initiator port to connect to only specified devices allows you to disable certain connected Fibre Channel targets.



The default configuration type is set to *Automatic*. Using the *Configuration Type* drop down, you can change this to manual. This allows you to enable or disable each individual target on the Fibre Channel link.



Select the FC target by clicking on its World Wide Port name, and then click *Enable* or *Disable*.

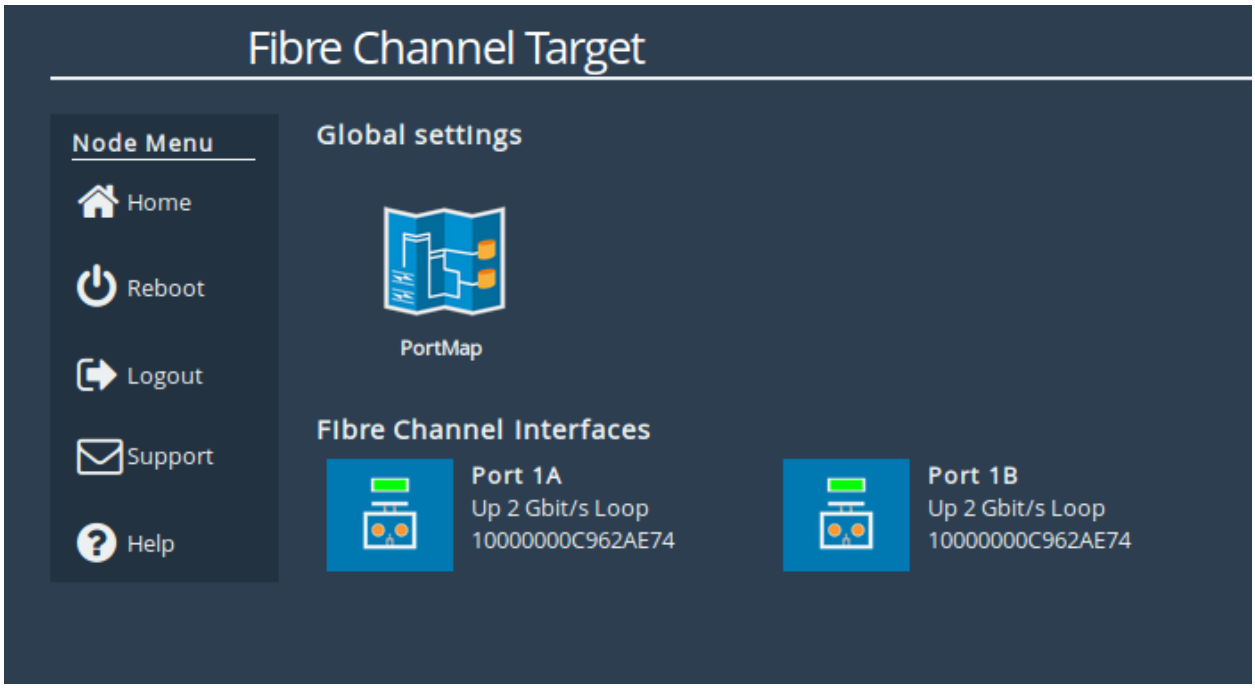
7 Fibre Channel Target Connections

	Note: You may skip reading this section if your WANrockIT Node does not have a Fibre Channel feature card installed.

This configuration page allows the user to configure ports designated as Fibre Channel Target interfaces. To designate a Fibre Channel port as a target, see Chapter 8: Fibre Channel Port Configuration.

From the Home screen of the web interface, select the *FC Target* icon from the *Devices and Protocols* section.

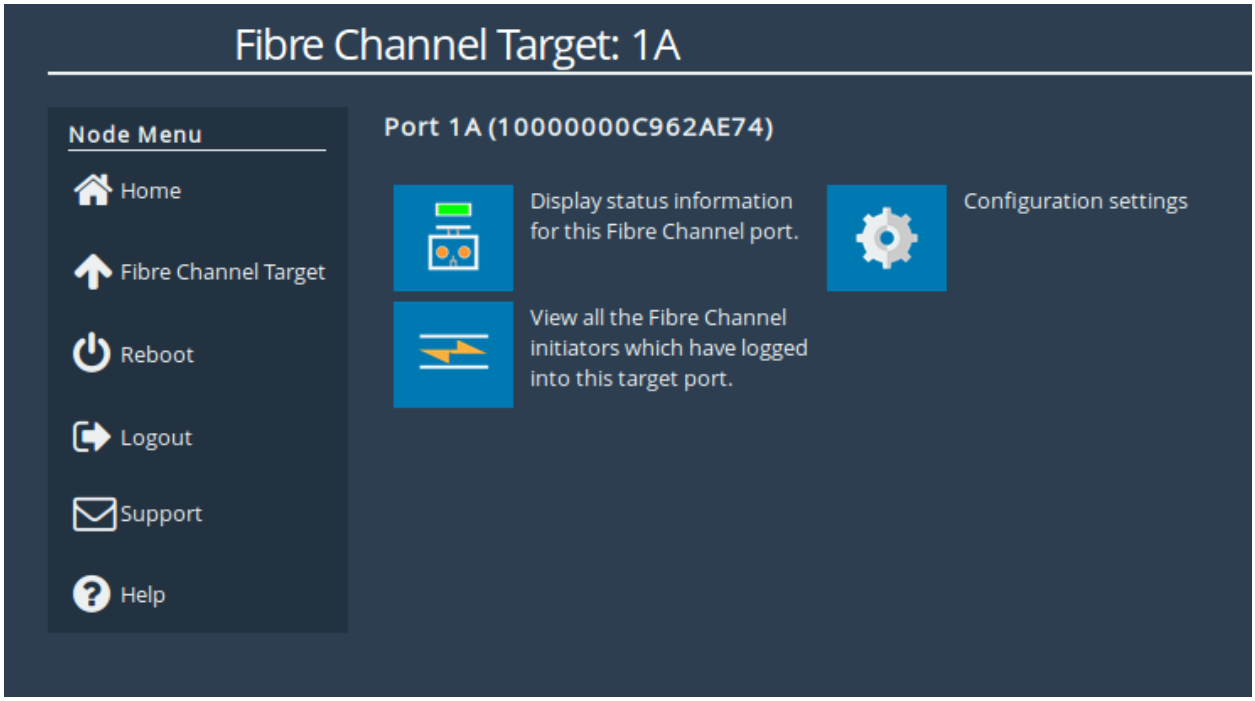
The web interface will then display the following:



The icons displayed in the *Fibre Channel Interfaces* section show the current state of each Fibre Channel Port.

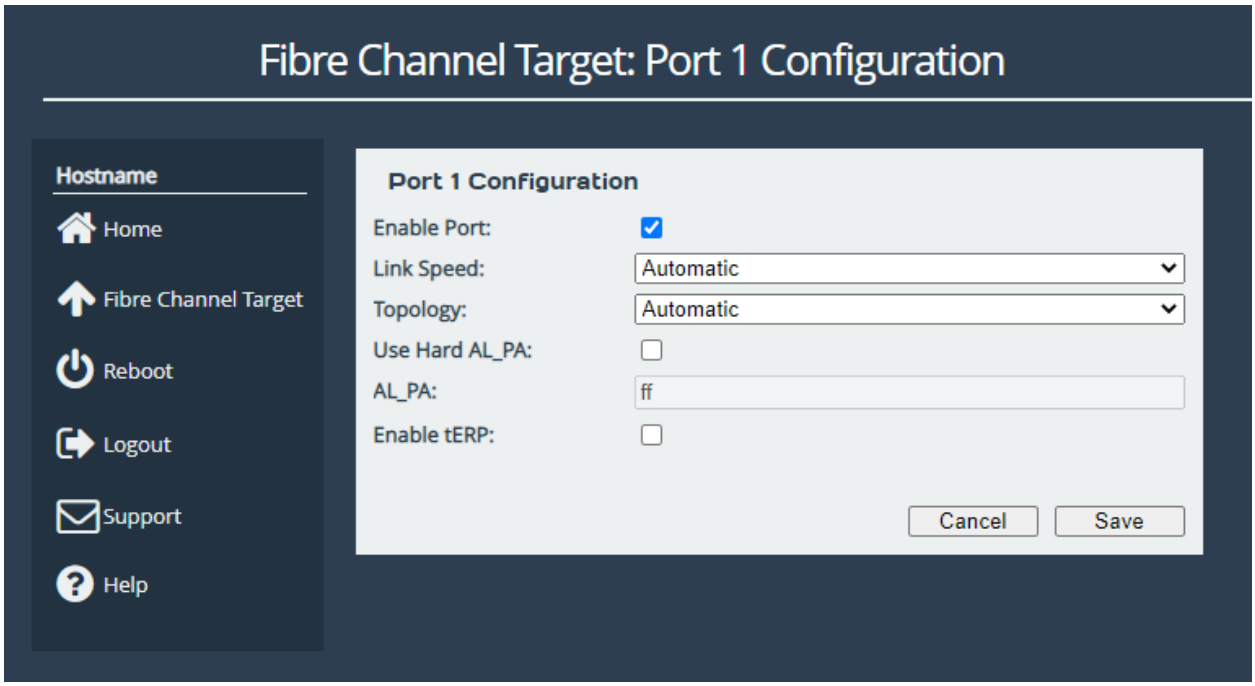
The green or red light in the icon display whether the port is up or down. This is also shown in text next to each icon with the negotiated Fibre Channel speed and the selected topology. The port WWN is also shown next to each icon.

Clicking on an icon will display different options related to the specific port as shown:



7.1 Port Configuration

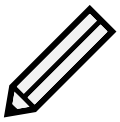
Selecting the *Configuration settings* icon will display the following:



The first parameter is the *Port Enable* check box. Check this to enable the link onto the Fibre Channel Storage Area Network (SAN).

The *Link Speed* drop down menu allows you to select the Fibre Channel network speed. In most cases this can be kept as *Automatic*.

The *Topology* drop down menu allows you to force the Fibre Channel topology when the Node logs on to the Fibre Channel SAN.

	Note: It is recommended to leave *Hard AL_PA* unchecked unless you are conversant with the lower levels of the Fibre Channel protocol, as certain AL_PA addresses are reserved.

The *Enable tERP* check box, which is only present for 8Gb/s cards, will enable or disable the Target Error Recovery Protocol for the port. tERP will attempt to recover frames that are missed or time out during transfer. For tERP to correctly function, the connected initiator must also support tERP.

Clicking *Save* will save the configuration to memory for use at the next reboot.

7.2 Connected Hosts

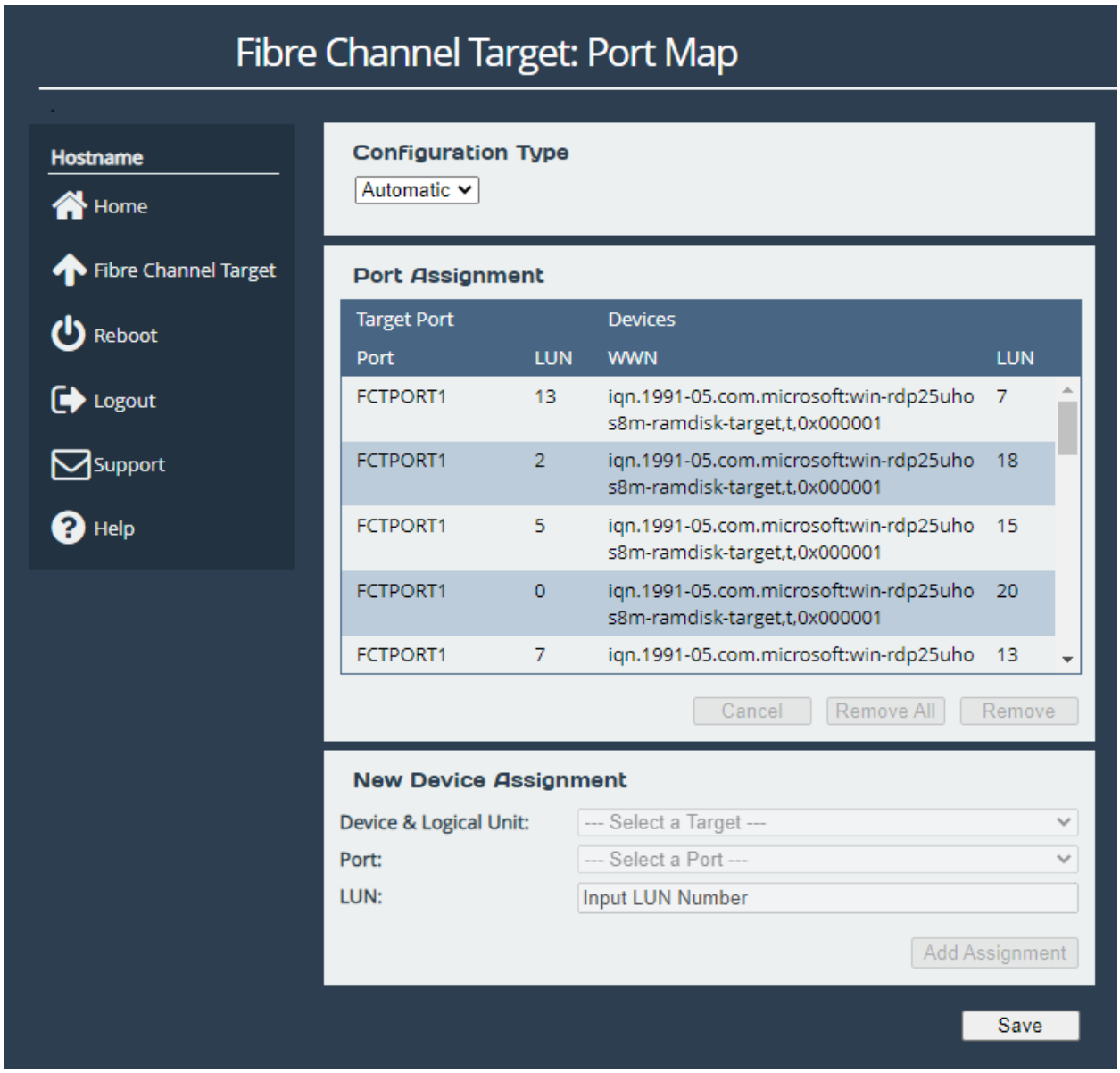
To list which hosts are connected to the Node, select a port under *Fibre Channel Interfaces*, then select the icon labelled *View all the Fibre Channel initiators which have logged into this target port*. The following will then be displayed:

7.3 Port Map

The *Port Map* page allows the user to assign devices to Fibre Channel ports with a fixed Logic Unit Number (LUN).

From the *Fibre Channel Target Management Console* page select the *Port Map* icon.

A screen similar to the following will be displayed:



There are two modes of operation:

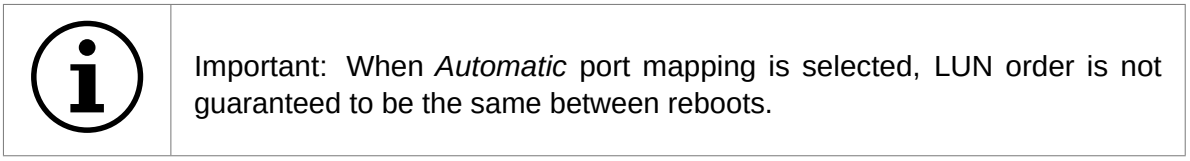
Automatic will assign all devices to all Fibre Channel target ports, so that any connected host will see all devices.

Manual will allow the user to manually assign which target devices appear on which Fibre Channel port.

When switching between modes all changes are held pending until the user selects *Save*.

7.3.1 Automatic

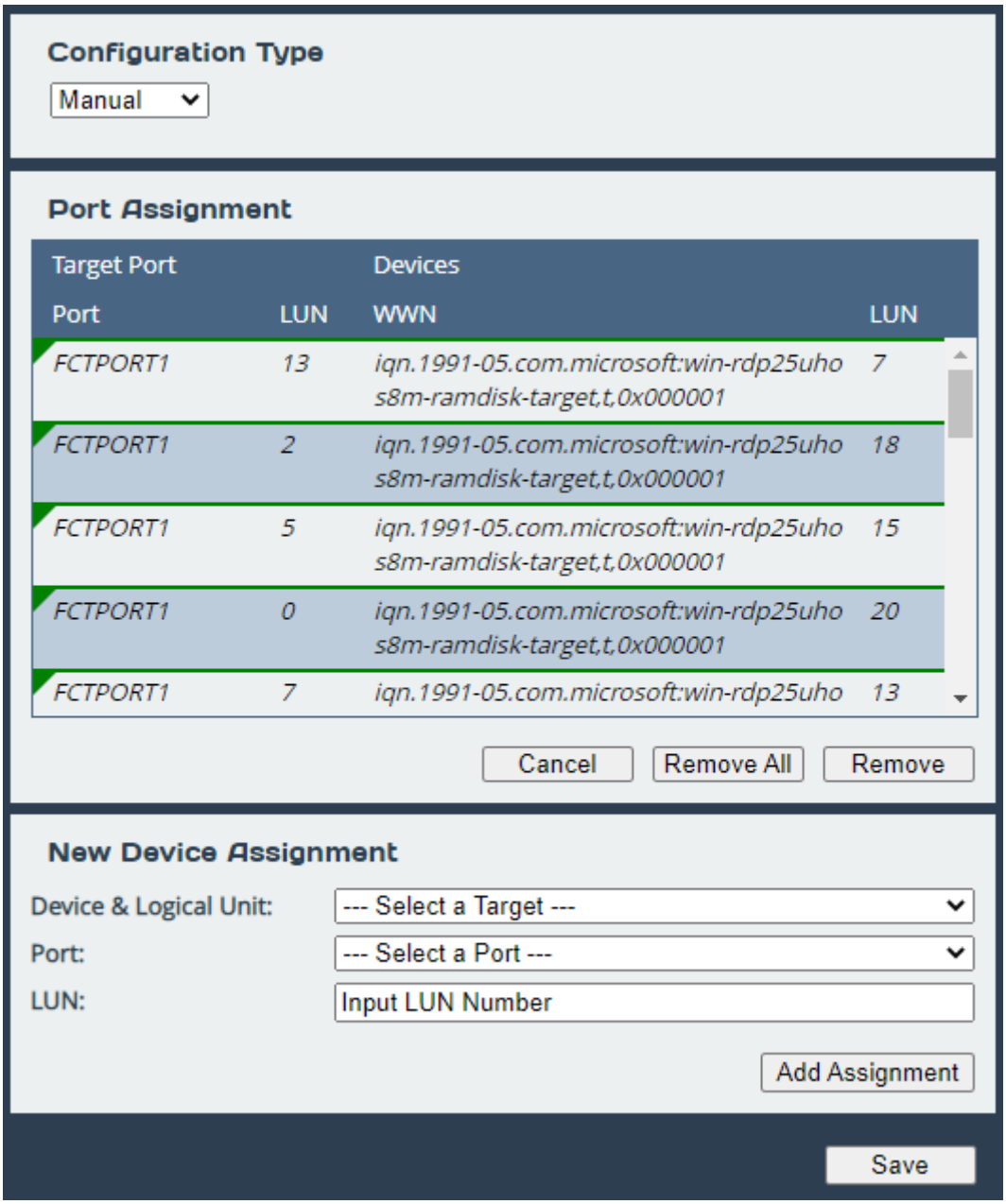
In this mode the *Port Assignments* table shows the active mappings. When switching from manual to automatic mode the display will show the manual mappings greyed out until user selects *Save* at which point they will be updated with the active automatic mappings.



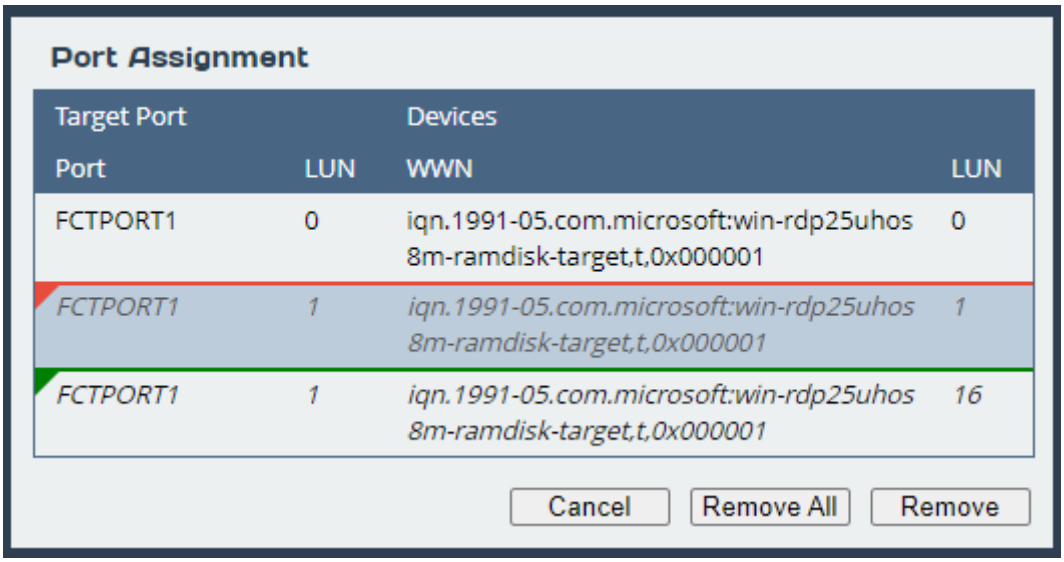
Important: When *Automatic* port mapping is selected, LUN order is not guaranteed to be the same between reboots.

7.3.2 Manual

Selecting *Manual* will show something similar to the following:



When switching from *Automatic* to *Manual* the mapping is prepopulated with the same settings as those currently active. Initially all entries are shown in green to indicate these are pending changes which will be added upon save. Similarly if the user deletes an active mapping it will be shown in red as a pending removal as shown in the following example:



To assign a target device to a Fibre Channel Port:

1. Select a target device from the list in the *Device & Logical Unit* drop down menu. Note that devices that are already mapped are greyed out.
2. Select which Fibre Channel Port you wish the device to appear on.
3. Select the LUN you wish the device to have on the selected Fibre Channel Port.
4. Click the *Add Assignment* button at the bottom of the panel.

To remove a mapped device, select the device from the table and click the *Remove* button below the table. To remove all mapped devices, click the *Remove All* button.

Selecting *Cancel* allows the user to abandon any pending changes.

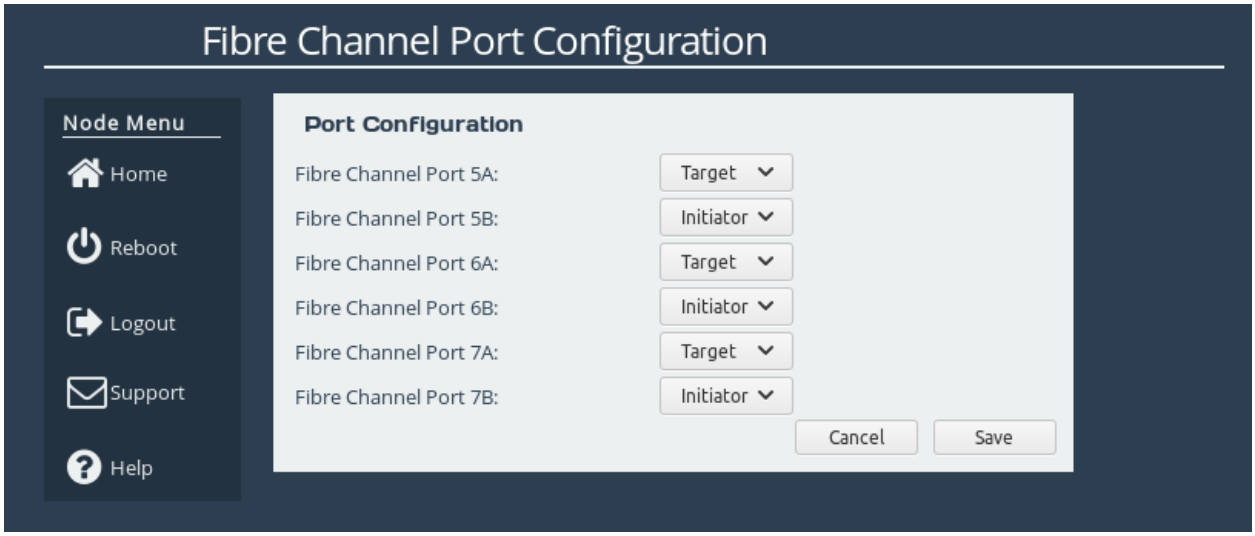
	Important: Manually assigned LUN mappings should be sequential and include a LUN 0 to ensure correct operation.

8 Fibre Channel Port Configuration

This page allows the administrator to designate whether a port is a target or an initiator.

From the Home screen of the web interface, select the *FC Port Configuration* icon from the *Devices and Protocols* section.

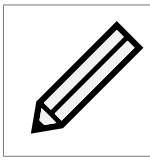
You will see the following page:



To change a port between a target or initiator use the drop down box next to the desired port and click on the *Save* button. Clicking *Cancel* will ignore any changes made on the page.

	Important: Changes to Fibre Channel Port designation will require a reboot to take effect.

9 iSCSI Initiator Configuration

	Note: You may skip reading this section if your WANrockIT Node does not have an iSCSI feature card installed.

This section details configurations for the iSCSI initiator. To help your understanding of iSCSI terms, please see Section 1.3: Definitions.

Adding a device to the iSCSI Node requires two basic steps:

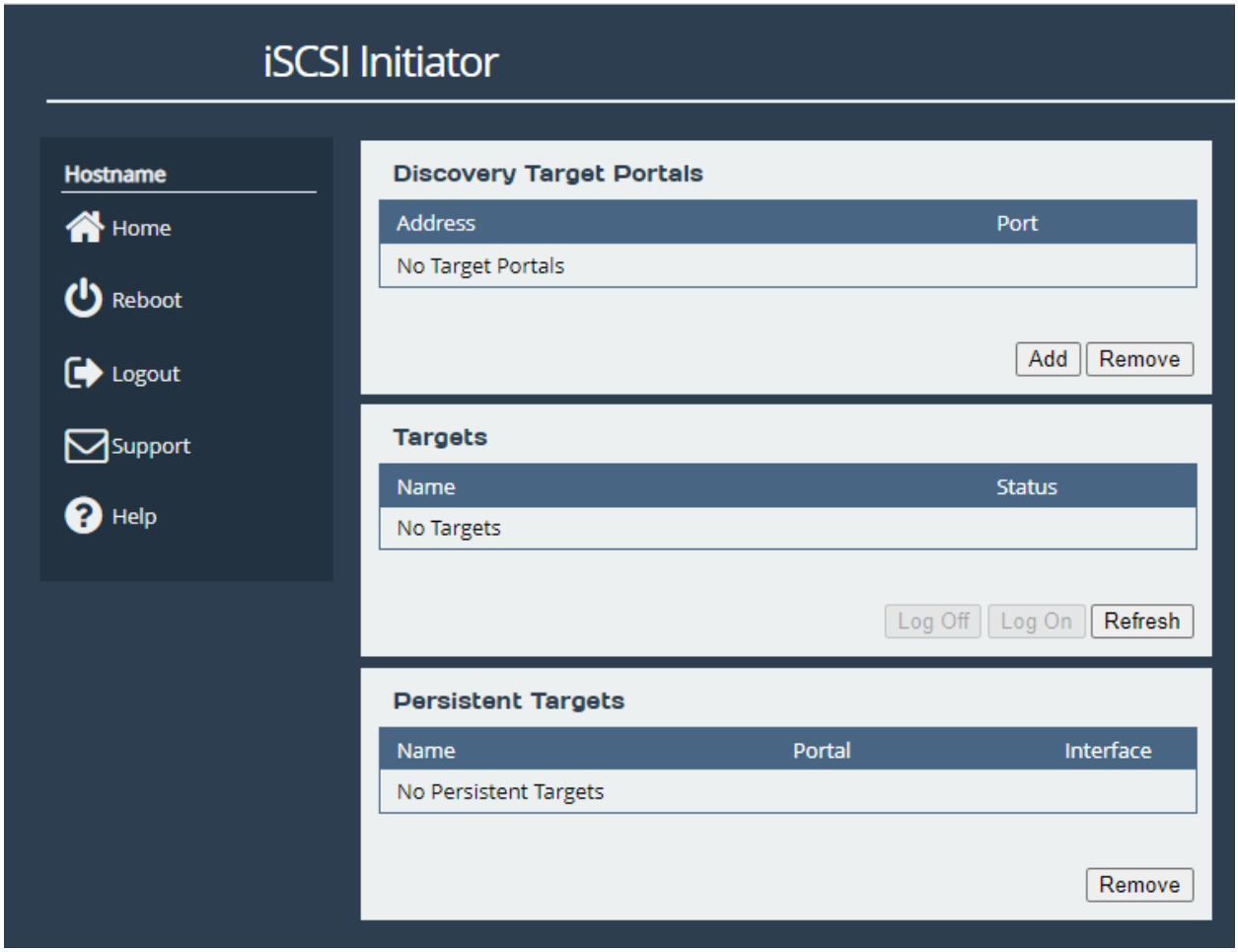
- Discover iSCSI target(s) on the target portal
- Log on to the iSCSI target(s)

The following sequence is repeated for each device you wish to connect to the iSCSI Node.

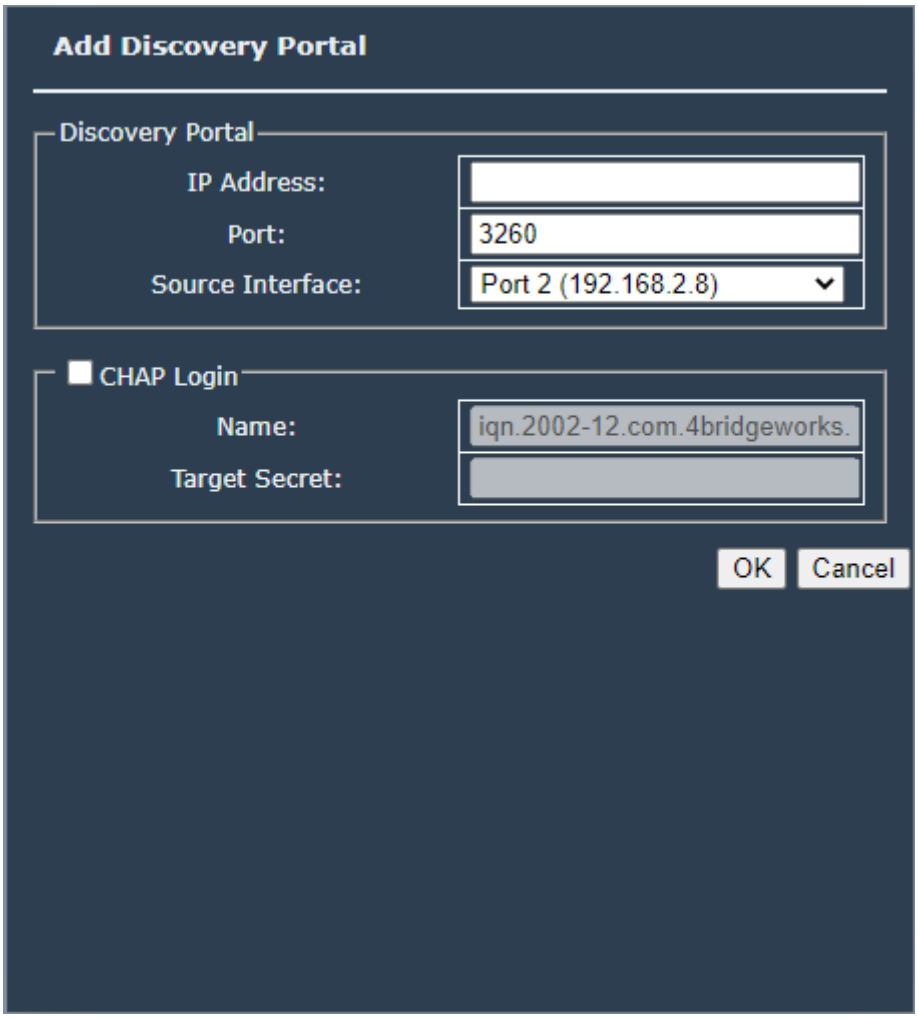
9.1 Discovering an iSCSI Target

From the Home screen, click on the *iSCSI Initiator* icon under the *Devices and Protocols* section.

The web interface will then display the following:



Click on the *Add* button in the *Discovery Target Portals* box. An *Add Discovery Portal* dialog box will then appear:



Insert the *IP Address* of the iSCSI target portal you wish to connect to and select the *Source Interface* from the drop down list.

If the iSCSI device has CHAP enabled for discoveries then you will need to check the *CHAP Login* box and fill in the name and target secret. When complete, click the *OK* button.

The Node will now perform an iSCSI Discovery. This will request the target portal to list the target devices connected to it. Any devices found will appear in the *Targets* list. If the iSCSI target has more than one device attached, then all of these devices will be shown.

In the example above we can see that the target portal with IP Address 192.168.2.4 has one device attached to it. The device's status is *inactive*, because the Node has not yet connected to it. To connect to the device, an iSCSI logon must be performed.

9.2 Removing an iSCSI Discovery Portal

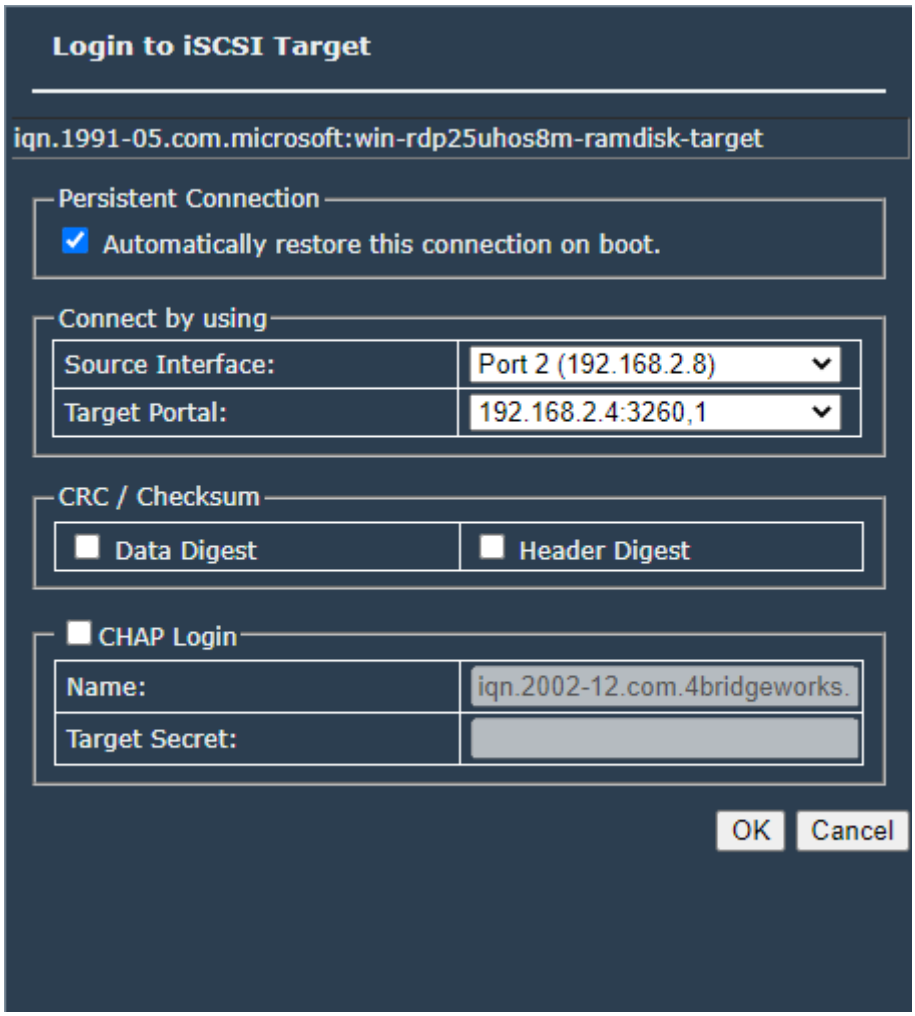
From the *Discovery Target Portals* list select the IP address of the target portal you wish to remove. The background colour of the IP address will change to yellow. Click the *Remove* button, and the following message will appear:

"Are you sure you want remove the selected discovery portal?"

Click the *OK* button to confirm.

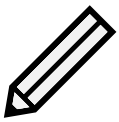
9.3 Log On to an iSCSI Target

To log on to an IQN, highlight the IQN by clicking on its entry in the *Targets* list and then click the *Log On* button. At this point a new window will appear, as shown:



9.3.1 Persistent Connection

If you wish for the Node to connect to this IQN after a reboot, select the *Automatically restore this connection on boot* checkbox. It is recommended that this feature is enabled.

	Note: Devices with *Persistent Connection* enabled will also be displayed in the *Persistent Targets* list below the *Targets* list.

9.3.2 CRC/Checksum

On the login page there are options in the CRC/Checksum section to enable *Data Digest* and *Header Digest*.

When Data Digest is enabled, the system performs a checksum over each Protocol Data Unit's (PDU's) data part and verifies using the CRC32C algorithm. This increases data integrity, but will impact performance.

When Header Digest is enabled, the system performs a checksum over each iSCSI PDU's header

part and verifies using the CRC32C algorithm. This increases data integrity.

9.3.3 CHAP Login

If the iSCSI target device has CHAP enabled, select the *CHAP Login* checkbox, enter the name and target secret to communicate with this device.

Once you have completed this window, click the *OK* button.

The Node should now display the IQN with the word *Connected* next to it. Repeat this process for all the required iSCSI target devices.

9.4 Log Off an iSCSI Session

From the *Targets* list, select the target you wish to remove. The background colour of the selected target will change to yellow. Click the *Log Off* button below, and the following message will appear:

“Are you sure you want to Log Off?”

Click the *OK* button if you wish for the target to become inactive.

