PORTrockIT
Software Manual
Eli-v5.03.148

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 **8**

1.1 Overview . . . 8

1.2 Manual Layout . . . 9

1.3 Definitions . . . 9

1.3.1 Node . . . 9

1.3.2 Endpoint . . . 9

2 Using the Web Interface **10**

2.1 Browsers . . . 10

2.2 Connecting to the Web Interface . . . 10

2.3 Quick Start Configuration . . . 12

2.4 Management Console (Home screen) . . . 14

3 Node Configuration **16**

3.1 Network Connections . . . 16

3.1.1 Network Interfaces . . . 17

3.1.2 Add Bond . . . 17

3.1.3 General Settings . . . 17

3.1.3.1 Hostname . . . 18

3.1.3.2 DNS Servers . . . 18

3.1.3.3 Default Route . . . 18

3.1.3.4 Dead Gateway Detection . . . 18

3.1.3.5 Enable VLANs . . . 20

3.1.4 Interface Statistics . . . 20

3.1.4.1 Data Transmission Rate . . . 21

3.1.4.2 Data Reception Rate . . . 21

3.1.4.3 Legend . . . 21

3.1.5 Network Routing . . . 22

3.1.5.1 Add Static Route . . . 22
3.1.6 Network Tools . . . 23
3.1.6.1 Ping . . . 24
3.1.6.2 Traceroute . . . 25
3.1.7 Port Settings . . . 26
3.1.7.1 Linked Interfaces . . . 27
3.1.7.2 Enable Port . . . 28
3.1.7.3 Setting the MTU . . . 28
3.1.7.4 Enable Routing . . . 28
3.1.7.5 Enabling Pass-Through or Bridged In-Path Mode . . . 28
3.1.7.6 Setting the IP Address . . . 29
3.1.7.7 Bypass Configuration . . . 30
3.1.7.8 Bonding Options . . . 30
3.1.7.9 Adding VLANs . . . 32
3.1.7.10 Committing the Changes . . . 33
3.2 Passwords & Security . . . 33
3.2.1 System Password . . . 34
3.2.2 Password Reset Options . . . 34
3.2.2.1 Password Reset via Email . . . 34
3.2.2.1.1 Setup . . . 34
3.2.2.1.2 Using Password Reset via Email . . . 35
3.2.2.2 Password Reset via Local Console or SSH . . . 37
3.2.2.2.1 Setup . . . 37
3.2.2.2.2 Using Password Reset via Local Console or SSH . . . 38
3.2.3 Secure Connection . . . 39
3.2.4 Secure Shell (SSH) . . . 40
3.2.4.1 Managing Public Keys . . . 40
3.2.4.2 Using SSH . . . 41
3.3 Service Control . . . 41
3.3.1 Simple Network Time Protocol . . . 42

3.3.2 SNMP Agent . . . 43
3.3.3 MIBs and OIDs . . . 43
3.3.4 Event Notification Email . . . 43
3.3.5 Simple Mail Transfer Protocol (SMTP) . . . 44
3.3.6 LAN Scan . . . 44

4 PORTrockIT Configuration 45

4.1 Service List . . . 45
4.1.1 Service Table . . . 45
4.1.2 Remove Service . . . 46
4.1.3 Add Service . . . 46
4.1.3.1 Name . . . 48
4.1.3.2 Address . . . 48
4.1.3.3 Public IP - Only available if NAT has been enabled . . . 48
4.1.3.4 Private IP - Only available if NAT has been enabled . . . 48
4.1.3.5 Protocol . . . 48
4.1.3.6 Outgoing Interface . . . 48
4.1.3.7 Topology . . . 48
4.1.3.8 Cancel . . . 49
4.1.3.9 Add Service . . . 49
4.1.4 Disabled Services . . . 49
4.2 Incoming Relationships . . . 49
4.2.0.1 Active Incoming Relationships . . . 50
4.2.1 Incoming Relationship . . . 51
4.2.1.1 Nodes . . . 51
4.2.1.2 Connections . . . 51
4.3 Client NAT Preservation . . . 51
4.3.1 Client NAT IP Addresses Table . . . 53
4.4 Node Management . . . 53
4.4.1 Remote Nodes . . . 54

4.4.1.1 Configured Nodes . . . 56
4.4.1.2 Non-Configured Nodes . . . 56
4.4.1.3 Orphaned Nodes . . . 56
4.4.2 Add Remote Node . . . 57
4.4.3 Transfer Statistics . . . 58
4.4.3.1 Data Transfer Rate . . . 60
4.4.3.2 Download 24 Hour Transfer History . . . 60
4.4.4 Access Control . . . 60
4.4.4.1 Remote Administration . . . 61
4.4.4.2 Whitelist . . . 61
4.4.5 IPsec . . . 62
4.4.5.1 Enabling IPsec service . . . 62
4.4.5.2 Adding a PSK (Pre-Shared Key) . . . 63
4.4.5.3 Encrypting Accelerated Traffic . . . 63
4.5 PORTrockIT Node Page . . . 64
4.5.1 Node Status . . . 65
4.5.2 Node Configuration . . . 66
4.5.3 Applications & Utilities . . . 66
4.5.4 Path Configuration . . . 66
4.5.4.1 Setting Primary and Failover Paths . . . 67
4.5.4.2 Filtering options . . . 68
4.5.4.3 Configuring a Node’s Bandwidth . . . 68
4.5.5 Node Specific Transfer Statistics . . . 69
4.5.5.1 Data Transfer Rate . . . 70
4.5.5.2 Download 24 Hour Transfer History . . . 70
4.5.6 Remove Node . . . 70
4.5.7 Relationships . . . 71
4.5.7.1 Prerequisites . . . 71
4.5.8 Services Table . . . 72
4.5.9 Toggling a Relationship . . . 73

4.5.10 Configure Services 74
4.5.11 Cancel 74
4.5.12 Save 74
4.5.13 Disabled Services 74
4.5.14 VPN Configuration 74
4.5.15 WCCPv2 76
4.5.15.1 Prerequisites 77
4.5.15.2 Configuring a Service Group 77
4.5.15.3 Monitoring a Service Group 78
4.5.15.4 WCCPv2 Service Group 78
4.5.16 Remote Control 80
4.5.17 Learn 81
4.5.17.1 Data Transfer Rate 83

5 Port Mappings **84**

5.1 Setting Port Mappings 85
5.2 Removing a Port Mapping 85
5.3 Saving Port Mappings 86
5.4 Available Port Mappings 86

6 Node Maintenance **88**

6.1 System Information 88
6.2 System Log 89
6.3 Load/Save Configuration 90
6.3.1 Loading a Saved Configuration 91
6.3.2 Saving the Configuration to Disk 91
6.3.3 Restoring to Factory Defaults 92
6.4 Firmware Updates 92
6.4.1 Automatic Firmware Update Checking 93
6.4.2 Updating Firmware Manually 94
6.5 Download CSP Image 95

6.6 Licence Key Management . . . 96
6.6.1 Uploading a Licence Key . . . 98
6.6.2 Removing a Licence Key . . . 98
6.6.3 Downloading a Licence Key . . . 98
6.7 Diagnostics . . . 99
6.8 Task Scheduler . . . 99
6.8.1 Adding Tasks . . . 100
6.8.2 Removing/Editing Tasks . . . 100
6.8.3 Task Wizard . . . 102
6.8.3.1 Action - Email Performance Statistics . . . 102
6.8.3.2 Action - PORTrockIT Bandwidth Limit . . . 103
6.8.3.3 Trigger . . . 104
6.8.3.4 Start Date . . . 105
6.8.3.5 End Date . . . 105
6.8.3.6 Summary . . . 106

7 Troubleshooting 107

7.1 Network Connectivity Problems . . . 107
7.2 Network Performance Problems . . . 107
7.3 Recovery Wizard . . . 108
7.3.1 Factory Restore . . . 109
7.3.2 Delete Configuration . . . 111

Appendix A IP Protocols and Port Numbers 114

A.1 Inbound LAN Protocols and Port Numbers . . . 114
A.2 Outbound LAN Protocols and Port Numbers . . . 114
A.3 WAN Protocols and Port Numbers . . . 115
A.4 PORTrockIT TCP Port Numbers . . . 115
A.4.1 Caringo Swarm Object Storage . . . 115
A.4.2 Commvault VM Backup and Recovery . . . 115
A.4.3 HTTP . . . 115

A.4.4 HTTPS 116
A.4.5 IBM Spectrum Protect 116
A.4.6 NetApp SnapMirror 116
A.4.7 NetApp StorageGRID 117
A.4.8 NFS 117
A.4.9 S3 117
A.4.10 SecuritEase 118
A.4.11 Veeam Backup & Replication 118
A.4.12 Veritas NetBackup 118
A.4.13 WANdisco Fusion 118
A.4.14 Web 119

Appendix B Accessing the Node from Windows using a static IP Address 120

Appendix C PORTrockIT Series Comparisons 124

C.1 Determining the Series Number 124
C.2 Number of Unique Protocols 124
C.3 Node Limits 124
C.3.1 Cloud Service Provider Nodes 124

Appendix D Transfer Statistics Graphing Instructions for Excel 2010 125

Appendix E Useful Links 132

Introduction

Thank you for purchasing the Bridgeworks PORTrockIT Node.

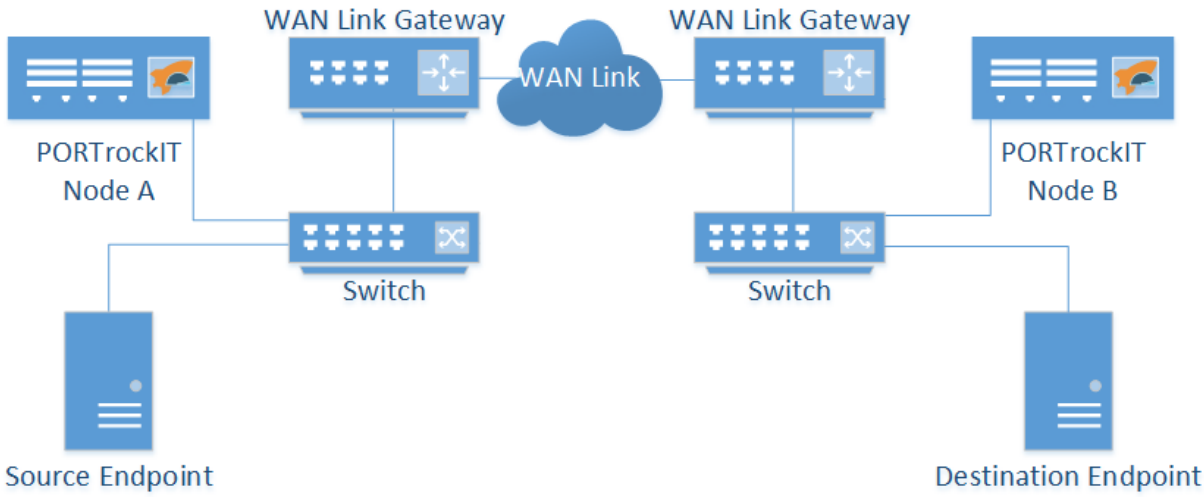
The PORTrockIT Node has been designed to ensure that in the majority of installations it will require minimal setup before use. However, we suggest you read the following section which will guide you through setting up your Node.

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

Overview

Bridgeworks latency mitigating technology allows you to accelerate your network traffic between two different sites. These sites may include data centres, your business centres and the Amazon Web Services (AWS) cloud. Each site will require either a PORTrockIT or WANrockIT Node to accelerate your desired traffic. These Nodes can be either physical hardware appliances, virtual machine images for popular platforms or Amazon Machine Images (AMIs).

The following diagram shows a basic example of how the PORTrockIT Nodes could be deployed.

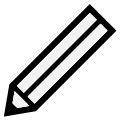


In this case data is accelerated from the *Source Endpoint* to the *Destination Endpoint*. *Node A* is set up to intercept traffic leaving the *Source Endpoint*, accelerating any data that matches the protocol across the *WAN Link* to the connected *Node B*. The traffic then continues on normally to its intended destination.

This basic setup can be extended to work in both directions allowing a bidirectional link between the two *Endpoints*. Depending on the specific protocol you wish to accelerate and your existing network setup, the exact topology you need will vary.

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.

Definitions

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

Node

A Node refers to a PORTrockIT unit

Endpoint

A host machine sending/receiving protocol data to be accelerated by PORTrockIT technology, as well as possibly other, non-accelerated data.

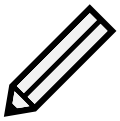
Using the Web Interface

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.

Browsers

This Node supports the following browsers:

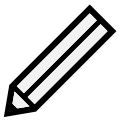
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Microsoft Edge[1]
- Mozilla Firefox 69.0.2 [1]
- Google Chrome 77 [1]



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.

Connecting to the Web Interface



Note:

- DHCP is enabled by default on the management interface.
- The default hostname is `bridgeworks`.
- The default fallback IP address of the management interfaces are:

  Management A/Port 1 `10.10.10.10`

  Management B `10.10.10.12`

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/`

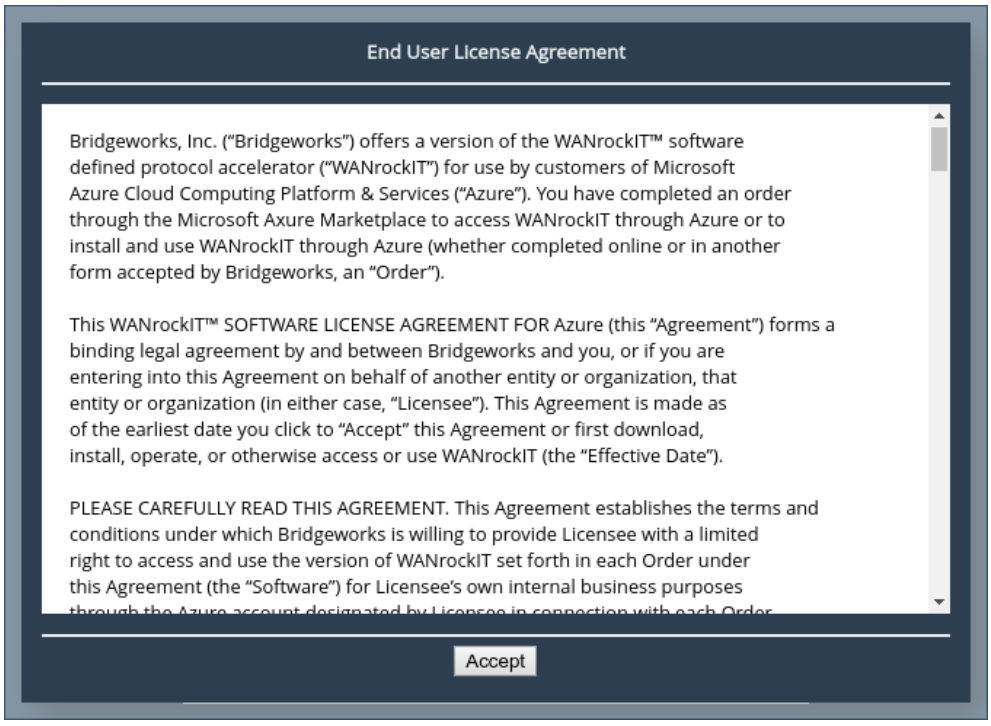
[1] Latest version as of release

If the Node fails to receive a DHCP address, the web interface can be accessed from the default static IP address by navigating to: `http://10.10.10.10/` or `http://10.10.10.12/`

	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.

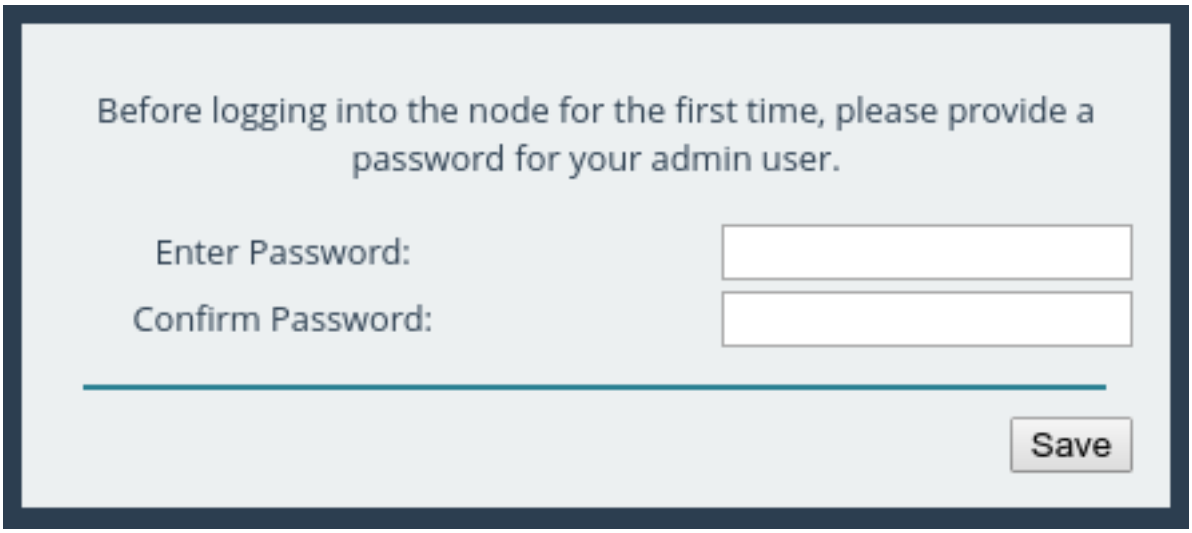
From within your web browser, connect to the Node's web interface using default hostname or IP address of a connected management interface.

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.

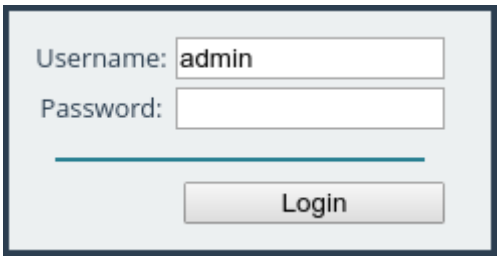
You will then see the entry page shown below:



	Important: AWS Nodes will require the instance ID and Azure Nodes will require the subscription ID to be able to set the initial password.

	Important: During deployment of Azure Nodes you are able to set the initial password if you choose to use password authentication. If you set up your password this way, you will be directed to the login screen.

Enter and confirm the new web interface password to be presented with the login screen. The password must be between 5 and 65 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*.

	Important: On Azure nodes, you will need to enter the username that you chose during deployment.

Quick Start Configuration

When you have logged in, the *Quick Configuration Guide* will be presented as shown below. This gives an overview of a typical set up, as well as key areas that will need to be configured to get the software operational. This page will continue to appear when you log in until *Port Mappings* have been configured.

Quick Configuration Guide

Welcome

Welcome to the Bridgeworks PORTrockIT series. In order to start using your product you will require another instance, one at each site between which you wish to accelerate traffic. An overview of the three main topologies are described in this guide, where traffic from an "Endpoint" on "Site A" is accelerated over a WAN link to an "Endpoint" on "Site B".

Bridged In-Path:

This topology requires two network ports to be configured as a network bridge. It is very important to ensure the port with WAN features ("Port 2" by default) and the port with LAN features (typically "Port 3") are on separate isolated networks. No additional network routing rules need to be implemented at either site.

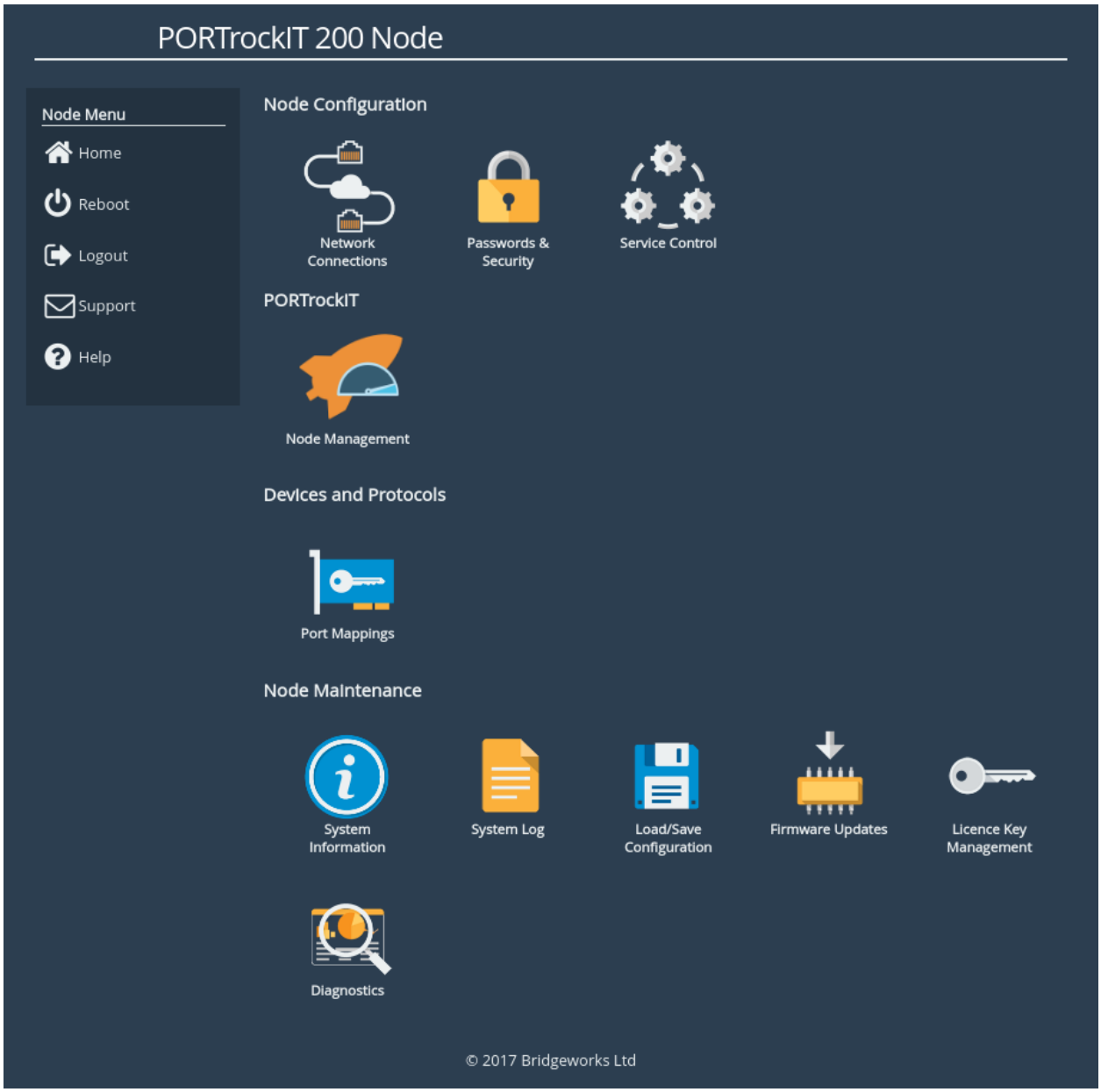
Policy Routed Logical-In-Path:

This topology requires that endpoints at "Site A" redirect traffic, destined for endpoints at "Site B", to the PORTrockIT unit at "Site A", and vice versa. This topology supports the use of a VPN connection, provided by the PORTrockIT units, to secure unaccelerated traffic between the sites.

Close | Pop out Page | Next

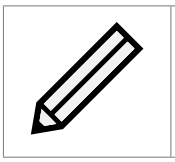
Management Console (Home screen)

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.

Node Configuration

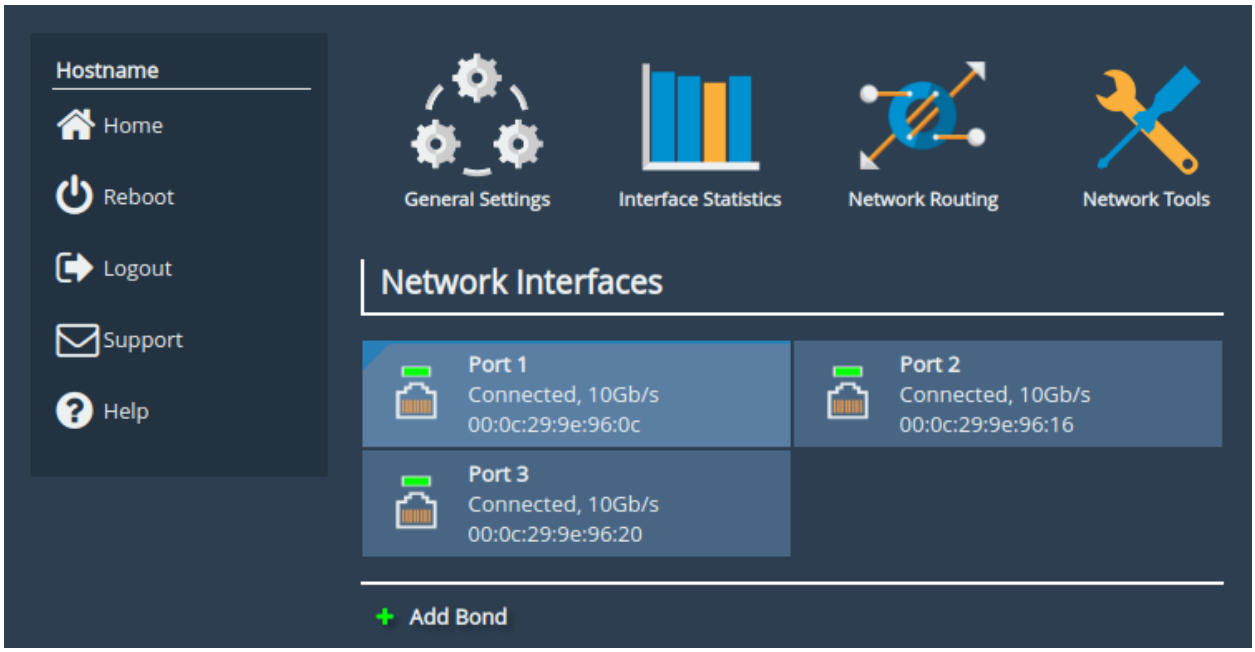
This section details the configuration of the Node's basic network and service settings.

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 3.1.3: General Settings
- Section 3.1.4: Interface Statistics
- Section 3.1.5: Network Routing
- Section 3.1.6: Network Tools

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 3.1.7: Port Settings.

Add Bond

This button will add a new network *Bond* to the system (also known as Link Aggregation/Bundling, Port Trunking, or NIC Teaming). This allows two or more *Network Interfaces* to be combined together, providing potential load balancing as well as greater levels of fault tolerance.

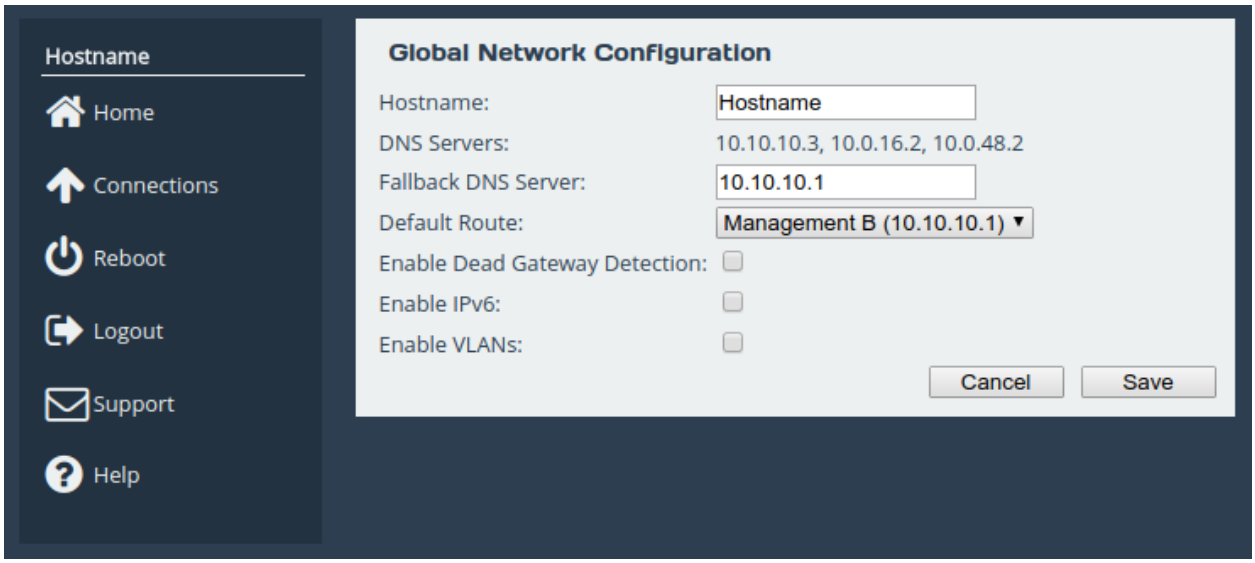
Once a new *Bond* has been created, click on it to access its settings and add the desired interfaces. More information on *Bond* settings is available in Section 3.1.7: Port Settings.

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.



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.

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.

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.

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.

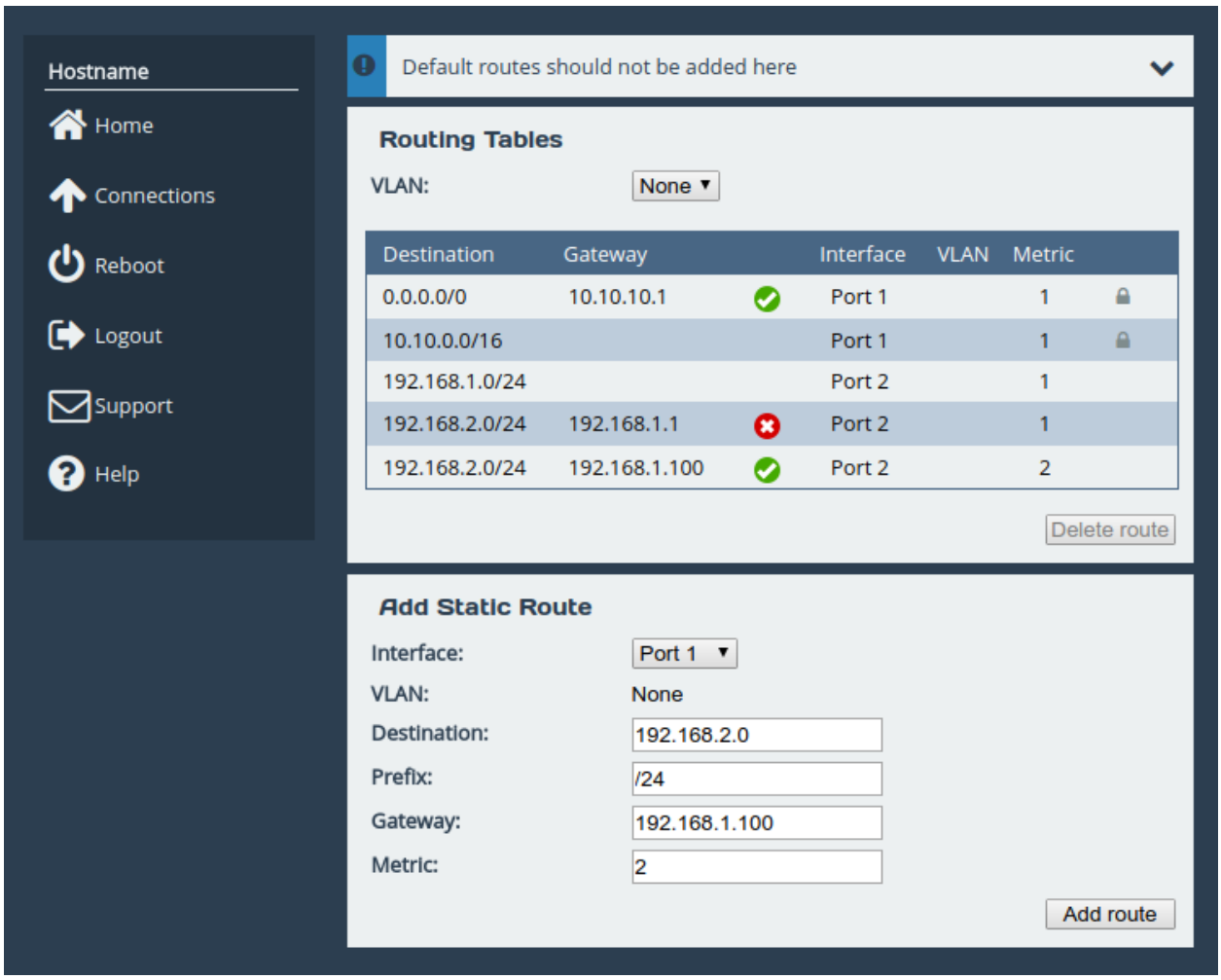
The status of each gateway is displayed on the *Routing* page. Refer to Section 3.1.5: Network Routing for information on viewing and modifying network routes. An icon next to each gateway

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.

Enable VLANs

When the *Enable VLANs* checkbox is selected, VLANs (IEEE 802.1Q) will be configurable for network interfaces on their respective port configuration page. Section 3.1.7: Port Settings

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.

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 horizonal line for each interface.

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 horizonal line for each interface.

Legend

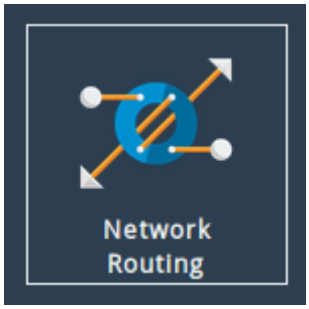
Each base network interface and each bond will be displayed using a unique colour for the data rate graphs. Each interfaces colour will be displayed alongside the ports name here.

Statistics for VLANs are included in the statistics for their parent interface.

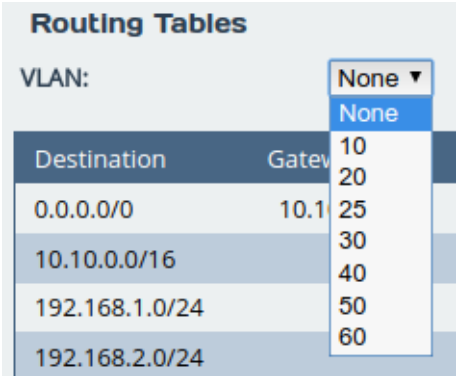
Network Routing

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.



Routes are only displayed for the selected VLAN. Using the *VLAN* dropdown at the top of the page will change which VLAN is selected. This also affects which VLAN a route is added to using the *Add Static Route* form. To view and add routes without a VLAN select *None*.



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.

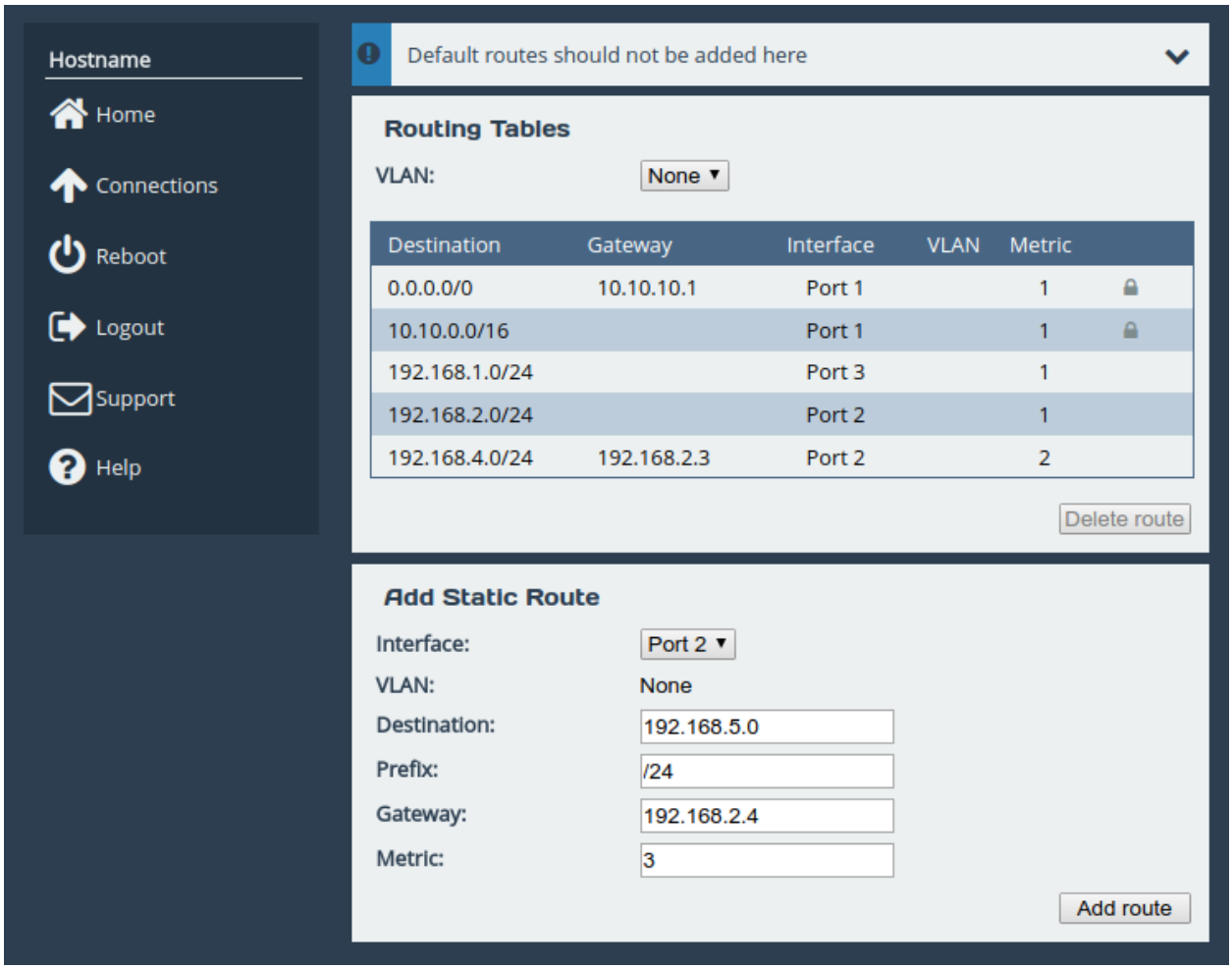
VLAN The VLAN on which the route applies. Selectable with the *VLAN* dropdown at the top of the page.

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.