9.5 Refresh Targets

If at a point after the initial discovery, a target portal has had additional targets added to it, the *Refresh* button will update the targets list to present those devices.

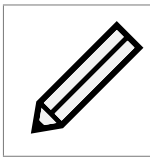
9.6 Remove Persistent Target

If a target has been made to be persistent, it will appear in the *Persistent Targets* list. To stop the iSCSI session from restoring on reboot, select the target from the *Persistent Targets* list. The background colour of the selected target will change to yellow. Click on the *Remove* button, and the following message will appear:

“Are you sure you want to remove the selected persistent target?”

Click the *OK* button if you wish to stop the iSCSI session from restoring on reboot.

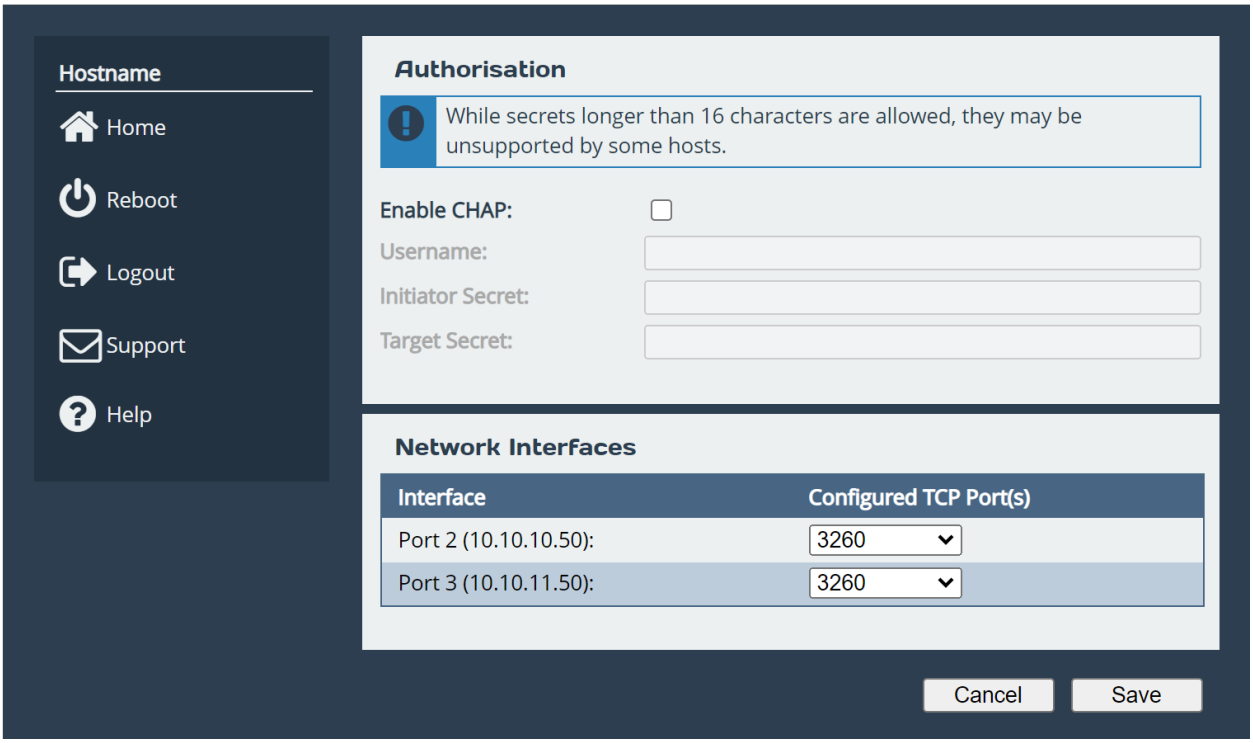
10 iSCSI Target Configuration

	Note: You may skip reading this section if your WANrockIT Node does not have an iSCSI feature card installed.

This page allows you to configure mutual CHAP authorisation, and TCP ports of each iSCSI target interface.

From the Home screen of the web interface, select the *iSCSI Target* icon under the *Devices and Protocols* section.

The web interface will then display the following:



10.1 Authorisation (CHAP)

CHAP is an authentication scheme used by servers to validate the identity of clients, and vice versa. When CHAP is enabled, the initiator must send the correct username and target password to gain

access to the iSCSI target of the Node.

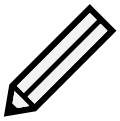
The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Bridge will authenticate itself with the initiator using the initiator secret.

To enable CHAP, select the *Enable CHAP* checkbox and enter the following details:

Username This is the same name as specified on the initiating host.

Initiator Secret This is the password defined on the initiating host. This must be 12 to 256 characters long. This should only be entered if mutual CHAP is enabled on the initiating host.

Target Secret This is the password that must be entered on the initiating host. This must be 12 to 256 characters long.



Note: While secrets longer than 16 characters are allowed, they may be unsupported by some hosts.

10.2 Network Interfaces

The table under the Network Interfaces section displays the interfaces and IP addresses the iSCSI target is presenting devices on.

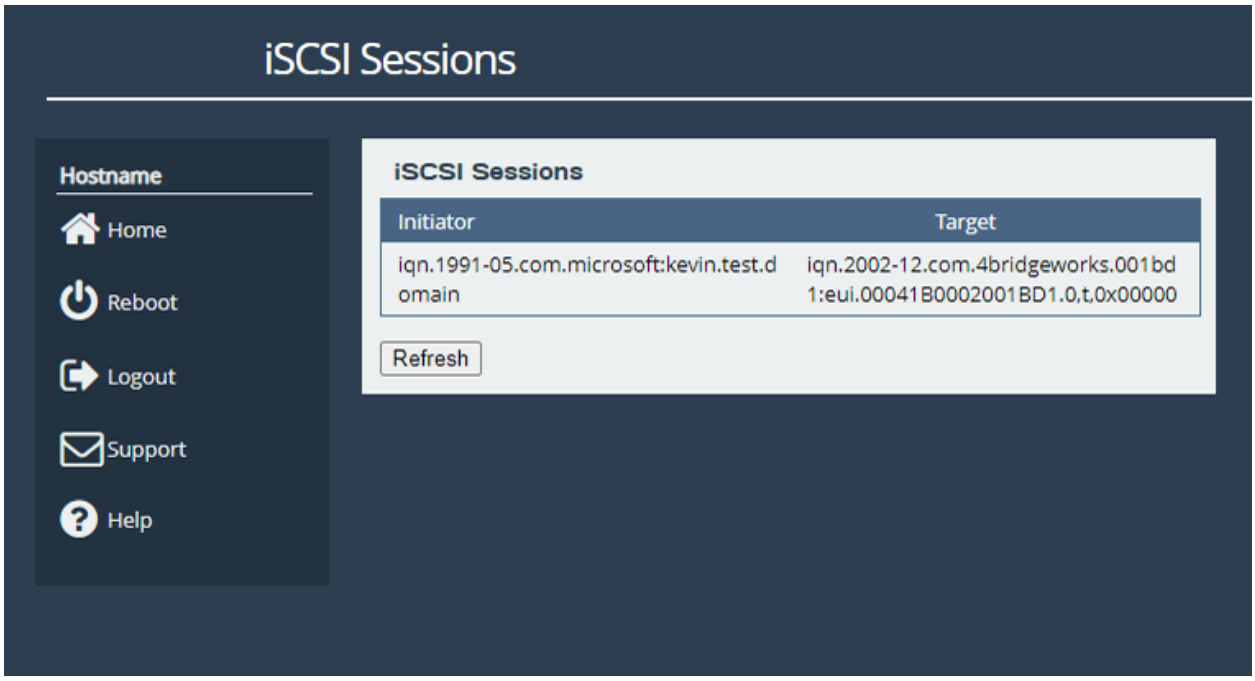
The iSCSI protocol officially uses two main TCP ports: 3260 and 860. For each iSCSI target interface, you can choose to enable either one these TCP ports, or both, or disable iSCSI on the interface completely, from the *Configured TCP Port(s)* dropdown.

10.3 iSCSI Sessions

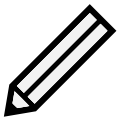
Each initiator will open at least one session with each target device it is logged on to. The iSCSI Sessions page in the web interface of the WANrockIT Node can be used to review these connections.

From the Home screen, select the *iSCSI Sessions* icon under the *Devices and Protocols* section.

The web interface will then display the following:



This page lists current connections to iSCSI initiators. The IQN of the initiator is shown in the *Initiator* column, and the IQN of the device it is logged on to is shown in the *Target* column. See Section 1.3.2: iSCSI Qualified Name (IQN) for more information.

	Note: It is possible that more than one initiating host may be connected to any target device, one host to multiple target devices, or one host has multiple connections to a single device.

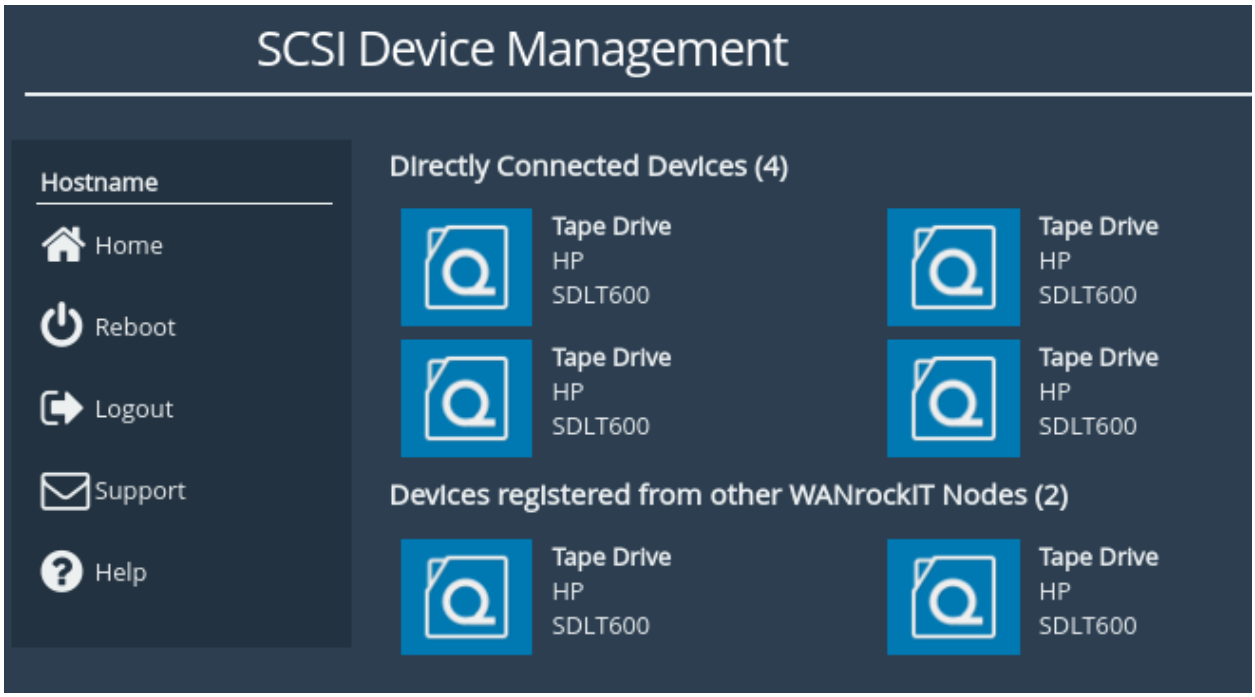
11 SCSI Device Management

This page allows you to view details of devices connected to the WANrockIT Node, and devices attached to a connected remote Node.

11.1 Viewing Attached Devices

From within the Home screen of the web interface, select the *SCSI Device Management* icon under the *Devices and Protocols* section.

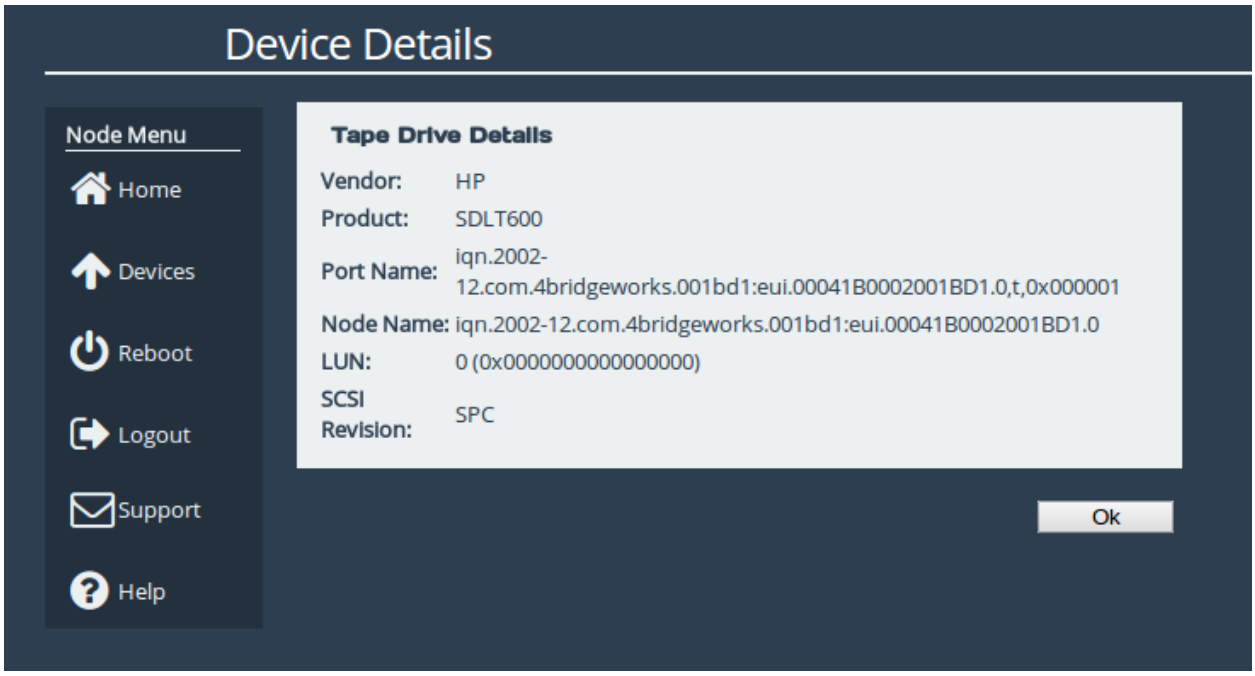
The web interface will then display the following:



You will be presented with a list of all the devices connected to the WANrockIT Node.

If your WANrockIT Node is connected to a remote Node, devices connected to the remote Node will also be displayed on this page under the *Devices registered from other WANrockIT Nodes* section.

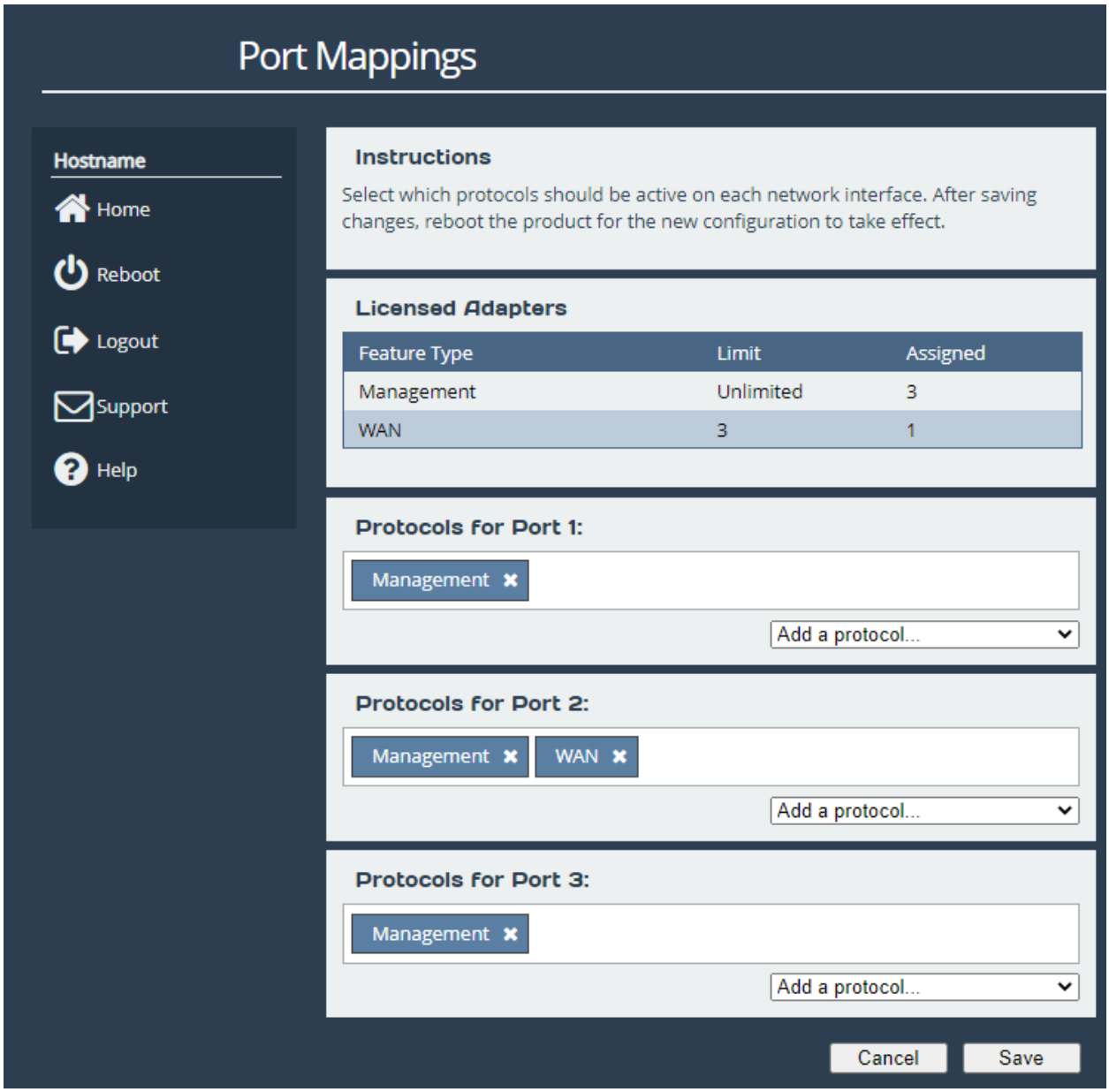
Clicking on a device will open a page displaying more information about the device, as shown below.


Device Details
Node Menu
Home
Devices
Reboot
Logout
Support
Help
Tape Drive Details
Vendor: HP
Product: SDLT600
Port Name: iqn.2002-12.com.4bridgeworks.001bd1:eui.00041B0002001BD1.0,t,0x000001
Node Name: iqn.2002-12.com.4bridgeworks.001bd1:eui.00041B0002001BD1.0
LUN: 0 (0x0000000000000000)
SCSI Revision: SPC
Ok

12 Port Mappings

Port Mappings allow you to configure which network ports will have support for which protocols. Navigate to the *Port Mappings* page from the main page of the web interface.

The web interface will display the following:

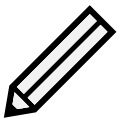


Hardware appliances have dedicated management ports, but can have the Management protocol assigned to additional ports.

12.1 Setting Port Mappings

To set up protocols on a network port, select an option from the corresponding *Add a protocol…* drop down box.

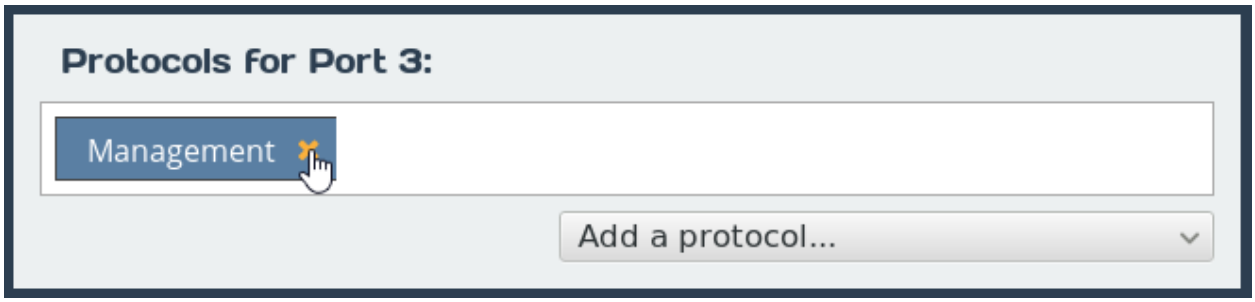
When a protocol has been applied to a port, a blue box corresponding to the protocol will appear under the port.



Note: Hardware appliances will apply some mappings to the PCI slot instead of individual ports, enabling the protocol for all ports on the card in that slot.

12.2 Removing a Port Mapping

To remove a mapping, click on the “X” next to the protocol as shown below.



12.3 Saving Port Mappings

To save the Port Mapping configuration, press the *Save* button at the bottom of the page. This will return you to the Home screen.

Important: Saving the Port Mappings configuration will require a reboot to take effect.

12.4 Available Port Mappings

Licences are required before mappings can be applied. Licences may have speed restrictions, limiting which ports the licence can be mapped to; these licences have an additional suffix after the protocol name. An example licence is *WAN 10 Gb* which can only be applied to ports capable of 10Gb speeds. See Section 13.5: Licence Key Management for help managing and uploading new licence keys.

A summary of licences is displayed in the *Licensed Adapters* table.

Provided the matching licences have been purchased and the product has the appropriate cards for the mapping, the following protocols can be added to an available port:

Fibre Channel
: Assign a port to be a Fibre Channel Initiator or Target.

iSCSI
: Assign a port to be an iSCSI Initiator or Target.

Management
: The Management mapping is required to access the Web interface of the Node, and also allows SSH and SNMP connections.

SAS
: Assign a port to be a SAS Initiator.

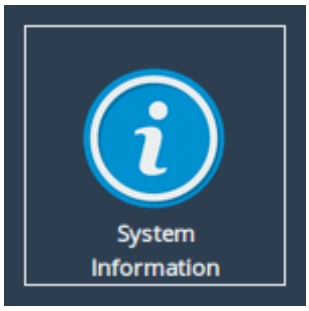
WAN
: The WAN port mapping allows this WANrockIT node to connect to another node.

13 Node Maintenance

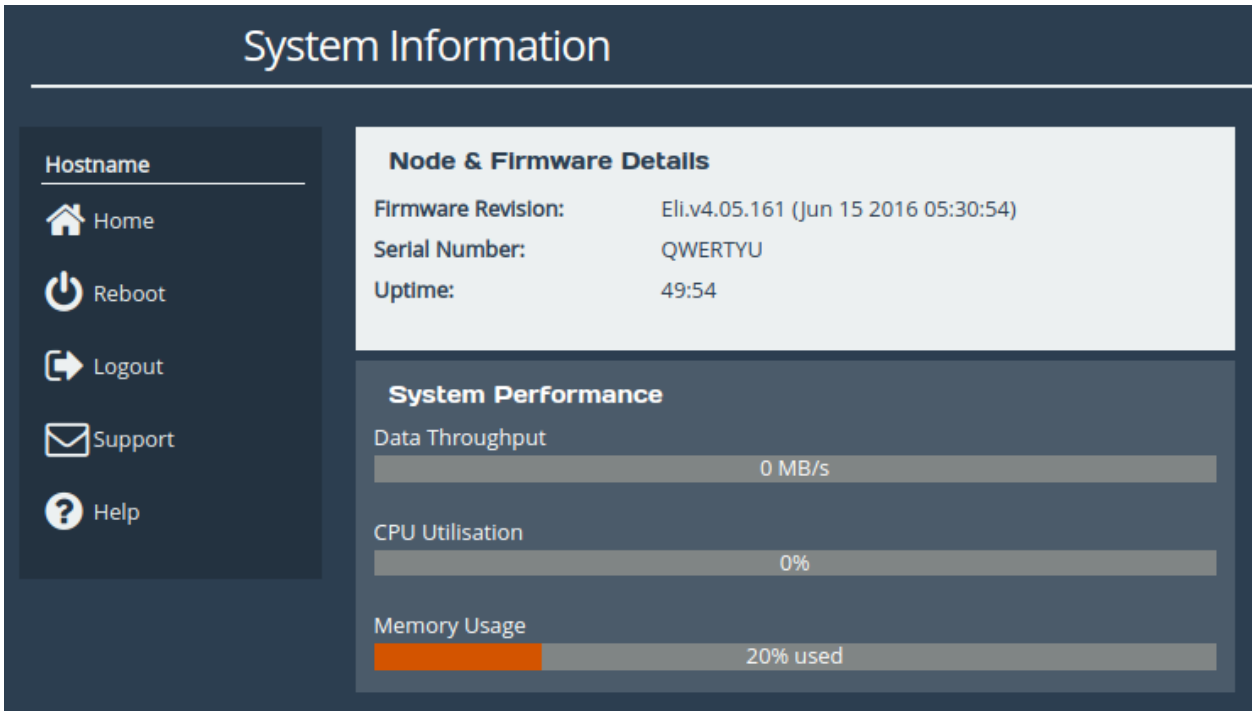
The following section describes the various pages that are available to the administrator to monitor performance and maintain the Node.

13.1 System Information

This page allows the administrator to view the performance of the Node. From the Home screen, select the *System Information* icon from the *Node Maintenance* section.



The following page will be displayed:



In the *Node & Firmware Details* section, the following information is displayed:

Firmware Revision is the installed firmware revision level.

Serial Number/UUID is the unique identifier of that specific WANrockIT Node.

iSCSI IQN is the iSCSI Qualified Name of that specific WANrockIT Node.

Uptime is the amount of time the WANrockIT Node has been powered on for.

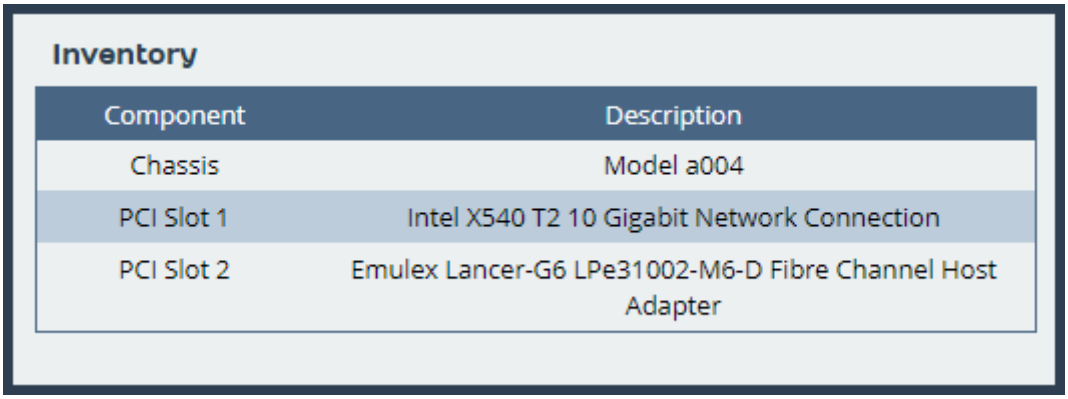
The *System Performance* section contains three meters which provide an approximation of the following performance parameters:

Data Throughput This indicates the current performance in MB/s.

CPU Utilisation This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces.

Memory Usage This indicates the percentage of memory used by all processes.

The following section will also appear on this page:

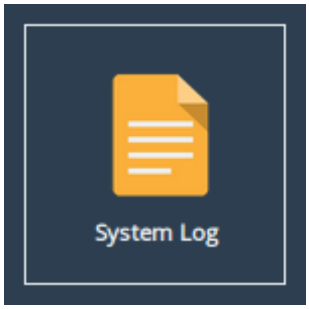


The *Inventory* section shows the hardware your Node is running on, including the board and any cards installed in it.

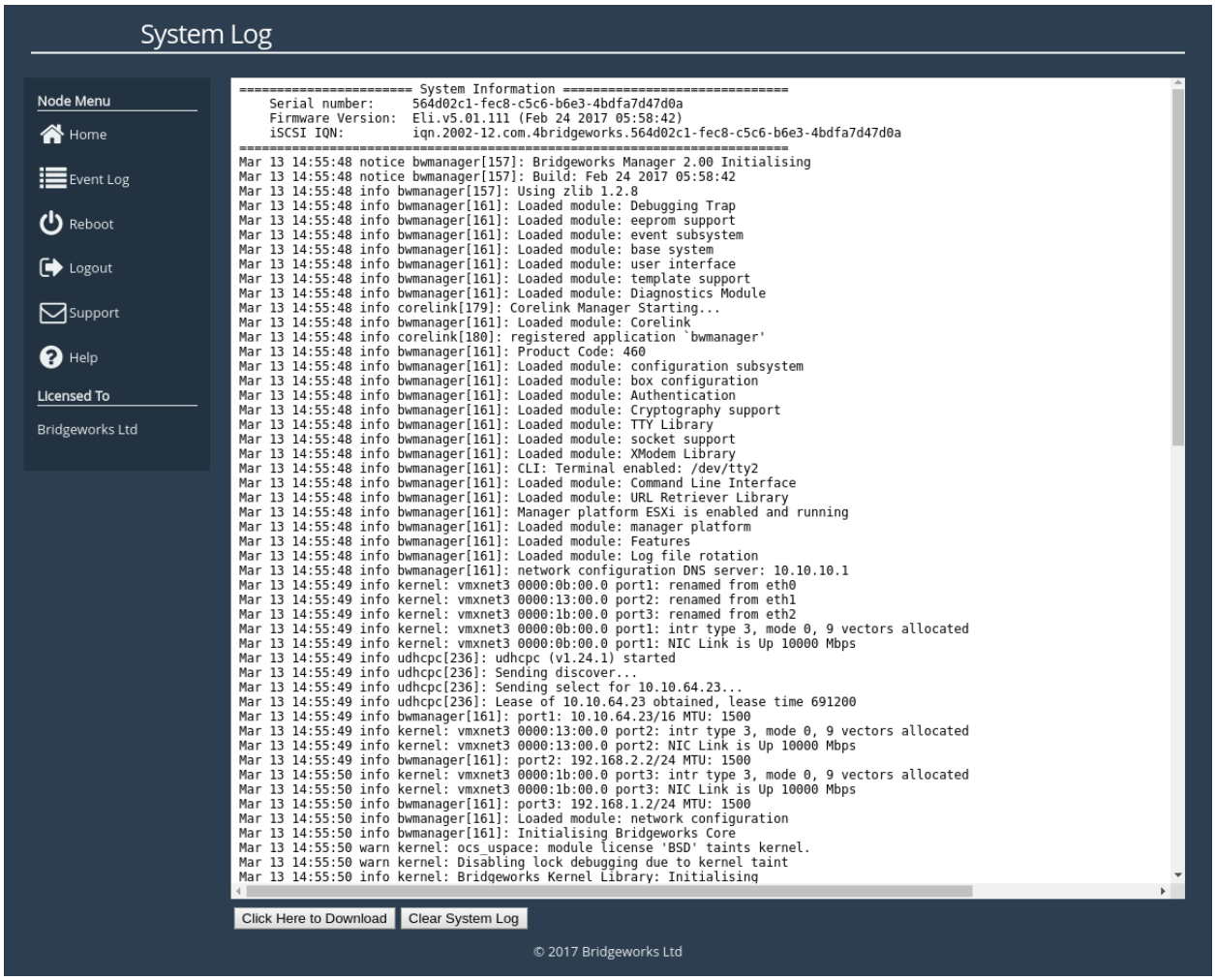
13.2 System Log

This page displays the system log, useful for diagnosing problems with the Node, attached devices and connections.

From the Home screen, select the *System Log* icon from the *Node Maintenance* section.



The web interface will now display the following:



Below the log display pane are two options:

Click Here to Download This will download the log file to your local machine.

Clear System Log This will clear all logs within the Node.

For information on troubleshooting your Node, see Chapter 14: Troubleshooting.

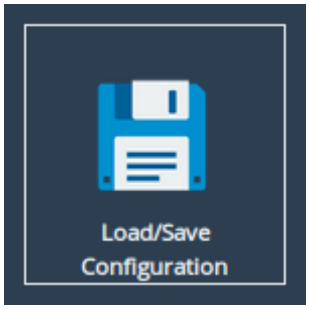
13.3 Load/Save Configuration

	Important: Loading/Saving configuration is unavailable on certain platforms.

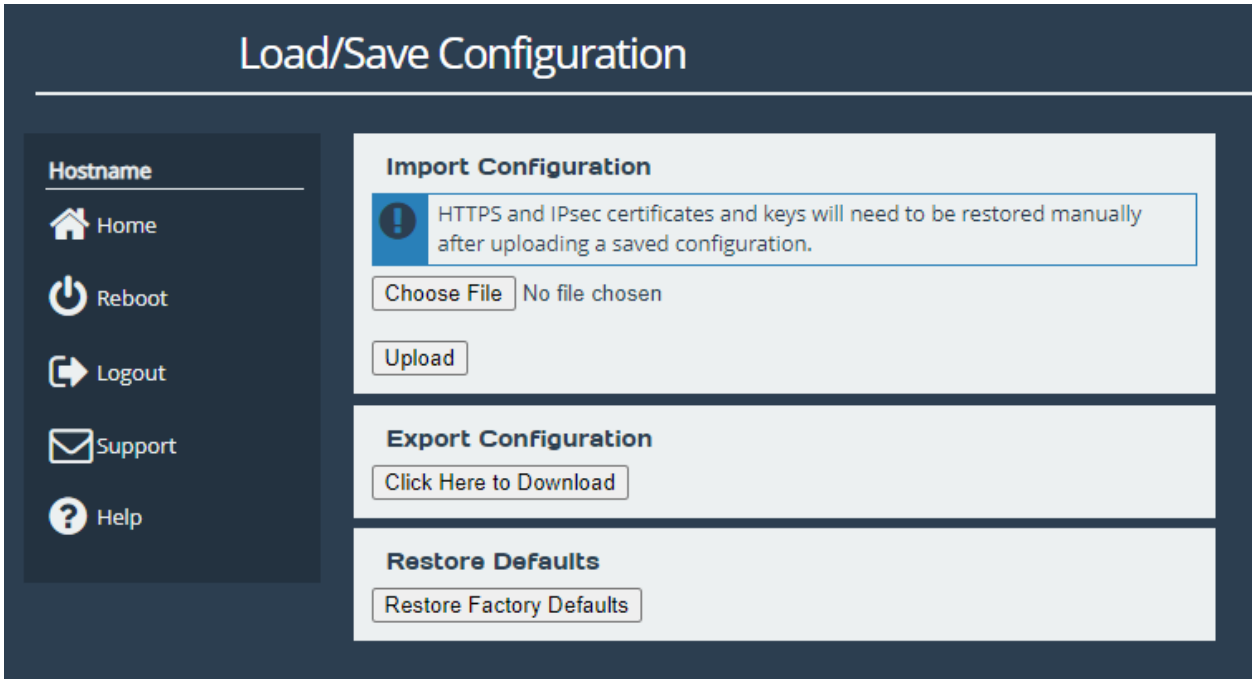
The configuration Load/Save feature allows you to save a copy of the Node's configuration to a file and optionally restore back to that configuration at a later time.

Once you have finished configuring your Node we recommend that you save your configuration data to a local disk. By doing so you could save valuable time if the Node requires replacement or if configuration is lost during upgrades.

From the Home screen, select the *Load/Save Configuration* icon from the *Node Maintenance* section.



The following page will be displayed:



13.3.1 Loading a Saved Configuration

To reload a configuration, click the *Choose file* button and locate the configuration file to upload to the Node. Once located, click the *Upload* button and the new configuration data will be uploaded.

	Important: Once a valid configuration file is uploaded, a reboot will automatically occur.

13.3.2 Saving the Configuration to Disk

To save the configuration data, click the *Click Here to Download* button. Then choose to save the file.

The Node will now download an encoded file that contains all of its configuration settings.

13.3.3 Restoring to Factory Defaults

To restore the Node to factory defaults, click the *Restore Factory Defaults* button. This resets all configuration parameters including the hostname, IP addresses and passwords. This option is useful to protect sensitive information if a Node appliance is ever returned for maintenance.

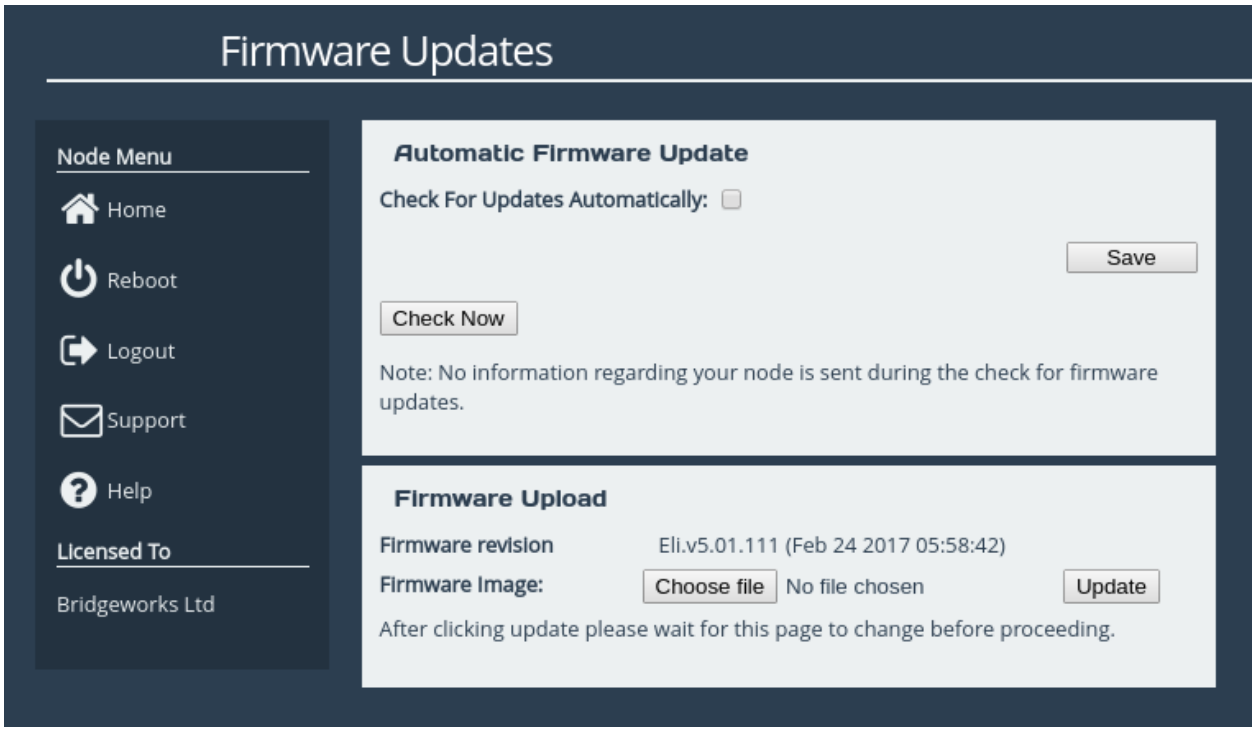
	Important: After clicking the *Restore Factory Defaults* button, a reboot will automatically occur.