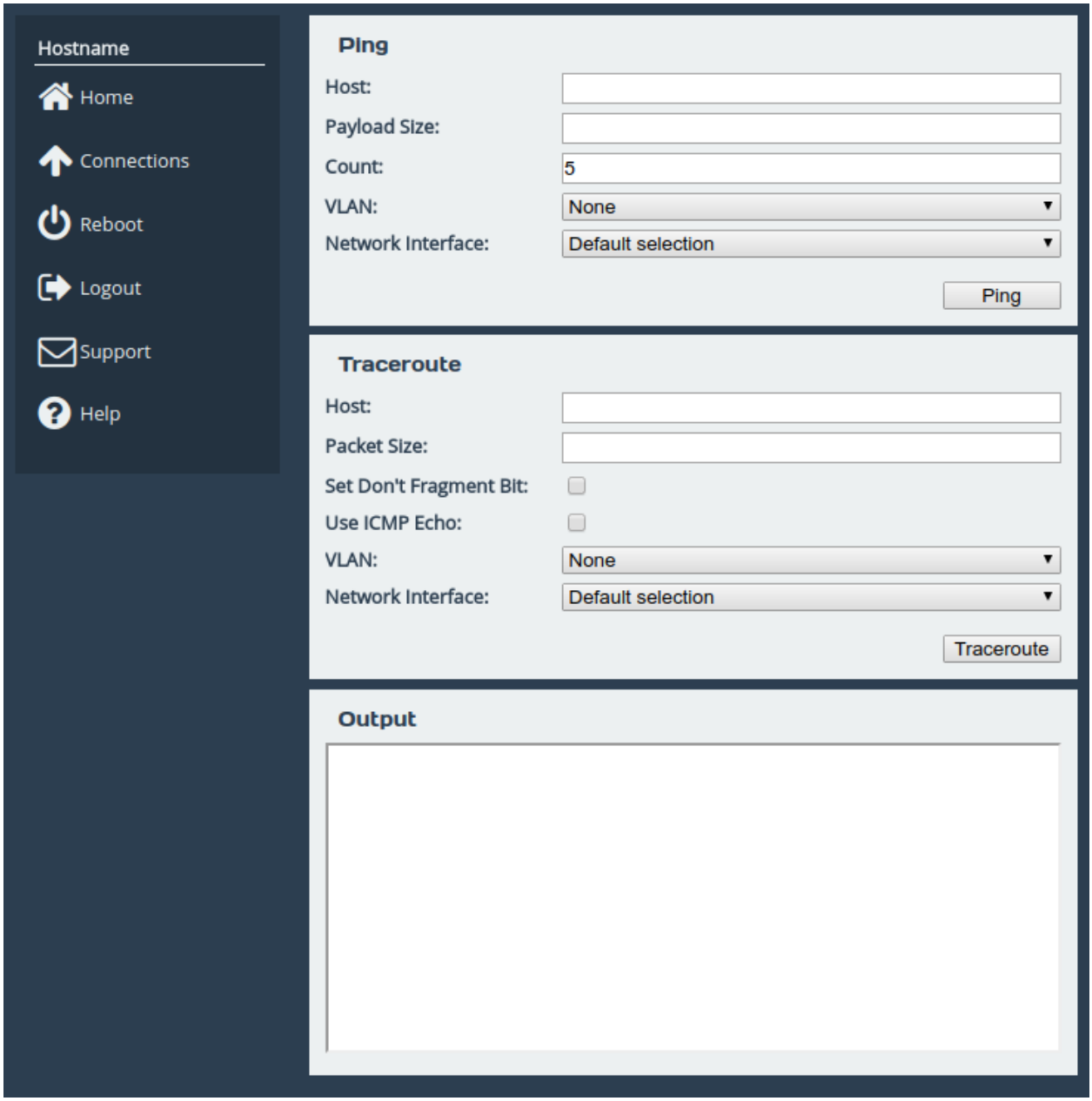
When dead gateway detection is enabled, each gateway in the table will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.3.4: Dead Gateway Detection for more information.

Network Tools

The PORTrockIT 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.



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.

VLAN The VLAN that the ping will be sent on. Changing this option will filter the interfaces in the *Network Interface* option.

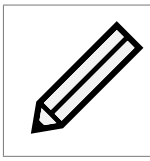
Network Interface The interface that you want to ping from. If you are checking the routing on the unit, leave this option set to

Default selection. Only interfaces with the selected VLAN will be displayed.

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
```



Note: *Address* is replaced with the IP address that you entered.

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:

Host The IP address of the network host.

Packet Size The traceroute payload size. Leave blank to default to 46 bytes.

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.

Use ICMP Echo Select to use ICMP echo requests instead of UDP datagrams. This can be useful when your firewall blocks UDP traffic.

VLAN The VLAN that the traceroute will be sent on. Changing this option will filter the interfaces in the *Network Interface* option.

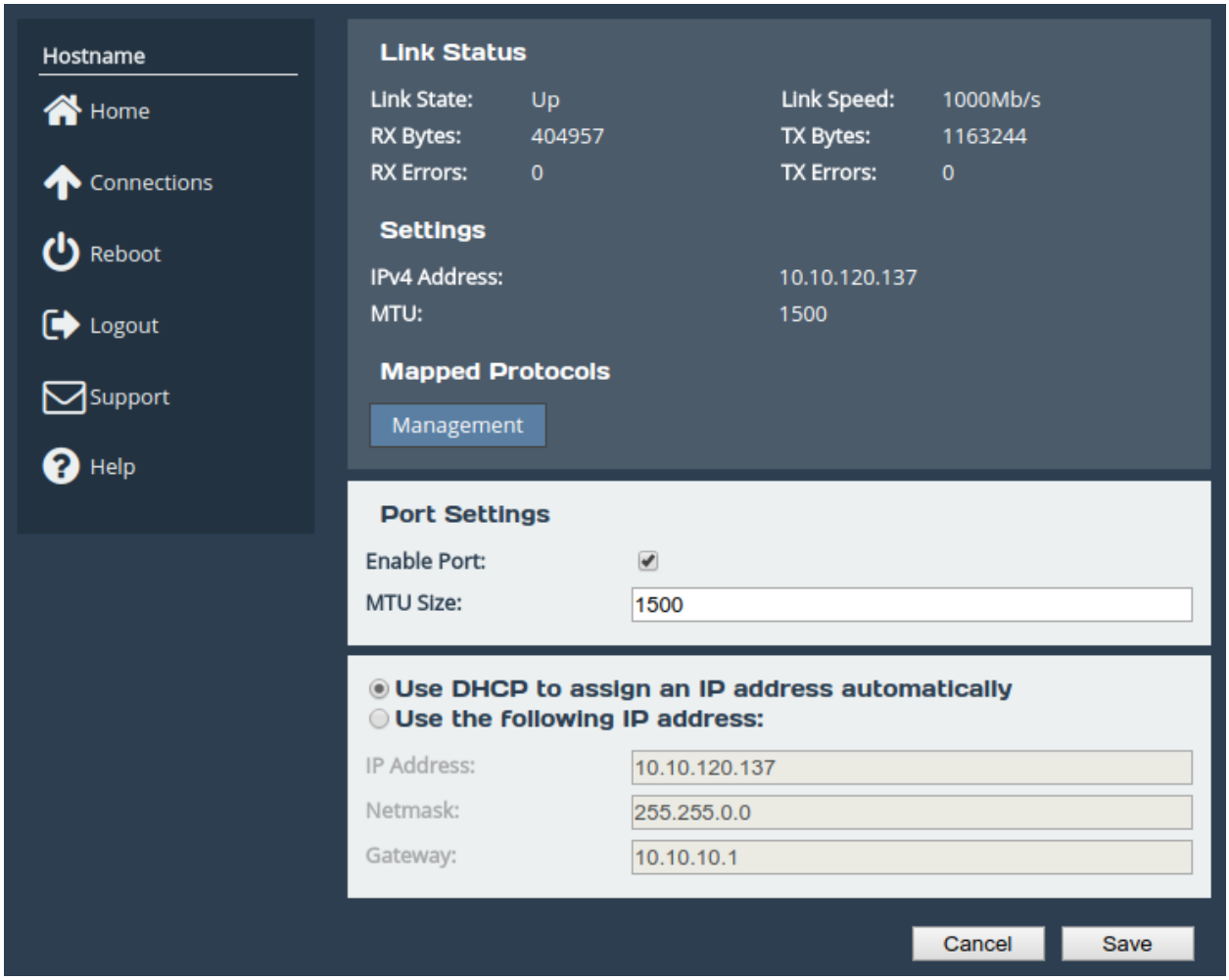
Network Interface The interface that traceroute packets will be sent from. Leave as *Default selection* for the interface to be selected according to the routing table.

Only interfaces with the selected VLAN will be displayed.

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

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.



The following is a list of all possible interface types, and the settings available for each.

	Linked Interfaces	Enable Port	MTU	Enable Routing	Pass-through Configuration*	IPv4	Bypass Configuration*	VLANs*	Bonding Options
Basic Interface		✔	✔	✔	✔	✔	✔	✔	
Bridged Interface (master)		✔	✔	✔	✔	✔	✔	✔	
Bridged Interface (slave)		✔			✔		✔		
Bond Interface (master)	✔		✔	✔	✔	✔	✔	✔	✔
Bonded Interface (slave)		✔							
VLAN Interface			✔	✔		✔			

Important: Pass-through Configuration will only be displayed if the interface is mapped with a PORTrockIT protocol.

Important: Bypass Configuration will only be displayed if the interface is part of a Hardware Bypass Card.

Important: VLANs will only be displayed if VLANs have been enabled (see Section 3.1.3: General Settings).

Linked Interfaces

Displays all Interfaces which are linked to make up a Bond. Additional interfaces can be added by clicking the *Add Interface* button, or deleted by clicking the *X* button on a particular interface and then clicking *Delete*.

Changes to the *Linked Interfaces* will be queued until the page is saved. This includes both adding and deleting of interfaces.

Important: Protocol mappings on a Bond are acquired by inheriting only the common mappings of the bonded interfaces.

Enable Port

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

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.

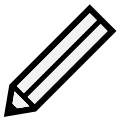
Important: Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches it might be required to add the necessary bytes needed for the frame header to the MTU size you specify in the Node's port configuration. 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.

Enable Routing

Firewall rules exist to block any traffic that is not destined for the PORTrockIT. Enabling this option will remove the firewall rules, allowing traffic to freely pass through the interface.

By default this option is enabled on LAN interfaces, but disabled on WAN interfaces. This will allow accelerated traffic through, but will block any unaccelerated traffic from leaving the Node. If required traffic is passing through the Node that is not being accelerated, this option should be enabled on all relevant interfaces.

Enabling Pass-Through or Bridged In-Path Mode



Note: You may skip reading this section if you wish to deploy your Node in the *Policy Routed Logical In-Path* or *Out-of-Path* topologies.

Important: Pass-through and subsequently Bridged In-Path Mode are unavailable on AWS, Azure and Hyper-V Nodes.

In order for the PORTrockIT acceleration to pass traffic through the network, the port that has a PORTrockIT protocol mapped to it (such as IBM Spectrum Protect or NetApp) must be configured

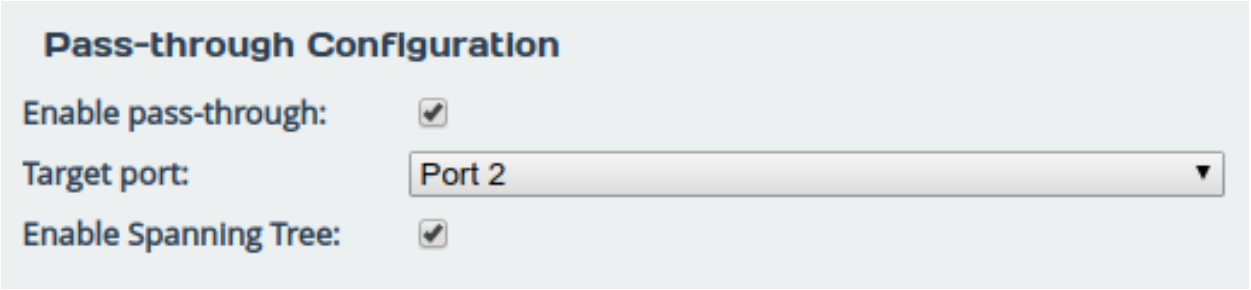
to enable “pass-through”, also called “bridged in-path mode”.

To enable pass-through, select the *Enable pass-through* checkbox, and select the *Target port* using the drop down list. This will be the WAN port used to establish the leading WAN link between the two units.

Please ensure these Nodes are not connected to the same Ethernet segment. To help protect against network issues, the PORTrockIT unit participates in STP (Spanning Tree Protocol) by default to ensure that network loops are not created. However this will prevent the PORTrockIT unit from operating as an acceleration device if it has to disable its bridging to protect the network.

In rare circumstances STP may need to be disabled. Clearing the *Enable Spanning Tree* checkbox will disable STP.

	Important: STP is disabled on Bypass cards and cannot be enabled.



Once the changes are complete click *Save*. A reboot of the PORTrockIT Node will be required for the change to become active. This should be completed on both PORTrockIT Nodes before continuing.

Setting the IP Address

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

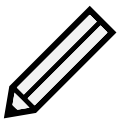
DHCP The Node will seek out your network’s DHCP server and obtain an IP address for this port each time it boots.

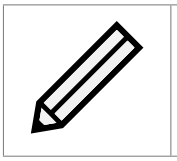
If the server is not found, this port will fall back to its saved static IP settings.

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`.

	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.

Bypass Configuration

Only available when a Bypass Card is installed in your system, this option will allow a user to configure the *Mode* of the card. Available modes include:

- *Auto* - Card will automatically switch to Bypass Mode if it detects that the PORTrockIT has powered off for any reason. This will allow traffic to continue flowing through the unit during a reboot or if the unit fails for any reason. When using this option the cards ports should be bridged together so that the network topology remains unchanged when Bypass Mode toggles on and off.
- *Force On* - Card will be forced into Bypass Mode causing all traffic to bridge between the card's ports without entering the PORTrockIT. No traffic will be accelerated or visible to the Node.
- *Force Off* - Card will never use Bypass Mode ensuring that traffic will never be bridged between the card's ports. This can be used when your network topology cannot use bridged mode, to guarantee a network loop will never be created.

Bonding Options

The *Bonding Options* define the behaviour of a network Bond. Depending on the *Mode* selected, different options will be available. The following is a list of all modifiable options.

Aggregation Mode:

Specifies which bonding policy the bond will operate under.

- *'Balance Round Robin' (default)* - Packets will be sent out of each bonded interface in turn (Round-Robin). Has both fault tolerance and load balancing.
- *'Active Backup'* - Traffic will be sent out of only one of the bonded interfaces. If that interface goes down another active bonded interface is used. Has fault tolerance.
- *'Broadcast'* - Traffic will be sent out of all bonded interfaces simultaneously. Has fault tolerance.
- *'LACP (IEEE 802.3ad)'* - Bonded interfaces will be grouped in to link aggregation groups (LAGs) with other interfaces in the bond that share the same speed and duplex settings. Only one LAG is active at any time. Traffic will be sent out of bonded interfaces in the active LAG based on the result of an XOR function performed on the MAC address of each packet. Has both fault tolerance and load balancing.

For more information about the different network bonding modes please refer to the *Bonding Guide*.

LAG Selection (compatible Modes - LACP):

Specifies which logic to use when selecting the active 802.3ad LAG.

- *'Highest Bandwidth (Stable)' (default)* - The LAG with the largest bandwidth is selected. LAG re-selection happens when all interfaces in the LAG are down.
- *'Highest Bandwidth (Always)'* - The LAG with the largest bandwidth is selected. LAG re-selection happens when:
  - Interfaces are added or removed from the bond.
  - An interface changes LAG.
  - The state of any of the interfaces in the bond changes.
  - The state of the bond changes to up.
- *'Highest Port Count (Always)'* - The LAG with the most interfaces is selected. LAG re-selection happens when:
  - Interfaces are added or removed from the bond.
  - An interface changes LAG.
  - The state of any of the interfaces in the bond changes.
  - The state of the bond changes to up.

Down Delay (compatible Modes - All):

Specifies the time to wait when a link failure is detected on a bonded interface before treating the interface as disabled. Down delay is measured in milliseconds, and should be a multiple of 100. The default is set to 0.

MAC Sharing (compatible Modes - Active Backup):

Specifies what the MAC addresses of the bonded interfaces should be set to.

- *'All Interfaces Copy Bond' (default)* - All bonded interfaces share the MAC address of the first interface in the bond.
- *'Bond Copies Active Interface'* - All bonded interfaces will retain their normal MAC address. The bond will take the MAC address of the active interface.
- *'Active Interface Copies Bond'* - All bonded interfaces will retain their normal MAC address when in fail over mode (not active). When an interface becomes active it will take the MAC address of the bond. The bond will take the MAC address of the first interface in the bond.

LACP Keep Alive Frequency (compatible Modes - LACP):

Specifies how frequently to transmit Link Aggregation Control Protocol Data Unit (LACPDU) 'keep alive' packets.

- *Slow (default)* - Every 30 seconds.
- *Fast* - Every 1 second.

Minimum Active Interfaces (compatible Modes - LACP):

Specifies the number of bonded interfaces that must be up in at least one LAG before the bond is reported as up. The default is set to 0. It should be noted that 0 has the same affect as 1.

Packets Per Interface (compatible Modes - Balance Round Robin):

Specifies how many packets should be sent via a bonded interface before the next interface is used. When set to 0 a random interface will be selected for each packet. The default is set to 1. There is a minimum value of 0, and a maximum value of 65535.

Primary Interface Re-Selection (compatible Modes - Active Backup):

Specifies the logic to use when selecting the active interfaces when the primary interface comes back up. The primary interface is the first interface in the bond.

- *As Soon As Possible (default)* - The primary interface becomes active whenever it comes back online.
- *Only If Better Than Current* - The primary interface becomes active if the speed and duplex is better than the currently active interface.
- *When Current Goes Down* - The primary interface becomes active if the currently active interface goes down.

If no interfaces are active, the first interface to come back up is selected as the active interface.

Up Delay (compatible Modes - All):

Specifies the time to wait when a link recovery is detected on a bonded interface before treating the interface as enabled. Up delay is measured in milliseconds, and should be a multiple of 100. The default is set to 0.

IGMP Membership Reports (compatible Modes - Balance Round Robin/Active Backup):

Specifies how many IGMP membership reports are sent when the active bonded interface changes. Membership reports are sent with 200ms intervals. Specifying a value of 0 prevents any reports being sent when the active interface changes. The default is set to 1. There is a minimum value of 0, and a maximum value of 255.

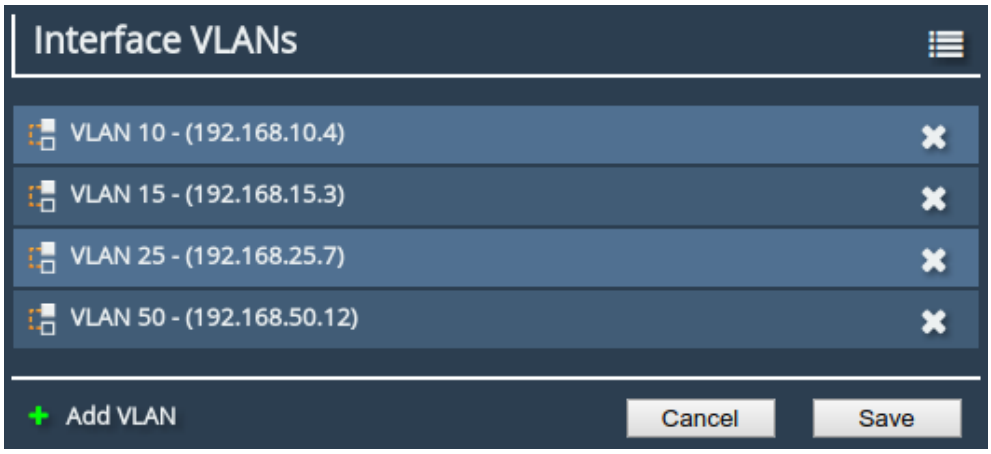
More information on these options can be found in the official Linux documentation:

https://www.kernel.org/doc/Documentation/networking/bonding.txt

Adding VLANs

If VLANs are enabled on the PORTrockIT they will be listed at the bottom of the port page. For each VLAN the ID and IP address are shown.

Refer to Section 3.1.3: General Settings for information about enabling VLANs on the PORTrockIT.



VLANs can be added to an interface by pressing the *Add VLAN* button. When the button is pressed an *Add VLAN* dialogue will appear. A VLAN can be created with an ID between 1 and 4094. A maximum of 64 different VLANs can be added to the PORTrockIT. To queue the VLAN for addition, press the *OK* button. The VLAN will not be added to the interface until the changes are committed. If the *Cancel* button is pressed or the page is navigated away from, the VLAN will not be added.

VLANs can be deleted by pressing the *X* to the right of the VLAN and selecting the *Delete* button. The VLAN will not be removed from the interface until the changes are committed. If the *Cancel* button is pressed or the page is navigated away from, the VLAN will not be removed.

The configuration page for a VLAN can be accessed by selecting the VLAN in the *VLANs* list. From the VLANs configuration page the IP address settings can be changed. See Section 3.1.7.6: Setting the IP Address.

Committing the Changes

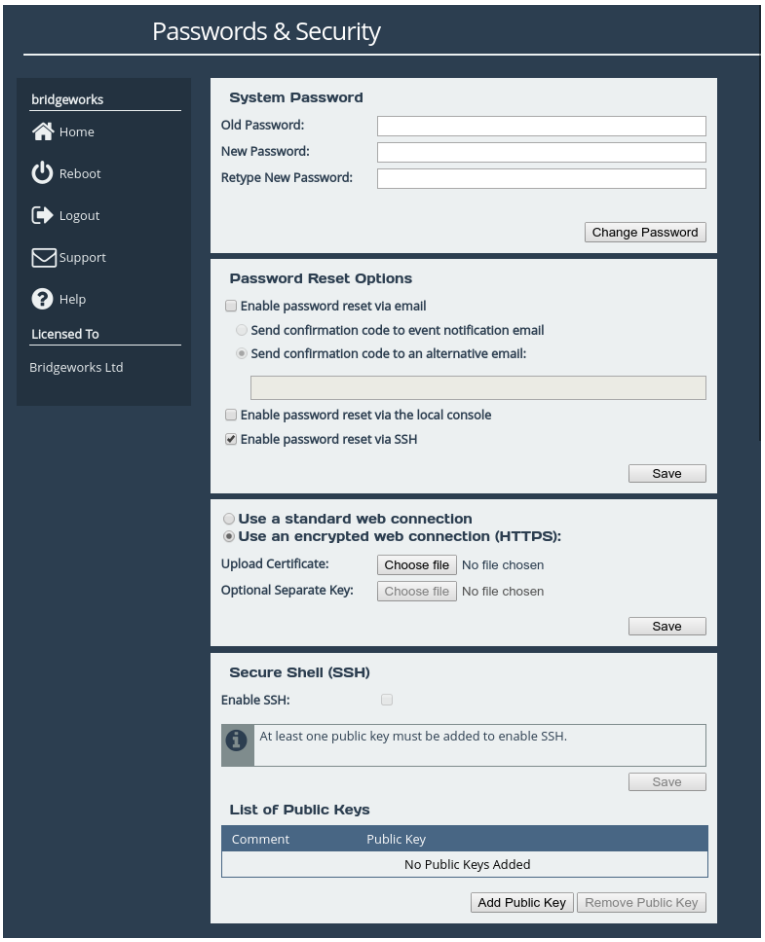
Click the *Save* button to save these parameters, then reboot the Node to apply them.

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:



System Password

This section allows the administrator to change the access password for the web interface. The new password must be between 5 and 65 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*.

Password Reset Options

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

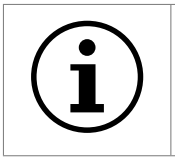
Password Reset via Email

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.

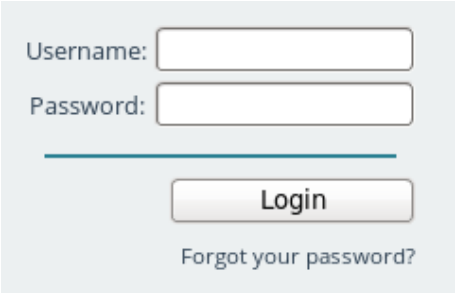
To enable password reset via email, SMTP settings will have to be configured first to allow the Node to send emails. Navigate to the *Service Control* page and enter your SMTP settings under the *Simple Mail Transfer Protocol (SMTP)* section. Refer to Section 3.3.5: Simple Mail Transfer Protocol (SMTP) 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.

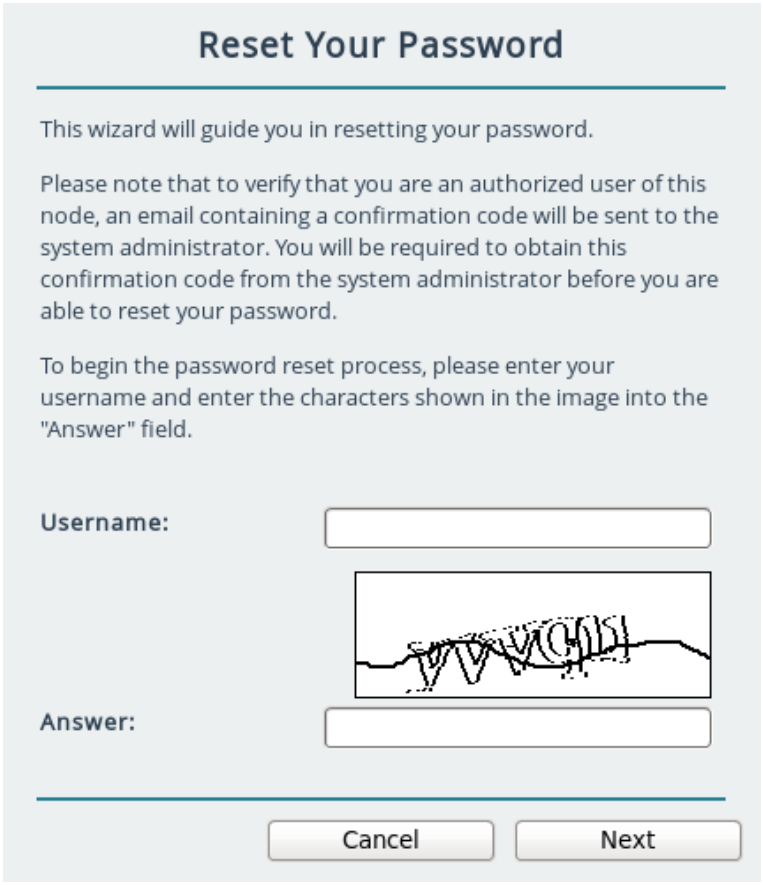
3.2.2.1.2 Using Password Reset via Email

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.

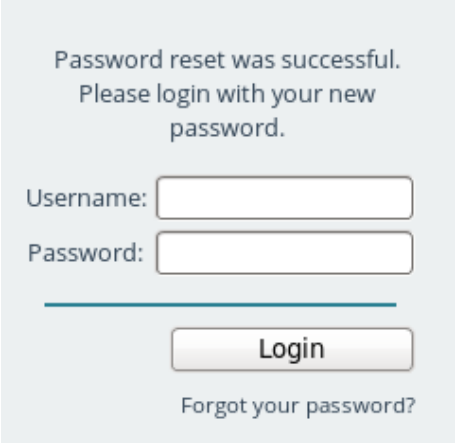


	Important: You can try a different captcha challenge by refreshing the web page.

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.



Password Reset via Local Console or SSH

	Important: Password reset via local console is unavailable on AWS or Azure Nodes due to the absence of a real console.

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.

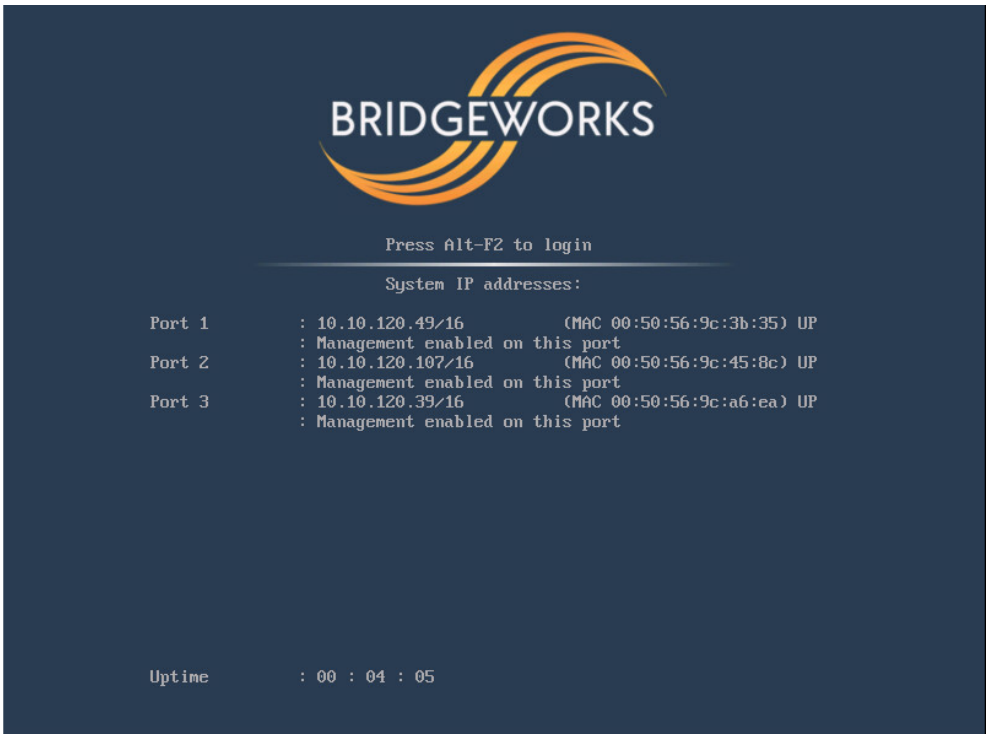
	Important: Resetting a password will log out any current sessions under that user name.

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:

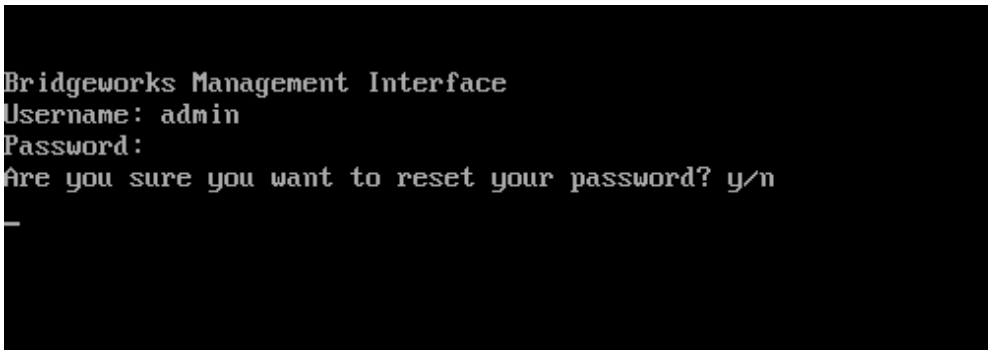


Press the “Alt” and “F2” keys at the same time to get access to the login prompt as shown:

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.

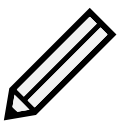
	Important: If the two passwords do not match, or you are attempting to set the password as “RESET”, then password reset will fail.

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.

Secure Connection

To enable HTTPS, select the *Use an encrypted web connection* radio button, and click Save.

	Note: By default, an HTTPS certificate & key will be generated when HTTPS is enabled.

You can use your own certifcate & 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.

Secure Shell (SSH)

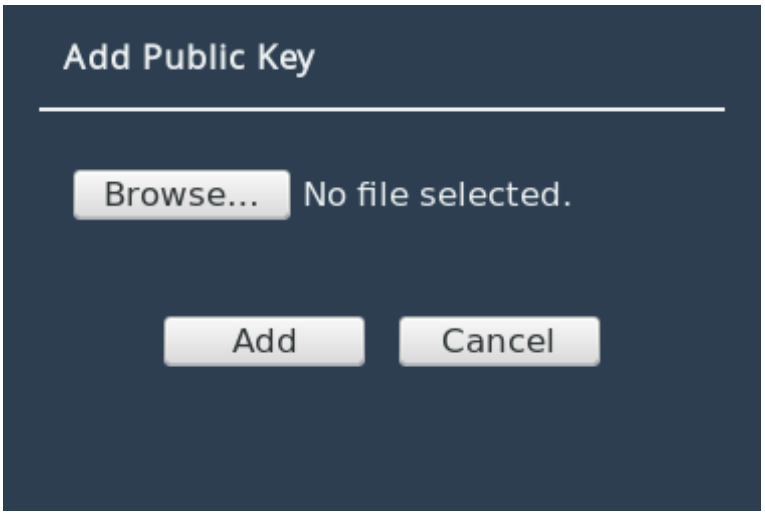
Secure Shell (SSH) is a protocol that allows for secure access to a Node's configuration console.

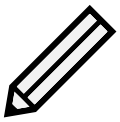
To enable SSH on network interfaces with the "Management" protocol mapped, tick the *Enable SSH* checkbox and click *Save*.

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.

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
```

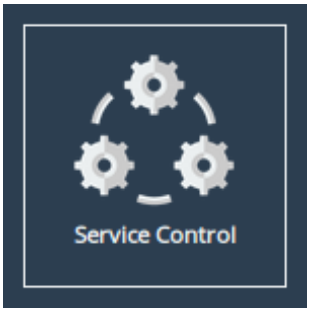
You will then be prompted for the username and password of the Node to log in to the configuration console.

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.

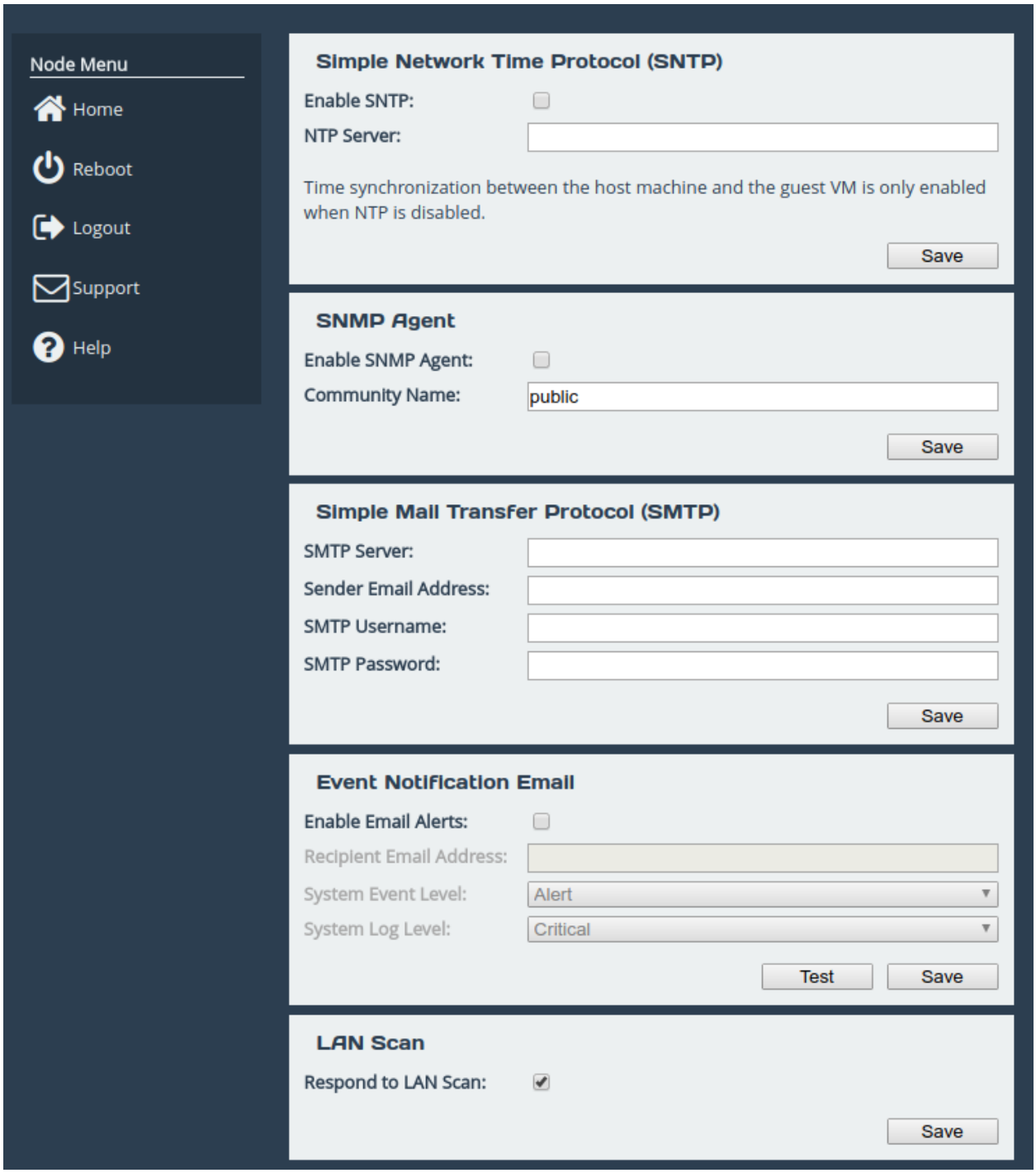
	Important: Logging in as root user is disabled on SSH.

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:



Simple Network Time Protocol

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 6.2: 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*.

SNMP Agent

To enable the Simple Network Management Protocol (SNMP) agent, select the *Enable SNMP Agent* checkbox and enter the *Community Name*. Then click *Save*.

Important: Only SNMP requests made with a matching community name will be responded to.

MIBs and OIDs

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

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 3.3.5: Simple Mail Transfer Protocol (SMTP) 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.

Simple Mail Transfer Protocol (SMTP)

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. It must be reachable from the Node's Management interface (or whichever port the default route is set to) on this address. Refer to Section 3.1.3.3: Default Route for information on setting the default route.

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.

LAN Scan

The LAN Scan software allows you retrieve the hostname, product name and port configuration of any Bridgeworks product on the local network.

To allow the Node to respond to LAN scan queries select the *Respond to LAN Scan* checkbox and click *Save* to apply.

PORTrockIT Configuration

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

Service List

The *Service List* page contains all the tools necessary to set up local services. A service defines a part of the local topology, including all information the PORTrockIT Node needs to connect to a target server.

These are linked to remote Nodes to define what traffic types are accelerated from which remote Nodes, to which target servers.

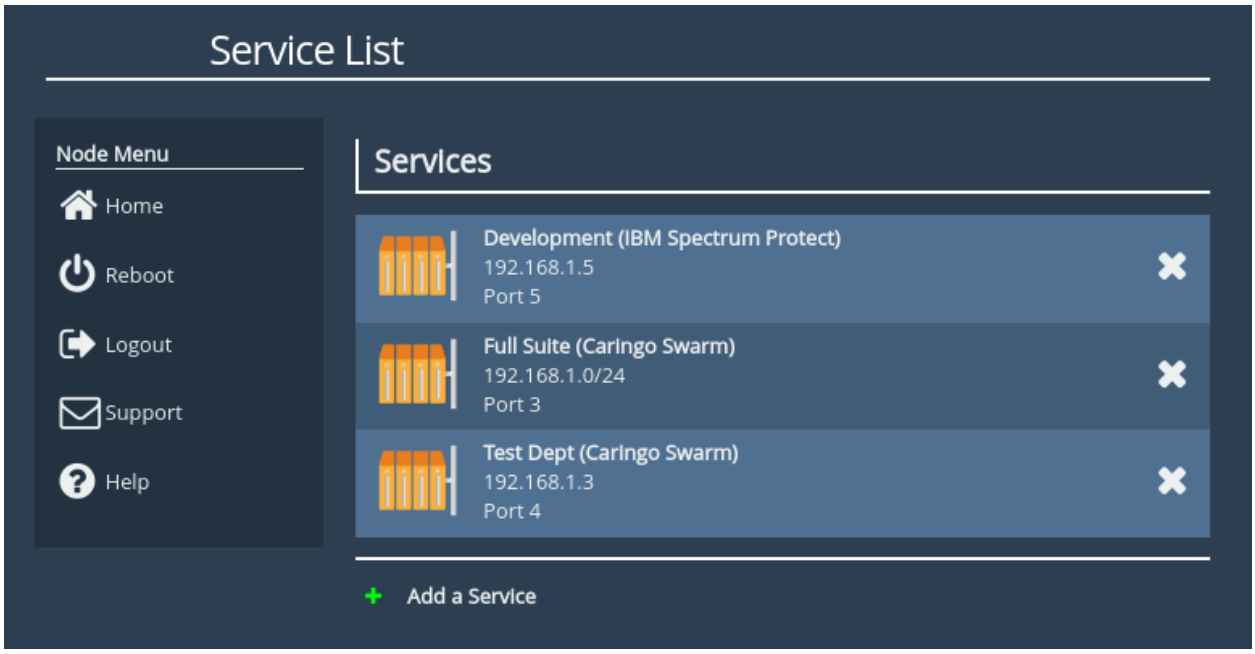
Preserving the IP addresses the endpoints previously connected with whilst traversing a NAT is required to prevent any re-configuration on your Endpoints. In this scenario the *Service List* page is able to set up local services within a previously established NAT environment. For complete NAT set up NAT mapping configuration is also needed.

Important: A WANdisco Fusion licence and a Cloud platform set up are currently required to establish a NAT preservation connection. For more information on NAT preservation mappings see Section 4.3: Client NAT Preservation.

From the Home screen, select the *Service List* icon under the *PORTrockIT* section.

Service Table

The page will display a table with all of the currently configured services listed as shown below.



Each service will give a summary including the designated *Name* and *Protocol*, followed by the given *Address* of that service and the *LAN Interface* that can be used to connect to that address.

Remove Service

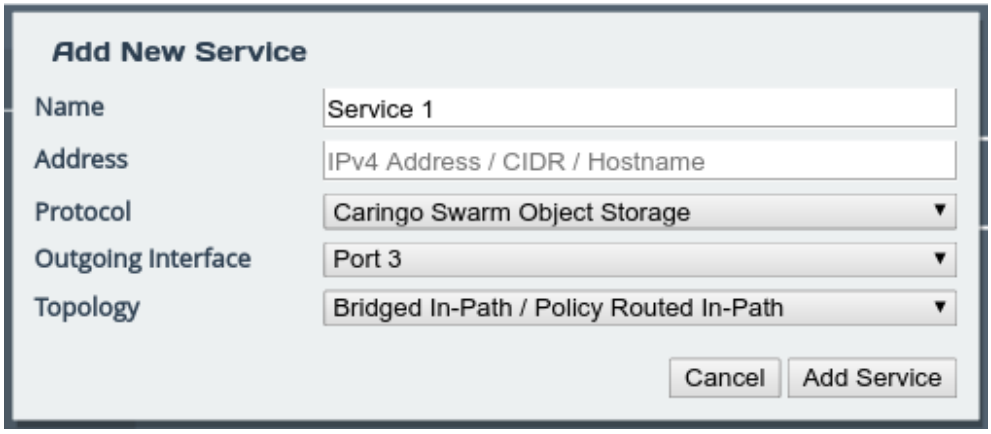
A service can be removed by clicking the 'X' icon on the right edge of the relevant table item. Confirmation will be required before the service is removed.

	Important: Removing a service will also remove all *Relationships* that use that service, potentially disrupting ongoing transfers.

Add Service

Clicking the *Add a Service* button will show a dialog which is used to configure a new service.

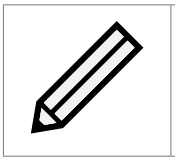
If a NAT preservation configuration has not been established for this PORTrockIT then the following box will be shown.



If NAT preservation is required on this system then an option to disable or enable NAT preservation for this service will be available.

Clearing the *Enable NAT* checkbox will disable endpoint NAT preservation and display the following dialog box.

Selecting the *Enable NAT* checkbox will enable endpoint NAT preservation and display the following dialog box.



Note: Available configuration options will vary depending on the exact mappings and protocols available to the PORTrockIT unit.

Name

A unique identifier used to differentiate between services. Must be between 1 and 45 characters long.

Address

The address of the local server being accessed. This can be either an IPv4 value, a CIDR block value, or a resolvable hostname.

Public IP - Only available if NAT has been enabled

The public IP of the local server being connected to. This must be a valid IPv4 address.

Private IP - Only available if NAT has been enabled

The private IP of the local server being connected to. This must be a valid IPv4 address.

Protocol

A selection of all currently mapped protocols. Used to define which specific traffic type this service will use. A protocol must be mapped to an interface using the *Port Mappings* page before it will appear as a selection. Only one protocol can be defined per service.

Outgoing Interface

A list of all interfaces with a valid PORTrockIT mapping. Only interfaces with the currently selected protocol mapped to them will be available for selection. This interface will be used for outgoing connections irrespective of global routing rules.

Topology

If the selected protocol does not require a two way connection, the exact topology used must be specified:

- **Bridged In-Path** - The PORTrockIT Node is placed directly in-Path between the server and WAN such that no additional routing rules are required for local traffic. The Node must be configured to act as a network bridge to use this topology.
- **Policy Routed In-Path** - The PORTrockIT Node is placed Logically In-Path between the server and WAN. Routing rules must be set up to ensure that traffic is passed through the Node on the local site.

  or

- **Out-of-Path** - Out-of-Path enables the acceleration of traffic where the PORTrockIT Node

is located in a different routing domain to the server. It achieves this using non-transparent addressing, and can only accelerate incoming connections to the server.

Cancel

Closes the dialog, discarding all current progress.

Add Service

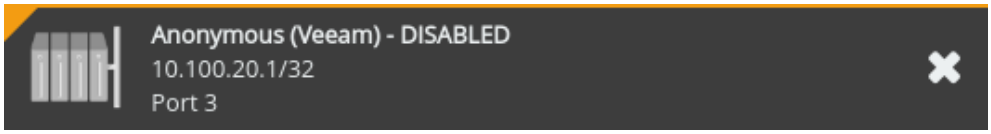
Completes the dialog, immediately setting up the service and updating the service list.

Disabled Services

Disabled services occur due to:

- Modifications to the licences and their association to a network interface
- An active interface, bond, or VLAN being deleted
- An active interface being bonded

If changes are made in this way, any active services that are no longer valid for the new configuration will be marked as disabled.



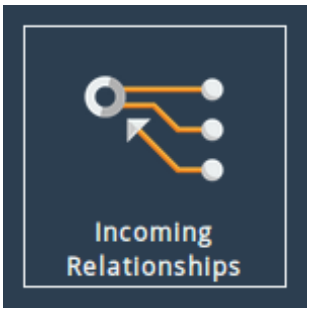
Any associated relationship configurations are immediately removed when a service is disabled resulting in potential disruption of traffic. Equally, it is not possible to activate a relationship using a disabled service.

In order to re-enable the service, the correct interface must be made available and mapped with the corresponding protocol licence as defined by the service listed (see Chapter 5: Port Mappings). Alternatively, the disabled service can be erased from the configurations (see Section 4.1.2: Remove Service).

Incoming Relationships

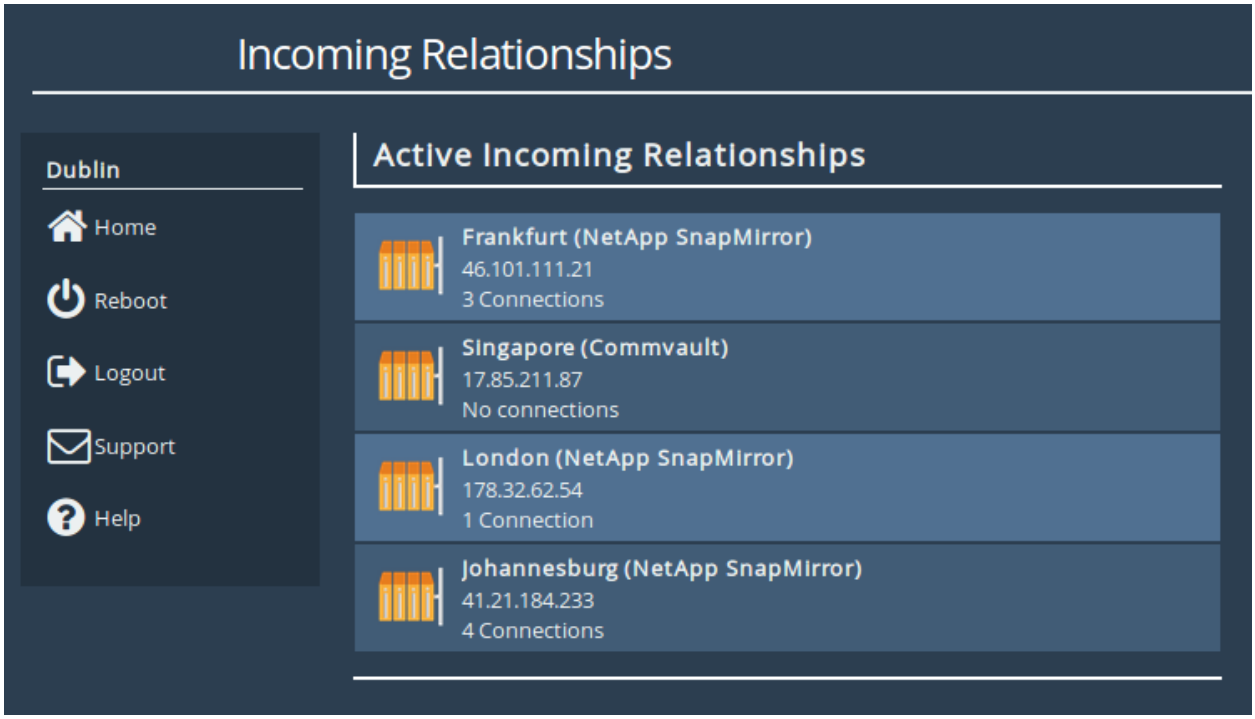
The *Incoming Relationships* page contains a list of service relationships that have been created by remote nodes.

From the Home screen, select the *Incoming Relationships* icon under the *PORTrockIT* section.



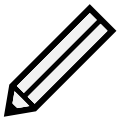
Active Incoming Relationships

The page will display a table with all of the currently configured service relationships that have been enabled for this node by remote nodes, as seen below.



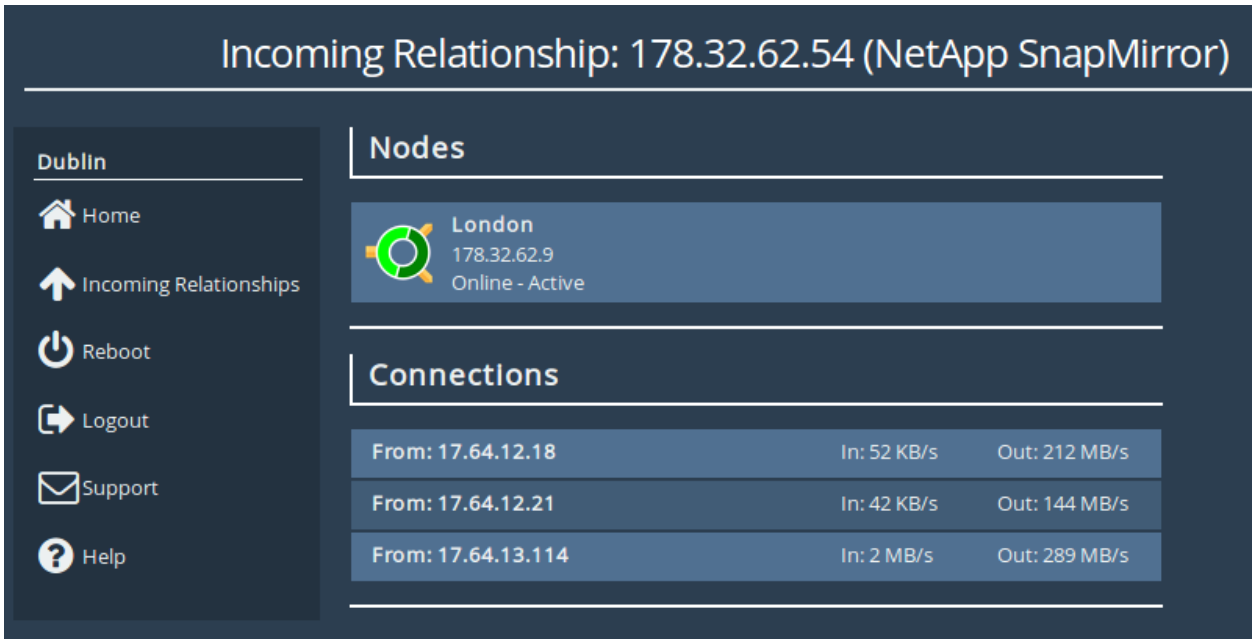
For each incoming relationship the following is displayed:

- Node hostname
- Service Protocol
- Service Address
- Number of connections using the service

	Note: All connections originating from the same IP address will be displayed as a single connection.

Incoming Relationship

Selecting an *Active Incoming Relationship* on the *Incoming Relationships* page will show the *Incoming Relationship* page.



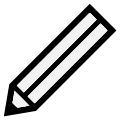
Nodes

This section will display the remote node that initiated the service relationship.

Connections

This section will show all connections that are currently using this service relationship. For each connection the following is displayed:

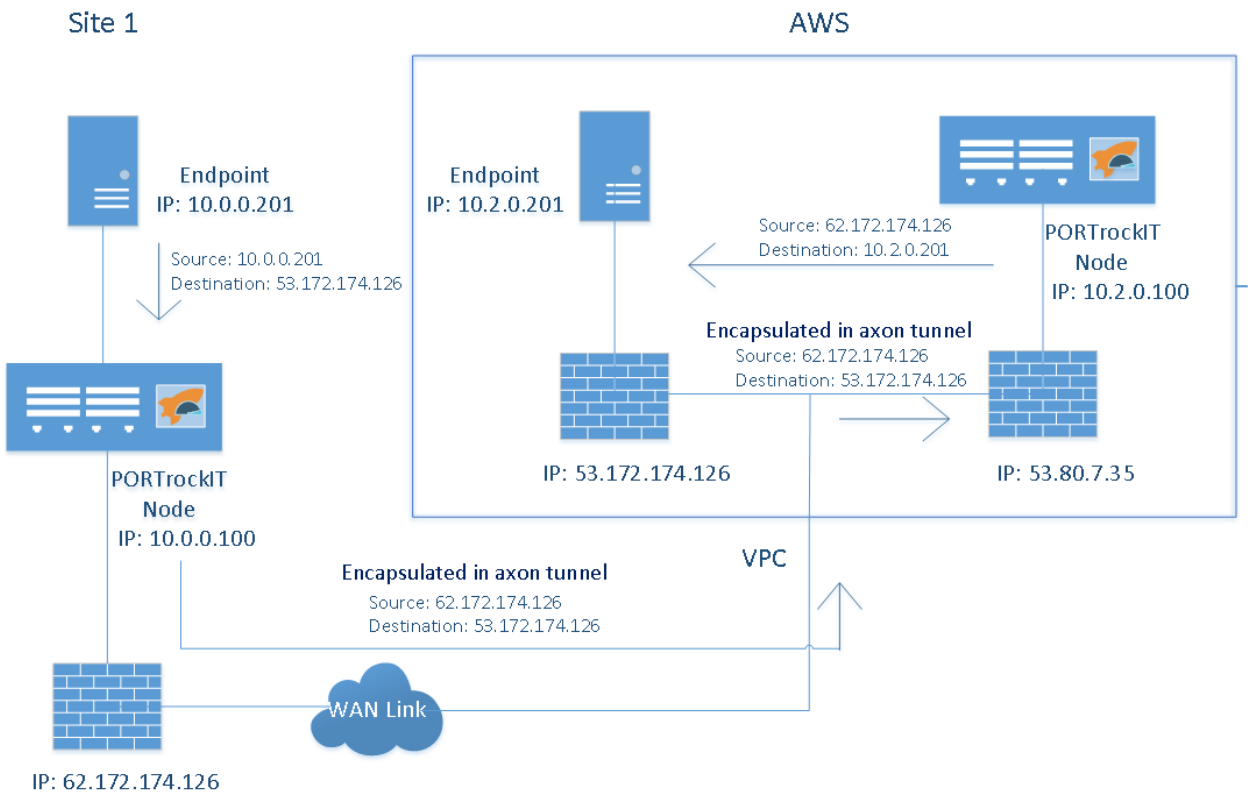
- Origin IP Address
- Incoming transfer rate
- Outgoing transfer rate

	Note: All connections originating from the same IP address will be displayed as a single connection.

Client NAT Preservation

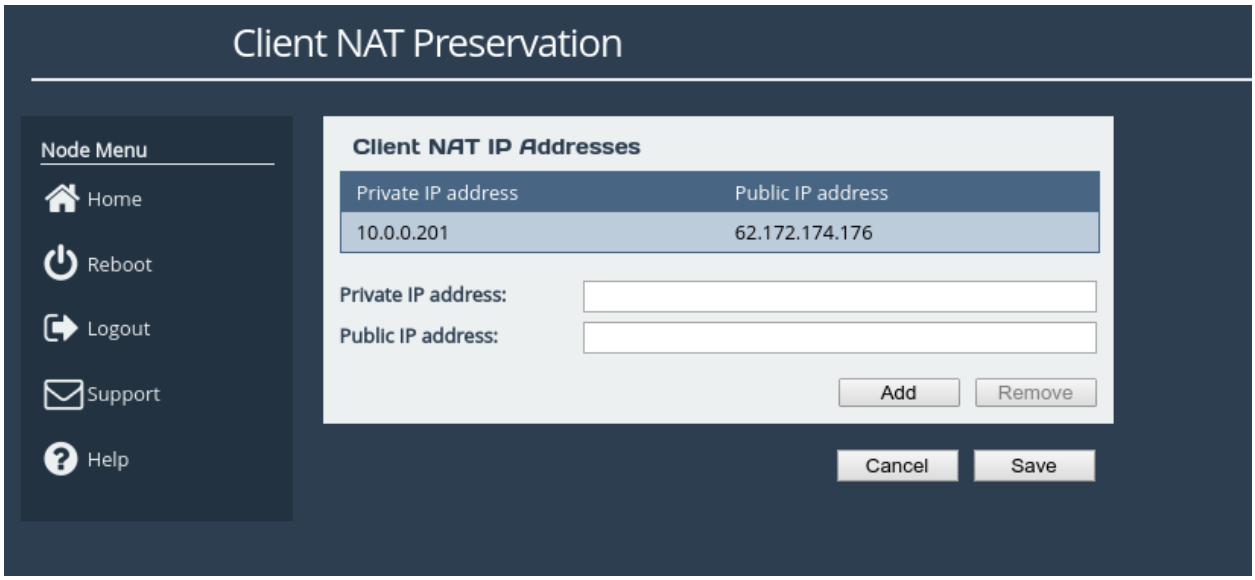
Client NAT preservation mappings are used for services that have been previously connected through a NAT, allowing the Endpoints to continue communicating without needing to modify their configuration. They map the Endpoints' old, public IP addresses to their new, private IP addresses.

The following diagram shows how this IP mapping works, demonstrating the source and destination addresses of traffic to be accelerated going between endpoints.



To configure client NAT preservation mappings, click on the *Client NAT Preservation* icon under the *PORTrockIT* section of the Home screen.

The following page will be displayed:



Client NAT IP Addresses Table

To establish a new mapping, enter the public and private IP pair into the table and click *Add*. Each IP must be a valid IPv4 address and the private IP must be unique.

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

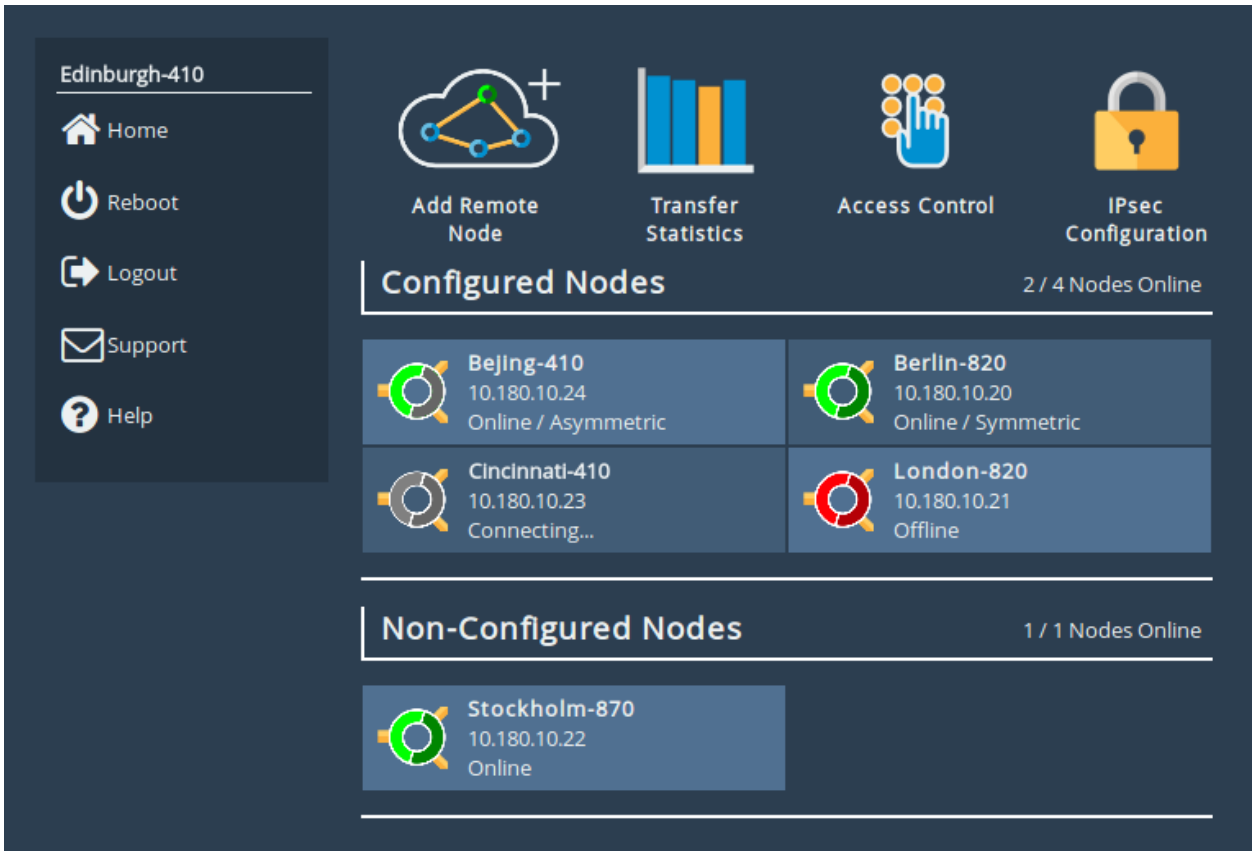
	Important: Adding or removing entries from the table will not take effect until the *Save* button is clicked.

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 *PORTrockIT* section.

The web interface will now display the following:

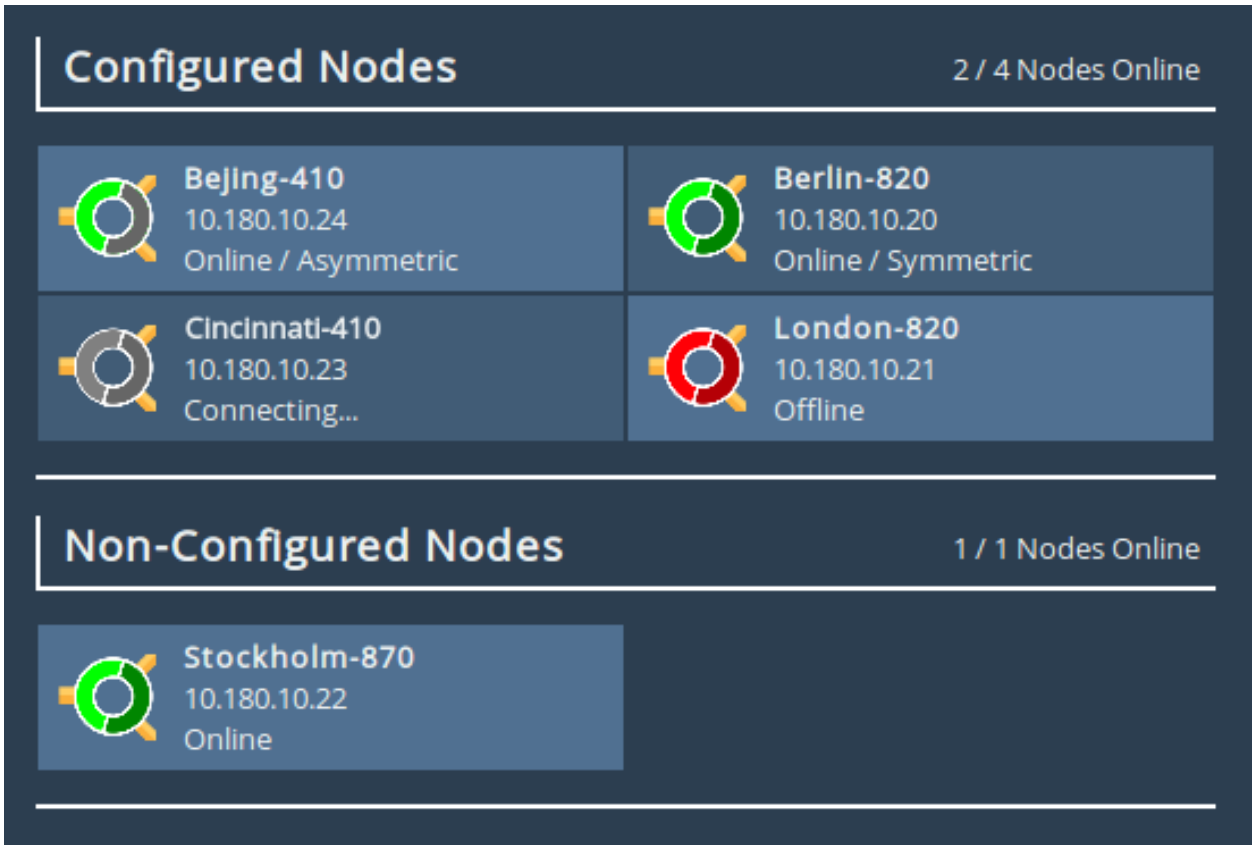


Options at the top of the page allow you to configure settings for your current Node. More information for these options can be found in the following sections:

- Section 4.4.2: Add Remote Node
- Section 4.4.3: Transfer Statistics
- Section 4.4.4: Access Control
- Section 4.4.5: IPsec

Remote Nodes

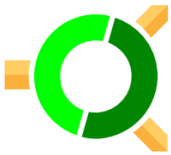
This section details the Nodes that have been configured with your appliance.



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.

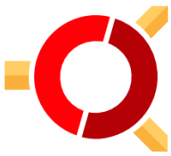
In addition to the hostname, the leading IP address will be displayed. This will usually be the IP address which was used to add the Node on the *Add Remote Node* page.

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.

Configured Nodes

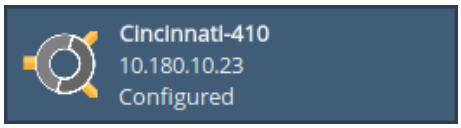
This list represents Nodes that have been directly added. Nodes in this list have additional configuration options available for them.

Non-Configured Nodes

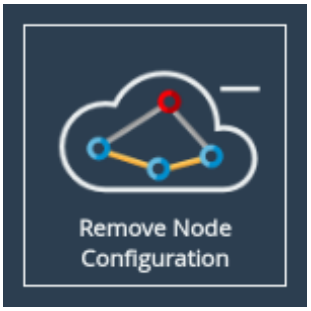
This list represents Nodes that have made an inbound connection, but have not been directly added. *Relationships* and *VPN* tunnels can still be created for Nodes in this state and acceleration can still be performed. A *Non-Configured Node* can become a *Configured Node* by performing the *Add Remote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

Orphaned Nodes

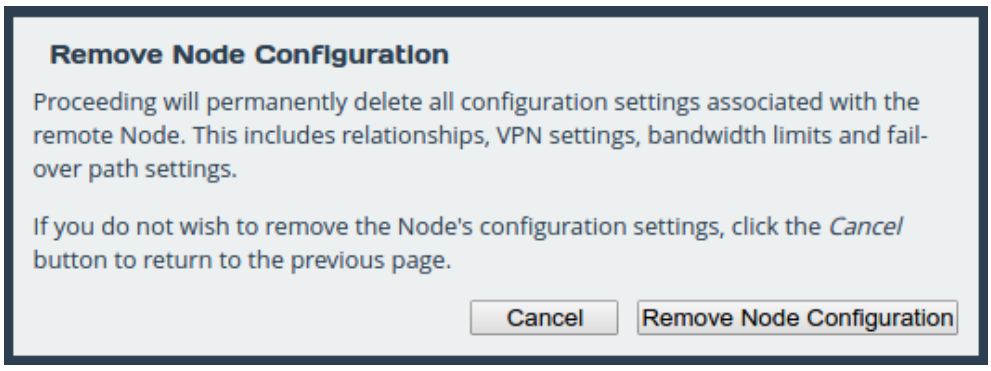
An orphaned Node is a remote Node which has configuration settings, hasn't been directly connected, and hasn't established the inbound connection to this Node. These Nodes will be displayed in the *Configured Nodes* list and look like the following example.



These configuration settings can be deleted by first clicking on the orphaned Node and then clicking on *Remove Node Configuration*.



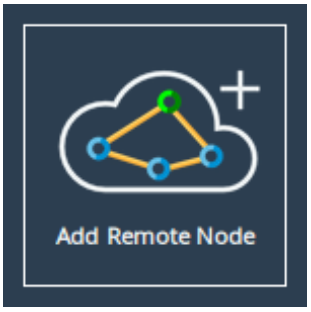
This takes you to the Remove Node Configuration page as shown below.



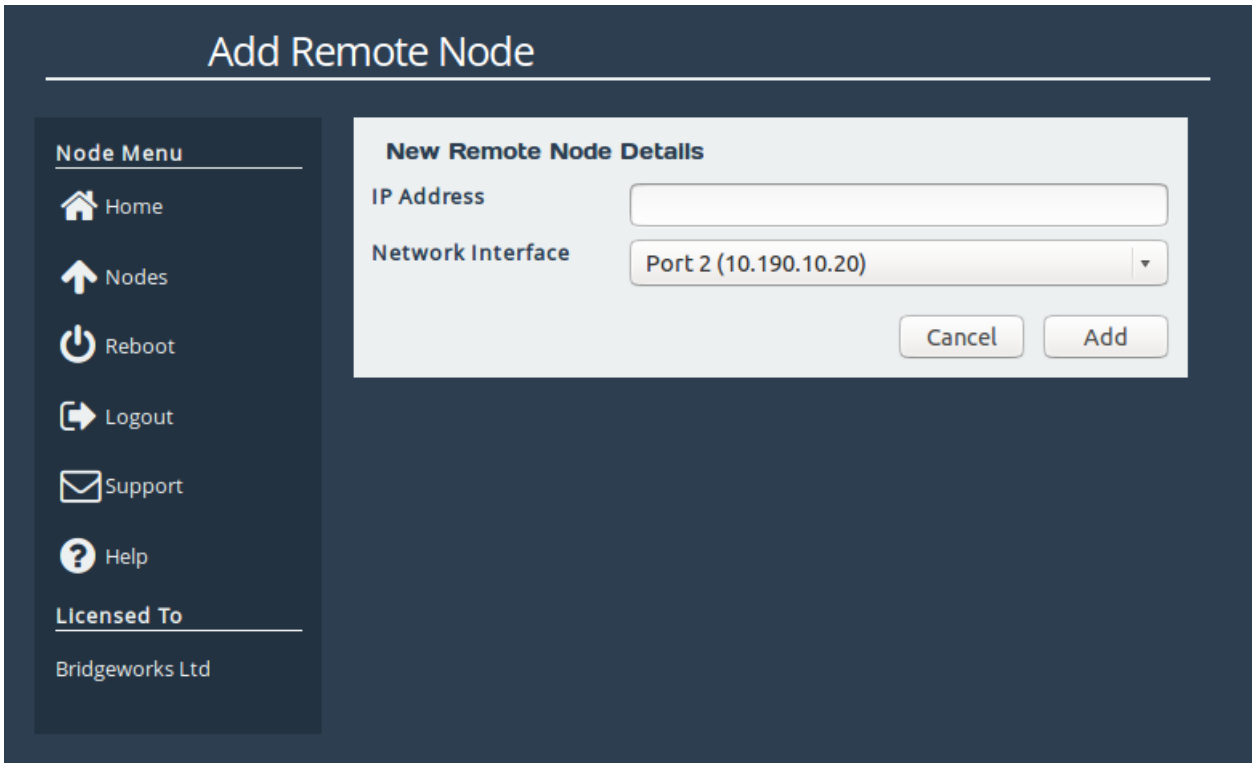
Click on the *Remove Node Configuration* button and confirm the removal to delete the saved configuration settings.

Add Remote Node

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 5: 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.

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.

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 red.

	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 red 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.

Download 24 Hour Transfer History

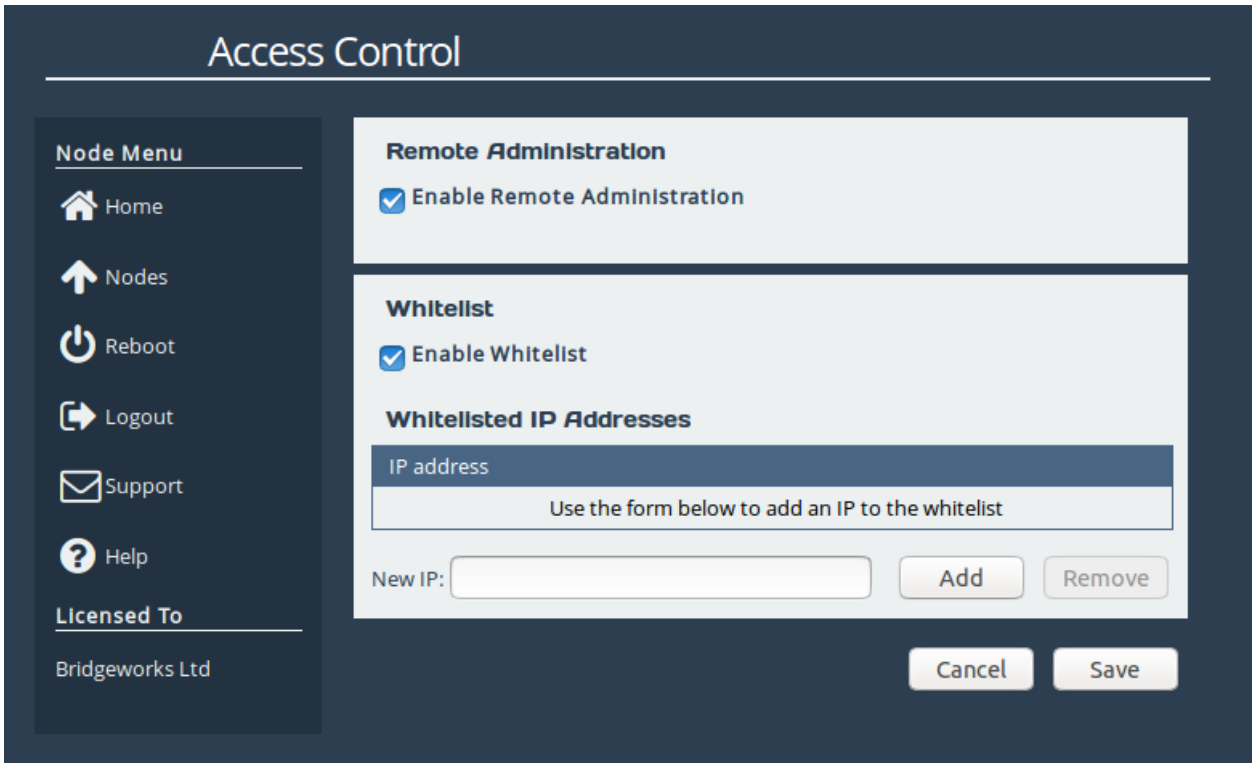
You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Click Here to Download* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix D: Transfer Statistics Graphing Instructions for Excel 2010 for information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

	Note: The 24 hour statistics are cleared on reboot.

Access Control

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

The following page will be displayed:



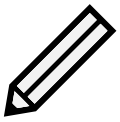
Remote Administration

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 4.5.16: Remote Control.

Whitelist

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

	Note: Adding a Node via Add Remote Node will automatically add its IP address to the whitelist.