13.4 Firmware Updates

From time to time it may be necessary to upgrade the firmware within the Node. New versions contain resolutions to known issues as well as new features and improvements to the functionality of the Node.

The *Firmware Updates* page allows the administrator to load new firmware onto the Node. From the Home screen, select the *Firmware Updates* icon from the *Node Maintenance* section.

The following page will be displayed:

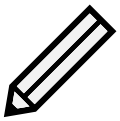


You can now instruct the Node to check for new firmware versions, alerting you when a new version is available and providing a button to perform the update. Alternatively, you can manually upload and update to a firmware version of your choosing.

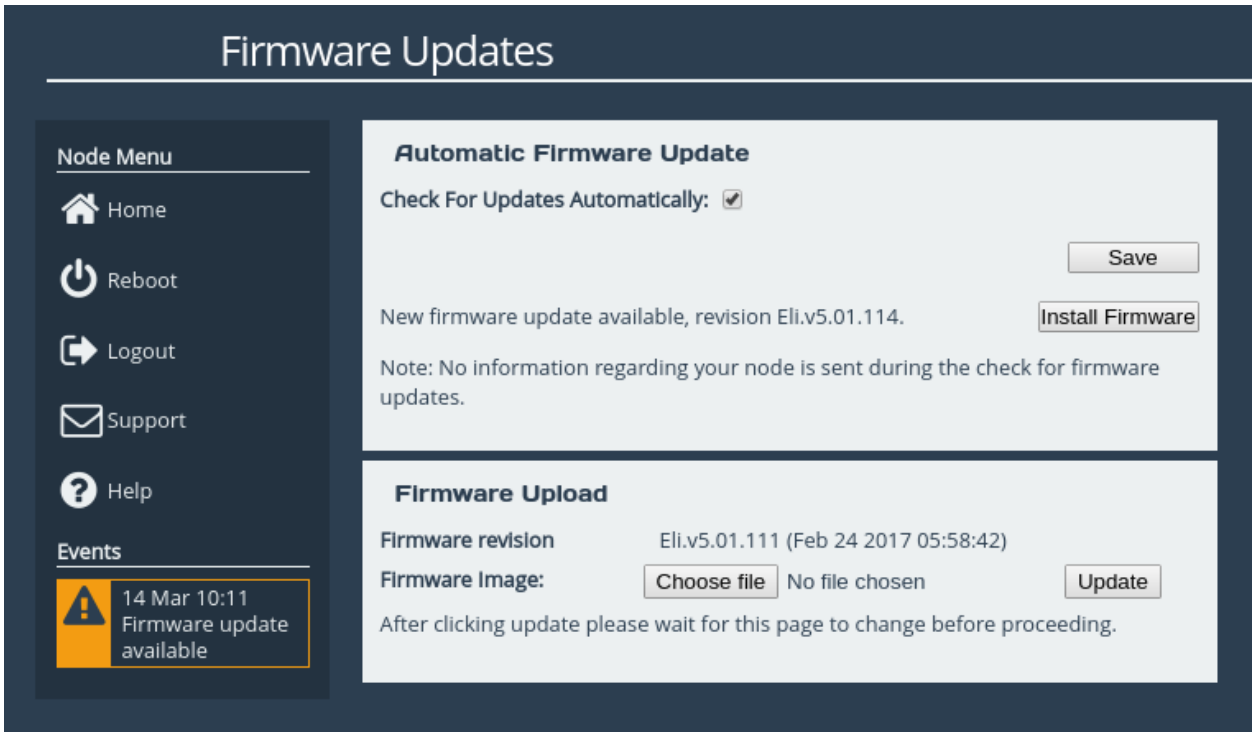
13.4.1 Automatic Firmware Update Checking

This section allows your Node to automatically check for new firmware versions, notifying you when a new version is available. This check occurs once per day.

To enable automatic firmware update checking, select the *Check For Updates Automatically* checkbox, then click the *Save* button. The check can be performed immediately by clicking the *Check Now* button.

	Note: No information regarding your Node is sent during the check for firmware updates.

When a new firmware version is available, a notification will appear under the *Node Menu*.



To start the firmware update process:

1. Click on the *Install Firmware* button. A progress bar labelled *Downloading* will appear showing the progress in downloading the new firmware on to the WANrockIT Node.
2. When the label above the progress bar changes to *Progress*, you can navigate away from this page and the installation will continue.

Updating the firmware will take a few minutes. After the update is complete, a notification will appear under the *Node Menu*, indicating that a system reboot is necessary. To reboot the Node, click on the *Reboot* button located in the *Node Menu* at the left side of the web interface.

13.4.2 Updating Firmware Manually

It is also possible to download new firmware versions and update manually.

Contact Bridgeworks support at support@4bridgeworks.com providing the serial number of your product to receive the latest version of the firmware.

⚠	Warning: Do not load on a firmware which has an earlier release revision unless you have been instructed to by the Bridgeworks support team. Always ensure that you have the correct firmware for your product. **If in any doubt, please contact Bridgeworks support. See Appendix G: Useful Links for contact information.**

Once you have downloaded the new firmware to your local machine:

1. Click on the *Choose file* button to locate the file you have downloaded from the Bridgeworks website.

2. Click on the *Update* button to start. A progress bar labelled *Uploading* will appear showing the progress in uploading the new firmware on to the WANrockIT Node.
3. When the label above the progress bar changes to *Progress*, you can navigate away from this page and the installation will continue.

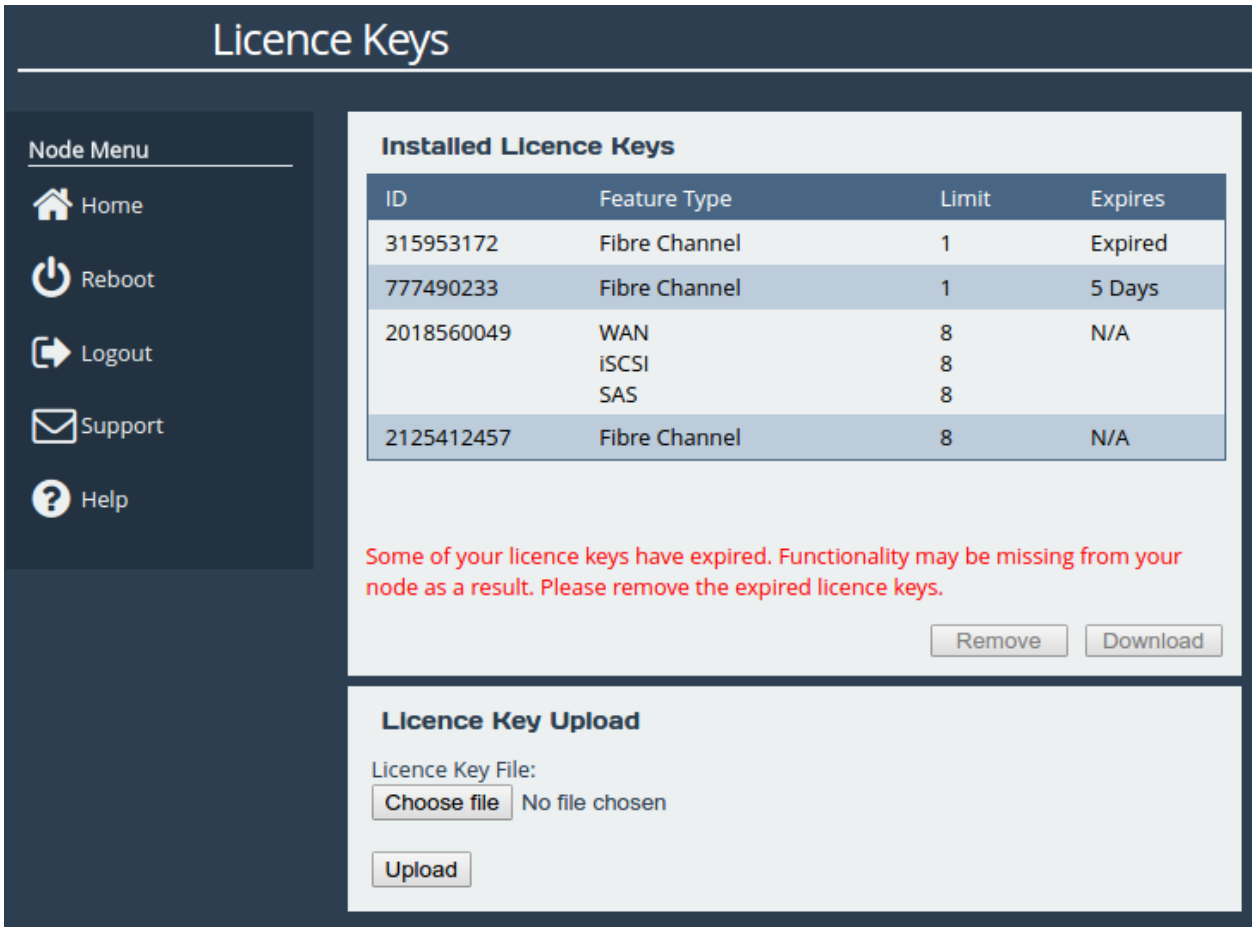
Updating the firmware will take a few minutes. After the update is complete, a notification will appear under the *Node Menu*, indicating that a system reboot is necessary. To reboot the Node, click on the *Reboot* button located in the *Node Menu* at the left side of the web interface.

13.5 Licence Key Management

This page allows you to view, upload, download or remove licence keys installed on the Node. Licence keys are required to enable features on installed feature cards. See Chapter 12: Port Mappings for information on assigning licence keys to interfaces.

From the Home screen, select the *Licence Key Management* icon from the *Node Maintenance* section.

The following page will be displayed:



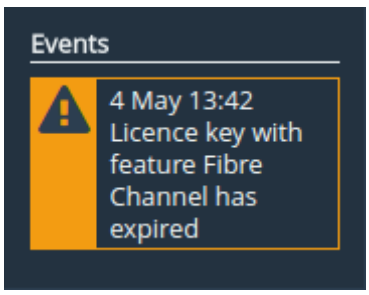
The *Installed Licence Keys* table displays the installed licence keys with the following information:

Feature Type The feature that the licence key enables.

Limit The number of interfaces that the feature may be mapped to.

Expires The amount of time left until a temporary licence key expires. If *N/A* is in this column, it indicates the licence key is not temporary.

When a temporary licence key has expired, there will be a warning on the page and the *Expires* field will say *Expired* as shown in the image above. At the point of expiration, an event will be displayed below the *Node Menu* similar to the one shown below.



13.5.1 Uploading a Licence Key

To upload a licence key:

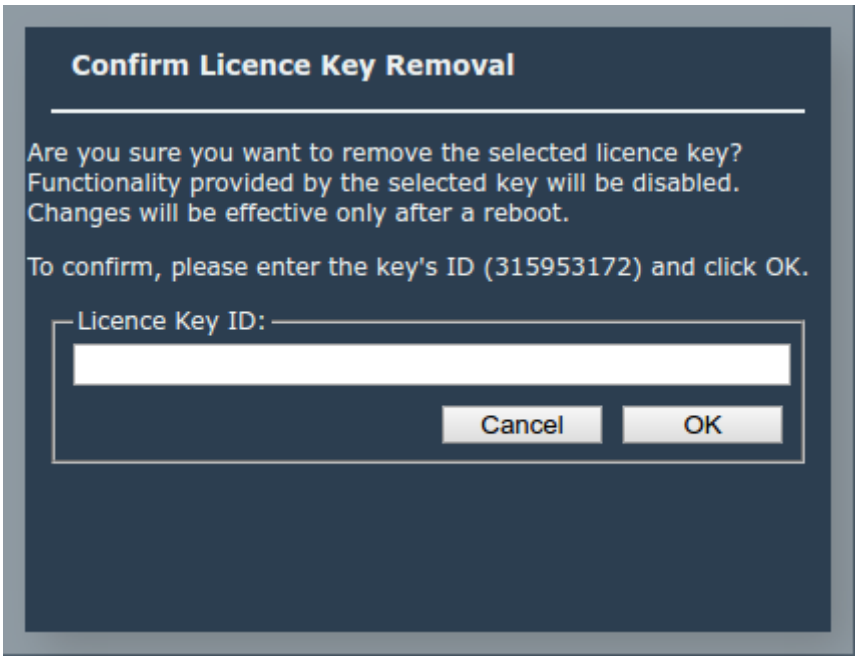
1. Click the *Choose file* button in the *Licence Key Upload* section.
2. Locate and select the licence key to upload.
3. Click the *Upload* button.

After the upload completes, a valid licence key will appear in the *Installed Licence Keys* table.

	Important: The Node will require a reboot for the licence key to be activated.

13.5.2 Removing a Licence Key

To remove a licence key, select the licence key from the *Installed Licence Keys* table, then click the *Remove* button. This will open a dialog box, as shown below.



Copy the licence key ID into the *Licence Key ID* field and click *OK*. The licence key will be removed from the Node and will no longer be displayed in the *Installed Licence Keys* table.

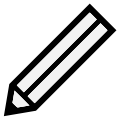
13.5.3 Downloading a Licence Key

To download a licence key, select the licence key from the *Installed Licence Keys* table, and click *Download*.

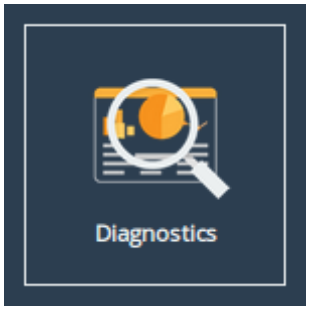
13.6 Diagnostics

In the unlikely event that a problem arises with your WANrockIT Node, you may be requested by Bridgeworks Support to provide a diagnostic file.

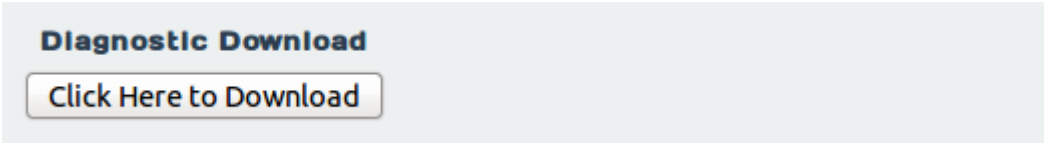
	Important: If an issue arises with your WANrockIT Node, check Chapter 14: Troubleshooting for information on how the issue may be resolved.

	Note: The following instructions are demonstrated in the Bridgeworks Support Video "WANrockIT: Downloading Diagnostic Information" found at https://www.youtube.com/watch?v=8RZXFGCy3ZU.

To download the diagnostic file, click on the *Diagnostics* icon on the Home screen:



Then click on the *Click Here to Download* button.



This will cause the WANrockIT Node to collect data regarding various modules and store them in a single file. Once this process is complete, a download for "diagnostics.bin" will begin.

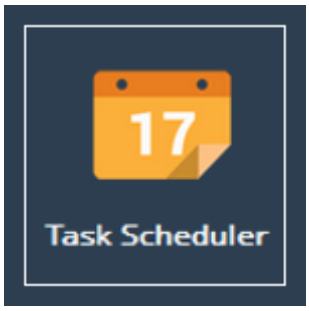
13.7 Task Scheduler

This page allows the administrator to schedule tasks with the following actions:

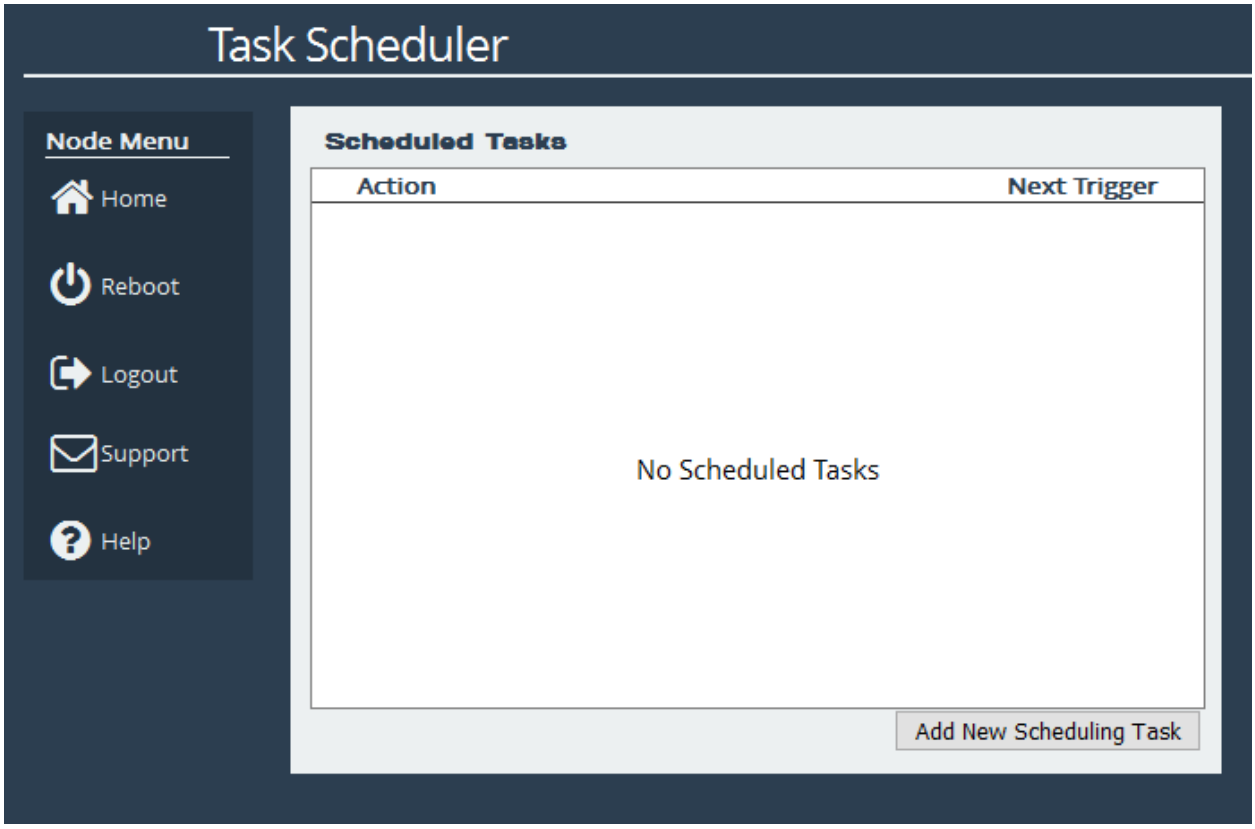
Email Performance Statistics This will email the log of the throughput rate to a given email address(es).

WANrockIT Bandwidth Limit This will restrict the WANrockIT transmission rate to a given number of Megabytes per second.

From the Home screen, select the *Task Scheduler* icon from the *Node Maintenance* section.



The web interface will now display the following:

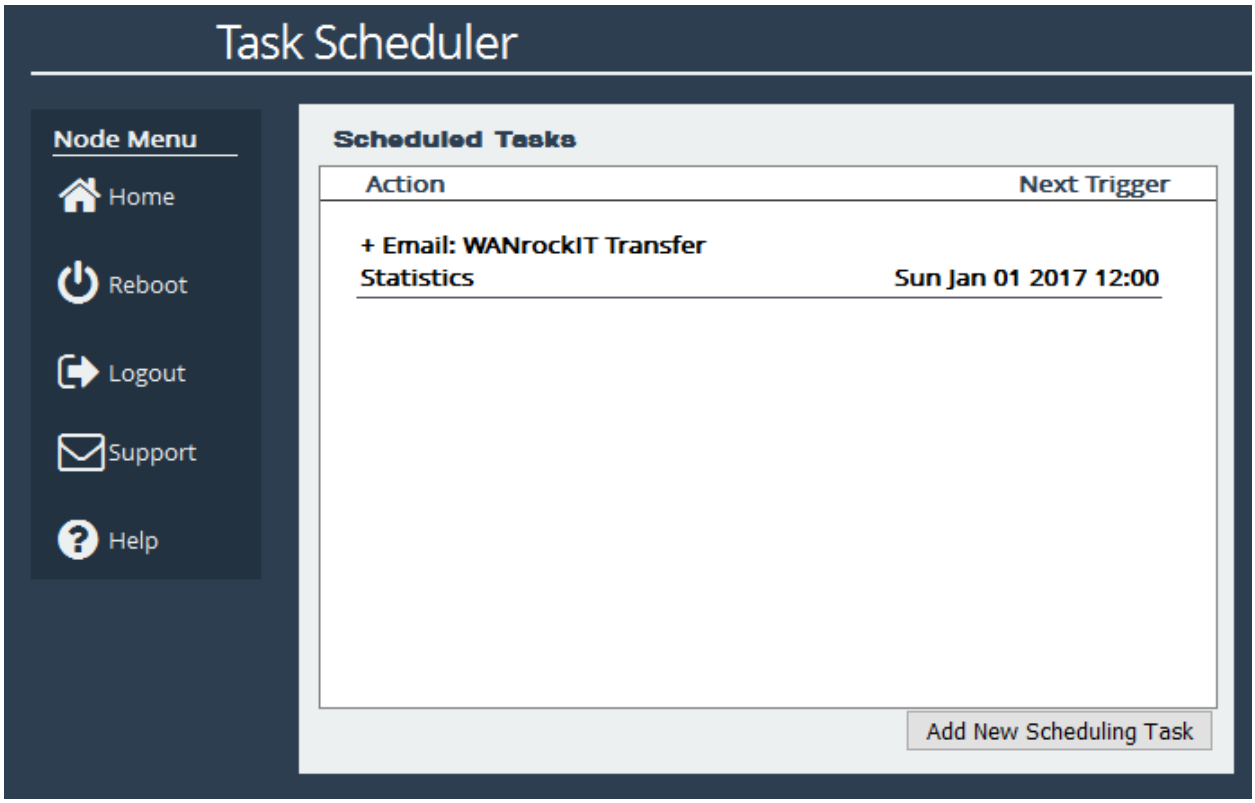


13.7.1 Adding Tasks

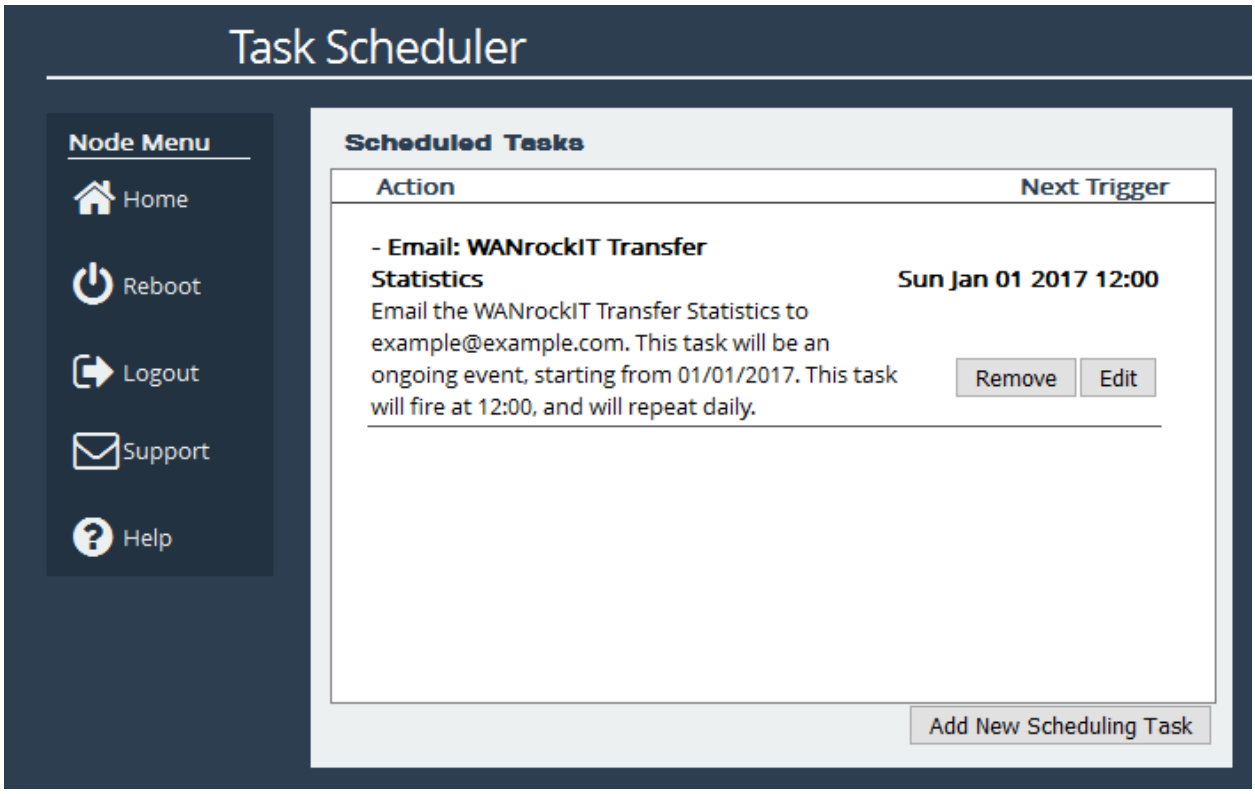
Tasks can be added by clicking on the *Add New Scheduling Task* button, which will start the task wizard.

13.7.2 Removing/Editing Tasks

If you already have some tasks added, they will be listed in the Scheduled Tasks window as shown:



Clicking on a task will expand it as shown:



Clicking the *Remove* button will remove the task from the task scheduler. Clicking the *Edit* button will start the task wizard for the task, allowing it to be edited.

13.7.3 Task Wizard

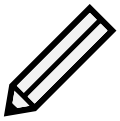
The task wizard will guide you through the adding or editing of scheduled tasks. There are a few common buttons across the individual sections of the wizard:

Help Clicking this button will display the Online Help page for the Task Scheduler.

Cancel Clicking this button will discard the changes being made to the task and close the wizard.

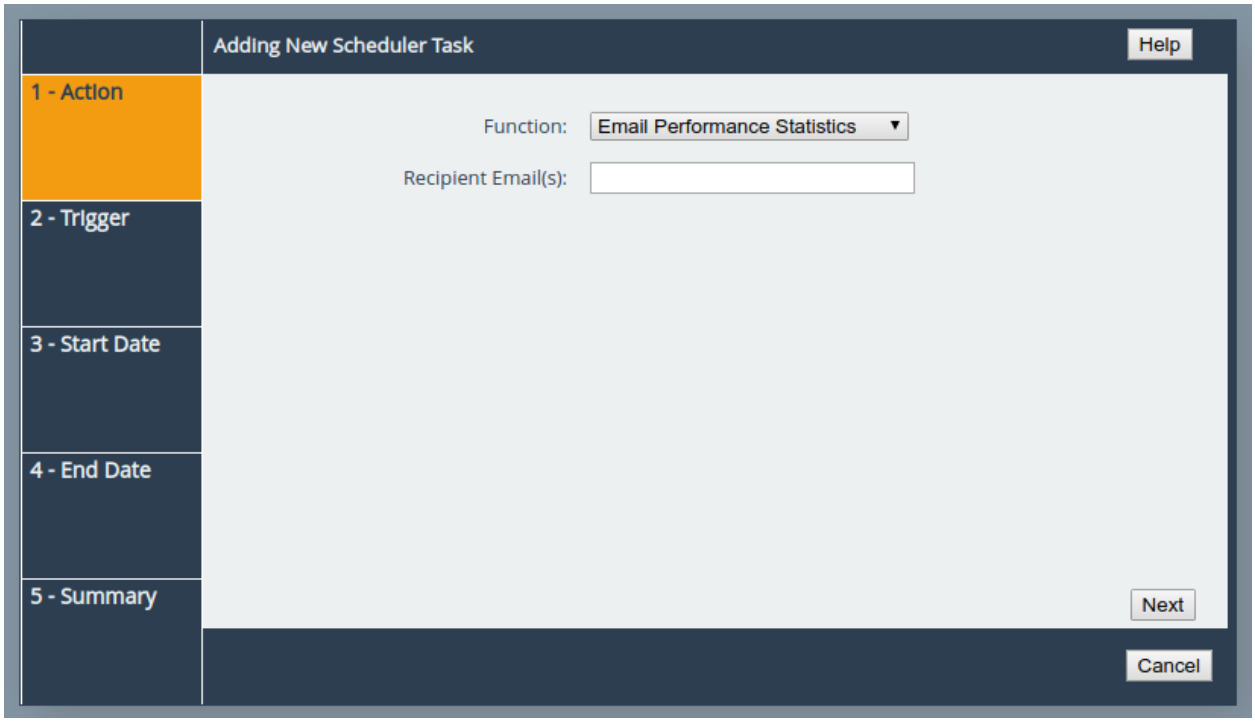
Next If present, this button will navigate you to the next section of the wizard.

Previous If present, this button will navigate you to the previous section of the wizard.



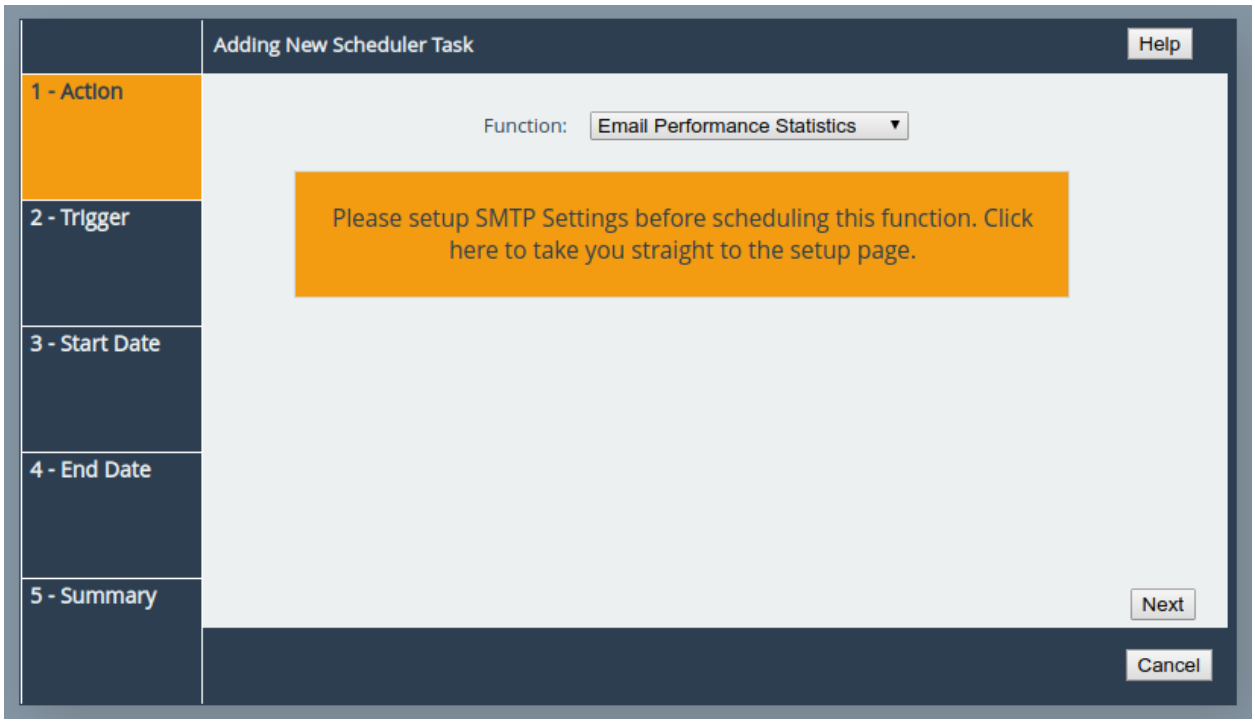
Note: The currently active section of the wizard will be highlighted in orange on the left-hand side.

13.7.3.1 Action - Email Performance Statistics

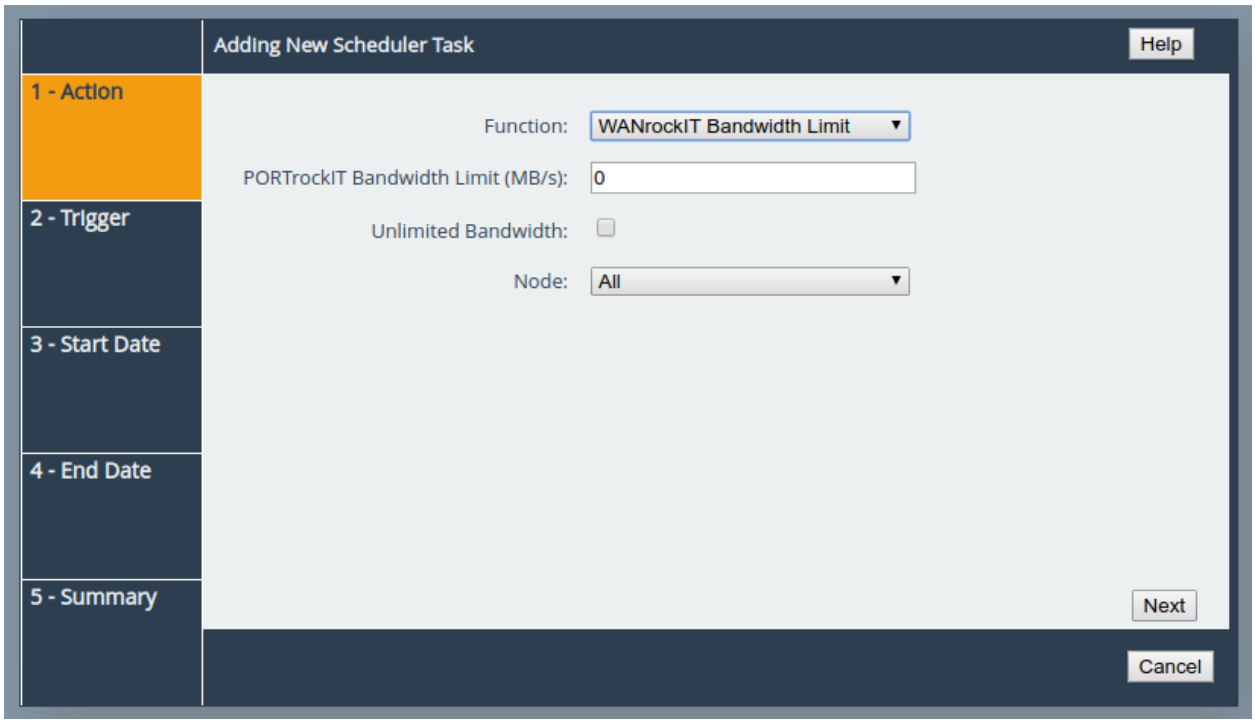


On the Action section of the wizard, enter the recipient email(s), separating multiple emails with semi-colons.

Important: If you see the following image, click on the yellow box to be taken to the Service Control page where SMTP can be set up. See Section 3.3.3: Email.

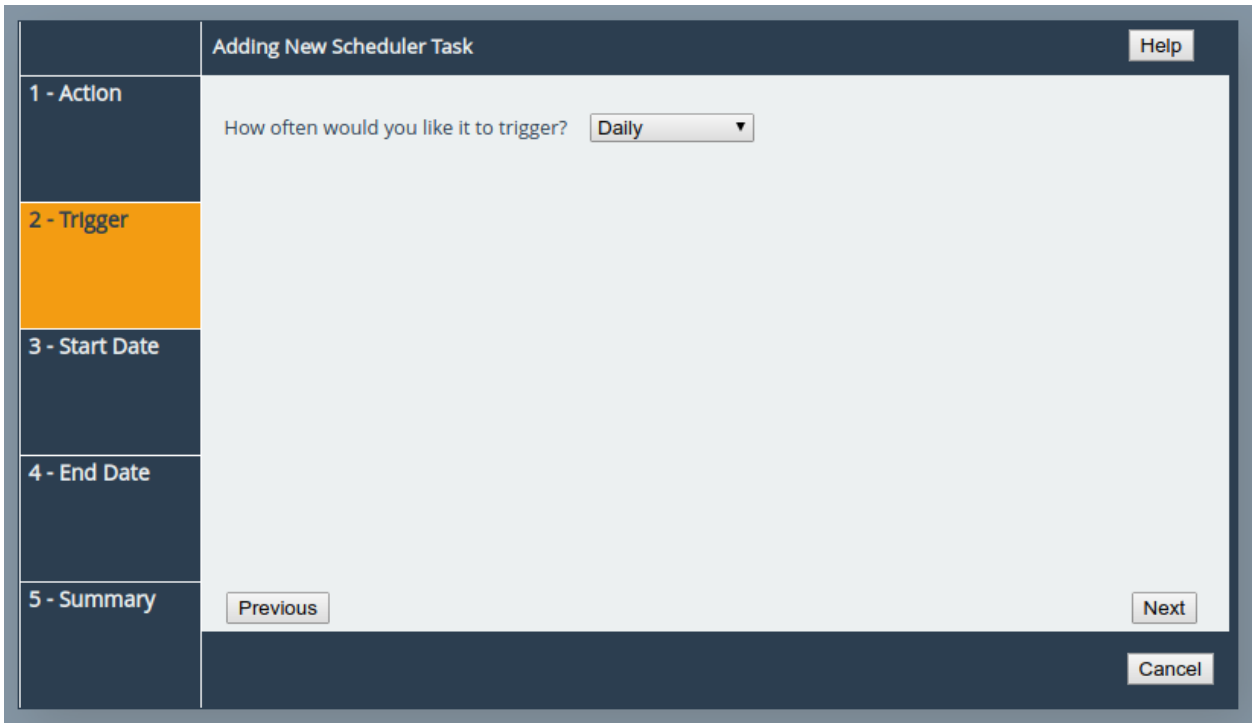


13.7.3.2 Action - WANrockIT Bandwidth Limit



On the Action section of the wizard, enter a bandwidth limit in Megabytes per second to apply a limit or select the *Unlimited Bandwidth* checkbox to remove a limit. Then select which Node and Path should be affected by the bandwidth limit. This limit will remain in place until another task overwrites it.