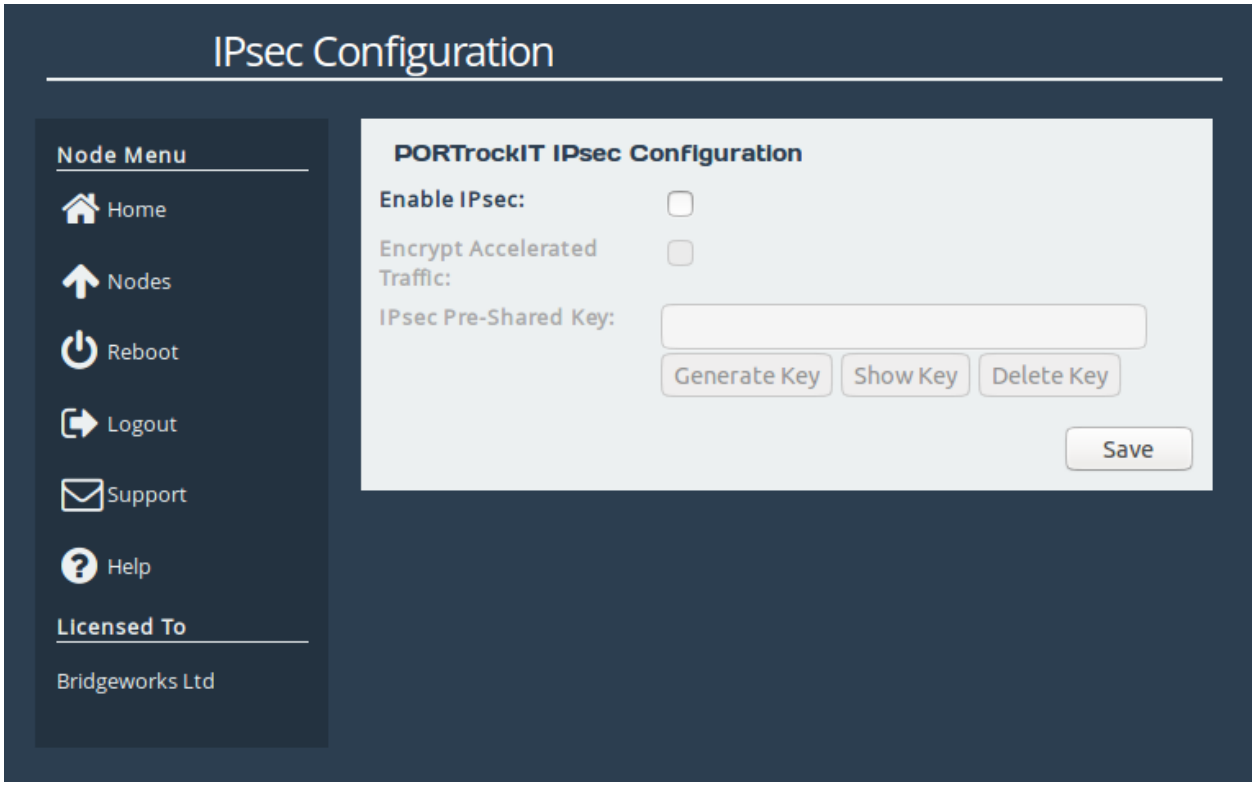
To delete a listing, select the entry in the *Whitelisted IP Addresses* table and then click *Remove*.

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

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

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.

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.

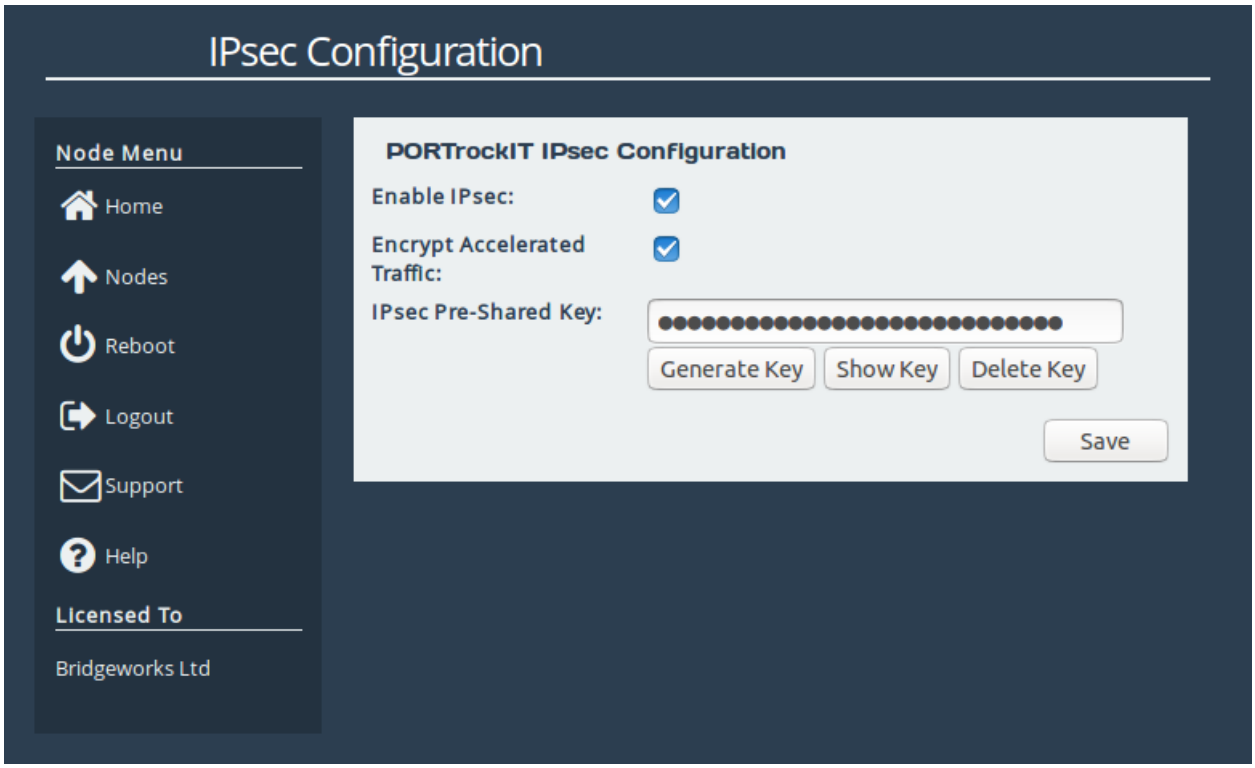
The pre-shared key will not display automatically when returning to this page. If you need to copy it to another Node, click the *Show Key* button.

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.

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.

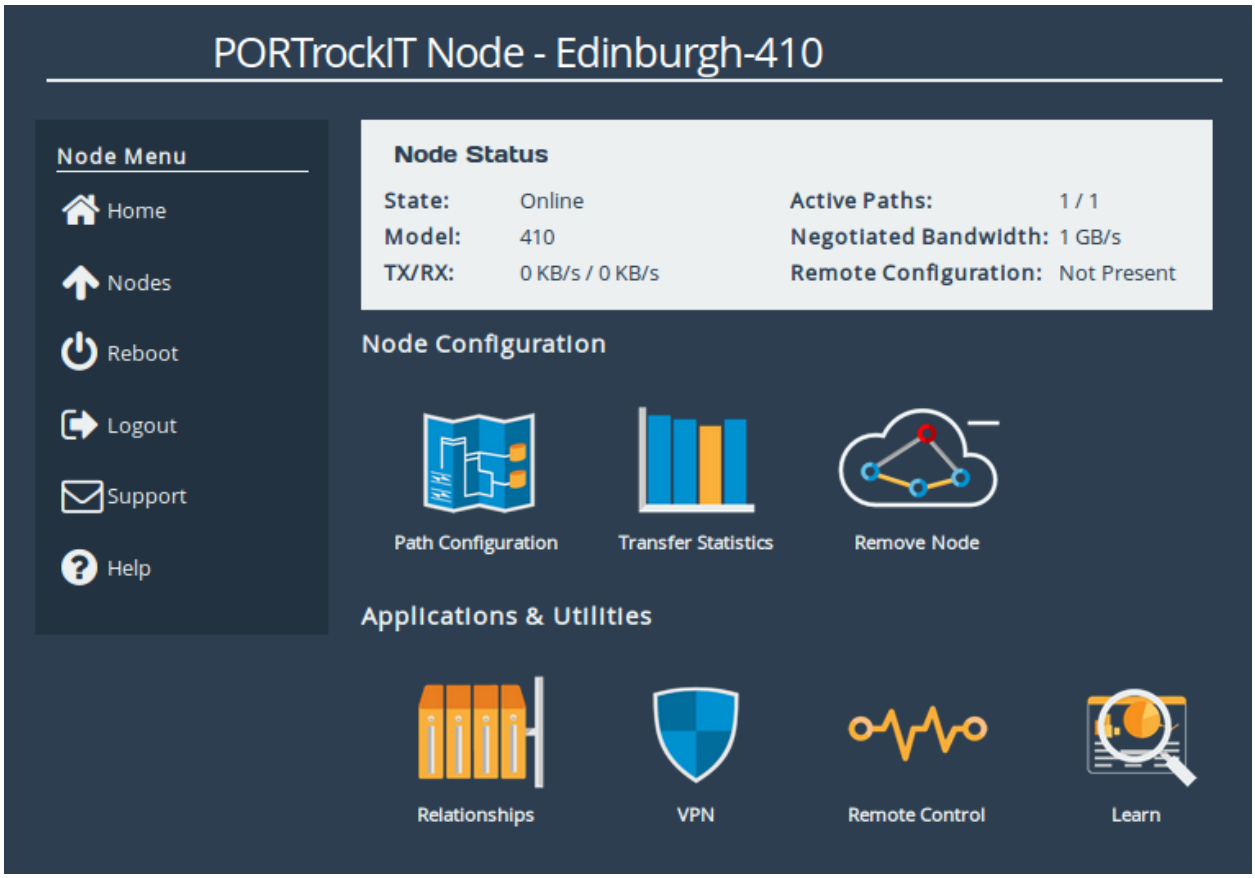


	Important: A pre-shared key is necessary for both VPN connections, and WAN link encryption.

PORTrockIT Node Page

The *PORTrockIT 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 *PORTrockIT 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*.

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*.

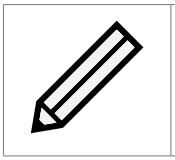
Active Paths Both the total number of available paths to the remote Node as well as the number that are currently active.

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*.

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 4.5.4: Path Configuration
- Section 4.5.5: Node Specific Transfer Statistics
- Section 4.5.6: Remove Node

Applications & Utilities

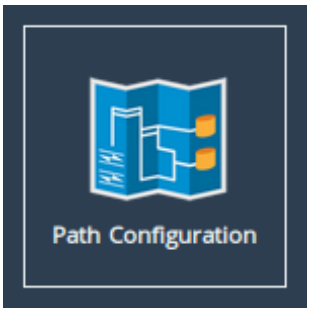
Any available *Applications* or *Utilities* are displayed here. More information for these options can be found in the following sections:

- Section 4.5.7: Relationships
- Section 4.5.14: VPN Configuration
- Section 4.5.16: Remote Control
- Section 4.5.17: Learn

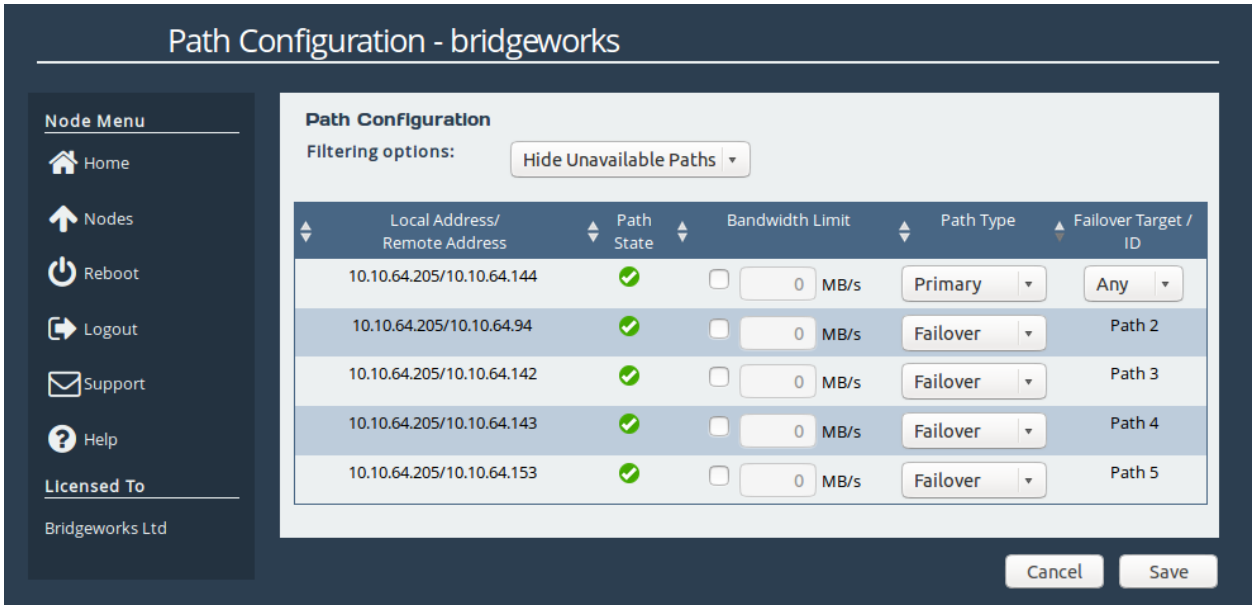
Path Configuration

The PORTrockIT Node will always attempt to get the best performance possible for the data it is transferring. Upon establishing a connection between two PORTrockIT 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.

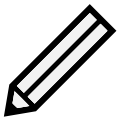


A table will be displayed showing all paths between the current Node and the remote Node.



Setting Primary and Failover Paths

A path is a connection between two IP addresses when you establish a link between two PORTrockIT 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 PORTrockIT 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.

Filtering options

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

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.

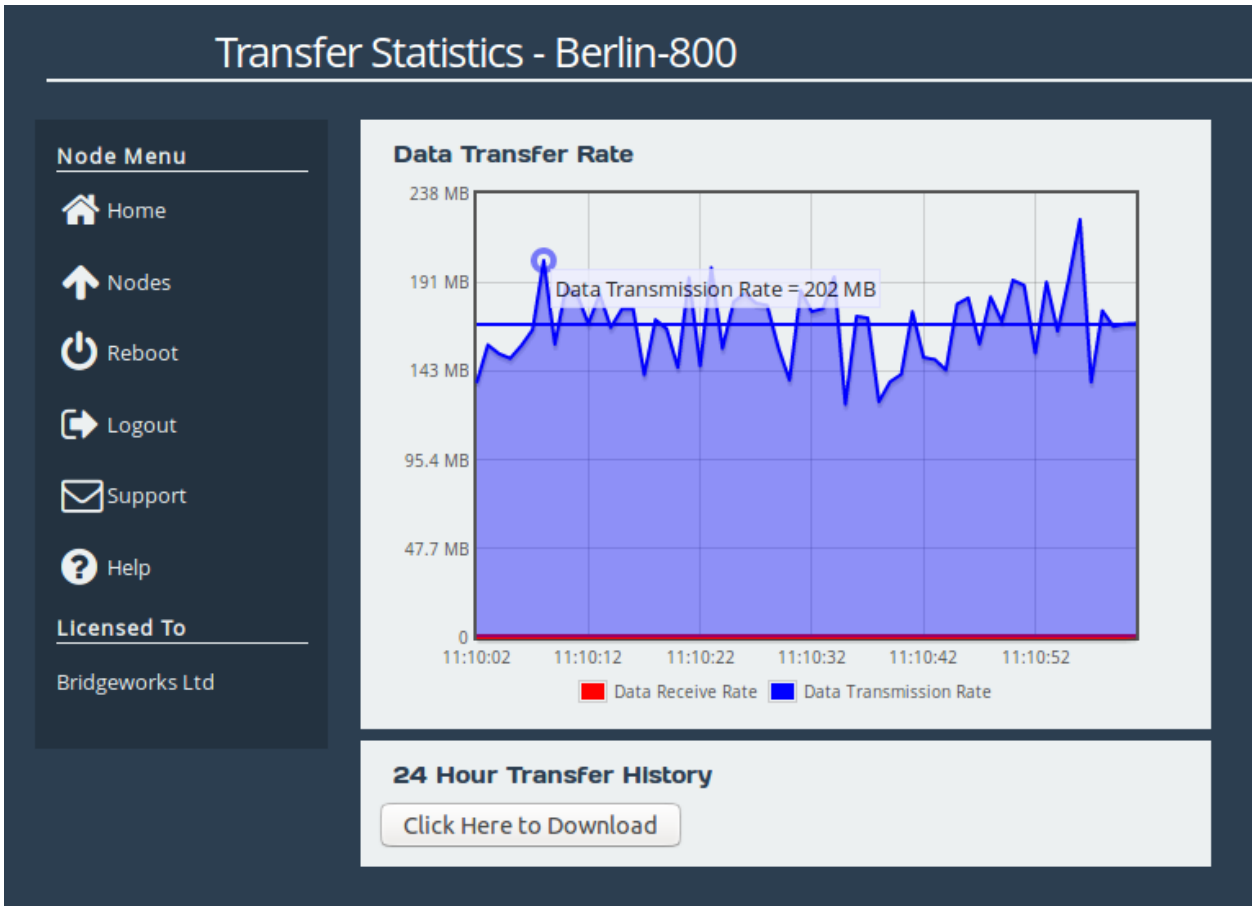
	Note: Any changes to the bandwidth limit will become effective immediately on pressing *Save*.

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.

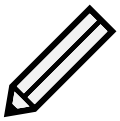
Navigate to the management page of the remote Node and click the *Transfer Statistics* icon.

The web interface will then display the following window:



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 red.

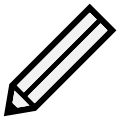
	Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and red 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.

Download 24 Hour Transfer History

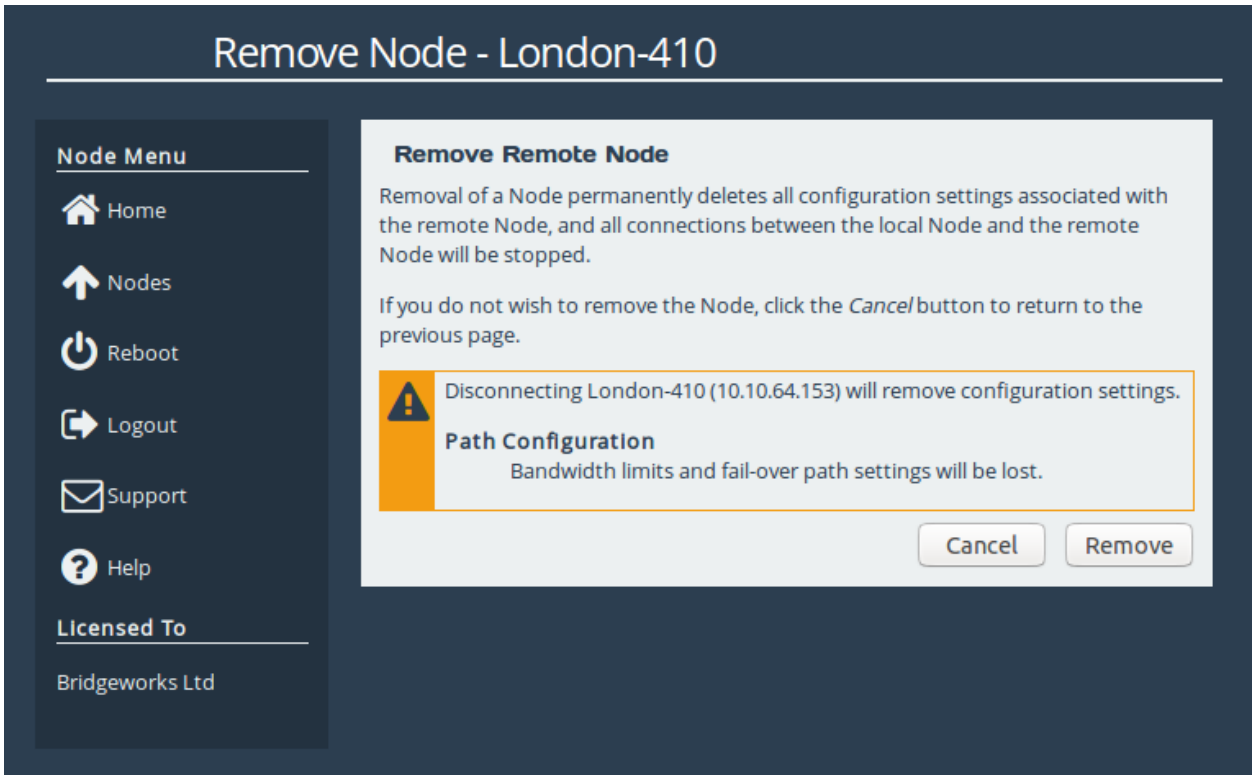
You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Click Here to Download* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix D: Transfer Statistics Graphing Instructions for Excel 2010 for information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

	Note: The 24 hour statistics are cleared on reboot.

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.

	Important: Removing a Node will not terminate existing transfers unless both Nodes have removed each other and been rebooted together.

Relationships

The *Relationship* between two Nodes dictates which traffic is accelerated by a remote Node. This is done by linking one of the pre-configured services (see Section 4.1: Service List) to a remote Node. The remote Node will then recognise any traffic that matches the service and accelerate it.

Prerequisites

In order to establish an acceleration link you must have the following:

- Two PORTrockIT Appliances or Virtual Instances.
- A WAN link established between the two PORTrockIT units see Chapter 4: PORTrockIT Configuration.
- Two NetApp units with SnapMirror IP replication enabled using the default TCP port numbers 11104 and 11105.

  or

- An IBM Spectrum Protect Client 7.1.2.0 (or above) and an IBM Spectrum Protect Server 6.3.5.0 (or above).

  or

- A CommServe server and a MediaAgent running Commvault 11 (or above).

  or

- A Veritas server and client running Veritas NetBackup 7.6.0.3 (or above).

  or

- A Caringo object storage server and client running Caringo Swarm version 7.5 (or above).

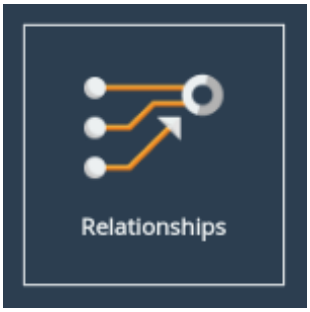
  or

- Two or more Veeam servers running Veeam Backup & Replication 8.5 (or above).

  or

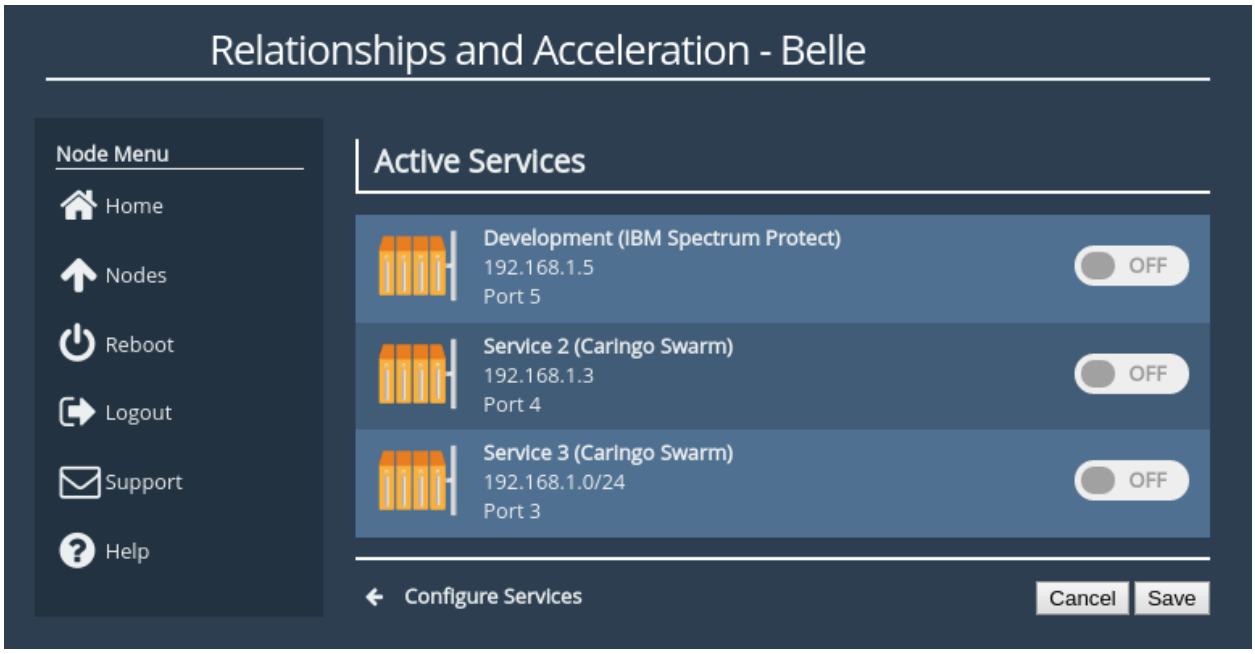
- Two or more WANdisco Fusion Nodes joined in a membership, running version 2.6.7 (or above).

To configure the *Relationships* for any remote Node, navigate to the management page of the remote Node you wish to configure and click the *Relationships* icon.



Services Table

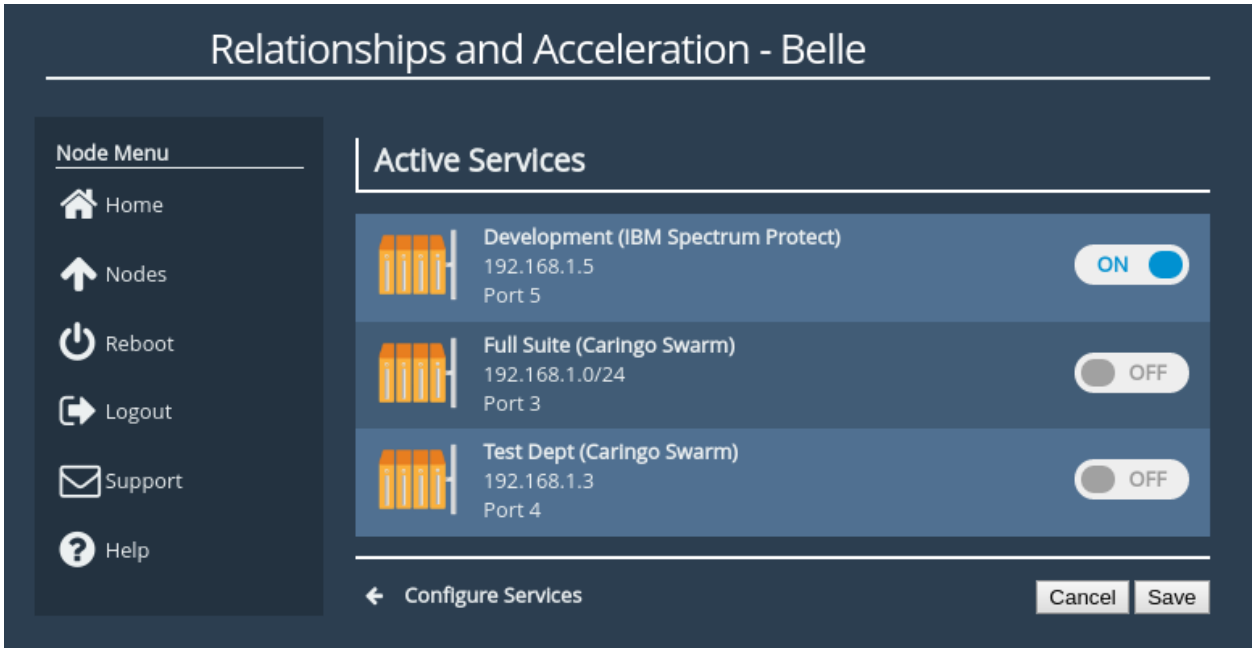
The page will display a table with all of the currently configured services listed as shown below.



Each service has a summary including the designated *Name* and *Protocol*, followed by the given *Address* of that service and the *LAN Interface* that can be used to connect to that address.

Toggling a Relationship

Services have a switch on the right edge of the table item. This will toggle the relationship off or on as shown.



The page must be saved for any changes to take effect.

Configure Services

This link will navigate directly to the *Service List* page, allowing new services to be configured if they have not already been set up.

Cancel

Returns to the *Node Specific* page discarding any changes.

Save

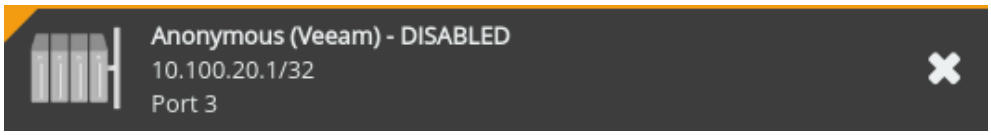
Commits any changes made, setting up *Relationships* for any services that have been linked to this remote Node.

Disabled Services

Disabled services occur due to:

- Modifications to the licences and their association to a network interface
- An active interface, bond, or VLAN being deleted
- An active interface being bonded

If changes are made in this way, any active services that are no longer valid for the new configuration will be marked as disabled.



Any associated relationship configurations are immediately removed when a service is disabled resulting in potential disruption of traffic. Equally, it is not possible to activate a relationship using a disabled service.

In order to re-enable the service, the correct interface must be made available and mapped with the corresponding protocol licence as defined by the service listed (see Chapter 5: Port Mappings). Alternatively, the disabled service can be erased from the configurations (see Section 4.1.2: Remove Service).

VPN Configuration

Connected PORTrockIT Nodes can set up a *VPN Tunnel* across the WAN link. This can be helpful if the PORTrockIT Nodes represent the only viable path between the two Endpoints, allowing non-accelerated traffic to pass through a dedicated link.

To begin setting up a VPN tunnel to a remote Node, navigate to the *VPN* page from the management page of the remote Node.

The following page should be displayed.

VPN settings can be enabled by ticking the *Enable VPN* checkbox.

The tunnel will require a CIDR block representing the *Local Subnet* to be entered into the *Local Subnet* input box.

	Important: The *VPN tunnel* will only initialise once the *Local Subnet* has been configured in this way on **both** the local and remote Nodes.

	Important: The *VPN tunnel* requires IPsec to be configured and running to the remote Node before it can be activated. See Section 4.4.5: IPsec for more details on configuring IPsec.

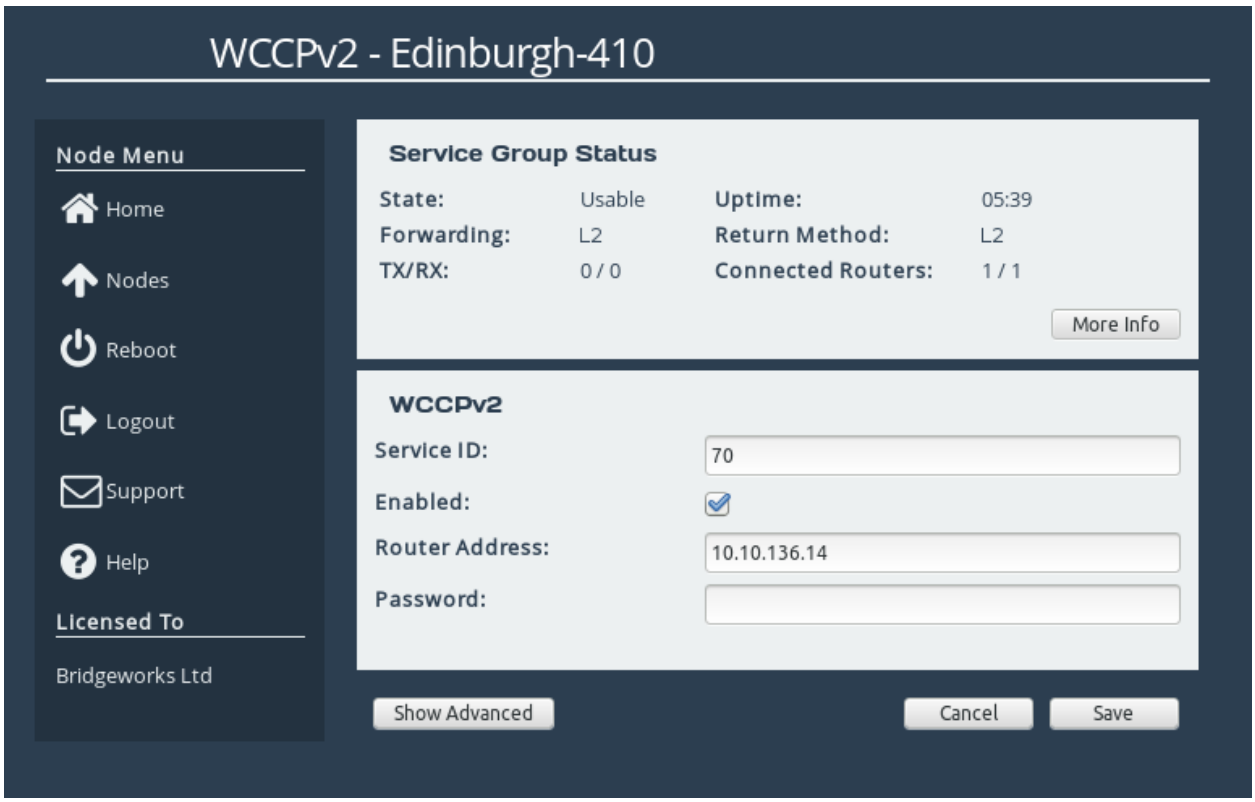
	Important: The *VPN tunnel* cannot be activated if any of the Node's Interfaces are configured to act as a *Network Bridge*.

WCCPv2

WCCPv2 allows traffic between two Nodes to be accelerated without any configuration at the endpoints. The web interface allows for configuration of a service group for each Node, as well as viewing the status of connected web-caches and routers.

To begin setting up a WCCPv2 connection with a remote Node, navigate to the *WCCPv2* page from the management page of the remote Node.

The following page will be displayed.



Prerequisites

In order to establish WCCPv2 acceleration you must have two PORTrockIT Appliances or Virtual Instances, with a WAN link established between them, and licensed TCP acceleration protocols. For more information on establishing a WAN link, see Chapter 4: PORTrockIT Configuration.

Configuring a Service Group

Details for a service group configured on a compatible Cisco router should be entered on this page in order for the Node to join the service group. Fields are available under the *WCCP* heading.

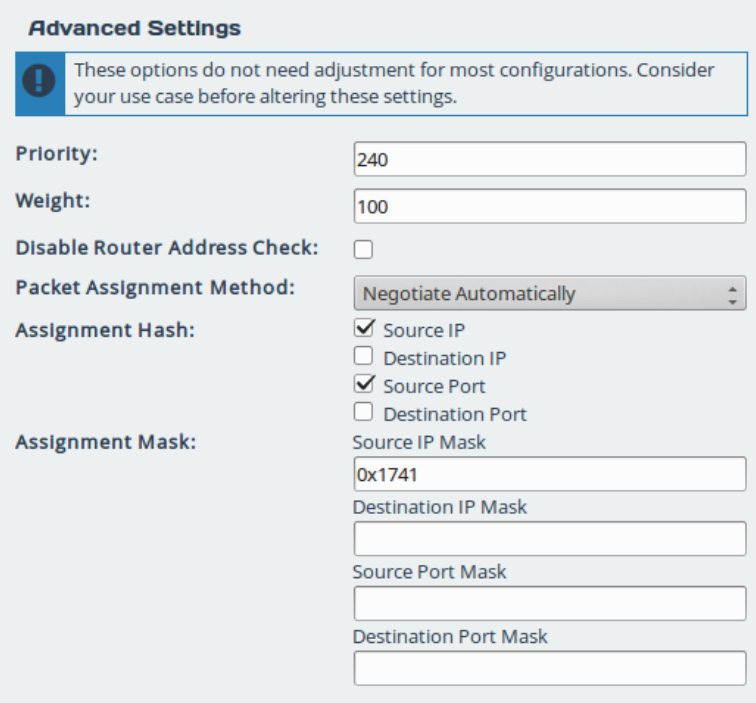
Service ID Service ID for this service group. This should be a number between 0 and 255 which matches the service ID value set on all routers in the service group.

Enabled Whether this Node should join the service group.

Router Address The address(es) used to communicate with the routers in the service group. This can be: a single router IP address; a comma-separated list of router addresses; or a single multicast address on which all routers in the service group must be configured to listen.

Password An optional password, up to eight characters long, used for MD5 authentication when joining a service group. This should match the WCCP security setting used on routers in the service group. This field can be left blank to disable MD5 authentication.

The above settings should be sufficient to begin WCCPv2 acceleration with most configurations. In the event of differing needs for specific hardware configurations, further settings are available under the *Advanced* heading. Click the *Show Advanced* button to display this section.



The settings available for further configuration are listed below.

Priority The priority with which packets for redirection are matched against those from other service groups. Valid inputs are 0 to 255, with 0 representing the lowest priority.

Weight The priority of the web-cache in relation to others in the service group, with 0 representing the lowest weight. Valid inputs are 0 to 65,535. Default value is 100.

Disable Router Address Check This option allows negotation with a router if it replies to the Node from an IP address other than that specified under *Router Address*. Selecting this option should only be done when absolutely necessary. It is not necessary if a multicast address is specified under *Router Address*.

Packet Assignment Method Method with which packets are allocated across routers within the service group. *Automatic* negotiates with the router to decide a method. If using the *Automatic* method, fields can be optionally filled in to be used in the case of negotiating to either *Hash* or *Mask* assignment. If a Packet Assignment Method is chosen, input fields are only available for the selected assignment method.

Assignment Hash Assignment Hash checkboxes represent elements of the packet to be used when the Packet Assignment Method is set to *Hash Assignment*.

Assignment Mask Assignment Mask fields take in a hexadecimal value of up to eight characters, in the format `0x00000000`. The values represent binary bitmasks used by routers to distribute traffic when the Packet Assignment Method is set to *Mask Assignment*. The maximum number of total high bits across all masks combined should be no more than 7.

Monitoring a Service Group

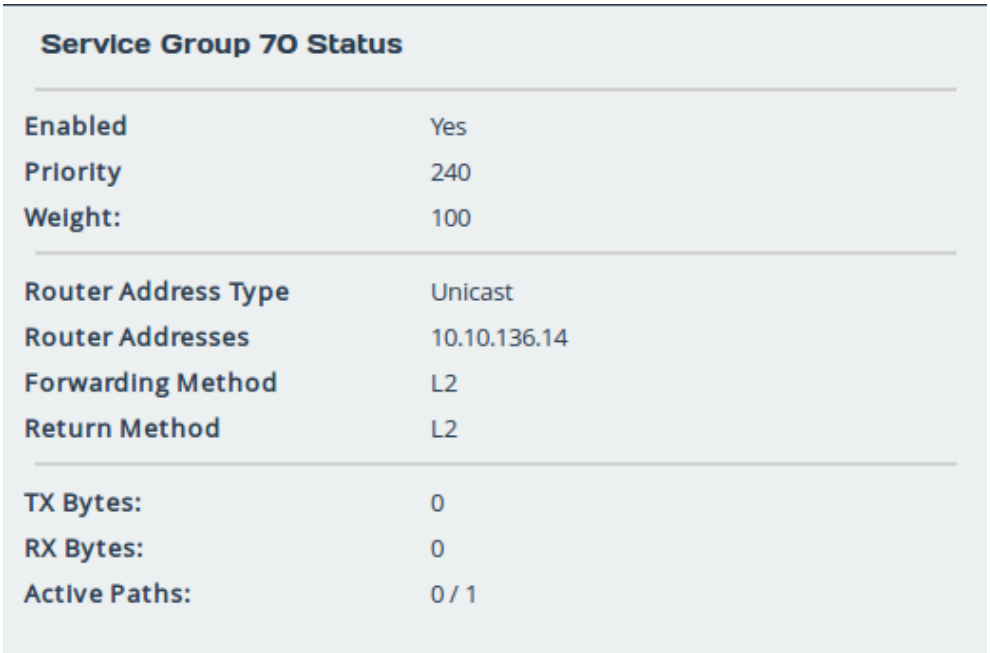
The status of the service group can be observed with the field under the *Service Group Status* heading. The fields display basic information about an established service group.

Clicking the *More Info* button in the *Service Group Status* field on the WCCPv2 page leads to the *Service Group Status* page. This page allows for more in-depth monitoring of a service group, and shows information for each connected router.

WCCPv2 Service Group

The *Service Group* page allows you to observe the state of a service group, an ensure that it is working as expected.

The *Service Group Status* section shows negotiated settings and current information for the service group.



Enabled Whether the service group is currently active.

Priority Priority of the web cache against other web caches connected to a router.

Weight The priority of the web-cache in relation to others in the service group.

Router Address Type Whether the router(s) are connected through unicast addresses or a multicast address.

Router Addresses Multicast address, or list of individual router addresses, which are visible to the Node in the service group.

Forwarding Method Negotiated forwarding method across all routers.

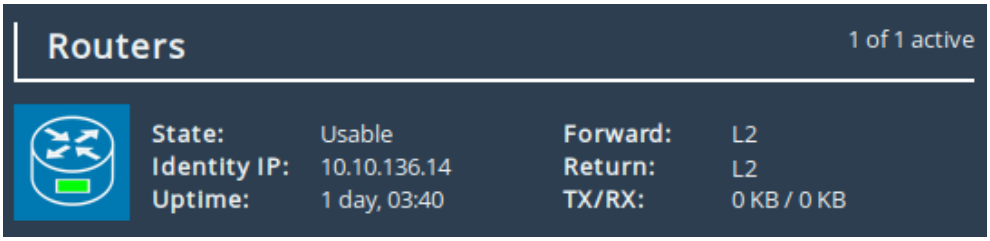
Return Method Negotiated return method across all routers.

TX Bytes Total bytes sent via WCCP redirection from this Node, for this service group.

RX Bytes Total bytes received via WCCP redirection to this Node, for this service group.

Active Paths The number of active and total paths to the specified routers.

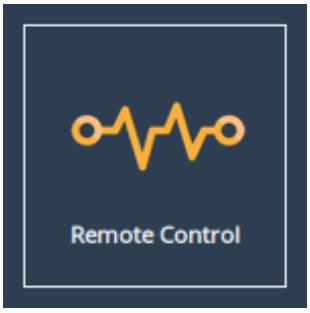
The *Routers* heading lists all known routers and an overview of their state.



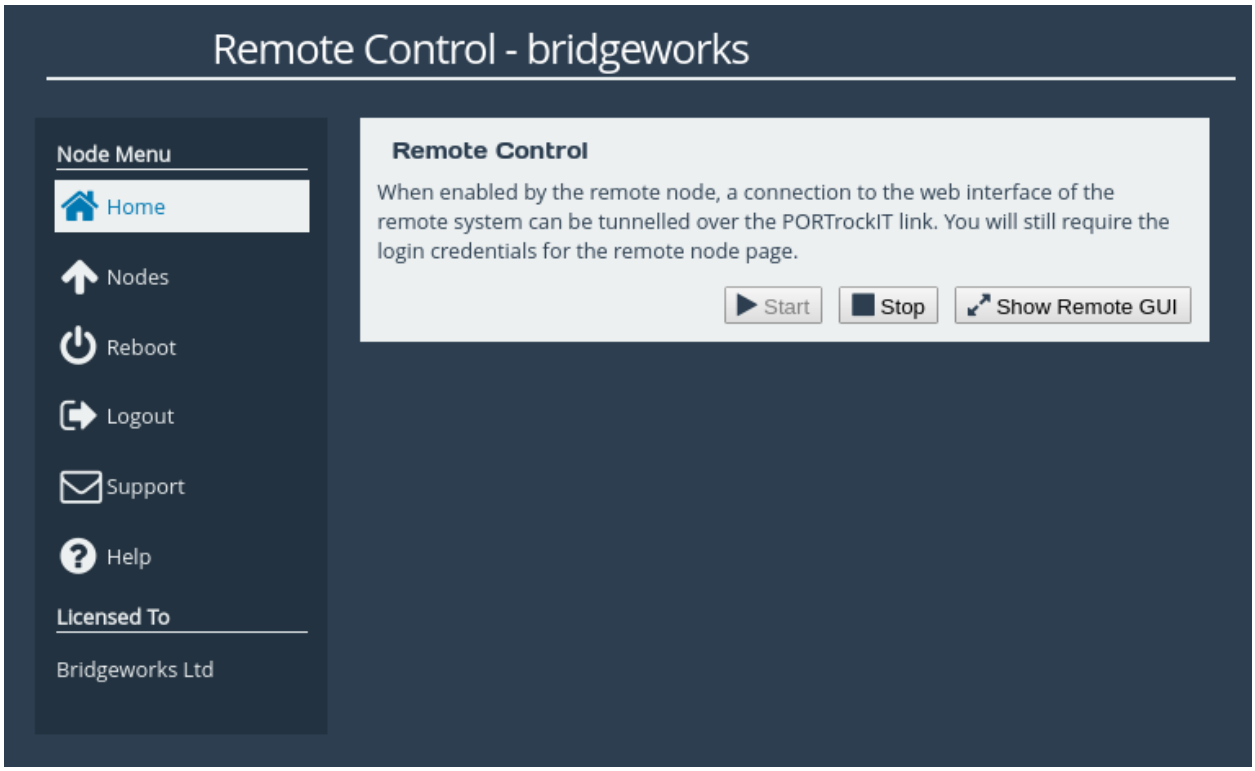
Remote Control

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.

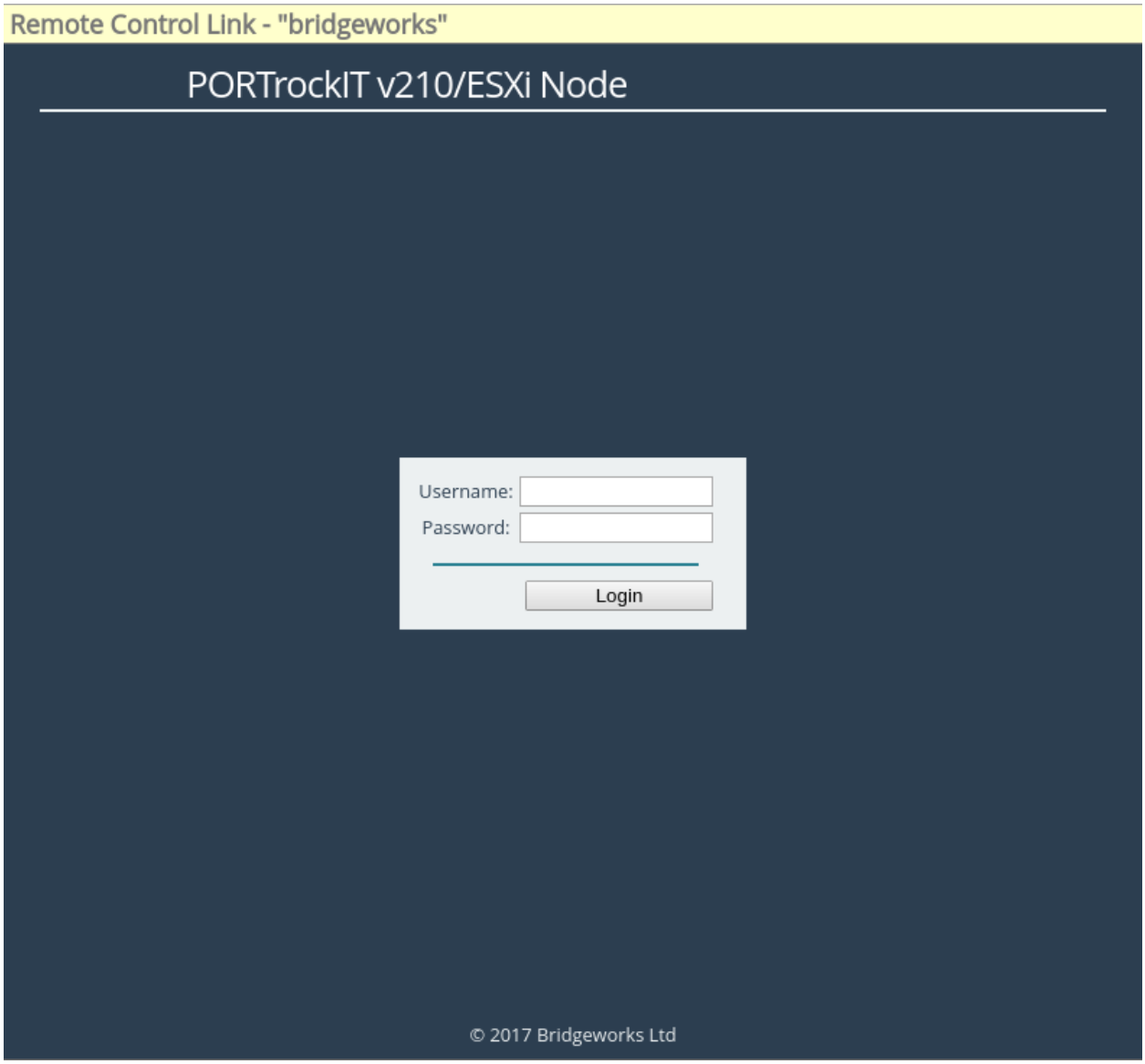


To enable remote control, click the *Start* button.



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.

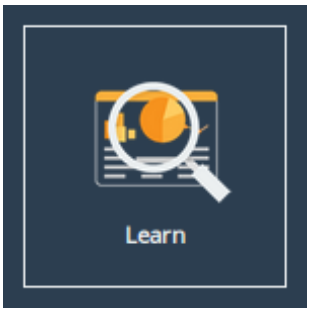


If you close the remote Node window with an HTTP connection, the session will continue to run. You may resume an HTTP remote session at any time by returning to the remote Node page and clicking the *Show Remote GUI* button. An HTTPS remote session to a Node will require reauthorisation if the session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

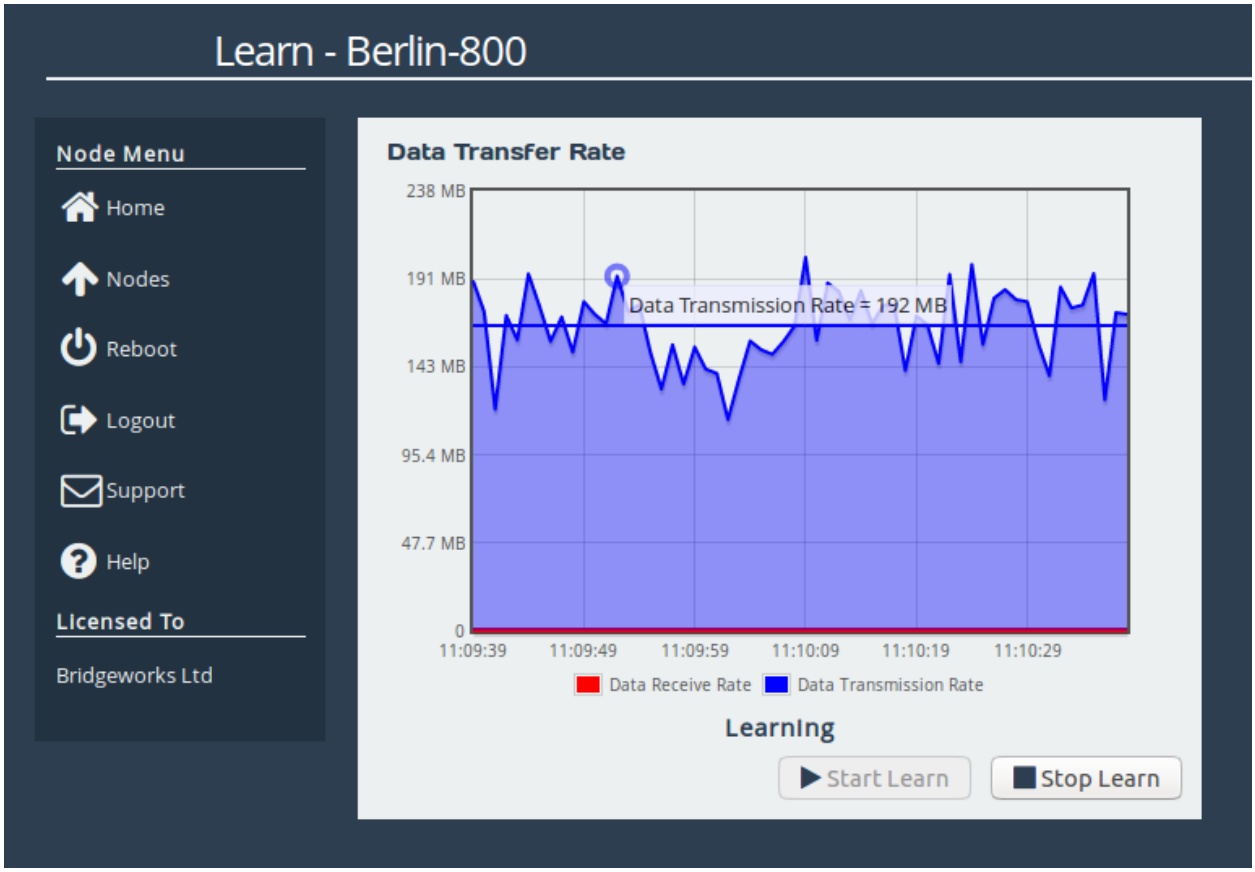
Learn

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:



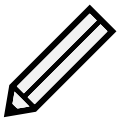
The learn process will take approximately five minutes. Navigating away from this page will not terminate the learn. The learn procedure can be run concurrently for multiple Nodes.

	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.

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 red.



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.

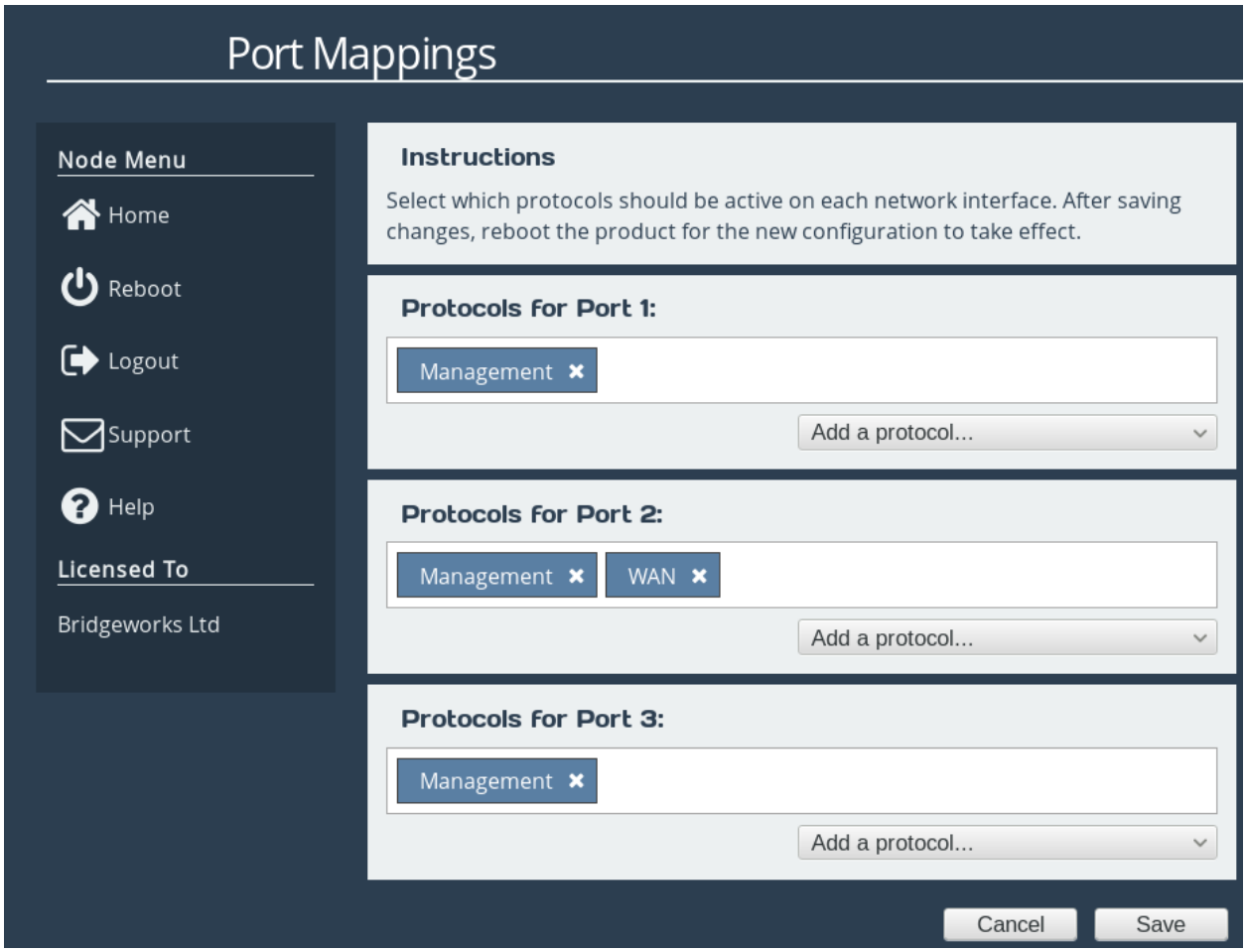
The solid, horizontal, blue and red lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

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

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:



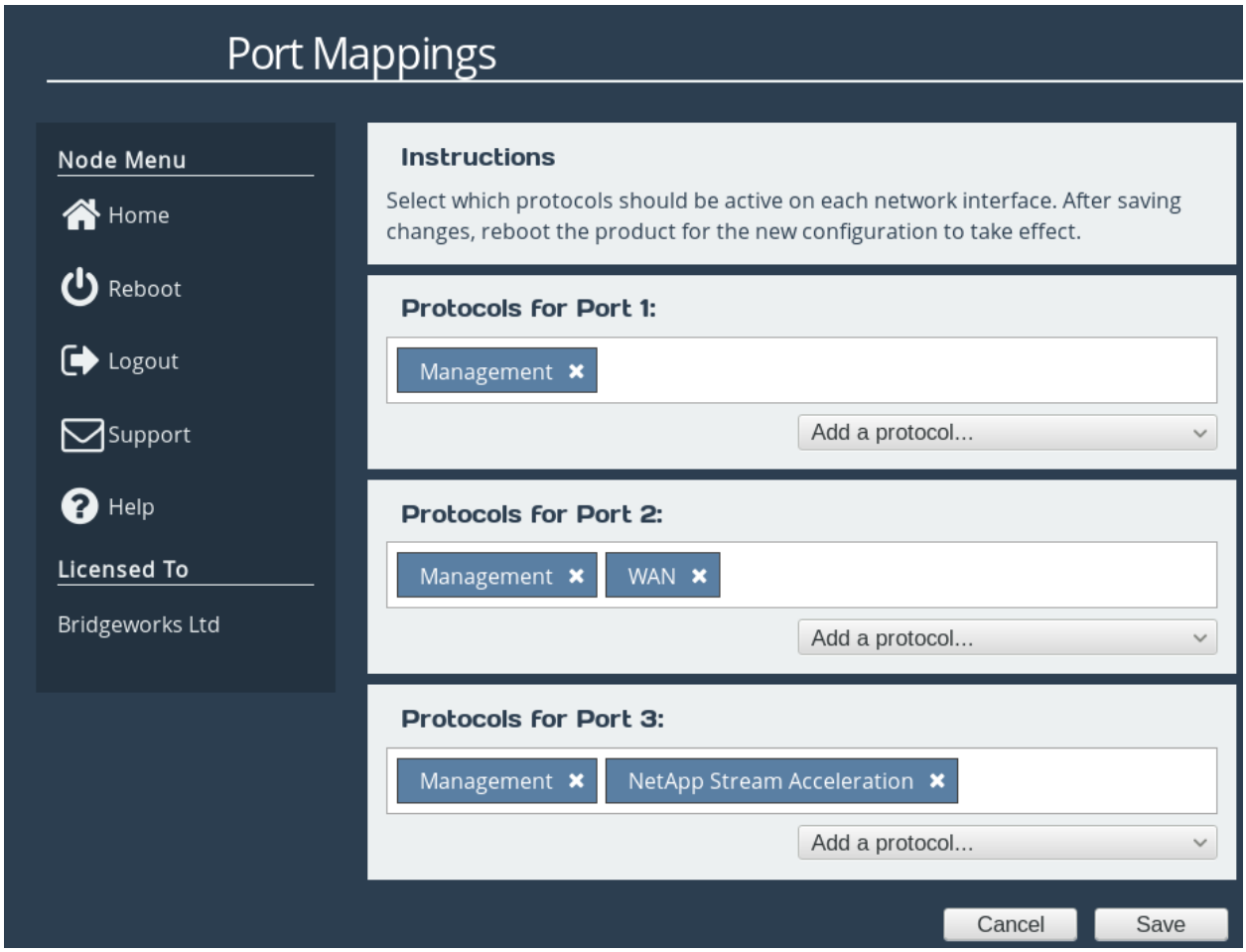
Hardware appliances have dedicated management ports, but can have the Management protocol assigned to additional ports.

Virtual instances will assign the Management protocol to all network ports on first load. The number of ports with the Management protocol assigned can be reduced, but at least one port must have it assigned.

Setting Port Mappings

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

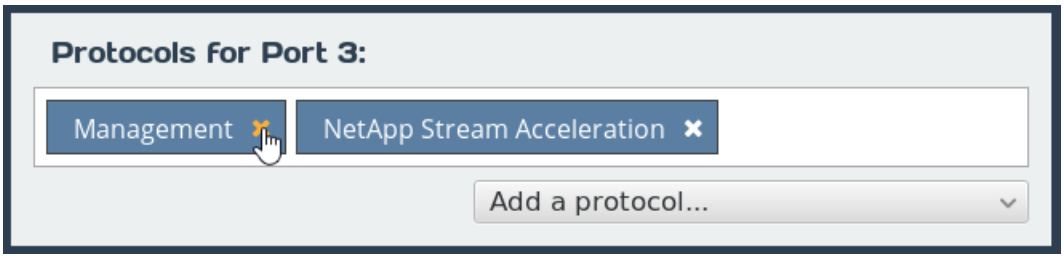
When a protocol has been applied to a port, a blue box corresponding to the protocol will appear under the port, as shown below.



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.

Removing a Port Mapping

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



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.

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 6.6: Licence Key Management for help managing and uploading new licence keys.

Hardware appliances will display a summary of licences in the *Licensed Adapters* table, as shown below.

Licensed Adapters

Feature Type	Limit	Assigned
Management	Unlimited	0
WAN 1 Gb	2	2

Virtual instances can have protocols applied to any port, however the number of unique protocols that can be applied is dependent on the product range. See Appendix C.2: Number of Unique Protocols for help determining the limit.

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:

	Important: Certain platforms have restrictions on available license mappings.

Caringo Swarm Object Storage
Accelerate a Caringo Swarm stream to, or from a remote Server.

Commvault VM Backup and Recovery
Accelerate a Commvault VM Backup stream to, or from a remote Server.

IBM Spectrum Protect
Accelerate traffic between IBM Spectrum Protect backup-archive clients and IBM Spectrum Protect servers.

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

NetApp Stream Acceleration
Accelerate a NetApp SnapMirror backup stream to a remote database.

Veeam Backup & Replication
Accelerate a Veeam Backup & Replication stream to, or from a remote Server.

Veritas NetBackup
Accelerate a Veritas NetBackup stream to, or from a remote Server.

WAN
The WAN port mapping is required for accelerating data to a remote target.

WANdisco Fusion
Accelerate a WANdisco Fusion stream to, and from other WANdisco Fusion clusters.

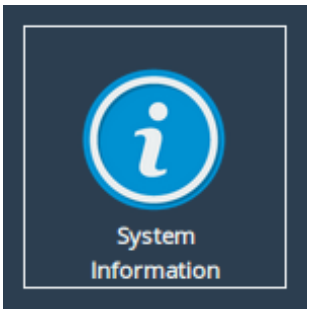
Important: If intending to configure a PORTrockIT protocol in the *Bridged In-Path* topology, two separate ports will be required; one with the PORTrockIT protocol mapped and the other with WAN mapped.

Node Maintenance

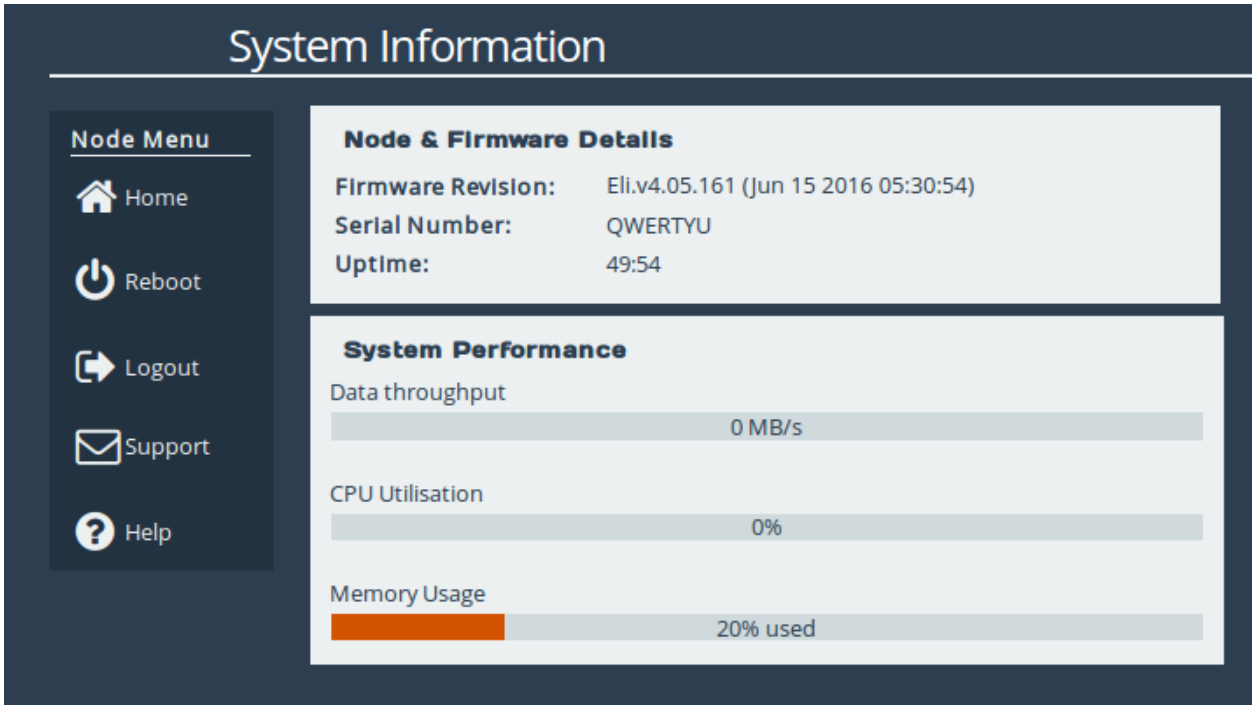
The following section describes the various pages that are available to the administrator to monitor performance and maintain the Node.

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 PORTrockIT Node.

Uptime is the amount of time the PORTrockIT 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.

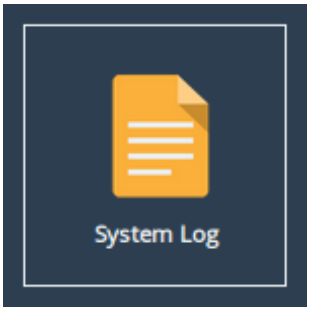
CPU Utilisation This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces.

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

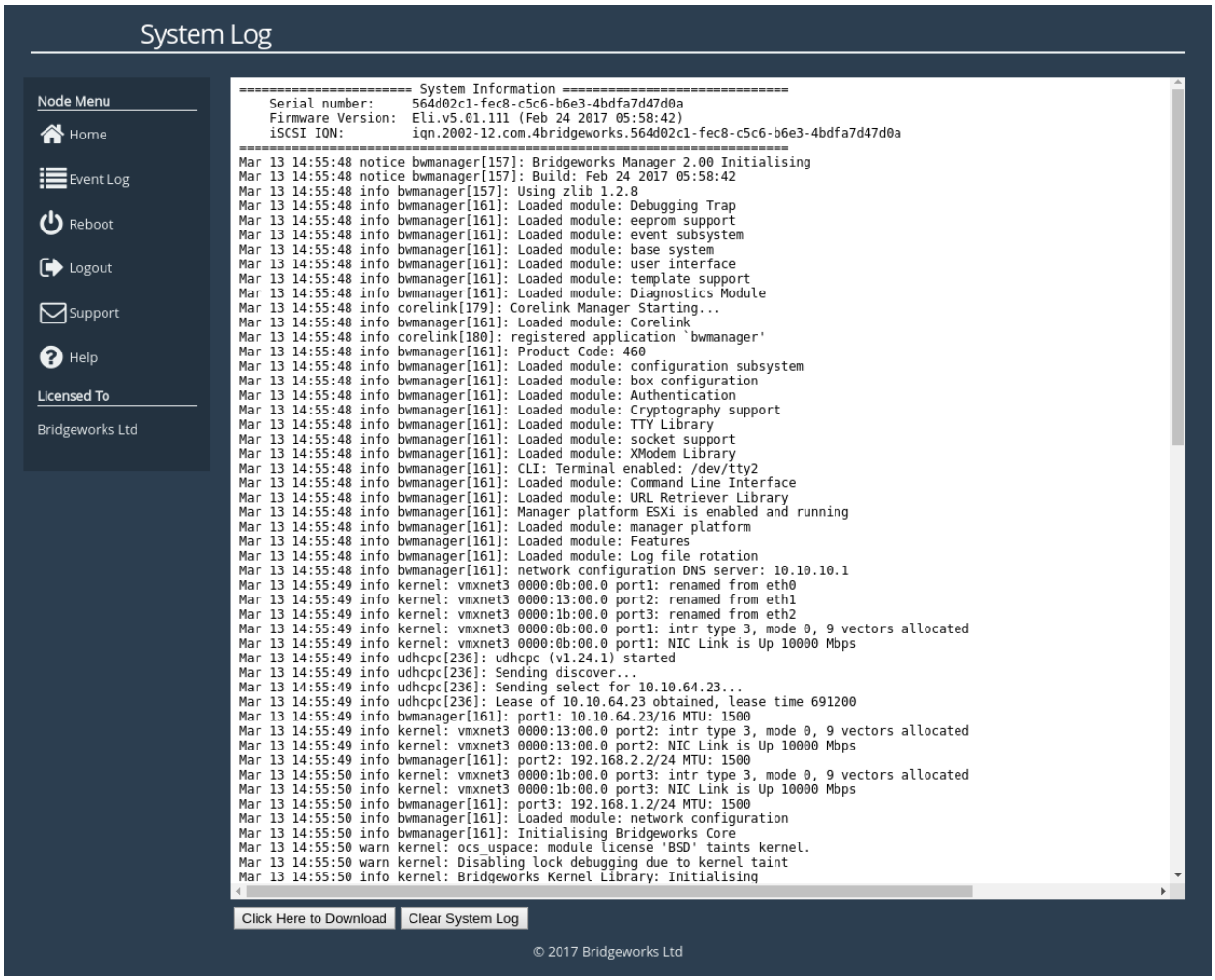
System Log

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 7: Troubleshooting.

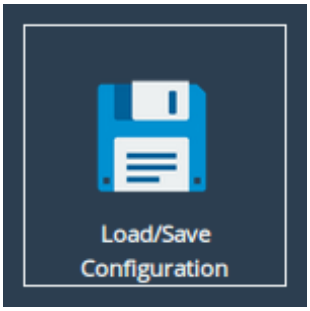
Load/Save Configuration

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

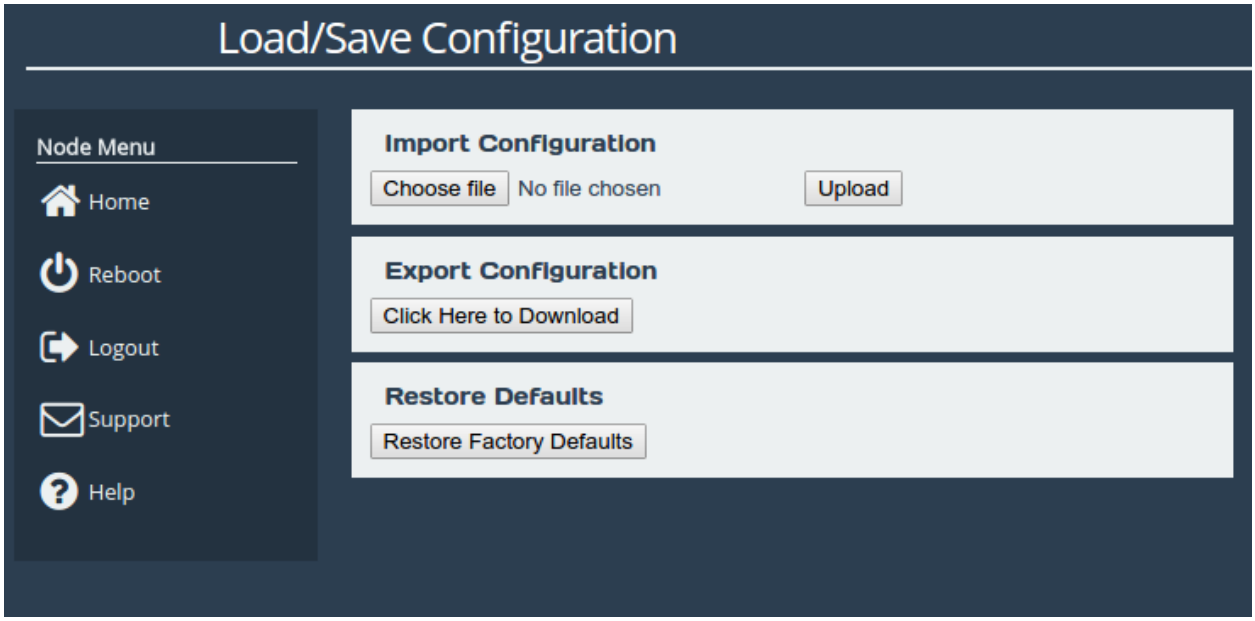
The configuration Load/Save feature allows you to save a copy of the Node's configuration to a file and optionally restore back to that configuration at a later time.

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:



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.

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.

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.

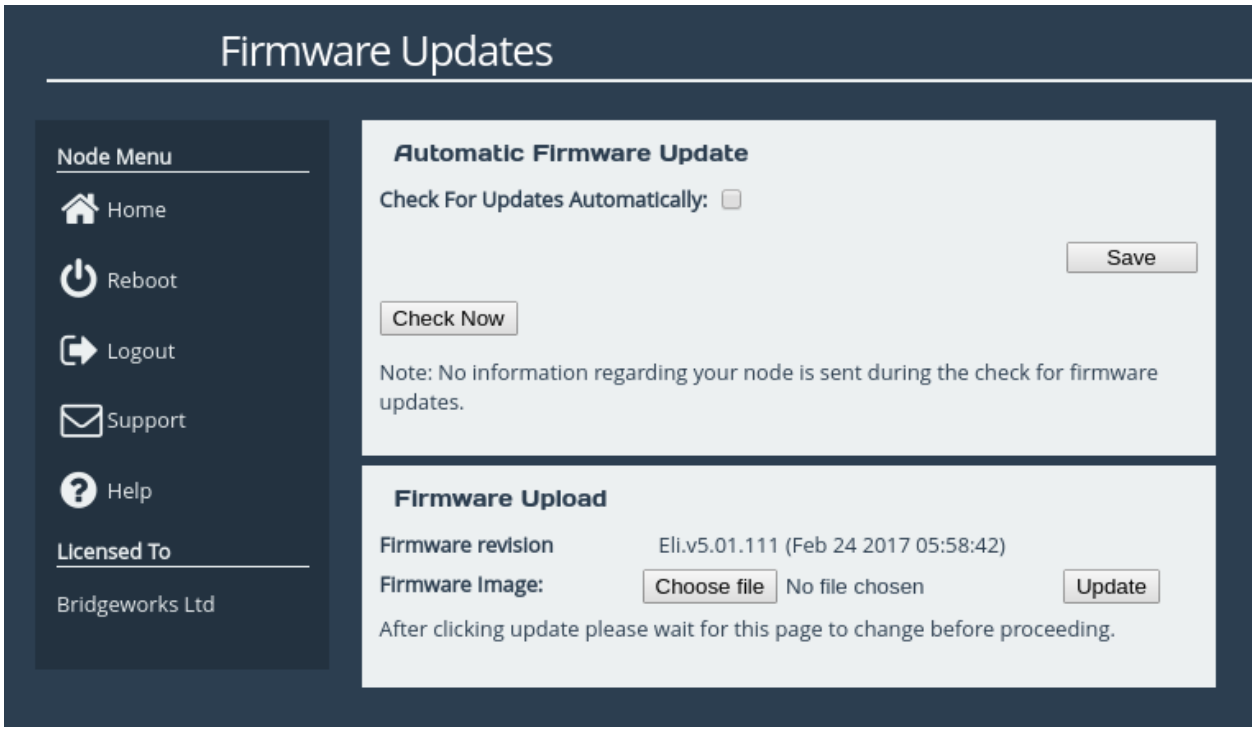
	Important: After clicking the *Restore Factory Defaults* button, a reboot will automatically occur.