13.7.3.3 Trigger

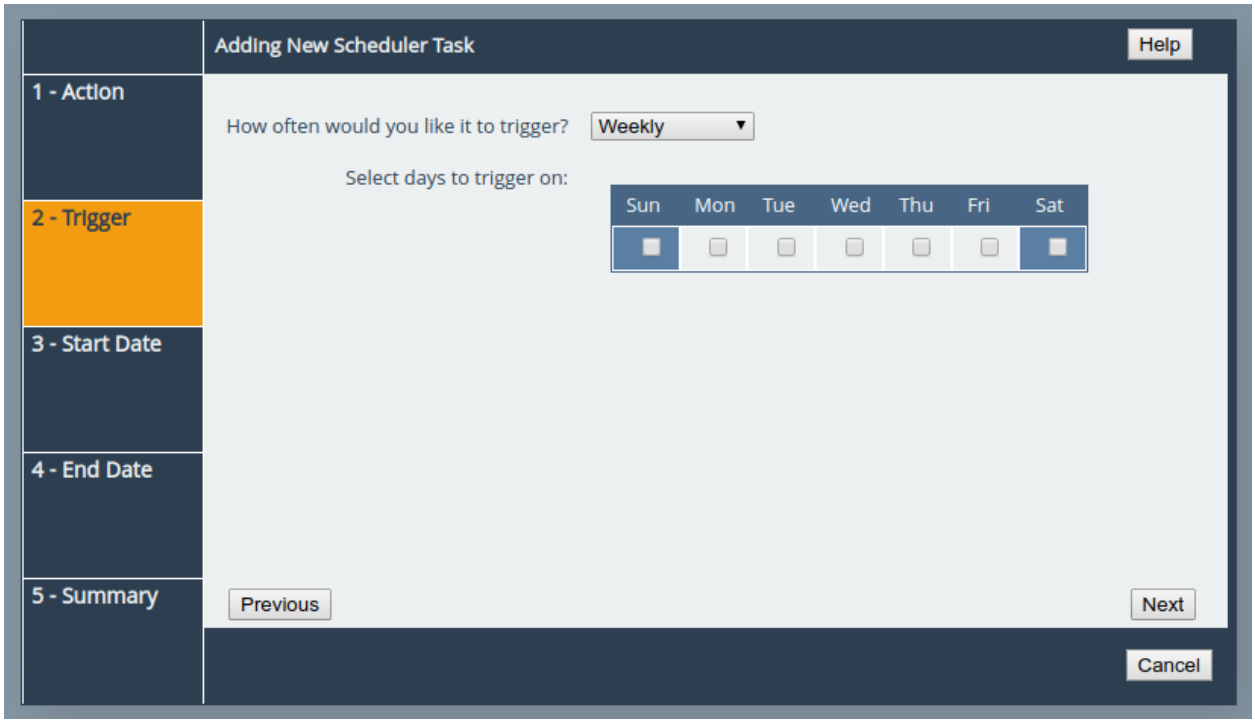


On the Trigger section of the wizard, you can pick the frequency of the event. The options are:

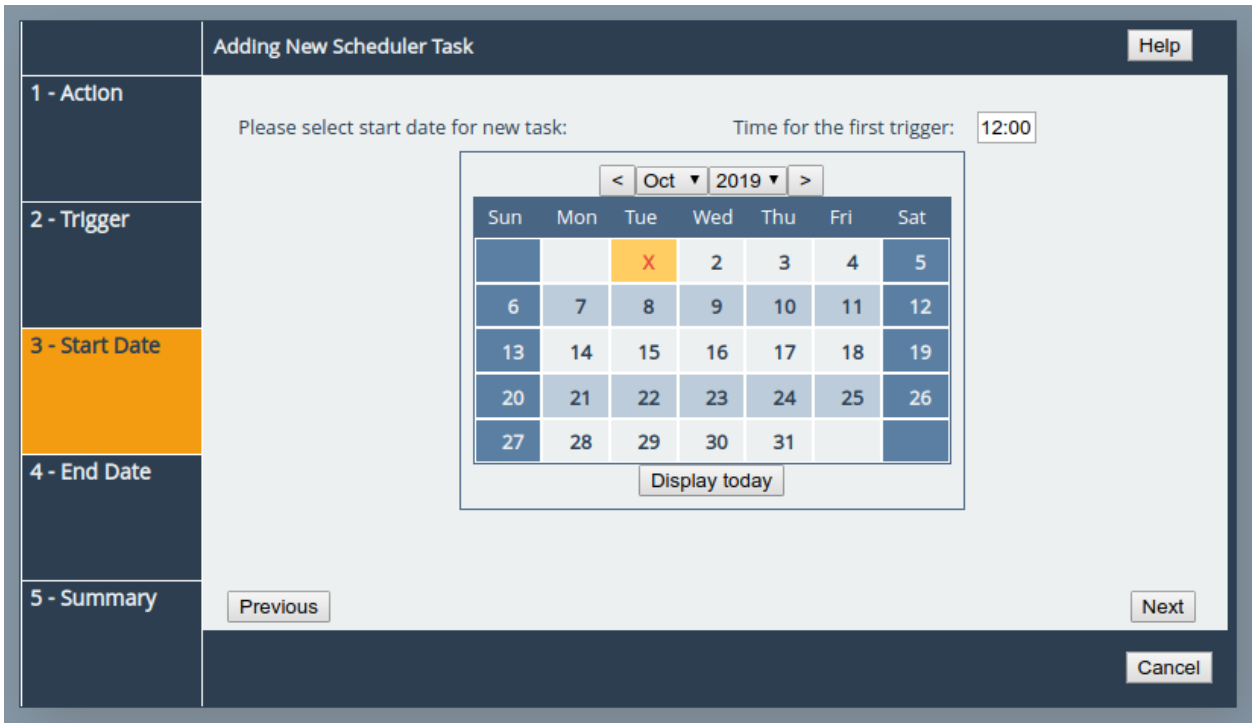
Once This means the action will be performed at the specified time and not repeat.

Daily This means the action will be performed every day at the specified time.

Weekly This means the action will be performed on specified days every week at the specified time. When selecting this option, you will be able to pick which days to trigger the action by selecting checkboxes. Each day will have its own checkbox, as shown:

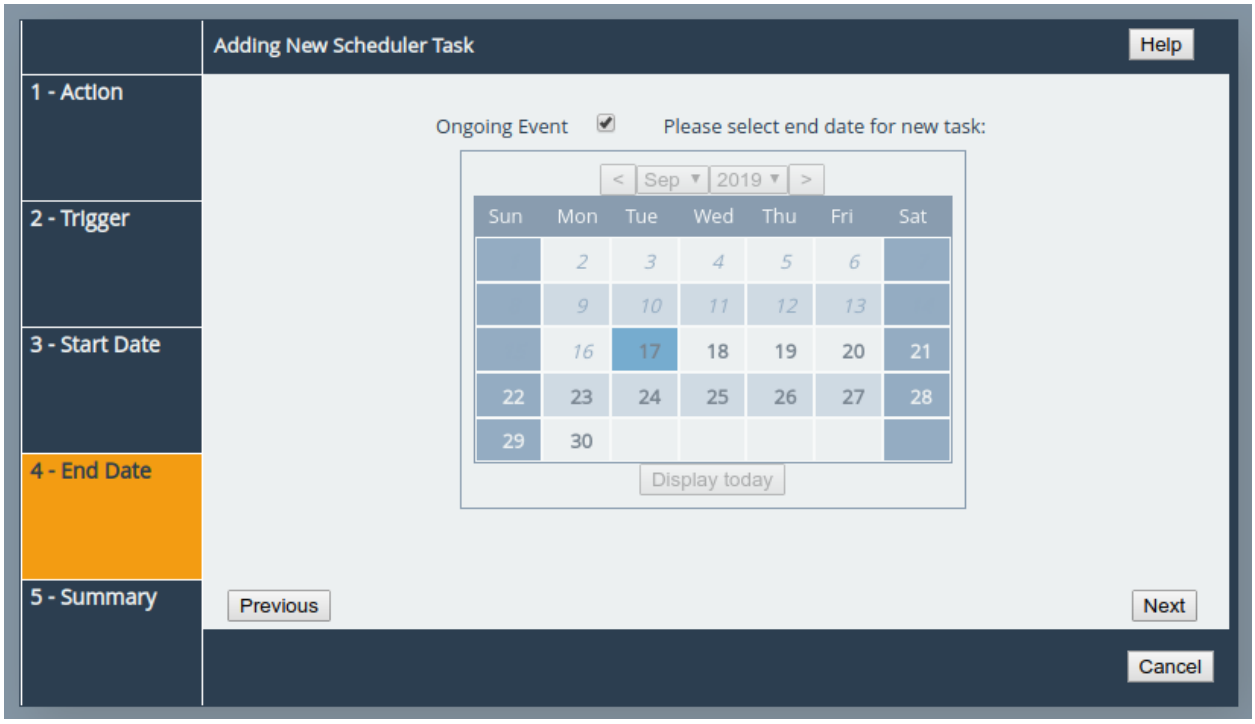


13.7.3.4 Start Date



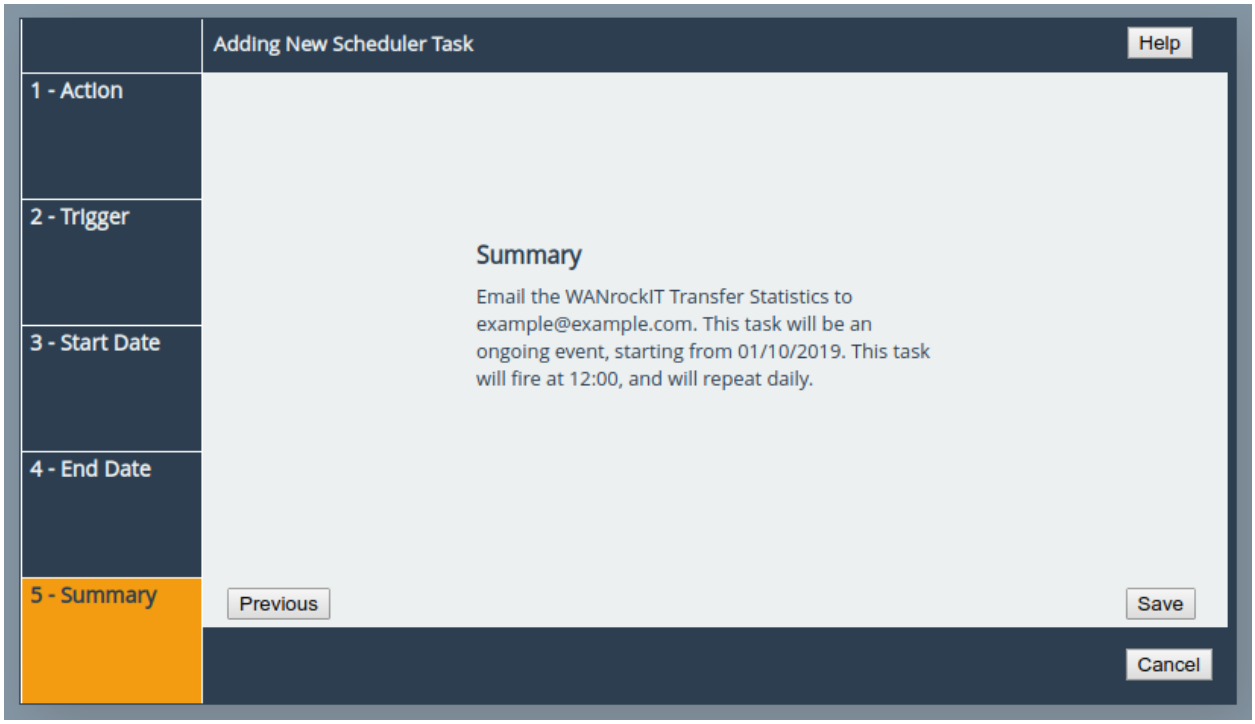
On the Start Date section of the wizard, you can pick the starting date and time for the new task. Enter a time into the *Time for the first trigger* box and select your start date using the calendar. The selected date will be marked with a red cross.

13.7.3.5 End Date



On the End Date section of the wizard, you can pick the end date for the new task. You can either select the *Ongoing Event* checkbox for a task that should run until cancelled, or select a date using the calendar. The selected date will be marked with a red cross.

13.7.3.6 Summary



On the Summary section of the wizard, a brief description of the task will be displayed. If you are happy with this task, click the *Save* button to add the task to the task scheduler. Saving will automatically close the wizard.

14 Troubleshooting

14.1 Network Connectivity Problems

Under normal operation, you should be able to “ping” the network address of the Node and receive a response. If this fails, run through the following list to identity and solve the problem.

- Ensure the Node is powered on. This can be verified on hardware appliances by checking that the power LED is illuminated.
- Ensure that the Ethernet cable is plugged in at both ends.
- For hardware appliances, ensure the *Link indicator* LED of the Ethernet connector is illuminated. If it is not, check with your Network Administrator. Refer to the *Visual Indicators* appendix within the relevant hardware manual for help identifying the LED.
- If you are using a Node with two Management ports and only one network cable, try using the other network address and/or the other Management port.
- If the Node is transferring large amounts of data, then the response from the web interface may seem slower than usual as the process that controls the web interface has the lowest priority for Network and CPU resources.
- If you can “ping” the Node but the web interface fails to appear, check the settings within the web browser you are using. If you are directly connected to the Node then any proxy settings will require adjustment and may require you to contact your Network Administrator.
- Ensure you are using the correct network address and netmask. See Appendix B: Accessing the Node from Windows using a static IP Address.

If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix G: Useful Links for information on how to contact Bridgeworks Support.

14.2 SCSI Device Related Problems

Once the Node has finished booting up, and the target devices have finished initialising, these devices should be available on the host machine. After checking that you have correctly configured the initiator, run through the following list to identify and solve the problem.

- Ensure that the devices are powered on and are ready - some libraries can take 5 minutes or more before they are ready and appear on the Node. The power up status of libraries are usually displayed on the front panel.
- Ensure that the cables between the Node and the devices are connected.
- Ensure that the CHAP settings for the initiator and the Node are the same.
- Force a rediscovery from the initiating iSCSI host.

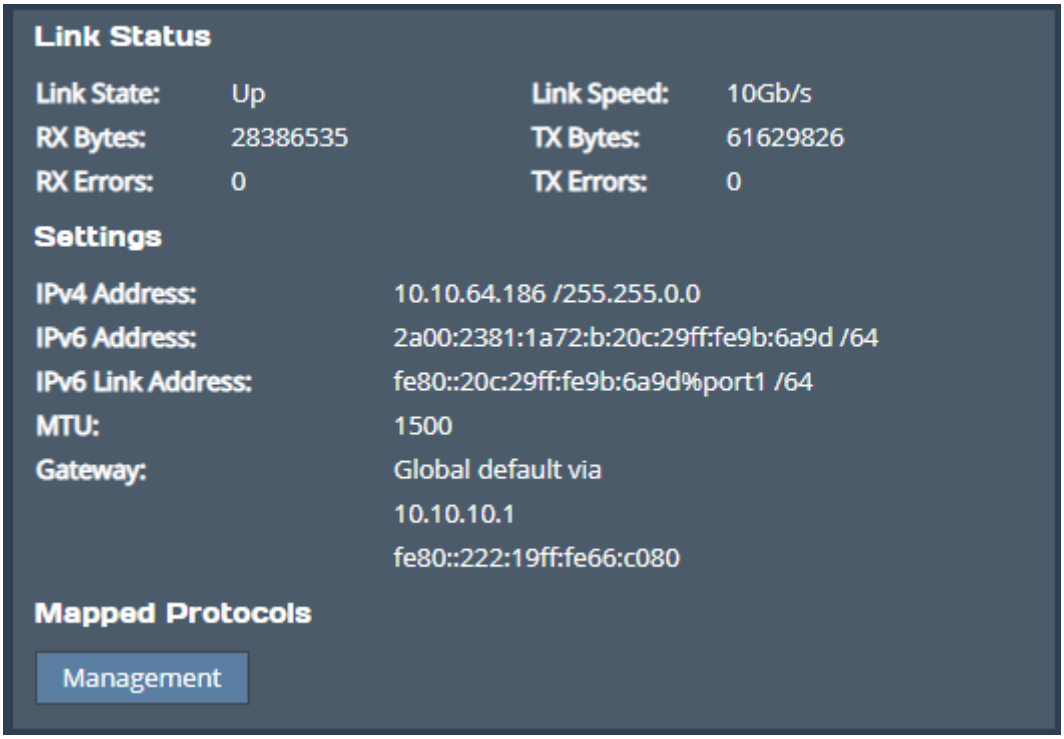
- A common mistake is when enabling CHAP only for a device after the initial discovery by the initiator. It will be necessary to remove the address from the discoveries tab and recreate it with the appropriate CHAP settings, otherwise any rediscoveries will be attempted without CHAP and no devices will be returned.
- Reboot the devices and the Node.

If none of the above resolves your problem, please contact support. See Appendix G: Useful Links for information on how to contact Bridgeworks Support.

14.3 Network Performance Problems

Poor network performance can be caused by many differing reasons. The following list is provided as a guide to where you may find ways to improve performance.

- Ensure that the entire network cabling between the network and the Node is of the correct standard.
- Ensure your network and Node are communicating at the fastest possible network speed. Current link speeds can be found next to each interface on the *Network Connections* page. The link speed should be *1000Mb/s* on a 1 Gigabit network link. If it is 10 or 100Mb/s, this will limit the performance dramatically. See Section 3.1: Network Connections for help finding the *Network Connections* page.
- Packet loss can be a cause of poor performance. Within the *Link Status Box* check the number of *TX* and *RX* errors for relevant network interfaces that are displayed on each *Network Port* page. This should be zero or a very small number. If these are showing large numbers of errors, check the connections between the Node and the network. See Section 3.1.6: Port Settings for help finding the *Network Port* page.



If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix G: Useful Links for information on how to contact Bridgeworks Support.

14.4 iSCSI Performance Problems

Poor iSCSI performance can be caused by many differing reasons. The following list is provided as a guide to where you may find ways to improve performance in addition to those found in Section 14.3: Network Performance Problems.

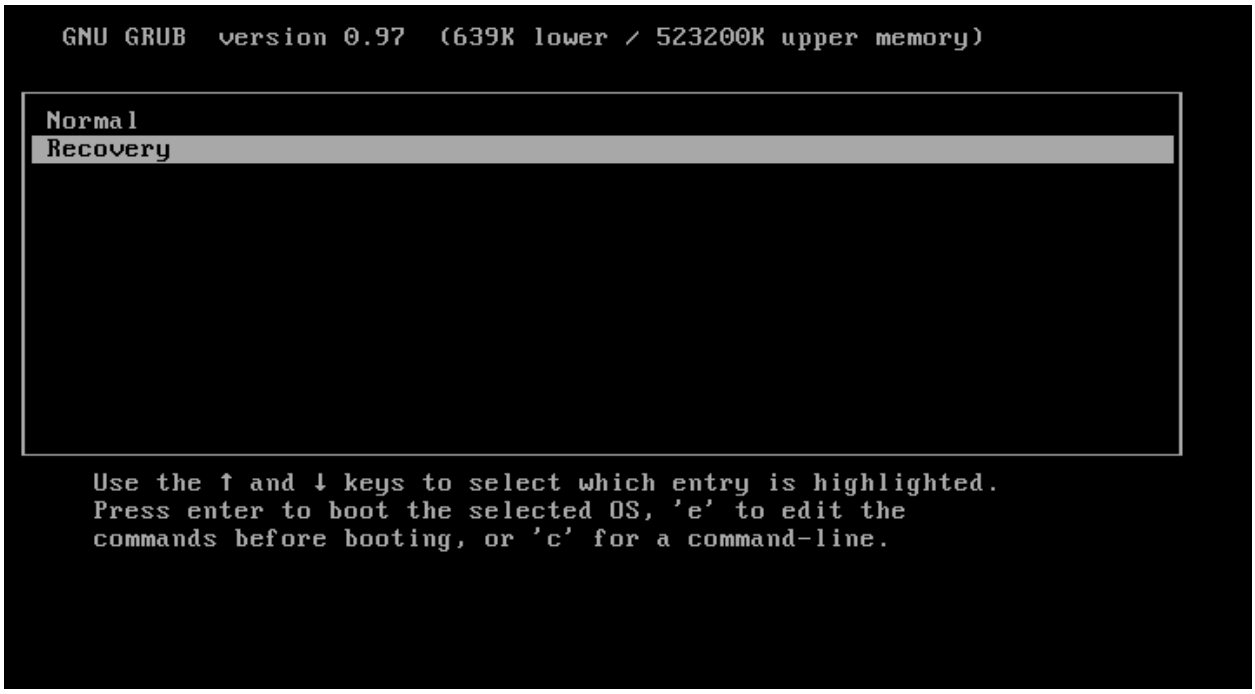
- *Data Digests* are an extra level of error checking on top of the standard TCP/IP checksum error checking (configured on the initiator). However, the calculation of these extra checksums can greatly affect overall performance. Therefore, *Header and Data Digests* should only be enabled where the integrity of the network connection is in doubt. Refer to Appendix C: Connecting to an iSCSI Device using the Microsoft iSCSI Initiator for more information.
- By enabling *Jumbo Frames* as explained in Section 3.1.6.2: Setting the MTU you can improve the throughput performance of the Node. This will only work if *all* of the components in the infrastructure between the initiator/target and the Node are enabled for jumbo frames. That includes the Host Bus Adapter (HBA), all switches and routers, and the Node itself. If any of the components are not enabled or not capable of handling jumbo frames, then unexplained packet loss or corruption may occur.

If none of the above resolves your problem, please contact support. See Appendix G: Useful Links for information on how to contact Bridgeworks Support.

14.5 Recovery Wizard

If access to the system is being disrupted because of problems with the configuration file then, in consultation with Bridgeworks support, the following procedures can be used to recover your system.

To access the Recovery Wizard press the *Esc* key during the unit's boot sequence as soon as you see the message "GRUB loading, please wait..." Select the *Recovery* option on the menu that follows.

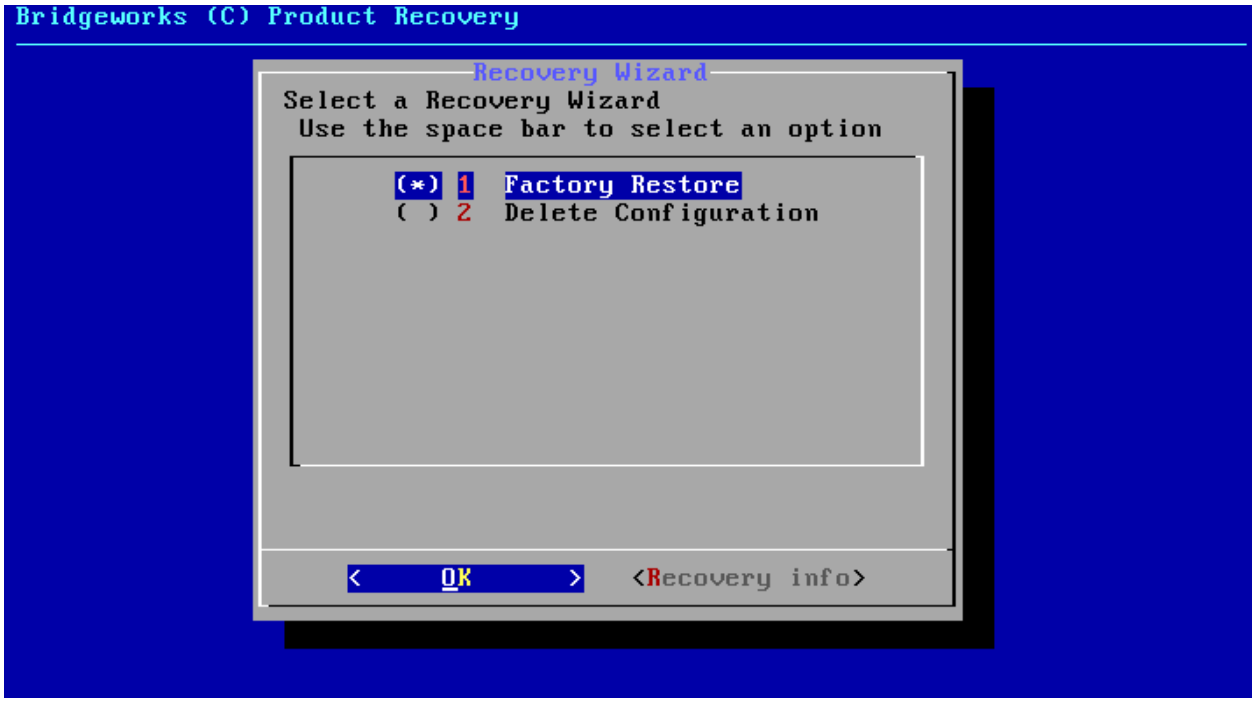


The Recovery Wizard provides two options for system recovery: restoring your unit to factory defaults, and deleting your configuration file.

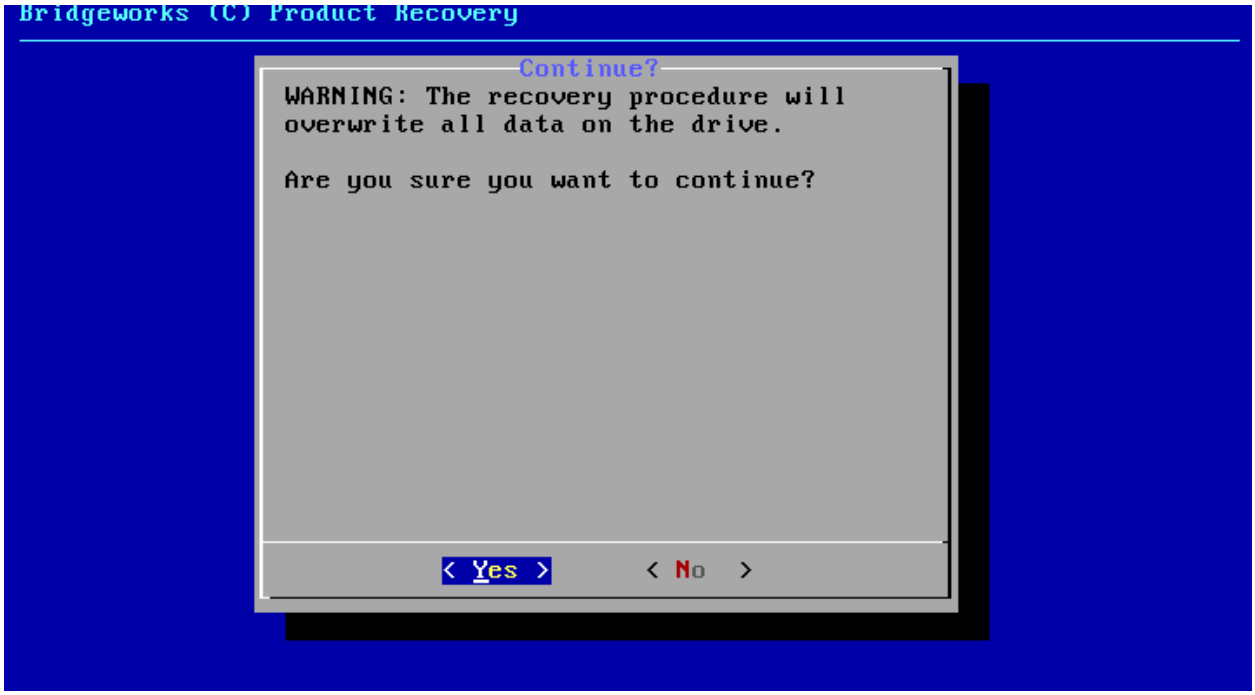
14.5.1 Factory Restore

This option will restore your unit to its factory defaults, removing any current configuration on your system including your current firmware and licence keys.

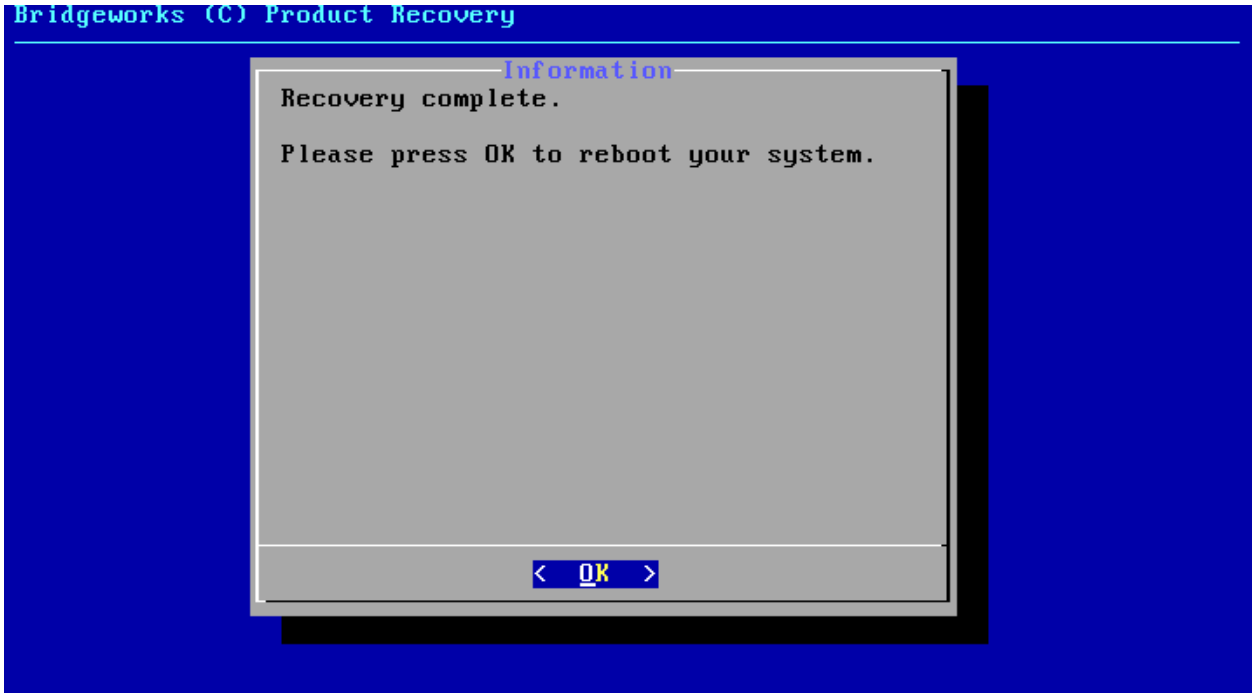
To restore your unit to defaults, ensure that the *Factory Restore* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the factory restore process.



This procedure cannot be undone once complete; only continue if you are sure that you wish to do so. You will be asked to confirm that you wish to proceed. Choosing *Yes* will restore your unit to defaults and *No* will exit the Recovery Wizard menu and drop to the shell.



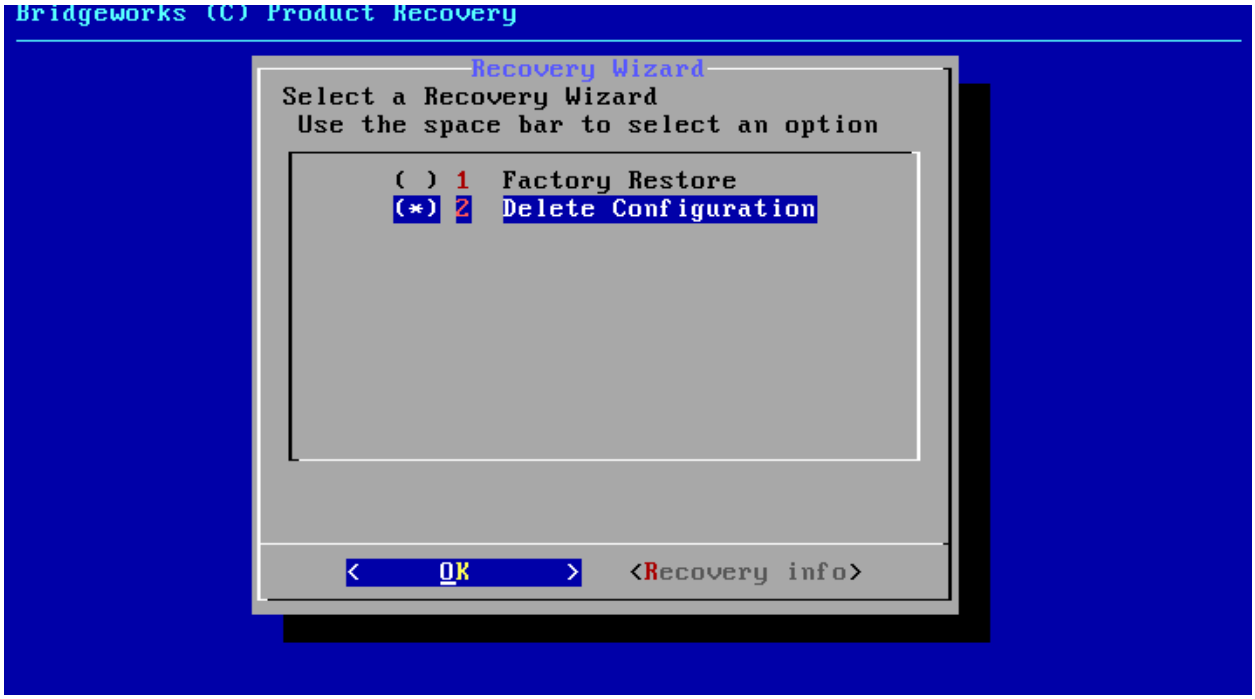
Once the factory restore procedure has completed successfully you will need to reboot your system.



14.5.2 Delete Configuration

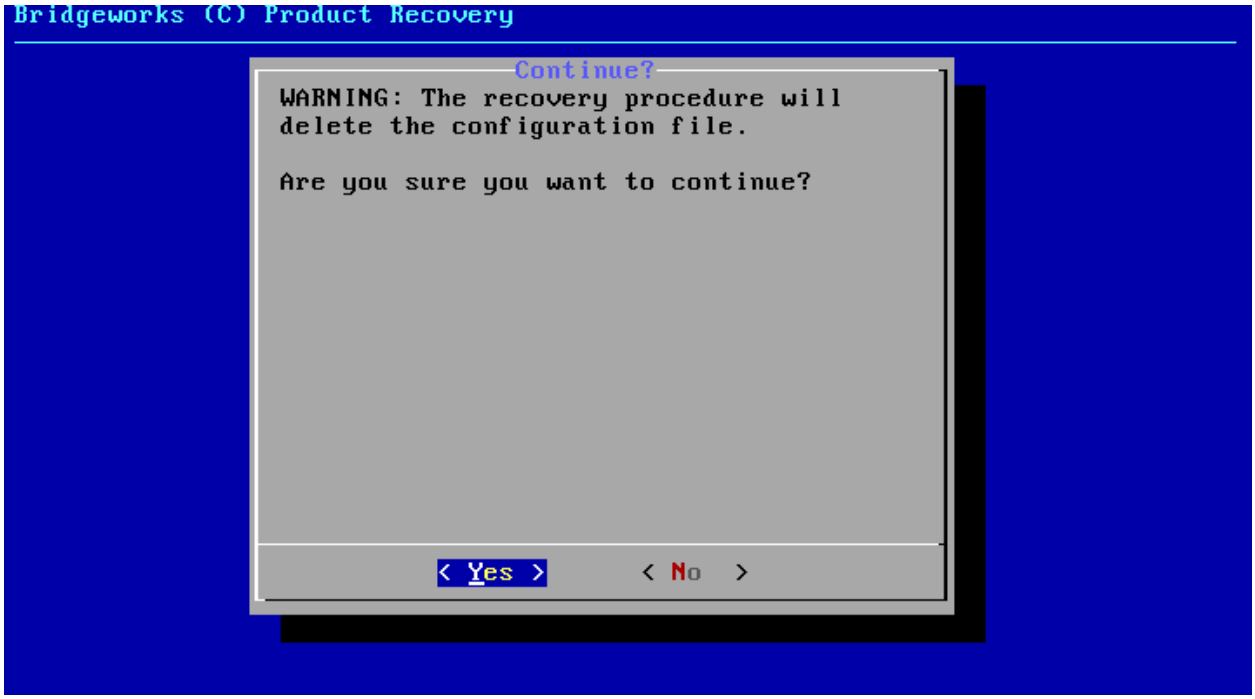
This option will delete your configuration file, removing any current configuration on your system but keeping your current firmware and licence keys.

To delete your configuration file, ensure that the *Delete Configuration* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the deletion process.

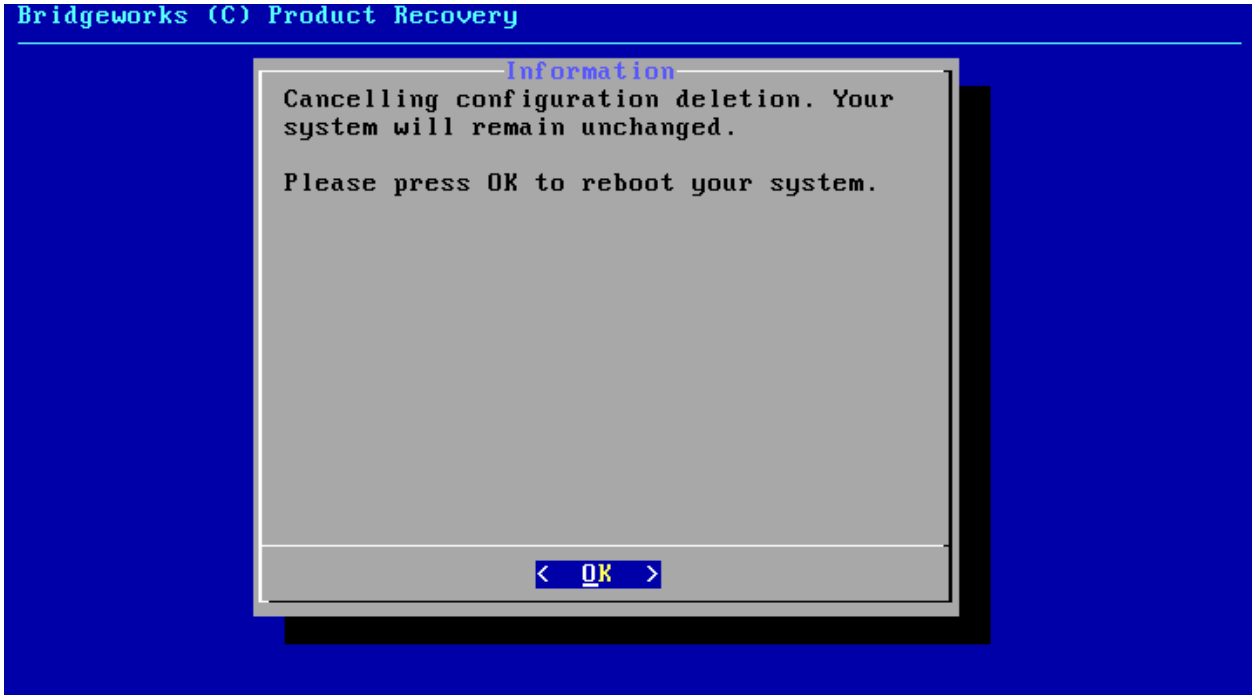


This procedure cannot be undone once complete; only continue if you are sure that you wish

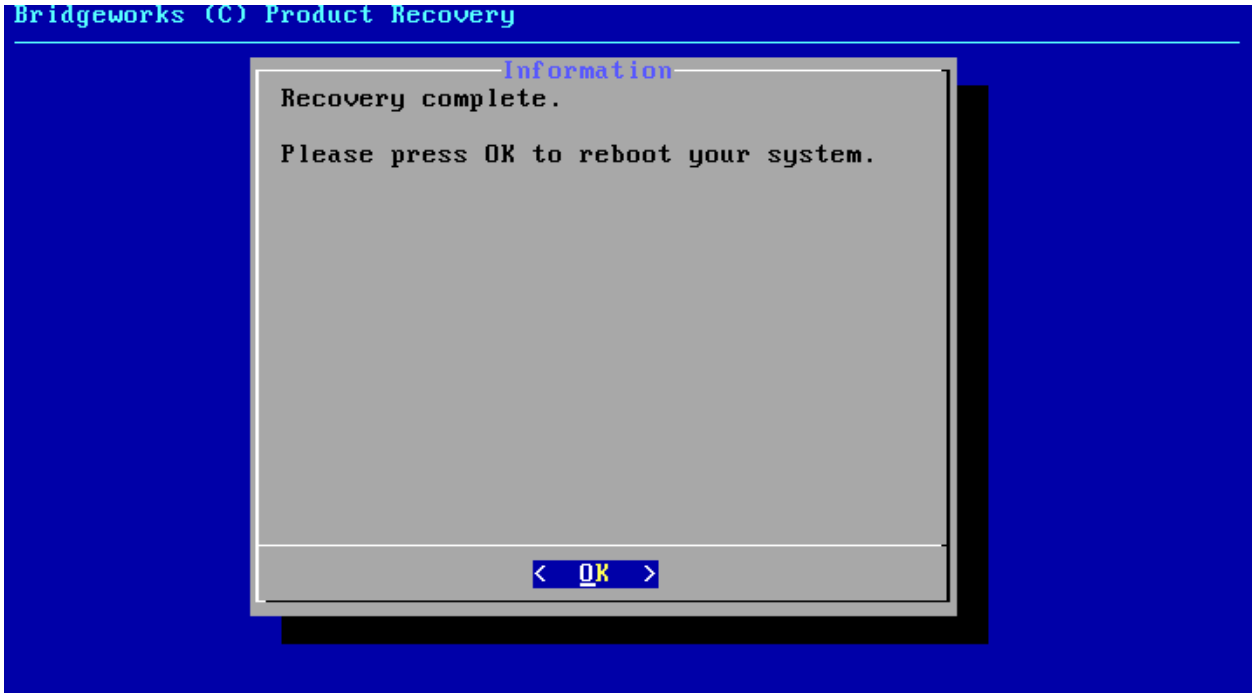
to do so. You will be asked to confirm that you wish to proceed. Choosing *Yes* will delete your configuration file and *No* will cancel the configuration deletion wizard.



If you cancel the deletion wizard at this point nothing on your system will be affected.



Once the delete configuration procedure has completed successfully you will need to reboot your system.



When the Recovery Wizard completes and you connect to the web interface of your unit, it will be reset to its original configuration. For help re-establishing your setup see Section 2.2: Connecting to the Web Interface.

A IP Protocols and Port Numbers

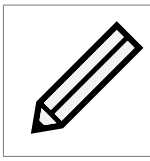
For the Node to be able to communicate with other network hosts, it may be necessary to contact your network administrator to ensure that the required IP protocols & port numbers are available.

A.1 Inbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 22	SSH	Required to access the configuration console through management interfaces when SSH is enabled. See Section 3.2.5: Secure Shell (SSH).
TCP 80	HTTP	Required to access the web interface through management interfaces when HTTP is enabled.
TCP 443	HTTPS	Required to access the web interface through management interfaces when HTTPS is enabled.
TCP 860/3260	iSCSI	The iSCSI Target can be configured to use one or both ports. See Chapter 10: iSCSI Target Configuration.
TCP 8002		Required to access the remote web interface using Remote Control when HTTP is enabled on the controlling Node. See Section 4.2.7: Remote Control.
TCP 8082		Required to access the remote web interface using Remote Control when HTTPS is enabled on the controlling Node.
UDP 161	SNMP	Required for management interfaces to respond to Simple Network Management Protocol requests, see Section 3.3.2: Simple Network Management Protocol (SNMP).

A.2 Outbound LAN Protocols and Port Numbers

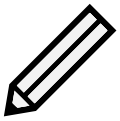
Protocol/Port	Name	Description
TCP 25	SMTP	Simple Mail Transfer Protocol, see Section 3.3.3: Email.
TCP 3205	iSNS	Internet Storage Name Service protocol, see Section 3.3.5: Internet Storage Name Service (iSNS).
UDP 123	NTP	Network Time Protocol, see Section 3.3.1: Network Time Protocol (NTP).
ICMP		Internet Control Message Protocol. Required by dead gateway detection (see Section 3.1.2.5: Dead Gateway Detection) and network debugging tools (see Section 3.1.5: Network Tools).



Note: The iSCSI Initiator uses TCP port 3260 by default, but may use any TCP port specified during target discovery. See Section 9.1: Discovering an iSCSI Target.

A.3 WAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 16665	axon-tunnel	Reliable multipath data transport for high latencies
UDP 4500	ipsec-nat-t	IPsec NAT-Traversal
UDP 500	isakmp	Internet Security Association and Key Management Protocol
ESP		IP Encapsulating Security Payload



Note: Only TCP Port 16665 is required if not using IPsec encryption or VPN functionality on the PORTrockIT product.

B Accessing the Node from Windows using a static IP Address

This appendix describes how to configure a Windows host to access the Node's web interface from its default static IP address, if DHCP is not enabled on the Node.

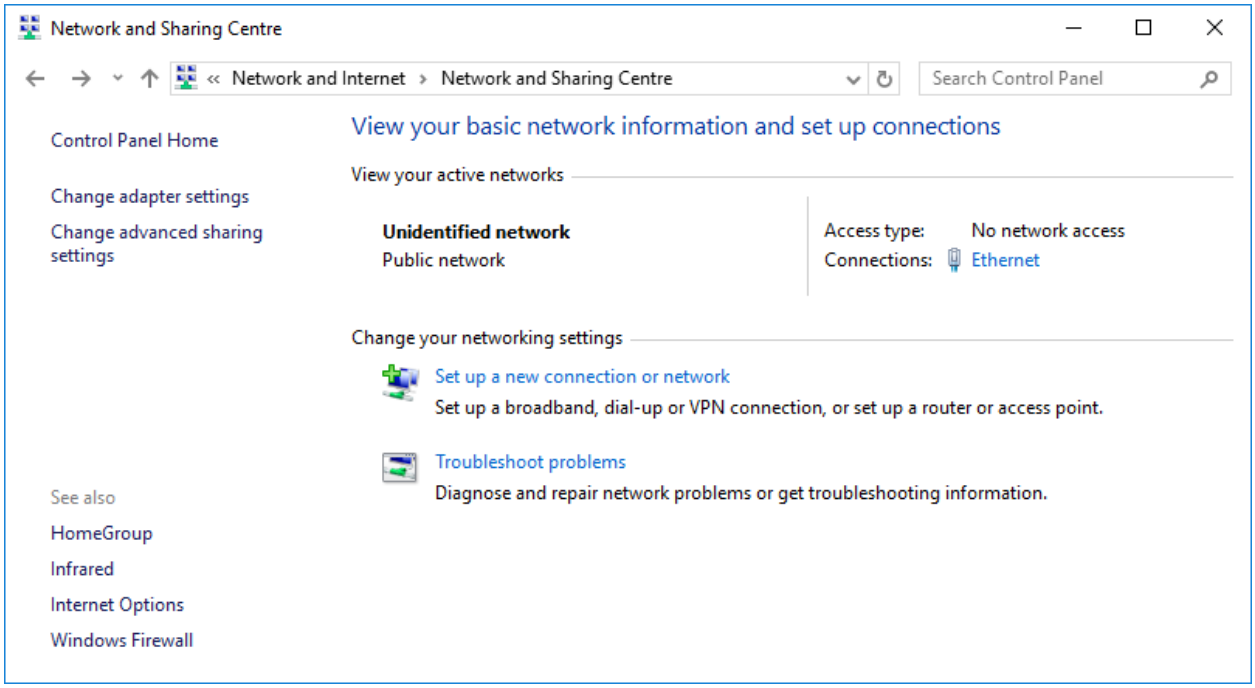
These instructions apply to Windows Vista, 7, 8, 10 and to Windows Server 2008, 2012, 2016, 2019 and their respective R2 versions.

⚠	Warning: Administrative privileges may be required to modify network device settings.

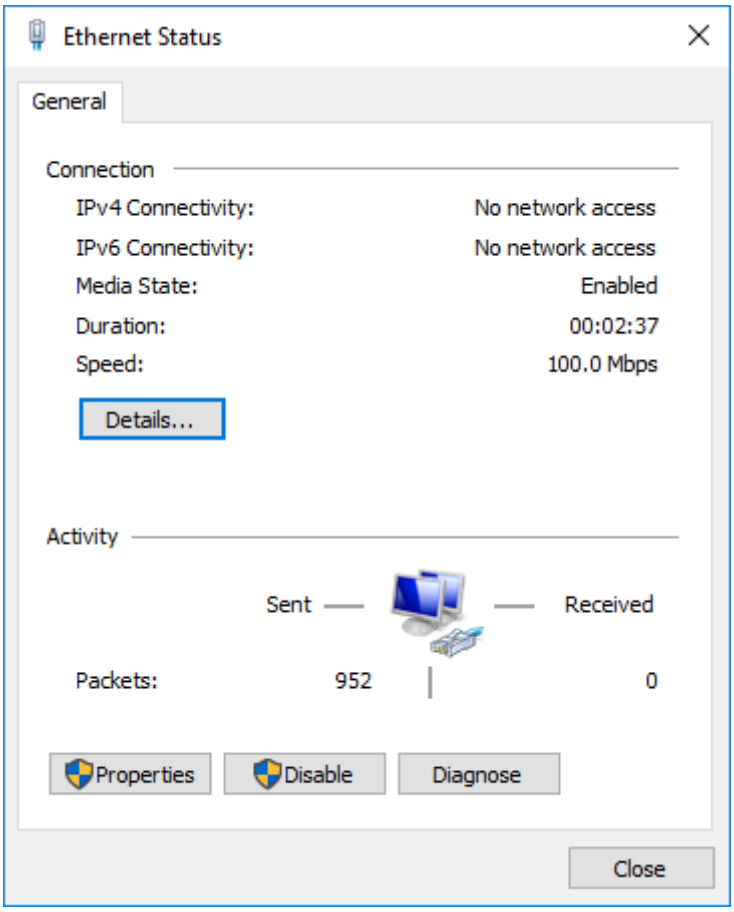
From the Start menu, select *Control Panel*.

ⓘ	Important: It may be required to search for "Control Panel" in the Start menu before it appears as an entry.

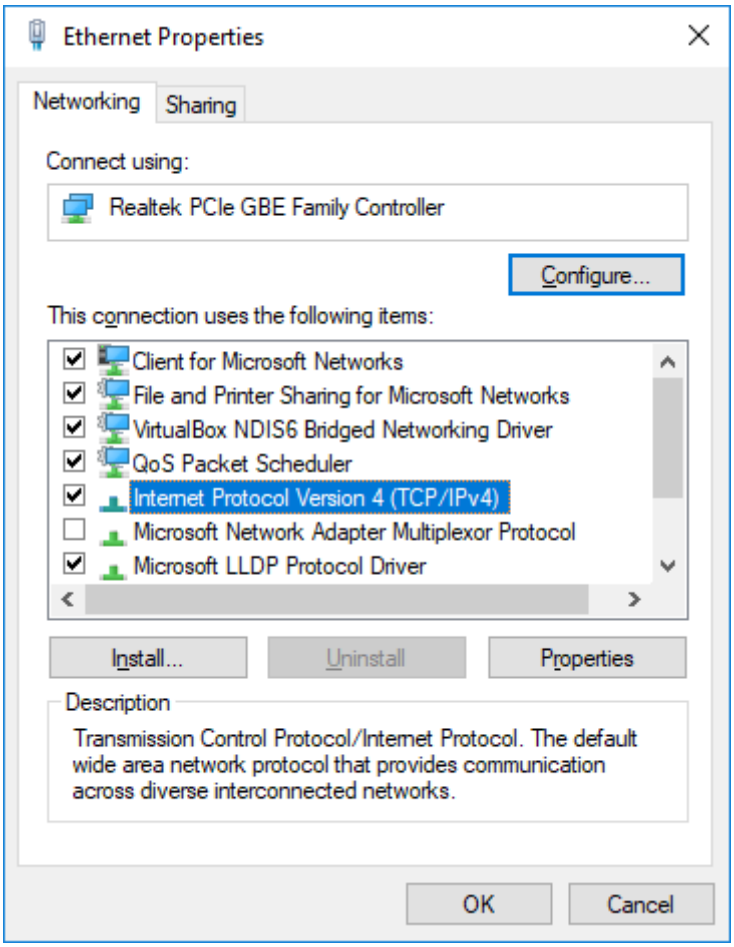
From the Control Panel select the *Network and Internet* link, followed by the *Network and Sharing Centre* link. Click on the link next to "Connections" for your respective network. This is named "Ethernet" in the screenshot below.



A general status page will be displayed. From within this page select *Properties*.

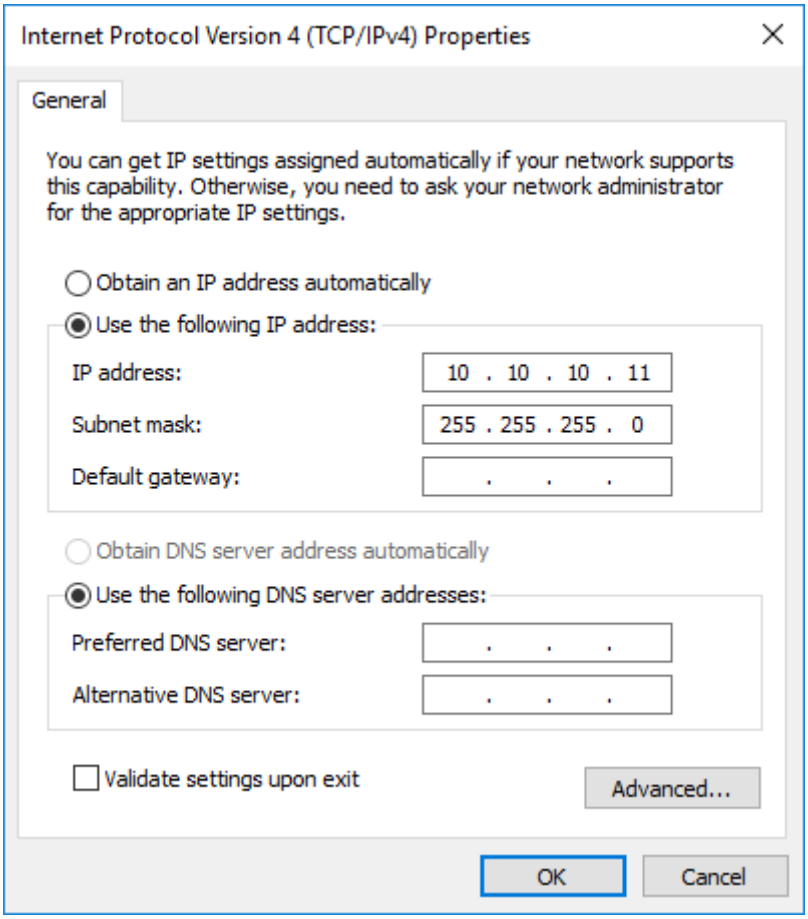


Select the *Internet Protocol Version 4 (TCP/IPv4)* entry and then *Properties*.



Before continuing, make a note of your current configuration as it will be modified. Afterwards,

1. Click *Use the following IP Address*.
2. Enter *10.10.10.11* into the *IP Address* field.
3. Enter *255.255.255.0* into the *Subnet Mask* field.
4. Finally click the *OK* button.



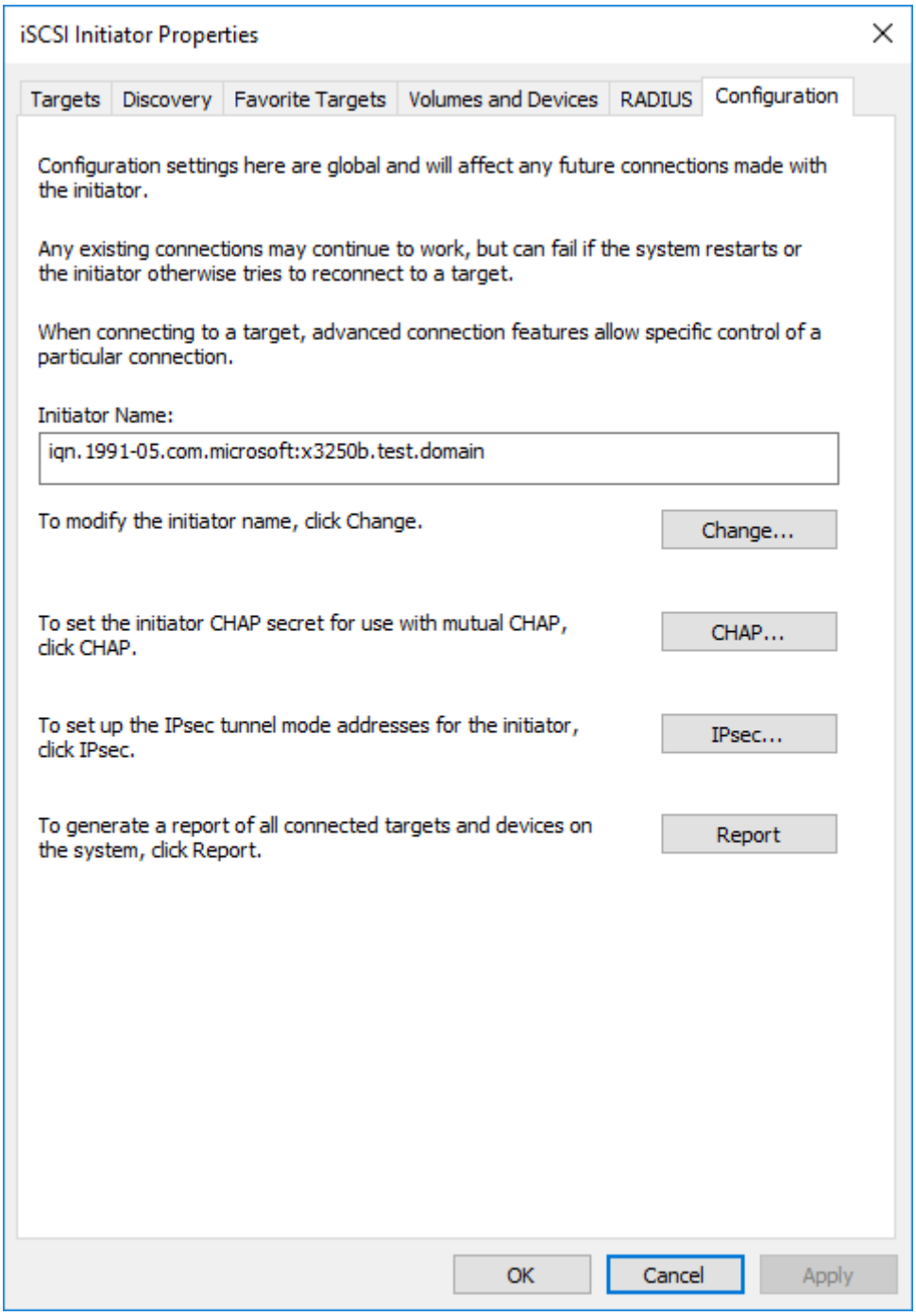
	Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

C Connecting to an iSCSI Device using the Microsoft iSCSI Initiator

There are many iSCSI Initiators available. However, for the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI Initiator that is available with Microsoft Windows Server 2019. However, the following procedure is similar for all versions of Microsoft iSCSI Initiator.

C.1 General Set up

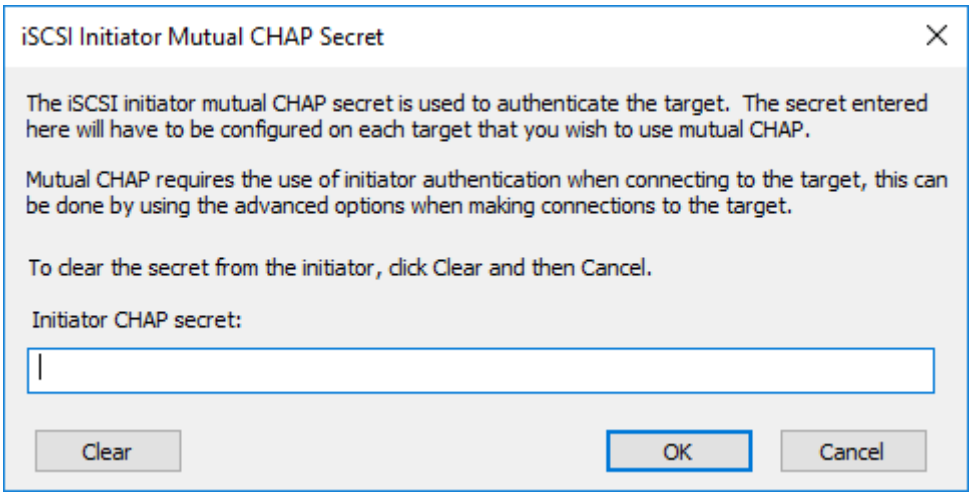
Open the iSCSI initiator and then click on the *Configuration* tab. You should see the following page:



From this page, you are able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.

If you intend to use Mutual CHAP authentication you must enter the Initiator secret from this page.

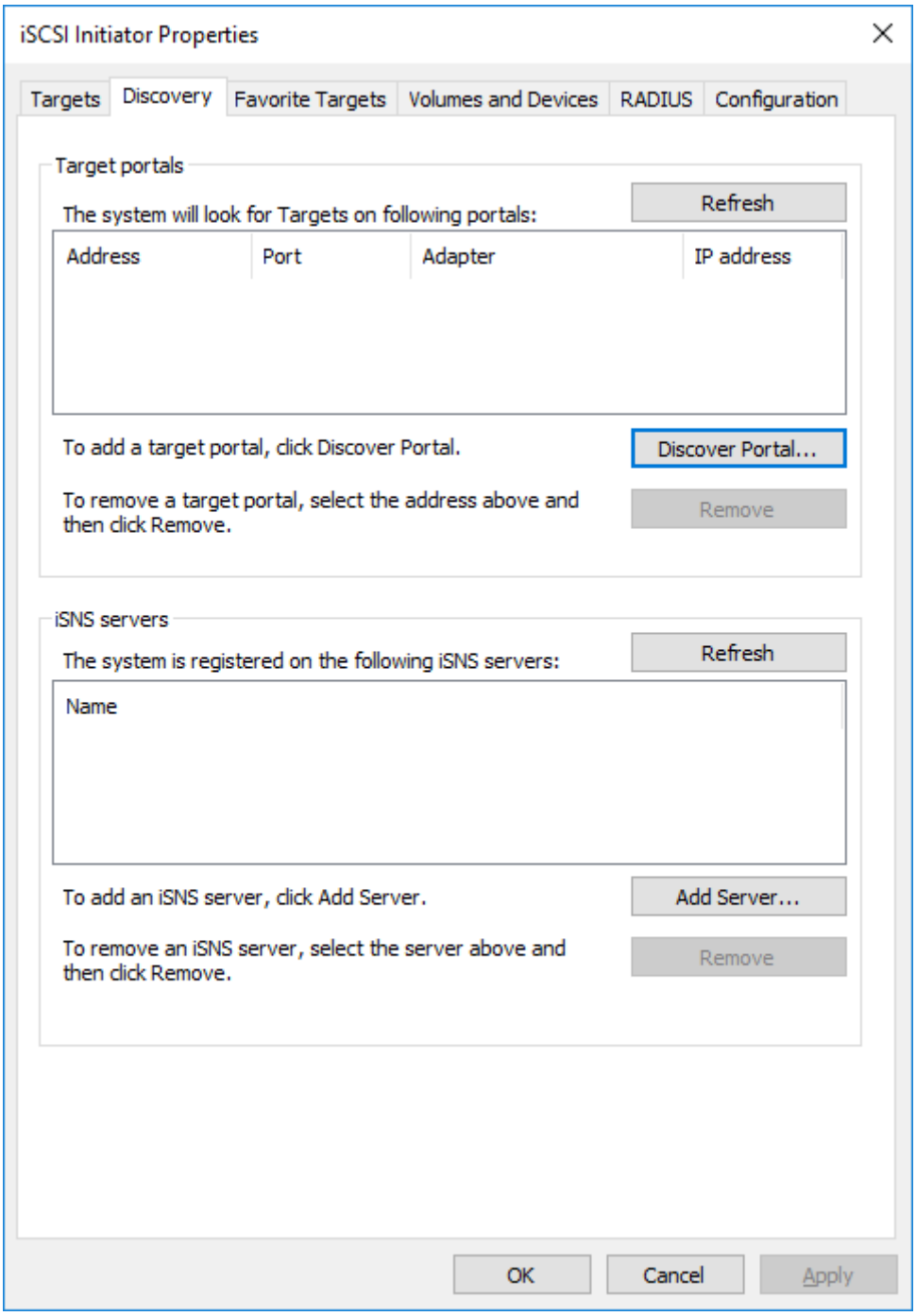
Click on the *CHAP...* button and the following window should be displayed:



Enter in the Initiator CHAP secret and click OK. The secret should be between 12 and 16 characters. Make a note of this secret as you will need to enter this as part of configuring CHAP on the iSCSI Node.

C.2 Discovery of Devices

Before you can connect to an iSCSI Target, the iSCSI targets must be discovered. Click on the *Discovery* tab and you should see the following page:

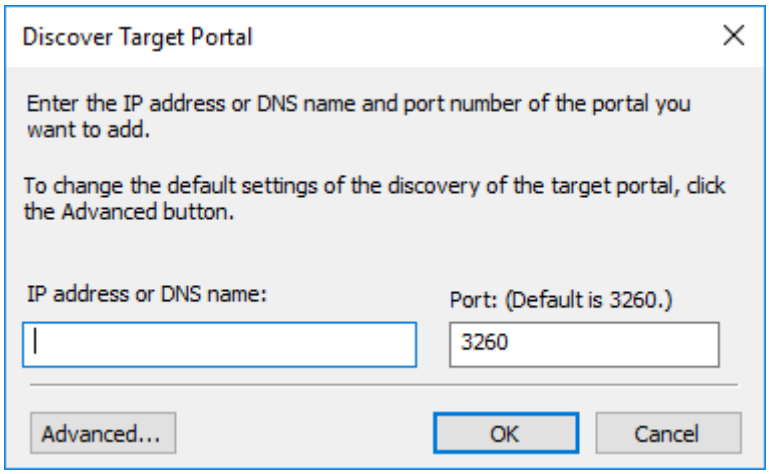


Devices can be discovered in one of two ways:

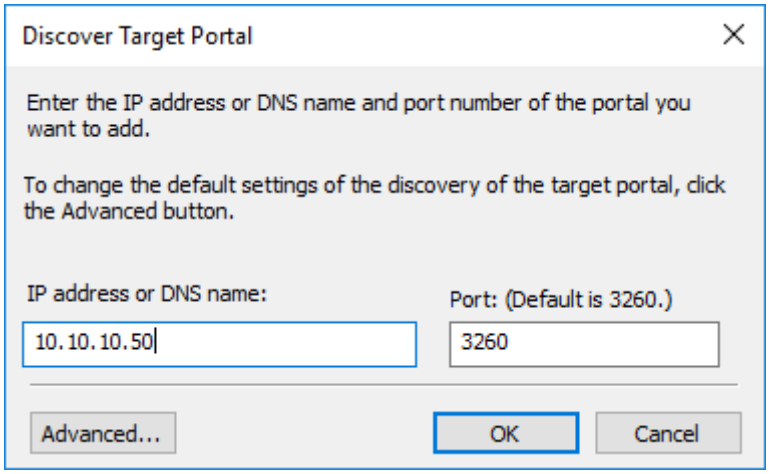
- Adding an iSCSI target portal and directly performing a discovery;
- Adding an iSNS server to which the target portal is registered.

C.2.1 Adding an iSCSI Target Portal

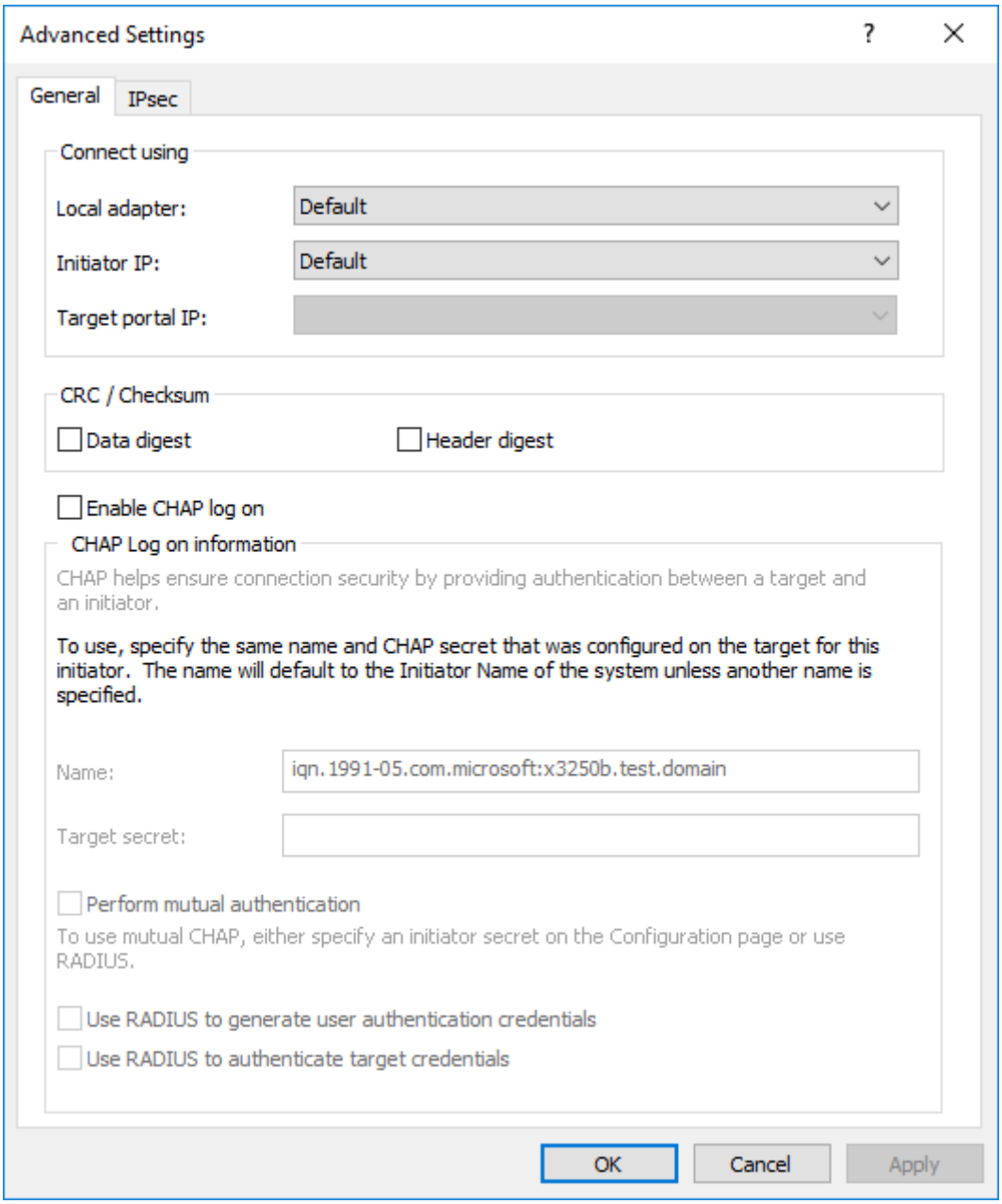
To add an iSCSI Target portal, click on *Discover Portal…*. You should now be presented with the following window:



Enter the IP address for the iSCSI Target. In this example we shall use the IP address `10.10.10.50`.

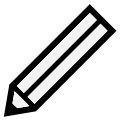


Leave the port at 3260 unless you have configured your iSCSI Node to only respond on port 860, in which case change it to 860. Click on the *Advanced* button to see the advanced options.



The *Connect using* section allows you to specify which iSCSI adapter to use and the Initiator IP. The *Local adapter* should only differ from Microsoft iSCSI Initiator if an iSCSI offload card has been installed. For the purpose of this guide, we shall only use the Microsoft iSCSI Initiator. Leaving this setting as *Default* will also use the Microsoft iSCSI Initiator.

The *Initiator IP* is used to specify upon which network adapter the discovery will be done. In most cases you will want to leave this as default. If multiple network interfaces are installed in the Server and you wish to select a particular interface, select the IP address of that network interface from the drop down list.

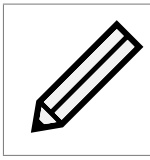


Note: You may need to select a specific local adapter in order to chose certain initiator IP addresses.

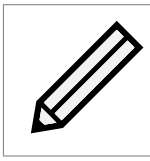
CRC/Checksum settings allow you to specify whether the discovery is done using Data and/or

Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

If the iSCSI Node has CHAP enabled, or you wish to authenticate the iSCSI Node, click on the checkbox *Enable CHAP log on* to enable CHAP. Now enter the username and target secret that are configured on the iSCSI Node. If you wish to authenticate the iSCSI Node, select *Perform mutual authentication*.



Note: For mutual CHAP to be performed, the *Initiator Secret* must be set on the general tab, and be the same as the one configured on the iSCSI Node.