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:

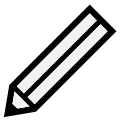


You can now instruct the Node to check for new firmware versions, alerting you when a new version is available and providing a button to perform the update. Alternatively, you can manually upload and update to a firmware version of your choosing.

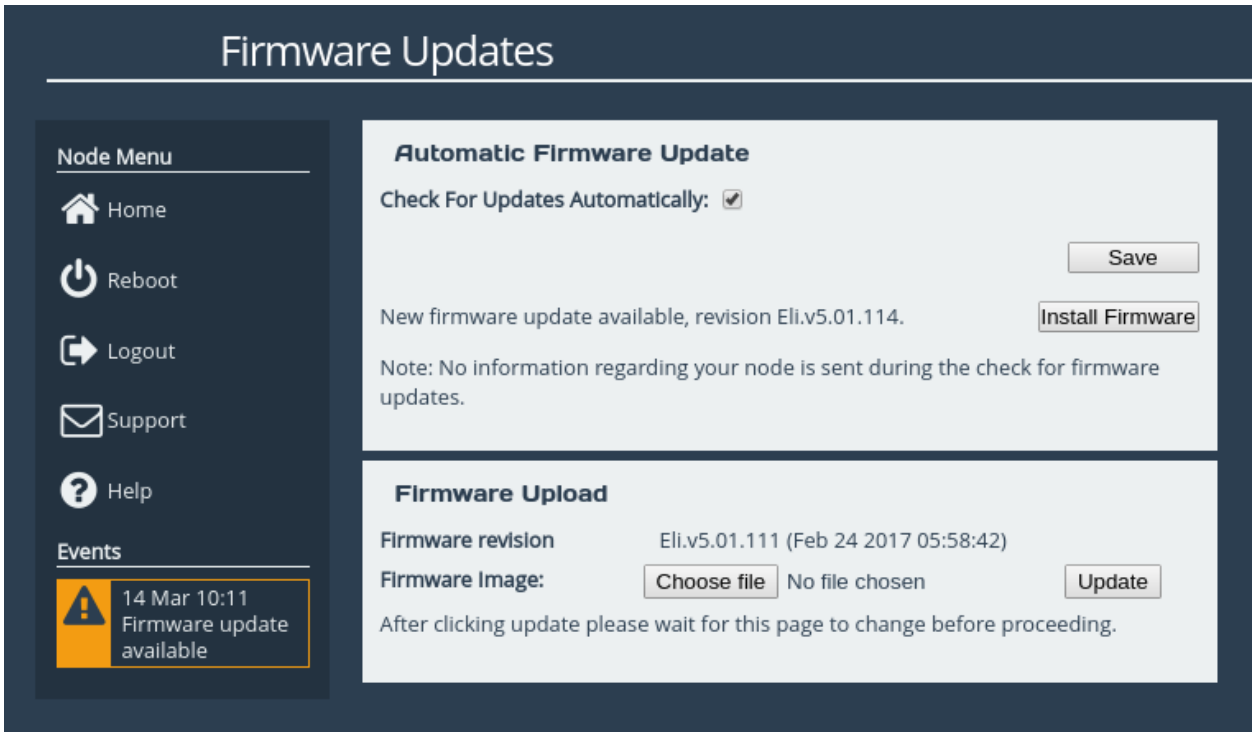
Automatic Firmware Update Checking

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 PORTrockIT 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.

Updating Firmware Manually

	Important: Manual firmware updating is unavailable on Cloud nodes.

It is also possible to download new firmware versions and update manually. Firmwares are downloadable from the Bridgeworks website at:

https://support.4bridgeworks.com/download-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 E: 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 PORTrockIT 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.

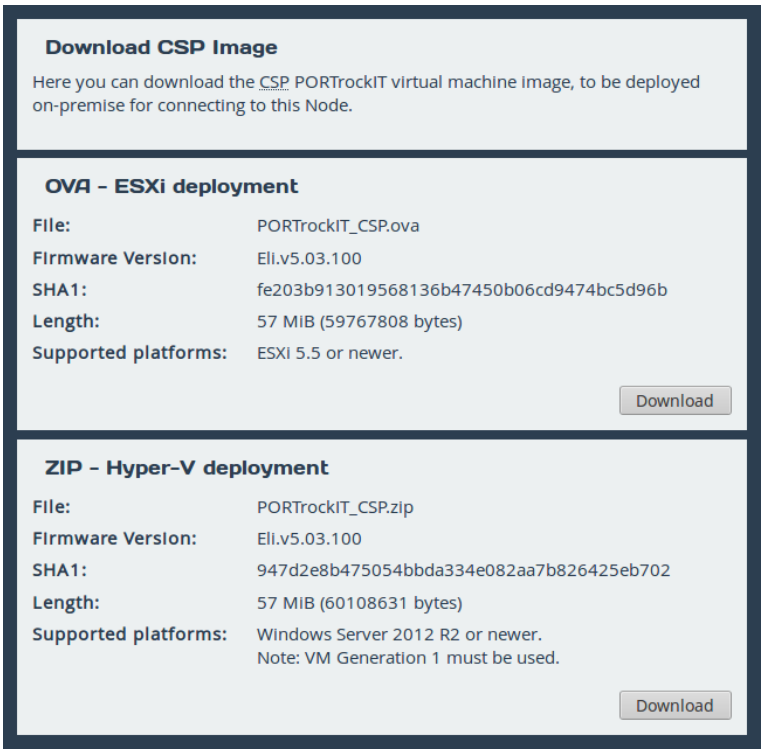
Download CSP Image

	Important: The CSP download is only available on Cloud Nodes.

This page contains the download links for the Cloud Service Provider (CSP) on platforms supported by the firmware. The CSP Node is included with the purchase of a Cloud Node which can be deployed on-premise and connected to a Cloud Node to accelerate traffic to and from the Cloud.

From the Home screen, select the *Download CSP Image* icon from the *Node Maintenance* section.

The following page will be displayed:



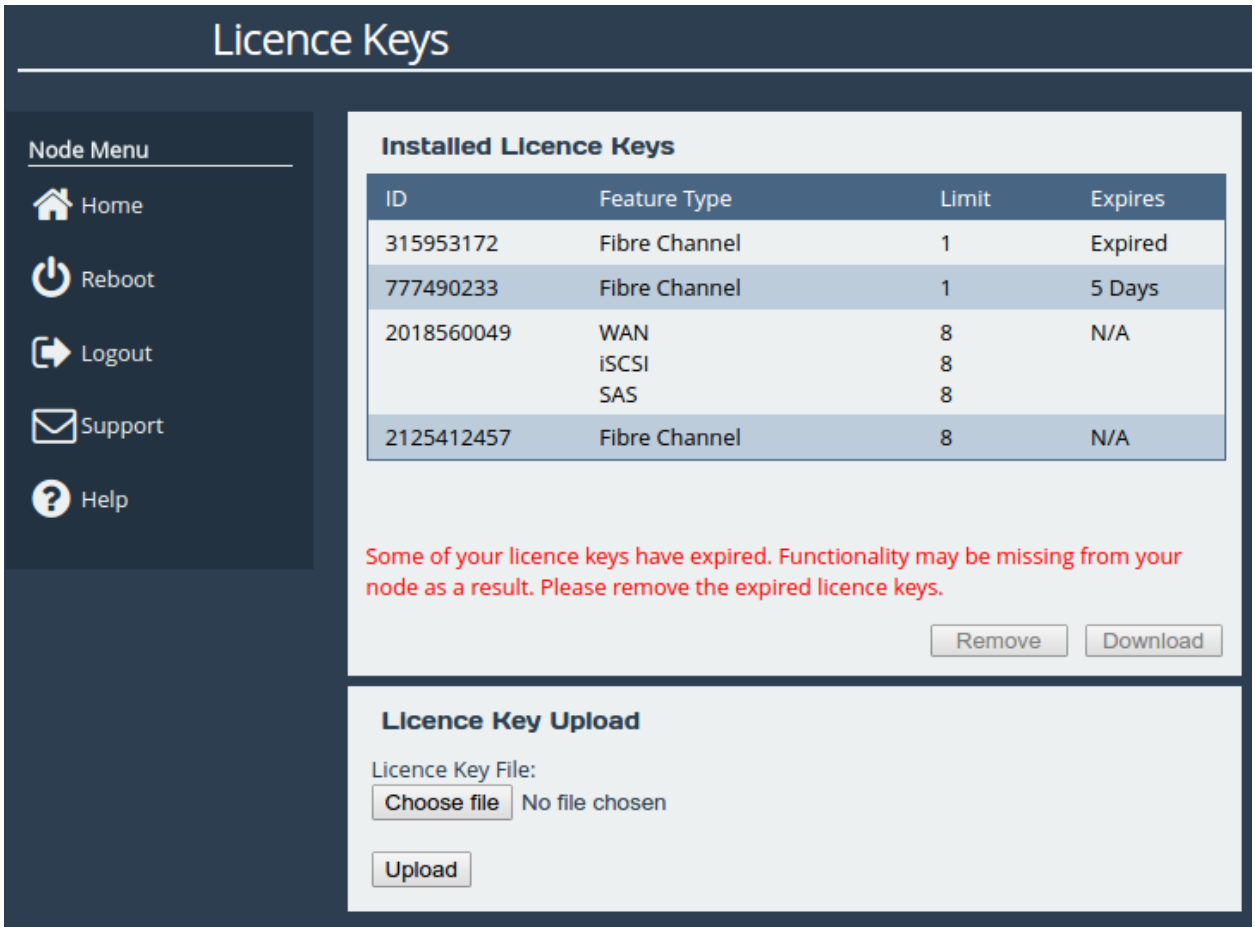
Click on the download link for your desired platform to download the CSP image.

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 5: 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:



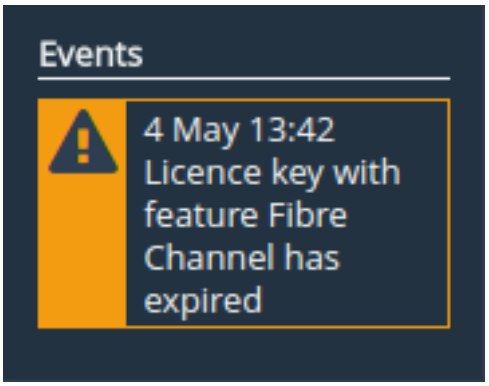
The *Installed Licence Keys* table displays the installed licence keys with the following information:

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.



Uploading a Licence Key

To upload a licence key:

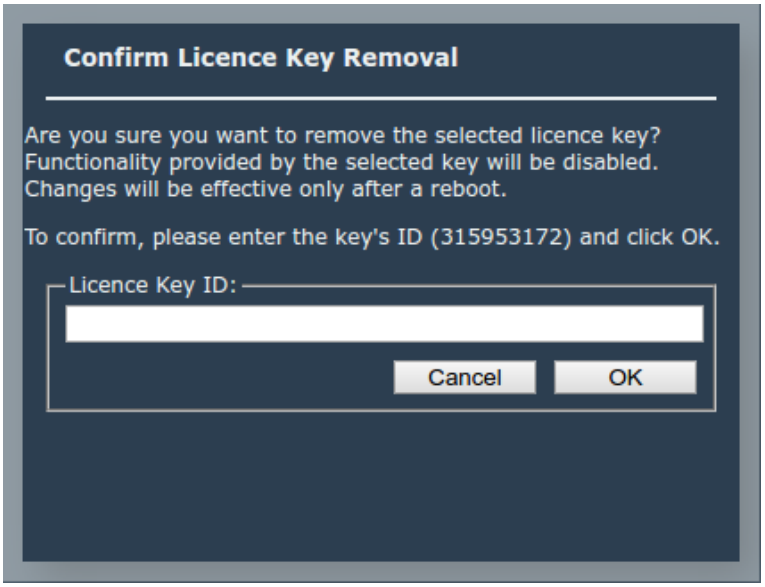
1. Click the *Choose file* button in the *Licence Key Upload* section.
2. Locate and select the licence key to upload.
3. Click the *Upload* button.

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.

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.

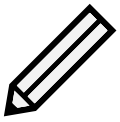
Downloading a Licence Key

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

Diagnostics

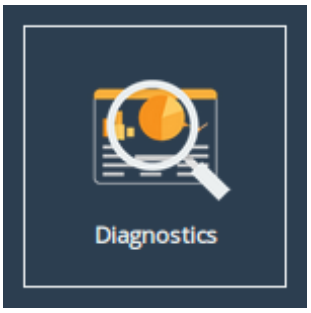
In the unlikely event that a problem arises with your PORTrockIT Node, you may be requested by Bridgeworks Support to provide a diagnostic file.

Important: If an issue arises with your PORTrockIT Node, check Chapter 7: Troubleshooting for information on how the issue may be resolved.

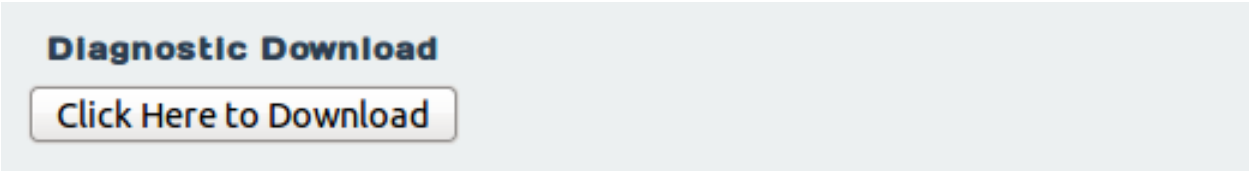


Note: The following instructions are demonstrated in the Bridgeworks Support Video "WANrockIT: Downloading Diagnostic Information" found at https://www.youtube.com/watch?v=8RZXFGCy3ZU.

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 PORTrockIT 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.

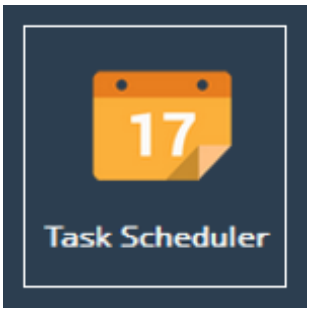
Task Scheduler

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

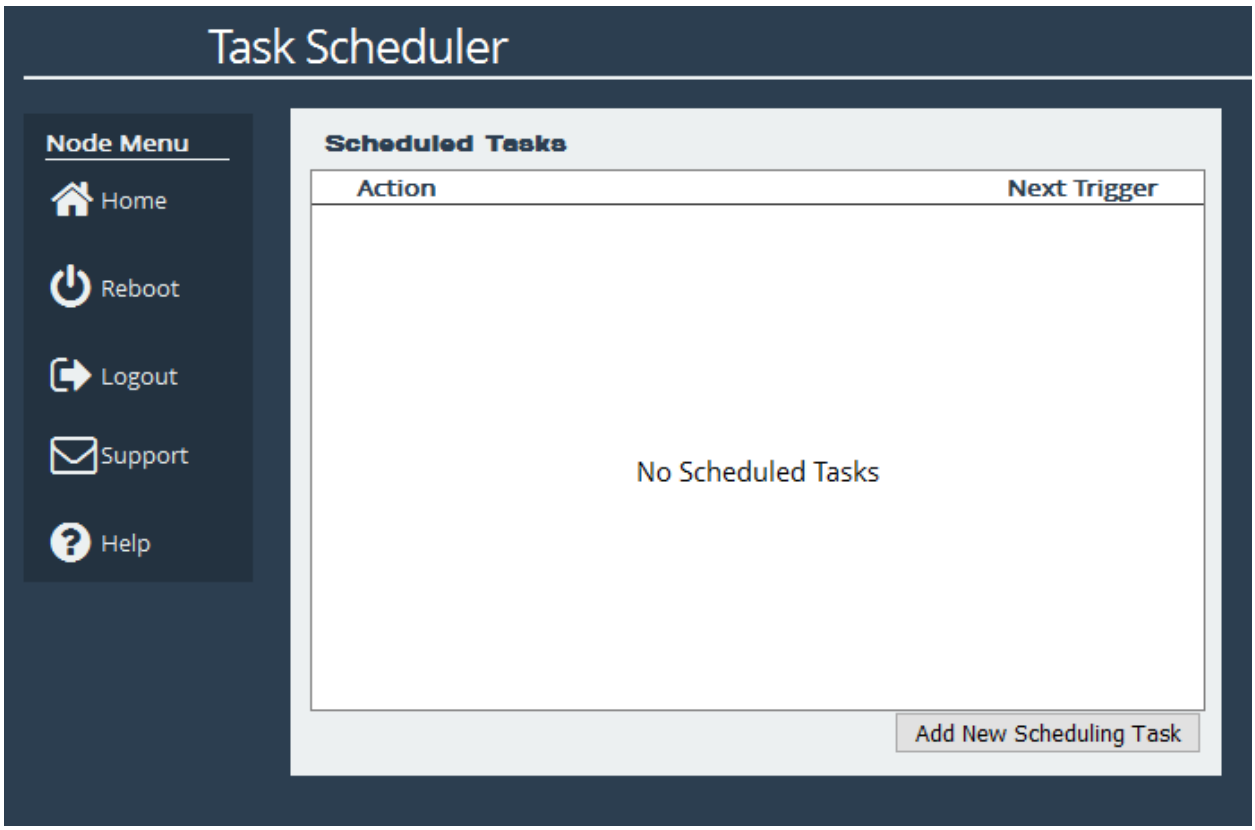
Email Performance Statistics This will email the log of the throughput rate to a given email address(es).

PORTrockIT Bandwidth Limit This will restrict the PORTrockIT 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:

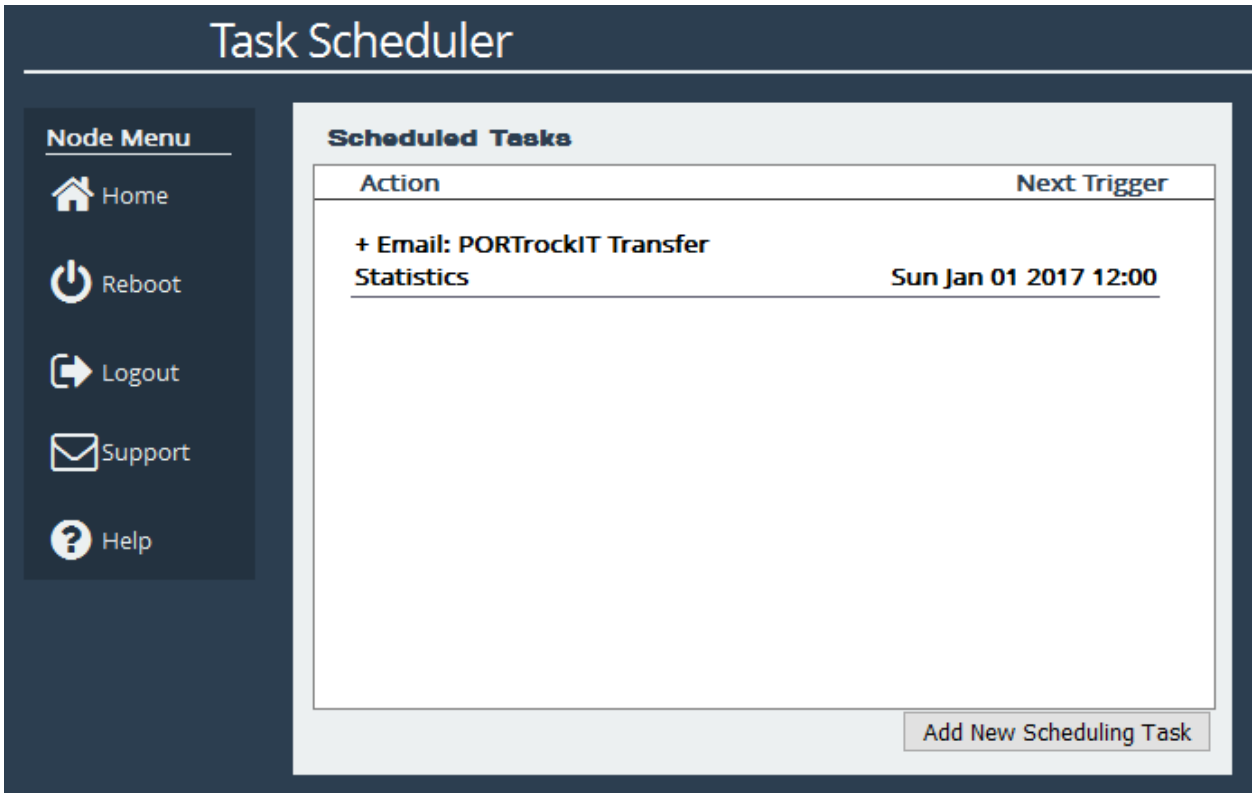


Adding Tasks

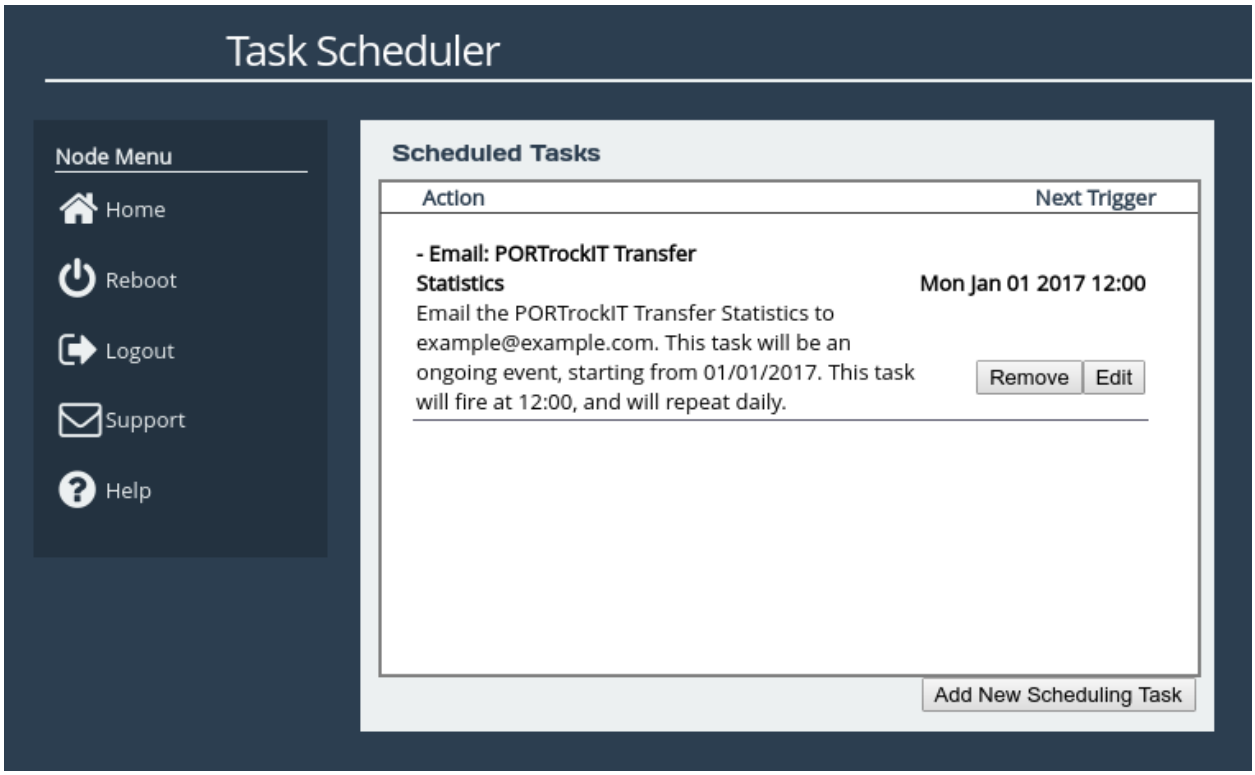
Tasks can be added by clicking on the *Add New Scheduling Task* button, which will start the task wizard.

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.

Task Wizard

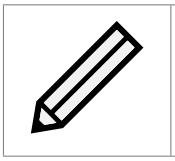
The task wizard will guide you through the adding or editing of scheduled tasks. There are a few common buttons across the individual sections of the wizard:

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.

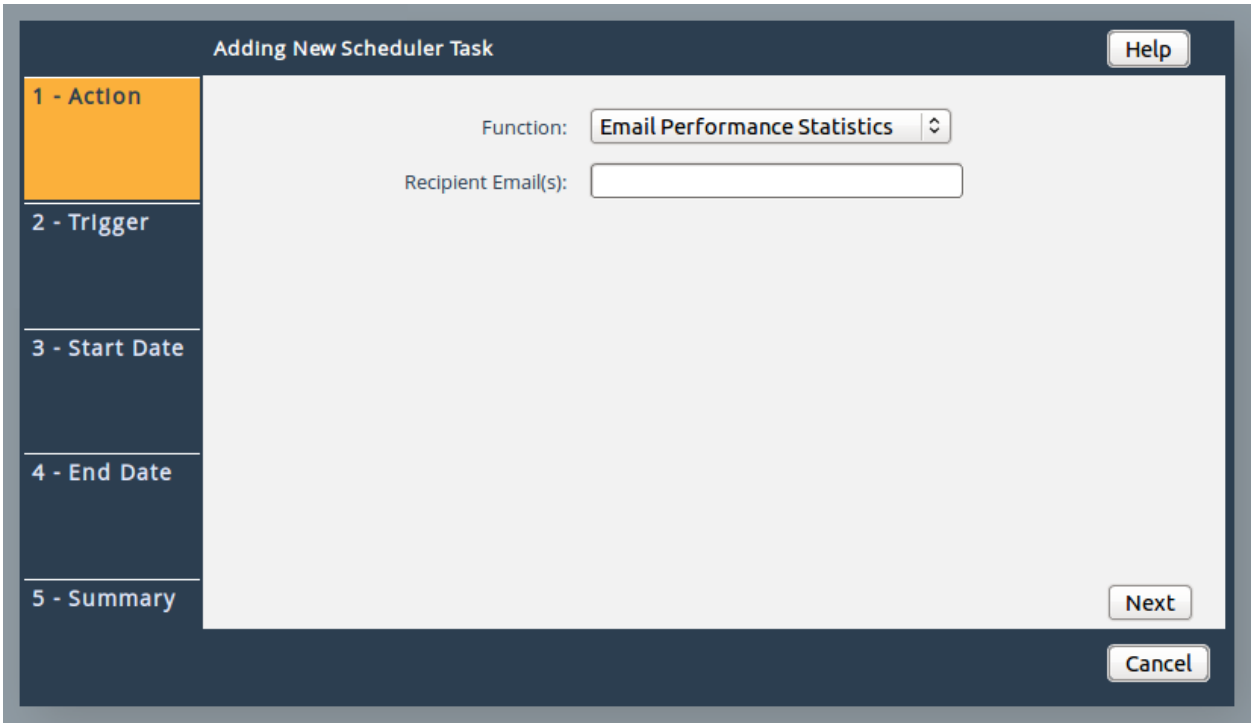
Next If present, this button will navigate you to the next section of the wizard.

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



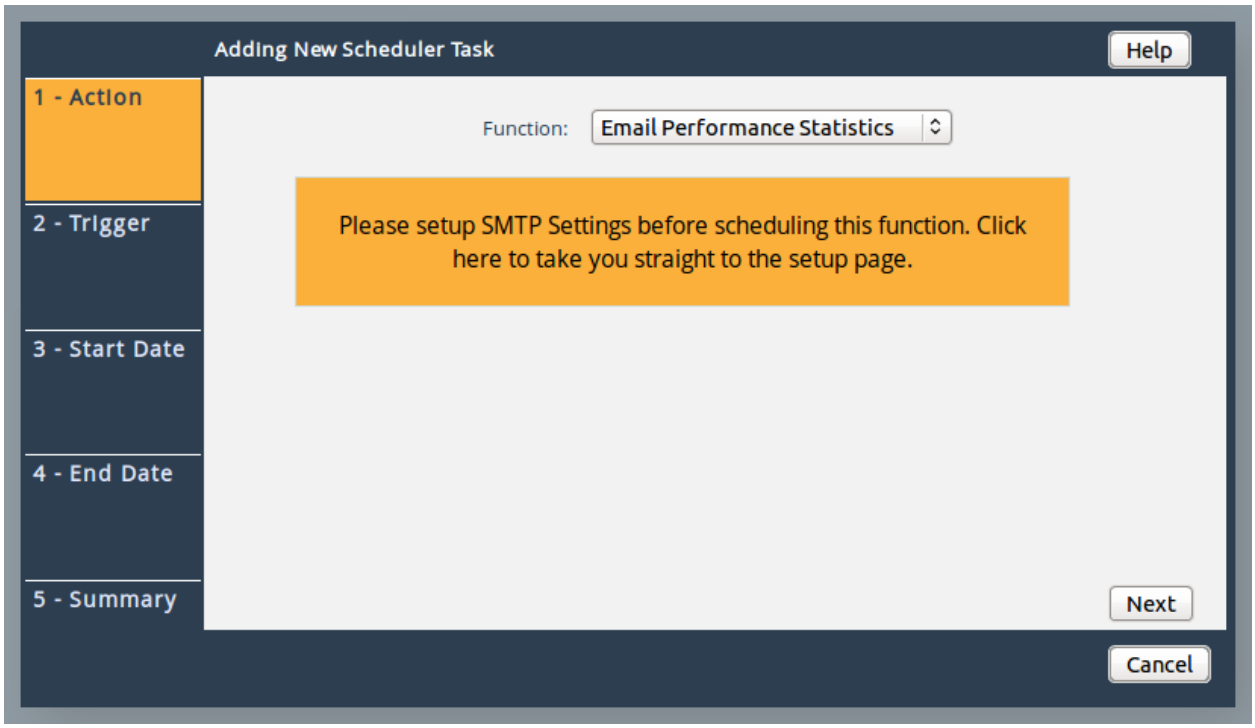
Note: The currently active section of the wizard will be highlighted in orange on the left-hand side.

Action - Email Performance Statistics

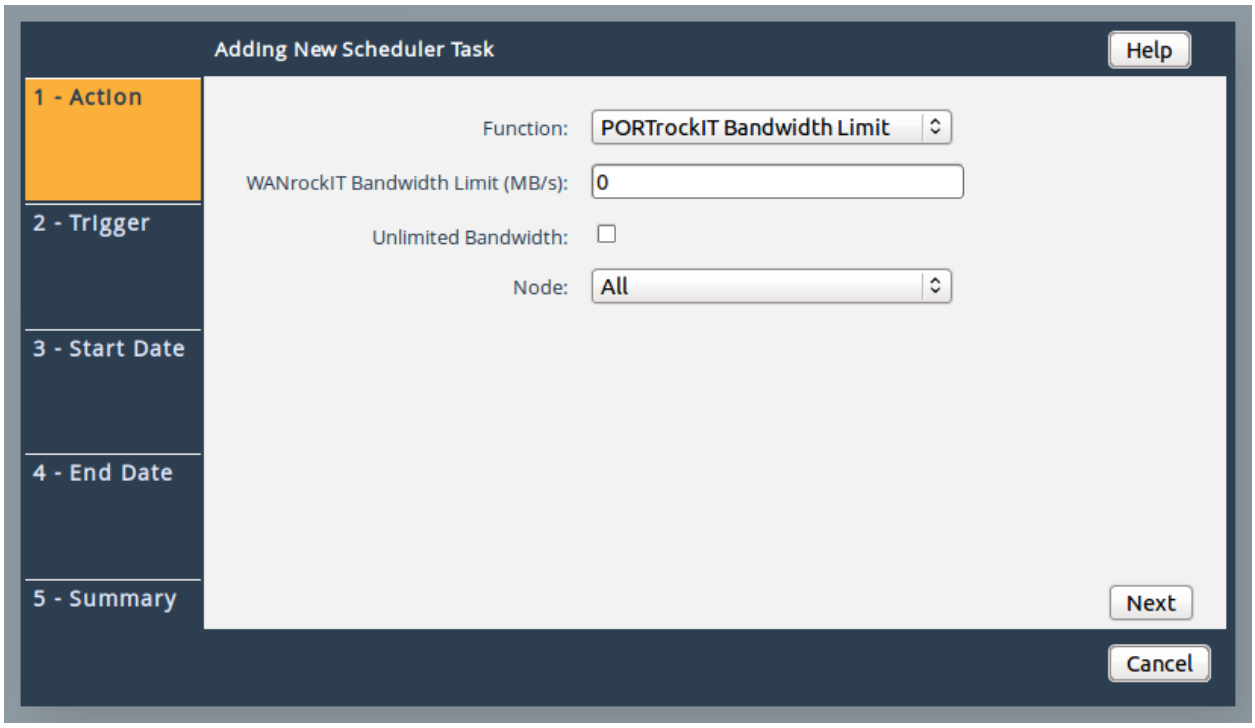


On the Action section of the wizard, enter the recipient email(s), separating multiple emails with either commas or semi-colons.

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 3.3.5: Simple Mail Transfer Protocol (SMTP).

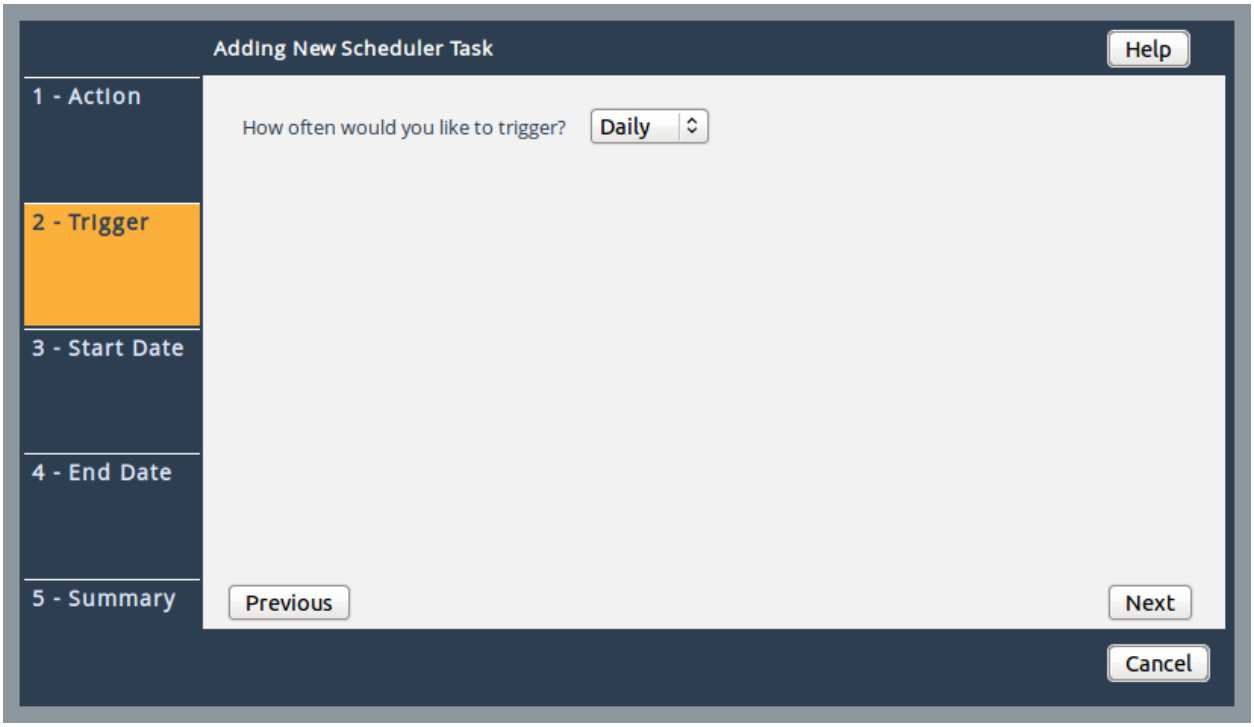


Action - PORTrockIT Bandwidth Limit



On the Action section of the wizard, enter a bandwidth limit in Megabytes per second or select the *Unlimited Bandwidth* checkbox. Then select which Node should be affected by the bandwidth limit.