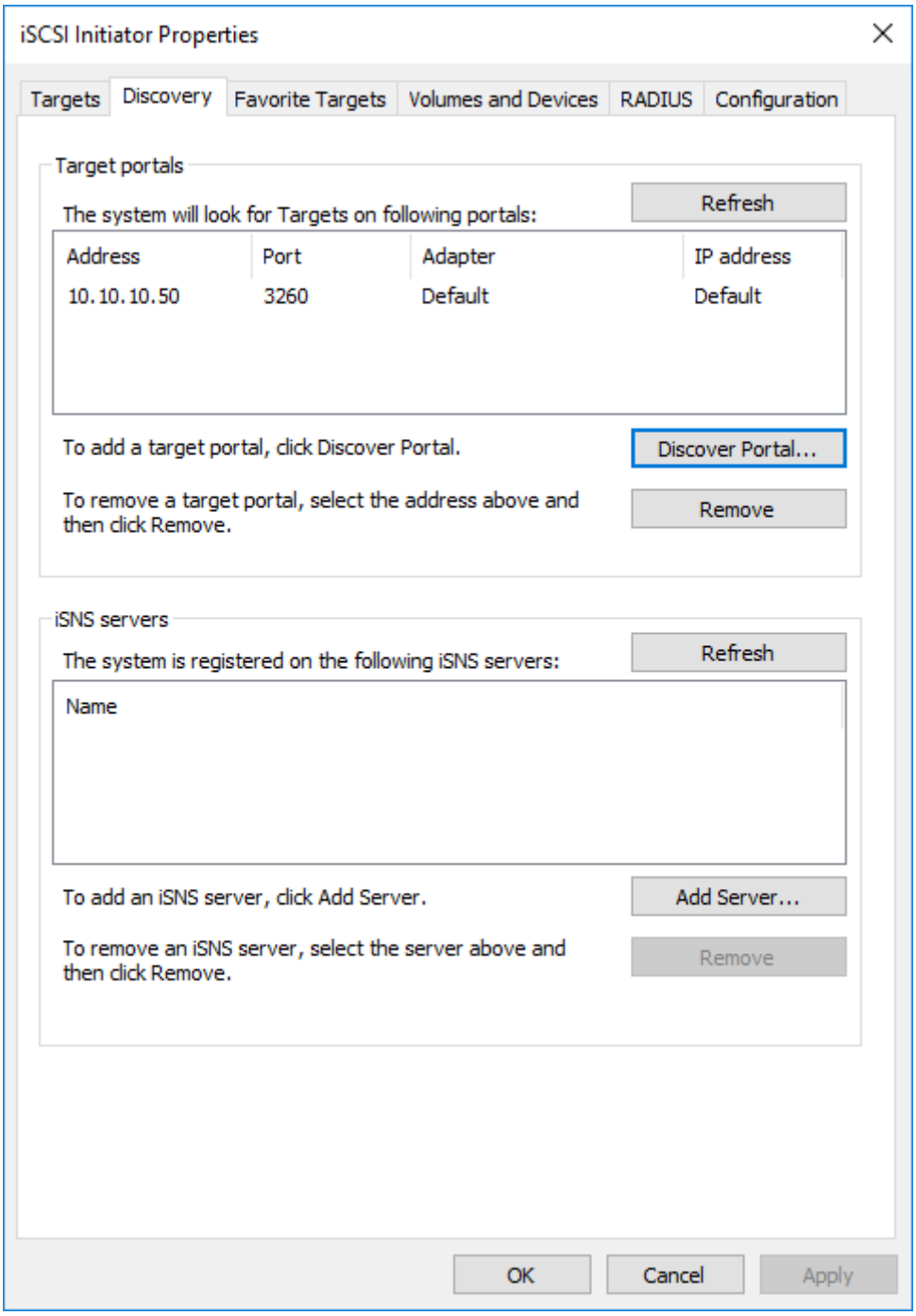


Note: The use of RADIUS is beyond the scope of this guide.

Once you are satisfied that all advanced options are correct, click OK.

Now click OK in the *Discover Target Portal* window, and the Microsoft iSCSI Initiator shall perform the discovery. This is usually a quick process, but can take up to a minute with multiple network ports.

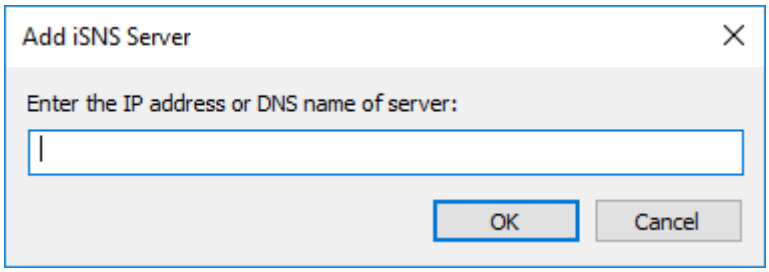
Once the discovery is complete, you should see the target listed in the *Target portals* list:



C.2.2 Adding an iSNS Server

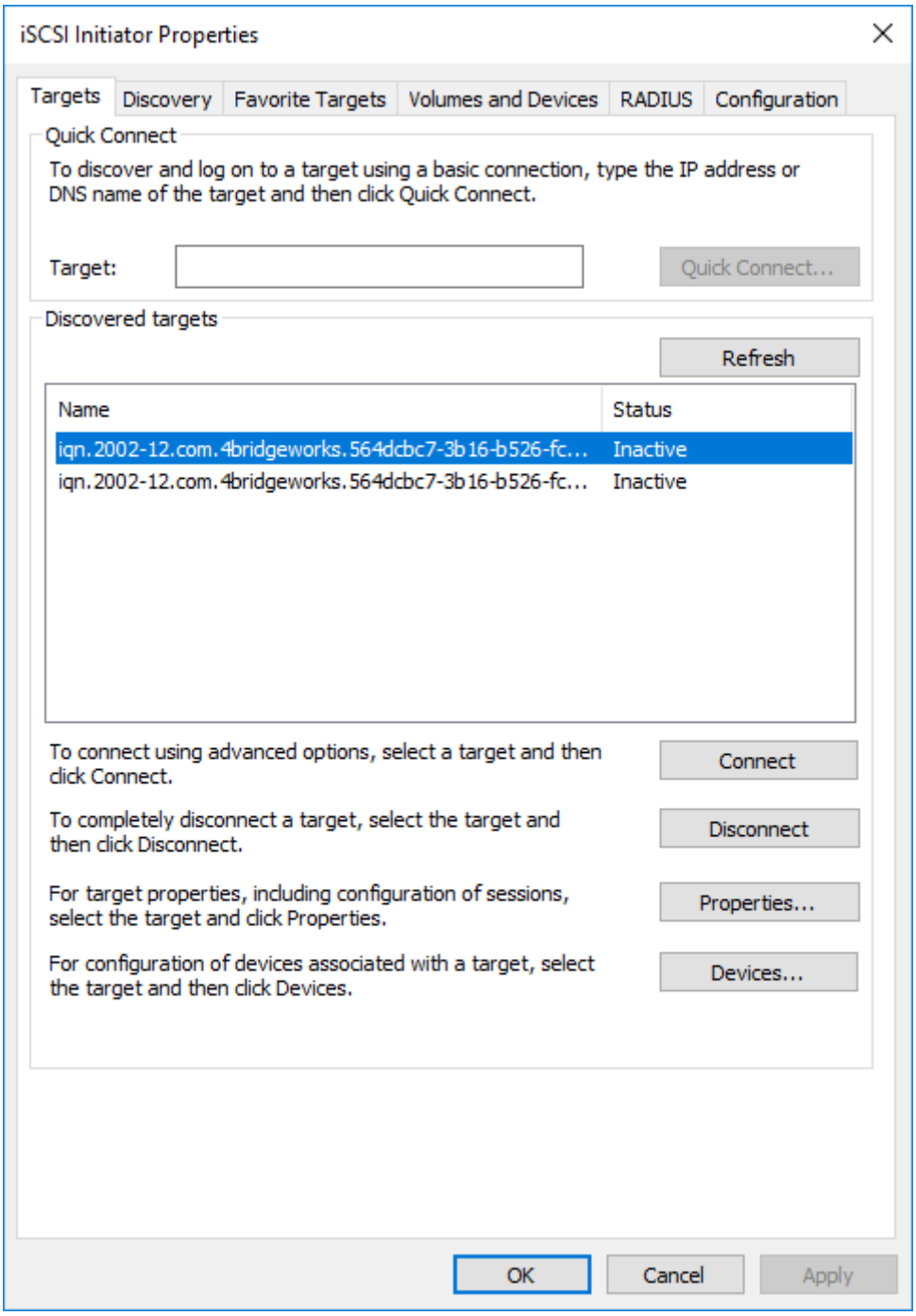
To discover iSCSI targets using this method, your iSCSI Node must be registered with your designated iSNS server. See Section 3.3.5: Internet Storage Name Service (iSNS) for more information.

Under *iSNS servers*, click *Add*. The following window should appear:



Enter the address of the iSNS server with which your iSCSI Node is registered, then click *OK*. The Microsoft iSCSI Initiator will now query the iSNS server and perform discoveries on registered target portals.

Click on the *Targets* tab. The discovered devices should now be listed.

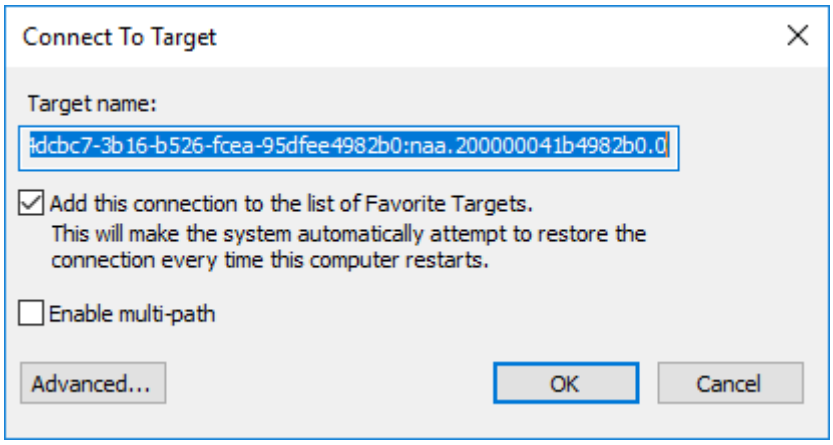


In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check that the settings used to perform the discovery, including CHAP settings, are correct. Then return to *Targets* tab and click *Refresh*.

If still no devices are displayed, check network cables and that the iSCSI Node is operational.

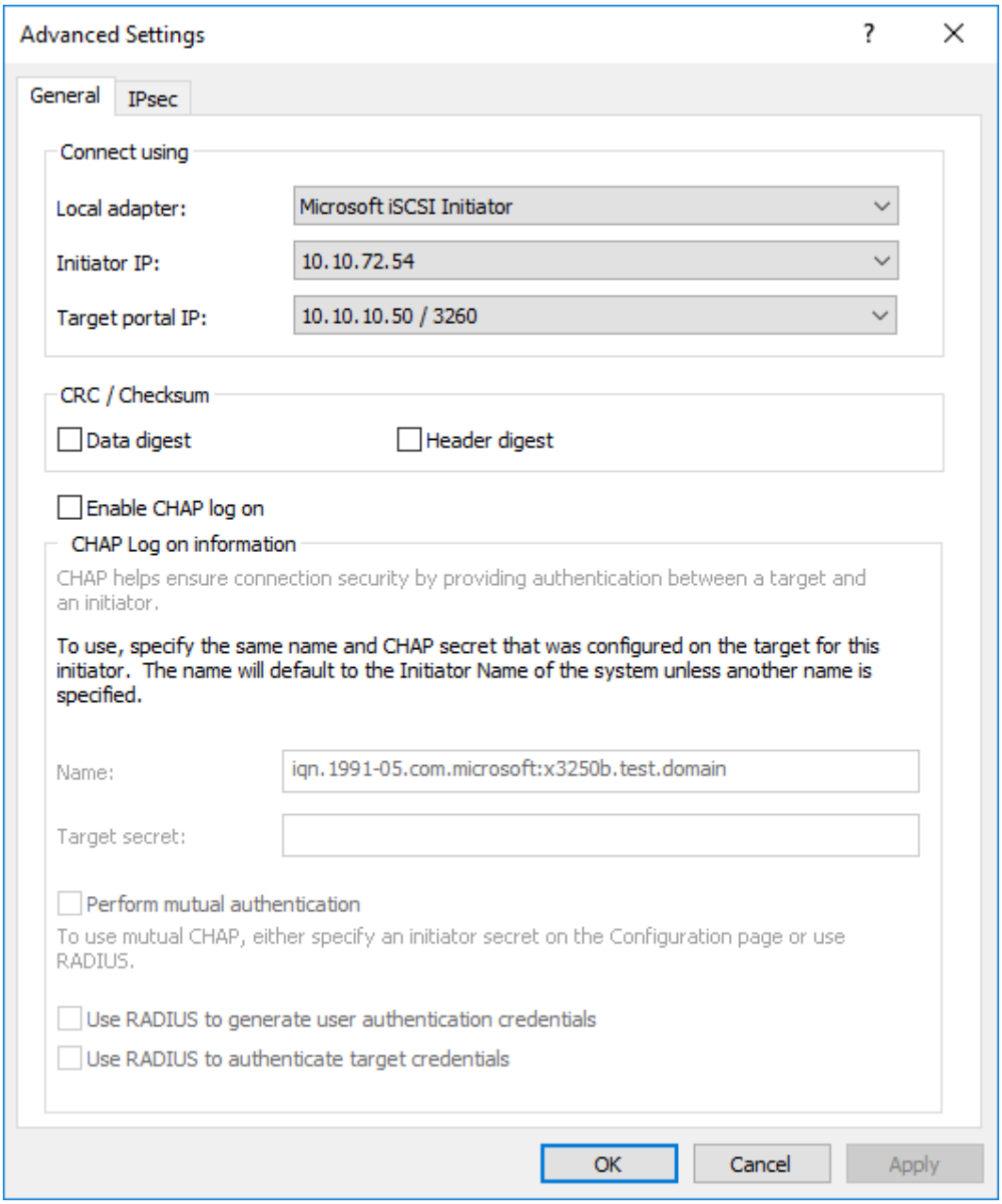
C.3 Connecting to a Target

To connect to one of the displayed iSCSI targets, click on its list entry, then click the *Connect* button. In this example we have chosen the first target. The following window should appear:



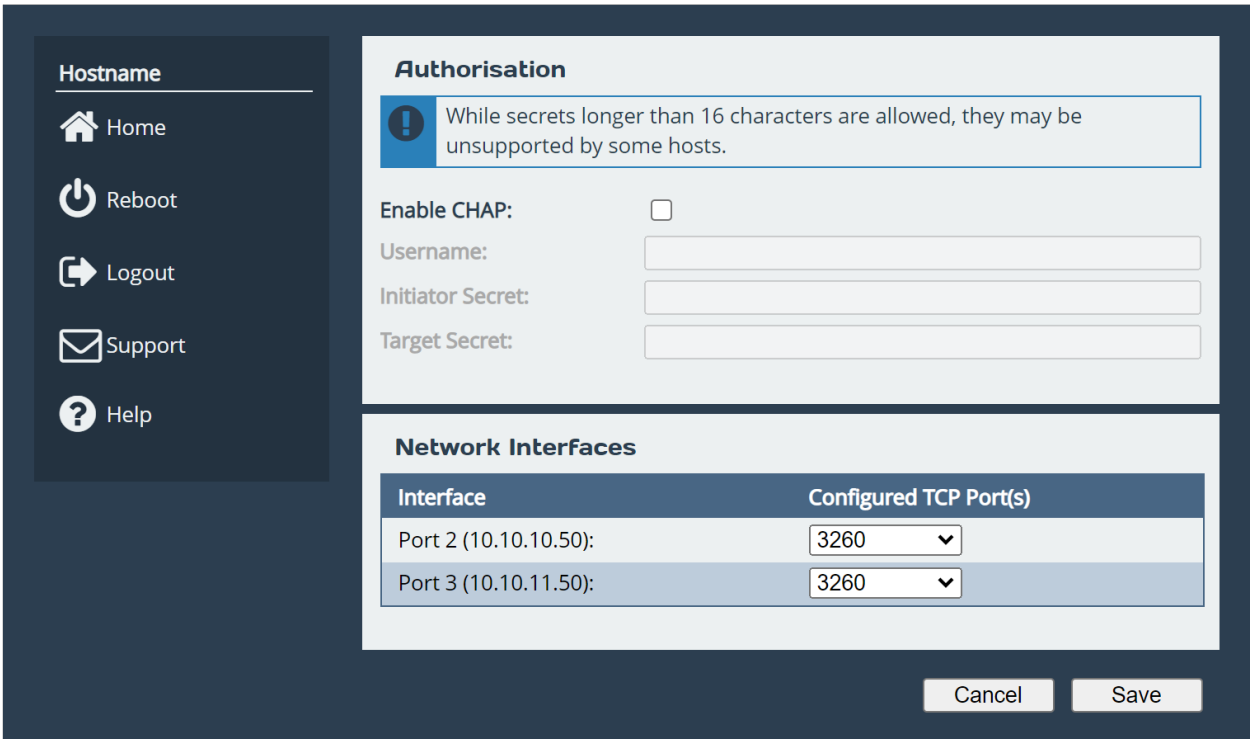
If you wish to reconnect to the target automatically when this Windows server reboots, select the *Add this connection to the list of Favorite Targets* checkbox.

Click on the *Advanced* button to see the advanced settings. The following window should appear:



The Advanced Settings page is the same as that of the discovery except for one addition. In the *Connect using* section, there is a *Target portal IP* option. This allows you to choose which interface of the iSCSI Node will be used to make the connection to the target. In this example we have chosen to connect to the IP address `10.10.10.50` on port 3260.

To see how this relates to the iSCSI Node configuration, note the IP addresses in the Network Interfaces subsection, on the iSCSI Target page of the iSCSI Node's web interface:

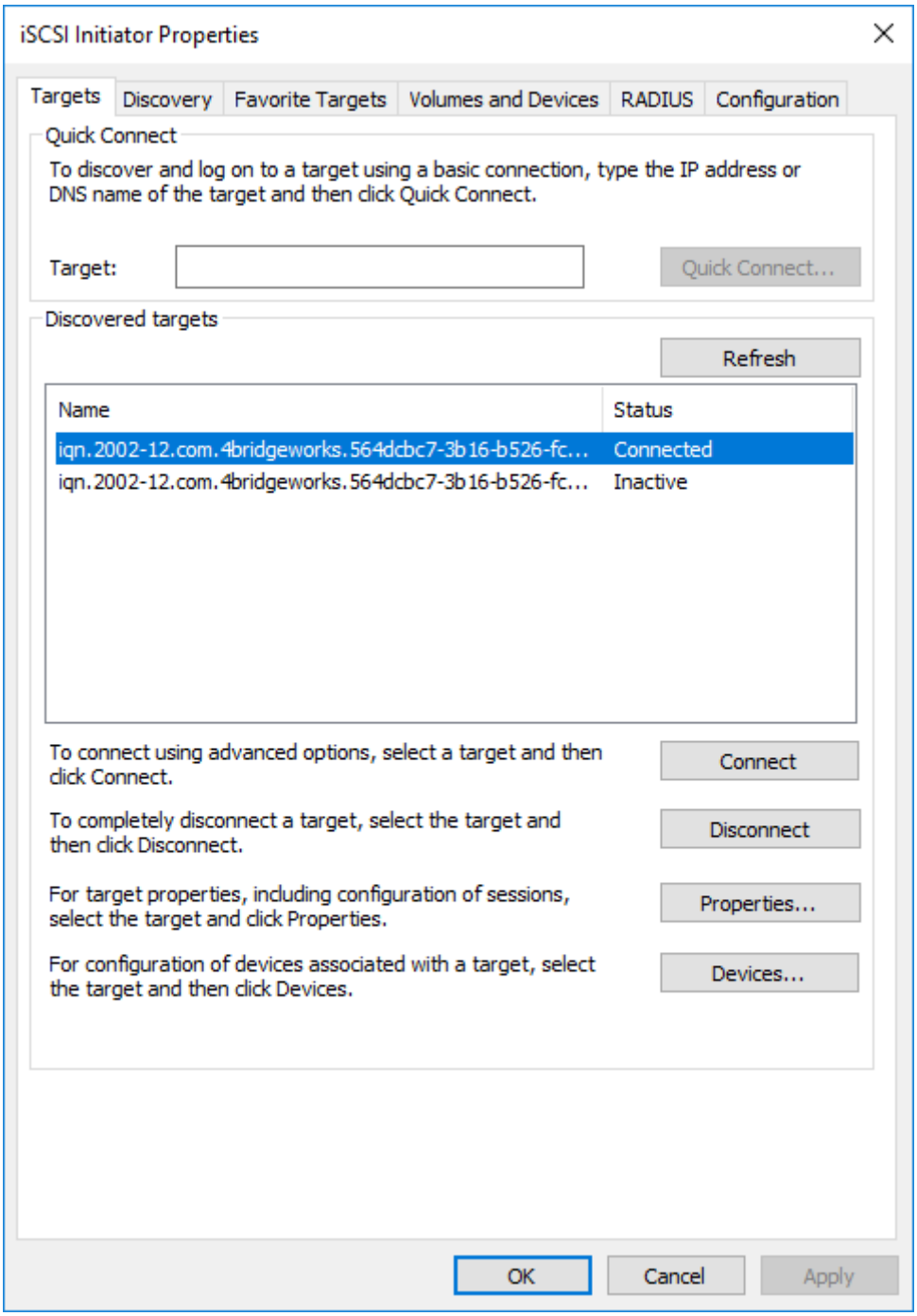


See Chapter 10: iSCSI Target Configuration for more information.

Important: If you wish to connect to a target over multiple network interfaces, see Appendix C.5: Creating Multiple Connections (Optional). For now, select the *Initiator IP* and *Target portal IP* for the first connection to the target.

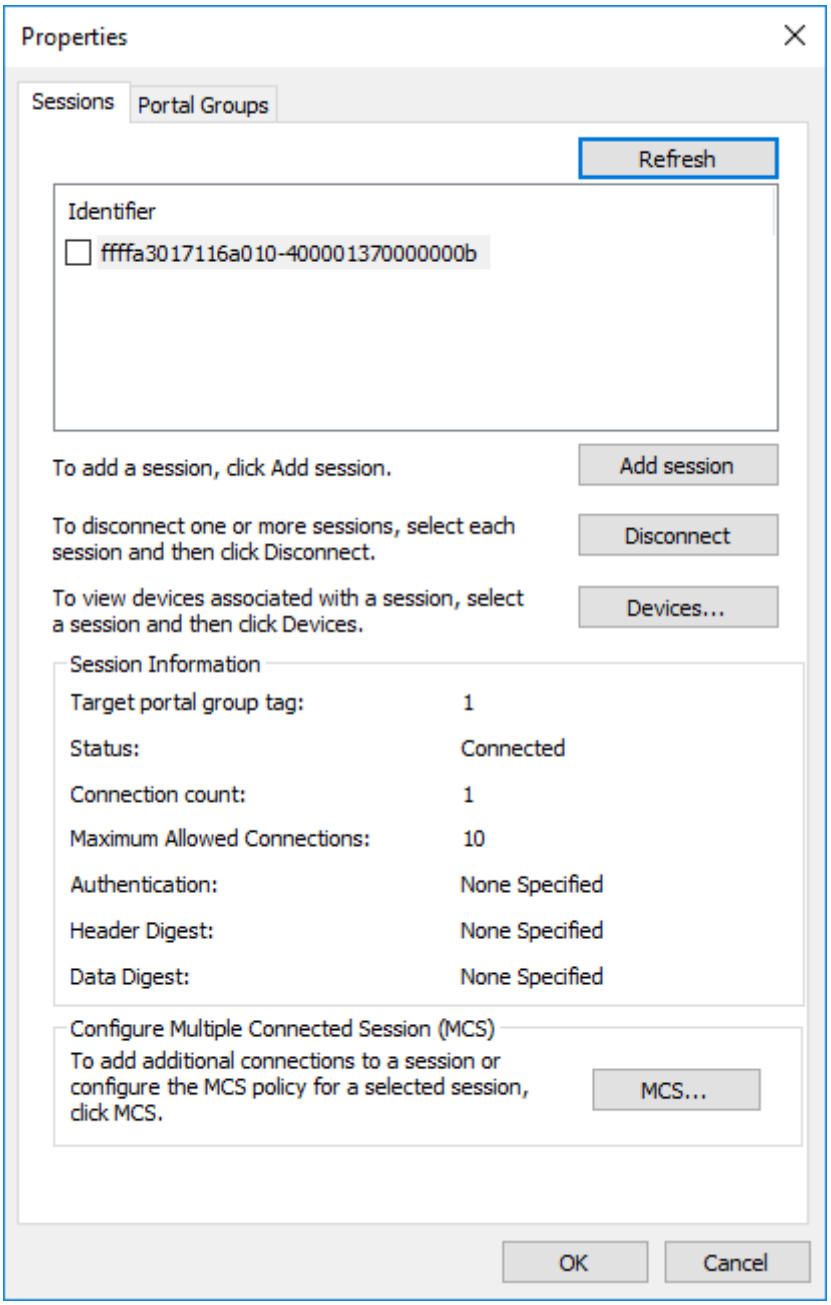
To set up the Digest and CHAP settings, see Appendix C.2: Discovery of Devices.

The list entry for the target should now display *Connected* in the *Status* column:



C.4 Viewing iSCSI Session Details

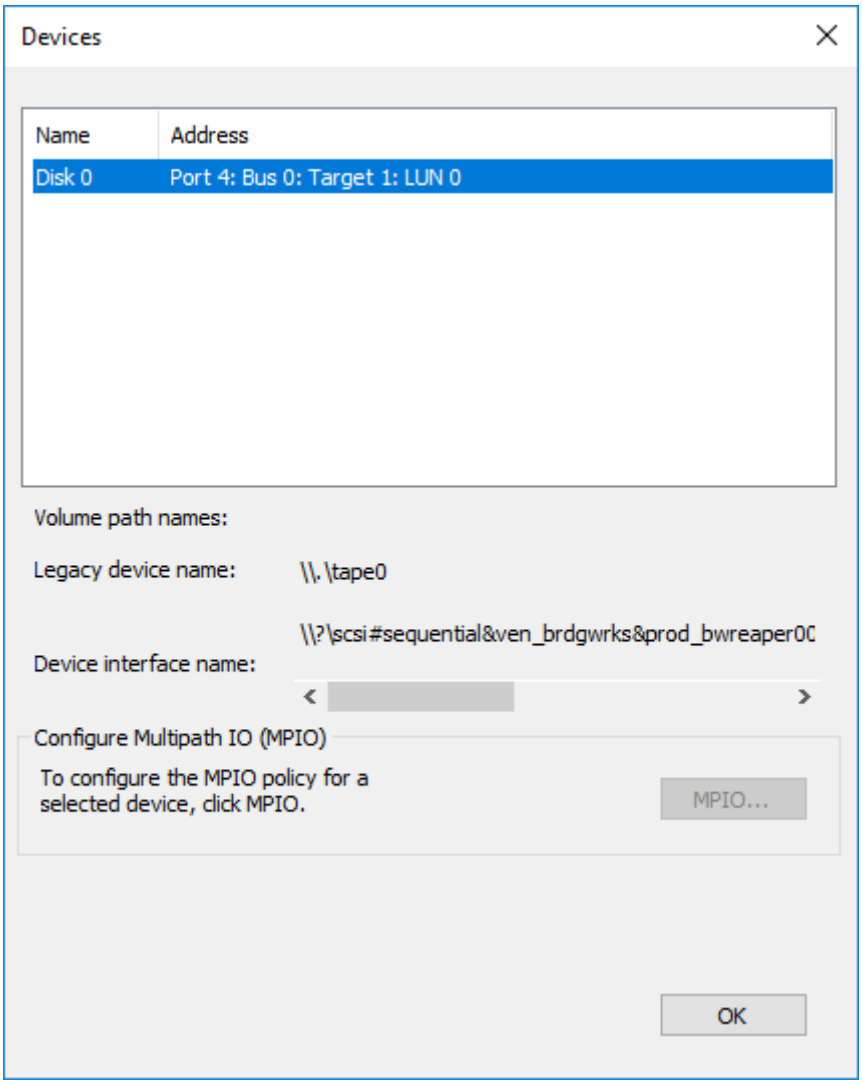
When you have connected to an iSCSI Target, you can check that the device is connected by clicking on the *Properties...* button. The following window will appear:



In this window you can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group.

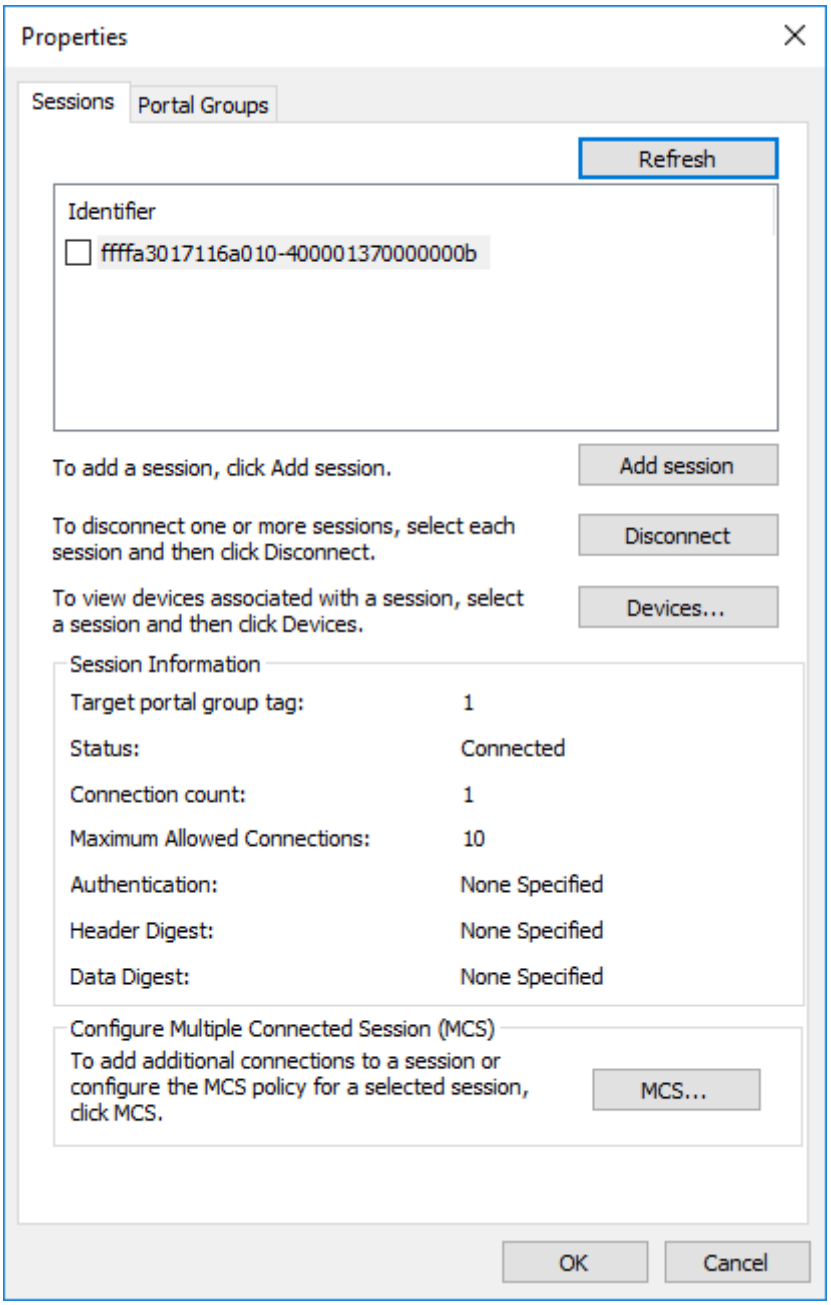
If you click on the *Devices…* button, details of the target device will be displayed. Here for example, we can see that the device is a tape drive. Indicated by it's legacy device name of

.
tape0.

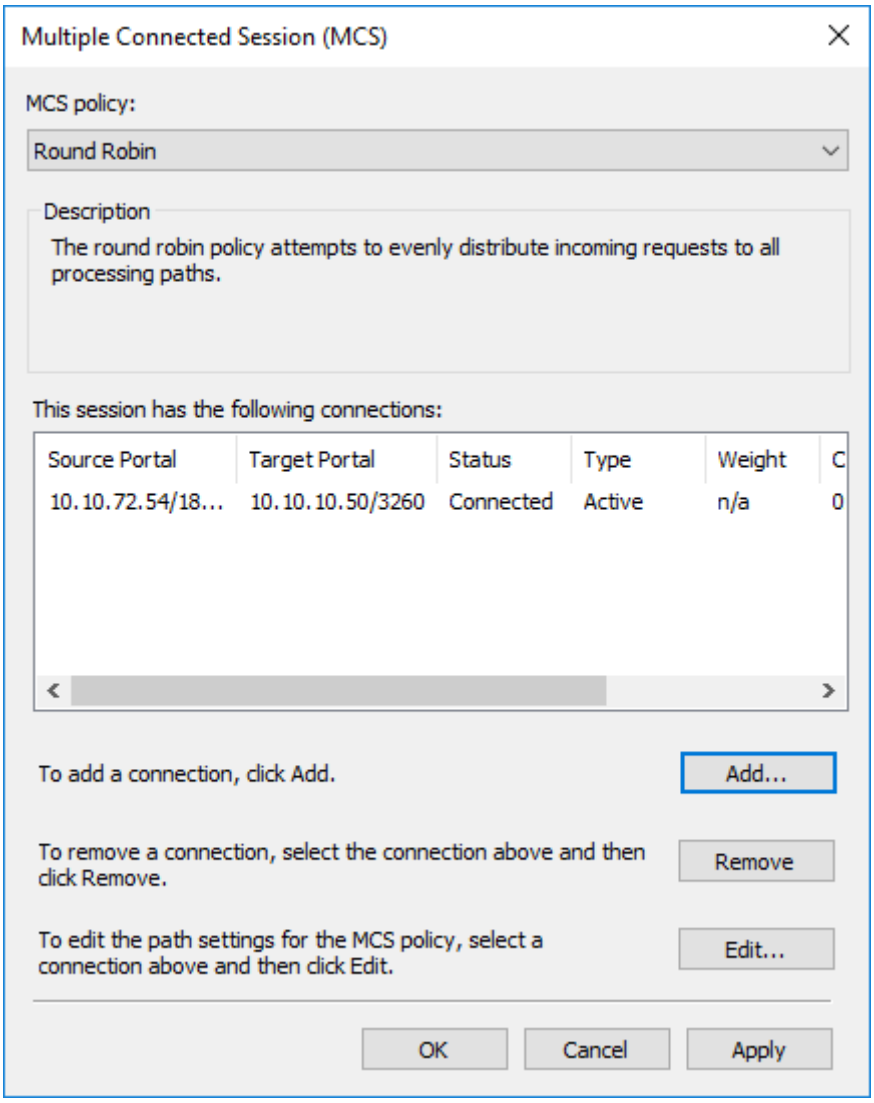


C.5 Creating Multiple Connections (Optional)

To set up Multiple Connections per Session (“MCS”), open the target properties window, by selecting the target from the *Discovered targets* list on the *Targets* tab and clicking *Properties…*.



Click on the *MCS…* button to open the *Multiple Connected Session (MCS)* window:



This shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions, there will be at least one leading connection.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

Note: The *MCS policy* specifies how the data is distributed over multiple connections. Unless you have reason to select one of the more advanced policies, *Round Robin* and *Fail Over Only* are recommended.

Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the *Active* connection for data transfer. If a connection should go down then the data transfer shall switch to one of the *standby* connections.

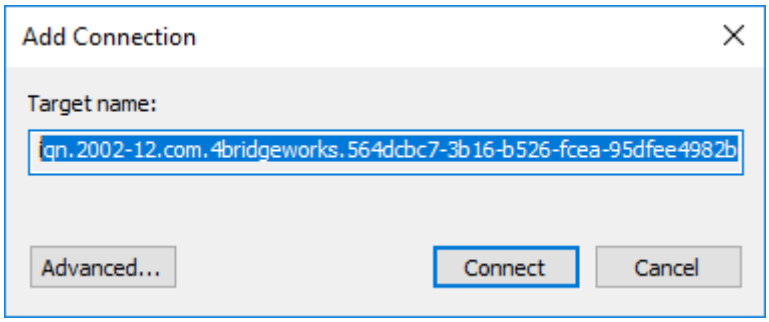
Round Robin With Subset combines *Round Robin* and *Fail Over* operating as *Round Robin* until all *Active* paths have failed, where upon *standby* paths will be tried.

Least Queue Depth assigns each new operation to the connection with the fewest commands already queued.

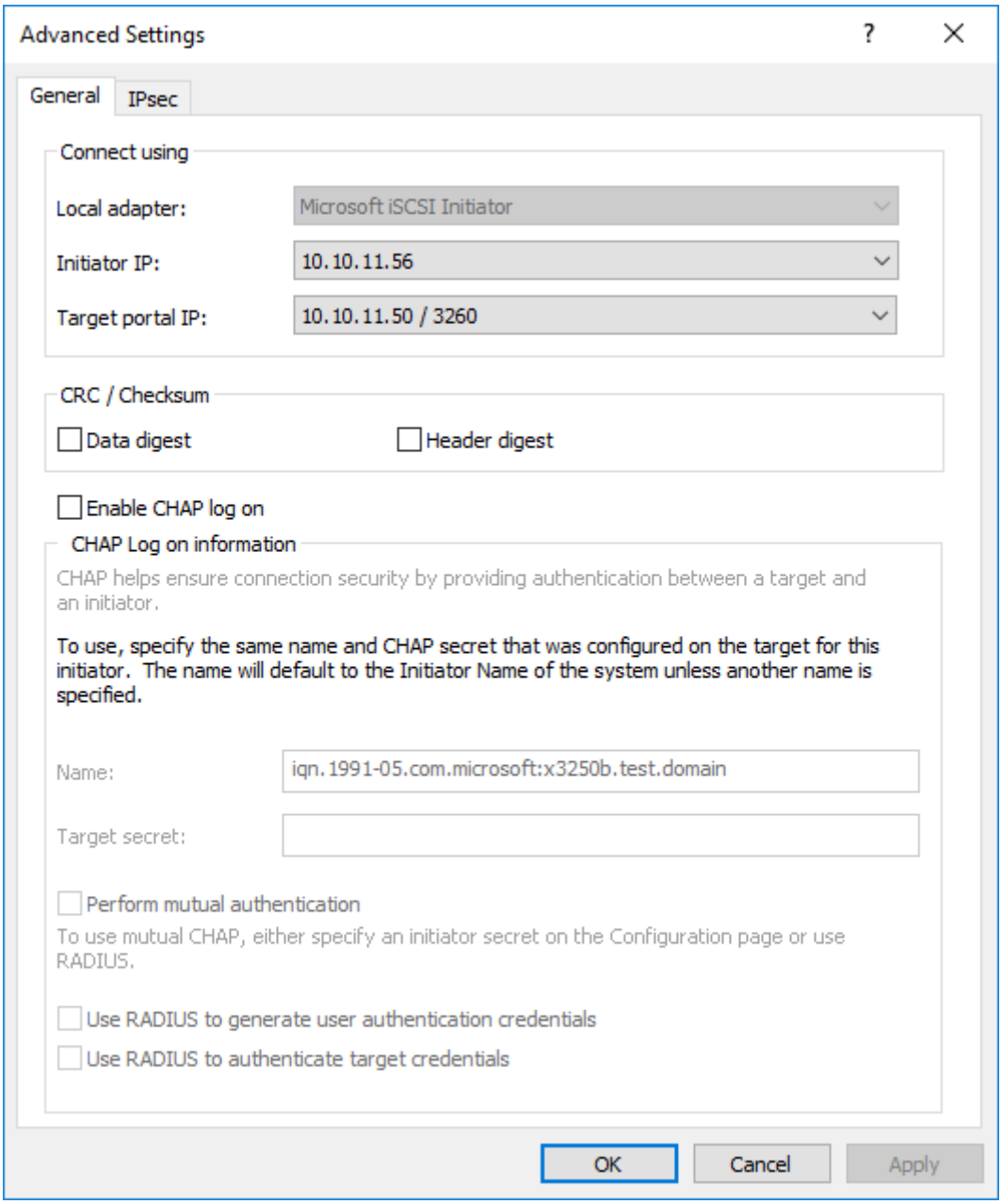
Weighted Paths allows the administrator to assign a path weight per connection, operations are queued to the least weighted available path.