Trigger

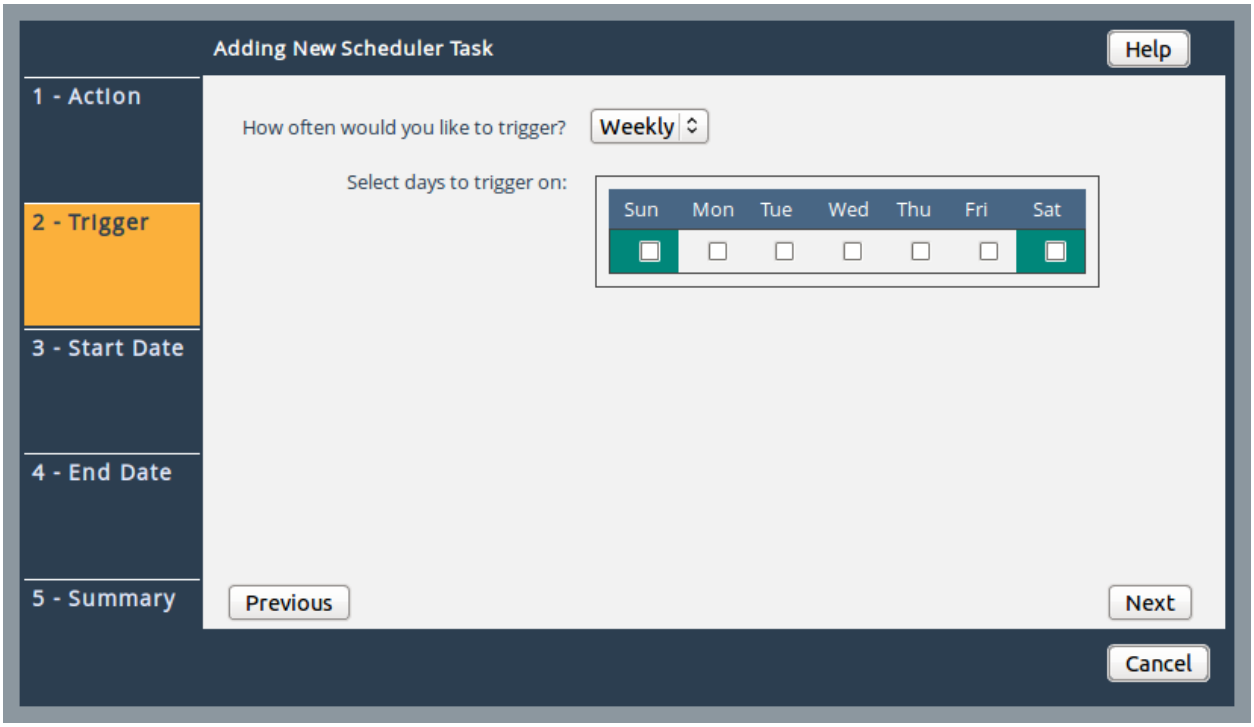


On the Trigger section of the wizard, you can pick the frequency of the event. The options are:

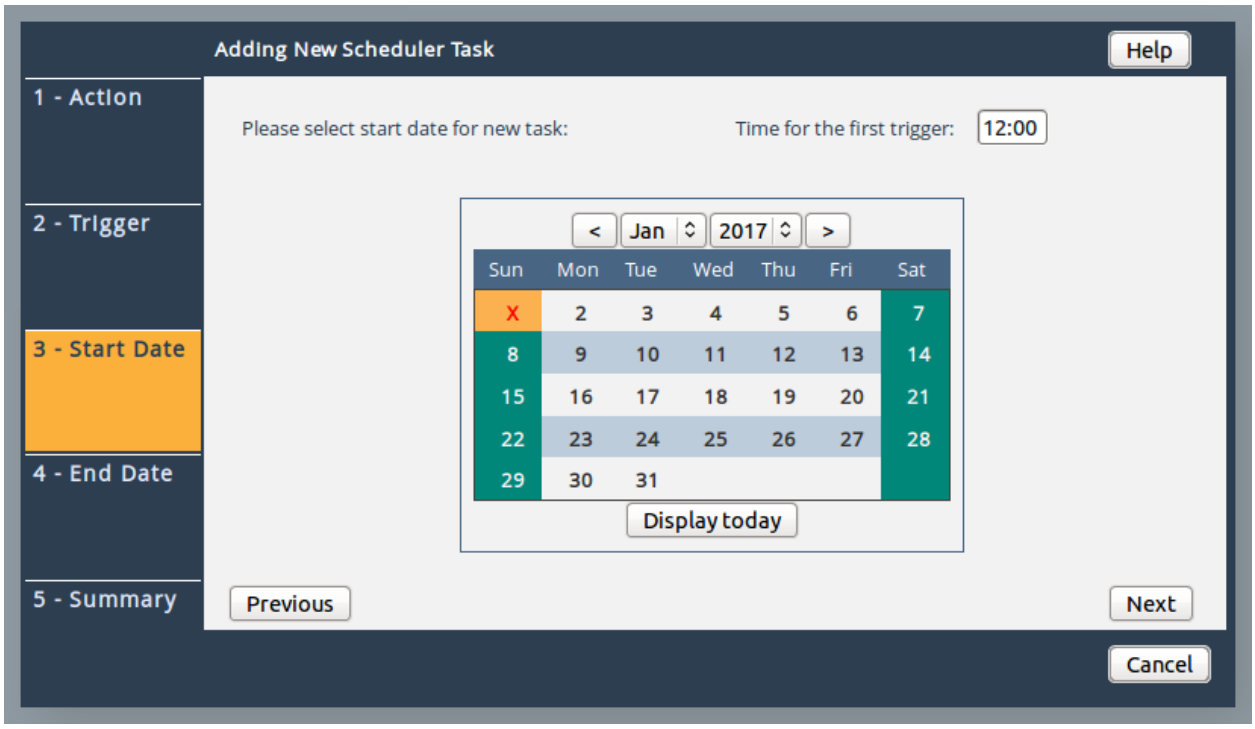
Once This means the action will be performed at the specified time and not repeat.

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:

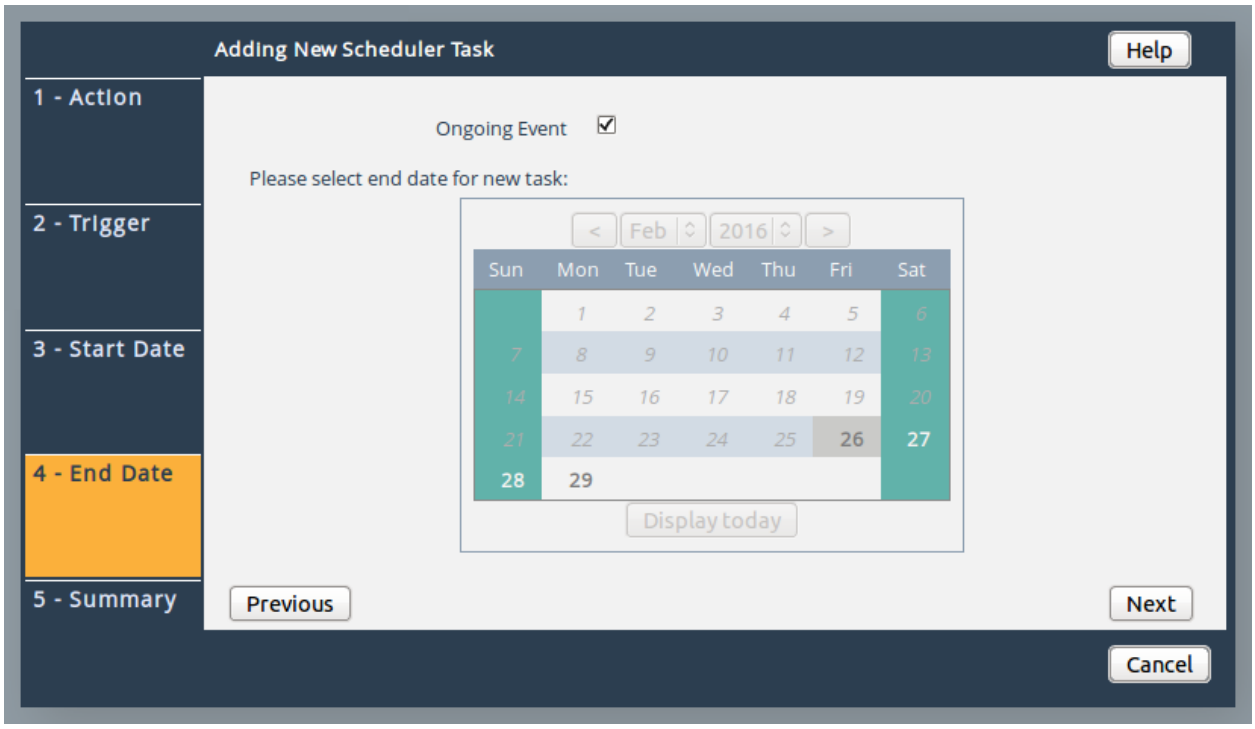


Start Date



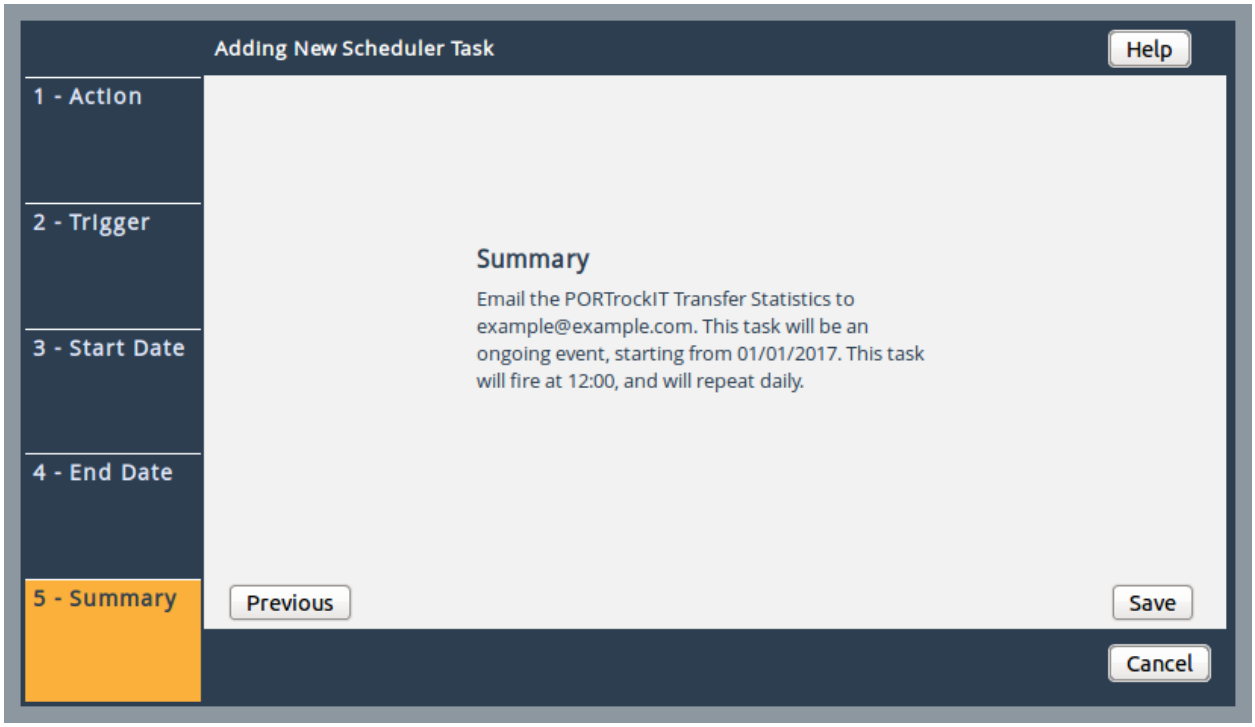
On the Start Date section of the wizard, you can pick the starting date and time for the new task. Enter a time into the *Time for the first trigger* box and select your start date using the calendar. The selected date will be marked with a red cross.

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.

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.

Troubleshooting

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.
- Scan the network using the *LAN Scan* utility to find all the Node’s connected to the network in case the network address is different than what was expected. See the LAN Scan guide found on the CD accompanying your PORTrockIT Node for more information.

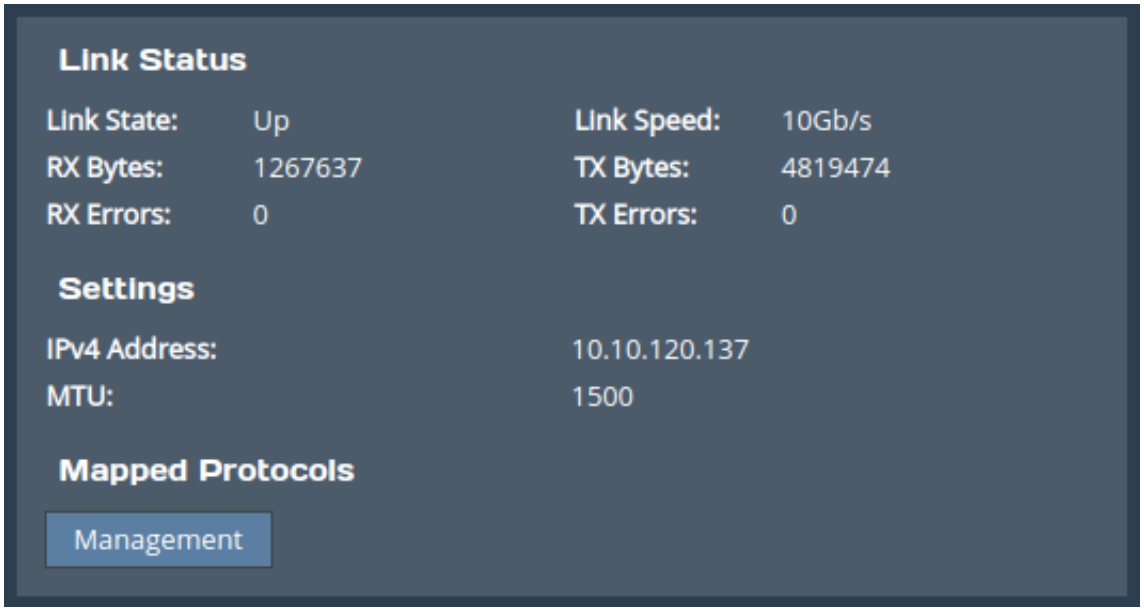
If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix E: Useful Links for information on how to contact Bridgeworks Support.

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 3.1.7: Port Settings for help finding the *Network Port* page.

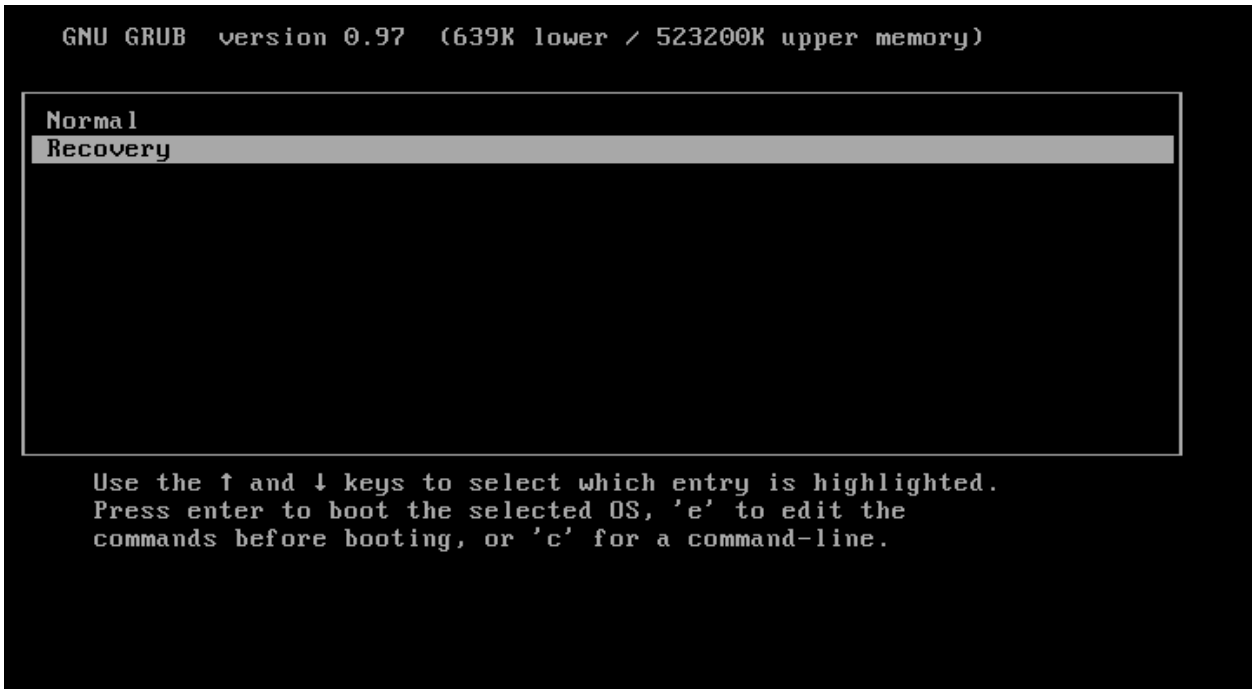


If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix E: Useful Links for information on how to contact Bridgeworks Support.

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 while the unit is booting. Select the *Recovery* option on the menu provided.

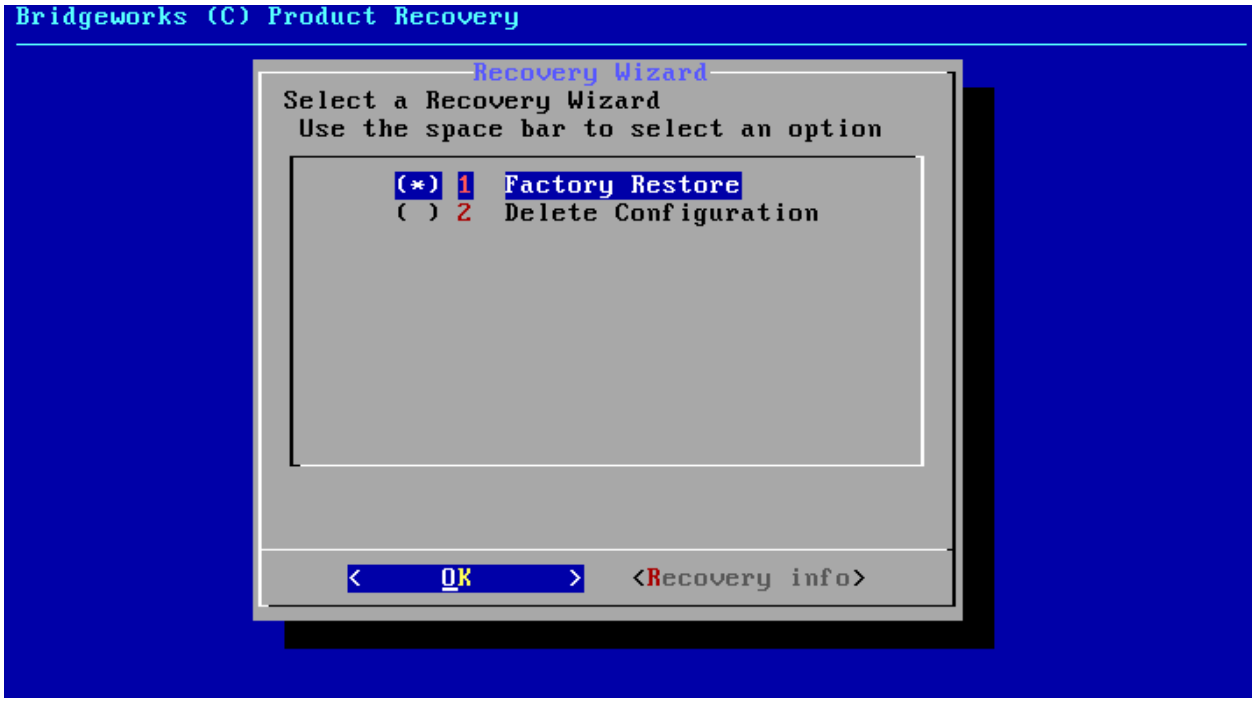


The Recovery Wizard provides two options for system recovery: restoring your unit to factory defaults, and deleting your configuration file.

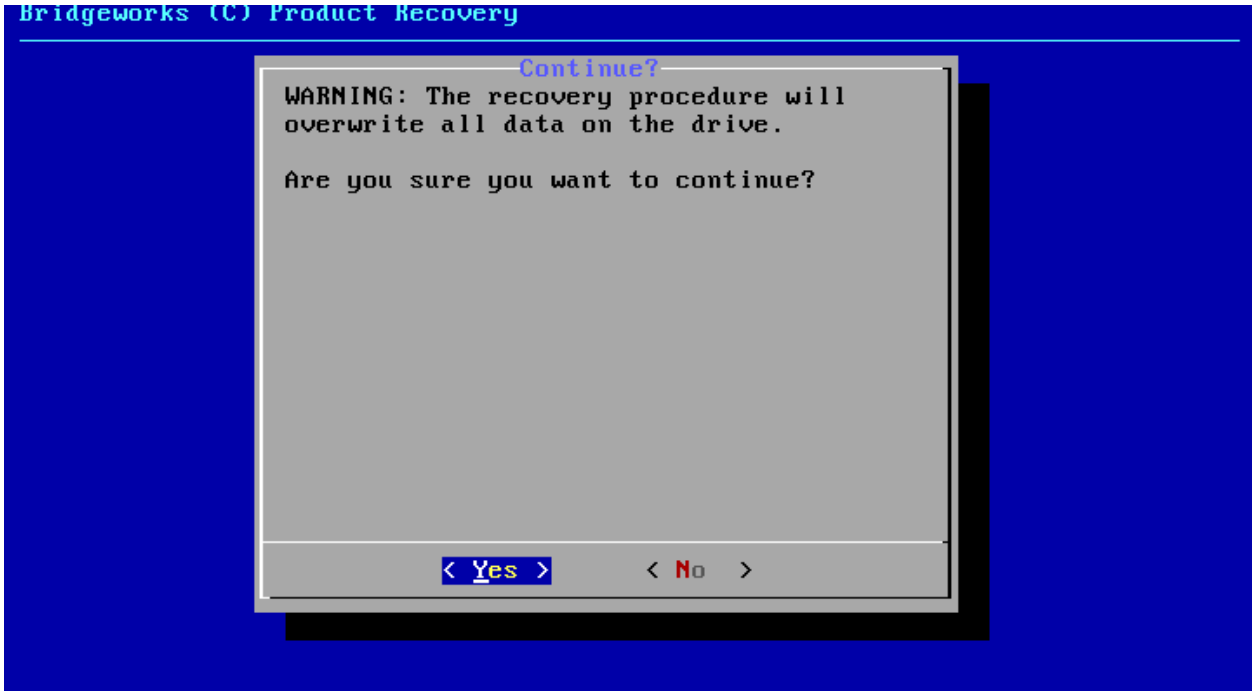
Factory Restore

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

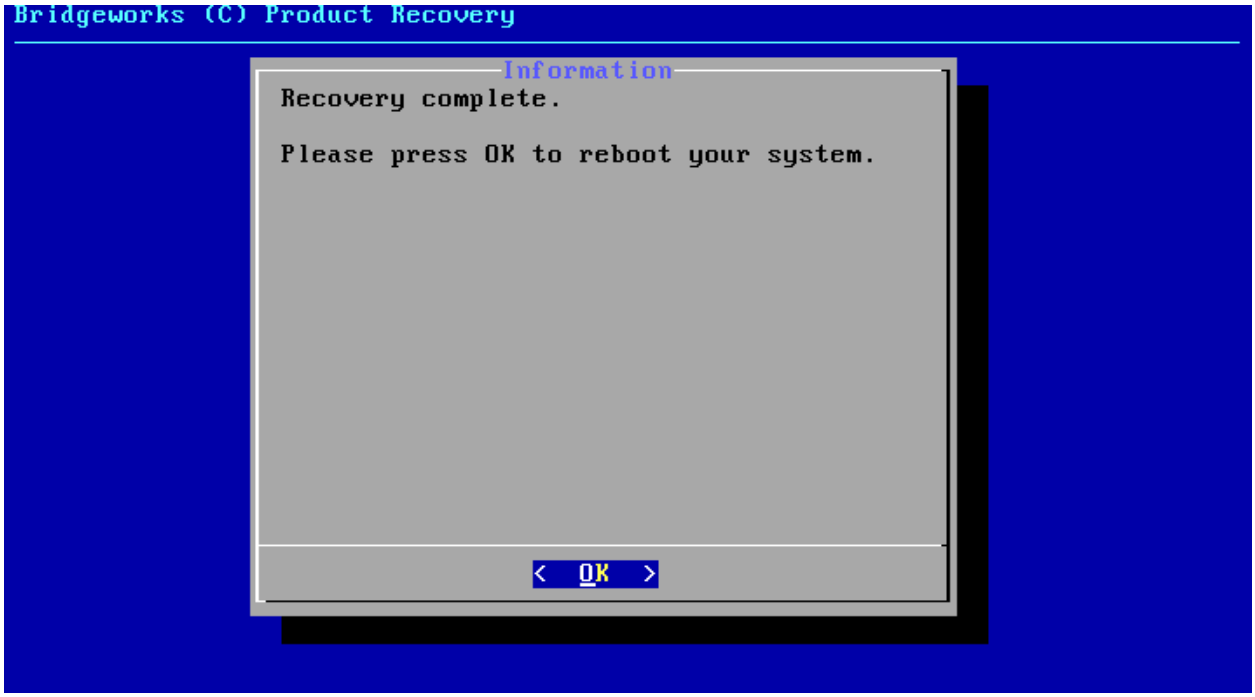
To restore your unit to defaults, ensure that the *Factory Restore* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the factory restore process.



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.



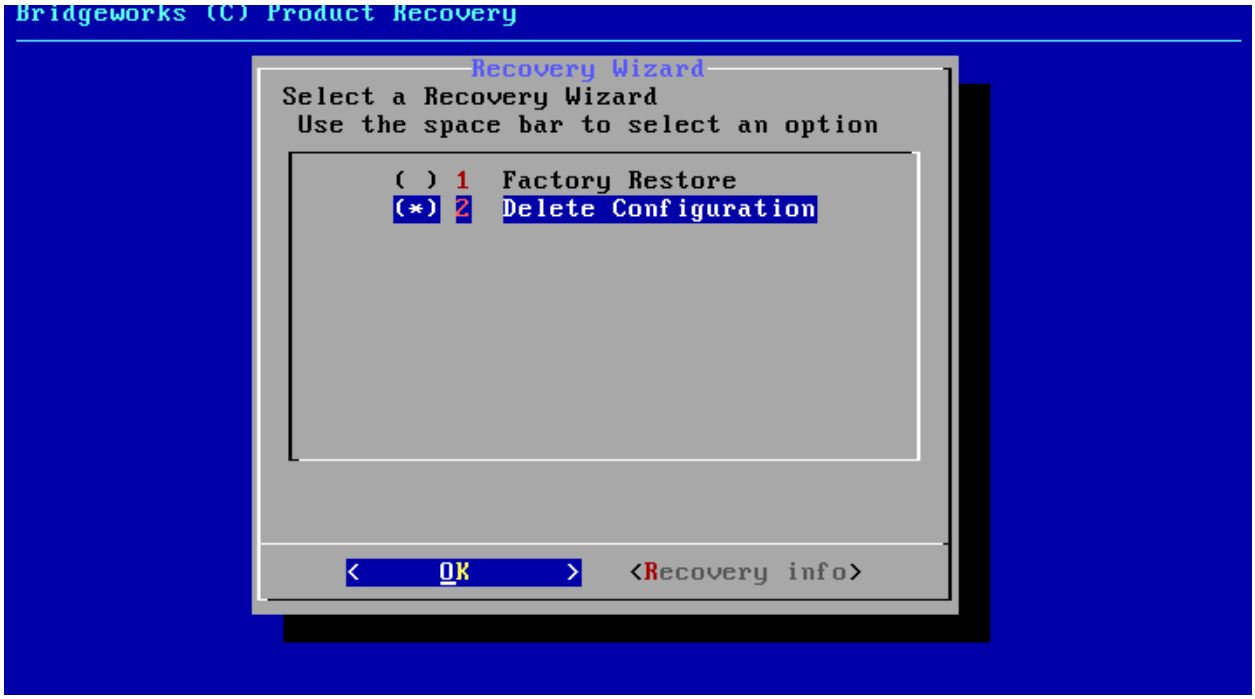
Once the factory restore procedure has completed successfully you will need to reboot your system.



Delete Configuration

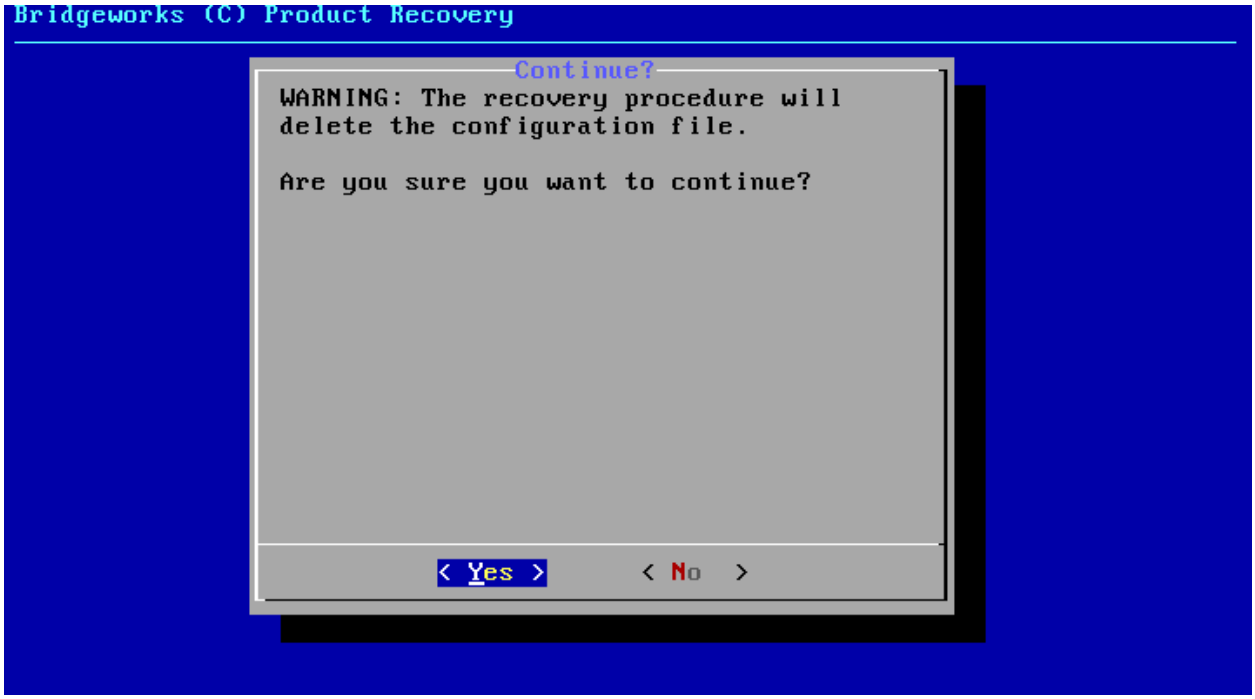
This option will delete your configuration file, removing any current configuration on your system but keeping your current firmware and licence keys.

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.

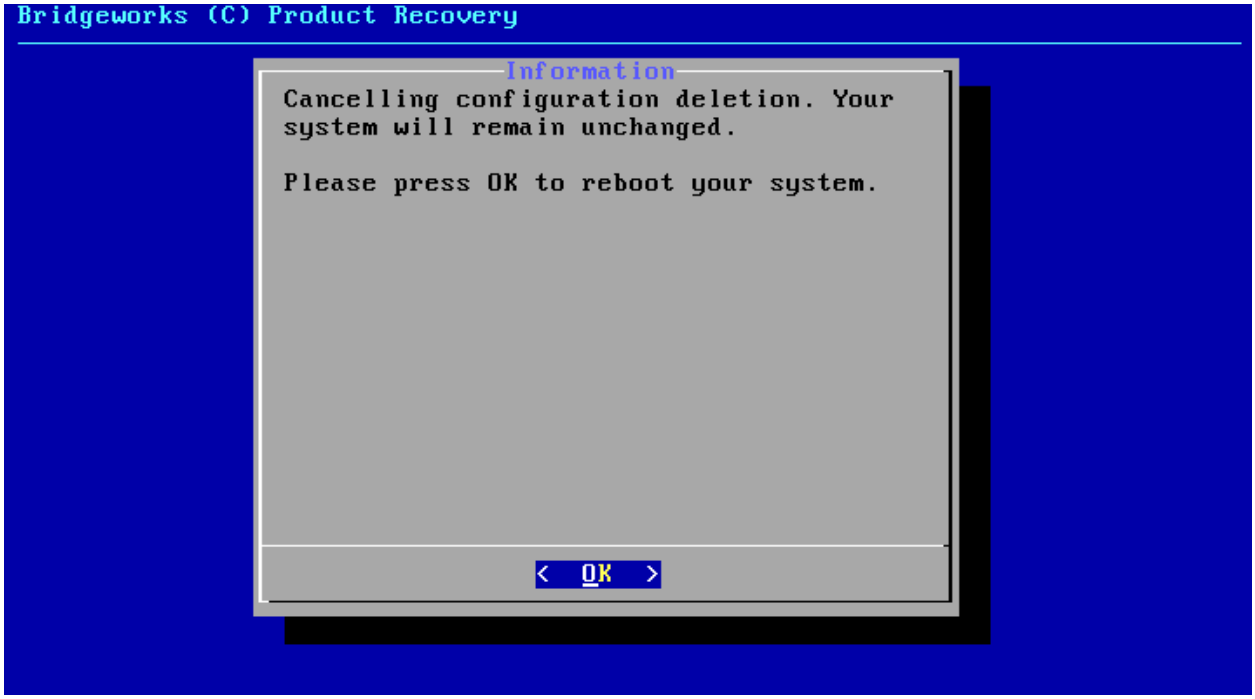


This procedure cannot be undone once complete; only continue if you are sure that you wish

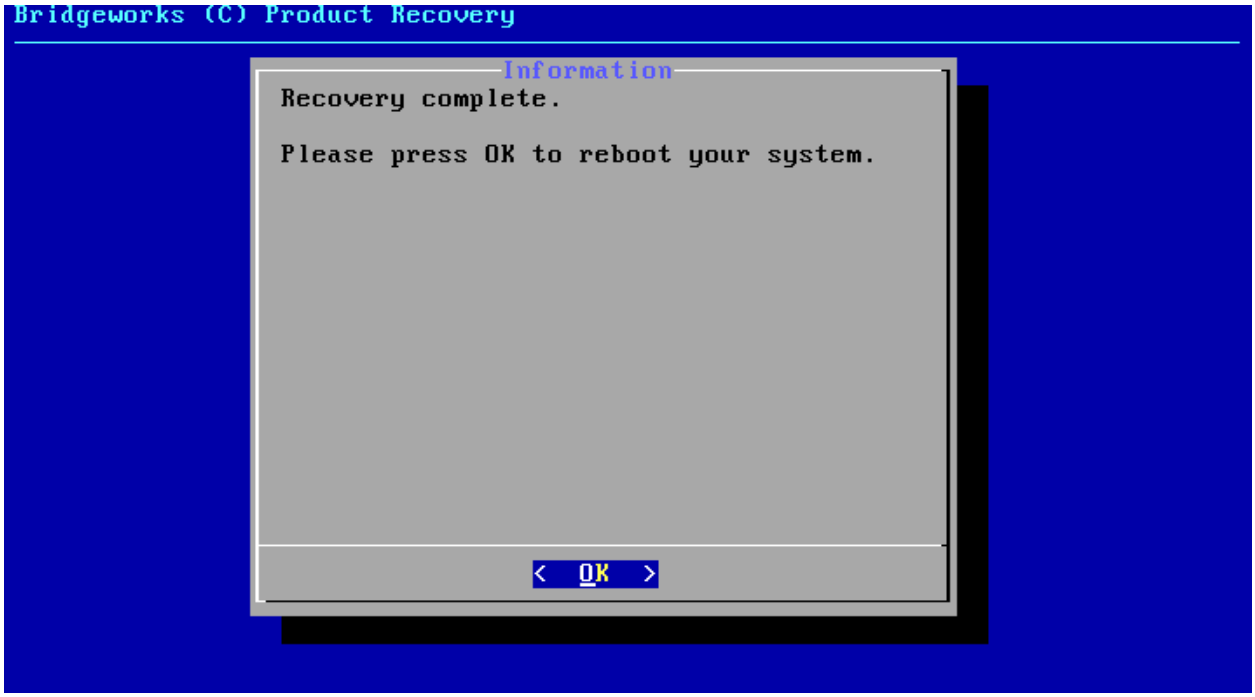
to do so. You will be asked to confirm that you wish to proceed. Choosing *Yes* will delete your configuration file and *No* will cancel the configuration deletion wizard.



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.

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.

Inbound LAN Protocols and Port Numbers

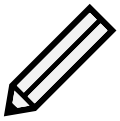
Protocol/Port	Name	Description
TCP 22	SSH	Required to access the configuration console through management interfaces when SSH is enabled. See Section 3.2.4: Secure Shell (SSH).
TCP 80	HTTP	Required to access the web interface through management interfaces when HTTP is enabled.
TCP 443	HTTPS	Required to access the web interface through management interfaces when HTTPS is enabled.
TCP 8002-8252		Required to access the remote web interface using Remote Control when HTTP is enabled on the controlling Node. One port is needed per Node being controlled remotely, with 8002 being the starting port, increasing incrementally with each Node added. See Section 4.5.16: 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: SNMP Agent.
UDP 28599		Required for the Node to respond to LAN Scan requests. See the LAN Scan guide found on the CD accompanying your PORTrockIT Node for more information.

Outbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 25	SMTP	Simple Mail Transfer Protocol, see Section 3.3.5: Simple Mail Transfer Protocol (SMTP).
UDP 123	NTP	Network Time Protocol, see Section 3.3.1: Simple Network Time Protocol.
UDP 2048	WCCP	Web Cache Communication Protocol. Allows accelerated traffic between nodes without endpoint configuration, see Section 4.5.15: WCCPv2.
ICMP		Internet Control Message Protocol. Required by dead gateway detection (see Section 3.1.3.4: Dead Gateway Detection) and network debugging tools (see Section 3.1.6: Network Tools).

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.

PORTrockIT TCP Port Numbers

Depending on the licences being used on the device, different TCP ports will need to be open for communication between the PORTrockIT Node and local Endpoint.

Caringo Swarm Object Storage

TCP Port/range	Description
80	Caringo Swarm Communication and Data Transfer

Commvault VM Backup and Recovery

TCP Port/range	Description
8400	Commvault Communications Service (GxCVD)
8401	Commvault Server Event Manager (GxEvMgrS)
8402	Commvault Client Event Manager (GxEvMgrC)
8403	Commvault Tunnel Communication
32768 - 65535	IANA standard Ephemeral port range

HTTP

TCP Port/range	Description
80	HTTP data transfer

HTTPS

TCP Port/range	Description
443	HTTPS data transfer

IBM Spectrum Protect

TCP Port/range	Description
1500	Inbound Client, server, admin
1501	Classic Scheduler listener for PROMPTED
1581	Web Client Listener

NetApp SnapMirror

TCP Port/range	Description
10565 - 10569	NetApp Data Transfer
11104	NetApp Intercluster Communication
11105	NetApp Intercluster Data Transfer

NetApp StorageGRID

TCP Port/range	Description
1139	LDR replication
1501	ADC service connection
1502	LDR service connection
1503	CMS service connection
1506	SSM service connection
1509	ARC service connection
1511	DDS service connection
7000	Cassandra inter-node cluster communication
7001	Cassandra SSL inter-node cluster communication
9042	Cassandra CQL Native Transport Port
9080	Used by all grid nodes to communicate with the primary Admin Node to coordinate when services are started
9081	StorageGRID Webscale Installer
9999	Metrics exporter
11139	ARC replication
18000	Account service connection
18001	Identity service connection
18002	Internal HTTP API connections from Admin Nodes and other Storage Nodes
18003	Platform services configuration service connections from Admin Nodes and other Storage Nodes
18080	HTTP query/retrieve and ingest

NFS

TCP Port/range	Description
111	NFS Service
2049	NFS Service

S3

TCP Port/range	Description
80	S3 data transfer
443	S3 encrypted data transfer

SecuritEase

TCP Port/range	Description
80	
443	
12000	
12001	

Veeam Backup & Replication

TCP Port/range	Description
902	Veeam Data Transmission to ESXi
2500 - 5000	Veeam Data Transmission
6160	Veeam Installer Service
6161	Veeam vPower NFS Service
6162	Veeam Data Mover Service

Veritas NetBackup

TCP Port/range	Description
1556	Symantec Private Branch Exchange Service
13722	Authorization Service (nbazd)
13724	NetBackup Network Service
13783	Authentication Service (nbatd)

WANdisco Fusion

TCP Port/range	Description
7000 - 7999	Data Transfer between Fusion Server and IHC servers
9000 - 9999	HTTP server that exposes JMX metrics from IHC servers

Web

TCP Port/range	Description
80	HTTP data transfer
443	HTTPS data transfer

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.