For most purposes, *Round Robin* will provide the best performance.

To add a new connection to a session, click on the *Add…* button to open the following window:

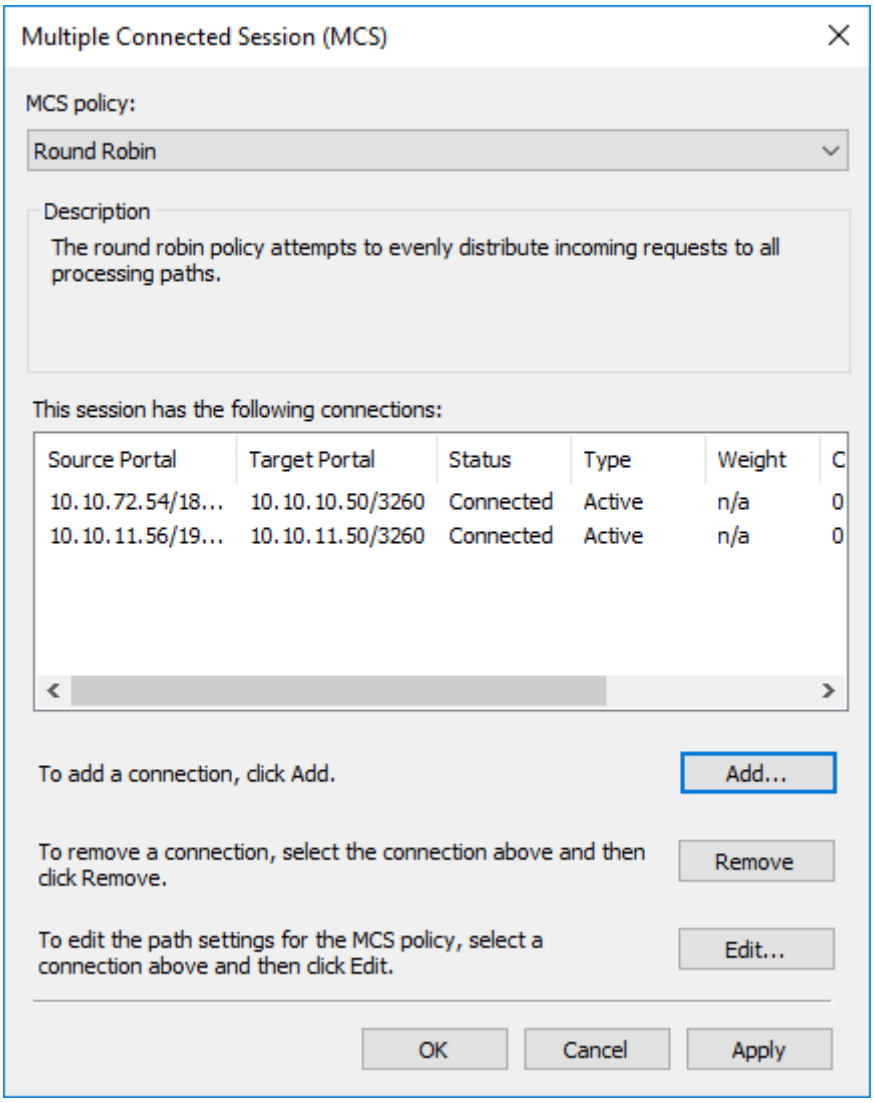


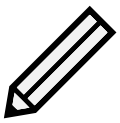
Then click *Advanced…* to open *Advanced Settings*:



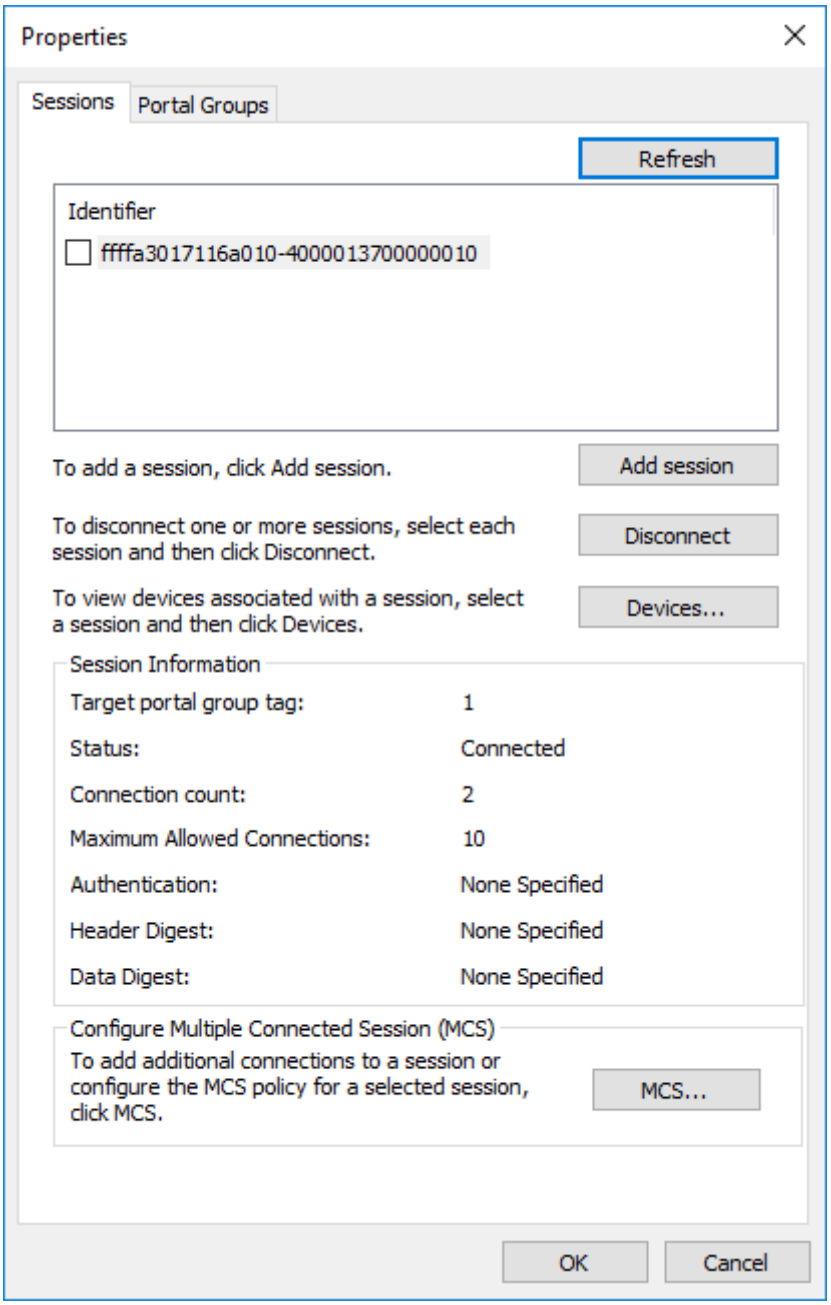
In the *Connect using* section, select the *Initiator IP* address and the *Target portal IP* address for the new connection. In most instances these should be different from the source and target addresses of the original connection. In this example we have connected to `10.10.10.50 / 3260` as the leading connection, and the second connection will be `10.10.11.50 / 3260`.

Configure CHAP and Header/Data Digest, and click OK. Then click OK within the *Add Connection* window and now you should see the new, additional connection listed in the *Multiple Connected Session (MCS)* window.



	Note: Up to 10 connections can be added to one session.

Once you have completed setting up the connections, click OK to return to the *Properties* window. Under *Session Information*, you will see that the *Connection count* value has increased:



Now click on OK to return to the Microsoft iSCSI Initiator main window.

	Important: If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to Chapter 14: Troubleshooting.

C.6 Logging off an iSCSI Session

To log off an iSCSI Session, follow the following procedure.

1. Open the Microsoft iSCSI Initiator and click on the *Targets* tab.
2. Click on the iSCSI session that you wish to log off and then click *Properties*….

3. In the *Properties* window, select the *Sessions Tab* and select the identifier that is to be logged off.
4. Click the *Disconnect* button. This will log off all connections associated with the iSCSI Session.
5. The session identifier should now be removed from the identifier list. Click *OK* to return to the main iSCSI Initiator window.

The iSCSI device should now show as inactive.

D Connecting to an iSCSI Device using iscsiadm

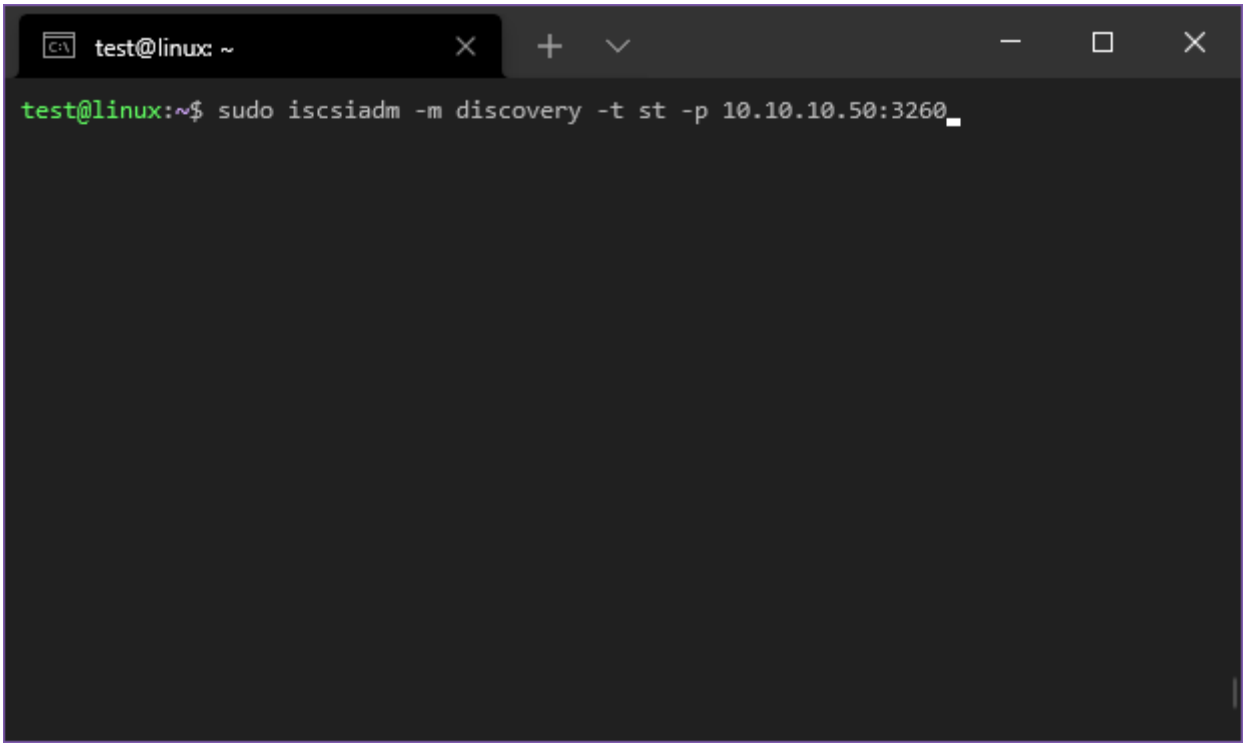
Important: The `iscsiadm` command may require root privileges to function. This guide will assume that the user has root privileges.

D.1 Discovering iSCSI Targets

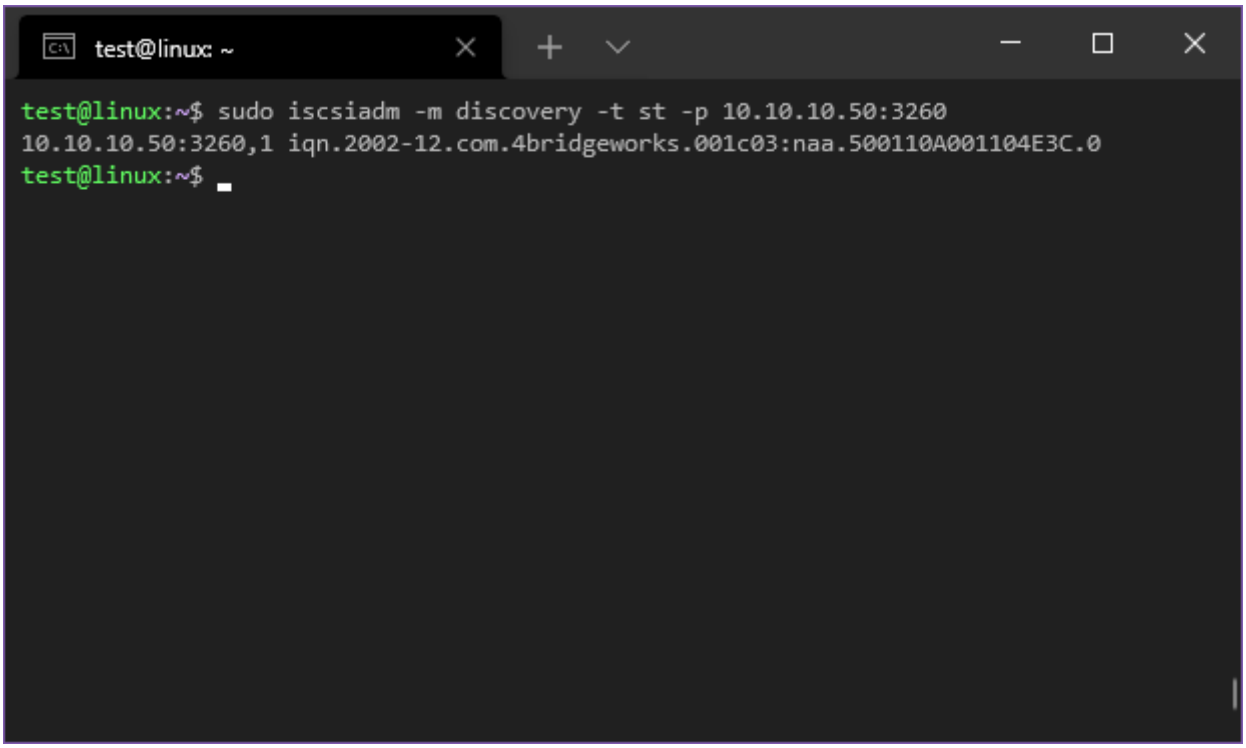
To get a list of available targets on the Node, run a discovery using the following command:

```
iscsiadm -m discovery -t st -p <Target IP Address>:<Port Number>
```

An example of this is shown below when performing a discovery on a target with the IP address 10.10.10.50 on port 3260.



When the command is run, you should see a list of available targets as shown below:

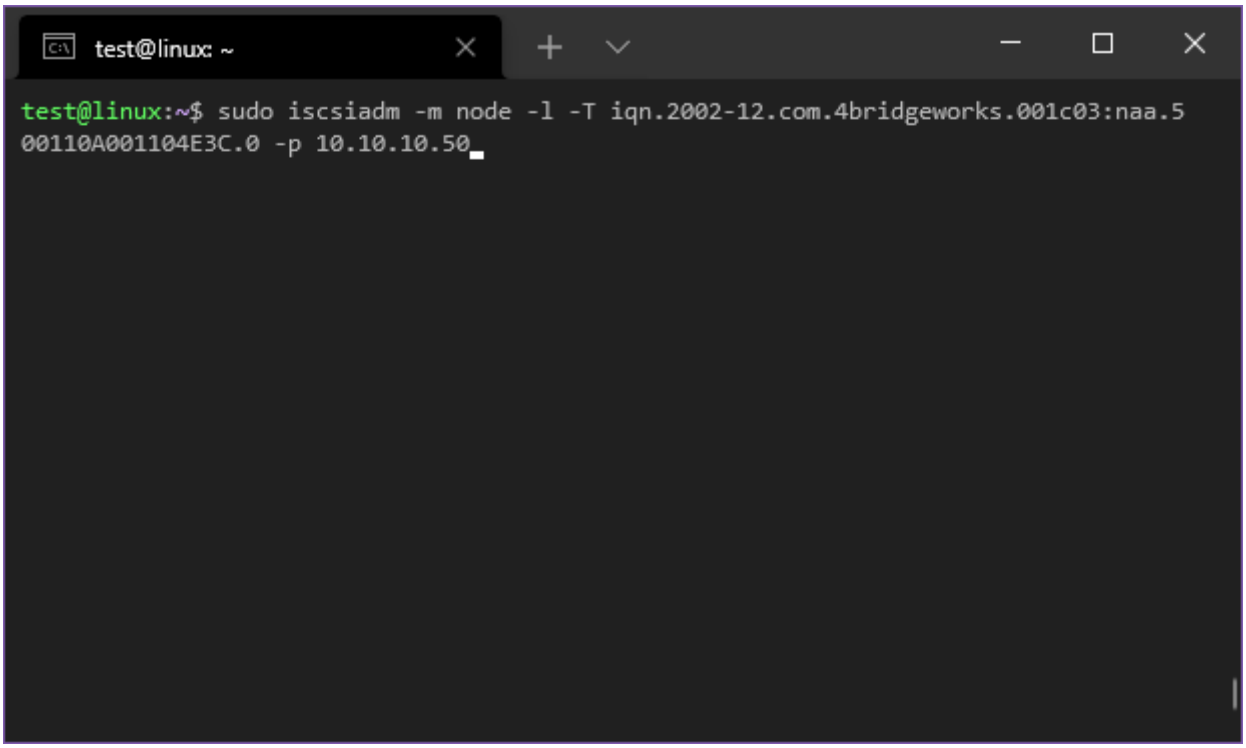


D.2 Logging into a target

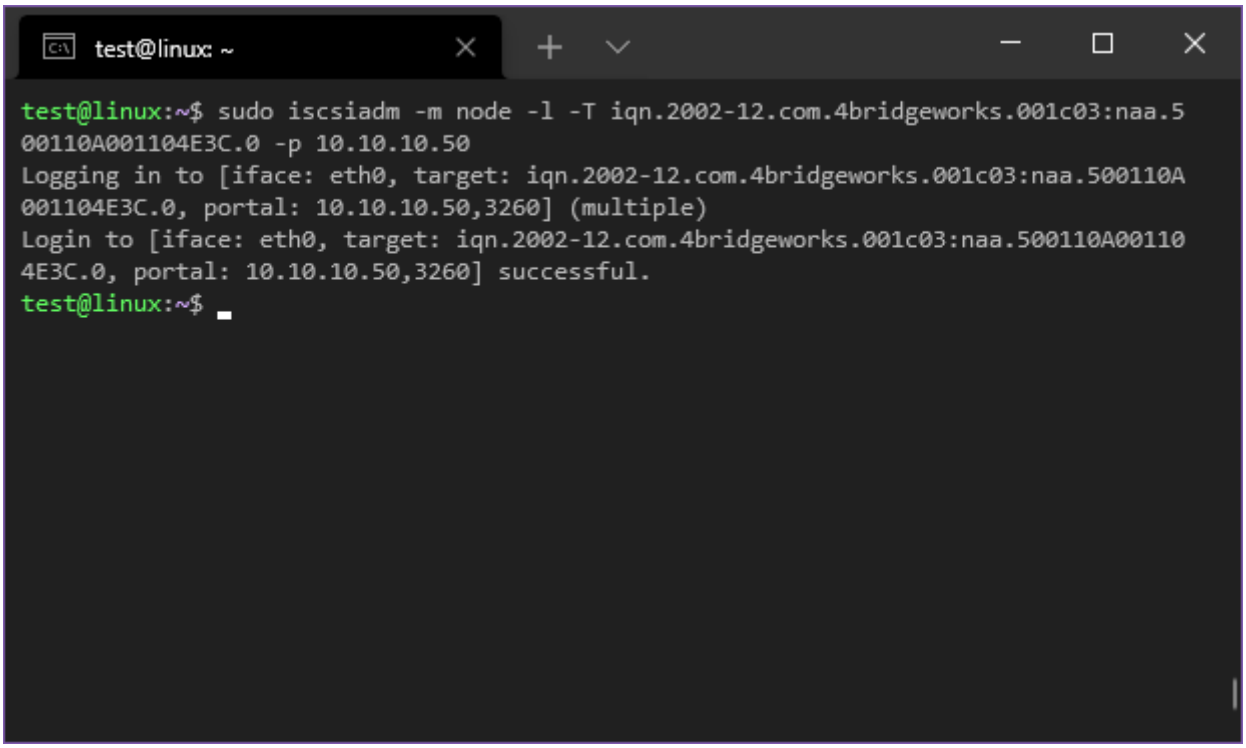
Once you have discovered the available targets, you can then login to the target. The following command will allow you to login to an individual target:

```
iscsiadm -m node -l -T <Complete Target Name> -p <Target IP Address>:<Port Number>
```

The example below shows logging into the discovered target `iqn.2002-12.com.4bridgeworks.001c03:naa.500110A001104E3C.0`:



When you have successfully logged in to the target device, the screen should update as shown below:



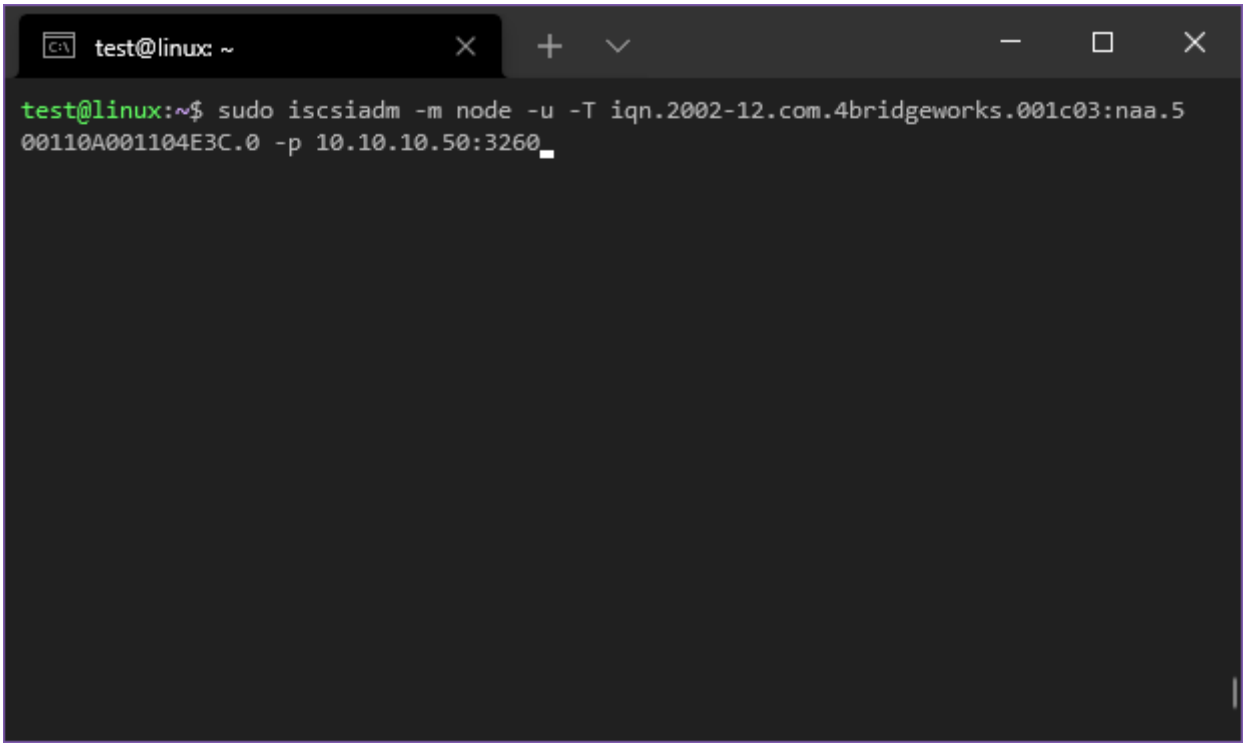
To login to all targets found, the following command can be used:

```
iscsiadm -m node -l
```

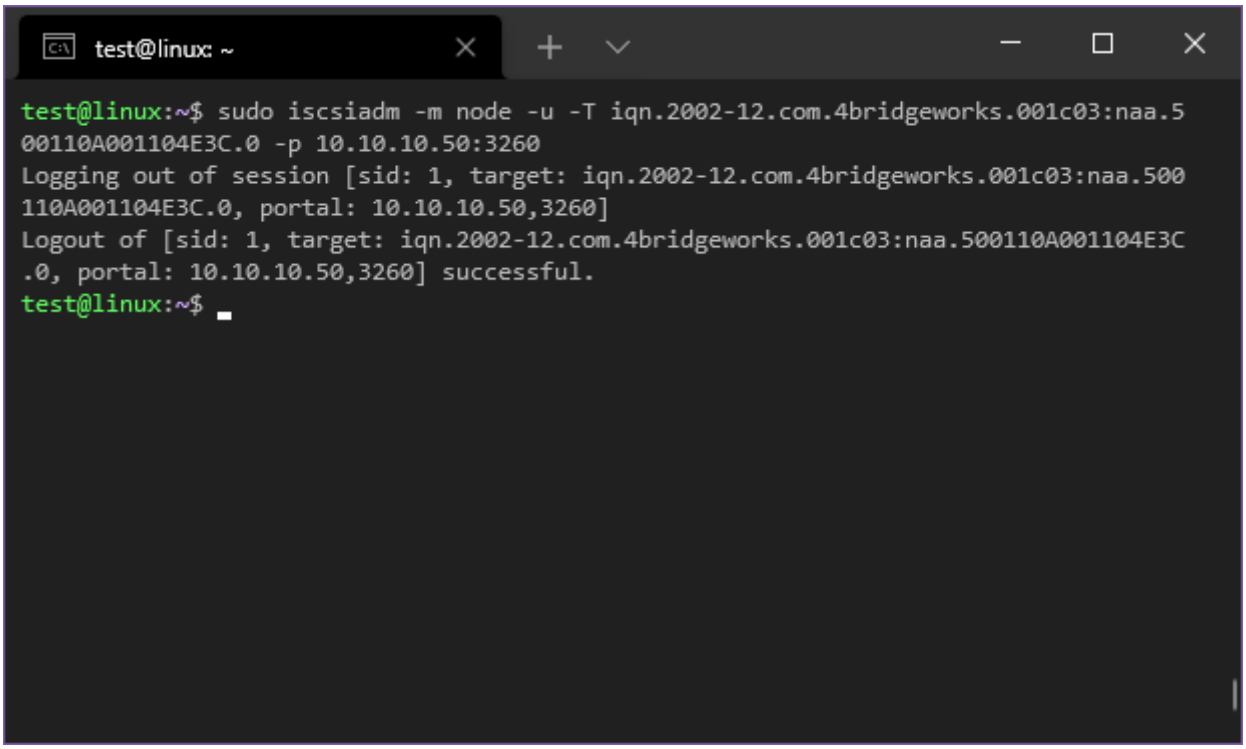
D.3 Logging out of a target

To log out of an individual target enter the following command at the prompt:

```
iscsiadm -m node -u -T <Complete Target Name> -p <Target IP Address>:<Port Number>
```



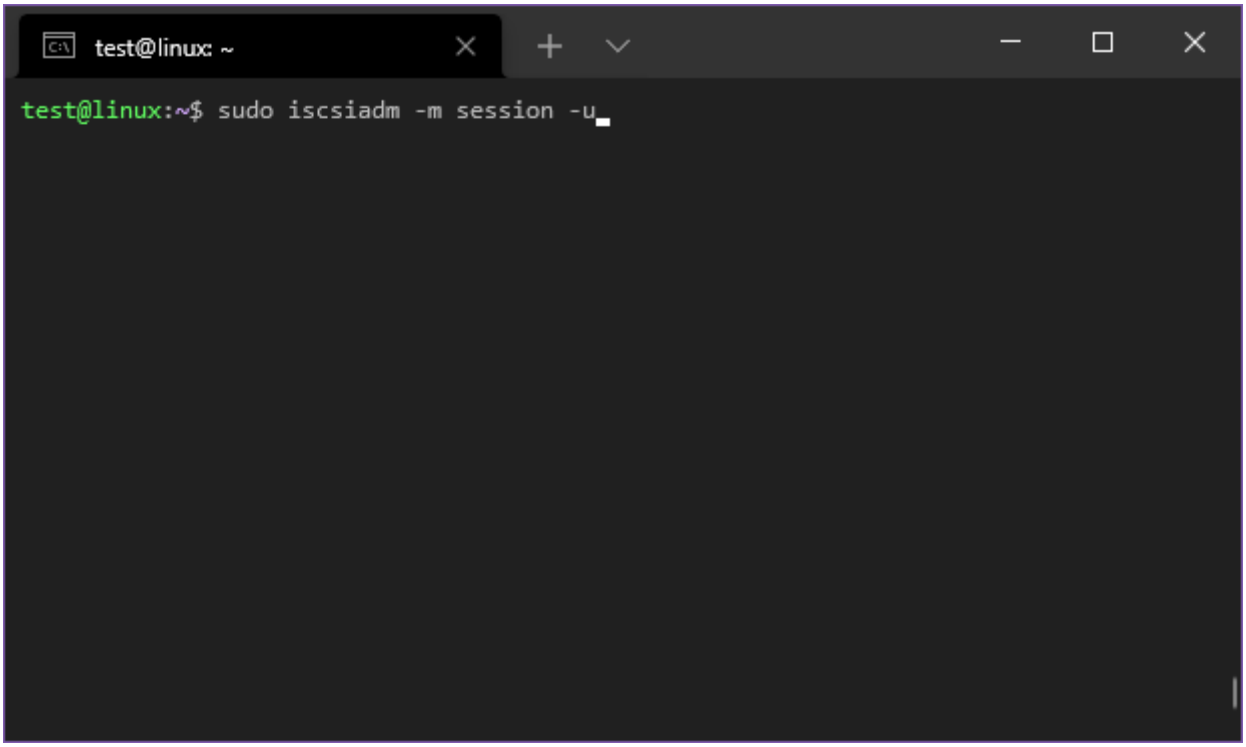
When you have successfully logged out of the target device, the screen should update as shown below:



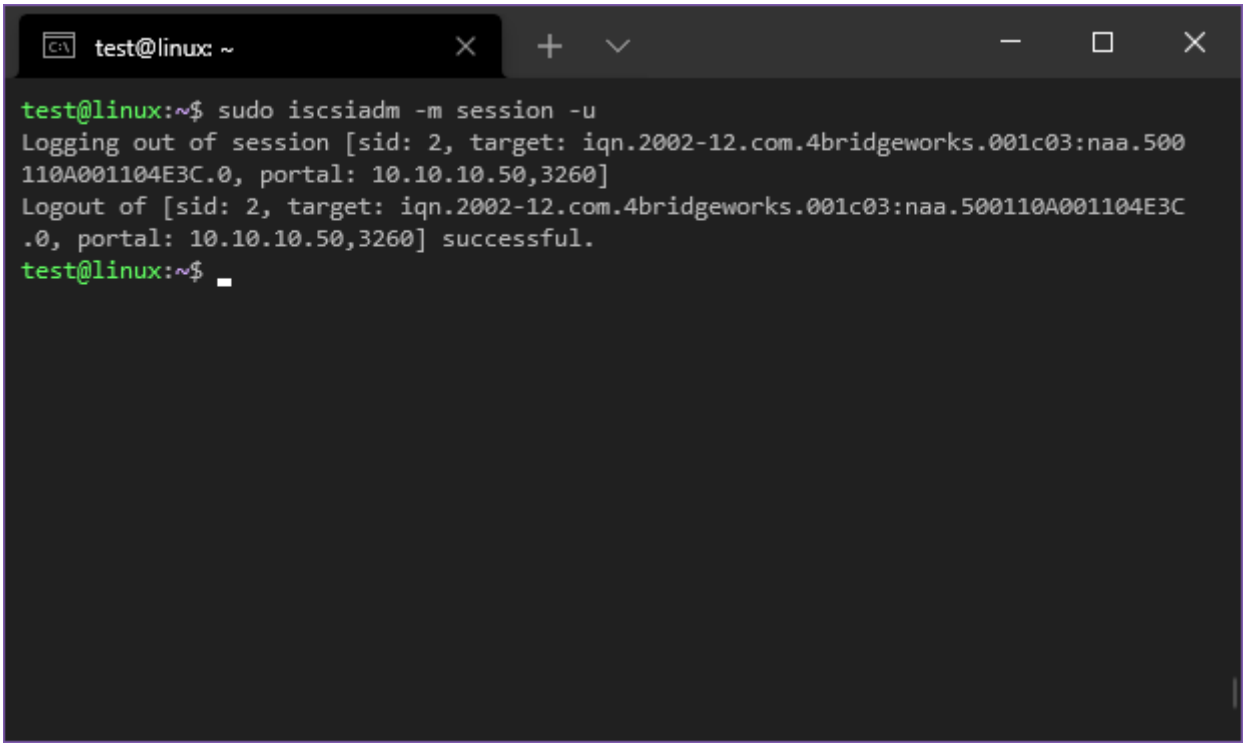
D.4 Logging out of all targets

To log out of all targets enter the following command at the prompt:

```
iscsiadm -m session -u
```



When you have successfully logged out of the targets, the screen should update as shown below:



E WANrockIT Series Comparisons

E.1 Node Limits

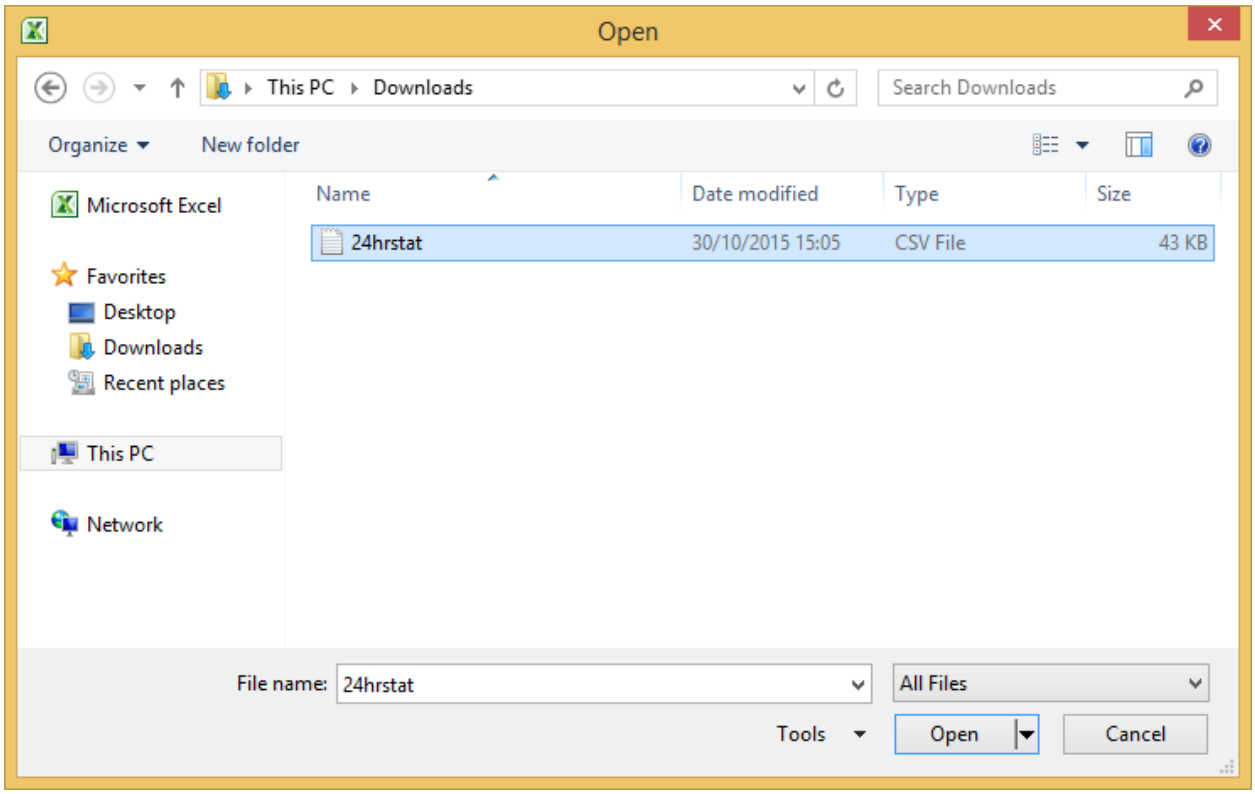
Series	Bandwidth	Maximum Connected Nodes
100	1 Gb/s	1
200	2 Gb/s	4
400	10 Gb/s	10
600	20 Gb/s	20

Bandwidth The bandwidth limit applied to accelerated transfers.

Maximum Connected Nodes The maximum number of Nodes that a Node may connect to.

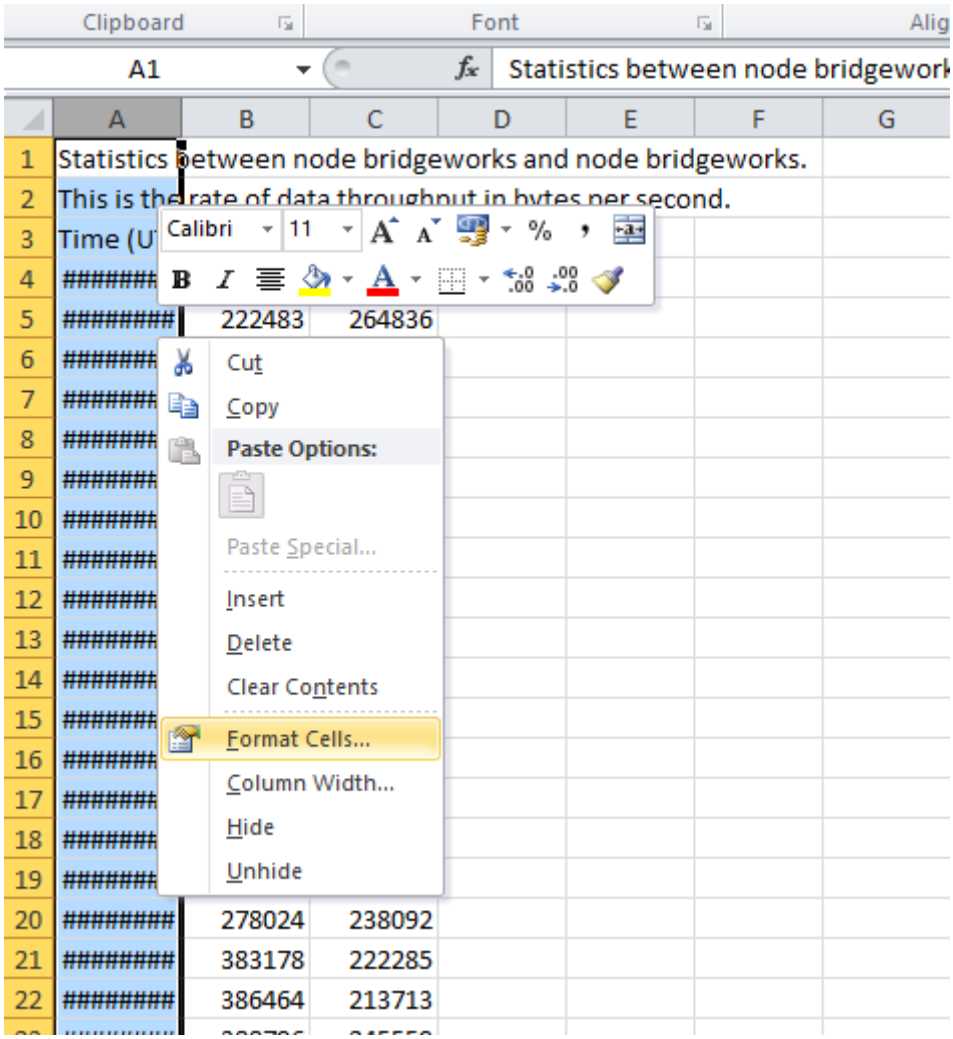
F Transfer Statistics Graphing Instructions for Excel 2010

Open Microsoft Excel 2010. From the *Open* dialog box, navigate to the download location for the transfer statistics. Open the file type drop down box and select the transfer statistics .csv file as shown:

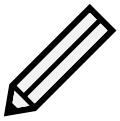


Note: For information on obtaining transfer statistics from your WANrockIT Node, see Section 4.1.3.2: Download 24 Hour Transfer History.

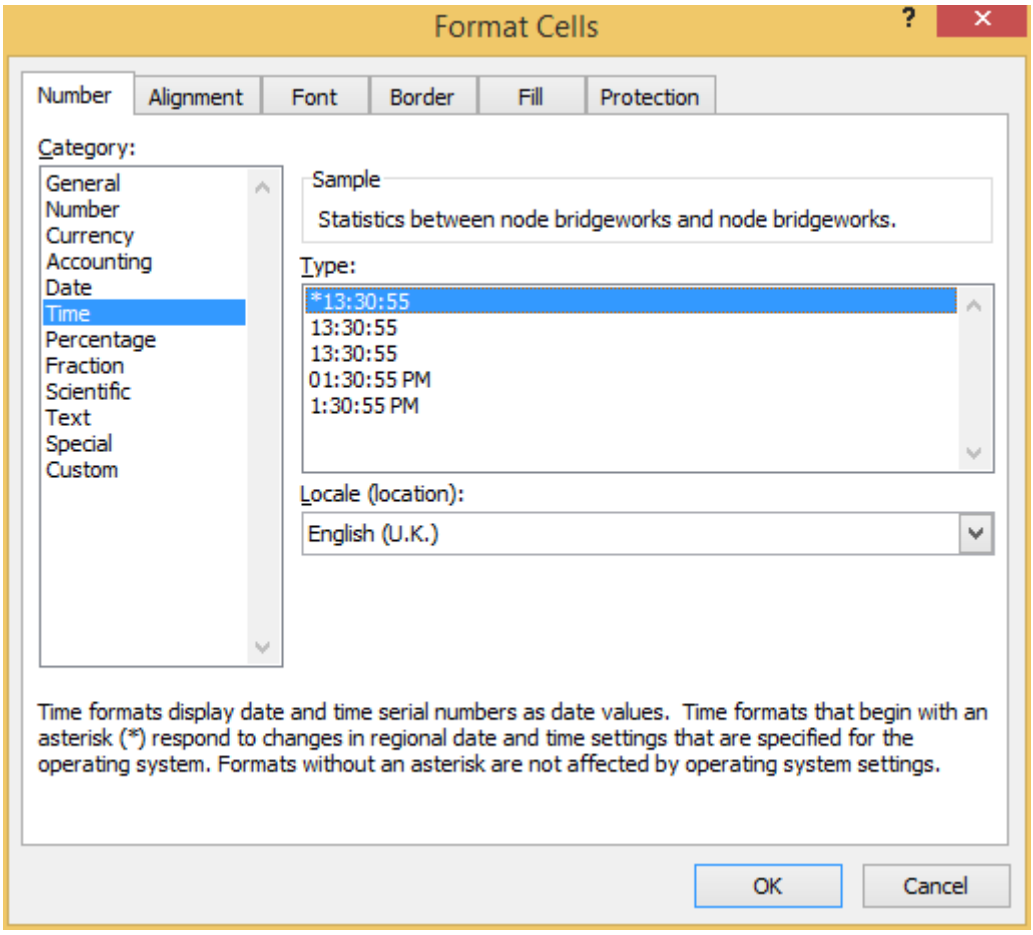
Select the *A* column of the newly generated worksheet, right-click, and select *Format Cells*.



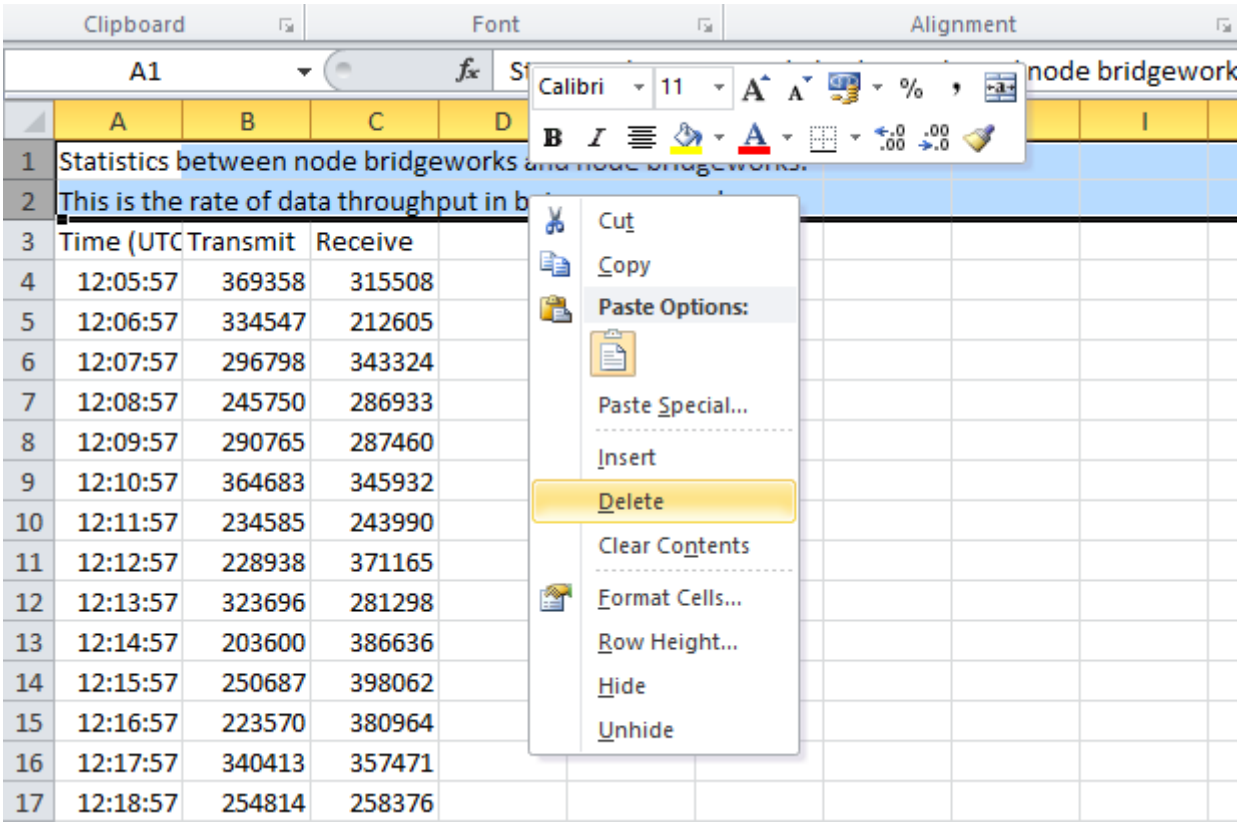
From the *Number* tab, select the *Time* category, and select the option `*13:30:55` as shown below then click *OK*.



Note: The time format chosen here is not the format in which the time will be displayed in the final graph.



Select the first two rows (row 1 and row 2) then right-click and select *Delete*.

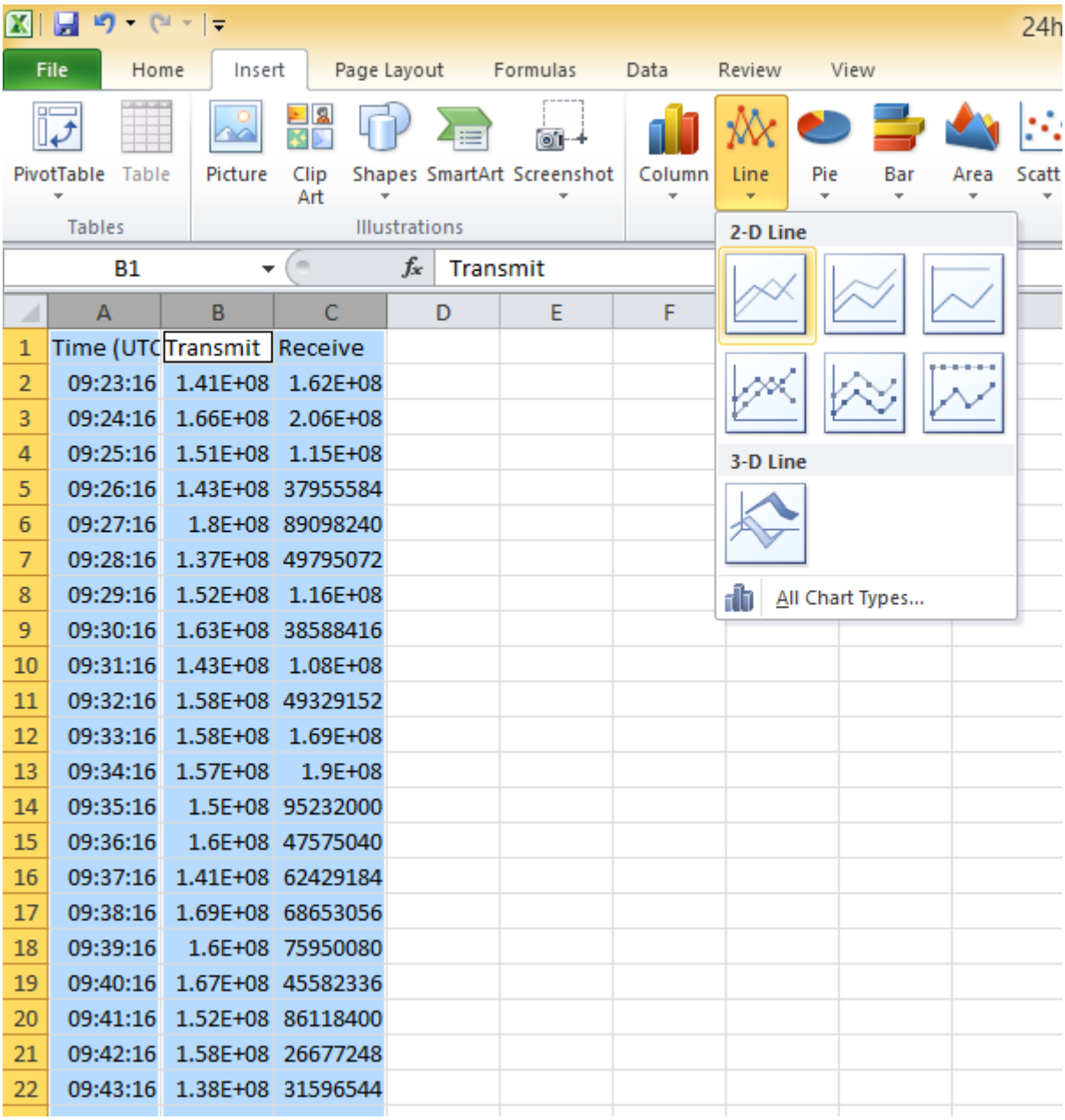


Select the first column by clicking on *A*. Then, hold down the `Ctrl` key on the keyboard and select the columns *B* and *C*. The three columns should now be selected as shown below:

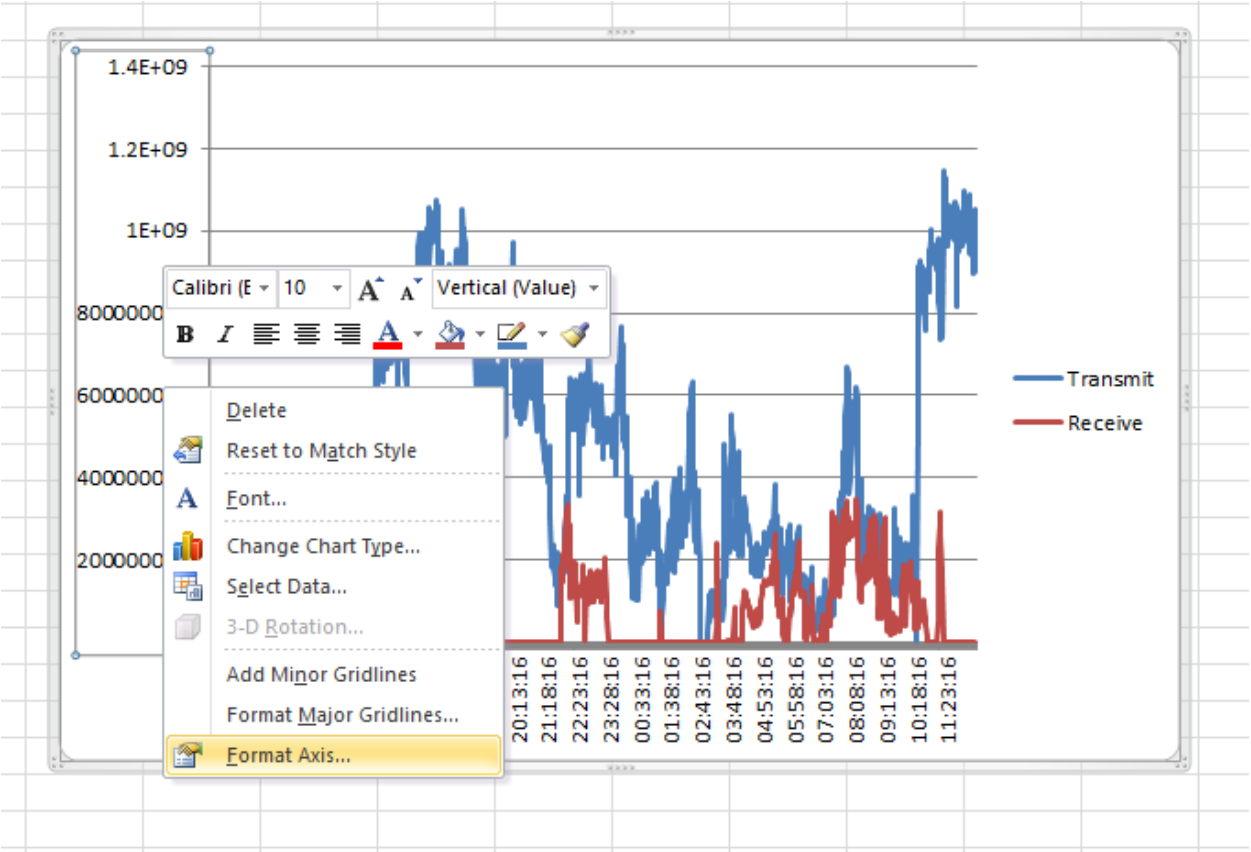
	A	B	C	D	E	F
1	Time (UTC	Transmit	Receive			
2	09:23:16	1.41E+08	1.62E+08			
3	09:24:16	1.66E+08	2.06E+08			
4	09:25:16	1.51E+08	1.15E+08			
5	09:26:16	1.43E+08	37955584			
6	09:27:16	1.8E+08	89098240			
7	09:28:16	1.37E+08	49795072			
8	09:29:16	1.52E+08	1.16E+08			
9	09:30:16	1.63E+08	38588416			
10	09:31:16	1.43E+08	1.08E+08			
11	09:32:16	1.58E+08	49329152			
12	09:33:16	1.58E+08	1.69E+08			
13	09:34:16	1.57E+08	1.9E+08			
14	09:35:16	1.5E+08	95232000			
15	09:36:16	1.6E+08	47575040			
16	09:37:16	1.41E+08	62429184			
17	09:38:16	1.69E+08	68653056			
18	09:39:16	1.6E+08	75950080			

Warning: Selecting all three columns at the same time may cause errors in generating the graph in the following steps. Remember to select column *A* first and then the other two columns with the `Ctrl` key held down.

On the *Insert* tab, in the *Charts* group, select the *Line* chart type and then the first icon shown.

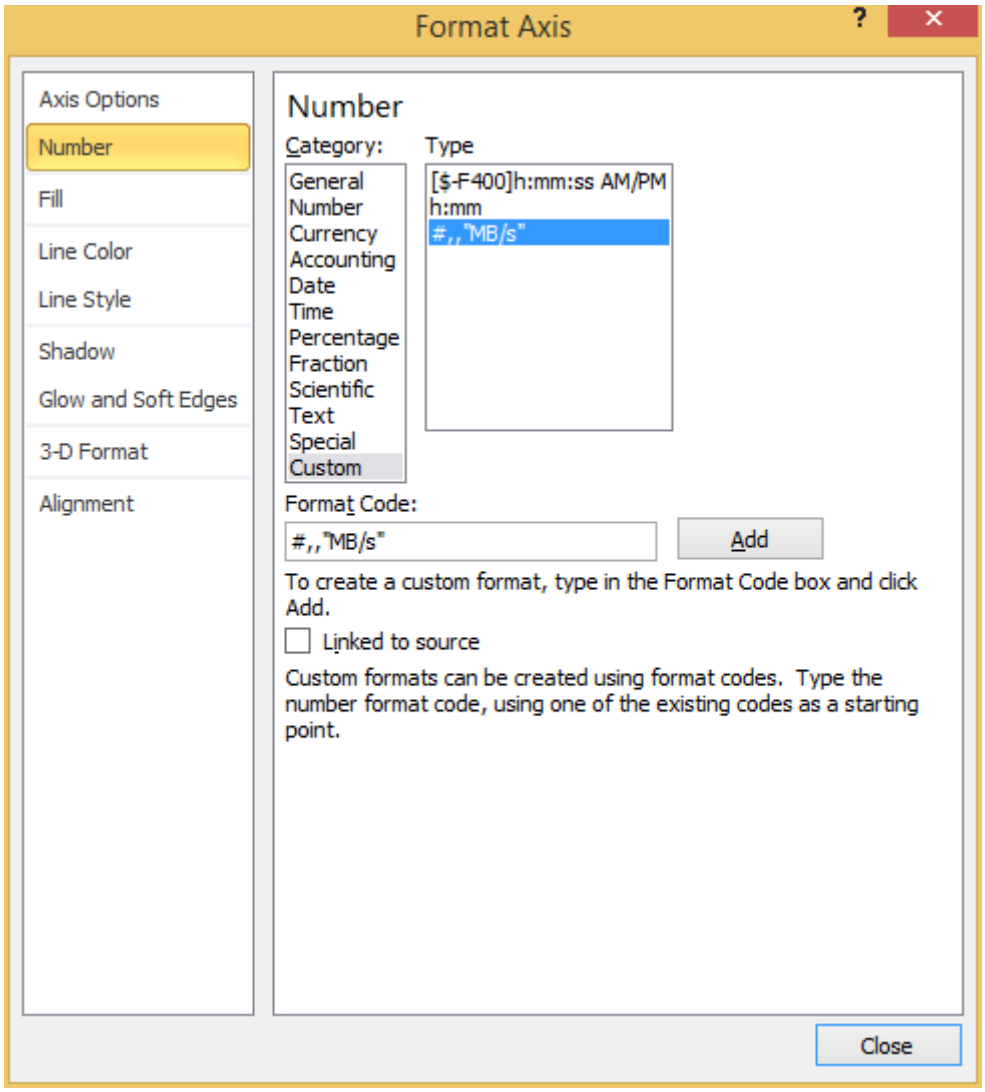


A new chart will be created. Right click the vertical axis on this chart and select *Format Axis*.



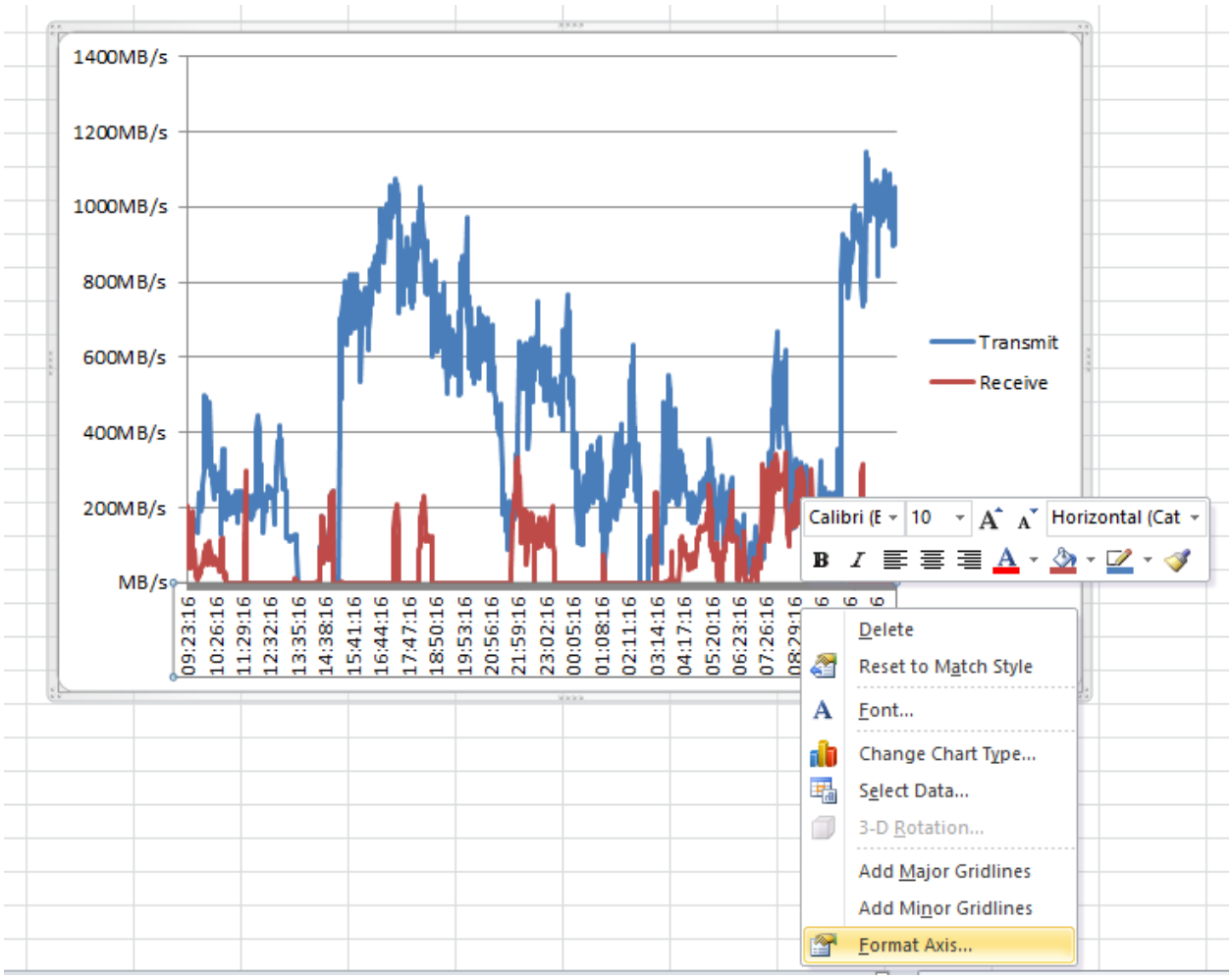
From the *Number* tab, select the *Custom* category. Enter the following in the *Format Code* field:

```
#,,"MB/s"
```

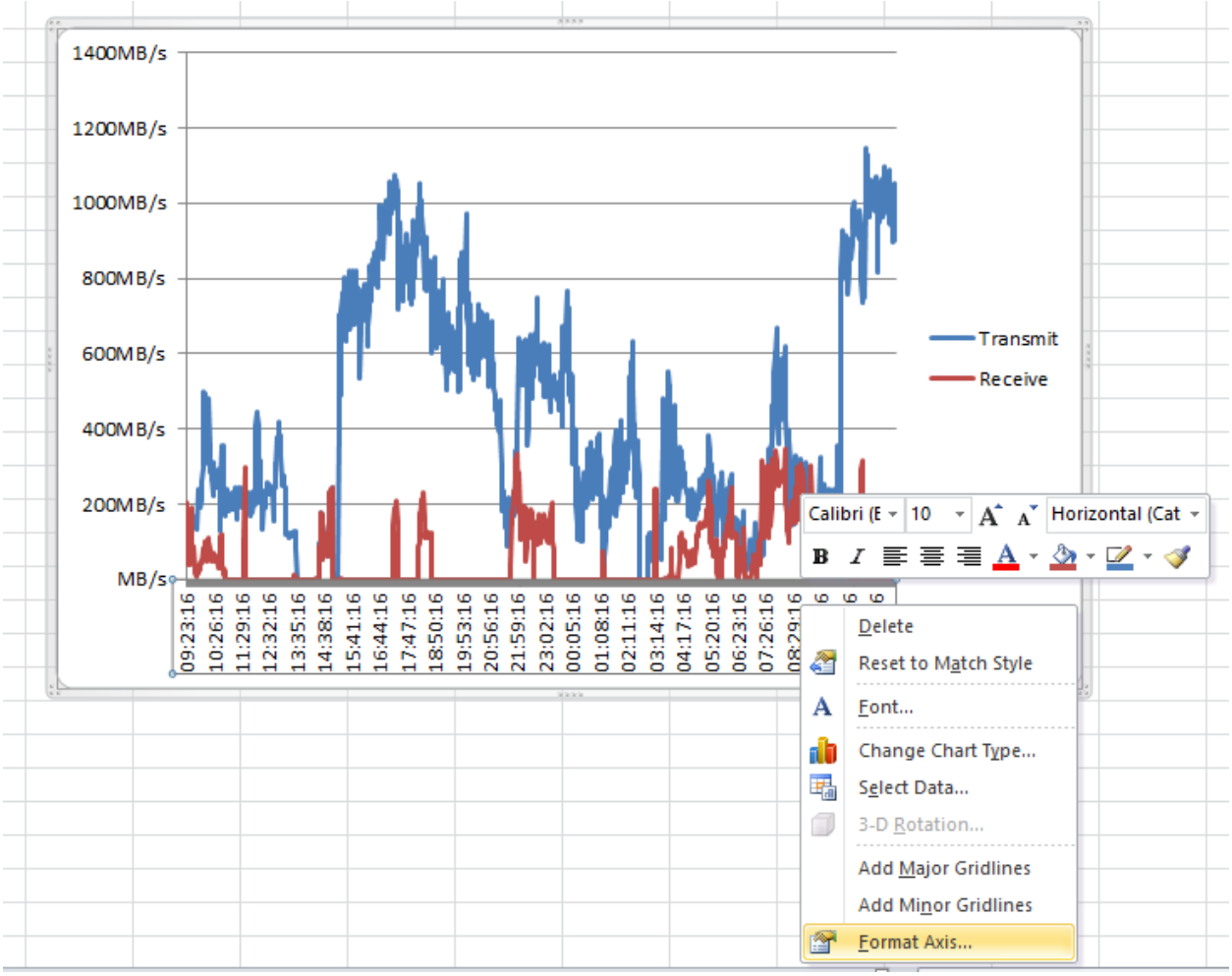


Click *Add*, then *Close*.

Now right click the horizontal axis and select *Format Axis*.

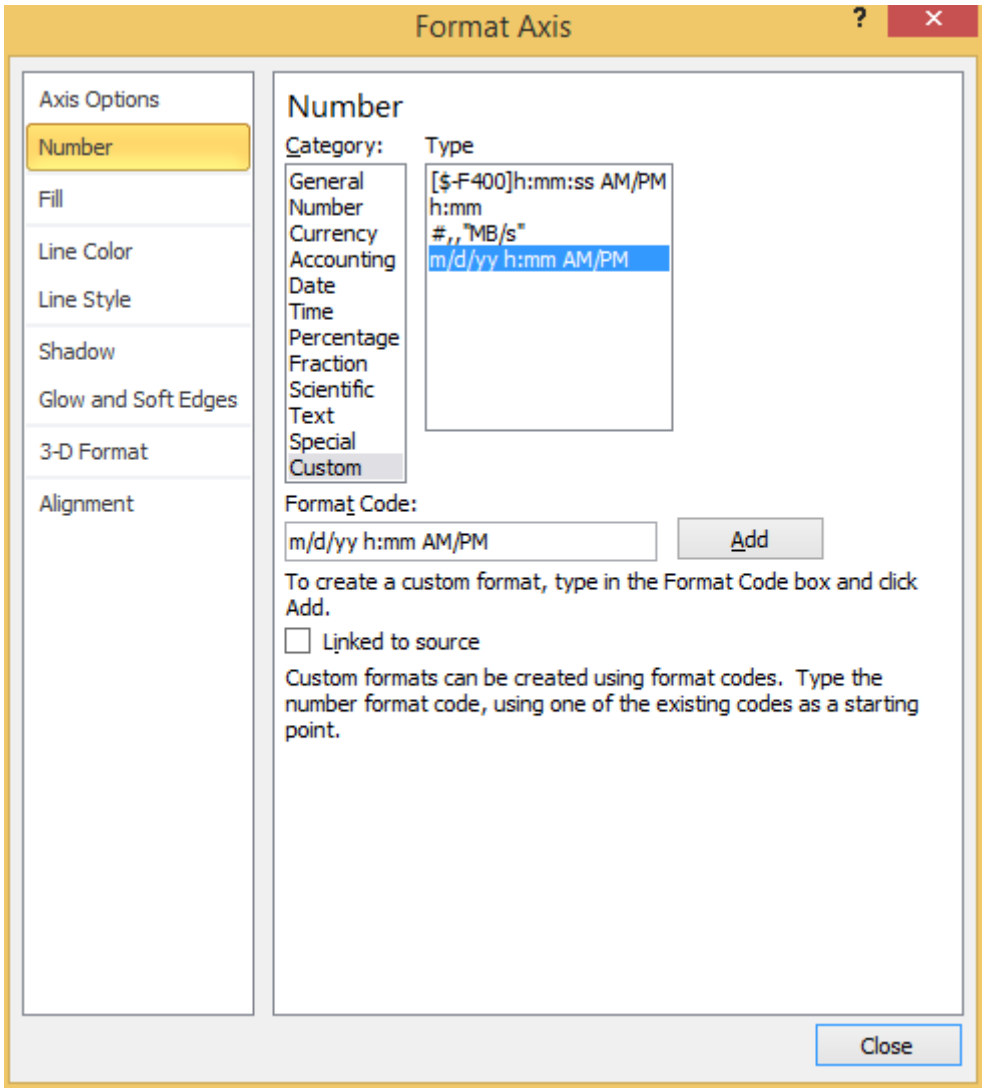


From the *Number* tab, select the *Time* category. Select the format you wish for the time to be displayed.

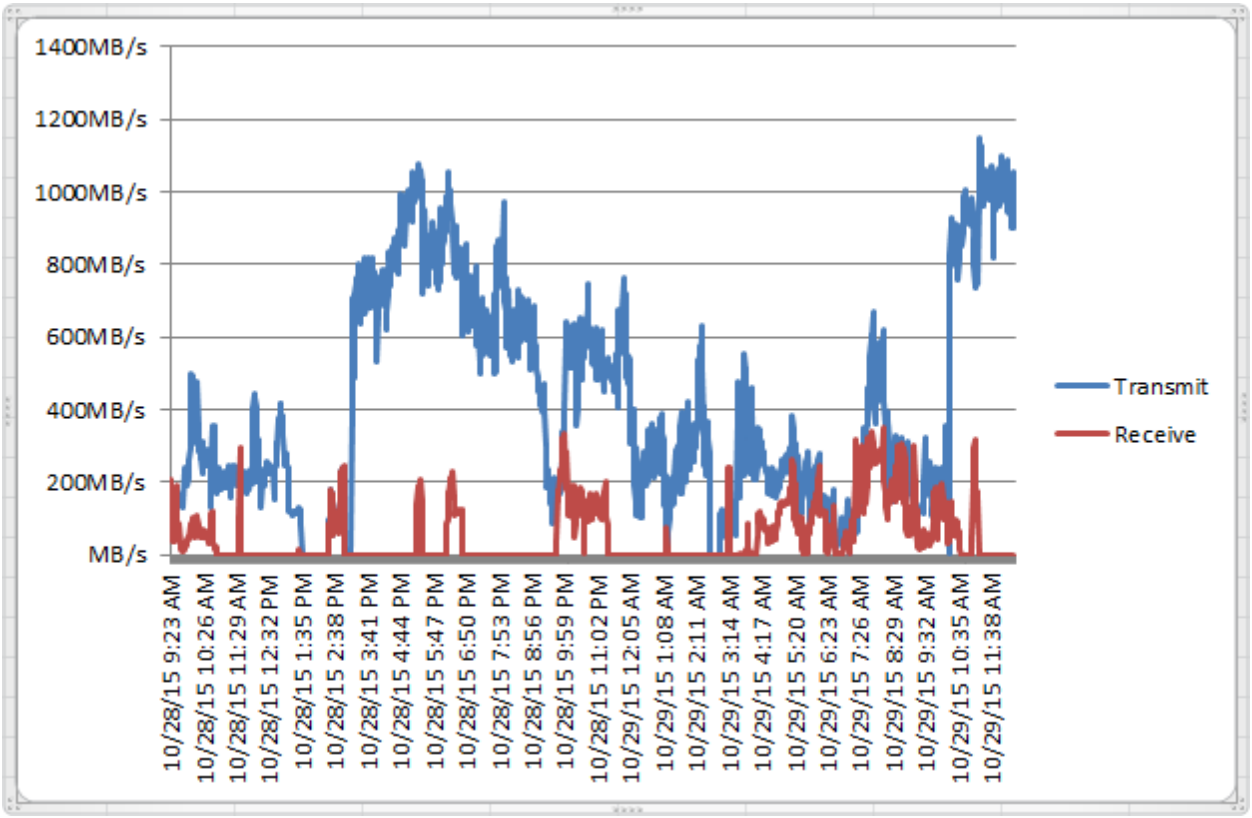


Alternatively, you can use a custom format for the date. In this case, select the *Custom* category, and enter your custom format in to the *Format Code* text field. The following is an example of a format code:

```
m/d/yy h:mm AM/PM
```



Click *Add* and then *Close*. Your chart should now look like the following:


1400MB/s
1200MB/s
1000MB/s
800MB/s
600MB/s
400MB/s
200MB/s
MB/s
10/28/15 9:23 AM
10/28/15 10:26 AM
10/28/15 11:29 AM
10/28/15 12:32 PM
10/28/15 1:35 PM
10/28/15 2:38 PM
10/28/15 3:41 PM
10/28/15 4:44 PM
10/28/15 5:47 PM
10/28/15 6:50 PM
10/28/15 7:53 PM
10/28/15 8:56 PM
10/28/15 9:59 PM
10/28/15 11:02 PM
10/29/15 12:05 AM
10/29/15 1:08 AM
10/29/15 2:11 AM
10/29/15 3:14 AM
10/29/15 4:17 AM
10/29/15 5:20 AM
10/29/15 6:23 AM
10/29/15 7:26 AM
10/29/15 8:29 AM
10/29/15 9:32 AM
10/29/15 10:35 AM
10/29/15 11:38 AM
Transmit
Receive

G Useful Links

Frequently Asked Questions If you experience problems with the WANrockIT Node, the frequently asked questions page may be able to help: https://support.4bridgeworks.com/documents/faqs/

Bridgeworks Support If you continue to experience problems with the WANrockIT Node, please contact support at https://support.4bridgeworks.com/contact/.

Bridgeworks Support Videos These videos will guide you through some of the instructions found in this manual. https://www.youtube.com/user/SANSlide/.

Product Manuals The latest product manuals can be found at https://support.4bridgeworks.com/documents/manuals/.