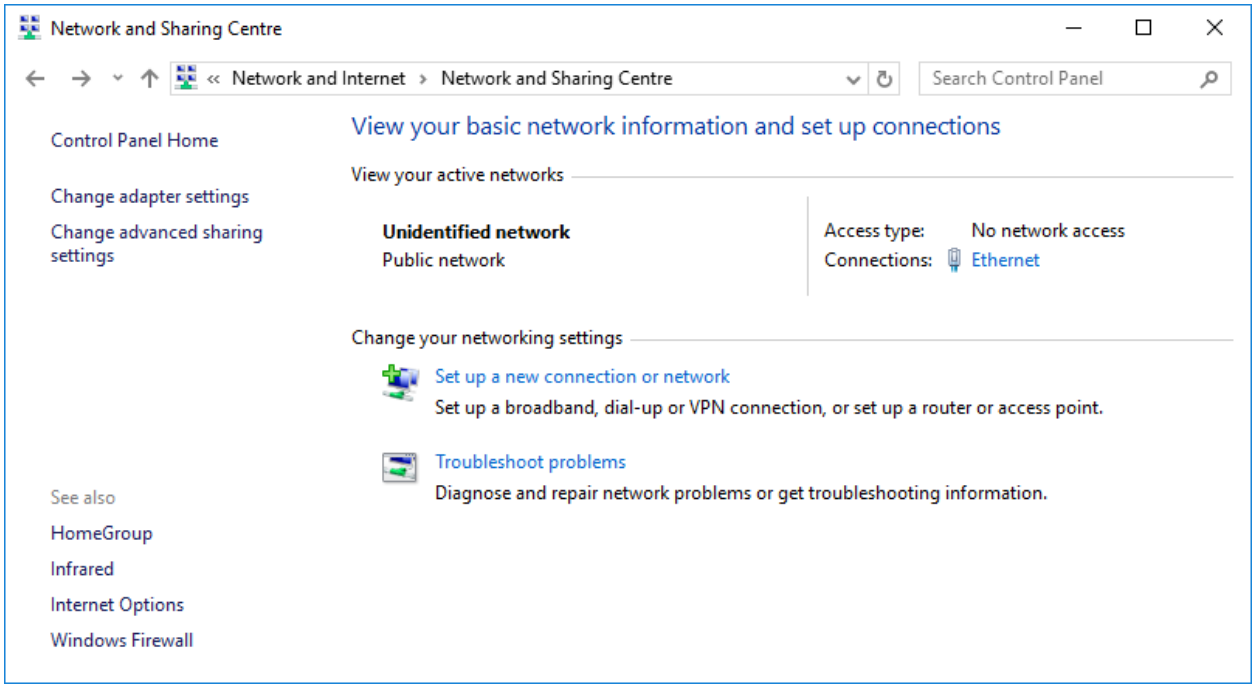
These instructions apply to Windows Vista, 7, 8, 10 and to Windows Server 2008, 2012, 2016, and their respective R2 versions.

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

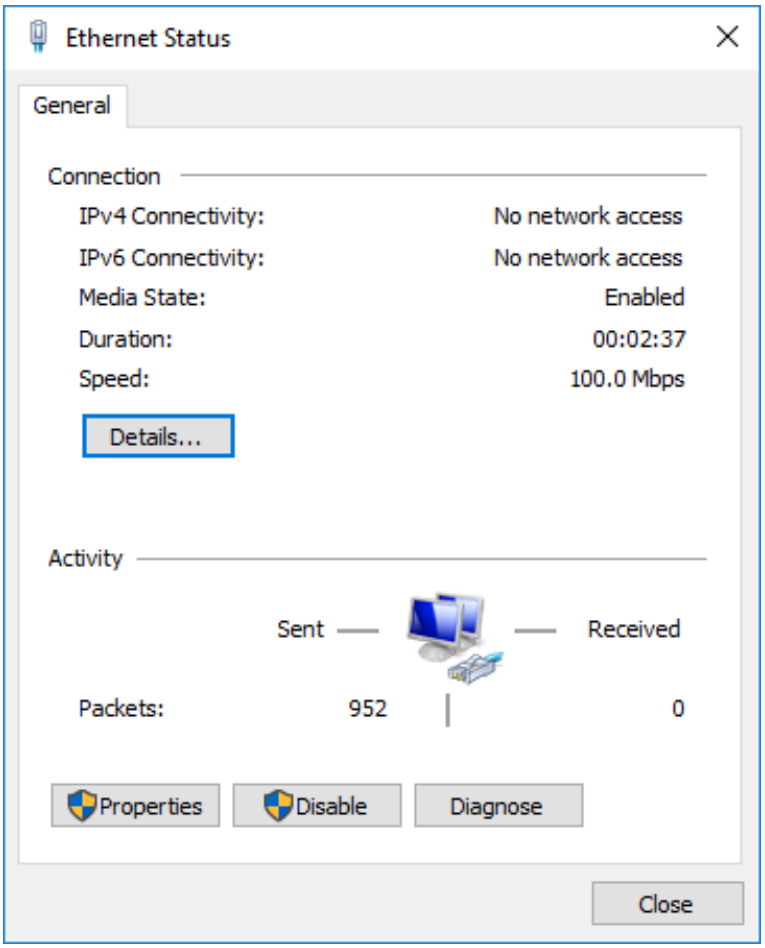
From the Start menu, select *Control Panel*.

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

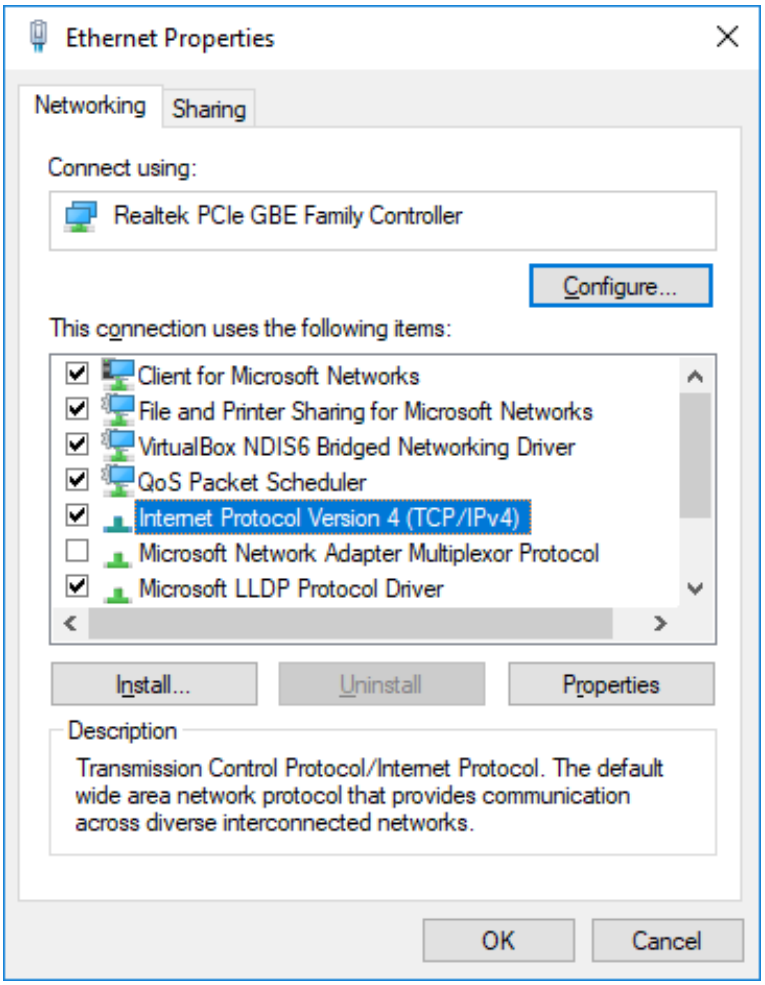
From the Control Panel select the *Network and Internet* link, followed by the *Network and Sharing Centre* link. Click on the link next to "Connections" for your respective network. This is named "Ethernet" in the screenshot below.



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

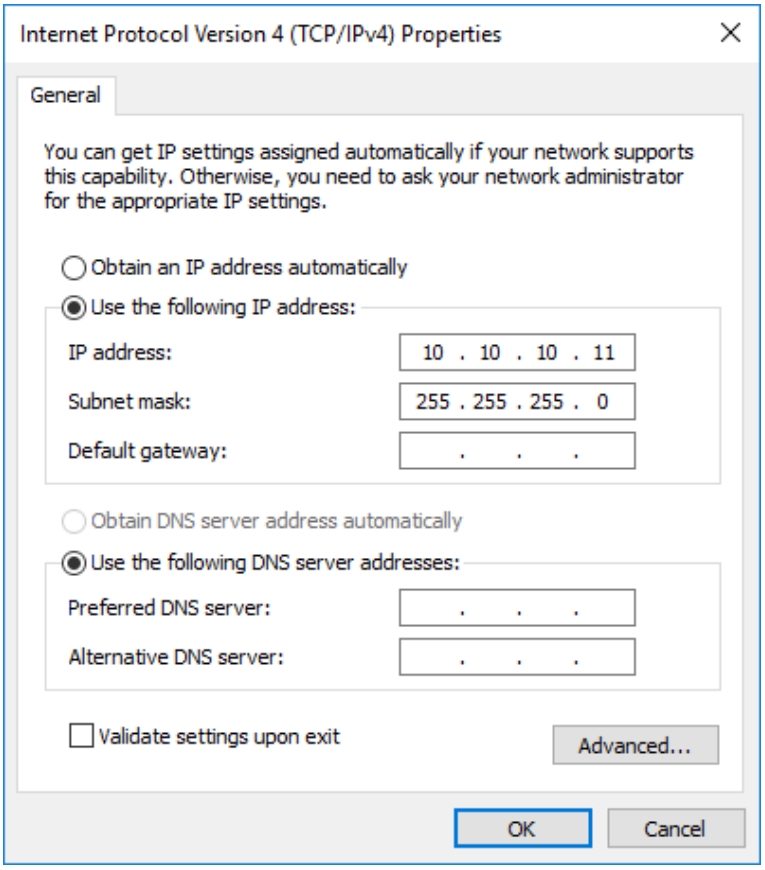


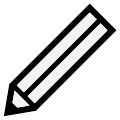
Select the *Internet Protocol Version 4 (TCP/IPv4)* entry and then *Properties*.



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.

PORTrockIT Series Comparisons

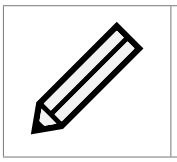
Determining the Series Number

The series number can be determined from the first digit of the PORTrockIT product code. For example, a 410 Node is part of the 400 series.

Number of Unique Protocols

Protocols can be applied to any port of the PORTrockIT, however for virtual instances the number of unique protocols that can be applied is limited.

The limit can be determined from the second digit of the PORTrockIT product code. For example, a 410 Node can have 1 unique protocol applied.



Note: WAN and Management capabilities do not count towards the unique protocol count.

Node Limits

Series	Bandwidth	Maximum Connected Nodes
50	50 MB/s	1
100	125 MB/s	1
200	250 MB/s	4
400	1 GB/s	10
800	Uncapped	250

Bandwidth The bandwidth limit applied to accelerated transfers.

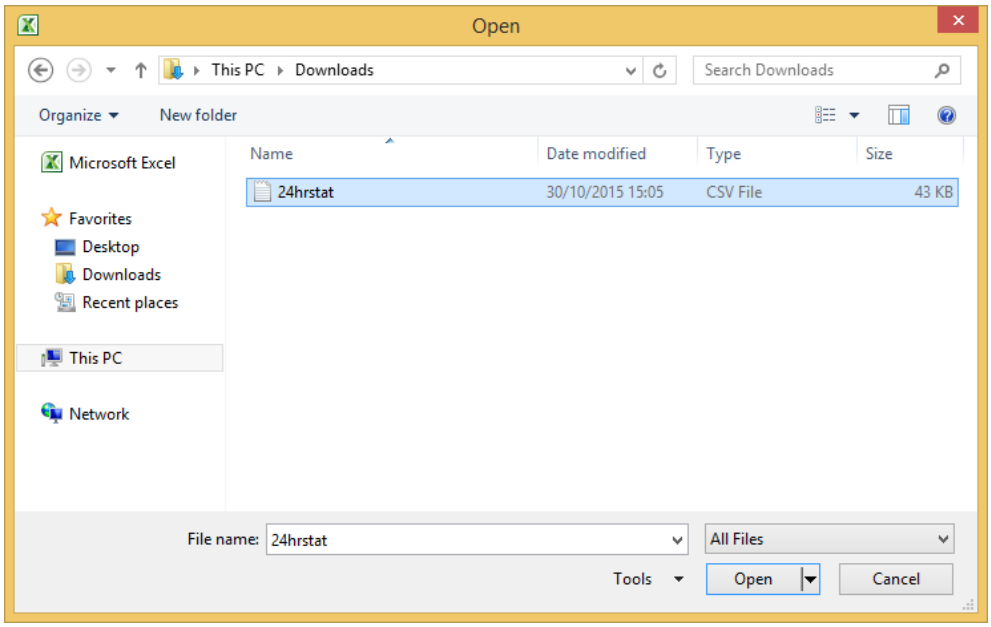
Maximum Connected Nodes The maximum number of Nodes that a Node may connect to.

Cloud Service Provider Nodes

Cloud Service Provider (CSP) Nodes are only permitted to connect to Cloud Nodes.

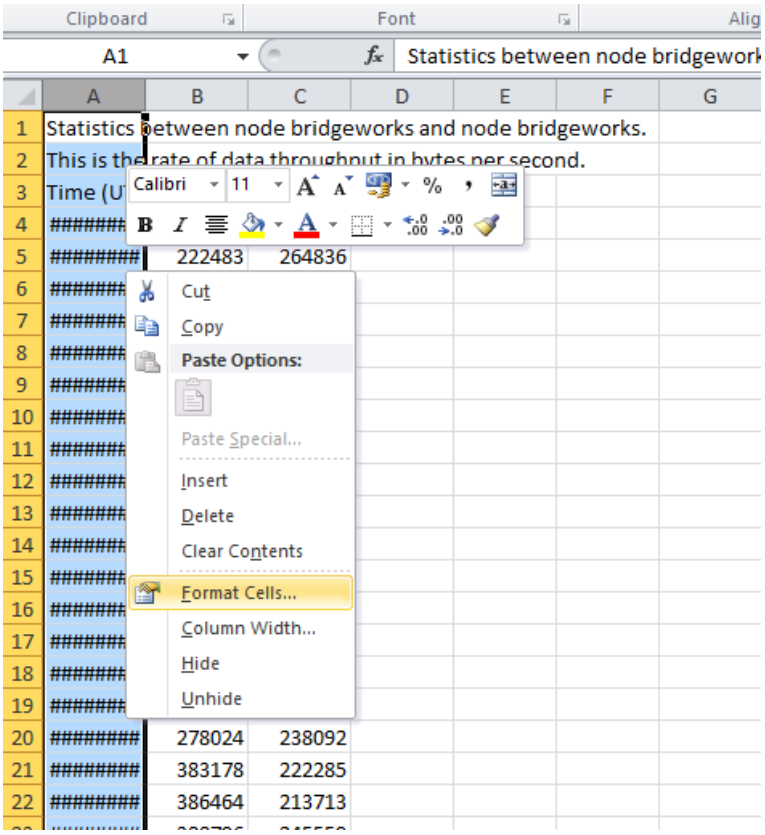
Transfer Statistics Graphing Instructions for Excel 2010

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:

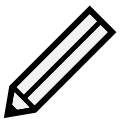


Note: For information on obtaining transfer statistics from your PORTrockIT Node, see Section 4.5.5.2: Download 24 Hour Transfer History.

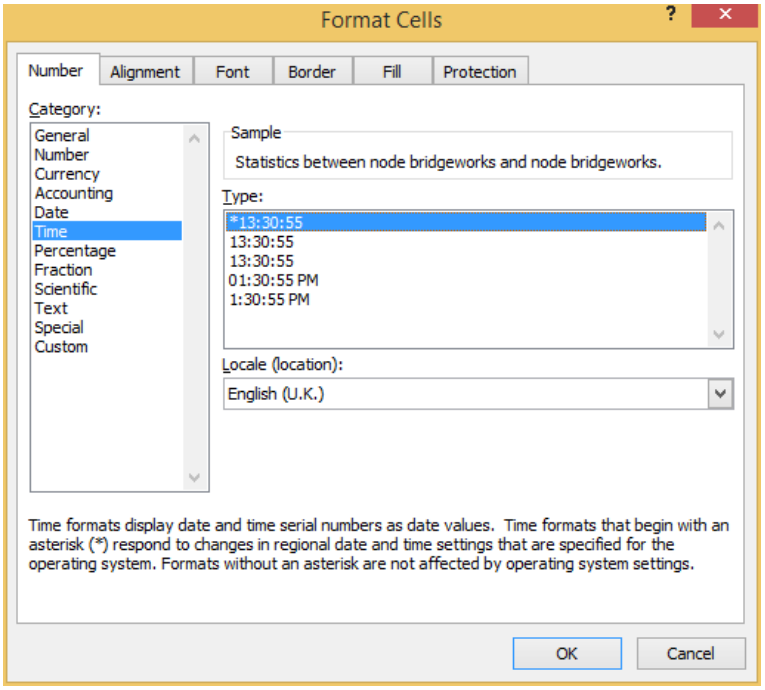
Select the *A* column of the newly generated worksheet, right-click, and select *Format Cells*.



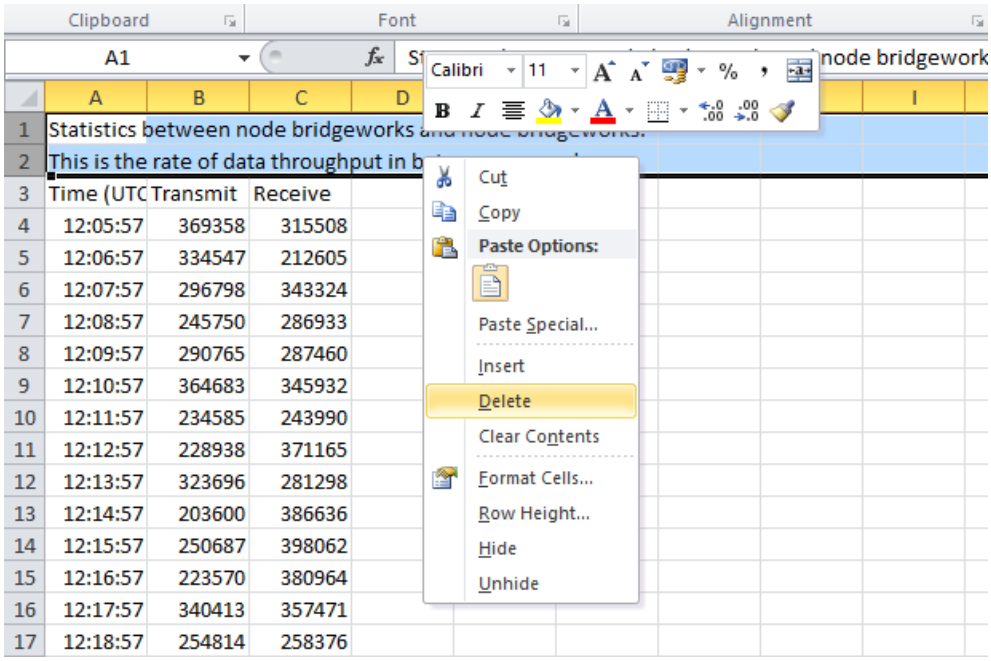
From the *Number* tab, select the *Time* category, and select the option `*13:30:55` as shown below then click *OK*.



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*.

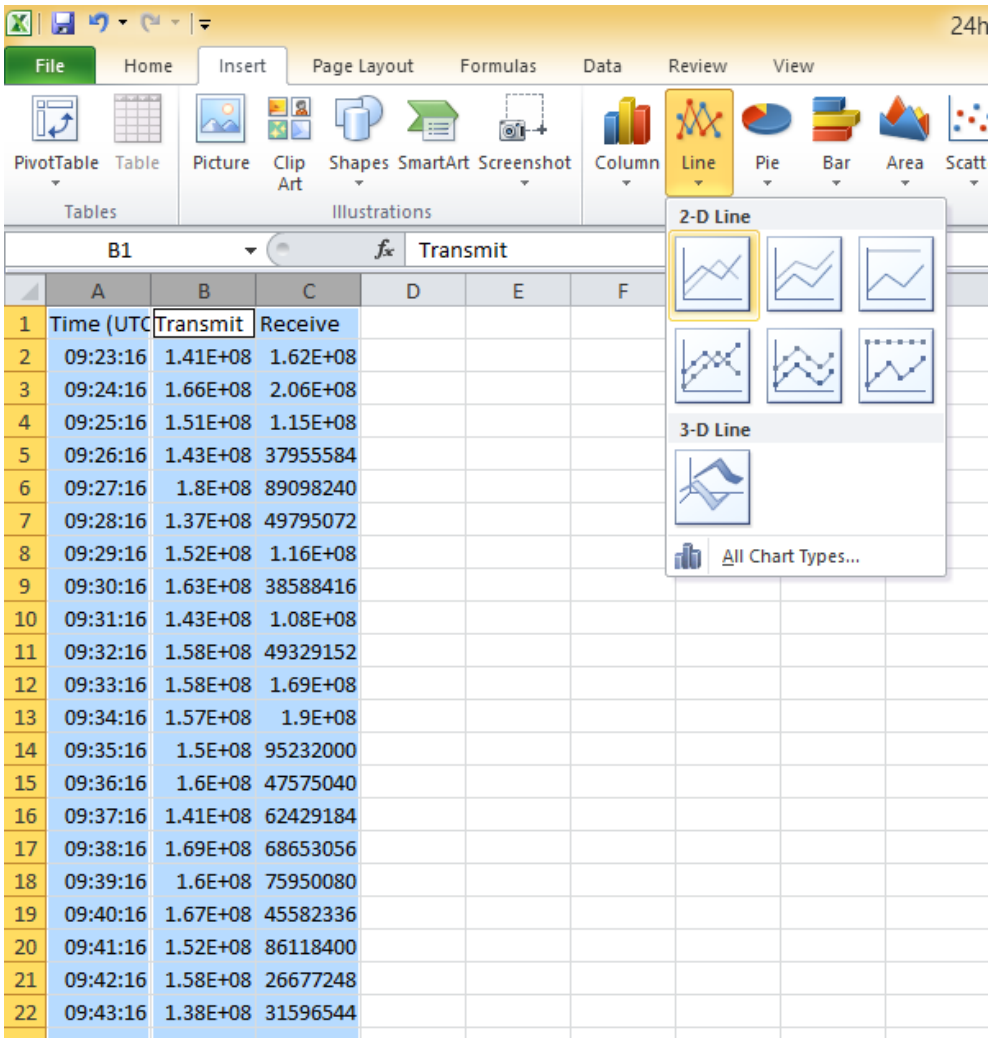


Select the first column by clicking on *A*. Then, hold down the `Ctrl` key on the keyboard and select the columns *B* and *C*. The three columns should now be selected as shown below:

	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			

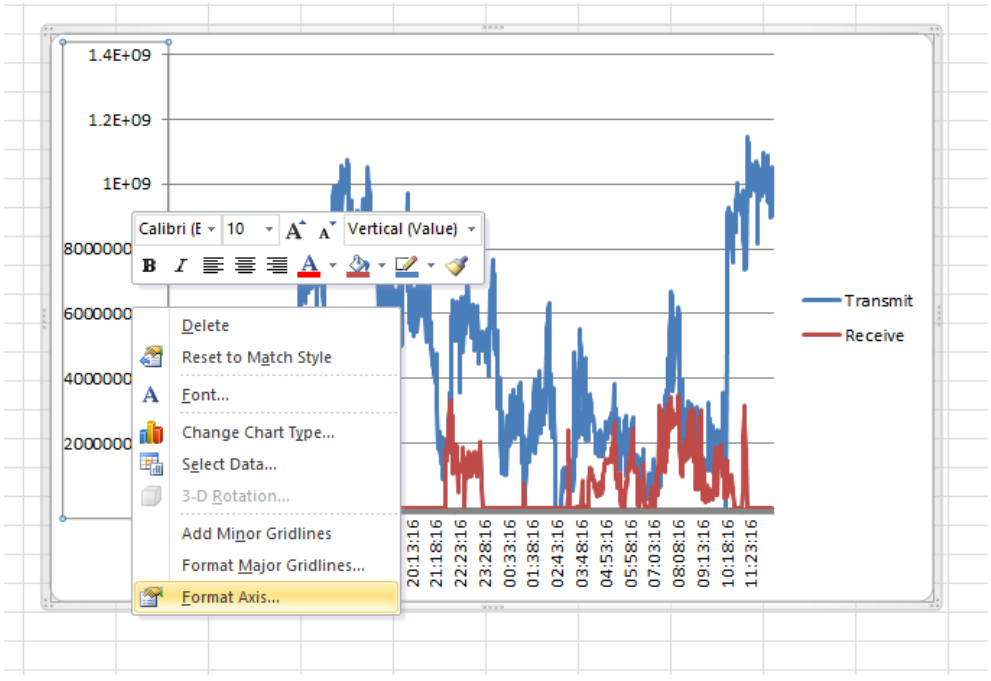
Warning: Selecting all three columns at the same time may cause errors in generating the graph in the following steps. Remember to select column *A* first and then the other two columns with the `Ctrl` key held down.

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



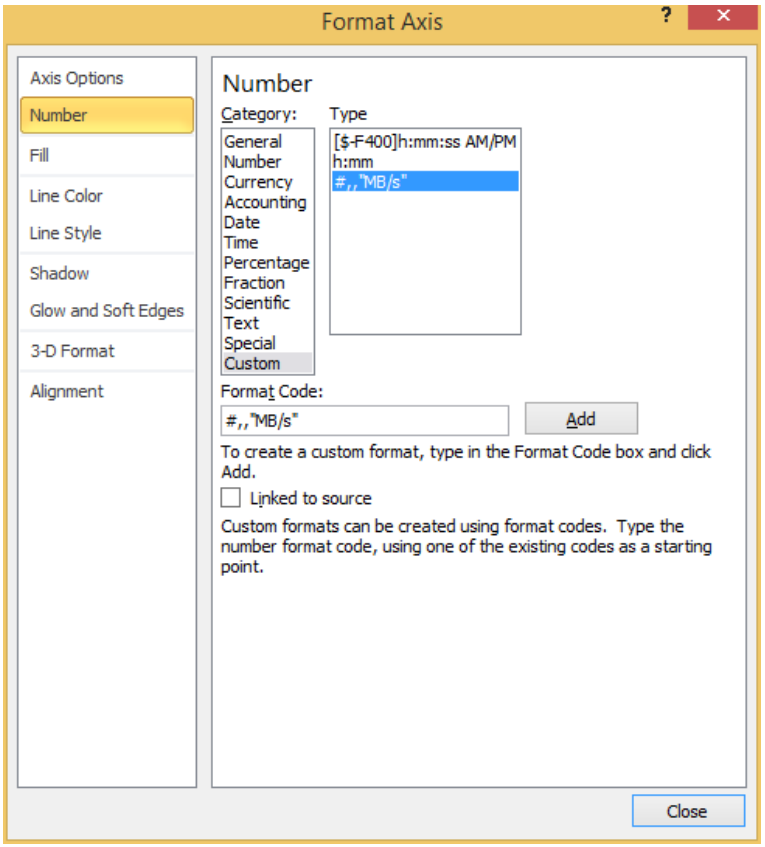
	A	B	C
1	Time (UTC	Transmit	Receive
2	09:23:16	1.41E+08	1.62E+08
3	09:24:16	1.66E+08	2.06E+08
4	09:25:16	1.51E+08	1.15E+08
5	09:26:16	1.43E+08	37955584
6	09:27:16	1.8E+08	89098240
7	09:28:16	1.37E+08	49795072
8	09:29:16	1.52E+08	1.16E+08
9	09:30:16	1.63E+08	38588416
10	09:31:16	1.43E+08	1.08E+08
11	09:32:16	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
19	09:40:16	1.67E+08	45582336
20	09:41:16	1.52E+08	86118400
21	09:42:16	1.58E+08	26677248
22	09:43:16	1.38E+08	31596544

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



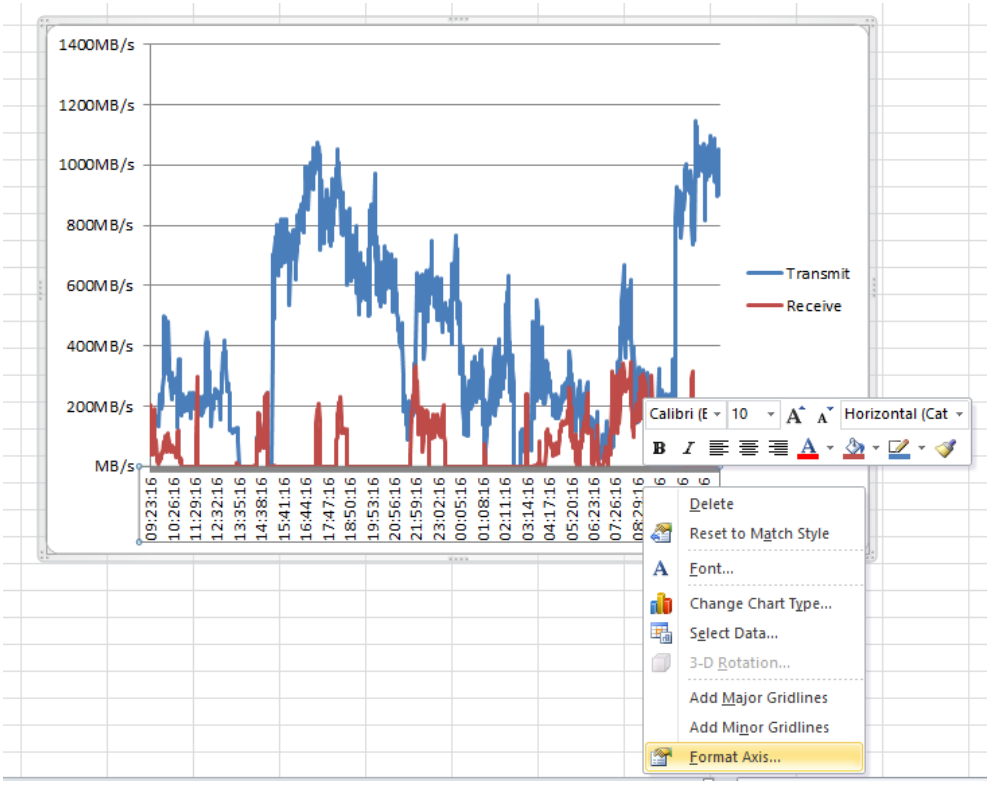
From the *Number* tab, select the *Custom* category. Enter the following in the *Format Code* field:

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

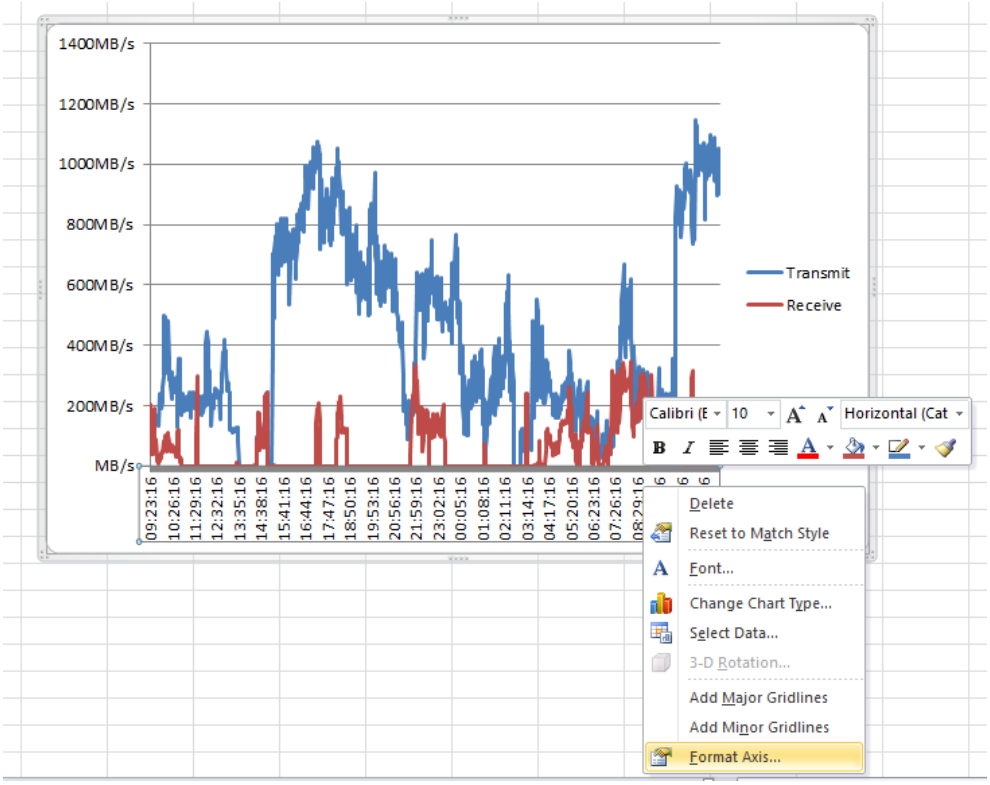


Click *Add*, then *Close*.

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

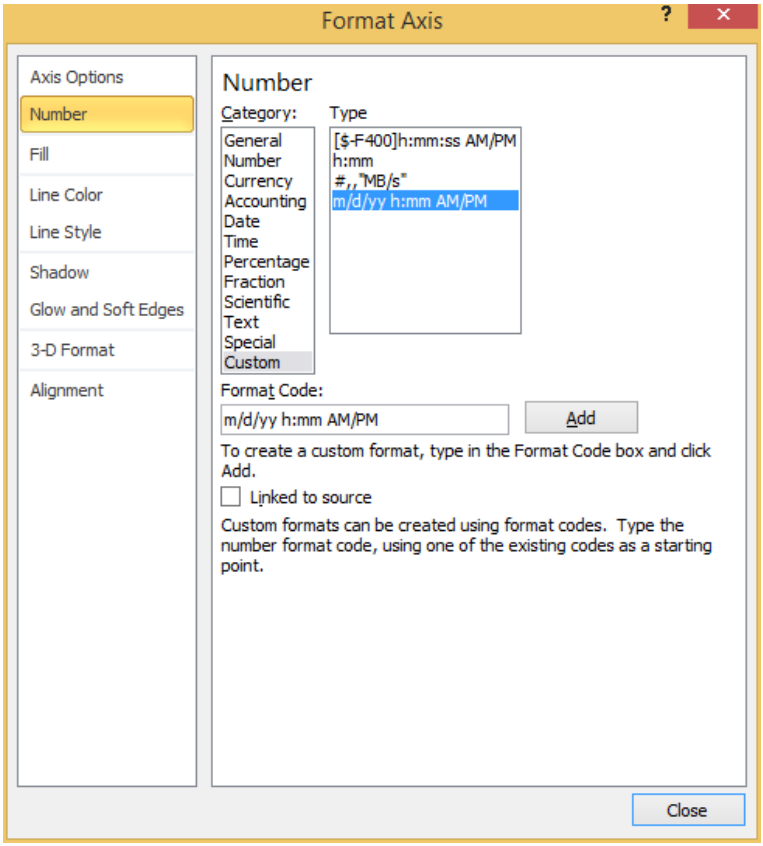


From the *Number* tab, select the *Time* category. Select the format you wish for the time to be displayed.

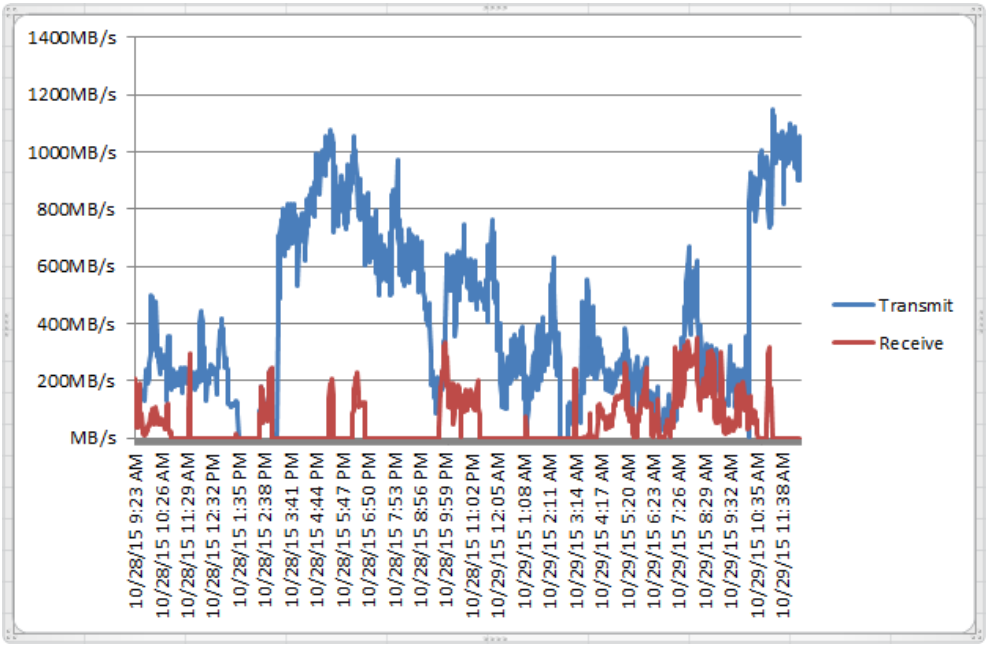


Alternatively, you can use a custom format for the date. In this case, select the *Custom* category, and enter your custom format in to the *Format Code* text field. The following is an example of a format code:

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



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



Useful Links

Frequently Asked Questions If you experience problems with the PORTrockIT 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 PORTrockIT 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/.

Firmware Downloads The latest software can be found at https://support.4bridgeworks.com/download-firmware/.